Martha Rzedowski Calderón

Departamento de Control Automático,
Centro de Investigación y de Estudios Avanzados del I.P.N.
mrzedowski@ctrl.cinvestav.mx

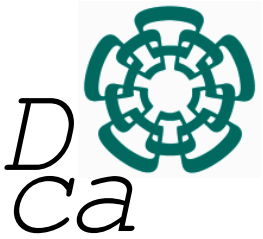
Gabriel Villa Salvador

Departamento de Control Automático,
Centro de Investigación y de Estudios Avanzados del I.P.N.
gvillasalvador@gmail.com, gvilla@ctrl.cinvestav.mx

Campos de Clase

Campos locales y campos globales

22 de diciembre de 2022



Departamento de Control Autómatico

Centro de Investigación y de Estudios Avanzados del I.P.N.

México D. F.

Índice general

1

Introducción

La teoría de campos de clase es esencialmente el estudio de las extensiones abelianas, en general finitas, aunque también se estudian las extensiones infinitas, de cuatro clases de campos: campos globales (campos numéricos y campos de funciones) y campos locales (de igual característica y de característica distinta). En primera instancia, no es así como se definen los campos de clase, sino más bien de otras formas (campos en donde un cierto conjunto de primos se descomponen totalmente o subgrupos de ciertos grupos que son normas, etc.), lo cual lleva, al final del día, a que es lo mismo que extensiones abelianas finitas.

Hay otros objetos los cuales pueden ser estudiados con la teoría de campos de clase que no están comprendidas en las cuatro anteriores: ciertos campos de funciones no congruentes. También hay una teoría de campos de clase no abeliana: el programa de Langlands. No haremos más historia de la teoría de campos de clase pues nos reservamos esto para la Subsección 2.5.

El objetivo de este capítulo es presentar los resultados fundamentales de la teoría de campos de clase con la profundidad necesaria para poder aplicarla a la teoría de números algebraica, principalmente para campos de funciones. Una opción pudiera haber sido presentar la teoría de campos de clase para campos numéricos desde el punto de vista de ideales. Un magnífico libro con este enfoque es el libro de Janusz [82]. Sin embargo esta aproximación no nos diría cuáles son las diferencias con respecto a los campos de funciones que son nuestro interés primario.

Para los lectores interesados en las demostraciones y desarrollos completos de la teoría de clase, hay muchos textos excelentes, tanto para campos globales como para locales y algunos de ellos para ambos. El texto fundamental es el trabajo de Artin–Tate [7]. Para campos locales podemos indicar los libros de Iwasawa y de Serre [77, 151] así como el artículo de Serre [150] comprendido en el libro cuyos editores son Cassels y Frölich [22]. Para campos globales podemos mencionar el artículo de Tate [157] el cual también se encuentra en el libro de Cassels y Frölich. Para el estudio de ambos casos, el local y el

global, debemos mencionar los libros de Neukirch [117, 119, 120] y el libro de Chevalley [25]. Tratados más clásicos son los trabajos de Hasse [52, 55, 56].

En la Sección 2 presentamos algunos preliminares aislados que ayudan a comprender el trabajo subsiguiente. Estos preliminares constan fundamentalmente de la teoría de Kummer, el automorfismo de Frobenius y el símbolo de Artin. La Subsección 2.5 tiene como objeto presentar una panorámica general de la historia de la teoría de campos de clase. Esta subsección es muy útil para el lector cuando esté leyendo los capítulos posteriores, pues puede consultar en que contexto los resultados fueron apareciendo y su razón de ser. Hay muchas referencias para esta parte pero nos basamos fundamentalmente en el magnífico artículo de Conrad [30]. Otras referencias estupendas son el artículo de Hasse [57] en el libro de Cassels y Frölich y los artículos y libros de Roquette [127, 128, 129].

La Sección 3 da un rápido repaso a la teoría de campos locales. En la Sección 4 estudiamos la cohomología de grupos que es el enfoque que damos para la teoría de campos de clase. La Sección 5 estudia la teoría local de campos de clase con énfasis en los grupos de Lubin–Tate. Decidimos presentar en la Subsección 5.4 la teoría de Neukirch [119] sobre el isomorfismo que lleva su nombre y el cual obtiene, con otro enfoque distinto a la de cohomología de grupos, el teorema de reciprocidad. Este mismo isomorfismo se puede aplicar a campos globales. Este subsección puede omitirse sin pérdida de continuidad.

La Sección 6 es la teoría global de campos de clase. El teorema de existencia es el tema de la Sección 6.8. La Sección 7 estudia los grupos de congruencias que transparentan un poco la correspondencia dada por el teorema de reciprocidad de Artin. En la Subección 7.1 estudiamos la teoría de campos de clase en campos numéricos, primero con del enfoque de idèles y posteriormente en la Subsección 7.4 con el enfoque de ideales y divisores. La Subsección 7.3 comprende de manera central el estudio de los campos de clase de Hilbert y de Hilbert extendido en campos de funciones. Finalizamos con un estudio de los campos de géneros desde el punto de vista de campos de clase en la Sección 8.

2

Preliminares y antecedentes

En esta primera parte, presentamos varios temas que ya sea son necesarios para el desarrollo de estas notas, o bien porque son partes de las demostraciones, posiblemente no presentadas aquí, de los teoremas fundamentales de la teoría.

2.1. Extensiones de Kummer y de Artin–Schreier

En esta sección estudiaremos las llamadas *extensiones de Kummer* y las *extensiones de Artin–Schreier*. Estas últimas pueden ser consideradas las extensiones de Kummer aditivas. Las extensiones de Kummer juegan un papel preponderante para los teoremas de existencia de campos de clase para las extensiones cíclicas de orden primo relativo a la característica y las extensiones de Artin–Schreier son usadas con el mismo fin en el caso de campos de funciones para extensiones cíclicas de grado igual a la característica. Nosotros no presentaremos todos los detalles de la demostración de los teoremas de existencia desde este punto de vista, pero si el lector quiere profundizar más en los detalles de las demostraciones de los teoremas de existencia, es necesario aplicar este tipo de extensiones.

Teorema 2.1.1 (Teorema de independencia de Artin). *Sean G un grupo multiplicativo, F un campo y $\sigma_1, \sigma_2, \ldots, \sigma_n$, n homomorfismos de grupos distintos de G en F^*. Entonces $\sigma_1, \sigma_2, \ldots, \sigma_n$ son independientes, es decir, si $a_1, \ldots, a_n \in F$ son tales que*

$$a_1\sigma_1(x) + a_2\sigma_2(x) + \cdots + a_n\sigma_n(x) = 0$$

para todo $x \in G$, entonces $a_1 = a_2 = \ldots = a_n = 0$.

Demostración. [92, Ch. IV, Section 4,Theorem 4.1]. □

Una aplicación del Teorema 2.1.1 es para el caso en que L es un campo arbitrario y $\sigma_1, \ldots, \sigma_n$ son distintos automorfismos de L. Entonces $\sigma_1, \ldots, \sigma_n$ son independientes. En este caso se toma $G = L^*$.

Teorema 2.1.2. *Sea L/K una extensión cíclica de grado n y sea $G = \mathrm{Gal}(L/K) = \langle\sigma\rangle$. Sea $\alpha \in L$. Entonces*

(a) $\mathrm{Tr}_{L/K}\,\alpha = 0 \iff$ *existe $\beta \in L$ tal que $\alpha = \beta - \sigma\beta$, donde $\mathrm{Tr}_{L/K} = \mathrm{Tr}$ denota la traza de L a K.*
(b) $\mathrm{N}_{L/K}\,\alpha = 1 \iff$ *existe $\beta \in L$ tal que $\alpha = \beta/\sigma\beta$, donde $\mathrm{N}_{L/K} = \mathrm{N}$ denota la norma de L a K.*

Demostración. (a) $\Leftarrow$) Si $\alpha = \beta - \sigma\beta$, entonces

$$\mathrm{Tr}_{L/K}\,\alpha = \mathrm{Tr}_{L/K}\,\beta - \mathrm{Tr}_{L/K}(\sigma\beta) = \mathrm{Tr}_{L/K}\,\beta - \mathrm{Tr}_{L/K}\,\beta = 0.$$

$\Rightarrow$) Puesto que L/K es separable, por el Teorema 2.1.1 se tiene que existe $\gamma \in L$ tal que $\mathrm{Tr}_{L/K}\,\gamma = a \neq 0$ con $a \in K$ (de hecho, L/K es separable $\iff \mathrm{Tr} \neq 0$). Por tanto $\mathrm{Tr}_{L/K}(a^{-1}\gamma) = a^{-1}\,\mathrm{Tr}_{L/K}\,\gamma = 1$.

Sea $\alpha \in L$ tal que $\mathrm{Tr}_{L/K}\,\alpha = 0$. Entonces $\sigma^0\alpha = \alpha = -\sum_{j=1}^{n-1}\sigma^j\alpha$. Sea $\beta = \sum_{i=0}^{n-2}\Big(\sum_{j=0}^{i}\sigma^j\alpha\Big)\sigma^i\gamma_1$ con $\mathrm{Tr}_{L/K}\,\gamma_1 = 1$. Entonces $\beta - \sigma\beta = \alpha$.
(b) $\Leftarrow$) Si $\alpha = \beta/\sigma\beta$, $\mathrm{N}\,\alpha = \mathrm{N}\,\beta/\,\mathrm{N}(\sigma\beta) = \mathrm{N}\,\beta/\,\mathrm{N}\,\beta = 1$.
$\Rightarrow$) Sea ahora $\mathrm{N}_{L/K}\,\alpha = 1$. Consideremos

$$\begin{aligned}\xi :&= c + \alpha\sigma(c) + \alpha\sigma(\alpha)\sigma^2(c) + \cdots + \alpha\sigma(\alpha)\cdots\sigma^{n-2}(\alpha)\sigma^{n-1}(c)\\ &= c + \sum_{j=1}^{n-1}\Big(\prod_{i=0}^{j-1}\sigma^i(\alpha)\Big)\sigma^j(c)\end{aligned}$$

con $c \in L$. Entonces

$$\begin{aligned}\alpha\sigma(\xi) &= \alpha\sigma(c) + \sum_{j=1}^{n-1}\Big(\prod_{i=0}^{j-1}\alpha\sigma^{i+1}(\alpha)\Big)\sigma^{j+1}(c)\\ &= \underset{\uparrow\; j=1}{\alpha\sigma(c)} + \sum_{j=2}^{n-1}\Big(\prod_{i=0}^{j-1}\sigma^i(\alpha)\Big)\sigma^j(c) + \Big(\underset{\quad\;\|\;1}{\prod_{i=0}^{n-1}\sigma^i(\alpha)}\Big)\,\underset{\quad\;\|\;c}{\sigma^n(c)}\\ &= c + \sum_{j=1}^{n-1}\Big(\prod_{i=0}^{j-1}\sigma^i(\alpha)\Big)\sigma^j(c) = \xi.\end{aligned}$$

Esto es, $\alpha\sigma(\xi) = \xi$. Por el Teorema 2.1.1, existe c tal que $\xi = \beta \neq 0$ y se tiene $\alpha\sigma(\beta) = \beta$ por lo que $\alpha = \beta/\sigma(\beta)$. □

Teorema 2.1.3 (Extensiones de Artin–Schreier). *Sea K un campo de característica $p > 0$, $\operatorname{car} K = p$. Entonces L/K es una extensión cíclica de grado $p \iff$ existe $z \in L$ tal que $L = K(z)$ e $\operatorname{Irr}(z, T, K) = T^p - T - a \in K[T]$ y, en particular, $z^p - z = a$.*

Demostración. $\Rightarrow$) Sea $G := \operatorname{Gal}(L/K) = \langle\sigma\rangle$, $o(\sigma) = p$. Se tiene $\operatorname{Tr}_{L/K} 1 = p = 0$. Por tanto existe $z \in L$ tal que $\sigma z - z = 1$, esto es, $\sigma z = z+1$. Se sigue que $\sigma^i z = z + i$ y $\sigma^i z = z \iff p|i$. Por lo tanto $\operatorname{Irr}(z, T, K) = \prod_{i=0}^{p-1}(T - (z + i))$ es de grado p.

Se tiene $\sigma(z^p - z) = (\sigma z)^p - (\sigma z) = (z + 1)^p - (z + 1) = z^p - z$ de donde obtenemos que $z^p - z = a \in K$ y $z^p - z - a = 0$. Por lo tanto $\operatorname{Irr}(z, T, K) = T^p - T - a = \prod_{i=0}^{p-1}(T - (z + i))$.
$\Leftarrow$)Si $L = K(z)$ e $\operatorname{Irr}(z, T, K) = T^p - T - a$, entonces para toda $i \in \mathbb{Z}$ setiene $i^p \equiv i$ mód p y $(z + i)^p - (z + i) = z^p + i^p - z - i = z^p - z = a$. Se sigue que $z, z+1, \ldots, z+(p-1)$ son los raíces de $\operatorname{Irr}(z, T, K)$. En particular z y $z+1$ son conjugados sobre K y $L = K(z)$ es de Galois sobre K. Sean $G = \operatorname{Gal}(L/K)$ y $\sigma \in G$ tal que $\sigma z = z + 1$, de donde $\sigma^i z = z + i$ y $o(\sigma) = p$ por lo que se tiene $G = \langle\sigma\rangle$ es un grupo cíclico de orden p. □

Teorema 2.1.4 (Extensiones de Kummer). *Sea K un campo de característica $p \geq 0$ y sea $n \in \mathbb{N}$ tal que $p \nmid n$ (en el caso $p = 0$, n es arbitrario). Supongamos que $\zeta_n \in K$ donde ζ_n es una raíz n–ésima primitiva de la unidad. Entonces L/K es una extensión cíclica de grado $n \iff$ existe $z \in L$ tal que $L = K(z)$ e $\operatorname{Irr}(z, T, K) = T^n - a \in K[T]$, esto es, $L = K(\sqrt[n]{a})$.*

Demostración. $\Rightarrow$) Sea $G = \operatorname{Gal}(L/K) = \langle\sigma\rangle$, $o(\sigma) = n$. Se tiene $\operatorname{N}\zeta_n = \zeta_n^n = 1$. Por lo tanto existe $z \in L$ tal que $\sigma z = \zeta_n z$ y $\sigma^i z = \zeta_n^i z$, por lo que $\sigma^i z = z \iff n|i$. Por lo tanto $z, \zeta_n z, \ldots, \zeta_n^{n-1} z$ son los distintos conjugados de z. Se sigue que $\operatorname{Irr}(z, T, K) = \prod_{i=0}^{n-1}(T - \zeta_n^i z)$.

Por otro lado $\sigma z^n = (\sigma z)^n = (\zeta_n z)^n = \zeta_n^n z^n = z^n$, esto es, $z^n = a \in K$ y $z, \zeta_n z, \ldots, \zeta_n^{n-1} z$ son raíces de $T^n - a \in K[T]$. Por lo tanto $\operatorname{Irr}(z, T, K) = T^n - a$ y $z^n = a$.
$\Leftarrow$) Para $a \neq 0$, $T^n - a$ es un polinomio separable debido a que $p|n$ y tiene distintas raíces $z, \zeta_n z, \ldots, \zeta_n^{n-1} z$ donde $z \in \bar{K}$ es tal que $z^n = a$, donde $\bar{K}$ es una cerradura algebraica de K. Se sigue que $L = K(z)$ es una extensión de Galois. Puesto que se supone que $T^n - a$ es irreducible y z y $\zeta_n z$ son conjugados. Por lo tanto existe $\sigma \in G = \operatorname{Gal}(L/K)$ tal que $\sigma z = \zeta_n z$. Por tanto $o(\sigma) = n = o(G) = [L : K]$ de donde se sigue que L/K es una extensión cíclica de grado n. □

Teorema 2.1.5. *Sea K tal que $\operatorname{car} K = p > 0$ y sean $L_i = K(z_i)/K$, $i = 1, 2$ dos extensiones cíclicas de grado p dadas por $z_i^p - z_i = a_i \in K$, $i = 1, 2$. Lo siguiente es equivalente*

(1) $L_1 = L_2$.
(2) $z_1 = j z_2 + b$ *para* $1 \leq j \leq p - 1$ *y* $b \in K$.

(3) $a_1 = ja_2 + (b^p - b) = ja_2 + \wp(b)$ *para* $1 \leq j \leq p-1$ *y* $b \in K$.
Aquí usamos la notación $\wp(b) = b^p - b$.

Demostración. (1) $\Leftrightarrow$ (2). Si $z_1 = jz_2 + b$, entonces $z_2 = iz_1 - ib$ con $ij \equiv 1 \bmod p$, por lo que $L_1 = L_2$. Recíprocamente, si $L_1 = L_2$, entonces si $G = \mathrm{Gal}(L_1/K) = \mathrm{Gal}(L_2/K) = \langle\sigma\rangle$ donde seleccionamos σ tal que $\sigma z_1 = z_1 + 1$. Ahora bien, puesto que σz_2 es conjugado de z_2 sobre K, entonces existe $1 \leq i \leq p-1$ tal que $\sigma z_2 = z_2 + i$. Sea $1 \leq j \leq p-1$ tal que $ij \equiv 1 \bmod p$. Entonces

$$\sigma(jz_2) = j\sigma(z_2) = jz_2 + ji = jz_2 + 1.$$

Por tanto $\sigma(z_1 - jz_2) = z_1 - jz_2$, por lo que $z_1 - jz_2 = b \in K$.
(2) $\Rightarrow$ (3) : Ahora si $z_1 = jz_2 + b$ se tiene $z_1^p - z_1 = a_1 = (jz_2+b)^p - (jz_2+b) = j(z_2^p - z_2) + \wp(b) = ja_2 + \wp(b)$.
(3) $\Rightarrow$ (2) : Recíprocamente, si $a_1 = ja_2 + \wp(b)$, $z_1^p - z_1 = (jz_2+b)^p - (jz_2+b)$, es decir, $(z_1 - (jz_2+b))^p - (z - (jz_2+b)) = 0$, por lo tanto $\omega = z_1 - jz_2 - b$ es una raíz de $\omega^p - \omega = 0$ por lo que $\omega \in \mathbb{F}_p$. Se sigue que $z_1 = jz_2 + b + \omega$ y $\wp(b+\omega) = \wp(b)$, por lo que $a_1 = ja_2 + \wp(b+\omega)$. □

Similarmente se puede probar

Teorema 2.1.6. *Sea* K *un campo de característica* $p \geq 0$ *tal que* $\zeta_n \in K$ *con* $p \nmid n$ *y* ζ_n *una raíz* n*–ésima primitiva de la unidad. Sean* $L_i = K(z_i)$, $i = 1, 2$, *dos extensiones cíclicas de* K *de grado* n *dadas por* $z_i^n = a_i \in K$. *Entonces lo siguiente es equivalente:*

(1) $L_1 = L_2$.
(2) $z_1 = z_2^j c$ *para algún* $1 \leq j \leq n-1$ *con* $\mathrm{mcd}(j, n) = 1$ *y* $c \in K$.
(3) $a_1 = a_2^j c^n$ *para algún* $1 \leq j \leq n-1$ *tal que* $\mathrm{mcd}(j, n) = 1$ *y* $c \in K$.
□

Con respecto a la ramificación en las extensiones de Kummer y de Artin–Schreier, los siguientes dos resultados se deben a Hasse. En este caso se tiene K/k un campo de funciones y supondremos k perfecto (en general consideraremos el caso $k = \mathbb{F}_q$, el cual es perfecto). Se tiene:

Teorema 2.1.7 (H. Hasse). *Sea* k *un campo perfecto de característica* $p > 0$ *y sea* $\mathfrak{p}$ *un lugar fijo de* K. *Si* L/k *es una extensión cíclica de grado* p, *entonces existe* $y \in L$ *tal que* $L = K(y)$ *con* $y^p - y = a$ *tal que, o bien* $v_{\mathfrak{p}}(a) \geq 0$, *o bien* $v_{\mathfrak{p}}(a) = -\lambda < 0$ *y* $p \nmid \lambda$.

Si $v_{\mathfrak{p}}(a) \geq 0$, *entonces* $\mathfrak{p}$ *es no ramificado. Si* $v_{\mathfrak{p}}(a) = -\lambda < 0$ *y* $p \nmid \lambda$, *entonces* $\mathfrak{p}$ *es ramificado y el diferente local está dado por* $\mathfrak{D}_{\mathfrak{P}} = \mathfrak{P}^{(\lambda+1)(p-1)}$ *donde* $\mathfrak{P}$ *es el lugar de* L *encima de* $\mathfrak{p}$, *es decir,* $\mathfrak{p} = \mathfrak{P}^p$.

Demostración. Ver cite[Theorems 5.8.10 y 5.8.11]Vil2006. □

Teorema 2.1.8 (H. Hasse). *Sea k un campo de característica $p \geq 0$. Sea L/K una extensión cíclica de grado n con $p \nmid n$ y tal que $\zeta_n \in k$ donde ζ_n es una raíz n–ésima primitiva de la unidad. Sea $\mathfrak{p}$ un lugar fijo de K. Entonces $L = K(y)$ tal que $y^n = a$ con $0 \leq v_{\mathfrak{p}}(a) \leq n-1$. Se tiene que $\mathfrak{p}$ es no ramificado en $L/K \iff v_{\mathfrak{p}}(a) = 0$.*

Si $v_{\mathfrak{p}}(a) = m > 0$ y $\mathfrak{P}$ es un divisor de L encima de $\mathfrak{p}$, tenemos $e(\mathfrak{P}|\mathfrak{p}) = \frac{n}{\mathrm{mcd}(n,m)}$ y $v_{\mathfrak{P}}(\mathfrak{D}_{\mathfrak{P}}) = \frac{n}{\mathrm{mcd}(n.m)} - 1$, donde $\mathfrak{D}_{\mathfrak{P}}$ denota al diferente local.

Demostración. [160, Theorem 5.8.12]. □

2.2. Automorfismo de Frobenius y símbolo de Artin

Dada una extensión finita de campos finitos $\mathbb{F}_{q^d}/\mathbb{F}_q$, se tiene que el grupo de Galois $G = \mathrm{Gal}(\mathbb{F}_{q^d}/\mathbb{F}_q)$ es un grupo cíclico de orden d. El generador $\tau\colon \mathbb{F}_{q^d} \to \mathbb{F}_{q^d}$ dado por $\tau(x) = x^q$ se le llama el *automorfismo de Frobenius*. Se tiene que $\tau(x) = x \iff x^q = x \iff x \in \mathbb{F}_q$.

Definición 2.2.1. Un *campo global* es, o bien una extensión finita de $\mathbb{Q}$, o bien un campo de funciones con campo de constantes un campo finito.

Los campos globales de funciones, reciben también el nombre de *campos de funciones congruentes*.

Ahora bien, dada una extensión de Galois de campos globales L/K, sea $\mathfrak{p}$ un primo de K y sea $\mathfrak{P}$ un primo de L sobre $\mathfrak{p}$. Sea $L(\mathfrak{P})/K(\mathfrak{p})$ la extensión de campos residuales. Si $D = D(\mathfrak{P}|\mathfrak{p})$ es el grupo de descomposición de $\mathfrak{P}/\mathfrak{p}$, el mapeo $D \overset{\varphi}{\hookrightarrow} \mathrm{Gal}(L(\mathfrak{P})/K(\mathfrak{p}))$, $\sigma \mapsto \bar{\sigma}$ = clase de σ módulo $\mathfrak{p}$, es un epimorfismo de grupos con núcleo $I = I(\mathfrak{P}|\mathfrak{p})$ el grupo de inercia de $\mathfrak{P}/\mathfrak{p}$. Es decir, tenemos $D/I \cong G$. Si $\mathfrak{P}/\mathfrak{p}$ es no ramificado, entonces $I = \{1\}$ y por tanto $D \cong G$. En particular, existe un único $\sigma_{\mathfrak{p}} \in D$ tal que $\sigma_{\mathfrak{p}} \overset{\varphi}{\to} \tau$ es el automorfismo de Frobenius. El automorfismo $\sigma_{\mathfrak{p}}$ se llama el *automorfismo de Frobenius de* $\mathfrak{P}/\mathfrak{p}$.

Definición 2.2.2. Se define la *norma absoluta* del campo residual $L(\mathfrak{P})$ de un campo ya sea local o global como $\mathrm{N}(\mathfrak{P}) := |L(\mathfrak{P})|$.

Sean $\mathrm{N}(\mathfrak{P}) = |L(\mathfrak{P})|$ y $\mathrm{N}(\mathfrak{p}) = |K(\mathfrak{p})|$, digamos $\mathrm{N}(\mathfrak{p}) = q^f$ con $f = [K(\mathfrak{p}) : \mathbb{F}_q]$ en el caso de campos de funciones, entonces $\sigma_{\mathfrak{P}}(\mathfrak{P}) = \mathfrak{P}$, $\sigma_{\mathfrak{P}}|_{\mathfrak{p}} = \mathrm{Id}$ y $\sigma_{\mathfrak{P}}(\mathcal{O}_{\mathfrak{P}}) = \mathcal{O}_{\mathfrak{P}}$. Es decir, $\sigma_{\mathfrak{P}}$ está caracterizados por

$$\overline{\sigma_{\mathfrak{P}}}(x) \equiv x^{\mathrm{N}(\mathfrak{p})} \text{ mód } \mathfrak{P} \quad \text{ para toda } \quad x \in \mathcal{O}_{\mathfrak{P}}.$$

Escribimos $\sigma_{\mathfrak{P}} = \left[\dfrac{L/K}{\mathfrak{P}}\right]$ y $\left[\dfrac{L/K}{\mathfrak{P}}\right](x) \equiv x^{\mathrm{N}(\mathfrak{p})}$ mód $\mathfrak{P}$ para toda $x \in \mathcal{O}_{\mathfrak{P}}$.

2.2.1. Propiedades del automorfismo de Frobenius

Aquí se supone que L/K es una extensión de Galois finita de campos globales.

Proposición 2.2.3. *Si $\sigma \in \mathcal{G} = \mathrm{Gal}(L/K)$, se tiene*

$$\left[\frac{L/K}{\sigma\mathfrak{P}}\right] = \sigma\left[\frac{L/K}{\mathfrak{P}}\right]\sigma^{-1}.$$

Demostración. Sea $y \in \mathcal{O}_L$ y sea $x \in \mathcal{O}_L$ tal que $y = \sigma^{-1}x$. Entonces

$$\left[\frac{L/K}{\mathfrak{P}}\right]y = \left[\frac{L/K}{\mathfrak{P}}\right]\sigma^{-1}x \equiv (\sigma^{-1}x)^q \text{ mód } \mathfrak{P}.$$

Aplicando σ a esta igualdad, obtenemos $\sigma\left[\frac{L/K}{\mathfrak{P}}\right]\sigma^{-1}x \equiv x^q$ mód $\sigma\mathfrak{P}$. Por la unicidad del automorfismo de Frobenius se sigue que $\sigma\left[\frac{L/K}{\mathfrak{P}}\right]\sigma^{-1} = \left[\frac{L/K}{\sigma\mathfrak{P}}\right]$. □

Proposición 2.2.4. *Sea una torre $K \subseteq E \subseteq L$. Sea $\mathfrak{q} = \mathfrak{P} \cap E$. Entonces*

$$\left[\frac{L/K}{\mathfrak{P}}\right]^{f(\mathfrak{q}|\mathfrak{p})} = \left[\frac{L/E}{\mathfrak{P}}\right],$$

donde $f(\mathfrak{q}|\mathfrak{p})$ es el grado de inercia de $\mathfrak{q}$ sobre $\mathfrak{p}$, esto es, $f(\mathfrak{q}|\mathfrak{p}) = [\mathcal{O}_L/\mathfrak{q} : \mathcal{O}_K/\mathfrak{p}]$.

Demostración. Se tiene $\mathbb{F}_q \subseteq \mathbb{F}_{q^{f_0}} \subseteq \mathbb{F}_{q^f}$ donde $f_0 = f(\mathfrak{q}|\mathfrak{p})$ y $f = f(\mathfrak{P}|\mathfrak{p})$.

El automorfismo de Frobenius generando $\mathrm{Gal}(\mathbb{F}_{q^f}/\mathbb{F}_{q^{f_0}})$ corresponde al mapeo $y \xrightarrow{\tau} y^{q^{f_0}}$. Si σ es el automorfismo de Frobenius de $\mathrm{Gal}(\mathbb{F}_{q^f}/\mathbb{F}_q)$, entonces $\tau = \sigma^{f_0}$. Ahora bien $\tau = \left[\frac{L/E}{\mathfrak{P}}\right]$ y $\sigma = \left[\frac{L/K}{\mathfrak{P}}\right]$. □

Proposición 2.2.5. *Sea $K \subseteq E \subseteq L$ donde E/K es también una extensión de Galois. Sea $\mathfrak{q} = \mathfrak{P} \cap E$. Entonces se tiene que la restricción satisface*

$$\left[\frac{E/K}{\mathfrak{q}}\right] = \mathrm{rest}_E\left[\frac{L/K}{\mathfrak{P}}\right] = \left[\frac{L/K}{\mathfrak{P}}\right]\Big|_E.$$

Esto es, $\mathrm{rest}_E\left[\frac{L/K}{\mathfrak{P}}\right] = \left[\frac{E/K}{\mathfrak{P}\cap E}\right]$.

Demostración. Se tiene $\mathrm{rest}_E\colon \mathrm{Gal}(L/K) \longrightarrow \mathrm{Gal}(E/K)$ está dada por $\sigma \longmapsto \sigma|_E$ y se tiene que $\mathrm{núc}\,\mathrm{rest}_E = H = \mathrm{Gal}(L/E)$.

Sea $\sigma = \left[\frac{L/K}{\mathfrak{P}}\right]$. Entonces $\sigma x \equiv x^q$ mód $\mathfrak{P}$ para $x \in \mathcal{O}_L$. Por tanto, si $x \in \mathcal{O}_E$, se tiene $\sigma x - x^q \in \mathcal{O}_E$ y $\sigma x \equiv x^q$ mód $\mathfrak{P}$. Se sigue que $\sigma x \equiv x^q$ mód $(\mathfrak{P} \cap \mathcal{O}_E) = x^q$ mód $\mathfrak{q}$. Así, $\sigma|_E = \left[\frac{E/K}{\mathfrak{q}}\right]$. □

Corolario 2.2.6. *Sean $K \subseteq E, F \subseteq L$ tales que E/K y F/K son extensiones de Galois. Sean $\mathfrak{q} = \mathfrak{P} \cap E$ y $\mathfrak{t} = \mathfrak{P} \cap F$. Supongamos que $L = EF$. Entonces el mapeo $\sigma \longrightarrow (\sigma|_E, \sigma|_F)$ de $\mathrm{Gal}(L/K)$ en $\mathrm{Gal}(E/K) \times \mathrm{Gal}(F/K)$, el cual es inyectivo, da lugar a*

$$\begin{array}{ccccc} \left[\dfrac{L/K}{\mathfrak{P}}\right] & \longrightarrow & \left[\dfrac{E/K}{\mathfrak{q}}\right] & \times & \left[\dfrac{F/K}{\mathfrak{t}}\right] \\ \| & & \| & & \| \\ \left[\dfrac{EF/K}{\mathfrak{P}}\right] & \longrightarrow & \left[\dfrac{E/K}{\mathfrak{P}\cap E}\right] & \times & \left[\dfrac{F/K}{\mathfrak{P}\cap F}\right]. \end{array}$$

Demostración. Se sigue inmediatamente de la Proposición 2.2.5. □

Proposición 2.2.7. *Se tiene $\mathfrak{p}$ in $\mathcal{O}_K$ se descompone totalmente en L/K si y sólo si $\left[\dfrac{L/K}{\mathfrak{P}}\right] = 1$.*

Demostración. Puesto que $\mathfrak{P}|\mathfrak{p}$ es no ramificada, $\mathfrak{p}$ se descompone totalmente si y sólo si $f(\mathfrak{P}|\mathfrak{p}) = 1$ si y sólo si

$$\mathcal{O}_L/\mathfrak{P} = \mathcal{O}_K/\mathfrak{p} \iff \mathrm{Gal}((\mathcal{O}_L/\mathfrak{P})/(\mathcal{O}_K/\mathfrak{p})) = \{1\} \iff \left[\frac{L/K}{\mathfrak{P}}\right] = 1. \quad \square$$

Corolario 2.2.8. *Sean E/K y F/K extensiones de Galois y $L = EF$. Entonces $\mathfrak{p}$ en $\mathcal{O}_K$ se descompone totalmente en L/K si y sólo si $\mathfrak{p}$ se descompone totalmente tanto en E/K como en F/K.*

Demostración. De la Proposición 2.2.7 se tiene que $\mathfrak{p}$ se descompone totalmente en $L/K \iff \left[\dfrac{L/K}{\mathfrak{P}}\right] = 1$ si y sólo si bajo el mapeo $\left[\dfrac{L/K}{\mathfrak{P}}\right] \longhookrightarrow \left[\dfrac{E/K}{\mathfrak{P}\cap E}\right] \times \left[\dfrac{F/K}{\mathfrak{P}\cap F}\right]$, se tiene $\left[\dfrac{E/K}{\mathfrak{P}\cap E}\right] = \left[\dfrac{F/K}{\mathfrak{P}\cap F}\right] = 1 \iff \mathfrak{p}$ se descompone totalmente tanto en E/K como en F/K. □

Sea L/K una extensión abeliana finita de campos globales. En este caso, para $\sigma \in \mathrm{Gal}(L/K)$, $\left[\dfrac{L/K}{\mathfrak{P}}\right] = \sigma\left[\dfrac{L/K}{\mathfrak{P}}\right]\sigma^{-1} = \left[\dfrac{L/K}{\sigma\mathfrak{P}}\right]$. Esto es, si L/K es abeliana, $\left[\dfrac{L/K}{\mathfrak{P}}\right]$ no depende de $\mathfrak{P}$ sino únicamente de $\mathfrak{p}$. En este caso escribimos

$$\left[\frac{L/K}{\mathfrak{P}}\right] = \left(\frac{L/K}{\mathfrak{p}}\right) = (L/K, \mathfrak{p}) = (\_, L/K, \mathfrak{p}) = (\_, L/K) = \psi_{L/K}(\mathfrak{p}),$$

el cual se llama el *símbolo de Artin*.

Observación 2.2.9. Se tiene que $(L/K,\mathfrak{p})=1 \iff (\mathfrak{P}|\mathfrak{p}$ es no ramificada y $L(\mathfrak{P})=K(\mathfrak{p})) \iff (\mathfrak{p}$ es totalmente descompuesto en $L)$.

En general se tiene que $o((L/K,\mathfrak{p}))=d_{L/K}(\mathfrak{P}|\mathfrak{p})=[L(\mathfrak{P}):K(\mathfrak{p})]$ el cual es el orden del automorfismo de Frobenius.

Teorema 2.2.10. *Sea L/K una extensión abeliana finita de campos globales. Sea E una extensión finita de K y sea F/E una extensión abeliana finita tal que $L\subseteq F$ (por tanto $LE\subseteq F$). Sea $\mathrm{N}_{E/K}\colon E\longrightarrow K$ la norma de E en K. Sea $\theta=\mathrm{rest}\colon \mathrm{Gal}(F/E)=\mathcal{G}\longrightarrow \mathrm{Gal}(L/K)=G$ la restricción. Sea $\mathfrak{q}$ un primo en E no ramificado en F y sea $\mathfrak{p}=\mathrm{N}_{E/F}\,\mathfrak{q}$ un primo en K no ramificado en L. Sea $\mathfrak{t}$ un primo en F sobre $\mathfrak{q}$ y $\mathfrak{P}$ un primo en L sobre $\mathfrak{p}$.*

Entonces $\left(\dfrac{L/K}{\mathrm{N}_{E/K}\,\mathfrak{q}}\right)=\mathrm{rest}_L\left(\dfrac{F/E}{\mathfrak{q}}\right)=\left(\dfrac{F/E}{\mathfrak{q}}\right)\Big|_L$.

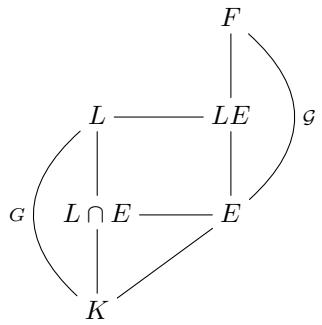
En otras palabras, si S es un conjunto finito de primos en K que contienen a todos los primos infinitos y a todos los primos ramificados y si S' es el conjunto de primos de E que están sobre S, entonces el diagrama

$$\begin{array}{ccc} D_E^{S_0'} & \xrightarrow{\psi_{F/E}} & \mathcal{G} \\ {\scriptstyle \mathrm{N}_{F/K}}\downarrow & & \downarrow{\scriptstyle \mathrm{rest}_L} \\ D_K^{S_0} & \xrightarrow[\psi_{L/K}]{} & G \end{array}$$

es conmutativo, donde $D_E^{S_0'}$ es el grupo libre generado por los divisores primos de E que no están en S' y análogamente $D_K^{S_0}$. Aquí $\psi_{F/E}$ y $\psi_{L/K}$ denotan los mapeos de Artin.

Demostración. Sea $f=f(\mathfrak{q}|\mathfrak{p})=f(E|F)=[\tilde{E}:\tilde{K}]=[\mathcal{O}_E/\mathfrak{q}:\mathcal{O}_K/\mathfrak{p}]$. Entonces $\mathrm{N}_{E/K}=\mathfrak{p}^f$.

Sea $\sigma=\psi_{F/E}(\mathfrak{q})=\left(\dfrac{F/E}{\mathfrak{q}}\right)=\left[\dfrac{F/E}{\mathfrak{Q}}\right]$ donde $\mathfrak{Q}$ es un primo en F sobre $\mathfrak{q}$ y sea $\tau=\psi_{L/K}(\mathfrak{p})=\left(\dfrac{L/K}{\mathfrak{p}}\right)=\left[\dfrac{L/K}{\mathfrak{P}}\right]$ con $\mathfrak{P}$ un primo en L sobre $\mathfrak{p}$.



Entonces $\psi_{L/K}(\mathrm{N}_{E/K}\,\mathfrak{q}) = \psi_{L/K}(\mathfrak{p}^f) = \psi_{L/K}(\mathfrak{p})^f = \tau^f$ y $\mathrm{rest}_L\,\psi_{F/E}(\mathfrak{q}) = \left(\frac{F/E}{\mathfrak{q}}\right)\Big|_L = \sigma|_L$.

Debemos probar que $\sigma = \tau^f$. Ahora bien, $\mathcal{O}_L/\mathfrak{P} \subseteq \mathcal{O}_F/\mathfrak{Q}$. Para $x \in \mathcal{O}_L/\mathfrak{P}$ se tiene $\sigma x = x^{\mathrm{N}(\mathfrak{Q})}$. Puesto que $\mathrm{N}(\mathfrak{Q}) = |\mathcal{O}_E/\mathfrak{Q}|$ y $[\mathcal{O}_E/\mathfrak{Q} : \mathcal{O}_K/\mathfrak{p}] = f$, se sigue que $|\mathcal{O}_E/\mathfrak{Q}| = |\mathcal{O}_K/\mathfrak{p}|^f$, esto es, $\mathrm{N}(\mathfrak{Q}) = \mathrm{N}(\mathfrak{p})^f$.

Por tanto $\sigma x = x^{\mathrm{N}(\mathfrak{Q})} = x^{\mathrm{N}(\mathfrak{p})^f} = \tau^f x$ puesto que $\tau x = x^{\mathrm{N}(\mathfrak{p})}$ por lo que $\tau^f x = x^{\mathrm{N}(\mathfrak{p})^f}$. De esta forma obtenemos que $\sigma = \tau^f$. □

Siempre que usamos el símbolo de Artin o el automorfismo de Frobenius, estaremos suponiendo que $\mathfrak{P}|\mathfrak{p}$ es no ramificado.

Recordemos que si $K = \mathbb{F}_q(T)$ y $K_M = K(\Lambda_M)$ es una extensión de campos de funciones ciclotómicas con $M \in R_T = \mathbb{F}_q[T]$, entonces si λ_M es un generador del R_T–módulo Λ_M y si $P \in R_T$ es un polinomio mónico e irreducible, con $P \nmid M$, entonces el símbolo de Artin está dado por $(K_M/k, P) = (\lambda_M \mapsto \lambda_M^P)$ ([136, Teorema 9.3.3]).

2.3. Extensiones de Galois infinitas

Sea Ω/k una extensión de Galois y sea $G = \mathrm{Gal}(\Omega/k)$. A G se le da la *topología de Krull* la cual se define como sigue. Para $\sigma \in G$, tomamos las clases $\sigma\,\mathrm{Gal}(\Omega/K)$ como una base de vecindades de σ donde K/k recorre el conjunto de todas las extensiones finitas de Galois con $k \subseteq K \subseteq \Omega$. Se tiene que las operaciones de grupo:

$$\begin{array}{lll} G \times G \to G & \text{y} & G \to G \\ (\sigma, \varphi) \mapsto \sigma\varphi & & \sigma \mapsto \sigma^{-1} \end{array}$$

son funciones continuas en la topología de Krull. De esta forma G se hace un *grupo topológico*. Cuando G es finito, la topología de Krull es la topología discreta, es decir todos los subconjuntos son abiertos y todos son cerrados.

Proposición 2.3.1. *Si Ω/k es una extensión de Galois, finita o infinita, $G = \mathrm{Gal}(\Omega/k)$ es Hausdorff y compacto.*

Demostración. [160, Theorem 11.4.5, página 402]. □

Teorema 2.3.2 (Correspondencia de Galois). *Sea Ω/k una extensión de Galois, finita o infinita. Entonces $K \to \mathrm{Gal}(\Omega/K)$ da lugar a una correspondencia biyectiva entre todas las subextensiones K/k con $k \subseteq K \subseteq \Omega$ y todos los subgrupos cerrados de $G = \mathrm{Gal}(\Omega/k)$.*

Los subgrupos abiertos de G corresponden a las subextensiones finitas k/k de Ω/k, es decir $[K : k] < \infty$.

Demostración. [136, Teorema 2.2.7]. □

Observación 2.3.3. Dado cualquier subgrupo $H < G$, el campo fijo de H, Ω^H es efectivamente un campo. De hecho, $\Omega^H = \Omega^{\bar{H}}$ donde $\bar{H}$ es la cerradura de H.

En efecto, el verificar que Ω^H es un campo es rutinario pues en esta parte no importan las características topológicas de H. Ahora bien, puesto que $H \subseteq \bar{H}$ se tiene $\Omega^{\bar{H}} \subseteq \Omega^H$. Por otro lado, si $x \in \Omega^H$, entonces $\sigma x = x$ para toda $\sigma \in H$. Dado $\psi \in \bar{H}$, entonces, puesto que estamos considerando la topología de Krull, si $N < G$ es de índice finito, $\psi N \cap H \neq \emptyset$. Se tiene $[K(x) : K] < \infty$ y si $\widetilde{K(x)}$ es la cerradura de Galois de $K(x)/K$, $[\widetilde{K(x)} : K] < \infty$. Sea $N = \mathrm{Gal}(\Omega/\widetilde{K(x)}) \lhd G$ y $[G : N] = [\widetilde{K(x)} : K] < \infty$. Por tanto existe $n \in N$, $h \in H$ tal que $\psi n = h$. Por tanto

$$(\psi n)x \underset{\substack{\uparrow \\ nx=x}}{=} \psi(x) = h(x) = x,$$

por lo que $x \in \Omega^{\bar{H}}$ y por tanto $\boxed{\Omega^H = \Omega^{\bar{H}}}$.

En el caso de un grupo profinito G, el conjunto de índices lo tomamos como $I := \{N \mid N \lhd G, N \text{ es abierto en } G\}$. Definimos $N \leq N_1 \iff N_1 \subseteq N$ y $G_N := G/N$. Entonces, para $N \leq N_1$, $\phi_{N_1,N} \colon G/N_1 \to G/N$, $gN_1 \mapsto gN$ y se tiene que $G \cong \varprojlim_N G/N$.

Para calcular el grupo de Galois de una extensión L/K de campos, donde L/K es una extensión algebraica, normal y separable, procedemos de la siguiente forma. Para $\alpha \in L$ se tiene $[K(\alpha) : K] < \infty$ y si $\widetilde{K(\alpha)}/K$ es la cerradura normal de $K(\alpha)/K$, entonces $\widetilde{K(\alpha)}/K$ es una extensión de Galois finita. Definimos $L_\alpha := \widetilde{K(\alpha)}$. Seleccionamos los $\beta \in L$ tales que $L_\beta = K(\beta)$ y si $I = \{\alpha \in L \mid K(\alpha)/K \text{ es una extensión de Galois (necesariamente es finita)}\}$, entonces $L = \cup_{\beta \in I} L_\beta = \varinjlim_\beta L_\beta$ donde definimos $\beta \leq \beta_1 \iff L_\beta \subseteq L_{\beta_1}$ y donde $\psi_{\beta,\beta_1} \colon L_\beta \longrightarrow L_{\beta_1}$ es el encaje.

Teorema 2.3.4. *Con las notaciones anteriores, se tiene que*

$$\mathrm{Gal}(L/K) = \mathrm{Gal}\left(\varinjlim_{\beta \in I} L_\beta/K\right) \cong \varprojlim_{\beta \in I} \mathrm{Gal}(L_\beta/K)$$

Demostración. Ver [136, Teorema 2.2.6]. □

Observación 2.3.5. Notemos que si $L_\beta \subseteq L_{\beta_1}$, entonces $\mathrm{Gal}(L_\beta/K) \cong \frac{\mathrm{Gal}(L_{\beta_1}/K)}{\mathrm{Gal}(L_{\beta_1}/L_\beta)}$.

Definimos $G_\beta := \mathrm{Gal}(L_\beta/K)$ y $G_\beta \leq G_{\beta_1} \iff G_\beta$ es un grupo cociente de G_{β_1} bajo el mapeo de restricción y definimos

$$\begin{aligned} \psi_{\beta_1,\beta} \colon \mathrm{Gal}(L_{\beta_1}/K) &\longrightarrow \mathrm{Gal}(L_\beta/K) \\ \sigma &\longmapsto \sigma|_{L_\beta}. \end{aligned}$$

El isomorfismo anunciado en el Teorema 2.3.4 está dado por

$$\begin{aligned} \mathrm{Gal}(L/K) &\longrightarrow \varprojlim_{\beta\in I} \mathrm{Gal}(L_\beta/K) \\ \sigma &\longmapsto \{\sigma|_{L_\beta}\}_{\beta\in I}. \end{aligned}$$

Ejemplo 2.3.6 ([136, Ejemplos 2.1.17]). Sean p un número primo, $m, n \in \mathbb{N}$, $m \geq n$ y

$$\phi_{m,n}\colon \mathbb{Z}/p^m\mathbb{Z} \longrightarrow \mathbb{Z}/p^n\mathbb{Z}$$

dada por $\phi_{m,n}(x \bmod p^m) = x \bmod p^n$. Se define $\mathbb{Z}_p = \big\{ \sum_{n=0}^{\infty} a_n p^n \mid a_n \in \{0, 1, \ldots, p-1\}\big\}$ y sea $\varphi_m\colon \mathbb{Z}_p \to \mathbb{Z}/p^m\mathbb{Z}$, dada por

$$\varphi_m\big(\sum_{n=0}^{\infty} a_n p^n\big) = \sum_{n=0}^{m-1} a_n p^n \bmod p^m.$$

De la discusión anterior se puede probar que $\mathbb{Z}_p \cong \varprojlim_m \mathbb{Z}/p^m\mathbb{Z}$.

Sea $\mathbb{Q}_n$ la subextensión de grado p^n de $\mathbb{Q}(\zeta_{p^{n+1}})/\mathbb{Q}$ cuando p es impar y si $p = 2$, $\mathbb{Q}_n$ es la subextensión cíclica de grado 2^n de $\mathbb{Q}(\zeta_{2^{n+2}})/\mathbb{Q}$ contenida en $\mathbb{R}$. Sea $\mathbb{Q}_\infty = \cup_{n=1}^{\infty}\mathbb{Q}_n$, entonces $\mathbb{Q}_\infty/\mathbb{Q}$ es de Galois y

$$\begin{aligned} \mathrm{Gal}(\mathbb{Q}_\infty/\mathbb{Q}) &= \mathrm{Gal}\big(\cup_{n=1}^{\infty}\mathbb{Q}_n/\mathbb{Q}\big) \cong \mathrm{Gal}(\varinjlim_n \mathbb{Q}_n/\mathbb{Q}\big) \\ &\cong \varprojlim_n \mathrm{Gal}(\mathbb{Q}_n/\mathbb{Q}) \cong \varprojlim_n \mathbb{Z}/p^n\mathbb{Z} \cong \mathbb{Z}_p. \end{aligned}$$

$\mathbb{Q}_\infty/\mathbb{Q}$ recibe el nombre de la $\mathbb{Z}_p$*–extensión ciclotómica de* $\mathbb{Q}$ (ver [136, Capítulo 16]).

Ejemplo 2.3.7. Sea $\mathbb{F}_q$ el campo finito de q elementos, $q = p^r$. Si $K/\mathbb{F}_q$ es una extensión de grado d, $K \cong \mathbb{F}_{q^d}$ y $\mathrm{Gal}(K/\mathbb{F}_q) \cong \mathbb{Z}/d\mathbb{Z}$. Por tanto $\overline{\mathbb{F}_q} = \mathbb{F}_q^{\mathrm{ab}} = \cup_{n=1}^{\infty}\mathbb{F}_{q^n}$ y

$$\begin{aligned} \mathrm{Gal}(\overline{\mathbb{F}_q}/\mathbb{F}_q) &= \mathrm{Gal}\big(\cup_{n=1}^{\infty}\mathbb{F}_{q^n}/\mathbb{F}_q\big) \cong \mathrm{Gal}(\varinjlim_n \mathbb{F}_{q^n}/\mathbb{F}_q) \\ &\cong \varprojlim_n \mathrm{Gal}(\mathbb{F}_{q^n}/\mathbb{F}_q) \cong \varprojlim_n \mathbb{Z}/n\mathbb{Z} \cong \hat{\mathbb{Z}} \cong \prod_p \mathbb{Z}_p \end{aligned}$$

donde $\hat{\mathbb{Z}}$ es el *anillo o grupo de Prüfer* y de hecho es la completación de $\mathbb{Z}$. (ver comentario después del Teorema 6.8.32 y [8, Ch. X]).

2.4. Teoría de Kummer

La Teoría de Kummer juega un papel relevante en el *Teorema de Existencia* en la teoría de campos de clase global (ver Subsección 5.7 y Teorema 6.8.9).

Sea K un campo de característica $p \geq 0$ y $n \in \mathbb{N}$ tal que $p \nmid n$. Sea W_n el *grupo de las n–raíces de unidad*. Se supone que $W_n \subseteq K$. Una *extensión de Kummer* de K de la forma $K(\sqrt[n]{\Delta}) := K(\{\sqrt[n]{\alpha} \mid \alpha \in \Delta\})$ donde Δ es un subgrupo de K^* tal que $(K^*)^n \subseteq \Delta \subseteq K^*$.

Si L/K es una extensión de Kummer, L/K es una extensión abeliana de exponente n, es decir, $\sigma^n = \mathrm{Id}_K$ para toda $\sigma \in \mathrm{Gal}(L/K)$, aunque L/K no es necesariamente finita.

Proposición 2.4.1. *Si L/K es una extensión abeliana no necesariamente finita de exponente n, entonces $L = K(\sqrt[n]{\Delta})$ con $\Delta = (L^*)^n \cap K^*$, es decir, $\sqrt[n]{\Delta} = L^* \cap \sqrt[n]{K^*}$.*

Demostración. Por definición se tiene que $K(\sqrt[n]{\Delta}) \subseteq L$. Ahora bien, L es la composición de sus subextensiones cíclicas. Sea M/K una subextensión cíclica de L/K, por lo tanto $\mathrm{Gal}(M/K)$ tiene orden un divisor de n, por lo que $M = K(\sqrt[n]{a})$ con $a \in (L^*)^n \cap K^*$ (Teorema 2.1.4), es decir, con $a \in K$ tal que $\sqrt[n]{a} \in L$. Se sigue que $M \subseteq K(\sqrt[n]{\Delta})$ y por tanto $L \subseteq K(\sqrt[n]{\Delta})$. □

Teorema 2.4.2 (Teoría de Kummer). *Las extensiones de Kummer de exponente n están en correspondencia biyectiva con los subgrupos Δ de K^* que contienen a $(K^*)^n$. Si $L = K(\sqrt[n]{\Delta})$, entonces $\Delta = (L^*)^n \cap K^*$ y se tiene el isomorfismo*

$$\widehat{\mathrm{Gal}(L/K)} = \mathrm{Hom}(\mathrm{Gal}(L/K), W_n) \cong \Delta/(K^*)^n.$$

El isomorfismo proviene de que dado $a \bmod (K^*)^n \in \Delta/(K^*)^n$, se le asocia el caracter $\chi_a \colon \mathrm{Gal}(L/K) \to W_n$ dado por $\chi_a(\sigma) = \frac{\sigma(\sqrt[n]{a})}{\sqrt[n]{a}}$.

Más explícitamente, la correspondencia de Kummer está dada por

$$L^* \longmapsto \Delta = (L^*)^n \cap K^*,$$
$$\Delta \longmapsto L = K\big(\sqrt[n]{\Delta}\big) = K_\Delta.$$

Además se tiene

$$\Delta_1\Delta_2 \longleftrightarrow K_{\Delta_1}K_{\Delta_2};$$
$$\Delta_1 \cap \Delta_2 \longleftrightarrow K_{\Delta_1} \cap K_{\Delta_2}.$$

Observación 2.4.3. Si L/K es una extensión de Kummer de exponente n infinita, entonces $\mathrm{Gal}(L/K)$ tiene la topología de Krull y $\mathrm{Hom}(\mathrm{Gal}(L/K), W_n)$ es el grupo de todos los homomorfismos continuos $\chi \colon \mathrm{Gal}(L/K) \longrightarrow W_n$ y donde W_n tiene la topología discreta.

Si $\mathrm{Gal}(L/K)$ es finito, $\mathrm{Gal}(L/K)$ tiene la topología discreta y todo homomorfismo $\chi \colon \mathrm{Gal}(L/K) \longrightarrow W_n$ es automáticamente continuo.

Demostración. (Teorema 2.4.2). Sea L/K una extensión de Kummer de exponente n. Entonces $L = K(\sqrt[n]{\Delta})$ con $\Delta = (L^*)^n \cap K^*$ (Proposición 2.4.1). Se define el homomorfismo

$$\Delta \xrightarrow{\theta} \mathrm{Hom}(\mathrm{Gal}(L/K), W_n), \quad a \mapsto \chi_a$$

definido por $\chi_a(\sigma) = \frac{\sigma(\sqrt[n]{a})}{\sqrt[n]{a}}$ con $\sigma \in \mathrm{Gal}(L/K)$. Ahora bien se tiene

$$\begin{aligned} a \in \text{núc}\,\theta &\iff \chi_a(\sigma) = \frac{\sigma(\sqrt[n]{a})}{\sqrt[n]{a}} = 1 \text{ para toda } \sigma \in \mathrm{Gal}(L/K) \\ &\iff \sqrt[n]{a} \in K^* \iff a \in (K^*)^n. \end{aligned}$$

Esto es, $\text{núc}\,\theta = (K^*)^n$. El homomorfismo $\tilde{\theta}$ inducido por θ

$$\Delta/(K^*)^n \xrightarrow{\tilde{\theta}} \mathrm{Hom}(\mathrm{Gal}(L/K), W_n)$$

es inyectivo.

Para demostrar que $\tilde{\theta}$ es suprayectivo, primero consideremos el caso en que L/K es una extensión finita. Sea $\chi \in \mathrm{Hom}(\mathrm{Gal}(L/K), W_n)$. Entonces $\chi\colon \mathrm{Gal}(L/K) \longrightarrow L^*$ es en particular un homomorfismo cruzado. Por el Teorema 4.3.1 se tiene que existe $y \in L^*$ tal que $\chi(\sigma) = \frac{\sigma y}{y}$ para toda $\sigma \in \mathrm{Gal}(L/K)$.

Ahora bien, $\sigma(y^n) = (\sigma y)^n = \chi(\sigma)^n y^n = y^n$ para toda $\sigma \in \mathrm{Gal}(L/K)$ lo cual implica que $y^n \in K^*$. Por tanto $y^n = x \in (L^*)^n \cap K^* = \Delta$ y

$$\chi_x(\sigma) = \frac{\sigma(\sqrt[n]{x})}{\sqrt[n]{x}} = \frac{\sigma(y)}{y} = \chi(\sigma) \quad \text{para toda} \quad \sigma \in \mathrm{Gal}(L/K),$$

de donde se sigue que $\chi = \chi_x = \tilde{\theta}(x)$.

Ahora consideremos una extensión infinita L/K. Sea $\{\Delta_\alpha/(K^*)^n\}_{\alpha\in\mathcal{A}}$ el conjunto de los subgrupos finitos de $\Delta/(K^*)^n$. Sea $K_\alpha := K(\sqrt[n]{\Delta_\alpha})$, $\alpha \in \mathcal{A}$. Se tiene

$$\Delta/(K^*)^n = \bigcup_{\alpha\in\mathcal{A}} \Delta_\alpha/(K^*)^n \quad \text{y} \quad L = \bigcup_{\alpha\in\mathcal{A}} K_\alpha.$$

Se sigue que $\{\mathrm{Gal}(L/K_\alpha)\}_{\alpha\in\mathcal{A}}$ forman una base de vecindades de $\mathrm{Id} \in \mathrm{Gal}(L/K)$.

Dado $\chi\colon \mathrm{Gal}(L/K) \longrightarrow W_n$ continuo, $\text{núc}\,\chi = \chi^{-1}(\{1\})$ es cerrado y de índice finito en $\mathrm{Gal}(L/K)$ y por tanto es abierto. Se sigue que existe $\alpha \in \mathcal{A}$ tal que $\mathrm{Gal}(L/K_\alpha) \subseteq \text{núc}\,\chi$.

Ahora bien, χ induce un homomorfismo $\bar{\chi}\colon \mathrm{Gal}(K_\alpha/K) \longrightarrow W_n$ de tal forma que $\chi(\sigma) = \bar{\chi}(\sigma|_{K_\alpha})$. Puesto que $\mathrm{Gal}(K_\alpha/K)$ es finito, por lo anterior, existe $a \in K_\alpha$ tal que $\bar{\chi} = \chi_a\colon \mathrm{Gal}(K_\alpha/K) \longrightarrow W_n$. Por tanto

$$\chi(\sigma) = \bar{\chi}(\sigma|_{K_\alpha}) = \frac{\sigma(\sqrt[n]{a})}{\sqrt[n]{a}} = \chi_a(\sigma),$$

por lo que $\chi = \chi_a$ y $\tilde{\theta}$ es suprayectiva.

Sea ahora $(K^*)^n \subseteq \Delta \subseteq K^*$ y $L = K(\sqrt[n]{\Delta})$. Entonces veamos que $\Delta = (L^*)^n \cap K^*$. Sea $\Delta_1 = (L^*)^n \cap K^*$. Entonces $\Delta \subseteq \Delta_1$. Ahora bien, por lo anteriormente probado, se tiene

$$\Delta_1/K^* \cong \mathrm{Hom}(\mathrm{Gal}(L/K), W_n).$$

Al subgrupo $\Delta/(K^*)^n \subseteq \Delta_1/(K^*)^n$ le corresponde el subgrupo

$$\mathrm{Hom}(\mathrm{Gal}(L/K)/H, W_n) \text{ de } \mathrm{Hom}(\mathrm{Gal}(L/K), W_n) \text{ donde}$$
$$H = \{\sigma \in \mathrm{Gal}(L/K) \mid \chi_a(\sigma) = 1 \text{ para toda } a \in \Delta\}.$$

Puesto que $\sigma(\sqrt[n]{a}) = \chi_a(\sigma)\sqrt[n]{a}$, obtenemos que el subgrupo H fija a los elementos de $\sqrt[n]{\Delta}$. Ya que $L = K(\sqrt[n]{\Delta})$, se tiene que H fija a L y por tanto $H = \{1\}$. Se sigue que $\mathrm{Hom}(\mathrm{Gal}(L/K)/H, W_n) = \mathrm{Hom}(\mathrm{Gal}(L/K), W_n)$ por lo que $\Delta/(K^*)^n = \Delta_1/(K^*)^n$, de donde se sigue que $\Delta = \Delta_1$.

De esta forma, el mapeo $\Delta \longrightarrow L = K(\sqrt[n]{\Delta})$ es la correspondencia dada en el enunciado del teorema. □

La composición de dos extensiones de Kummer de exponente n es nuevamente una extensión de Kummer de exponente n y por lo tanto todas las extensiones de Kummer de exponente n están contenidos en la extensión de Kummer de exponente n máxima: $\tilde{K} = K(\sqrt[n]{K^*})$ y se tiene

$$\mathrm{Hom}(\mathrm{Gal}(\tilde{K}/K), W_n) \cong \frac{K^*}{(K^*)^n}.$$

2.5. Historia de la teoría de campos de clase

En esta subsección pretendemos dar un panorama más o menos general de lo que trata la teoría de campos de clase.

Lo tratado en esta pequeña subsección es un extracto de [30].

2.5.1. ¿Que es la teoría de campos de clase?

La teoría de campos de clase es la descripción de las extensiones abelianas de *campos globales* (extensiones finitas de $\mathbb{Q}$ y campos de funciones con campo de constantes un campo finito $\mathbb{F}_q$) y de *campos locales* (extensiones finitas del campo de los racionales números p–ádicos $\mathbb{Q}_p$ y las series de Laurent $\mathbb{F}((x))$ donde $\mathbb{F}$ es un campo finito). La razón de llamar a uno de estos campos *un campo de clase* se refiere a que estos campos están relacionados a grupos de clases de ideales. Uno de los teoremas principales es que los campos de clase son los mismos que las extensiones abelianas.

Para una extensión de campos L/K ponemos

$$\mathrm{Spl}(L/K) = \{\mathfrak{p} \text{ lugar de } K \mid \mathfrak{p} \text{ se descompone totalmente en } L\}.$$

Podemos pensar que la teoría de campos de clase se origina con el trabajo de Kronecker y más específicamente con el *Teorema de Kronecker–Weber* (1853): toda extensión abeliana finita de $\mathbb{Q}$ está contenida en algún campo

ciclotómico. La primera demostración y completa y correcta del Teorema de Kronecker–Weber la dio Hilbert en 1896 (sin él saber que las anteriores tenían alguna laguna, ver [136, Capítulo 4]).

Se tiene que si L/K es una extensión de Galois de campos numéricos, $\mathrm{Spl}(L/K)$ tiene densidad $1/[L:K]$ (Kronecker). Como consecuencia se tiene (Bauer): sean L_1, L_2 dos extensiones de Galois de K entonces $L_1 \subseteq L_2 \iff \mathrm{Spl}(L_2/K) \subseteq \mathrm{Spl}(L_1/K)$ (salvo un número finito de primos) y en particular $L_1 = L_2 \iff \mathrm{Spl}(L_1/K) = \mathrm{Spl}(L_2/K)$ con la igualdad salvo un número finito de primos.

El término *campo de clase* fue introducido en 1891 por Weber. En 1897 Weber extendió el concepto de grupo de clases de ideales: para un campo numérico K y un ideal no cero $\mathfrak{m}$ de $\mathcal{O}_K$, sea $D_K^{\mathfrak{m}}$ el grupo de ideales fraccionarios en K primos relativos a $\mathfrak{m}$ y sea $P_{K,\mathfrak{m}}^{+}$ el grupo de ideales fraccionarios $\big(\alpha/\beta\big)$ con $\alpha, \beta \in \mathcal{O}_K$ tales que (α) y (β) son primos relativos a $\mathfrak{m}$, $\alpha \equiv \beta \bmod \mathfrak{m}$, en el sentido de que $\alpha/\beta - 1 \in \mathfrak{m}$ y α/β es totalmente positivo, es decir, si $\varphi\colon K \to \mathbb{R}$ es un encaje real de K, $\varphi\big(\alpha/\beta\big) \in \mathbb{R}^+$, es decir, $\varphi\big(\alpha/\beta\big) > 0$.

Se tiene que $[D_K^{\mathfrak{m}} : P_{K,\mathfrak{m}}^{+}] < \infty$ y todo grupo intermedio $P_{K,\mathfrak{m}}^{+} \subseteq H \subseteq D_K^{\mathfrak{m}}$ se llama un *grupo de ideales con módulus* $\mathfrak{m}$ y el cociente $D_K^{\mathfrak{m}}/H$ se llama *grupo de ideales generalizado*.

Si $\mathfrak{m} = (1)$ y P_K es el grupo de los ideales principales, se tiene $P_{K,(1)}^{+} \subseteq P_K \subseteq D_K^{(1)}$ y $I_K := D_K^{(1)}/P_K$ es el grupo de clases de ideales usuales.

Teorema 2.5.1 (Weber). *Para cualquier ideal no cero de* $\mathfrak{m}$ *de* $\mathcal{O}_K$ *y para un grupo de ideales* H *con módulus* $\mathfrak{m}$*, supongamos que hay una extensión de Galois* L/K *tal que* $\mathrm{Spl}(L/K) \subseteq H$ *con un número finito de excepciones. Entonces* $[D_K^{\mathfrak{m}} : H] \leq [L:K]$.

Si $\mathrm{Spl}(L/K) = H$ *con un número finito de excepciones, entonces* $[D_K^{\mathfrak{m}} : H] = [L:K]$ *y hay una infinidad de primos en cada clase de* $D_K^{\mathfrak{m}}/H$. □

Definición 2.5.2 (Weber). Para un ideal no cero $\mathfrak{m}$ de $\mathcal{O}_K$ y para un grupo de ideales H con módulus $\mathfrak{m}$, el *campo de clase* sobre K para H es una extensión de Galois L/K tal que para los primos $\mathfrak{p} \nmid \mathfrak{m}$ en K, $\mathfrak{p}$ se descompone totalmente en $L \iff \mathfrak{p} \in H$ (si tal L existe, entonces L es único).

David Hilbert propuso una ley cuadrática de reciprocidad: $\prod_v (a,b)_v = 1$ para cualesquiera $a, b \in K^*$ y v recorre los lugares de K. La prueba de Hilbert de esta fórmula no funciona para extensiones no ramificadas. La prueba de Hilbert del Teorema de Kronecker–Weber funcionó en parte debido a que $\mathbb{Q}$ no tiene extensiones propias no ramificadas. Debido a lo anterior, Hilbert se interesó en las extensiones abelianas no ramificadas como un obstáculo en las demostraciones.

Conjetura 2.5.3 (Hilbert 1898). Para cualquier campo numérico K hay una única extensión K_H/K tal que:

(I) K_H/K es Galois y $\mathrm{Gal}(K_H/K) \cong I_K$.
(II) K_H/K es no ramificada y toda extensión abeliana con esta propiedad está contenida en K_H.
(III) Para cualquier primo $\mathfrak{p}$ de K, el grado $f_\mathfrak{p}$ de los campos residuales es el orden de $\mathfrak{p}$ en I_K.
(IV) Todo ideal K se hace principal en K_H.

Así K_H es un campo de clase en el sentido de Weber: el campo de clase para el grupo de los ideales principales fraccionarios de K.

Takagi empezó, aproximadamente en 1914, con una nueva definición de campos de clase, usando normas de ideales ($\mathrm{N}_{L/K}\,\mathfrak{P} = \mathfrak{p}^{f(\mathfrak{P}|\mathfrak{p})}$, $\mathfrak{p} = \mathfrak{P} \cap K$, $f(\mathfrak{P}|\mathfrak{p})$ el grado de inercia) en lugar de leyes de descomposición y también incorporó los primos infinitos dentro de la definición de los módulus .

La liga entre los puntos de vista de Weber y de Takagi es que cuando L/K es Galois y $\mathfrak{p}$ es no ramificada en L, $\mathfrak{p}$ se descompone totalmente en $L \iff \mathfrak{p}$ es la norma de algún ideal de L.

Así, de ahora en adelante, un *módulus* es $\mathfrak{m} = \mathfrak{m}_f\mathfrak{m}_\infty$, $\mathfrak{m}_f$ la parte finita de $\mathfrak{m}$ (es el de antes) y $\mathfrak{m}_\infty$ es un producto formal de encajes reales de K. Un ideal fraccionario se dice primo relativo a $\mathfrak{m}$ si lo es a $\mathfrak{m}_f$. Sea $D_K^\mathfrak{m}$ el grupo de los ideales fraccionarios primos relativos a $\mathfrak{m}$ y sea $P_{K,\mathfrak{m}}^+$ el grupo de los ideales fraccionarios principales $\big(\alpha/\beta\big)$ con $\alpha, \beta \in \mathcal{O}_K \setminus \{0\}$ tales que:

(I) (α) y (β) son primos relativos a $\mathfrak{m}$,
(II) $\alpha \equiv \beta \bmod \mathfrak{m}_f$, en el sentido $\alpha/\beta - 1 \in \mathfrak{m}$,
(III) $v\big(\alpha/\beta\big) > 0$ para toda $v|\mathfrak{m}_\infty$.

Un subgrupo intermedio $P_{K,\mathfrak{m}}^+ \subseteq H \subseteq D_K^\mathfrak{m}$ se llama un *grupo de ideales con módulus* $\mathfrak{m}$. Para una extensión finita L/K, sea $\mathrm{N}_\mathfrak{m}(L/K) = \{\mathfrak{a}$ en $K \mid \mathfrak{a} = \mathrm{N}_{L/K}(\mathfrak{c})$ para $\mathfrak{c}$ en L y $\mathfrak{a}$ y $\mathfrak{c}$ primos relativos a $\mathfrak{m}\}$. Sea $H^\mathfrak{m}(L/K) = P_{K,\mathfrak{m}}^+\,\mathrm{N}_\mathfrak{m}(L/K)$ el cual se llama *subgrupo de normas*.

Resulta ser que todo subgrupo de $D_K^\mathfrak{m}/P_{K,\mathfrak{m}}^+$ es el grupo de normas de alguna extensión abeliana finita de K. Se tiene que $P_{K,\mathfrak{m}}^+(\text{Weber}) = P_{K,\mathfrak{m}\infty}^+$ donde ∞ denota el producto de todos los lugares reales de K.

Se tiene que los primos que no dividen a $\mathfrak{m}$ y se descomponen totalmente en L, están en $\mathrm{N}_\mathfrak{m}(L/K) \subseteq H^\mathfrak{m}(L/K)$, es decir, $\mathrm{Spl}(L/K) \subseteq H^\mathfrak{m}(L/K)$ con excepción de los primos que dividen a $\mathfrak{m}$.

Así, como antes, $[D_K^\mathfrak{m} : H^\mathfrak{m}(L/K)] \leq [L : K]$ (primera desigualdad).

Definición 2.5.4 (Takagi). Una extensión de Galois de campos numéricos L/K se llama *campo de clase* si $[D_K^\mathfrak{m} : H^\mathfrak{m}(L/K)] = [L : K]$ para algún módulus $\mathfrak{m}$ (un tal módulus $\mathfrak{m}$ se llama un *módulus admisible* o *módulus de definición* para L/K).

Teorema 2.5.5 (Takagi 1920). *Sea K un campo numérico.*

(I) Existencia: *Para cada grupo de ideales H hay un campo de clase sobre K.*

(II) Isomorfismo: *Si H es un grupo de ideales con módulus $\mathfrak{m}$ y tiene campo de clase L/K, entonces* $\mathrm{Gal}(L/K) \cong D_K^{\mathfrak{m}}/H$. *En particular L/K es abeliana.*

(III) Completitud: *Toda extensión abeliana finita de K es un campo de clase. En particular, campo de clase de K y extensión abeliana finita de K, es lo mismo.*

(IV) Comparación: *Si H_1 y H_2 son grupos de ideales con módulus común $\mathfrak{m}$ y ellos tiene campos de clase L_1 y L_2, entonces, $L_1 \subseteq L_2 \iff H_2 \subseteq H_1$.*

(V) Conductor: *Para toda extensión abeliana L/K, los lugares de K que aparecen en el soporte del conductor $\mathfrak{f}_{L/K}$ son los primos ramificados en L/K.*

(VI) Descomposición: *Si H es un grupo de ideales con módulus $\mathfrak{m}$ y campo de clase L/K, entonces cualquier primo $\mathfrak{p} \nmid \mathfrak{m}$ es no ramificado en L y el grado de inercia $f_{\mathfrak{p}}$ es igual al orden de $\mathfrak{p}$ en $D_K^{\mathfrak{m}}/H$.* □

En su demostración, Takagi probó la *segunda desigualdad* para una extensión abeliana: $[D_K^{\mathfrak{m}} : H^{\mathfrak{m}}(L/K)] \geq [L : K]$ para alguna $\mathfrak{m}$. La primera desigualdad vale para toda extensión de Galois y la segunda desigualdad es válida únicamente para extensiones abelianas, es decir, si L/K es una extensión de Galois no abeliana, entonces

$$[D_K^{\mathfrak{m}} : H^{\mathfrak{m}}(L/K)] < [L : K] \quad \text{para todo módulus} \quad \mathfrak{m},$$

ver Teorema 6.9.7.

¿Como funciona la teoría de campos de clase? Si queremos una correspondencia tipo Galois, se tiene que si tomamos todos los campos de clase de golpe, tenemos el siguiente problema de comparación: los moduli admisibles para dos campos de clase pueden no ser el mismo por lo que tenemos que pasar a un módulus común para poder compararlos.

Para poder tener una biyección tipo Galois necesitamos identificar todos los grupos de ideales que tienen el mismo campo de clase. ¿Como hacerlo?

Si H y H' son grupos de ideales para K definidos moduli $\mathfrak{m}$ y $\mathfrak{m}'$, es decir, $P_{K,\mathfrak{m}}^{+} \subseteq H \subseteq D_K^{\mathfrak{m}}$ y $P_{K,\mathfrak{m}'}^{+} \subseteq H' \subseteq D_K^{\mathfrak{m}'}$, llamamos a H y H' *equivalentes* si existe un módulus $\mathfrak{m}''$ divisible tanto por $\mathfrak{m}$ como por $\mathfrak{m}'$ tal que los homomorfismos naturales $D_K^{\mathfrak{m}''} \mapsto D_K^{\mathfrak{m}}/H$ y $D_K^{\mathfrak{m}''} \mapsto D_K^{\mathfrak{m}'}/H'$ tienen el mismo núcleo, es decir $H \cap D_K^{\mathfrak{m}''} = H' \cap D_K^{\mathfrak{m}''}$.

Los grupos de ideales equivalentes, tienen el mismo campo de clase y entonces la correspondencia entre campos de clase sobre K y los grupos de ideales en K, hasta equivalencia, es biyectiva. Esto hace las cosas complicadas.

Cuando pasamos al lenguaje de *idèles*, todos los grupos de ideales equivalentes se fusionan en un único subgrupo de idèles, haciendo la teoría de campos de clase un poco más simple, o mejor dicho, menos complicada.

Ahora bien, el teorema de descomposición de Takagi muestra que para un primo $\mathfrak{p} \nmid \mathfrak{m}$, $\mathfrak{p}$ se descompone totalmente $\iff \mathfrak{p} \in H$ así que las nociones de campos de clase de Weber y de Takagi coinciden.

Por otro lado, las condiciones sobre los primos para que se descompongan totalmente se da por condiciones de congruencia. Por ejemplo, los primos que se descomponen totalmente en $\mathbb{Q}(i)/\mathbb{Q}$ son los primos $p \equiv 1 \bmod 4$, y 2 es el único primo ramificado. Los primos que se descomponen totalmente en $\mathbb{Q}(\sqrt{6})/\mathbb{Q}$ son los primos p tales que $p \equiv 1, 5, 19, 23 \bmod 24$. Finalmente, los primos que se descomponen totalmente en $\mathbb{Q}(\zeta_n)/\mathbb{Q}$, donde $\mathbb{Q}(\zeta_n)$ es el n–ésimo campo ciclotómico, son los primos p tales que $p \equiv 1 \bmod n$.

En general los primos de que no dividen a $\mathfrak{m}$ y que están en $\mathrm{Spl}(L/K)$ son aquellos en el subgrupo $H_{\mathfrak{m}}/P^{+}_{K,\mathfrak{m}}$ de $D^{\mathfrak{m}}_K/P^{+}_{K,\mathfrak{m}}$ y que pertenecen a un subgrupo que puede ser pensado como condiciones generalizadas de congruencias (por esto, los grupos $H_{\mathfrak{m}}$ se llaman *grupos de congruencia*).

Ahora bien, puesto que los campos de clase y extensiones abelianas son lo mismo, la descomposición total en una extensión abeliana está descrita por congruencias. Resulta ser que el recíproco también se cumple.

Teorema 2.5.6. *Sea L/K una extensión finita de campos numéricos y supongamos que existe un módulus $\mathfrak{m}$ y un conjunto finito S de primos que contienen a todos los que dividen a $\mathfrak{m}$, de tal forma que la condición de que un primo $\mathfrak{p} \notin S$ es o no totalmente descompuesto en L está determinado por la clase de $\mathfrak{p}$ en $D^{\mathfrak{m}}_K/P^{+}_{K,\mathfrak{m}}$. Entonces L/K es una extensión abeliana.* □

Corolario 2.5.7. *Para un campo numérico $L/\mathbb{Q}$ y $m \in \mathbb{N}$ las siguientes condiciones son equivalentes:*

(I) *Para cualquier primo positivo $p \nmid m$, la descomposición de p está determinada por una condición de congruencia en $p \bmod m$.*
(II) $L \subseteq \mathbb{Q}(\zeta_m)$. □

Takagi probó que hay un isomorfismo $D^{\mathfrak{m}}_K/H_{\mathfrak{m}} \cong \mathrm{Gal}(L/K)$ para todos los moduli $\mathfrak{m}$ que son K–admisibles. Sin embargo no dio ningún isomorfismo; el isomorfismo fue obtenido de manera indirecta. Hoy sabemos que sus argumentos pertenecen a la cohomología de grupos. Artin describió este isomorfismo por medio de la *Ley de Reciprocidad*.

Definición 2.5.8. Para una extensión abeliana L/K y un K–módulus divisible por todos los primos que se ramifican en L, el *mapeo de Artin* $\psi_{L/K,\mathfrak{m}} \colon D^{\mathfrak{m}}_K \to \mathrm{Gal}(L/K)$ está dado por $\psi_{L/K,\mathfrak{m}}(\mathfrak{p}) = (\mathfrak{p}, L/K) = \left(\dfrac{L/K}{\mathfrak{p}}\right)$.

Teorema 2.5.9 (Ley de Reciprocidad de Artin, Artin 1927).
El mapeo de Artin $\psi_{L/K,\mathfrak{m}}$ es suprayectivo y su núcleo contiene a $\mathrm{N}_{\mathfrak{m}}(L/K)$. Cuando $\mathfrak{m}$ es admisible, el núcleo de $\psi_{L/K,\mathfrak{m}}$ es $P^{+}_{K,\mathfrak{m}}\,\mathrm{N}_{\mathfrak{m}}(L/K) = H_{\mathfrak{m}}(L/K)$, esto es, $D^{\mathfrak{m}}_{K}/H_{\mathfrak{m}}(L/K) \cong \mathrm{Gal}(L/K)$ mediante el mapeo de Artin. □

La parte más difícil en la ley de reciprocidad es probar que el núcleo de $\psi_{L/K,\mathfrak{m}}$, con $\mathfrak{m}$ admisible, contiene a $P^{+}_{K,\mathfrak{m}}$. Es decir, probar que si $(\alpha) \in P^{+}_{K,\mathfrak{m}}$, entonces $\psi_{L/K,\mathfrak{m}}((\alpha)) = 1$.

2.5.2. Campos de clase vía idèles (C. Chevalley)

La teoría de campos de clase locales (o teoría local de campos de clase) fue establecida por sus propios méritos y no como reducción de la teoría global principalmente por H. Hasse.

Teorema 2.5.10 (H. Hasse, F.K. Schmidt, 1930). *Para una extensión abeliana de campos locales E/F (de característica 0), el* mapeo local de Artin *o* símbolo residual de la norma *, $\psi_{E/F}\colon F^{*} \twoheadrightarrow \mathrm{Gal}(E/F)$ es un epimorfismo con núcleo $\mathrm{N}_{E/F}\,E^{*}$ por lo que $F^{*}/\,\mathrm{N}_{E/F}\,E^{*} \cong \mathrm{Gal}(E/F)$.* □

De esta forma, asociando a E el grupo $\mathrm{N}_{E/F}(E^{*})$ obtenemos una correspondencia biyectiva que voltea el orden entre las extensiones abelianas finitas de F y los subgrupos abiertos de índice finito en F^{*}.

La imagen de las unidades de F, $U_F := \mathcal{O}_F^{*}$ bajo el mapeo local de Artin es el grupo de inercia $I(E/F)$, es decir, $\psi_{E/F}(U_F) = I(E/F)$, así que

$$e(E|F) = [U_F\,\mathrm{N}_{E/F}(E^{*}) : \mathrm{N}_{E/F}(E^{*})] = [U_F : \mathrm{N}_{E/F}\,U_E]$$

(ver Corolario 3.4.7). En consecuencia,

$$f(E|F) = \frac{[E:F]}{e(E|F)} = [F^{*} : U_F\,\mathrm{N}_{E/F}(E^{*})]$$

es el orden de π en $F^{*}/U_F\,\mathrm{N}_{E/F}(E^{*})$ para cualquier elemento primo π de F.

Cuando la extensión E/F es no abeliana, se tiene

$$[F^{*} : \mathrm{N}_{E/F}(E^{*})] < [E:F].$$

Una vez que la teoría local de campos de clase fue establecida, el siguiente paso fue obtener los teoremas de la teoría global de campos de clase por medio de aquéllos de la teoría local. El concepto que permite hacer esto son los *idèles*, los cuales también permiten teoría de campos de clase globales para extensiones abelianas infinitas.

Definición 2.5.11 (Chevalley, 1936). El *grupo de idèles* J_K de un campo numérico K es el conjunto de sucesiones $\vec{x} = (x_v)_v$ indexadas por el conjunto de lugares v de K, tales que $x_v \in K_v^*$ para toda v y además $x_v \in \mathcal{O}_v^* = U_{K_v} = U_v$ para casi todos los lugares v (es decir, para todos, salvo un número finito) y donde $\mathcal{O}_v$ denota al anillo de enteros de K_v, el campo completado de K en v, y $U_{K_v} = \mathcal{O}_v^*$ es el grupo de unidades de $\mathcal{O}_v$.

Un elemento de J_K se llama *idèle*. Este fue el nombre sugerido por Hasse a Chevalley, el cual los había llamado originalmente como *elemento ideal*. J_K es un grupo bajo la multiplicación entrada por entrada. Se tiene el encaje diagonal $K^* \hookrightarrow J_K$ y la imagen se llama el *grupo de los idèles principales*. Similarmente se tiene el encaje $\lceil\ \rfloor_v \colon K_v^* \hookrightarrow J_K$ tal que $x_v \in K_v^*$ se mapea a x_v en la entrada v y con 1 en las demás componentes.

Para $\vec{x} \in J_K$ se tiene el ideal fraccionario (recordemos que estamos en campos numéricos),

$$\imath(\vec{x}) = \mathfrak{a}_{\vec{x}} = \prod_{v \nmid \infty} \mathfrak{p}_v^{v(x_v)}$$

lo cual permite pasar de idèles a ideales.

Usando este paso de idèles a ideales se tiene que cualquier grupo de clase generalizado de K se puede realizar como un grupo cociente de J_K como sigue: sea $\mathfrak{m}$ un K–módulus. Sean $\vec{x} \in J_K$, $\alpha_0 \in K^*$ tal que para todo $\mathfrak{p}$ en el soporte de $\mathfrak{m}$, se cumple $v_\mathfrak{p}(x_\mathfrak{p}/\alpha_0 - 1) \geq v_\mathfrak{p}(\mathfrak{m})$ cuando $\mathfrak{p}|\mathfrak{m}_f$ (la parte finita de $\mathfrak{m}$) y $x_\mathfrak{p}/v_\mathfrak{p}(\alpha_0) > 0$ cuando $\mathfrak{p}|\mathfrak{m}_\infty$ (la parte infinita de $\mathfrak{m}$). Lo anterior se puede lograr gracias al Teorema de Aproximación de Artin, Teorema 2.1.1.

El idèle $\frac{\vec{x}}{\alpha_0} = \left(\ldots, \frac{x_\mathfrak{q}}{\alpha_0}, \ldots\right)_\mathfrak{q}$ tiene ideal correspondiente $\imath\left(\frac{\vec{x}}{\alpha_0}\right) \in D_K^\mathfrak{m}$ y además $\overline{\imath\left(\frac{\vec{x}}{\alpha_0}\right)} \in D_K^\mathfrak{m}/P_{K,\mathfrak{m}}^+$ está bien definido. El núcleo del mapeo $J_K \to D_K^\mathfrak{m}/P_{D,\mathfrak{m}}^+$ contiene a los ideales principales, por lo que $D_K^\mathfrak{m}/P_{K,\mathfrak{m}}^+ \cong J_K/K^*S_\mathfrak{m}$ para algún $S_\mathfrak{m} \subseteq J_K$.

Resulta que dos grupos de ideales H y H' son equivalentes (es decir $H \cap D_K^{\mathfrak{m}''} = H' \cap D_K^{\mathfrak{m}''}$ para algún múltiplo $\mathfrak{m}''$ de $\mathfrak{m}$ y $\mathfrak{m}'$) corresponden al mismo grupo de idèles.

El mapeo de Artin es el siguiente:

$$\psi_{L/K} \colon J_K \longrightarrow D_K^\mathfrak{m}/P_{K,\mathfrak{m}}^+ \xrightarrow{\psi_{L/K,\mathfrak{m}}} \mathrm{Gal}(L/K),$$

y se tiene que $\psi_{L/K}$ es suprayectiva e independiente de la elección del módulus admisible $\mathfrak{m}$. Además $\psi_{L/K}(K^*) = 1$.

Si L/K es una extensión de Galois, se define la norma de J_L a J_K como $\mathrm{N}_{L/K} \colon J_K \to J_K$ definida por $\mathrm{N}_{L/K}(\vec{y}) = \vec{x}$ donde $x_\mathfrak{p} = \prod_{\mathfrak{P}|\mathfrak{p}} \mathrm{N}_{L_\mathfrak{P}/K_\mathfrak{p}}(y_\mathfrak{P})$.

Entonces $\mathrm{núc}\, \psi_{L/K} = K^* \mathrm{N}_{L/K}(J_L)$ en el caso de que L/K sea una extensión abeliana.

Para que la correspondencia entre extensiones abelianas de K y subgrupos de idèles sea biyectiva, se necesita hacer de J_K un espacio topológico. La topología dada es la topología del producto restringido: una base de vecindades

abiertas de $\vec{1} \in J_K$ está formado por los conjuntos $\prod_{\mathfrak{p}} V_{\mathfrak{p}}$ donde $V_{\mathfrak{p}}$ es una vecindad abierta de $1 \in K_{\mathfrak{p}}^*$ para toda $\mathfrak{p}$ y $V_{\mathfrak{p}} = U_{\mathfrak{p}} = \mathcal{O}_{\mathfrak{p}}^*$ para casi todo $\mathfrak{p}$. Entonces J_K es un grupo topológico localmente compacto (la topología producto no es localmente compacta).

Teorema 2.5.12. *Para una extensión abeliana finita de campos numéricos L/K, el mapeo de Artin $\psi_{L/K}$ es un epimorfismo de J_K sobre* $\mathrm{Gal}(L/K)$ *con núcleo $K^* \,\mathrm{N}_{L/K}(J_L)$ por lo que $J_K/K^* \,\mathrm{N}_{L/K}(J_L) \cong \mathrm{Gal}(L/K)$. La correspondencia que asocia a cada extensión abeliana finita L de K con el subgrupo $K^* \,\mathrm{N}_{L/K}(J_L)$ es biyectiva entre las extensiones abelianas finitas de K y los subgrupos abiertos de índice finito de J_K y que contienen a K^*. La correspondencia voltea contenciones.* □

Para un lugar $\mathfrak{p}$ de K, la composición

$$L_{\mathfrak{P}}^* \xrightarrow{\mathrm{N}_{L_{\mathfrak{P}}/K_{\mathfrak{p}}}} K_{\mathfrak{p}}^* \xrightarrow{\lceil\ \rceil_{\mathfrak{p}}} J_K \xrightarrow{\psi_{L/K}} \mathrm{Gal}(L/K)$$

tiene como imagen el grupo de descomposición $D(\mathfrak{P}|\mathfrak{p})$ y la imagen de $\mathcal{O}_{\mathfrak{P}}^* = U_{\mathfrak{P}}$ es el grupo de inercia $I(\mathfrak{P}|\mathfrak{p})$. Además $\mathrm{Gal}(K^{\mathrm{ab}}/K)$ es el máximo grupo cociente de J_K/K^* totalmente disconexo.

Más aún, para $\vec{x} \in J_K$, $\psi_{L/K}(\vec{x}) = \prod_{\mathfrak{p}}(x_{\mathfrak{p}}, L_{\mathfrak{P}}/K_{\mathfrak{p}})$ donde $(x_{\mathfrak{p}}, L_{\mathfrak{P}}/K_{\mathfrak{p}})$ es mapeo local de Artin, $(x_{\mathfrak{p}}, L_{\mathfrak{P}}/K_{\mathfrak{p}}) \in \mathrm{Gal}(L_{\mathfrak{P}}/K_{\mathfrak{p}}) \cong D(\mathfrak{P}|\mathfrak{p})$ y para cada $\mathfrak{p}$ seleccionamos un único $\mathfrak{P}|\mathfrak{p}$, cualquiera pero únicamente uno y en general se denota $L_{\mathfrak{p}}$ en lugar de $L_{\mathfrak{P}}$.

2.5.3. Campos de funciones

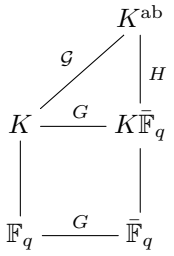
Hasse probó que los teoremas de teoría local de campos de clase son los mismos en característica 0 que en característica $p > 0$, excepto que necesitamos ser explícitos acerca de usar subgrupos abiertos de índice finito.

En 1935 Witt probó el *Teorema de Existencia* para extensiones abelianas con grado divisible por p lo cual completó el trabajo de Schmidt para extensiones abelianas de grado no divisible por p.

El punto de vista de Chevalley por medio de idèles funciona en ambos casos, campos numéricos y campos de funciones, sin embargo tenemos una diferencia entre los dos casos para extensiones abelianas infinitas. Para un campo de funciones K, como en el caso numérico, el mapeo de Artin $J_K/K^* \to \mathrm{Gal}(K^{\mathrm{ab}}/K)$ tiene imagen densa, pero ahora el mapeo es inyectivo en lugar de suprayectivo (la demostración de la suprayectividad en el caso de campos de números falla en el caso de campos de funciones pues no existen lugares arquimedianos en estos últimos).

La imagen del mapeo de Artin en el caso de campos de funciones está caracterizado como el conjunto de elementos de $\mathrm{Gal}(K^{\mathrm{ab}}/K)$ los cuales, en la cerradura algebraica del campo de constantes de K, son potencias enteras del automorfismo de Frobenius.

Más precisamente, se tiene $\bar{\mathbb{F}}_q = \mathbb{F}_q^{\mathrm{ab}}$ y el siguiente diagrama



Sean $\mathcal{G} = \mathrm{Gal}(K^{\mathrm{ab}}/K)$, $H = \mathrm{Gal}(K^{\mathrm{ab}}/K\bar{\mathbb{F}}_q)$ y $G = \mathrm{Gal}(K\bar{\mathbb{F}}_q/K) \cong \mathrm{Gal}(\bar{\mathbb{F}}_q/\mathbb{F}_q) \cong \hat{\mathbb{Z}}$ la completación de $\mathbb{Z}$. Entonces $G \cong \mathcal{G}/H$.

El mapeo $\psi\colon J_K/K^* \longrightarrow \mathcal{G} = \mathrm{Gal}(K^{\mathrm{ab}}/K)$ satisface que $\operatorname{im}\psi = \{\sigma \in \mathcal{G} \mid \sigma|_{K\bar{\mathbb{F}}_q} \in \mathbb{Z}\}$ donde $\sigma|_{K\bar{\mathbb{F}}_q} \in \mathbb{Z}$ significa que si τ es el Frobenius de K, esto es, $\tau x = x^q$, entonces $\sigma|_{K\bar{\mathbb{F}}_q} = \tau^m$ para alguna $m \in \mathbb{Z}$.

Para finalizar, la teoría de campos de clase no provee campos de clase de manera explícita. En el caso de campos de números, únicamente tenemos los campos de clase explícitos para $\mathbb{Q}$ (Teorema de Kronecker–Weber, campos ciclotómicos) y para los campos cuadráticos imaginarios. De hecho, en 1880 Kronecker en una carta a Dedekind describió su "*sueño de juventud*" ("*Jugendtraum*" en alemán), como poder describir las extensiones abelianas de un campo numérico por medio de extensiones generadas por raíces de algunas funciones transcendentes. El sueño de Kronecker no se ha materializado todavía.

Para campos de funciones, D. Hayes en 1974, basado en el trabajo de su asesor, L. Carlitz, construyó una teoría de campos de clase explícita sobre el campo de funciones racionales $\mathbb{F}_q(T)$. Ver [136, Capítulo 9].

Drinfeld en el mismo año (1974), usando "*módulos elípticos*", ahora conocidos como "*módulos de Drinfeld*", hizo explícita la obtención de los campos de clase sobre cualquier campo de funciones congruente.

Lo que hace diferente lo explícito entre los campos numéricos y los campos de funciones es que, en característica $p > 0$, hay muchas funciones aditivas (ver el [136, Capítulo 15] sobre los módulos de Drinfeld).

3

Campos locales

3.1. Generalidades

En esta sección presentamos los resultados fundamentales de los campos locales. Hacemos notar que varios de los resultados para campos locales siguen siendo válidos para campos completos con respecto a una valuación.

Definición 3.1.1. Dados un campo K y $v = v_K \colon K^* \to \mathbb{R}$ una valuación, es decir, v satisface $v(xy) = v(x) + v(y)$ y $v(x+y) \geq \text{mín}\{v(x), v(y)\}$ para cualesquiera $x, y \in K^*$, donde escribimos $v(0) = \infty$, se define el *valor absoluto* por $|x|_v = |x| = c^{v(x)}$ con $0 < c < 1$ fijo arbitrario. La topología dada a K por $|\ |_v$ es independiente del c seleccionado.

Definición 3.1.2. Una valuación se llama *discreta* si $v(K^*) \cong \mathbb{Z}$. Una valuación discreta v se llama *normalizada* si $v(K^*) = \mathbb{Z}$.

En este capítulo únicamente se estudiarán valuaciones discretas.

Consideraremos campos completos con respecto a $|\ |_v$. Sea $\mathcal{O}_K = \{x \in K \mid v(x) \geq 0\}$ el *anillo de valuación*. Entonces $\mathcal{O}_K$ es un anillo local (de hecho, es un anillo de valuación) con ideal máximo $\mathfrak{p}_K = \mathfrak{p} = \{x \in K \mid v(x) > 0\}$. Se tiene que $\mathcal{O}_K = \bar{B}_{|\ |_v}(0,1) = \{x \in K \mid |x|_v \leq 1\}$ es la bola cerrada, $\mathfrak{p} = B_{|\ |_v}(0,1) = \{x \in K \mid |x|_v < 1\}$ es la bola abierta y $\tilde{K} = K(\mathfrak{p}) = \mathcal{O}_K/\mathfrak{p}$ es el *campo residual*.

Definición 3.1.3. Las unidades de K se definen por $U_K := \mathcal{O}_K^* = \mathcal{O}_K \setminus \mathfrak{p} = \{a \in K^* \mid v(x) = 0\} = \{x \in K \mid |x|_v = 1\}$, es decir, U_K es la frontera de la bola unitaria con centro en 0.

Si v_K es discreta, entonces $v_K(K^*) = \beta\mathbb{Z}$ para algún $\beta \in \mathbb{R}^+$. Sea $\pi \in K$ con $v_K(\pi) = \beta$. Sea $\xi \in \mathfrak{p}$, digamos $v_K(\xi) = \beta n$ para algún $n \geq 1$. De esta forma tenemos que $v_K(\xi\pi^{-n}) = 0$, esto es, $\xi\pi^{-n} = u \in U_K$ es una unidad y $\xi = u\pi^n \in \mathfrak{p}$. Se sigue que $\mathfrak{p} = \langle\pi\rangle$ es principal. Recíprocamente, si $\mathfrak{p} = \langle\pi\rangle$ es principal, sea $v_K(\pi) = \alpha \in \mathbb{R}^+$. Para $\xi \in K^*$, $\xi = \frac{a}{b}$, $a, b \in \mathcal{O}_K$, con $b \neq 0$, se

tiene $v_K(\xi) = v_K(a) - v_K(b)$. Para $a \in \mathcal{O}_K$, si $a \in U_K$, $v_K(a) = 0 = 0 \cdot \alpha$; si $a \in \mathfrak{p}_K$, $a = a_1\pi$ con $a_1 \in \mathcal{O}_K$. Repitiendo el proceso para a_1 concluimos que existe $n \in \mathbb{N}$ y $a_n \in U_K$ con $a = a_n\pi^n$. Se sigue que $v_K(a) = n\alpha$. Por tanto $v_K(K^*) = \alpha\mathbb{Z}$ y v_K es discreta. En resumen, hemos probado que

Proposición 3.1.4. *Una valuación v_K es discreta si y sólo si $\mathfrak{p}_K$ es un ideal principal.* □

Si $\operatorname{car} \tilde{K} = 0$ entonces $\operatorname{car} K = 0$. Si $\operatorname{car} \tilde{K} = p > 0$, entonces puede ser $\operatorname{car} K = p$ o $\operatorname{car} K = 0$.

Definición 3.1.5. Un campo K completo con respecto a una valuación se llama *local* si $\tilde{K}$ es un campo finito.

Por razones técnicas para la teoría de campos globales, a veces se consideran tanto a $\mathbb{R}$ como a $\mathbb{C}$ como campos locales.

En el caso de un campo local, se seleccionará al número $0 < c < 1$ que define el valor absoluto como $c = q^{-1}$ donde el campo residual de K es $\mathbb{F}_q$.

Definición 3.1.6. Sea v normalizada. Un *elemento primo* o *elemento uniformizante* $\pi_K = \pi$ de K es cualquier elemento de valuación 1: $v(\pi) = 1$.

Sea L/K una extensión de campos, w una valuación de L y sea $v := w|_K$. Entonces $\mathcal{O}_K = K \cap \mathcal{O}_L$, $\mathfrak{p}_K = K \cap \mathfrak{p}_L$, $\tilde{K} = \mathcal{O}_K/\mathfrak{p}_K = \mathcal{O}_K/(\mathcal{O}_K \cap \mathfrak{p}_L) \cong (\mathfrak{p}_L + \mathcal{O}_K)/\mathfrak{p}_L \subseteq \mathcal{O}_L/\mathfrak{p}_L = \tilde{L}$. Se tiene que $v(K^*) \subseteq w(L^*) \subseteq \mathbb{R}^+$. Además $U_K = \{x \in \mathcal{O}_K \mid v(x) = 0\}$ y $K^*/U_K \cong v(K^*)$.

Definición 3.1.7. El *índice de ramificación* e, y el *grado de inercia* f, se definen por:

$$e = e(\mathfrak{p}_L|\mathfrak{p}_K) = e(w|v) = e(L|K) = [w(L^*) : v(K^*)],$$
$$f = f(\mathfrak{p}_L|\mathfrak{p}_K) = f(w|v) = f(L|K) = [\tilde{L} : \tilde{K}].$$

Dado cualquier campo K con valuación v, sea $\bar{K}$ la completación de K con respecto a la topología dada por v. Entonces dado $x \in \bar{K}$, existe $\{x_n\}_{n=0}^{\infty} \subseteq K$ con $\lim_{n\to\infty} x_n = x$. Entonces v se extiende a $\bar{K}$ como $\bar{v}(x) = \lim_{n\to\infty} v(x_n) = \lim_{n\to\infty} \bar{v}(x_n)$. Es claro que $\bar{v}$ no depende la sucesión $\{x_n\}_{n=0}^{\infty}$ y que $\bar{v}$ es única. Sea $w := \bar{v}$. Como w no depende de la sucesión, si $x = 0$ podemos tomar $x_n = 0$ para toda n y $w(0) = \infty = v(x_n)$.

Sea $x \neq 0$, $x_n \neq 0$ y $v(x_n) \xrightarrow[n\to\infty]{} w(x) \neq 0$. Por otro lado $x - x_n \xrightarrow[n\to\infty]{} 0$, por lo que $v(x - x_n) \xrightarrow[n\to\infty]{} \infty$. Por tanto

$$w(x) = w(x - x_n + x_n) = \min\{w(x - x_n), w(x_n)\} = w(x_n) = v(x_n),$$

para toda n suficientemente grande. Por tanto $w(\bar{K}^*) = v(K^*)$ de donde se sigue que $e = e(\bar{K}|K) = 1$. También, tenemos el isomorfismo $\tilde{\bar{K}} = \tilde{K}$ de donde se obtiene que $f = f(\bar{K}|K) = 1$.

Un resultado para campos completos con respecto a una valuación es el Lema de Hensel. La versión que es útil para nuestros fines es la siguiente.

Teorema 3.1.8 (Lema de Hensel). *Sea K un campo completo con respecto a una valuación v y anillo de enteros $A = \{x \mid v(x) \geq 0\}$ un anillo de valuación discreta. Sean $f(x) \in A[x]$ un polinomio y $\bar{f} := f \bmod \mathfrak{p}$ donde $\mathfrak{p}$ es el ideal máximo de A. Entonces cualquier raíz simple λ de $\bar{f}$ en $A/\mathfrak{p}$ se levanta de manera única a una raíz de f en A, es decir, existe un único $\alpha \in A$ tal que $f(\alpha) = 0$ y donde $\bar{\alpha} = \lambda$.*

Demostración. Sea $\beta \in A$ una tal raíz de f, es decir, $\bar{\beta} = \lambda$. Entonces $f(x) = (x-\beta)g(x)$ con $\bar{g}(\lambda) \neq 0$. Si γ es otra raíz de f con $\bar{\gamma} = \lambda$, entonces $f(\gamma) = (\gamma-\beta)g(\gamma) = 0$. Ahora bien $g(\gamma) \bmod \mathfrak{p} = \bar{g}(\lambda) \neq 0$, por lo que $g(\gamma) \in A \setminus \mathfrak{p}$, es decir, $g(\gamma)$ es invertible en A. Por tanto $\gamma = \beta$, de donde se sigue la unicidad del levantamiento de la raíz.

Para la existencia, sea $\beta_1 \in A$ tal que $\bar{\beta}_1 = \lambda$. Entonces $f(\beta_1) \equiv 0 \bmod \mathfrak{p}$. Supongamos que hemos hallado $\beta_n \in A$ tal que $\bar{\beta}_n = \lambda$ y $f(\beta_n) \equiv 0 \bmod \mathfrak{p}^n$. Hallaremos $\beta_{n+1} \in A$ tal que $\beta_{n+1} = \beta_n \bmod \mathfrak{p}^n$ y $f(\beta_{n+1}) \equiv 0 \bmod \mathfrak{p}^{n+1}$.

Sea $h \in \mathfrak{p}^n$ por determinarse y sea $\beta_{n+1} = \beta_n + h$. Desarrollando en serie de Taylor se tiene $f(\beta_{n+1}) = f(\beta_n) + hf'(\beta_n) + h^2 y$ para algún $y \in A$. Se tiene que $h^2 y \in \mathfrak{p}^{2n}$. Necesitamos que $f(\beta_n) + hf'(\beta_n) \equiv 0 \bmod \mathfrak{p}^{n+1}$. Puesto que λ es raíz simple de $\bar{f}$, se tiene que $\bar{f}'(\lambda) = \bar{f}'(\bar{\beta}_n) \neq 0$. Se sigue que $f'(\beta_n) \in A \setminus \mathfrak{p}$, esto es, $f'(\beta_n)$ es invertible y la ecuación

$$h = \frac{\xi - f(\beta_n)}{f'(\beta_n)} \in \mathfrak{p}^n,$$

con $\xi \in \mathfrak{p}^{n+1}$ arbitrario ($\xi - f(\beta_n) \in \mathfrak{p}^n$) tiene solución y $f(\beta_n) + hf'(\beta_n) \equiv \xi \equiv 0 \bmod \mathfrak{p}^{n+1}$.

Sea $\beta := \lim_{n\to\infty} \beta_n$ el cual existe, $\beta \in A$ y $f(\beta) = 0$. □

En el caso de un campo de funciones congruente, $\mathscr{K}/\mathbb{F}_q$, si $\mathfrak{p}$ es un lugar de $\mathscr{K}$ y $\mathscr{K}_\mathfrak{p}$ es la completación con respecto a la valuación $v_\mathfrak{p}$, $\mathscr{K}_\mathfrak{p} \cong \mathbb{F}_{q^d}((\pi))$ donde $[\tilde{\mathscr{K}} : \mathbb{F}_q] = d$, esto es, $\tilde{\mathscr{K}} = \mathbb{F}_{q^d}$ y $\pi \in \mathscr{K}$ es un elemento tal que $v_\mathfrak{p}(\pi) = 1$.

Se tiene que los campos residuales de $\mathscr{K}_\mathfrak{p}$ y de $\mathscr{K}$ en $\mathfrak{p}$ son isomorfos, es decir, $\mathcal{O}_{\tilde{\mathfrak{p}}}/\tilde{\mathfrak{p}} \cong \mathcal{O}_\mathfrak{p}/\mathfrak{p}$. El isomorfismo se sigue del mapeo $\xi\colon \mathcal{O}_\mathfrak{p} \hookrightarrow \mathcal{O}_{\tilde{\mathfrak{p}}} \twoheadrightarrow \mathcal{O}_{\tilde{\mathfrak{p}}}/\tilde{\mathfrak{p}}$ donde el primer mapeo es la inyección natural y el segundo es la proyección natural; ξ es suprayectiva y $\operatorname{núc}\xi = \mathfrak{p}$ (ver [160, Proposition 2.3.10]). Ponemos $\mathfrak{p} = \mathfrak{p}_K$.

Proposición 3.1.9. *Si K es un campo local, entonces como grupo multiplicativo se tiene*

$$K^* = \langle\pi\rangle \times U_K = \langle\pi\rangle \times \mathbb{F}_q^* \times U_K^{(1)}$$

donde $\mathbb{F}_q$ es el campo residual $\tilde{K}$ de K,

$$U_K^{(n)} = 1 + \mathfrak{p}_K^n = \{a \in K \mid a \equiv 1 \bmod \pi^n\}, \quad n \geq 1,$$
$$U_K = U_K^{(0)} = \{a \in K \mid v_K(a) = 0\} = \{a \in K \mid |a|_v = 1\},$$

esto es, $U_K = \mathcal{O}_K^*$ *es la circunferencia unitaria y* $q = |\tilde{K}|$. *Notemos que* $U_K^{(0)} \neq 1 + \mathfrak{p}^0 = \mathcal{O}_K$.

Al grupo $U_K^{(n)}$ *se le llama el grupo de las* n–unidades principales, $n \geq 1$ *y se define* $|x|_v = q^{-v(x)}$, *es decir, seleccionamos* $c = q^{-1}$ *en la Definición* 3.1.1. *Además* $\mathbb{F}_q^* \cong W_{q-1}$, *donde* W_t *denota al grupo de las* t–*raíces de uno,* $\mathfrak{p} = \pi\mathcal{O}_K$, $\langle\pi\rangle = \{\pi^m \mid m \in \mathbb{Z}\} \cong \mathbb{Z}$.

Finalmente tenemos

$$U_K/U_K^{(1)} \cong \tilde{K}^* = \mathbb{F}_q^* \text{ (}\textit{multiplicativo}\text{) } y$$
$$U_K^{(n)}/U_K^{(n+1)} \cong \mathfrak{p}_K^n/\mathfrak{p}_K^{n+1} \cong \tilde{K} \cong \mathbb{F}_q, n \geq 1 \text{ (}\textit{aditivo}\text{).}$$

Demostración. Sea $a \in K^*$ con $v_K(a) = n \in \mathbb{Z}$. Entonces $v_K(a\pi^{-n}) = 0$, es decir, $a\pi^{-n} = u \in U_K$ y $a = \pi^n u$. Por tanto la descomposición $a = \pi^{v_K(a)}u$ es única.

Veamos que la representación es única. Digamos que $a = \pi^m u_1 = \pi^n u$, por lo que $v_K(a) = m = n$ y $u_1 = u$. Se sigue que la función $K^* \to \langle\pi\rangle \times U_K$, $a \mapsto (\pi^{v_K(a)}, a\pi^{-v_K(a)})$ es un isomorfismo de grupos.

Ahora $U_K \xrightarrow{\varphi} \left(\mathcal{O}_K/\mathfrak{p}_K\right)^*$, $u \mapsto u \bmod \mathfrak{p}_K$ es un homomorfismo de grupos y $\operatorname{núc}\varphi = \{u \in U_K \mid u \equiv 1 \bmod \mathfrak{p}_K\} = U_K^{(1)}$. Se tiene que φ es un epimorfismo pues si $\xi \bmod \mathfrak{p} \in \left(\mathcal{O}_K/\mathfrak{p}_K\right)^*$ se tiene $v_K(\xi) = 0$, por lo que $\xi \in U_K$.

La ecuación $X^{q-1} - 1$ se descompone totalmente en $\mathcal{O}_K$ por el Lema de Hensel, Teorema 3.1.8. Las raíces de $X^{q-1} - 1$ son los elementos de $\mathbb{F}_q^*$ y por tanto la sucesión

$$1 \longrightarrow U_K^{(1)} \longrightarrow U_K \longrightarrow \left(\mathcal{O}_K/\mathfrak{p}_K\right)^* \cong \mathbb{F}_q^* \longrightarrow 1,$$

se escinde y $U_K \cong \mathbb{F}_q^* \times U_K^{(1)}$ como grupos.

Para $n \geq 1$ se tiene que $U_K^{(n)} \xrightarrow{\theta} \mathcal{O}_K/\mathfrak{p}_K$ dada por $1 + x\pi^n \longrightarrow x \bmod p_K$ es un epimorfismo y $\operatorname{núc}\theta = \{1 + x\pi^n \mid x \in \mathfrak{p}_K\} = U_K^{(n+1)}$. Por tanto $U_K^{(n)}/U_K^{(n+1)} \cong \mathcal{O}_K/\mathfrak{p}_K \cong \mathbb{F}_q$.

Finalmente, se verifica directamente que el mapeo

$$U_K^{(n)}/U_K^{(n+1)} \xrightarrow{g} \mathfrak{p}_K^n/\mathfrak{p}_K^{n+1}, \qquad (1 + a\pi^n) \bmod U_K^{(n+1)} \mapsto a\pi^n \bmod \mathfrak{p}_K^{n+1}$$

es un isomorfismo de grupos. □

Notemos que, puesto que $U_K \supseteq U_K^{(1)} \supseteq \cdots \supseteq U_K^{(n)}$, se obtiene el siguiente corolario.

Corolario 3.1.10. *Para* $n \geq 1$,

$$\left|U_K/U_K^{(n)}\right| = \prod_{i=0}^{n-1} \left|U_K^{(i)}/U_K^{(i+1)}\right| = \left|U_K/U_K^{(1)}\right| \cdot \left|\prod_{i=1}^{n-1} \left|U_K^{(i)}/U_K^{(i+1)}\right|\right.$$
$$= \left|\mathbb{F}_q^*\right| \cdot \left|\prod_{i=1}^{n-1} \mathfrak{p}^i/\mathfrak{p}^{i+1}\right| = \left|\mathbb{F}_q^*\right| \cdot \left|\prod_{i=1}^{n-1} \mathcal{O}_K/\mathfrak{p}\right| = (q-1)q^{n-1}.$$

Además, tenemos

$$\mathcal{O}_K/\mathfrak{p}_K \xrightarrow{\cong} \mathfrak{p}_K^n/\mathfrak{p}_K^{n+1}, \quad x \longmapsto x\pi_K^n$$

y

$$\left|\mathcal{O}_K/\mathfrak{p}_K\right| = \Big|\prod_{m=1}^{n} \mathfrak{p}_K^{m-1}/\mathfrak{p}_K^m\Big| = q^n. \qquad \square$$

Ejemplo 3.1.11. . Consideremos $K = \mathbb{Q}_p$ el campo de los números p–ádicos. El anillo de enteros de K es el anillo de los enteros p–ádicos: $\mathcal{O}_K = \mathbb{Z}_p$. Ahora bien $U_K = \mathcal{O}_K^* \cong \mathbb{Z}_p^*$. Se tiene $\mathbb{Z}_p^* = \left\{\xi\big(1 + p\sum_{n=0}^{\infty} a_n p^n\big) \mid \xi \in \mathbb{F}_p^*, a_n \in \mathbb{F}_p\right\} \cong \mathbb{F}_p^* \times (1 + p\mathbb{Z}_p) = \mathbb{F}_p^* \times U_K^{(1)}$. Esto es $U_K^{(1)} \cong 1 + p\mathbb{Z}_p$. Notemos que si $p = 2$, $U_K = U_K^{(1)} \cong 1 + 2\mathbb{Z}_2$. De esta forma tenemos que $\mathbb{Z}_p^* \cong \mathbb{F}_p^* \times (1 + p\mathbb{Z}_p)$ y

$$1 + p\mathbb{Z}_p = \begin{cases} \mathbb{Z}_p, & p \geq 3, \\ C_2 \times (1 + 4\mathbb{Z}_2), & p = 2. \end{cases}$$

Más en general, para $n \in \mathbb{N}$, se tiene $U_K^{(n)} = 1 + p^n\mathbb{Z}_p$.

Definición 3.1.12. Sea K un campo cualquiera con un valor absoluto $|\ |_K$. Sea V un espacio vectorial de dimensión n, entonces una *norma* $\mathcal{N}$ de V es función $\mathcal{N}\colon V \longrightarrow \mathbb{R}^+ \cup \{0\}$ tal que

(1) $\mathcal{N}(v) \geq 0$ para toda $v \in V$ y $\mathcal{N}(v) = 0 \iff v = 0$.
(2) $\mathcal{N}(v_1 + v_2) \leq \mathcal{N}(v_1) + \mathcal{N}(v_2)$ para cualesquiera $v_1, v_2 \in V$.
(3) $\mathcal{N}(\alpha v) = |\alpha|_K \mathcal{N}(v)$ para toda $\alpha \in K$ y toda $v \in V$.

Teorema 3.1.13. *Sean K un campo valuado completo y V un K-espacio vectorial de dimensión finita n. Entonces cualesquiera dos normas $\mathcal{N}_1, \mathcal{N}_2$ de V definen la misma topología de V y V es un espacio completo con la métrica inducida.*

Demostración. Por inducción en n. Para $n = 1$, si $\{w_1\}$ es base de V/K ($V \cong K$), entonces si $\mathcal{N}$ es una norma en V, entonces para $v = \alpha_1 w_1 \in V$, $\mathcal{N}(v) = |\alpha_1|_K \mathcal{N}(w_1) = \lambda|\alpha_1|_K$ con $\lambda = \mathcal{N}(w_1) > 0$. Por tanto $\mathcal{N} = \lambda|\ |_K$ y el resultado se sigue.

Sea $n > 1$ y suponemos cierto el resultado para cualquier K-espacio vectorial de dimensión $m \leq n - 1$. Sea $\{w_1, \ldots, w_n\}$ una base de V/K. Sea $\mathcal{N}_\infty$ la norma infinita de V, es decir,

$$\mathcal{N}_\infty(\alpha_1 w_1 + \cdots + \alpha_n w_n) = \max_{1 \leq j \leq n} \{|\alpha_j|_K\}.$$

Se tiene que $\mathcal{N}_\infty$ es una norma de V y V es completo con respecto a $\mathcal{N}_\infty$.

Sea $\mathcal{N}$ una norma arbitraria de V. Sea $v = \alpha_1 w_1 + \cdots + \alpha_n w_n$, entonces $\mathcal{N}(v) = \mathcal{N}(\alpha_1 w_1 + \cdots + \alpha_n w_n) \leq \sum_{j=1}^n \mathcal{N}(\alpha_j w_j) = \sum_{j=1}^n |\alpha_j|_K \mathcal{N}(w_j) \leq$

$c\mathcal{N}_\infty(v)$ donde $c = \sum_{j=1}^n \mathcal{N}(w_j) > 0$. Por tanto $\mathcal{N}(v) \leq c\mathcal{N}_\infty(v)$ para toda $v \in V$.

Lo anterior prueba que la topología definida por $\mathcal{N}_\infty$ es más fina que la definida de $\mathcal{N}$. Para probar que la topología de $\mathcal{N}$ es más fina que la definida por $\mathcal{N}_\infty$, basta probar que dado $r > 0$, existe $\delta = \delta(r) > 0$ tal que si $v = \sum_{j=1}^n \alpha_j w_j$ es tal que $\mathcal{N}(v) < \delta$, entonces $\mathcal{N}_\infty(v) < r$.

Supongamos que no se cumple la condición anterior, es decir, existe $r > 0$ tal que dado $\delta > 0$, existe $v_\delta \in V$ con $\mathcal{N}(v_\delta) < \delta$ pero $\mathcal{N}_\infty(v_\delta) \geq r$. Para $\delta_m = \frac{1}{m} > 0$, existe $v_{\delta_m} =: v_m$ con $\mathcal{N}(v_m) < \frac{1}{m}$ pero $\mathcal{N}_\infty(v_m) \geq r$. Consideremos $\{v_m\}_{m=1}^\infty$, $\mathcal{N}_\infty(v_m) = |\alpha_j^{(m)}|_K \geq r$ donde $v_m = \alpha_1^{(m)} w_1 + \cdots + \alpha_n^{(m)} w_n$. Puesto que $\{v_m\}_{m=1}^\infty$ es infinito, existe un índice j_0 y una subsucesión $\{v_{m_t}\}_{t=1}^\infty$ con $\mathcal{N}_\infty(v_{m_t}) = |\alpha_{j_0}^{(m_t)}|_K \geq r$. Sin pérdida de generalidad, podemos suponer $j_0 = n$ y $\{v_{m_t}\}_{t=1}^\infty = \{v_m\}_{m=1}^\infty$, es decir $\mathcal{N}(v_m) < \frac{1}{m}$ pero $|\alpha_n^{(m)}|_K \geq r > 0$.

Sea $u_m := \frac{v_m}{\alpha_n^{(m)}} = \xi_1^{(m)} w_1 + \cdots + \xi_{n-1}^{(m)} w_{n-1} + w_n$ donde $\xi_j^{(m)} = \frac{\alpha_j^{(m)}}{\alpha_n^{(m)}}$. Entonces $\mathcal{N}(u_m) < \frac{1}{mr}$, $r \leq |\alpha_n^{(m)}|_K$, $\frac{1}{|\alpha_n^{(m)}|_K} \leq \frac{1}{r}$.

Además $u_m - u_t = \sum_{j=1}^{n-1} (\xi_j^{(m)} - \xi_j^{(t)}) w_j$ y $\mathcal{N}(u_m - u_t) \leq \mathcal{N}(u_m) + \mathcal{N}(u_t) < \frac{1}{mr} + \frac{1}{tr}$.

Por hipótesis de inducción, $\mathcal{N}|_{V'}$ induce la misma topología a la de $\mathcal{N}_\infty|_{V'}$ donde V' es el subespacio de V generado por $\{w_1, \ldots, w_{n-1}\}$. Ahora, dado $\epsilon > 0$, existe $t \in \mathbb{N}$ tal que para toda $m \geq t$, se tiene $u_m - u_t \in B_{\mathcal{N}}(0, \epsilon)$. Como $\mathcal{N}_\infty$ induce la misma topología, existe $\delta > 0$ tal que $u_m - u_t \in B_{\mathcal{N}_\infty}(0, \delta) \subseteq B_{\mathcal{N}}(0, \epsilon)$ y $\mathcal{N}_\infty(u_m - u_t) = \max_{1 \leq j \leq n-1} |\xi_j^{(m)} - \xi_j^{(t)}|_K$ para toda j con $1 \leq j \leq n-1$. Por tanto $\{\xi_j^{(m)}\}_{m=1}^\infty$ es una sucesión de Cauchy y como K es completo, la sucesión es convergente.

Sea $\xi_j^{(0)} = \lim\limits_{\substack{m \to \infty \\ |\ |_K}} \xi_j^{(m)}$ y sea $u_0 := \xi_1^{(0)} w_1 + \cdots + \xi_{n-1}^{(0)} w_{n-1} + w_n$. Entonces $\mathcal{N}(u_0 - u_m) = \mathcal{N}\big(\sum_{j=1}^{n-1} (\xi_j^{(0)} - \xi_j^{(m)}) w_j\big) \leq \sum_{j=1}^{n-1} |\xi_j^{(0)} - \xi_j^{(m)}|_K \mathcal{N}(w_j) \xrightarrow[m \to \infty]{} 0$. Por tanto $\mathcal{N}_\infty(u_0 - u_m) \xrightarrow[m \to \infty]{} 0$. Se sigue que $u_m \xrightarrow[m \to \infty]{\mathcal{N}_\infty} u_0$.

En particular, tenemos

$$\mathcal{N}(u_0) = \mathcal{N}(u_0 - u_m + u_m) \leq \mathcal{N}(u_o - u_m) + \mathcal{N}(u_m) \xrightarrow[m \to \infty]{} 0,$$

puesto que $\mathcal{N}(u_m) < \frac{1}{mr}$. Se sigue que $u_0 = 0 = \xi_1^{(0)} w_1 + \cdots + \xi_{n-1}^{(0)} w_{n-1} + w_n$ lo cual contradice que $\{w_1, \ldots, w_n\}$ es un conjunto linealmente independiente. □

Teorema 3.1.14. *Sea K un campo valuado completo y sea L/K una extensión finita de grado n. Entonces existe una única extensión $|\ |_L$ a L del valor absoluto $|\ |_K$ de K el cual está dado por*

$$|y|_L = |\,\mathrm{N}_{L/K}(y)|_K^{1/n},$$

para $y \in L$ y $\mathrm{N}_{L/K}\colon L \to K$ es la norma. Más aún, L es un campo completo con el valor absoluto $|\ |_L$.

Finalmente, la valuación normalizada v_L está dada por

$$v_L(y) := \frac{e}{n} v_K(\mathrm{N}_{L/K}(y)).$$

Demostración. La existencia de v_L está garantizada por el Lema de Chevalley [160, Corollary 2.4.5].

Ahora bien, si $\alpha \in L^*$, sea $\beta = \frac{\alpha^n}{\mathrm{N}(\alpha)}$, donde $\mathrm{N} = \mathrm{N}_{L/K}$. Entonces

$$\mathrm{N}(\beta) = \frac{N(\alpha^n)}{(\mathrm{N}(\alpha))^n} = \frac{(\mathrm{N}(\alpha))^n}{(\mathrm{N}(\alpha))^n} = 1.$$

Veamos que $|\gamma|_L < 1$ implica $|\,\mathrm{N}(\gamma)|_K < 1$. Sea $\gamma^t = x_1^{(t)} w_1 + \cdots + x_n^{(t)} w_n$ donde $\{w_1, \ldots, w_n\}$ es una base L/K y donde $x_j^{(t)} \in K$.

Puesto que $|\gamma|_L < 1$, se tiene $\gamma^t \xrightarrow[t\to\infty]{} 0$. Puesto que $|\ |_L$ y $\mathcal{N}_\infty$ definen la misma topología, se tiene que $\mathcal{N}_\infty(\gamma^t) = \max_{1\le j\le n} |x_j^{(t)}| \xrightarrow[t\to\infty]{} 0$. Se sigue que $x_j^{(t)} \xrightarrow[t\to\infty]{} 0$ para toda $1 \le j \le n$. Por tanto $|\,\mathrm{N}(\gamma)|_K < 1$.

Ahora si $|\gamma|_L > 1$, entonces $|1/\gamma|_L < 1$ por lo que $|\,\mathrm{N}(1/\gamma)|_K < 1$ y por tanto $|\,\mathrm{N}(\gamma)|_K < 1$.

En resumen, si $\mathrm{N}(\gamma) = 1$, necesariamente $|\gamma|_L = 1$. Puesto que $\mathrm{N}(\beta) = 1$, se tiene

$$1 = |\beta|_L = \frac{|\alpha|_L^n}{|\,\mathrm{N}(\alpha)|_K}.$$

Por tanto $|\alpha|_L = \sqrt[n]{|\,\mathrm{N}(\alpha)|_K}$.

Finalmente $v_L(\beta) = 0 = v_L\big(\frac{\alpha^n}{\mathrm{N}(\alpha)}\big) = n v_L(\alpha) - v_L(\mathrm{N}(\alpha)) = n v_L(\alpha) - e v_K(\mathrm{N}(\alpha))$ por lo que $v_L(\alpha) = \frac{e}{n} v_K(\mathrm{N}(\alpha))$. □

Corolario 3.1.15. *En el caso de un campo local, $n = ef$ (Teorema 3.3.5) por lo que $v_L(\alpha) = \frac{1}{f} v_K(\mathrm{N}(\alpha))$.* □

Corolario 3.1.16. *Si K es un campo valuado completo y L/K es una extensión finita, entonces*

(1) *Si $a, b \in L$ son conjugados, entonces $|a|_L = |b|_L$ y $v_L(a) = v_L(b)$.*
(2) *Si L/K is Galois con grupo G, entonces para toda $\sigma \in G$ se tiene $v_L \circ \sigma = v_L$.*

Demostración. (1) Si F es la cerradura normal de L/K y si $b = \sigma a$, $|b|_L = |\,\mathrm{N}_{L/K}(\sigma a)|_K^{1/n} = |\,\mathrm{N}_{L/K}(a)|_K^{1/n} = |a|_L$.

(2) Se tiene

$$\begin{aligned}(v_L \circ \sigma)(\alpha) = v_L(\sigma\alpha) &= \frac{e}{n} v_K(\mathrm{N}_{L/K}(\sigma\alpha)) \\ &= \frac{e}{n} v_K(\mathrm{N}_{L/K}(\mathrm{N}_{L/K}(\alpha)) = v_L(\alpha)\end{aligned}$$

de donde se sigue que $v_L \circ \sigma = v_L$. □

3.2. Propiedades de las unidades de un campo local

Sea K un campo local con campo residual $\tilde{K} \cong \mathbb{F}_q$.

Notemos que $U_K^{(n)} = 1 + \mathfrak{p}_K^n$, $n \geq 0$, es un subgrupo abierto de $\mathcal{O}_K$ pues

$$\begin{aligned}U_K^{(n)} &= \{x \in K^* \mid v_K(x-1) > n-1\} \\ &= \{x \in K^* \mid |x-1| < q^{-(n-1)}\} = B(1, q^{-(n-1)}),\end{aligned}$$

y claramente $\bigcap_{n=0}^{\infty} U_K^{(n)} = \{1\}$ por lo que $\left\{U_K^{(n)}\right\}_{n\geq 0}$ forman un sistema fundamental de vecindades abiertas de $1 \in K^*$.

Por otro lado $U_K^{(n)}$, $n \geq 0$, es un subgrupo de K^*. Sea R un conjunto de representantes de $K^*/U_K^{(n)}$ con $1 \in R$, $U_K^{(n)} = K^* \setminus \left(\bigcup_{r\in R, r\neq 1} rU_K^{(n)}\right)$. Se sigue que $U_K^{(n)}$ es cerrado. Resumimos lo anterior en

Proposición 3.2.1. *Los conjuntos $U_K^{(n)}$, $n \geq 0$, son a la vez abiertos y cerrados en K^*.* □

Proposición 3.2.2. *El conjunto $U_K^{(n)}$, $n \geq 0$, es compacto.*

Demostración. Sea I una colección de subconjuntos abiertos de K^* que recubren a $U_K^{(n)}$. Si $U_K^{(n)}$ no pudiesen ser cubiertas por un número finito de conjuntos de I y puesto que $U_K^{(n+1)}$ es de índice finito en $U_K^{(n)}$, alguna clase $uU_K^{(n+1)} \subseteq U_K^{(n)}$ no sería cubierta por un número finito de elementos de I. Continuando con este proceso, tenemos que existe una sucesión

$$u_1 U_K^{(n+1)} \supseteq u_2 U_K^{(n+2)} \supseteq \ldots,$$

tal que ningún $u_j U_K^{(n+j)}$ puede ser cubierto por un número finito de elementos de I.

Puesto que $U_K^{(n)}$ es un subconjunto cerrado de K^* y K^* es completo, se tiene que $U_K^{(n)}$ es completo, de donde se sigue que $\bigcap_{j=1}^{\infty} u_j U_K^{(n+j)} \neq \emptyset$. Sea $u_0 \in \bigcap_{j=1}^{\infty} u_j U_K^{(n+j)}$. Entonces $u_0 U_K^{(n+j)} = u_j U_K^{(n+j)}$ para todo $j \geq 1$. Los conjuntos de I son conjuntos abiertos y $u_0 U_K^{(n+j)}$ es una vecindad fundamental

de u_0, por lo que existe $T \in I$ con $u_0 U_K^{(n+j)} \subseteq T$. Esto último contradice que $u_j U_K^{(n+j)} = u_0 U_K^{(n+j)}$ no puede ser cubierto por un número finito de elementos de I. Por tanto, $U_K^{(n)}$ es un conjunto compacto. □

Con respecto a los ideales $\mathfrak{p}_K^n$ tenemos:

Proposición 3.2.3. *Los ideales $\mathfrak{p}_K^n$, $n \geq 0$ son a la vez conjuntos abiertos y cerrados de K^*.*

Demostración. Se sigue inmediatamente de que $U_K^{(n)} = 1 + \mathfrak{p}_K^n$ y de la Proposición 3.2.1. Una demostración directa es la siguiente. Se tiene que para $n \geq 0$, $\mathfrak{p}_K^n = \{x \in K \mid v_K(x) \geq n\} = \{x \in K \mid v_K(x) > n-1\}$, es decir, $\mathfrak{p}_K^n = v_K^{-1}\big((n-1,\infty]\big) = v_K^{-1}\big([n,\infty]\big)$, $v_K \colon K \to \mathbb{R} \cup \{0\} = (-\infty, \infty]$ es claramente una función continua (si $x_n \xrightarrow[n\to\infty]{} x$, $v_K(x_n) \xrightarrow[n\to\infty]{} v_K(x)$). Puesto que $(n-1,\infty]$ es abierto y $[n,\infty]$ es cerrado en $\mathbb{R} \cup \{0\}$ se sigue lo afirmado. □

Corolario 3.2.4. *Sea K un campo local. Entonces K es un campo totalmente disconexo y no discreto. El grupo multiplicativo K^* de K, es localmente compacto, no compacto y totalmente disconexo.*

Demostración. Puesto que $U_K^{(n)}$, $n \geq 0$ es un sistema fundamental de vecindades de $1 \in K^*$, y puesto que $U_K^{(n)}$ es compacto, se sigue que K^* es localmente compacto. Ahora bien K^* no es compacto pues si $\pi = \pi_K$, $K^* = \bigcup_{n=0}^{\infty} \pi^n U_K$ donde cada conjunto $\pi^n U_K$ es abierto y la unión es una unión disjunta a pares. El hecho de que K^* es totalmente disconexo se prueba de manera análoga a que K es totalmente disconexo y cuya prueba damos enseguida.

Para ver que K es totalmente disconexo, consideremos $x \neq 0$. Entonces $v_K(x) = n \in \mathbb{Z}$. Entonces $x \notin \mathfrak{p}_K^m$ con $m \geq \text{máx}\{1, n+1\}$, esto es $0 \in \mathfrak{p}_K^m$, $x \in K \setminus \mathfrak{p}_K^m$ siendo $\mathfrak{p}_K^m$ y $K \setminus \mathfrak{p}_K^m$ conjuntos abiertos disjuntos. Finalmente K no es discreto pues $\mathfrak{p}_K^n$, $n \geq 0$ es un sistema fundamental de vecindades de $\{0\}$ y $\mathfrak{p}_K^n \neq \{0\}$, esto es, $\{0\}$ no es un conjunto abierto. □

El isomorfismo $\tilde{K} \cong \mathfrak{p}_K^n / \mathfrak{p}_K^{n+1}$ se sigue del hecho de que $\mathfrak{p} = \pi \mathcal{O}_K$, por lo que la multiplicación por π^n induce el isomorfismo. Más precisamente, sea $\varphi \colon \mathcal{O}_K \longrightarrow \mathcal{O}_K$ dada por $\varphi(x) = \pi^n x$. Entonces φ es un homomorfismo de grupos aditivos. Además, $\operatorname{im} \varphi = \pi^n \mathcal{O}_K = \mathfrak{p}_K^n$ y $\varphi^{-1}(\mathfrak{p}_K^{n+1}) = \pi \mathcal{O}_K = \mathfrak{p}_K$, de donde se sigue que $\mathcal{O}_K / \mathfrak{p}_K \cong \mathfrak{p}_K^n / \mathfrak{p}_K^{n+1}$.

Además el mapeo $\psi \colon \mathcal{O}_K \longrightarrow \mathcal{O}_K$ dado por $\psi(u) = u - 1$ da lugar al homomorfismo de grupos $U_K^{(n)} \longrightarrow \mathfrak{p}_K^n / \mathfrak{p}_K^{n+1}$ con $U_K^{(n)}$ un grupo multiplicativo y $\mathfrak{p}_K^n / \mathfrak{p}_K^{n+1}$ un grupo aditivo, el cual es suprayectivo por definición y $\operatorname{núc} \psi = 1 + \mathfrak{p}_K^{n+1}$. De hecho, lo anterior se debe a que

$$\psi(uv) = uv - 1 = (u-1)(v-1) + (u-1) + (v-1)$$

por lo que $uv - 1 \equiv (u-1) + (v-1)$ mód $\mathfrak{p}_K^{2n}$ y $2n \geq n+1$.

Como consecuencia se tiene:

Proposición 3.2.5. *Sea p la característica del campo residual del campo local K.*

(1) *Para todo $n \geq 1$, $(U_K^{(n)})^p \subseteq U_K^{(n+1)}$.*
(2) *Para $m \in \mathbb{N}$ con $\operatorname{mcd}(m,p) = 1$, se tiene que para cada $n \geq 1$, el mapeo $u \longrightarrow u^m$ es un automorfismo de $U_K^{(n)}$, en particular $\left(U_K^{(n)}\right)^m = U_K^{(n)}$ para toda $n \geq 1$ y toda m con $p \nmid m$.*

Demostración. (1) Se tiene $U_K^{(n)}/U_K^{(n+1)} \overset{\theta}{\cong} \mathbb{F}_q$. Por tanto, si $x \in U_K^{(n)}$, se tiene $\theta(\bar{x}^p) = p\theta(\bar{x}) = 0$, de lo cual obtenemos que $x^p \in U_K^{(n+1)}$.

(2) Sea $f\colon U_K^{(n)} \longrightarrow U_K^{(n)}$ dado por $f(u) = u^m$, con $n \geq 1$ arbitrario. Entonces f es un endomorfismo. Sea $x \in U_K^{(n)}$ con $x^m = 1$. Se tiene $x = 1+u\pi^n$ con $u \in \mathcal{O}_K$. Si $u \neq 0$, $u = \pi_K^s u_0$ para algunos $u_0 \in U_K$ y $s \geq 0$. Por tanto

$$x = 1 + u_0\pi_K^{n+s} \quad \text{y} \quad x^m = 1 + mu_0\pi_K^{n+s} + \text{ términos con valuación mayor.}$$

Puesto que $v_K(m) = 0$, $mu_0 \neq 0$ lo cual es absurdo. Por tanto $u = 0$ y $x = 1$. Por tanto f es inyectiva.

Ahora sea $x \in U_K^{(n)}$. Para toda $r \in \mathbb{N}$, existen $a_r, b_r \in \mathbb{Z}$ tales que $a_r m + b_r p^r = 1$, $x = x^1 = x^{a_r m + b_r p^r} = (x^{a_r})^m \cdot (x^{b_r})^{p^r} = \xi_r \mu_r$. Sea $x^{b_r} = 1 + c_r$ con $c_r \in \mathfrak{p}_K$. Entonces $\mu_r = (x^{b_r})^{p^r} \equiv 1 + p^r c_r \mod p^{r+1}\mathfrak{p}_K$ y $v_K(\mu_r - 1) \geq r + 1$ y $\lim_{r\to\infty} \mu_r = 1$. Se sigue que $y := \lim_{r\to\infty} x^{a_r}$ existe y $x = y^m$, por lo que f es suprayectiva. □

Proposición 3.2.6. *Sean $v = v_K$ la valuación de K y $m \in \mathbb{N}$ tal que la característica de K no divida a m. Entonces para $n > v_K(m)$, el mapeo g, $x \mapsto x^m$ da lugar a un isomorfismo $U_K^{(n)} \longrightarrow U_K^{(n+v_K(m))}$. En particular, si $\operatorname{car} K = p > 0$, $v_K(m) = 0$ y $U_K^{(n)} = \left(U_K^{(n)}\right)^m$ para toda $n \geq 1$ y para $p \nmid m$.*

Demostración. Sea π un elemento primo de K, esto es, $v_K(\pi) = 1$. Sea $x = 1 + a\pi^n \in U_K^{(n)}$, $a \in \mathcal{O}_K$. Entonces

$$x^m = 1 + ma\pi^n + \binom{m}{2} a^2\pi^{2n} + \cdots \equiv 1 \mod \mathfrak{p}_K^{n+v_K(m)}.$$

Por tanto $x^m \in U_K^{(n+v_K(m))}$ para toda n.

Para probar que el mapeo es suprayectivo, debemos probar que para $a \in \mathcal{O}_K$ arbitrario, existe $x \in \mathcal{O}_K$ tal que

$$1 + a\pi^{n+v_K(m)} = (1 + x\pi^n)^m,$$

lo cual equivale a que $1 + a\pi^{n+v_K(m)} = 1 + m\pi^n x + \pi^{2n} f(x)$ donde $f(x) \in \mathcal{O}_K[x]$. Si K es de característica prima relativa a m, $m = u\pi^{v_K(m)}$ con $u \in U_K$. Si $\operatorname{car} K = p > 0$ y $p|m$, $m = 0$ en K. Así

$$1 + a\pi^{n+v_K(m)} = \begin{cases} 1 + u\pi^{n+v_K(m)}x + \pi^{2n}f(x) & \text{si } p \nmid m, \\ 1 + \pi^{2n}f(x) & \text{si } p \mid m. \end{cases}$$

Por lo tanto necesitamos resolver

$$0 = \begin{cases} -a + ux + \pi^{n-v_K(m)}f(x) & \text{si } p \nmid m, \\ -a + \pi^{n-v_K(m)}f(x) & \text{si } p \mid m. \end{cases}$$

La primera ecuación tiene solución por el Lema de Hensel, pero la segunda ecuación no tiene solución. Más precisamente, la primera ecuación es equivalente a resolver la ecuación $-a + ux + \pi^{n-v_K(m)}f(x) = 0$. Puesto que $n > v_K(m)$, módulo $\mathfrak{p}_K$ se tiene $\bar{a} + \bar{u}\bar{x} = 0$ con $\bar{u} \neq 0$. Por tanto $\overline{h(x)} = \overline{-a + ux + \pi^{n-v_K(m)}f(x)} = 0$ tiene una raíz simple y por el Lema de Hensel, Teorema 3.1.8, la raíz $\bar{x} = \frac{\bar{a}}{\bar{u}}$ se levanta a $\mathcal{O}_K$ a una raíz de $h(x)$ y por tanto $g\colon U_K^{(n)} \longrightarrow U_K^{(n+v_K(m))}$, $x \mapsto x^m$, es suprayectiva.

Ahora, núc $g = W_m = \{\xi \in U_K^{(n)} \mid \xi^m = 1\}$. Sea $\xi \in$ núc g, $\xi = 1 + u\pi^n$ con $u \in \mathcal{O}_K$. Entonces $\xi \equiv 1$ mód $\mathfrak{p}_K^n$, por lo tanto $\xi^r \equiv 1$ mód $\mathfrak{p}_K^n$ para toda $r \geq 1$. Se tiene

$$0 = (\xi^m - 1) = (\xi - 1)(\xi^{m-1} + \cdots + \xi + 1).$$

Puesto que $n > v_K(m)$ y $\xi^{m-1} + \cdots + \xi + 1 \equiv m$ mód $\mathfrak{p}_K^n = u\pi^{v_K(m)}$ mód $\mathfrak{p}_K^n$ con $u \in U_K$, se sigue que $\xi^{m-1} + \cdots + \xi + 1 \notin \mathfrak{p}_K^n$ y en particular $\xi^{m-1} + \cdots + \xi + 1 \neq 0$. Por tanto $\xi = 1$ y g es inyectiva. □

Corolario 3.2.7. *Para $m \in \mathbb{N}$ tal que* car $K \nmid m$, *se tiene que $\left(K^*\right)^m$ es un subgrupo abierto de K^*.*

Además, si car $K = 0$, *se tiene que $\bigcap_{m=1}^{\infty} \left(K^*\right)^m = \{1\}$.*

Demostración. Para $x \in K^*$, $x^m \in \left(K^*\right)^m$, y para $n > v_K(m)$ con $p \nmid m$, $p =$ car K, $x^m U_K^{(n+v_K(m))} = \left(xU_K^{(n)}\right)^m \subseteq \left(K^*\right)^m$, la cual es una vecindad abierta de x^m. Se sigue que $\left(K^*\right)^m$ es abierto en K^*.

Sea ahora car $K = 0$ y sea $a \in \bigcap_{m=1}^{\infty} \left(K^*\right)^m \subseteq \bigcap_{\substack{m=1 \\ p \nmid m}}^{\infty} \left(K^*\right)^m$. Si $v_K(a) \neq 0$, para cada $m \in \mathbb{N}$ con $p \nmid m$, existe $y_m \in K^*$ con $a = y_m^m$, por lo tanto $v_K(a) = mv_K(y_m)$ con $v_K(y_m) \neq 0$. Por tanto, $m | v_K(a)$ para toda m con $p \nmid m$, lo cual es absurdo. Se sigue que $v_K(a) = 0$ y $a \in U_K$. Por tanto $a \in \bigcap_{m=1}^{\infty} \left(U_K\right)^m$, esto es, $a = u_m^m$ con $u_m \in U_K$ para toda m.

Sea $n \in \mathbb{N}$ y sea $[U_K : U_K^{(n)}] = m$. Entonces $u_m^m \in U_K^{(n)}$ de donde obtenemos que $a \in \bigcap_{m=1}^{\infty} U_K^{(n)}$ y $v_K(a-1) \geq n$ para toda $n \in \mathbb{N}$. Por tanto $v_K(a-1) = \infty$ y $a = 1$. □

Observación 3.2.8. Si K es un campo local de característica $p > 0$, entonces $\left(K^*\right)^p$ no es abierto en K^* pues si este fuese el caso, existiría m tal que

$U_K^{(m)} \subseteq \left(K^*\right)^p$. En particular $1+\pi_K^m = x^p$ para algún $x \in K^*$. De esta forma, tendríamos que $x^p - 1 = (x-1)^p = \pi_K^m$ lo cual no es posible puesto que de lo contrario tendríamos que $m = pv_K(x-1)$ y entonces $p|m$. Puesto que $U_K^{(n)} \subseteq U_K^{(m)}$ esto diría que $p|n$ para toda $n \geq m$ lo cual es absurdo.

Por otro lado, $\left(K^*\right)^p$ si es cerrado pues $K^* \cong \langle \pi_K \rangle \times U_K$ como grupos y $\left(K^*\right)^p = \langle \pi_K^p \rangle U_K^p$ y como U_K es compacto, U_K^p es compacto y por tanto cerrado.

Cuando $\operatorname{car} K = 0$, un resultado que probaremos usando el cociente de Herbrand en cohomología es que para $m \in \mathbb{N}$, $\left(K^*\right)^m$ es de índice finito en K^* y de hecho $[K^* : \left(K^*\right)^m] = mq^{v_K(m)}|\mu_m(K)| = m \cdot |m|_{\mathfrak{p}_K}^{-1} \cdot |\mu_m(K)|$, donde $|\tilde{K}| = q$ y $\mu_m(K) = \{\xi \in K^* \mid \xi^m = 1\}$.

3.3. Representación, normas, valores absolutos y extensiones de campos locales

Empezamos con un resultado fundamental sobre extensiones finitas de campos locales.

Proposición 3.3.1. *Sea L/K una extensión finita de campos locales con anillos de valuación $\mathcal{O}_L$ y $\mathcal{O}_K$ respectivamente. Sean $\mathfrak{p}_K = \langle \pi_K \rangle$ y $\mathfrak{p}_L = \langle \pi_L \rangle$ con π_K y π_L elementos primos de K y de L respectivamente. Sean $f = f(L|K) = [\mathcal{O}_L/\mathfrak{p}_L : \mathcal{O}_K/\mathfrak{p}_K] = [\tilde{L} : \tilde{K}]$ y $e = e(L|K)$ el índice de ramificación. Sea $\{\omega_1, \ldots, \omega_f\}$ una base de $\tilde{L}/\tilde{K}$. Sean $\alpha_i \in \mathcal{O}_L$ tales que $\bar{\alpha}_i = \omega_i$, $1 \leq i \leq f$. Sea $\eta_{ij} = \alpha_i \pi_L^j$, $1 \leq i \leq f$, $0 \leq j \leq e-1$. Entonces $\{\eta_{ij}\}_{i,j}$ es un sistema linealmente independiente sobre K^* y en particular $[L : K] \geq ef$. Más aún se tiene que:*

(1) *Si $y = \sum_{i=1}^f A_i \alpha_i$ con $A_i \in K$, entonces se tiene que $v_L(y) = \min_{1 \leq i \leq f}\{ev_K(A_i)\}$.*
(2) *Si $z = \sum_{i=1}^f \sum_{j=0}^{e-1} c_{ij}\eta_{ij}$ con $c_{ij} \in K$, entonces*

$$v_L(z) = \min_{\substack{1 \leq i \leq f \\ 0 \leq j \leq e-1}} \{ev_K(c_{ij}) + j\}.$$

Demostración. (1) Sea $y = \sum_{i=1}^f A_i \alpha_i$ con $A_i \in K$. Si $A_1 = \cdots A_f = 0$, el resultado se sigue inmediatamente. Por tanto, rearreglando, podemos suponer que $v_K(A_1) = \cdots = v_K(A_s) < v_K(A_i)$, $s+1 \leq i \leq f$. Sea $B_i := \frac{A_i}{A_1}$, $1 \leq i \leq f$. Entonces $B_1 = 1$ y $B_i \in \mathcal{O}_K$ para toda i. Además se tiene que $\frac{y}{A_1} = \sum_{i=1}^f B_i \alpha_i \in \mathcal{O}_L$. Si $y/A_1 \in \mathfrak{p}_K$ entonces se tendría que $\frac{\bar{y}}{A_1} = 0 = \bar{\alpha_1} + \sum_{i=1}^f \bar{B}_i \bar{\alpha_i}$ lo que contradice que $\{\omega_1, \ldots, \omega_f\}$ es un conjunto linealmente independiente sobre $\tilde{K}$. Se sigue que $y/A_1 \notin \mathfrak{p}_L$ por lo que $v_L(y/A_1) = 0$ y $v_L(y) = v_L(A_1) = ev_K(A_1) = e \min_{1 \leq i \leq f}\{v_K(A_i)\} = \min_{1 \leq i \leq f}\{ev_K(A_i)\}$.

(2) Sea $z = \sum_{ij} c_{ij}\eta_{ij}$ con $c_{ij} \in K$. Sea $y_j = \sum_{i=1}^{f} c_{ij}\alpha_i$, $0 \leq j \leq e-1$ y por tanto $z = \sum_{j=0}^{e-1} y_j \pi_L^j$. Si $y_j \neq 0$, $v_L(y_j)$ es múltiplo de e y $v_L(y_j\pi_L^j) \equiv j$ mód e. Por tanto los valores $\{v_L(y_j) \mid y_j \neq 0\}_{j=0}^{e-1}$ son todos distintos y por tanto

$$\begin{aligned} v_L(z) &= \min_{0\leq j\leq e-1}\{v_L(y_j\pi_L^j)\} = \min_{0\leq j\leq e-1}\{v_L(y_j)+j\} \\ &= \min_{0\leq j\leq e-1}\{\min_{1\leq i\leq f}\{ev_K(c_{ij})+j\}\} = \min_{\substack{0\leq j\leq e-1\\ 1\leq i\leq f}}\{ev_K(c_{ij})+j\}. \end{aligned}$$

Ahora sea $\sum_{ij} x_{ij}\eta_{ij} = 0$ para algunos $x_{ij} \in K$. Por tanto $\infty = v_L(0) = \min_{ij}\{ev_K(x_{ij})+j\}$. Por tanto $v_K(x_{ij}) = \infty$ para todo i, j y por tanto $x_{ij} = 0$ para todo i, j, probando que $\{\eta_{ij}\}_{ij}$ es un conjunto linealmente independiente de L. □

Ahora probaremos que $\{\eta_{ij}\}_{ij}$ es de hecho una base de L/K. Esto lo haremos viendo que los campos locales, de hecho los campos completos bajo una valuación discreta, se pueden representar por medio de series de Laurent.

Sea K un campo completo con respecto a una valuación discreta v_K normalizada, esto es, $v_K(K^*) = \mathbb{Z}$ y sea $\mathcal{O}_K/\mathfrak{p}_K = \tilde{K}$ el campo residual. Sea R un sistema completo de representantes de $\tilde{K}$, $R \subseteq \mathcal{O}_K$ y tal que $0 \in R$, 0 es el representante de $0 + \mathfrak{p}_K = \mathfrak{p}_K$ en R. Para cada $n \in \mathbb{Z}$, sea $\pi_n \in K$ tal que $v_K(\pi_n) = n$. Consideremos cualquier suma $\sum_{n=m}^{\infty} r_n\pi_n$ donde $m \in \mathbb{Z}$ y $r_n \in R$. Se tiene que $v_K(r_n\pi_n) = v_K(r_n) + v_K(\pi_n) \geq n$ ($= n$ si $r_n \neq 0$ y ∞ si $r_n = 0$). Por tanto $v_K(r_n\pi_n) \xrightarrow[n\to\infty]{} \infty$ y por tanto $\sum_{n=m}^{\infty} r_n\pi_n$ converge en K.

Entenderemos $\sum_{n=m}^{\infty} r_n\pi_n = \sum_{-\infty}^{\infty} r_n\pi_n$ con $r_n = 0$ para toda $n < m$.

Teorema 3.3.2. (1) *Cada $x \in K$ se expresa de manera única como $x = \sum_{n=m}^{\infty} r_n\pi_n$, $r_n \in R$. Si $x \neq 0$ y $r_m \neq 0$, entonces $v_K(x) = m$.*
(2) *Sean $x = \sum_{n=m}^{\infty} r_n\pi_n$, $y = \sum_{n=m}^{\infty} s_n\pi_n$ con $r_n, s_n \in R$. Entonces para $i \in \mathbb{Z}$, se tiene que $v_K(x-y) \geq i \iff r_n = s_n$ para toda $n < i$.*

Demostración. (1) La unicidad se sigue de (2): Si $x = \sum r_n\pi_n = \sum r'_n\pi_n$ fuesen dos expresiones de x y si $r_m \neq r'_m$ para algún $m \in \mathbb{Z}$, podemos seleccionar el mínimo tal m y $v_K(0) = v_K(x-x) = m$ lo cual es absurdo.

La valuación de x también se sigue de (2). Se tiene que $0 = \sum 0\pi_n$ y $x = \sum r_n\pi_n$, $x \neq 0$, si $m \in \mathbb{Z}$ es mínimo $m \in \mathbb{Z}$ con $r_m \neq 0$, Entonces $v_K(x-0) = v_K(x) = m$.

Para la representación de $x \in K$, $x \neq 0$ y $v_K(x) = m < \infty$, se tiene, para $n \in \mathbb{Z}$, $\mathfrak{p}_K^n = \{x \in K \mid v_K(x) \geq n\} = \mathcal{O}_K \cdot \pi_n$. De que $\mathcal{O}_K = R + \mathfrak{p}_K$, se sigue que

$$\mathfrak{p}_K^n = R\pi_n + \mathfrak{p}_K^{n+1} = R\pi_n + R\pi_{n+1} + \cdots + R\pi_t + \mathfrak{p}_K^{t+1}$$

para toda $t \geq n$. Puesto que $x \in \mathfrak{p}_K^m$, existen $r_m, r_{m+1}, r_{m+2}, \ldots$ tales que $x \equiv \sum_{n=m}^{t} r_n \pi_n$ mód $\mathfrak{p}_K^{t+1}$ para $t \geq m$, de donde, $x = \lim_{t\to\infty} \sum_{n=m}^{\infty} r_n \pi_n$.

Así pues, toda la demostración se seguirá de probar (2).

(2) Si $r_n = s_n$ para toda n, entonces $x = y$ y $v_K(x-y) = \infty$. Supongamos ahora que existe $m \in \mathbb{Z}$ con $r_m \neq s_m$ y $r_n = s_n$ para toda $n < m$. Así, $x - y = \sum_{n=m}^{\infty}(r_n - s_n)\pi_n$. Puesto que $r_m, s_m \in R$, $r_m \not\equiv s_m$ mód $\mathfrak{p}$ por lo que $v_K(r_m - s_m) = 0$ y $v_K((r_m - s_m)\pi_m) = m$. Para $n > m$, $v_K((r_n - s_n)\pi_n) \geq v_K(\pi_n) = n > m = v_K((r_m - s_m)\pi_m)$. Puesto que $m = v_K((r_m - s_m)\pi_m) < v_K\big(\sum_{n=m+1}^{\infty}(r_n - s_n)\pi_n\big) (\geq m+1)$, se sigue que $v_K(x-y) = v_K((r_m - s_m)\pi_m) = m$. Esto prueba (2). □

Corolario 3.3.3. *Sea* $R^\infty = \prod_{i=0}^{\infty} R = \{(r_i)_{i=0}^{\infty} \mid r_i \in R\} = \prod_{n=0}^{\infty} R_n$ *con* $R_n = R$ *para toda* n. *Consideremos* R^∞ *con la topología producto y cada* R_n *tiene la topología discreta. Entonces*

$$R^\infty \xrightarrow{\mu} \mathcal{O}_K, \qquad (r_n)_{n=0}^{\infty} \longmapsto \sum_{n=0}^{\infty} r_n \pi_n,$$

es un homeomorfismo de R^∞ *en* $\mathcal{O}_K$. *En particular* $\mathcal{O}_K$ *es un conjunto compacto. Además,* $\mathcal{O}_K \cong \mathfrak{p}_K^n$ *para toda* $n \geq 0$ *y* $\mathfrak{p}_K^n$ *es compacto.*

Demostración. La parte (1) del Teorema 3.3.2 prueba que μ es biyectiva y la parte (2) prueba que es un homeomorfismo. La compacidad de $\mathcal{O}_K$ se sigue del Teorema de Tychonoff.

El mapeo $x \longmapsto x\pi_K^n$ es un homeomorfismo de $\mathcal{O}_K$ en $\mathfrak{p}_K^n$. □

Notemos que $\mathcal{O}_K = \bigcup_{n=0}^{\infty} \pi_K^n U_K$ y cada $\pi_K^n U_K$ es abierto, por tanto $\mathcal{O}_K$ es abierto. Por otro lado $\bigcap_{n=0}^{\infty} \mathfrak{p}_K^n = \{0\}$ pues si $x \in \bigcap_{n=0}^{\infty} \mathfrak{p}_K^n$, $v_K(x) \geq n$ para toda n de donde se sigue que $v_K(x) = \infty$ y $x = 0$.

Tomando los mapeos canónicos $\mathcal{O}_K/\mathfrak{p}_K^m \longrightarrow \mathcal{O}_K/\mathfrak{p}_K^n$ para $m \geq n$, se sigue que

$$\mathcal{O}_K \cong \varprojlim_n \mathcal{O}_K/\mathfrak{p}_K^n.$$

Similarmente

$$U_K^{(1)} \cong \varprojlim_n U_K^{(1)}/U_K^{(n)}$$

con respecto a los mapeos canónicos $U_K^{(1)}/U_K^{(m)} \longrightarrow U_K^{(1)}/U_K^{(n)}$ con $m \geq n$.

Teorema 3.3.4. *Sea* K *un campo local.*

(1) *Si* $\operatorname{car} K = 0$, $[K : \mathbb{Q}_p] = ef = d$, $U_K^{(1)} \cong W_K \oplus \mathbb{Z}_p^d$ *con* $W_K = \{\xi \in K \mid \xi^{p^m} = 1$ *para algún* $m\} \cong \mathbb{Z}/p^a\mathbb{Z}$ *para algún* $a \geq 0$.

(2) *Si* $\operatorname{car} K = p > 0$, $U_K^{(1)} \cong \prod_{i=1}^{\infty} \mathbb{Z}_p$.

Demostración. [77, Propositions 2.6, 2.7, 2.8]. □

Teorema 3.3.5. *Con las notaciones de la Proposición* 3.3.1*, se tiene que* $\{\eta_{ij}\}_{\substack{1\le i\le f\\ 0\le j\le e-1}}$ *es una base de* L/K *y* $[L:K] = ef$.

Más aún, $\{\eta_{ij}\}_{\substack{1\le i\le f\\ 0\le j\le e-1}}$ *es una base* $\mathcal{O}_L$ *sobre* $\mathcal{O}_K$*, esto es,* $\mathcal{O}_L$ *es un* $\mathcal{O}_K$*-módulo libre de rango* ef.

Demostración. Sea R un conjunto de representantes de $\mathcal{O}_K/\mathfrak{p}_K$ en $\mathcal{O}_K$ con $0 \in R$ y sea $R' = \{\sum_{i=1}^{f} r_i\alpha_i \mid r_1, \ldots, r_f \in R\}$. Entonces R' es un conjunto de representantes de $\mathcal{O}_L/\mathfrak{p}_L$ en $\mathcal{O}_L$ y $0 \in R'$. Sean π_K y π_L elementos primos de K y L respectivamente.

Para $m \in \mathbb{Z}$, escribamos $m = te + j$, $t \in \mathbb{Z}$ y $0 \le j \le e-1$ y definimos $\pi_{L,m} := \pi_K^t \pi_L^j$. Ahora como $v_L|_K = ev_K$, se tiene $v_L(\pi_{L,m}) = et + j = m$.

Dado $y \in L$, y se escribe de manera única en la forma

$$y = \sum_{m=-\infty}^{\infty} r'_m \pi_{L,m},$$

con $r'_m \in R'$. Sea $r'_m = \sum_{i=1}^{f} r_{i,m}\alpha_i$ con $r_{i,m} \in R$. Se sigue que

$$y = \sum_{m} \sum_{i=1}^{f} r_{i,m}\alpha_i\pi_{L,m} = \sum_{i=1}^{f} \sum_{j=0}^{e-1} \beta_{ij}\alpha_i\pi_L^j,$$

donde $\beta_{ij} = \sum_{i=-\infty}^{\infty} r_{i,te+j}\pi_K^i \in K$. Por tanto $\{\eta_{ij}\}_{ij}$ genera L/K y por la Proposición 3.3.1, este conjunto es linealmente independiente, por lo tanto es base y $[L:K] = ef$.

Ahora bien $\{\eta_{ij}\}_{ij} \subseteq \mathcal{O}_L$. Sea $x \in \mathcal{O}_L$, $x = \sum_{ij} c_{ij}\eta_{ij}$. Entonces, por la Proposición 3.3.1, tenemos que $v_K(x) = \min_{ij}\{ev_K(c_{ij}) + j\} \ge 0$ por lo que $ev_K(c_{ij}) \ge -j$ para todas i, j. Si se tuviese $v_K(c_{ij}) \le -1$, entonces $ev_K(c_{ij}) = -le \ge -j$, $l \ge 1$ lo que implicaría que $j \ge e$ lo cual es absurdo. Por tanto $v_K(c_{ij}) \ge 0$ para todas i, j. Es decir $c_{ij} \in \mathcal{O}_K$ y el resultado se sigue. □

Teorema 3.3.6. *Sea* K *un campo local y sea* L/K *una extensión finita de* K*. Sean* $\mathrm{N} = \mathrm{N}_{L/K}$ *y* $T := \mathrm{Tr}_{L/K}$ *la norma y la traza de* L *en* K *respectivamente:* $\mathrm{N}, T\colon L \longrightarrow K$*. Entonces* N *y* T *son funciones continuas. Además* $\mathrm{N}(\mathcal{O}_L) \subseteq \mathcal{O}_K$ *y* $T(\mathcal{O}_L) \subseteq \mathcal{O}_K$.

Demostración. Sea $\{\eta_{ij}\}_{ij}$ la base de L/K dada por la Proposición 3.3.5. Sean $y \in L$ y $y\eta_{ij} = \sum_{s=1}^{f}\sum_{t=0}^{e-1} x_{ijst}\eta_{st}$ para toda i, j con $x_{ijst} \in K$. Se tiene

$$v_L(y)+j = v_L(y)+v_L(\eta_{ij}) = v_L(y\eta_{ij}) = \min_{s,t}\{ev_K(x_{ijst})+t\}$$
$$\leq ev_K(x_{ijst})+t.$$

Por tanto

$$v_K(x_{ijst}) \geq \frac{1}{e}(v_L(y)+j-t) \quad \text{para todas } i,j,s,t.$$

Se sigue que $y \longrightarrow 0 \iff v_L(y) \longrightarrow \infty \Longrightarrow v_K(x_{ijst}) \longrightarrow \infty \iff x_{ijst} \longrightarrow 0$ para todas $1 \leq i,s \leq f$ y para todas $0 \leq j,t \leq e-1$.

Se sigue que las x_{ijst}'s dependen continuamente de $y \in L$. Puesto que T y N son la traza y el determinante de la $n \times n$ matriz (x_{ijst}) respectivamente, tenemos que T y N son funciones continuas.

Finalmente, si $y \in \mathcal{O}_L$, $v_L(y) \geq 0$ lo que implica que $v_K(x_{ijst}) \geq 0$ de donde obtenemos que $T(\mathcal{O}_L) \subseteq \mathcal{O}_K$ y $\mathrm{N}(\mathcal{O}_L) \subseteq \mathcal{O}_K$. □

Un resultado de especial relevancia para nosotros para la teoría local de campos de clase es que si L/K es una extensión finita de campos locales, entonces $\mathrm{N}_{L/K}(L^*)$ es un conjunto cerrado en K^*.

Teorema 3.3.7. *Sea L/K una extensión finita de campos locales y se* N *la norma de L en K. Entonces $\mathrm{N}(U_L)$ es un subgrupo compacto y por tanto cerrado en K^* y $\mathrm{N}(L^*)$ es un subgrupo cerrado de K^*.*

Demostración. Puesto que la norma N es continua (Teorema 3.3.6) y U_L es compacto (Proposición 3.2.2) por lo que $\mathrm{N}(U_L)$ es compacto en K^* y $\mathrm{N}(U_L) \subseteq U_K$. Puesto que K^* es Hausdorff, $\mathrm{N}(U_L)$ es cerrado en K^*.

Ahora bien, $\mathrm{N}(U_L) = \mathrm{N}(L^*) \cap U_K \subseteq U_K$. Como U_K es abierto, $\mathrm{N}(U_L)$ es abierto en $\mathrm{N}(L^*)$ y también es cerrado en $\mathrm{N}(L^*)$. Se sigue que $\mathrm{N}(L^*)/\mathrm{N}(U_L)$ es un espacio discreto: si $\xi \in \mathrm{N}(L^*)$, $\xi\,\mathrm{N}(U_L)$ es abierto en $\mathrm{N}(L^*)$ y $\xi\,\mathrm{N}(U_L) = \pi^{-1}(\bar{\xi})$, $\pi\colon \mathrm{N}(L^*) \longrightarrow \mathrm{N}(L^*)/\mathrm{N}(U_L)$ la proyección natural de donde se sigue que $\bar{\xi}$ es abierto en $\mathrm{N}(L^*)/\mathrm{N}(U_L)$. Por tanto $\mathrm{N}(L^*)/\mathrm{N}(U_L)$ es un subgrupo discreto de $K^*/\mathrm{N}(U_L)$. Ahora bien, por ser $\mathrm{N}(U_L)$ cerrado, se sigue que $K^*/\mathrm{N}(U_L)$ es Hausdorff (se tiene en general que si G es un grupo topológico Hausdorff y H es un subgrupo cerrado de G, entonces G/H es Hausdorff). Por el Lema 3.3.8 abajo, se sigue que $\mathrm{N}(L^*)$ es un subgrupo cerrado de K^*. □

Lema 3.3.8. *Sean G un grupo topológico Hausdorff y $H < G$ un subgrupo discreto de G. Entonces H es cerrado.*

Demostración. **Paso 1:** Sea U una vecindad abierta tal que $U \cap H = \{e\}$, entonces existe una vecindad abierta $V \subseteq U$ tal que $VV^{-1} \subseteq U$ y $e \in V$.

En efecto, sea $\sigma : U \times U \longrightarrow G$, $\sigma(y_1,y_2) = y_1y_1^{-1}$. Por continuidad, existe una vecindad $N \subseteq U \times U$ de (e,e) tal que $\sigma(N) = U$ y N contiene una vecindad abierta de la forma $V_1 \times V_2$ con $V_1, V_2 \subseteq U$ y $e \in V_1 \cap V_2$. Entonces $V := V_1 \cap V_2$ es la vecindad buscada.

Paso 2: Sea $x \in G \setminus H$. Sea U una vecindad abierta de e con $U \cap H = \{e\}$. El mapeo $L_x \colon G \to G$, $L_x(y) = xy$ con $x \in G$ es un homeomorfismo con inverso $L_{x^{-1}}$. Sea $V \subseteq U$ una vecindad de e tal que $e \in V$ y $VV^{-1} \subseteq U$. Sea $W = L_x(V)$. Se tiene que W tiene a lo más un elemento de H. Si $W \cap H = \emptyset$, W es la vecindad buscada, Si $W \cap H = xV \cap H = \{h\}$, existen abiertos U_x y U_h de G con $x \in U_x$ y $h \in U_h$ y $U_x \cap U_h = \emptyset$. Finalmente $xV \cap U_x$ es una vecindad abierta de x disjunta de H.

Por tanto H es cerrado en G. □

3.4. Clasificación de campos locales. Extensiones no ramificadas

A continuación caracterizamos los campos locales.

Proposición 3.4.1. *Sea K un campo local de característica 0, esto es, $\mathbb{Q} \subseteq K$. Sea $e := v_K(p)$ donde $p = \operatorname{car}(\mathcal{O}_K/\mathfrak{p}_K) = \operatorname{car} \tilde{K}$. Entonces K es una extensión finita de $\mathbb{Q}_p$, los números p-ádicos y $[K : \mathbb{Q}_p] = ef$ donde $f = [\mathcal{O}_K/\mathfrak{p}_K : \mathbb{F}_p]$. Finalmente, $\mathcal{O}_K$ es un $\mathbb{Z}_p$-módulo libre de rango ef: $\mathcal{O}_K \cong \mathbb{Z}_p^{ef}$ como $\mathbb{Z}_p$-módulo.*

Demostración. Sean v la valuación de K y $w := v|_{\mathbb{Q}}$. Se tiene que $p = p \cdot 1_K \neq 0$ y) $< w(p) = v(p) = e < \infty$. Se tiene que w es equivalente a la valuación p-ádica v_p de $\mathbb{Q}$. Sea L la cerradura de $\mathbb{Q}$ en K. Puesto que K es completo, L es completo con $v|_L$ y es una completación de $\mathbb{Q}$.

Puesto que w es equivalente a v_p, se sigue que $L \cong \mathbb{Q}_p$. Ahora $v(p) = e(K|\mathbb{Q}_p)v_p(p) = e(K|\mathbb{Q}_p) = e$. Se tiene que $\mathcal{O}_K/\mathfrak{p}_K = \mathbb{F}_{p^f}$ con $f = [\mathcal{O}_K/\mathfrak{p}_K : \mathbb{Z}_p/p\mathbb{Z}_p] = [\mathcal{O}_K/\mathfrak{p}_K : \mathbb{F}_p]$. Se sigue del Teorema 3.3.5 que $[K : \mathbb{Q}_p] = ef$ y que $\mathcal{O}_K$ es un $\mathbb{Z}_p$-módulo libre de rango ef. □

Lema 3.4.2. *Sea K un campo local con $\tilde{K} \cong \mathbb{F}_q$, q una potencia de p.*

(1) *Para cada $x \in \mathcal{O}_K$, el límite*

$$\omega(x) := \lim_{n \to \infty} x^{q^n}$$

existe en $\mathcal{O}_K$ y el mapeo ω satisface

$$\omega(x) \equiv x \bmod \mathfrak{p}_K, \qquad \omega(x)^q = \omega(x), \qquad \omega(xy) = \omega(x)\omega(y).$$

(2) *Sea $A = \{x \in K \mid x^{q-1} = 1\}$, $R = A \cup \{0\} = \{x \in K \mid x^q = x\}$. Entonces R es un conjunto completo de representantes de $\mathcal{O}_K/\mathfrak{p}_K$ en $\mathcal{O}_K$, conteniendo a 0. A es el conjunto de todas las $(q-1)$-raíces de la unidad en K y el homomorfismo canónico $\mathcal{O}_K \to \tilde{K}$ induce un isomorfismo de grupos multiplicativos: $A \cong \mathbb{F}_q^*$.*

Demostración. (1) Por inducción probaremos las congruencias $x^{q^n} \equiv x^{q^{n-1}} \bmod \mathfrak{p}_K^n$ para $n \geq 1$. Para $n = 1$, $x^q \equiv x \bmod \mathfrak{p}_K$ se sigue del hecho de que $\tilde{K}$ es el campo finito de q elementos. Supongamos que la congruencia se cumple para $n \geq 1$ de tal manera que $x^{q^n} = x^{q^{n-1}} + y$ con $y \in \mathfrak{p}_K^n$. El caso de $\operatorname{car} K = p$ se sigue inmediatamente tomando la q potencia de esta igualdad. Aquí presentamos el caso general. Se tiene

$$x^{q^{n+1}} = \sum_{i=0}^{q} \binom{q}{i} x^{iq^{n-1}} y^{q-i}.$$

Para $0 < i < q$, el entero $\binom{q}{i} = \frac{q}{i}\binom{q-1}{i-1}$ es divisible por p por lo que $\binom{q}{i} y^{q-i} \in \mathfrak{p}_K^{n+1}$. Para $i = 0$ lo anterior también se cumple, por lo cual obtenemos lo deseado: $x^{q^{n+1}} \equiv x^{q^n} \bmod \mathfrak{p}_K^{n+1}$.
Por tanto $\{x^{q^n}\}_{n=1}^{\infty}$ es una sucesión de Cauchy por lo que es convergente a un elemento $\omega(x)$ en $\mathcal{O}_K$ pues $\mathcal{O}_K$ es cerrado y K es completo. De las congruencias, obtenemos que $x^{q^n} \equiv x \bmod \mathfrak{p}_K$ y por tanto que $\omega(x) \equiv x \bmod \mathfrak{p}_K$. También obtenemos que

$$\omega(x)^q = \lim_{n\to\infty} x^{q^{n+1}} = \omega(x), \qquad \omega(xy) = \lim_{n\to\infty} (x^{q^n} y^{q^n}) = \omega(x)\omega(y).$$

(2) Sea $V = \{\omega(x) \mid x \in \mathcal{O}_K\}$. Puesto que $\omega(x) \equiv x \bmod \mathfrak{p}_K$, cada clase residual de $\mathcal{O}_K \bmod \mathfrak{p}_K$ contiene al menos un elemento de V. Por otro lado, puesto que $\omega(x)^q = \omega(x)$, V es un subconjunto de R. Ahora bien, el número de elementos x en K que satisfacen $x^q - x = 0$ es a lo más q mientras que el número de elementos de $\tilde{K}$ es q. Se sigue que $V = R$ y R es un sistema completo de representantes de $\mathcal{O}_K/\mathfrak{p}_K$ en $\mathcal{O}_K$. Se tiene $0 = \omega(0) \in R$. Puesto que $\omega(xy) = \omega(x)\omega(y)$, las propiedades enunciadas para A se siguen inmediatamente. □

Proposición 3.4.3. *Sea K un campo local de característica $p > 0$, es decir, $\mathbb{F}_p \subseteq K$. Entonces $(K, v_K) \cong (\mathbb{F}_q((T)), v_T)$ donde $v_T\big(\sum_{n=m}^{\infty} a_n T^n\big) = m$ si $a_m \neq 0$ para algún $q = p^f$, $f \geq 1$. De hecho, $\mathbb{F}_q \cong \mathcal{O}_K/\mathfrak{p}_K$ es el campo residual.*

Demostración. Puesto que K es un campo de característica p, el conjunto $R = \{x \in K \mid x^q = x\}$ en el Lema 3.4.2 es un subcampo de K de q elementos. Por tanto $\mathbb{F}_q = R \subseteq K$. Sea $\pi = \pi_K$ un elemento primo y representamos a K como en el Teorema 3.3.2 con $\pi_n = \pi^n$, $n \in \mathbb{Z}$. Entonces el mapeo $\sum_n a_n \pi^n \longmapsto \sum_n a_n T^n$, $a_n \in \mathbb{F}_q$, define un $\mathbb{F}_q$-isomorfismo $(K, v_K) \cong (\mathbb{F}_q((T)), v_T)$. □

Resumimos en el siguiente resultado la caracterización de los campos locales.

Teorema 3.4.4. *Sea K un campo local. Entonces*

(1) *Si* $\operatorname{car} K = 0$, $K/\mathbb{Q}_p$ *es una extensión finita de grado* ef, $e = v_K(p) = e(K|\mathbb{Q}_p)$ *y* $f = [\mathcal{O}_K/\mathfrak{p}_K : \mathbb{F}_p] = f(K|\mathbb{Q}_p)$.
(2) *Si* $\operatorname{car} K = p > 0$ *y* $\tilde{K} = \mathcal{O}_K/\mathfrak{p}_K \cong \mathbb{F}_q$, *entonces* $(K, v_K) \cong (\mathbb{F}_q((T)), v_T)$. □

A continuación veremos que las extensiones no ramificadas de campos locales están en correspondencia con las extensiones de los campos finitos.

Teorema 3.4.5. *Sea* K *un campo local con campo residual* $\tilde{K} = \mathcal{O}_K/\mathfrak{p}_K \cong \mathbb{F}_q$. *Para cada* $n \in \mathbb{N}$, *existe una extensión* L/K *no ramificada de grado* n, L *es único, es el campo de descomposición del polinomio* $x^{q^n} - x$ *sobre* K *y* L/K *es una extensión cíclica de grado* n. *Cada elemento* $\sigma \in \operatorname{Gal}(L/K)$ *induce un automorfismo* σ' *de* $\tilde{L}/\tilde{K}$ *y el mapeo* $\sigma \to \sigma'$ *induce un isomorfismo* $\operatorname{Gal}(L/K) \cong \operatorname{Gal}(\tilde{L}/\tilde{K})$.

Más aún, $L = K(A)$ *donde* $A = \{x \in \bar{K} \mid x^{q^n} = x\}$.

Demostración. El campo finito $\tilde{K} \cong \mathbb{F}_q$ tiene una extensión de grado n, la cual es única y es cíclica. Por tanto existe un polinomio mónico irreducible $g(x) \in \tilde{K}[x]$ de grado n. Sea $f(x) \in \mathcal{O}_K[x]$ mónico tal que $\overline{f(x)} = g(x) = f(x)$ mód $\mathfrak{p}_K$. Sea ω una raíz de $f(x)$, $f(\omega) = 0$. Sea $L := K(\omega)$.

Sea $f(x) = x^n + \sum_{i=0}^{n-1} a_i x^i \in \mathcal{O}_K[x]$. Entonces $\omega^n = -\sum_{i=0}^{n-1} a_i \omega^i$ con $a_i \in \mathcal{O}_K$. Por tanto

$$v_L(\omega^n) = n v_L(\omega) = v_L\Big(-\sum_{i=0}^{n-1} a_i \omega^i\Big) \geq \min_{0 \leq i \leq n-1} \{v_L(a_i) + i v_L(\omega)\}$$
$$\geq \min_{0 \leq i \leq n-1} \{i v_L(\omega)\} = i_0 v_L(\omega),$$

para algún $0 \leq i_0 \leq n-1$. Por tanto $(n - i_0) v_L(\omega) \geq 0$ de donde se sigue que $v_L(\omega) \geq 0$ y $\omega \in \mathcal{O}_L$. Sea $\alpha = \bar{\omega} \in \mathcal{O}_L/\mathfrak{p}_L$. Por tanto $g(\alpha) = 0 = \overline{f(\omega)}$. Como $g(x)$ es irreducible, se sigue que $[\tilde{K}(\alpha) : \tilde{K}] = \operatorname{gr} g(x) = n$.

Por otro lado, $f(\omega) = 0$ implica $[L : K] = [K(\omega) : K] \leq \operatorname{gr} f(x) = n$. Se sigue que

$$n = [\tilde{K}(\alpha) : \tilde{K}] \leq [\tilde{L} : \tilde{K}] = f(L|K) \leq [L : K] \leq n,$$

de donde se obtiene $[L : K] = f(L|K) = n$. Se sigue que L/K es una extensión no ramificada de grado n.

Sea E/K cualquier extensión no ramificada de grado n. Entonces $n = [E : K] = f(E|K) = [\tilde{E} : \tilde{K}]$ por lo que $\tilde{E} \cong \mathbb{F}_{q^n}$. Se tiene que $A = \{x \in \mathcal{O}_E \mid x^{q^n} = x\}$ es un conjunto completo de representantes de $\tilde{E}$ en $\mathcal{O}_E$ y A tiene q^n elementos, es decir, A es el conjunto de raíces de $x^{q^n} - x \in \mathcal{O}_E[x]$. Se sigue que $K(A)$ es el campo de descomposición de $x^{q^n} - x$ sobre K y como este polinomio es separable, la extensión $F = K(A)/K$ es separable y por tanto $K(A)/K$ es Galois.

Se tiene que $\tilde{K} \subseteq \tilde{F} \subseteq \tilde{E}$ y puesto que $A \subseteq F$, $\tilde{E} = \tilde{F} \cong \mathbb{F}_{q^n}$. Además $\tilde{F}/\tilde{K}$ es una extensión cíclica de grado n. Cada $\sigma \in \mathrm{Gal}(F/K)$ induce un automorfismo $\sigma' \in \mathrm{Gal}(\tilde{F}/\tilde{K})$ y el mapeo $\sigma \mapsto \sigma'$ define un homomorfismo $\mathrm{Gal}(F/K) \xrightarrow{\varphi} \mathrm{Gal}(\tilde{F}/\tilde{K})$.

Si $\sigma' = 1$, esto es, $\sigma \to 1$, $\sigma(A) = A$ pues A es el conjunto de raíces de $x^{q^n} - x$ y puesto que A es un conjunto completo de representantes de $\tilde{F}$, $\sigma' = 1$ implica que σ fija a cada elemento de A y, puesto que $F = K(A)$, $\sigma = 1$. Por lo tanto φ es inyectiva y

$$[F : K] = |\,\mathrm{Gal}(F/K)| \leq |\,\mathrm{Gal}(\tilde{F}/\tilde{K})| = [\tilde{F} : \tilde{K}] = f(F|K) \leq [F : K],$$

de donde se sigue que $[F : K] = f(F|K) = [\tilde{F} : \tilde{K}] = n$ y F/K es una extensión no ramificada de grado n. Por tanto $F = E$. Se sigue que $E = K(A)$ y por tanto E es único y $\mathrm{Gal}(E/K) \cong C_n$. □

Para finalizar esta sección, presentamos algunos resultados sobre la imagen de la norma de unidades y n-unidades indicando algunas referencias para su demostración más adelante.

Sea L/K una extensión finita y separable de campos locales con valuaciones v_K y v_L respectivamente. Se tiene la sucesión exacta $1 \longrightarrow U_K \longrightarrow K^* \xrightarrow{v_K} \mathbb{Z} \longrightarrow 0$ y el diagrama conmutativo

$$\begin{array}{ccccccccc}
1 & \longrightarrow & U_K & \longrightarrow & K^* & \xrightarrow{v_K} & \mathbb{Z} & \longrightarrow & 0 \\
 & & \downarrow{\scriptstyle i} & & \downarrow{\scriptstyle i} & & \downarrow{\scriptstyle \mathrm{Id}} & & \\
1 & \longrightarrow & U_L & \longrightarrow & L^* & \xrightarrow{v_L} & \mathbb{Z} & \longrightarrow & 0
\end{array}$$

donde las filas son exactas e i denota al encaje.

Proposición 3.4.6. *Sea* $\mathrm{N}_{L/K} \colon L^* \longrightarrow K^*$ *la norma. Entonces se tiene el siguiente diagrama conmutativo, donde las filas son exactas:*

$$\begin{array}{ccccccccc}
1 & \longrightarrow & U_L & \xhookrightarrow{\iota} & L^* & \xrightarrow{v_L} & \mathbb{Z} & \longrightarrow & 0 \\
 & & \downarrow{\scriptstyle \phi = \mathrm{N}_{L/K}} & & \downarrow{\scriptstyle \psi = \mathrm{N}_{L/K}} & & \downarrow{\scriptstyle f} & & \\
1 & \longrightarrow & U_K & \xhookrightarrow{\iota} & K^* & \xrightarrow{v_K} & \mathbb{Z} & \longrightarrow & 0
\end{array}$$

es decir, $f v_L(x) = v_K(\mathrm{N}_{L/K}\, x)$ *donde* $\mathrm{N}_{L/K}\, \mathfrak{p}_L = \mathfrak{p}_K^f$, $\mathfrak{p}_L$ *denota al ideal máximo de* $\mathcal{O}_L$ *y donde* $f = [\mathcal{O}_L/\mathfrak{p}_L : \mathcal{O}_K/\mathfrak{p}_K]$.

En particular tenemos $v_K(\mathrm{N}_{L/K}\, y) = f v_L(y)$ *para* $y \in L^*$.

Demostración. Se tiene que $\mathrm{N}_{L/K}\, U_L \subseteq U_K$ y $\iota \circ \varphi = \psi \circ \iota$ pues esto es simplemente $\iota \circ \mathrm{N}_{L/K} = \mathrm{N}_{L/K} \circ \iota$. La igualdad $v_K \circ \mathrm{N}_{L/K} = f v_L$ es el contenido del Teorema 3.1.14 y del Corolario 3.1.15. □

Corolario 3.4.7. *Si L/K es una extensión abeliana finita de campos locales, se tiene que $e = [U_K : \mathrm{N}_{L/K} U_L]$.*

Demostración. En general, para una extensión finita y separable de campos locales, tenemos, aplicando el Lema de la Serpiente (ver Teorema 4.1.8 más adelante), al diagrama de la Proposición 3.4.6, la sucesión exacta

$$\cdots \longrightarrow \text{núc}\, f = \{0\} \longrightarrow \text{conúcleo}\, \phi \longrightarrow \text{conúcleo}\, \psi \longrightarrow \text{conúcleo}\, f \longrightarrow 0,$$

donde el mapeo f es multiplicación por f. Por tanto

$$0 \longrightarrow \frac{U_K}{\mathrm{N}_{L/K} U_L} \longrightarrow \frac{K^*}{\mathrm{N}_{L/K} L^*} \longrightarrow \frac{\mathbb{Z}}{f\mathbb{Z}} \longrightarrow 0.$$

Se sigue que $[K^* : \mathrm{N}_{L/K} L^*] = [U_K : \mathrm{N}_{L/K} U_L] f$.

En el caso particular en que la extensión L/K sea abeliana, como veremos más adelante (Teorema 5.3.17), se tiene $[K^* : \mathrm{N}_{L/K} L^*] = [L : K] = ef$ y por tanto $e = [U_K : \mathrm{N}_{L/K} U_L]$. □

Proposición 3.4.8. *Sea L/K una extensión finita no ramificada de campos locales (y por tanto Galois). Entonces $\mathrm{N} := \mathrm{N}_{L/K} \colon U_L^{(n)} \longrightarrow U_K^{(n)}$ para toda n, esto es, $\mathrm{N}(U_L^{(n)}) \subseteq U_K^{(n)}$.*

Demostración. Sea $x = 1 + y \in U_L^{(n)}$ con $y \in \mathfrak{p}_L^n$. Para $\sigma \in G = \mathrm{Gal}(L/K)$ se tiene $\sigma x = 1 + \sigma y$ y por tanto

$$\mathrm{N}\, x = \prod_{\sigma \in G} \sigma x = \prod_{\sigma \in G} (1 + \sigma y) \equiv \Big(1 + \sum_{\sigma \in G} \sigma y\Big) \text{ mód } \mathfrak{p}_L^{2n}.$$

Ahora bien, como L/K es una extensión no ramificada, $\mathfrak{p}_L^n \cap U_K = \mathfrak{p}_K^n$ y $\sum_{\sigma \in G} \sigma y \in \mathfrak{p}_L^n \cap U_K = \mathfrak{p}_K^n$ lo cual implica que $\mathrm{N}\, x \equiv 1$ mód $\mathfrak{p}_K^n$. □

Pasando a los cocientes en la Proposición 3.4.8, tenemos

$$\mathrm{N} \colon U_L^{(n)}/U_L^{(n+1)} \longrightarrow U_K^{(n)}/U_K^{(n+1)}.$$

Para $n = 0$, $U_L^{(0)}/U_L^{(1)} = U_L/U_L^{(1)} \cong \tilde{L}^*$ y $U_K^{(0)}/U_K^{(1)} = U_K/U_K^{(1)} \cong \tilde{K}^*$.

Así, $\mathrm{N}_0 \colon \tilde{L}^* \longrightarrow \tilde{K}^*$ es la norma de campos residuales. Para $n \geq 1$, $U_L^{(n)}/U_L^{(n+1)} \cong \mathfrak{p}_L^n/\mathfrak{p}_L^{n+1}$ es un espacio vectorial de dimensión 1 sobre $\tilde{L}$, esto es, $\mathfrak{p}_L^n/\mathfrak{p}_L^{n+1} \cong \tilde{L}$.

Teorema 3.4.9. *Sea L/K una extensión no ramificada de campos locales (de Galois). Entonces*

(1) $\mathrm{N}(U_L^{(n)}) = U_K^{(n)}$ *para toda* $n \geq 1$.
(2) $U_K/\mathrm{N}\, U_L \cong \tilde{K}^*/\mathrm{N}\, \tilde{L}^*$.

(3) $K^*/\operatorname{N} L^* \cong \mathbb{Z}/f\mathbb{Z} \times \tilde{K}^*/\operatorname{N}\tilde{L}^*$ *donde* $f = [L:K] = [\tilde{L}:\tilde{K}]$ *(pues* L/K *es no ramificada).*

En nuestro caso, $\tilde{K}$ *y* $\tilde{L}$ *son campos finitos, por lo que* $\tilde{K}^*/\operatorname{N}\tilde{L}^* = \{1\}$ *y* $K^*/\operatorname{N} L^* \cong \mathbb{Z}/f\mathbb{Z}$.

Demostración. (1) Ver Teorema 5.1.11. Recordemos en general que si $\mathfrak{D}_{L/K}$ denota al diferente de la extensión L/K, entonces

$$\mathfrak{D}_{L/K}^{-1} = \{x \in L \mid \operatorname{Tr}(x\mathcal{O}_L) \subseteq \mathcal{O}_K\}.$$

Puesto que L/K es no ramificada, $\mathfrak{D}_{L/K}^{-1} = (1) = \mathcal{O}_L$. Se sigue que $\operatorname{Tr}\mathcal{O}_L = \mathcal{O}_K$.

De esta forma si $\pi \in \mathcal{O}_K$ con $v_K(\pi) = 1$, se tiene que $v_L(\pi) = 1$ al ser L/K no ramificada. Si $u \in U_L^{(n)}$, $u = 1 + \pi^n$ con $x \in \mathcal{O}_L$,

$$\operatorname{N} u = \prod_{\sigma\in G}(\sigma u) = \prod_{\sigma\in G}\sigma(1+\pi^n x) = \prod_{\sigma\in G}(1+\pi^n\sigma x) = 1 + \pi^n \operatorname{Tr} x + \pi^{n+1}\xi$$

con $\xi \in \mathcal{O}_K$ pues $\operatorname{N} u \in \mathcal{O}_K$.

Veamos que $(\operatorname{N} U_L^{(n)})U_K^{(n+1)} = U_K^{(n)}$. Se tiene $(\operatorname{N} U_L^{(n)})U_K^{(n+1)} \subseteq U_K^{(n)}$. Sea $a \in U_K^{(n)}$ arbitrario. Escribamos $a = 1 + \pi^n z$ con $z \in \mathcal{O}_K$. Sea $x \in \mathcal{O}_L$ tal que $\operatorname{Tr} x = z$. Se tiene

$$\operatorname{N}(1+\pi^n x) = 1 + \pi^n \operatorname{Tr} x + \pi^{n+1}\xi = 1 + \pi^n z + \pi^{n+1}\xi$$

con $\xi \in \mathcal{O}_K$ puesto que $\operatorname{N}(1+\pi^n x) \in \mathcal{O}_K$.

Queremos hallar $y \in \mathcal{O}_K$ tal que $(\operatorname{N}(1+\pi^n x))(1+\pi^{n+1}y) = 1 + \pi^n z = a$. Se tiene

$$\begin{aligned}\operatorname{N}(1+\pi^n x)(1+\pi^{n+1}y) &= 1 + \pi^n z + \pi^{n+1}\xi + \pi^{n+1}y + \pi^{2n+1}zy + \pi^{2n+2}y\xi \\ &= a + \pi^{n+1}(\xi + y(1 + \pi^n z + \pi^{n+1}\xi)).\end{aligned}$$

Esto es, necesitamos resolver $\xi + y(1+\pi^n z + \pi^{n+1}\xi) = 0$, es decir, $yw = -\xi$ donde $w = 1 + \pi^n z + \pi^{n+1}\xi \in U_K^{(n)} \subseteq U_K$. En este caso, $y = -\xi w^{-1}$ satisface lo deseado.

Así, dado $a \in U_K^{(n)}$, existen $x_1 \in U_L^{(n)}$ y $z_1 \in U_K^{(n+1)}$ tales que $a = (\operatorname{N} x_1)z_1$. Ahora, puesto que $z_1 \in U_K^{(n+1)}$, entonces existen $x_2 \in U_L^{(n+1)}$ y $z_2 \in U_K^{(n+2)}$ tales que $z_1 = (\operatorname{N} x_2)z_2$ por lo cual $a = \operatorname{N}(x_1x_2)z_2$.

Continuando el proceso, tenemos que para toda $t \in \mathbb{N}$, existen $x_1, \ldots, x_t \in \mathcal{O}_L$ y $z_t \in U_K^{(n+t)}$ tales que $a = \operatorname{N}(x_1 \cdots x_t) \cdot z_t$. Ahora $z_t \xrightarrow[t\to 1]{} 1$ por lo que $\lim_{t\to\infty} \operatorname{N}(x_1\cdots x_t)z_t = \operatorname{N}\big(\lim_{t\to\infty}(x_1\cdots x_t)\big) = a$.

Así, $x_1 \cdots x_t$ converge por ser L un campo completo y puesto que $x_i \in U_L^{(n+i)} \subseteq U_L^{(n)}$, el límite es un elemento de $U_L^{(n)}$. De esta forma, si $x_0 = \lim_{t\to\infty}(x_1\cdots x_t)$, $a = \operatorname{N} x_0$ con $x_0 \in U_L^{(n)}$. Se sigue que

$$\mathrm{N}\, U_L^{(n)} = U_K^{(n)}.$$

(2) Se tiene el siguiente diagrama conmutativo

$$\begin{array}{ccccccccc}
1 & \longrightarrow & U_L^{(1)} & \longrightarrow & U_L & \longrightarrow & \tilde{L}^* & \longrightarrow & 0 \\
 & & \downarrow{\scriptstyle \mathrm{N}_{L/K}} & & \downarrow{\scriptstyle \mathrm{N}_{L/K}} & & \downarrow{\scriptstyle \mathrm{N}_{L/K}} & & \\
1 & \longrightarrow & U_K^{(1)} & \longrightarrow & U_K & \longrightarrow & \tilde{K}^* & \longrightarrow & 0 \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
 & & 0 & & U_K/\mathrm{N}\, U_L & & \tilde{K}^*/\mathrm{N}\, \tilde{L}^* & &
\end{array}$$

Por el Lema de la Serpiente (ver Teorema 4.1.8 más adelante) se obtiene (2).

(3) Sea $\pi \in \mathcal{O}_K$, $v_K(\pi) = v_L(\pi) = 1$. Se tiene $K^* \cong (\pi) \times U_K$, $L^* \cong (\pi) \times U_L$. Por tanto $\mathrm{N}\, L^* = (\pi^f) \times \mathrm{N}\, U_L$. Se sigue

$$\frac{K^*}{\mathrm{N}\, L^*} \cong \frac{(\pi)}{(\pi^f)} \times \frac{U_K}{\mathrm{N}\, U_L} \cong \frac{\mathbb{Z}}{f\mathbb{Z}} \times \frac{\tilde{K}^*}{\mathrm{N}\, \tilde{L}^*}. \qquad \square$$

Corolario 3.4.10. *Sea L/K una extensión finita no ramificada de campos locales. Entonces las siguientes condiciones son equivalentes*

(1) $[K^* : \mathrm{N}\, L^*] = f = [\tilde{L} : \tilde{K}]$.
(2) $U_K = \mathrm{N}\, U_L$.
(3) $\tilde{K}^* = \mathrm{N}\, \tilde{L}^*$. $\square$

Observación 3.4.11. Si L/K es una extensión no ramificada no necesariamente Galois, la Proposición 3.4.8 y el Teorema 3.4.9 siguen siendo válidos.

Esto es aplicable para cuando L/K es una extensión de campos completos con respecto a valores absolutos no arquimedianos con campos residuales no necesariamente finitos. Cuando L y K son campos locales, si la extensión es finita no ramificada, necesariamente L/K es una extensión cíclica (ver el Teorema 3.4.5).

4

Cohomología de grupos finitos

4.1. Generalidades

En esta primera parte damos una serie de propiedades generales de módulos que detallaremos más adelante. Los resultados básicos de cohomología se pueden consultar en [149, 151, 160].

Definición 4.1.1. Sea G un grupo finito con identidad 1 y sea A un grupo abeliano. Entonces A se llama *G-módulo* (izquierdo) si G actúa en A ($G \times A \longrightarrow A$, $(\sigma, a) \longmapsto \sigma a$) tal que para todos $\sigma, \tau \in G$ y para todos $a, b \in A$, se tiene

(1) $1 \cdot a = a$
(2) $\sigma(a + b) = \sigma a + \sigma b$
(3) $(\sigma\tau)(a) = \sigma(\tau a)$

Sea $\mathbb{Z}[G] = \{\sum_{\sigma \in G} n_\sigma \sigma \mid n_\sigma \in \mathbb{Z}\}$. Entonces $\mathbb{Z}[G]$ es un grupo abeliano libre en $|G|$ generadores. La multiplicacion definida por

$$\Big(\sum_{\sigma \in G} n_\sigma \sigma\Big)\Big(\sum_{\sigma \in G} m_\sigma \sigma\Big) = \sum_{\tau \in G} \Big(\sum_{\varepsilon\delta = \tau} n_\varepsilon m_\delta\Big)\tau,$$

hace de $\mathbb{Z}[G]$ un anillo y $\mathbb{Z}[G]$ se llama el *anillo grupo* $\mathbb{Z}[G]$. Notemos que los conceptos de G-módulo y $\mathbb{Z}[G]$-módulo coinciden:

$$\Big(\sum_{\sigma \in G} n_\sigma \sigma\Big)a = \sum_{\sigma \in G} n_\sigma(\sigma a), \qquad a \in A.$$

Se tiene que $\mathbb{Z}[G]$, como grupo aditivo, es un G-módulo.

Sea $\mathrm{N}_G = \sum_{\sigma \in G} \sigma$, es decir, $n_\sigma = 1$ para toda $\sigma \in G$. Entonces $\mathbb{Z}\,\mathrm{N}_G = \{\sum_{\sigma \in G} n\sigma \mid n \in \mathbb{Z}\}$ es un ideal de $\mathbb{Z}[G]$ y $I_G := \{\sum_{\sigma \in G} n_\sigma \sigma \mid \sum_{\sigma \in G} n_\sigma = 0\}$ es también un ideal llamado el *ideal aumentación*.

Se tiene que $I_G = \text{núc}\,\varphi$, donde $\varphi\colon \mathbb{Z}[G] \longrightarrow \mathbb{Z}$, $\varphi\big(\sum_{\sigma\in G} n_\sigma\sigma\big) = \sum_{\sigma\in G} n_\sigma$ y la sucesión $0 \longrightarrow I_G \longrightarrow \mathbb{Z}[G] \xrightarrow{\varphi} \mathbb{Z}\ (\cong \mathbb{Z}\,\mathrm{N}_G) \longrightarrow 0$ es exacta. N_G se llama *norma* o *traza* de $\mathbb{Z}[G]$.

El mapeo $\mu\colon \mathbb{Z} \longrightarrow \mathbb{Z}[G]$, $\mu(n) := n\,\mathrm{N}_G$ se llama *coaumentación*. Sea $J_G := \mathbb{Z}[G]/\mathbb{Z}\,\mathrm{N}_G$. Entonces se tienen las sucesiones exactas de G-módulos

$$0 \longrightarrow I_G \longrightarrow \mathbb{Z}[G] \xrightarrow{\varphi} \mathbb{Z} \longrightarrow 0,$$
$$0 \longrightarrow \mathbb{Z} \xrightarrow{\mu} \mathbb{Z}[G] \longrightarrow J_G \longrightarrow 0.$$

Definición 4.1.2. Sea A un G-módulo. Se tienen los siguientes submódulos:

(1) $A^G = \{a \in A \mid \sigma a \text{ para toda } a \in A\}$ el *módulo fijo* de A.
(2) $\mathrm{N}_G A = \{\mathrm{N}_G a \mid a \in A\} = \{\sum_{\sigma\in G} \sigma a \mid a \in A\}$ el *grupo norma* de A.
(3) ${}_G A = {}_{\mathrm{N}_G}A = \{a \in A \mid \mathrm{N}_G a = \sum_{\sigma\in G} \sigma a = 0\}$ el núcleo de la norma.
(4) $I_G A = \{\sum_{\sigma\in G} n_\sigma(\sigma a_\sigma - a_\sigma) \mid a_\sigma \in A\} = \langle(\sigma - 1)A \mid \sigma \in G\rangle$.

Se verifica directamente que $\mathrm{N}_G A \subseteq A^G$ y $I_G A \subseteq {}_G A$. Formamos los cocientes $A^G/\mathrm{N}_G A$ y ${}_G A/I_G A$ los cuales son los grupos de cohomología (de Tate) de A en dimensiones 0 y -1 respectivamente.

Sea A un G-módulo y H un subgrupo de G. Entonces A es un H-módulo. Si además $H \lhd G$, A^H es un G/H-módulo.

Definición 4.1.3. Sean A y B dos G-módulos. Entendemos por un G-homomorfismo $f\colon A \longrightarrow B$ a un homomorfismo de grupos abelianos tal que $f(\sigma a) = \sigma f(a)$ para todas $a \in A$ y $\sigma \in G$.

Dados dos G-módulos A y B, $\mathrm{Hom}(A, B)$ denota el grupo de los $\mathbb{Z}$-homomorfismos (es decir, homomorfismos de grupos abelianos) de A en B. El grupo $\mathrm{Hom}(A, B)$ se puede hacer un G-módulo así: Si $f \in \mathrm{Hom}(A, B)$ y $\sigma \in G$, se define la acción de σ en f por:

$$\sigma \circ f = \sigma f = \sigma \circ f \circ \sigma^{-1},$$

es decir,

$$(\sigma f)(a) = \sigma f(\sigma^{-1} a),$$

para $a \in A$. Se tiene que el grupo de G-homomorfismos $\mathrm{Hom}_G(A, B)$ de A en B es un G-submódulo de $\mathrm{Hom}(A, B)$ y de hecho se tiene

$$(\mathrm{Hom}(A, B))^G = \mathrm{Hom}_G(A, B) \quad \text{(Proposición 4.5.6)}.$$

Para dos grupos abelianos A y B, el producto tensorial de A y B sobre $\mathbb{Z}$ se denota simplemente $A \otimes B$. Esto es, $A \otimes B = A \otimes_{\mathbb{Z}} B$. Se tiene que

$$\mathbb{Z} \otimes A \cong A, \quad (x \otimes a) \mapsto xa,$$
$$A \otimes B \cong B \otimes A.$$

Las siguientes propiedades son de verificación directa.

Proposición 4.1.4. *Sea $\{X_i \mid i \in I\}$ una familia de G-módulos y sea Y otro G-módulo. Entonces se tienen los siguientes isomorfismos*

(1) $Y \otimes \left(\bigoplus_{i\in I} X_i\right) \cong \bigoplus_{i\in I}(Y \otimes X_i)$.
(2) $\mathrm{Hom}\left(\bigoplus_{i\in I} X_i, Y\right) \cong \prod_{i\in I} \mathrm{Hom}_G(X_i, Y)$.
(3) $\mathrm{Hom}_G\left(Y, \prod_{i\in I} X_i\right) \cong \prod_{i\in I} \mathrm{Hom}_G(Y, X_i)$.
Si además Y es finitamente generado como grupo abeliano, se tiene
(4) $Y \otimes \left(\prod_{i\in I} X_i\right) \cong \prod_{i\in I}(Y \otimes X_i)$.
(5) $\mathrm{Hom}_G\left(Y, \bigoplus_{i\in I} X_i\right) \cong \bigoplus_{i\in I} \mathrm{Hom}_G(Y, X_i)$. □

Sean A, B, C, D cuatro G-módulos y $h\colon A \to C$ un G-homomorfismo. Entonces se tiene homomorfismos

$$h^*\colon \mathrm{Hom}(C, B) \longrightarrow \mathrm{Hom}(A, B), \quad f \longmapsto h^*(f) = f \circ h$$

y

$$h'\colon A \otimes B \longrightarrow C \otimes B, \quad a \otimes b \longmapsto h(a) \otimes b.$$

Sea $g\colon B \longrightarrow D$ un G-homomorfismo, se tienen los homomorfismos

$$g_\star\colon \mathrm{Hom}(A, B) \longrightarrow \mathrm{Hom}(A, D), \quad f \longmapsto g_\star(f) = g \circ f$$

y

$$g'\colon A \otimes B \longrightarrow A \otimes D, \quad a \otimes b \longmapsto a \otimes g(b).$$

También se tiene

$$h \otimes g\colon A \otimes B \longrightarrow C \otimes D, \quad (h \otimes g)(a \otimes b) = h(a) \otimes g(b).$$

Finalmente, si $H\colon C \longrightarrow A$ y $G\colon B \longrightarrow D$ son G-homomorfismos, se tiene

$$(H, G)\colon \mathrm{Hom}(A, B) \longrightarrow \mathrm{Hom}(C, D), \quad f \longmapsto G \circ f \circ H.$$

Definición 4.1.5. Un G-módulo X se llama *proyectivo* si satisface cualquiera de las siguientes condiciones equivalentes

(1) Todo diagrama $\begin{array}{ccccc} & & X & & \\ & \swarrow^{\varphi} & & & \\ B & \xrightarrow[\mu]{} & C & \longrightarrow & 0 \end{array}$ de G-modulos con μ suprayectiva, se puede extender $\psi\colon X \longrightarrow B$ tal que $\begin{array}{ccccc} & & X & & \\ & \swarrow & \vdots & \searrow^{\varphi} & \\ B & \xrightarrow[\mu]{} & C & \longrightarrow & 0 \end{array}$ es conmutativo, esto es, $\mu \circ \psi = \varphi$.

(2) X es sumando directo de un G-módulo libre.
(3) Cualquier sucesión exacta $0 \longrightarrow A \longrightarrow B \longrightarrow X \longrightarrow 0$ se escinde y $B \cong A \oplus X$.

Proposición 4.1.6. *Si X es un G-módulo y $0 \longrightarrow A \xrightarrow{h} B \xrightarrow{g} C \longrightarrow 0$ es una sucesión exacta de G-módulos, entonces la sucesión inducida*

$$0 \longrightarrow \mathrm{Hom}_G(X, A) \xrightarrow{h^*} \mathrm{Hom}_G(X, B) \xrightarrow{g^*} \mathrm{Hom}_G(X, C)$$

es exacta. Si X es proyectivo, entonces g^* es suprayectiva.

Demostración. Se deja al cuidado del lector. □

Proposición 4.1.7. (1) *Si $\cdots \longrightarrow X_{q+1} \xrightarrow{d_{q+1}} X_q \xrightarrow{d_q} X_{q-1} \longrightarrow \cdots$ es una sucesión exacta de $\mathbb{Z}$-módulos libres y si D es cualquier $\mathbb{Z}$ módulo, entonces la sucesión*

$$\cdots \longrightarrow \mathrm{Hom}(X_{q-1}, D) \xrightarrow{d_q^*} \mathrm{Hom}(X_q, D) \xrightarrow{d_{q+1}^*} \mathrm{Hom}(X_{q+1}, D) \longrightarrow \cdots$$

es exacta.
(2) *Si $0 \longrightarrow A \longrightarrow B \longrightarrow C \longrightarrow 0$ es una sucesión exacta de $\mathbb{Z}$-módulos libres y si X es cualquier $\mathbb{Z}$-módulo, entonces la siguiente sucesión es exacta:*

$$0 \longrightarrow A \otimes X \longrightarrow B \otimes X \longrightarrow C \otimes X \longrightarrow 0.$$

(3) *Si $0 \longrightarrow A \longrightarrow B \longrightarrow C \longrightarrow 0$ es una sucesión exacta de $\mathbb{Z}$-módulos y si X es un $\mathbb{Z}$-módulo libre, entonces la siguiente sucesión es exacta:*

$$0 \longrightarrow A \otimes X \longrightarrow B \otimes X \longrightarrow C \otimes X \longrightarrow 0.$$

Demostración. Se deja al cuidado del lector. □

Uno de los resultados centrales en cohomología de grupos es

Teorema 4.1.8 (Lema de la serpiente). *Sea*

$$\begin{array}{ccccccc} & & A & \xrightarrow{f} & B & \xrightarrow{g} & C & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle \alpha} & & \downarrow{\scriptstyle \beta} & & \downarrow{\scriptstyle \gamma} & & \\ 0 & \longrightarrow & A' & \xrightarrow{f'} & B' & \xrightarrow{g'} & C' & & \end{array}$$

un diagrama conmutativo de G–módulos, en donde las filas son exactas. Entonces existe un homomorfismo de conexión $\delta : \mathrm{núc}\,\gamma \longrightarrow \mathrm{conúcleo}\,\alpha$ *tal que*

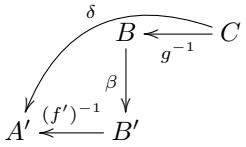
$$\text{núc}\,\alpha \xrightarrow{\tilde{f}} \text{núc}\,\beta \xrightarrow{\tilde{g}} \text{núc}\,\gamma \xrightarrow{\delta} \text{conúcleo}\,\alpha \xrightarrow{\tilde{f'}} \text{conúcleo}\,\beta \xrightarrow{\tilde{g'}} \text{conúcleo}\,\gamma$$

es una sucesión exacta, donde $\tilde{f}'$ y $\tilde{g}'$ son los homomorfismos inducidos de f' y g' respectivamente y $\tilde{f}$ y $\tilde{g}$ son las restricción de f y g respectivamente.

Además, si f es inyectiva, entonces $\tilde{f}$ es inyectiva y si g' es suprayectiva, $\tilde{g}'$ es suprayectiva.

Formalmente, tenemos $\delta = (f')^{-1} \circ \beta \circ g^{-1}$.

Demostración. Los detalles pueden ser consultados en [160, Theorem A.1.16]. El mapeo de conexión δ está dado de la siguiente forma. Sea $z \in \text{núc}\,\gamma$, entonces $z = g(y)$ para algún $y \in B$. Por tanto $0 = \gamma(z) = (\gamma \circ g)(y) = (g' \circ \beta)(y)$. Por tanto $\beta(y) \in \text{núc}\,g' = \text{im}\,f'$. Sea $\beta(y) = f'(a)$ para algún $a \in A'$. Sea $\delta(z) := a + \text{im}\,\alpha$. El mapeo de conexión se puede representar por $\delta := (f')^{-1} \circ \beta \circ g^{-1}$.



Se verifica que δ está bien definida y que la sucesión es exacta. □

Definición 4.1.9. Una *resolución proyectiva* P de $\mathbb{Z}$ es una sucesión exacta de G-módulos de la forma

$$P: \qquad \cdots \longrightarrow P_n \xrightarrow{\partial_n} P_{n-1} \xrightarrow{\partial_{n-1}} \cdots \longrightarrow P_1 \xrightarrow{\partial_1} P_0 \xrightarrow{\partial_0} \mathbb{Z} \longrightarrow 0,$$

donde $\mathbb{Z}$ se considera el G-módulo trivial: $g \circ x = x$ para todas $g \in G$ y $x \in \mathbb{Z}$ y los módulos P_n son proyectivos para toda $n \in \mathbb{N} \cup \{0\}$. En particular $\partial_n \circ \partial_{n+1} = 0$ para toda $n \geq 0$.

Dada una resolución proyectiva de $\mathbb{Z}$ y dado un G-módulo A se tienen las sucesiones

$$0 \longrightarrow \text{Hom}_G(P_0, A) \xrightarrow{\partial_1^*} \text{Hom}_G(P_1, A) \xrightarrow{\partial_2^*} \cdots \longrightarrow$$
$$\longrightarrow \text{Hom}_G(P_{n-1}, A) \xrightarrow{\partial_n^*} \text{Hom}_G(P_n, A) \longrightarrow \cdots$$

y

$$\cdots \longrightarrow P_n \otimes_G A \xrightarrow{\partial_n^+} P_{n-1} \otimes_G A \longrightarrow \cdots \longrightarrow P_1 \otimes_G A \xrightarrow{\partial_1^+} P_0 \otimes_G A \longrightarrow 0,$$

donde $\partial_n^*(\varphi) = \varphi \circ \partial_n$, $\partial_n^+(x \otimes a) = \partial_n x \otimes a$ y donde $\partial_0^* = 0$, $\partial_0^+ = 0$.

Definición 4.1.10. Para $n = 0, 1, \ldots,$ el *n-ésimo grupo de cohomología* del G-módulo A con respecto a la resolución proyectiva P : se define como el grupo:

$$H^n(P,A) := \text{núc}\,\partial^*_{n+1}/\,\text{im}\,\partial^*_n$$

y el *n-ésimo grupo de homología* como

$$H_n(P,A) := \text{núc}\,\partial^+_n/\,\text{im}\,\partial^+_{n+1}$$

Uno de los resultados centrales para la cohomología de grupos es que los grupos de cohomología y de homología no dependen de la resolución dada.

Teorema 4.1.11. *Si P y P' son dos resoluciones proyectivas de $\mathbb{Z}$, se tiene $H^n(P,A) \cong H^n(P',A)$ $H_n(P,A) \cong H_n(P',A)$ para toda $n = 0,1,\ldots$ y para todo G-módulo A.*

Demostración. Ver [160, Theorem A.1.19]. □

Definición 4.1.12. Para un G-módulo arbitrario A y para $n = 0,1,\ldots$ se definen los *grupos de cohomología* $H^n(G,A)$ como $H^n(P,A)$ y los *grupos de homología* $H^n(G,A)$ como $H^n(P,A)$ donde P es cualquier resolución proyectiva de $\mathbb{Z}$.

Gracias al Teorema 4.1.11, para tener los grupos de homología y de cohomología, basta hallar una resolución proyectiva de $\mathbb{Z}$. Sea $G^{n+1} = \underbrace{G \times \cdots \times G}_{n+1}$, $P_n := \mathbb{Z}[G^{n+1}]$ el anillo grupo. G actúa en P_n así: $x \circ (g_0,\ldots,g_n) = (xg_0,\ldots,xg_n)$, $x \in G$, $(g_0,\ldots,g_n) \in G^{n+1}$. Entonces P_n es un $\mathbb{Z}$-módulo libre con base $\{(g_0,\ldots,g_n) \mid g_i \in G\}$. Además P_n es un $\mathbb{Z}[G]$-módulo libre con base $\{(1,x_1,\ldots,x_n) \mid x_i \in G\}$.

Sea $\partial_n \colon P_n \longrightarrow P_{n-1}$ dada por

$$\partial_n(g_0,g_1,\ldots,g_n) := \sum_{i=0}^{n}(-1)^i(g_0,g_1,\ldots,\hat{g_i},\ldots,g_n),$$

donde $\hat{g_i}$ significa que el elemento g_i ha sido removido. Ahora $\partial_0 \colon P_0 = \mathbb{Z}[G] \longrightarrow \mathbb{Z}$ es la aumentación $\partial_0(g) = 1$ para toda $g \in G$. Se tiene que la sucesión

$$\cdots \longrightarrow P_n \xrightarrow{\partial_n} P_{n-1} \longrightarrow \cdots \longrightarrow P_1 \xrightarrow{\partial_1} P_0 \xrightarrow{\partial_0} \mathbb{Z} \longrightarrow 0$$

es G-exacta y se llama la *resolución canónica*.

Esto prueba la existencia tanto de los grupos de homología como los de cohomología para cualquier G-módulo A.

Sean A y B dos G-módulos y sea $f \colon A \to B$ un G-homomorfismo. Se definen $H^n(f) \colon H^n(G,A) \to H^n(G,B)$ y $H_n(f) \colon H_n(G,A) \to H_n(G,B)$, $n \geq 0$, de la siguiente forma: Sea

$$P: \qquad \cdots \longrightarrow P_n \xrightarrow{\partial_n} P_{n-1} \longrightarrow \cdots \longrightarrow P_1 \xrightarrow{\partial_1} P_0 \xrightarrow{\partial_0} \mathbb{Z} \longrightarrow 0$$

cualquier resolución proyectiva. Denotemos $P_i \otimes_G A = P_i \otimes_{\mathbb{Z}[G]} A$ y sea

$$f_n \colon P_n \otimes_G A \longrightarrow P_n \otimes_G B, \quad f_n(x \otimes_G a) = x \otimes_G f_n(a) = (1_{P_n} \otimes f)(x \otimes_G a).$$

Entonces f induce naturalmente el mapeo $H_n(f) \colon H_n(G, A) \longrightarrow H_n(G, B)$.

Ahora consideremos la sucesión

$$0 \longrightarrow \mathrm{Hom}_G(P_0, A) \xrightarrow{\partial_1^*} \mathrm{Hom}_G(P_1, A) \xrightarrow{\partial_2^*} \cdots \longrightarrow$$
$$\longrightarrow \mathrm{Hom}_G(P_{n-1}, A) \xrightarrow{\partial_n^*} \mathrm{Hom}_G(P_n, A) \longrightarrow \cdots$$

Sea $f_n^* \colon \mathrm{Hom}_G(P_n, A) \longrightarrow \mathrm{Hom}_G(P_n, B)$ dado por $f_n^*(\varphi) = f_n \circ \varphi$. Se tiene que f_n^* induce naturalmente $H^n(f) \colon H^n(G, A) \longrightarrow H^n(G, B)$, $n = 0, 1, 2, \ldots$.

Como consecuencia del lema de la serpiente, se puede demostrar

Teorema 4.1.13. *Si $0 \to A \xrightarrow{f} B \xrightarrow{g} C \to 0$ es una sucesión exacta de G–módulos, entonces existen homomorfismos de grupos $\varepsilon_n \colon H_{n+1}(G, C) \longrightarrow H_n(G, A)$ y $\delta_n \colon H^n(G, C) \longrightarrow H^{n+1}(G, A)$, $n = 0, 1, \ldots$ llamados de* conexión*, tales que las siguientes sucesiones infinitas de homología y de cohomología*

$$\cdots \longrightarrow H_{n+1}(G, B) \xrightarrow{H_{n+1}(g)} H_{n+1}(G, C) \xrightarrow{\varepsilon_n} H_n(G, A) \xrightarrow{H_n(f)} H_n(G, B) \longrightarrow$$
$$\cdots \xrightarrow{\varepsilon_0} H_0(G, A) \xrightarrow{H_0(f)} H_0(G, B) \xrightarrow{H_0(g)} H_0(G, C) \longrightarrow 0$$

y

$$0 \longrightarrow H^0(G, A) \xrightarrow{H^0(f)} H^0(G, B) \xrightarrow{H^0(g)} H_0(G, C) \xrightarrow{\delta_0} H^1(G, A) \longrightarrow \cdots$$
$$\xrightarrow{\delta_{n-1}} H^n(G, A) \xrightarrow{H^n(f)} H^n(G, B) \xrightarrow{H^n(g)} H^n(G, C) \xrightarrow{\delta_n} H^{n+1}(G, A) \longrightarrow \cdots$$

son sucesioes exactas de grupos.

Los mapeos de conexión están dados por el Lema de la Serpiente, a saber: si $\{P_n\}_n$ es una resolución proyectiva, $\partial_n \colon P_n \longrightarrow P_{n-1}$, $X_n = P_n \otimes_G X$, $X^n = \mathrm{Hom}_G(P_n, X)$, $X \in \{A, B, C\}$, $f_n \colon A_n \longrightarrow B_n$, $f_n(x \otimes a) = x \otimes f(a)$, $g_n \colon B_n \longrightarrow C_n$, $g_n(y \otimes b) = y \otimes g(b)$; $f^n \colon A^n \longrightarrow B^n$, $f^n(\mu) = f \circ \mu$, $g^n \colon B^n \longrightarrow C^n$, $g^n(\psi) = g \circ \psi$; $\partial_{n,X}^+ \colon X_n \longrightarrow X_{n-1}$, $\partial_{n,X}^+(\alpha \otimes x) = \partial_{n,X}(\alpha) \otimes x$ y $\partial_{n,X}^* \colon X^{n-1} \longrightarrow X_n$, $\partial_{n,X}^*(\mu) = \mu \circ \partial_{n,X}$, entonces, formalmente se definen:

$$\varepsilon_n = f_n^{-1} \circ \partial_{n+1,B}^+ \circ g_{n+1}^{-1} \qquad y \qquad \delta_n = (f^{n+1})^{-1} \circ \partial_{n+1,B}^* \circ (g^n)^{-1}.$$

Demostración. [160, Theorem A.3.6]. □

4.2. Homología y cohomología en bajas dimensiones

Sea A un G-módulo y P la resolución proyectiva canónica. Se tiene que $P_0 \otimes A \cong A$. Por tanto

$$H_0(G,A) = (P_0 \otimes A)/\operatorname{im}(\partial_1 \otimes 1).$$

Ahora $(\partial_1 \otimes 1)((g_1,g_2)\otimes a) = g_1 a - g_2 a$ por lo que $\operatorname{im}(\partial_1 \otimes 1) = \langle a - ga \mid g \in G, a \in A\rangle = DA \subseteq A$. Por tanto

$$H_0(G,A) = A_G = A/DA.$$

Sea $I_G = \big\{ \sum_{\sigma\in G} a_\sigma \sigma \mid \sum_{\sigma\in G} a_\sigma = 0\big\}$ el ideal aumentación de $\mathbb{Z}[G]$. Se tiene $\mathbb{Z}[G]/I_G \cong \mathbb{Z}$. Si $\sum_{\sigma\in G} a_\sigma\sigma \in I_G$, $a_1 = -\sum_{\sigma\neq 1} a_\sigma$. Por tanto

$$\begin{aligned}\sum_{\sigma\in G} a_\sigma\sigma &= a_1\cdot 1 + \sum_{\sigma\neq 1} a_\sigma\sigma = \big(-\sum_{\sigma\neq 1} a_\sigma\big)\cdot 1 + \sum_{\sigma\neq 1} a_\sigma\sigma \\ &= \sum_{\sigma\in G} a_\sigma(\sigma-1) \in \langle \sigma - 1 \mid \sigma\in G\rangle.\end{aligned}$$

Recíprocamente, $\sigma - 1 \in I_G$ para toda $\sigma \in G$. Por tanto $DA = \langle a - \sigma a \mid \sigma \in G, a \in A\rangle = I_G A$ y

$$H_0(G,A) = A/I_G A.$$

Sea ahora P la resolución canónica de A. Se tiene que la sucesión

$$0 \longrightarrow \operatorname{Hom}_G(\mathbb{Z},A) \xrightarrow{\partial_0^*} \operatorname{Hom}_G(P_0,A) \xrightarrow{\partial_1^*} \operatorname{Hom}_G(P_1.A)$$

es exacta tanto en $\operatorname{Hom}_G(\mathbb{Z},A)$ como en $\operatorname{Hom}_G(P_0,A)$ de donde obtenemos que

$$H^0(G,A) = \text{núc}\,\partial_1^* = \operatorname{im}\partial_0^* = \operatorname{Hom}_G(\mathbb{Z},A) \cong (\operatorname{Hom}(\mathbb{Z},A))^G \cong A^G.$$

Para calcular $H^1(G,A)$ consideremos P la resolución canónica

$$\cdots \longrightarrow P_n \xrightarrow{\partial_n} P_{n-1} \longrightarrow \cdots \longrightarrow P_1 \xrightarrow{\partial_1} P_0 \xrightarrow{\partial_0} \mathbb{Z} \longrightarrow 0,$$

donde $P_n = \mathbb{Z}[G^{n+1}]$. Sea $K_n := \operatorname{Hom}_G(P_n,A)$. Se tiene

$$0 \longrightarrow K_0 \xrightarrow{\partial_0^*} K_1 \longrightarrow \cdots \xrightarrow{\partial_n^*} K_n \xrightarrow{\partial_{n+1}^*} \cdots$$

Entonces

$$\begin{aligned}H^n(G,A) &= \text{núc}\,\partial_{n+1}^*/\operatorname{im}\partial_n^* = Z^n(G,A)/B^n(G,A) \\ &= n\text{-cociclos}/n\text{-cofronteras.}\end{aligned}$$

En particular se tiene $H^1(G,A) = \text{núc}\,\partial_2^*/\operatorname{im}\partial_1^* = Z^1(G,A)/B^1(G,A)$ donde

$$\begin{aligned}Z^1(G,A) &= \{f\colon G \longrightarrow A \mid f(gh) = gf(h) + f(g), g,h \in G\} \\ &= \text{grupo de los homomorfismos cruzados de } G \text{ en } A = 1\text{-cociclos}\end{aligned}$$

y

$$B^1(G,A) = \{f\colon G \longrightarrow A \mid \text{existe } a \in A \text{ con } f(g) = ga - a \text{ para toda } g \in G\}$$
$$= 1\text{-cofronteras.}$$

En otras palabras

$$H^1(G,A) = \frac{\{f(gh) = gf(h) + f(g)\}}{\{f(g) = ga - a\}}.$$

Por ejemlo, si G actúa de manera trivial en A, entonces $Z^1(G,A) = \mathrm{Hom}(G,A)$ y $B^1(G,A) = 0$, por lo que $H^1(G,A) = \mathrm{Hom}(G,A)$. En particular, si G es un grupo finito y $\mathbb{Z}$ tiene acción G-trivial, entonces $H^1(G,\mathbb{Z}) = \mathrm{Hom}(G,\mathbb{Z}) = \{0\}$.

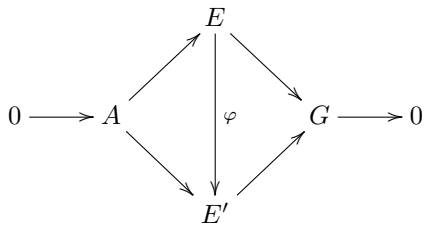
Un ejemplo importante es el grupo $H^2(G,A)$ el cual está en correspondencia biyectiva con las clases de equivalencia de extensiones de G por A. Más precisamente, un elemento $f \in Z^2(G,A)$ (llamado *conjunto de factores*) determina un único grupo E tal que $A \lhd E$ y $E/A \cong G$, es decir, E está definido por medio de la sucesión exacta

$$0 \to A \hookrightarrow E \xrightarrow{\pi} G \to 1$$

donde G actúa en el grupo abeliano A por:

$$\text{si } g = \pi(e) \in G, \text{ entonces } g \circ a := eae^{-1}.$$

Dos tales campos E, E', se llaman *equivalentes* si existe un isomorfismo $\varphi\colon E \to E'$ tal que el diagrama



es conmutativo.

Observación 4.2.1. Si E es equivalente a E', entonces E y E' son isomorfos pero puede ser que E y E' sean isomorfos pero no equivalentes.

Así, si A es un grupo abeliano y G es otro grupo que actúa sobre A, $g \circ a\colon G \times A \to A$, entonces hay exactamente $|H^2(G,A)|$ grupos $\mathcal{G}$, salvo equivalencia, tales que $1 \to A \to \mathcal{G} \to G \to 1$ es exacta con la acción de G en A dada.

Por ejemplo, se tiene que $H^2(\mathbb{Z}/p\mathbb{Z}, \mathbb{Z}/p\mathbb{Z}) \cong \mathbb{Z}/p\mathbb{Z}$ donde $G = \mathbb{Z}/p\mathbb{Z}$ actúa en $A = \mathbb{Z}/p\mathbb{Z}$ de manera trivial. Por tanto hay p clases de equivalencia de grupos de orden p^2, los cuales son necesariamente abelianos, pero únicamente hay dos grupos abelianos de orden p^2 no isomorfos entre sí, a saber $\mathbb{Z}/p^2\mathbb{Z}$ y $\mathbb{Z}/p\mathbb{Z} \oplus \mathbb{Z}/p\mathbb{Z}$. De hecho el elemento identidad de $H^2(\mathbb{Z}/p\mathbb{Z}, \mathbb{Z}/p\mathbb{Z})$ corresponde a $\mathbb{Z}/p\mathbb{Z} \oplus \mathbb{Z}/p\mathbb{Z}$ y los otros $p-1$ elementos corresponden a diversos grupos $\mathbb{Z}/p^2\mathbb{Z}$ (isomorfos pero inequivalentes).

4.3. Cohomología de Galois y grupos de cohomología de Tate

Sea G un grupo de Galois de alguna extensión de campos L/K y sea A un G-módulo asociado de alguna manera a la extensión L/K. Entonces los G-grupos de cohomología y de homología de A si llaman *grupos de cohomología de Galois*.

Uno de los resultados centrales de *cohomología de Galois* es

Teorema 4.3.1 (Teorema 90 de Hilbert). *Si L/K es una extensión finita de Galois con grupo $G = \mathrm{Gal}(L/K)$ entonces $H^1(G, L^*) = \{1\}$.*

Demostración. Sea $f \in Z^1(G, L^*)$, $f\colon G \to L^*$, $f(\theta\sigma) = f(\theta) \cdot \theta f(\sigma)$ para cualesquiera $\theta, \sigma \in G$.

Del Teorema 2.1.1 seleccionamos $x \in L^*$ tal que $y = \sum_{\sigma\in G} f(\sigma)\sigma(x) \in L^*$, es decir, $\sum_{\sigma\in G} f(\sigma)\sigma \neq 0$. Entonces $\theta(y) = f(\theta)^{-1}y$ para toda $\theta \in G$ y por tanto $f(\theta) = \theta(y^{-1})y = \theta(y)^{-1}y = \frac{y}{\theta(y)} \in B^1(G, L^*)$. Se sigue que $H^1(G, L^*) = \{1\}$. □

Observación 4.3.2. En realidad, el Teorema 4.3.1 es una generalización del Teorema 90 de Hilbert, el cual es este mismo resultado pero únicamente para G un grupo cíclico finito. El Teorema 4.3.1 se debe a E. Noether y por tanto este teorema es de Hilbert–Noether.

Observación 4.3.3. El Teorema 2.1.2 (b) (extensiones de Kummer) es una aplicación del Teorema 90 de Hilbert con $G = \langle\sigma\rangle$ un grupo cíclico y usando que en este caso $H^1(G, L^*) \cong H^{-1}(G, L^*)$.

Para las extensiones de Artin–Schreier (Teorema 2.1.2 (a)), se usa que $H^1(G, L) = 0$ lo cual se cumple para cualquier grupo $G = \mathrm{Gal}(L/K)$ y cualquier campo. Ver la Observación 4.3.4.

Observación 4.3.4. Si L/K es una extensión finita de Galois, entonces el Teorema de la Base Normal (ver [136, Teorema T1.4.3]) establece que existe $z \in L$ tal que $\{\sigma z\}_{\sigma\in G}$, con $G = \mathrm{Gal}(L/K)$, es una base de L/K. Esto nos dice que, como G–módulos, se tiene

$$L \cong K[G] = \Big\{ \sum_{\sigma\in G} \alpha_\sigma\sigma \mid \alpha_\sigma \in K \Big\} \cong K \otimes_{\mathbb{Z}} \mathbb{Z}[G]$$

de donde se sigue que $H^n(G, L) = 0$ para toda $n \in \mathbb{Z}$. Ver Corolario 4.4.9.

A continuación presentamos los llamados grupos de cohomología de Tate, que son una amalgama entre la homología y la cohomología, modificando ligeramente los grupos $H_0(G, A)$ y $H^0(G, A)$ y re-indexando adecuadamente. El proceso también se puede obtener por medio de la resolución completa, ver Subsección 4.5.

Sean $\mathrm{N} = \sum_{\sigma\in G}\sigma \in \mathbb{Z}[G]$ y I_G el ideal aumentación. Se tiene $\mathrm{N}((\sigma-1)a) = 0$ para cualquier $\sigma \in G$ y por tanto $I_G \subseteq \text{núc}\,\mathrm{N}$. Por otro lado $\mathrm{N}\,\sigma a = \sigma\,\mathrm{N}\,a = \mathrm{N}\,a$, de donde obtenemos que $\operatorname{im}\mathrm{N} \subseteq A^G$. Recordemos que $H_0(G,A) = A_G = A/I_GA$ y que $H^0(G,A) = A^G$. Por tanto, pasando a cocientes, N^* define un homomorfismo $\mathrm{N}^*\colon H_0(G,A) \longrightarrow H^0(G,A)$. Sea $\widehat{H}_0(G,A) = \text{núc}\,\mathrm{N}^* = \text{núc}\,\mathrm{N}\,/I_GA$ y $\widehat{H}^0(G,A) = \text{conúcleo}\,\mathrm{N}^* = A^G/\,\mathrm{N}\,A$.

Se tienen las sucesión exactas

$$0 \longrightarrow \widehat{H}_0(G,A) \longrightarrow H_0(G,A) \xrightarrow{\mathrm{N}_A^*} H^0(G,A) \longrightarrow \widehat{H}^0(G,A) \longrightarrow 0.$$

Teorema 4.3.5. *Sea G un grupo finito y sea $0 \longrightarrow A \xrightarrow{f} B \xrightarrow{g} C \longrightarrow 0$ una sucesión exacta de G-módulos. Entonces el diagrama*

$$\begin{array}{ccccccccc}
H_1(G,C) & \xrightarrow{\varepsilon_0} & H_0(G,A) & \xrightarrow{H_0(f)} & H_0(G,B) & \xrightarrow{H_0(g)} & H_0(G,C) & \longrightarrow & 0 \\
\downarrow & & \downarrow{\scriptstyle \mathrm{N}_A^*} & & \downarrow{\scriptstyle \mathrm{N}_B^*} & & \downarrow{\scriptstyle \mathrm{N}_C^*} & & \downarrow \\
0 & \longrightarrow & H^0(G,A) & \xrightarrow[H^0(f)]{} & H^0(G,B) & \xrightarrow[H^0(g)]{} & H^0(G,C) & \xrightarrow[\delta_0]{} & H^1(G,A)
\end{array}$$

es conmutativo y las filas son exactas, donde ε_0 y δ_0 son los homomorfismos de conexión. □

Por el Lema de la Serpiente (Teorema 4.1.8), se obtiene:

Corolario 4.3.6. *Existe un homomorfismo canónico (*$\text{núc}\,\mathrm{N}_C^* = \hat{H}_0(G,C)$ *y* $\text{conúcleo}\,\mathrm{N}_A^* = \hat{H}^0(G,A)$*)*

$$\delta\colon \widehat{H}_0(G,C) \longrightarrow \widehat{H}^0(G,A)$$

que hace que la sucesión de grupos

$$\widehat{H}_0(G,C) \longrightarrow \widehat{H}_0(G,B) \longrightarrow \widehat{H}_0(G,C) \xrightarrow{\delta}$$
$$\xrightarrow{\delta} \widehat{H}^0(G,A) \longrightarrow \widehat{H}^0(G,B) \longrightarrow \widehat{H}^0(G,C)$$

sea exacta. Formalmente $\delta = f^{-1} \circ \mathrm{N}_B^* \circ g^{-1}$.

Además δ nos da una sucesión exacta

$$\cdots \longrightarrow H_1(G,C) \xrightarrow{\varepsilon_0} \widehat{H}_0(G,C) \longrightarrow \widehat{H}_0(G,B) \longrightarrow \widehat{H}_0(G,C) \xrightarrow{\delta}$$
$$\xrightarrow{\delta} \widehat{H}^0(G,A) \longrightarrow \widehat{H}^0(G,B) \longrightarrow \widehat{H}^0(G,C) \xrightarrow{\delta_0} H^1(G,A) \longrightarrow \cdots$$ □

Definición 4.3.7. Sea G un grupo finito. Se definen los *grupos de cohomología de Tate* de A, con exponentes en $\mathbb{Z}$, se definen por:

$$\widehat{H}^n(G,A) = H^n(G,A) \text{ para } n \geq 1.$$
$$\widehat{H}^0(G,A) = A^G/\,\mathrm{N}\,A.$$
$$\widehat{H}^{-1}(G,A) = \text{núc}\,\mathrm{N}_A\,/I_GA.$$
$$\widehat{H}^{-n}(G,A) = H_{n-1}(G,A) \text{ para } n \geq 2.$$

Como consecuencia del Corolario 4.3.6 y del Teorema 4.1.13, se obtiene

Teorema 4.3.8. *Si* $0 \longrightarrow A \longrightarrow B \longrightarrow C \longrightarrow 0$ *es una sucesión exacta de* G*-módulos, entonces*

$$\cdots \longrightarrow \widehat{H}^{n-1}(G,C) \longrightarrow \widehat{H}^n(G,A) \longrightarrow \widehat{H}^n(G,B) \longrightarrow$$
$$\longrightarrow \widehat{H}^n(G,C) \longrightarrow \widehat{H}^{n+1}(G,A) \longrightarrow \cdots$$

es una sucesión exacta para toda $n \in \mathbb{Z}$*. Los mapeos de conexión están dados como en el Teorema* 4.1.13. □

Notación 4.3.9. Sean G un grupo finito y A un G-módulo. Los grupos de cohomología de Tate de G con coeficientes en A serán indistintamente denotados por $\widehat{H}^n(G,A)$ y por $H^n(G,A)$. En adelante, a menos que se diga lo contrario, los grupos de cohomología serán los grupos de cohomología de Tate.

4.3.1. Grupos cíclicos

Sea $G = \langle \sigma \rangle$ un grupo finito de orden n. Sea $\mathrm{N} = \sum_{i=0}^{n-1} \sigma^i$ y $D = \sigma - 1$. Se tiene que $ND = DN = \sigma^n - 1 = 0$. Consideremos el ideal aumentación $I_G = \langle g - 1 \mid g \in G \rangle = \langle \sigma - 1 \rangle = D\mathbb{Z}[G]$.

Proposición 4.3.10. *Se tiene* $\operatorname{núc} \mathrm{N} = I_G = \operatorname{im} D$ *y* $\operatorname{núc} D = \mathbb{Z}[G]^G = \operatorname{im} \mathrm{N}$. □

Sean $T_i := \mathbb{Z}[G]$, $i = 0, 1, \ldots$ y $\partial_i \colon T_i \longrightarrow T_{i-1}$ dada por

$$\partial_i = \begin{cases} D & \text{si } i \text{ es impar,} \\ \mathrm{N} & \text{si } i \text{ es par,} \end{cases}, \quad i \geq 1.$$

Sea $\varepsilon \colon \mathbb{Z}[G] \longrightarrow \mathbb{Z}$ el homomorfismo aumentación: $\varepsilon\big(\sum_{i=0}^{n-1} a_i \sigma^i\big) = \sum_{i=0}^{n-1} a_i$.

Se tiene que la sucesión

$$\cdots \longrightarrow T_i \xrightarrow{\partial_i} T_{i-1} \longrightarrow \cdots \longrightarrow T_1 \xrightarrow{\partial_1} T_0 \xrightarrow{\varepsilon} \mathbb{Z} \longrightarrow 0,$$

de G-módulos es exacta.

Esta es una resolución libre de $\mathbb{Z}$ y por tanto, para $n = 1, 2, \ldots$, se tiene

$$\widehat{H}^{2n-1}(G,A) = H^{2n-1}(G,A) = \frac{\operatorname{núc} \mathrm{N}^*}{\operatorname{im} D^*} = \frac{\operatorname{núc} \mathrm{N}_A}{DA} = \widehat{H}^{-1}(G,A),$$
$$\widehat{H}^{2n}(G,A) = H^{2n}(G,A) = \frac{\operatorname{núc} D^*}{\operatorname{im} \mathrm{N}^*} = \frac{A^G}{\mathrm{N}\,A} = \widehat{H}^0(G,A).$$

Similarmente, para homología, obtenemos para $n = 1, 2, \ldots$,

$$\widehat{H}^{-2n}(G,A) = H_{2n-1}(G,A) = \frac{\operatorname{núc} D_*}{\operatorname{im} \mathrm{N}_*} = \frac{A^G}{\mathrm{N}\,A} = \widehat{H}^0(G,A),$$
$$\widehat{H}^{-(2n+1)}(G,A) = H_{2n}(G,A) = \frac{\operatorname{núc} \mathrm{N}_*}{\operatorname{im} D_*} = \frac{\operatorname{núc} \mathrm{N}_A}{DA} = \widehat{H}^{-1}(G,A) = \widehat{H}^1(G,A).$$

Teorema 4.3.11. *Sea G un grupo cíclico finito. Entonces, para cualquier G-módulo A, tenemos*

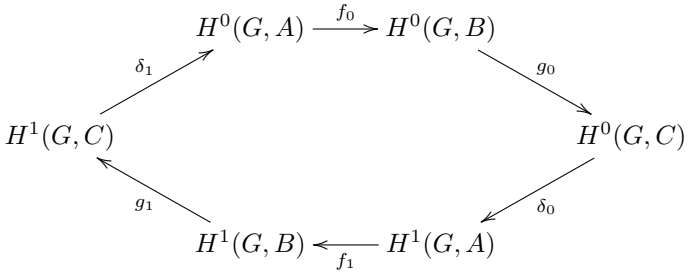
$$\widehat{H}^{2n}(G,A) = \widehat{H}^{0}(G,A) = \frac{A^G}{\mathrm{N}\,A},$$
$$\widehat{H}^{2n+1}(G,A) = \widehat{H}^{-1}(G,A) = \frac{\text{núc}\,\mathrm{N}_A}{DA},$$

para $n \in \mathbb{Z}$. □

Definición 4.3.12. Sea G es un grupo cíclico finito y sea A un G–módulo tal que $H^0(G,A)$ y $H^1(G,A)$ son finitos de órdenes $h_0(A)$ y $h_1(A)$ respectivamente. Se define el *cociente de Herbrand* de A por $h(A) := \frac{h_0(A)}{h_1(A)}$.

Se tiene

Teorema 4.3.13. *Sea G un grupo cíclico finito y sea $0 \to A \xrightarrow{f} B \xrightarrow{g} C \to 0$ una sucesión exacta de G–módulos. Se tiene que el siguiente hexágono es exacto:*



y si dos de $h(A)$, $h(B)$ y $h(C)$ están definidos, el tercero también está definido y se tiene $h(B) = h(A)h(C)$.

Demostración. Se sigue inmediatamente de la sucesión larga de cohomología (Teorema 4.1.13) y del hecho de que $H^0(G,X) \cong H^2(G,X)$ (Teorema 4.3.11). □

Proposición 4.3.14. *Si G es un grupo cíclico finito y A es un G–módulo finito, entonces $h(A) = 1$, esto es, $|H^i(G,A)|$ es constante para toda $i \in \mathbb{Z}$.*

Demostración. [160, Proposition A.4.6]. □

Corolario 4.3.15. *Sea $f\colon A \longrightarrow B$ un G-homomorfismo tal que* núc f *y* conúcleo f *son finitos. Entonces $h(A)$ está definido $\iff$ $h(B)$ lo está y en este caso $h(A) = h(B)$.*

En particular, si $A < B$ es de índice finito, entonces $h(A) = h(B)$. □

Como consecuencia de la Proposición 4.1.4, se tiene la aditividad de la cohomología. Ver también [117, Propositions (3.7) y (3.8), Part I].

Proposición 4.3.16. *Sean G un grupo finito y $\{A_i\}_{i\in\mathcal{I}}$ una familia de G–módulos. Entonces*

(1) $H^n(G, \bigoplus_i A_i) \cong \bigoplus_i H^n(G, A_i)$,
(2) $H^n(G, \prod_i A_i) \cong \prod_i H^n(G, A_i)$,

para toda $n \in \mathbb{Z}$. □

4.4. Módulos inducidos y co-inducidos

Definición 4.4.1. Sea X un grupo abeliano y sea G actuando en X de manera trivial $g \circ x = x$ para toda $g \in G$ y para toda $x \in X$. El G-módulo $A := \mathrm{Hom}(\mathbb{Z}[G], X)$ se llama *G-módulo coinducido* por X.

Se tiene para $\varphi \in A$, $g, g' \in G$, $(g \circ \varphi)(g') = g\varphi(g^{-1}g') = \varphi(g^{-1}g')$.

Definición 4.4.2. Un G-módulo A se llama inducido si tiene la forma $A = \mathbb{Z}[G] \otimes D$ donde D es un grupo abeliano (considerado como G-módulo trivial).

Proposición 4.4.3. *Sea G un grupo finito y sea D un grupo abeliano con G-acción trivial. Entonces*

$$\mathbb{Z}[G] \otimes D \cong \mathrm{Hom}(\mathbb{Z}[G], D) \cong \bigoplus_{\sigma\in G} \sigma D.$$

Esto es, cuando G es finito, inducido y co-inducido es lo mismo.

Demostración. Sea $A = \mathbb{Z}[G] \otimes D$. Para $a \in A$, $a = \big(\sum_{\sigma\in G} \alpha_\sigma \sigma\big) \otimes d = \sum_{\sigma\in G} \sigma(\alpha_\sigma \otimes d) = \sum_{\sigma\in G} \sigma(a_\sigma d) \in \sum_{\sigma\in G} \sigma D$ y claramente la suma es directa. De aqui obtenemos que $\mathbb{Z}[G] \otimes D \cong \bigoplus_{\sigma\in G} \sigma D$.

Por otro lado, Sea $\Lambda\colon\ \mathrm{Hom}(\mathbb{Z}[G], D) \longrightarrow \bigoplus_{\sigma\in G} \sigma D$, $f \longmapsto \sum_{\sigma\in G} \sigma f(\sigma) = \big(f(\sigma)\big)_{\sigma\in G}$. Entonces Λ es un isomorfismo. □

Teorema 4.4.4. *Sea A un G-módulo co-inducido, entonces $H^q(G, A) = 0$ para toda $q \geq 1$.*

Demostración. Sea B cualquier G-módulo y sea A un G-módulo co-inducido, $A = \sum_{\sigma\in G} \sigma D$ con D un grupo abeliano, G-módulo trivial.

Veamos que $\mathrm{Hom}_G(B, A) = \mathrm{Hom}(B, D)$.

Sea $f \in \mathrm{Hom}_G(B, A) = \big(\mathrm{Hom}(B, A)\big)^G$. Entonces $f(b) = \sum_{\sigma\in G} \sigma f_{b,\sigma}$ con $f_{b,\sigma} \in D$. Se tiene que $\tau f(b) = \sum_{\sigma\in G} \tau\sigma f_{b,\sigma} = \sum_\theta \theta f_{b,\tau^{-1}\theta} = f(b)$. Por tanto $f_{b,\mu} = f_b$ constante para toda $\mu \in G$.

Por tanto $f(b) = \sum_{\sigma\in G} \sigma f_b = \big(\sum_{\sigma\in G} \sigma\big) f_b$, $f_b \in D$. Definimos

$$\Lambda\colon \operatorname{Hom}_G(B,A) \longrightarrow \operatorname{Hom}(B,D) \quad \text{dada por } \Lambda(f)=\tilde{f},\ \tilde{f}(b)=f_b\in D.$$

Entonces Λ es un isomorfismo.

Sea

$$(P) \qquad \cdots \longrightarrow P_i \longrightarrow P_{i-1} \longrightarrow \cdots \longrightarrow P_1 \longrightarrow P_0 \longrightarrow \mathbb{Z} \longrightarrow 0$$

una resolución y sea $K_i = \operatorname{Hom}_G(P_i,A) = \operatorname{Hom}(P_i,D)$. Puesto que P_i es $\mathbb{Z}$-libre, la sucesión

$$\begin{aligned} 0 \longrightarrow \operatorname{Hom}(\mathbb{Z},D) \xrightarrow{d_0} \operatorname{Hom}(P_0,D) \xrightarrow{d_1} \operatorname{Hom}(P_1,D) \xrightarrow{d_2} \cdots \\ \longrightarrow \operatorname{Hom}(P_{i-1},D) \xrightarrow{d_i} \operatorname{Hom}(P_i,D) \longrightarrow \cdots \end{aligned}$$

es exacta (Proposición 4.1.7) y $H^q(G,A) = \frac{\text{núc } d_{q+1}}{\text{im } d_q} = 0$ para $q \geq 1$. □

Teorema 4.4.5. *Si A es un G-módulo inducido, entonces $H_q(G,A)=0$ para toda $q\geq 1$.*

Demostración. Sea B cualquier G-módulo. Se tiene

$$B \otimes_G A \cong B \otimes_G \big(\mathbb{Z}[G] \otimes_{\mathbb{Z}} D\big) \cong \big(B \otimes_G \mathbb{Z}[G]\big) \otimes_{\mathbb{Z}} D \cong B \otimes_{\mathbb{Z}} D.$$

Esto es

$$B \otimes_G A \cong B \otimes_{\mathbb{Z}} D.$$

Consideremos la resolución

$$(P) \qquad \cdots \longrightarrow P_i \longrightarrow P_{i-1} \longrightarrow \cdots \longrightarrow P_1 \longrightarrow P_0 \longrightarrow \mathbb{Z} \longrightarrow 0.$$

Obtenemos que

$$\begin{aligned} 0 \longrightarrow \mathbb{Z} \otimes_G A \longrightarrow P_0 \otimes_G A \longrightarrow P_1 \otimes_G A \longrightarrow \cdots \\ \longrightarrow P_{i-1} \otimes D \longrightarrow P_i \otimes D \longrightarrow \cdots \end{aligned}$$

y por tanto

$$\begin{aligned} 0 \longrightarrow \mathbb{Z} \otimes D \longrightarrow P_0 \otimes D \longrightarrow P_1 \otimes D \longrightarrow \cdots \\ \longrightarrow P_{i-1} \otimes D \longrightarrow P_i \otimes D \longrightarrow \cdots \end{aligned}$$

Puesto que los módulos P_i son $\mathbb{Z}$-libres, la última sucesión es exacta (Proposición 4.1.7) de donde se sigue que $H_q(G,A)=0$ para toda $q\geq 1$. □

Observación 4.4.6. Para la cohomología usual, es decir, no la cohomología de Tate, $H_0(G,A)$ y $H^0(G,A)$ no tiene por que ser 0 si A es inducido y/o co-inducido. Por ejemplo $H^0(G,A) = A^G \cong D$. Veremos que para la cohomología de Tate, estos dos grupos son 0.

Teorema 4.4.7. *Si G es un grupo finito y A es un G-módulo inducido o co-inducido, $\widehat{H}^0(G,A) = \widehat{H}_0(G,A) = 0$.*

Demostración. Veamos que $\widehat{H}_0(G,A) = 0$ con A un G-módulo inducido. Sea $A = \bigoplus_{\sigma\in D} \sigma D$. Sea $a \in A$, $a = \big(\sigma a_\sigma\big)_{\sigma\in G} = \sum_{\sigma\in G} a_\sigma\sigma$. Si $a \in A^G$,

$$\tau a = \sum_{\sigma\in G} \tau\sigma a_\sigma = \sum_{\theta\in G} \theta a_{\tau^{-1}\theta} = \sum_{\sigma\in G} \sigma a_{\tau^{-1}\sigma} = \sum_{\sigma\in G} a_\sigma\sigma = a$$

para toda $\tau \in G$. Por tanto $a_\sigma = a_0 \in D$ constante. Se sigue que $a = \big(\sum_{\sigma\in G}\sigma\big)a_0 = \mathrm{N}_G\, a_0$ de donde se sigue que $A^G \subseteq \mathrm{N}_G\, A$ y por tanto $\widehat{H}^0(G,A) = \frac{A^G}{\mathrm{N}_G\, A} = \{0\}$.

Ahora veamos que $\widehat{H}_0(G,A) = \frac{\text{núc}\,\mathrm{N}_G}{I_G A} = \{0\}$. Sea $a \in A$ como antes. Entonces

$$\begin{aligned}\mathrm{N}_G\, a &= \sum_{\tau\in G} \tau \sum_{\sigma\in G} \sigma a_\sigma = \sum_{\tau\in G}\sum_{\sigma\in G} \tau\sigma a_\sigma \\ &= \sum_{\theta\in G} \theta\big(\sum_{\tau\in G} a_{\tau^{-1}\theta}\big) = \big(\sum_{\theta\in G}\theta\big)\big(\sum_{\sigma\in G} a_\sigma\big).\end{aligned}$$

Por tanto $\mathrm{N}_G\, a = 0 \iff \sum_{\sigma\in G} a_\sigma = 0$, esto es, $\sum_{\sigma\in G}\sigma a_\sigma \in I_G A$ y por tanto $\hat{H}_0(G,A) = \{0\}$. □

Definición 4.4.8. Un G-módulo A se llama *cohomológicamente trivial* si $\widehat{H}^q(H,A) = \{0\}$ para toda $q \in \mathbb{Z}$ y para todo subgrupo H de G.

Corolario 4.4.9. *Si G es un grupo finito y A es un G-módulo inducido o co-inducido, entonces A es cohomológicamente trivial.*

Demostración. Se sigue de los Teoremas 4.4.4, 4.4.5 y 4.4.7 y del hecho de que si A es G-inducido o G-co-inducido, entonces A es H-inducido o H-co-inducido para todo subgrupo H de G. □

Sea L/K una extensión finita de Galois con grupo G. Entonces tanto L como L^* son G-módulos. Además, L/K tiene una base normal, esto es, existe $\alpha \in L$ tal que $\{\sigma\alpha\}_{\sigma\in G}$ es una base de la extensión L/K ([136, Teorema 1.4.3]). Como G-módulo se tiene que $L = \bigoplus_{\sigma\in G} K(\sigma\alpha) \cong K \otimes_{\mathbb{Z}} \mathbb{Z}[G]$. En particular L es G-inducido y por el Corolario 4.4.9 L es cohomológicamente trivial.

El mapeo $f\colon G \longrightarrow I_G/I_G^2$ dado por $f(\sigma) = (\sigma - 1) + I_G^2$ induce un isomorfismo

$$G/G' \cong I_G/I_G^2,$$

donde G' es el subgrupo conmutador de G. El isomorfismo inverso está dado por $h((\sigma-1)+I_G^2) = \sigma G'$.

4.5. Resolución completa

El estudio de la homología y la cohomología hecha hasta aquí, se rompe en dos partes, una para cada una de ellas. John Tate desarrolló un complejo en el cual la homología y la cohomología se funden en un solo grupo a partir de una resolución completa, la cual presentamos aquí por conveniencia y para futura referencia.

Sea C un $\mathbb{Z}$-módulo. Definimos $\widehat{C} := \mathrm{Hom}(C, \mathbb{Z})$. Entonces $\widehat{C}$ es un $\mathbb{Z}$-módulo. Sea A cualquier $\mathbb{Z}$-módulo. Definimos

$$\Phi\colon C \otimes A \longrightarrow \mathrm{Hom}(\widehat{C}, A)$$

el homomorfismo de $\mathbb{Z}$-módulos dado por

$$\Phi(c \otimes a)(\xi) = \xi(c) \cdot a, \quad c \in C, a \in A, \xi \in \hat{c}, \xi(c) \in \mathbb{Z}. \tag{4.5.1}$$

Si C es un $\mathbb{Z}$-módulo libre finitamente generado, esto es, $C \cong \mathbb{Z}^m$ para algún $m \in \mathbb{N}$, entonces $\widehat{C} \cong C \cong \mathbb{Z}^m$. El isomorfismo está dado de la siguiente forma. Si $\{e_i\}_{i=1}^m$ es una base de C como $\mathbb{Z}$-módulo, se define $e_i^* \in \widehat{C}$ por $e_i^*(e_j) = \langle e_i^*, e_j \rangle = \delta ij$, la delta de Kronecker. Entonces $\{e_i^*\}_{i=1}^m$ es una $\mathbb{Z}$-base de $\widehat{C}$. Se tiene un isomorfismo natural $\widehat{\widehat{C}} \cong C$ identificando e_i^{**} con e_i.

Proposición 4.5.1 (homotopía de contracción). *Dada una sucesión exacta de $\mathbb{Z}$-módulos libres*

$$\cdots \longrightarrow X_{n+1} \xrightarrow{d_{n+1}} X_n \xrightarrow{d_n} X_{n-1} \longrightarrow \cdots,$$

existe un $\mathbb{Z}$-homomorfismo $s_n\colon X_n \longrightarrow X_{n+1}$ tal que

$$d_{n+1}s_n + s_{n-1}d_n = \mathrm{Id}_{X_n}.$$

Demostración. Sea $U_n = \mathrm{núc}\, d_n = \mathrm{im}\, d_{n+1}$. Como $U_n < X_n$ y X_n es un $\mathbb{Z}$-módulo libre, U_n es un $\mathbb{Z}$-módulo libre. Se tiene la sucesión exacta

$$0 \longrightarrow U_n \xhookrightarrow{i_n} X_n \xrightarrow{d_n} U_{n-1} \longrightarrow 0. \tag{4.5.2}$$

Como U_{n-1} es un $\mathbb{Z}$-módulo libre, la sucesión (4.5.2) se escinde.

Sean $\psi_n\colon U_{n-1} \longrightarrow X_n$, $\varphi\colon X_n \longrightarrow U_n$ los mapeos de escisión. Entonces $d_n \circ i_n = 0$, $\varphi_n \circ \psi_n = 0$, $d_n \circ \psi_n = \mathrm{Id}_{U_{n-1}}$ y $\varphi_n \circ i_n = \mathrm{Id}_{U_n}$. Sea $s_n := \psi_{n+1} \circ \varphi_n\colon X_n \longrightarrow X_{n+1}$. Escribiendo $X_n = i_n(U_n) \oplus \psi_n(U_{n-1})$, se verifica el resultado. □

Corolario 4.5.2. *Dada una sucesión exacta de $\mathbb{Z}$-módulos libres*

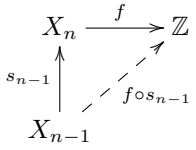
$$(X) \qquad \cdots \longrightarrow X_{n+1} \xrightarrow{d_{n+1}} X_n \xrightarrow{d_n} X_{n-1} \longrightarrow \cdots,$$

entonces la sucesión

$$(\widehat{X}) \qquad \cdots \longrightarrow \widehat{X}_{n-1} \xrightarrow{\widehat{d}_{n+1}} \widehat{X}_n \xrightarrow{\widehat{d}_n} \widehat{X}_{n+1} \longrightarrow \cdots,$$

es exacta, donde $\widehat{d}_n\colon \widehat{X}_n \longrightarrow \widehat{X}_{n+1}$ está dada por $\widehat{d}_n(f) = f \circ d_{n+1}$.

Demostración. Sea $\widehat{s}_{n-1}\colon \widehat{X}_{n-1} \longrightarrow \widehat{X}_n$, definido por $\widehat{s}_{n-1}(f) = f \circ s_{n-1}$



. Entonces $\widehat{d}_n \circ \widehat{s}_n + \widehat{s}_{n+1} \circ \widehat{d}_n = \mathrm{Id}_{\widehat{X}_n}$. De aquí, se verifica directamente que la sucesión $(\widehat{X})$ es exacta. □

Ahora consideremos $\mathbb{Z}[G]$-módulos, G un grupo finito. Sea C un G-módulo izquierdo y $\widehat{C} = \mathrm{Hom}(C, \mathbb{Z})$ es un G-módulo izquierdo con la acción usual:

$$(\sigma f)(c) = \sigma(f(\sigma^{-1}c)) = f(\sigma^{-1}c),$$

pues G actúa trivialmente en $\mathbb{Z}$.

Consideremos Φ dado en (4.5.1). Directamente se verifica que $\sigma(\Phi(c \otimes a)) = \Phi(\sigma(c \otimes a))$ y por tanto Φ es un G-homomorfismo.

Si C es un $\mathbb{Z}$-módulo libre de rango finito, Φ es biyectiva. De hecho, sea $\{e_i\}_{i=1}^n$ una base de C como $\mathbb{Z}$-módulo. Si $\Phi(c \otimes a) = 0$, entonces si $c = \sum_{i=1}^n \alpha_i e_i$, evaluando en $\xi = e_j^*$ obtenemos $\xi(c) \cdot a = \alpha_j a = 0$ para toda j. Por tanto $c \otimes a = \sum_{i=1}^n \alpha_i e_i \otimes a = \sum_{i=1}^n e_i \otimes \alpha_i a = 0$ de donde se sigue que Φ es inyectiva.

Ahora, sea $f \in \mathrm{Hom}(\widehat{C}, A)$. Sea $f(e_j^*) = a_j$ para $1 \leq j \leq n$. Entonces $\Phi\big(\sum_{i=1}^n e_i \otimes a_i\big) = f$ y Φ es suprayectiva.

Con lo anterior, hemos probado

Teorema 4.5.3. *Sea C un $\mathbb{Z}[G]$-módulo libre con base finita. Entonces*

$$C \otimes A \cong \mathrm{Hom}(\widehat{C}, A)$$

como G-módulos izquierdos y donde el isomorfismo esta dado por Φ definido en (4.5.1). *También tenemos que $\widehat{\widehat{C}} \cong C$ como G-módulos.* □

Proposición 4.5.4. *Si C es un $\mathbb{Z}[G]$-módulo libre con una base finita, entonces $\widehat{C}$ también lo es y $\widehat{C} \cong C$ como $\mathbb{Z}[G]$-módulos.*

Demostración. Primero supongamos $C \cong \mathbb{Z}[G]$. Si probamos que $\widehat{C} \cong \mathbb{Z}[G]$, entonces para $C = \bigoplus_{i=1}^n \mathbb{Z}[G]f_i$, se seguirá que $\widehat{C} \cong \bigoplus_{i=1}^n \widehat{\mathbb{Z}[G]f_i} \cong \bigoplus_{i=1}^n \mathbb{Z}[G]f_i^*$. Por tanto basta probar el caso $C \cong \mathbb{Z}[G]$, esto es, debemos probar que $\mathrm{Hom}(\mathbb{Z}[G], \mathbb{Z}) \cong \mathbb{Z}[G]$.

Sea $\{e_i\}_{i=1}^n$ una base de $C = \mathbb{Z}[G]$ como $\mathbb{Z}$-módulo (por ejemplo, $\{e_i\}_{i=1}^n = G$). Sea $\{e_i^*\}_{i=1}^n \subseteq \widehat{C}$ la base dual, esto es, $e_j^*(e_i) = \delta_{ij}$ para $1 \leq i, j \leq n$. Sea φ el $\mathbb{Z}$-isomorfismo $\varphi\colon C \longrightarrow \widehat{C}$ dado por $\varphi(e_i) = e_i^*$, $1 \leq i \leq n$. Es inmediato que φ es $\mathbb{Z}[G]$-isomorfismo. □

Hemos probado

Proposición 4.5.5. *Dada una sucesión exacta de $\mathbb{Z}[G]$-módulos izquierdos y $\mathbb{Z}[G]$-homomorfismos*

$$(X) \qquad \cdots \longrightarrow X_{n+1} \xrightarrow{d_{n+1}} X_n \xrightarrow{d_n} X_{n-1} \longrightarrow \cdots,$$

tales que cada X_n es un $\mathbb{Z}[G]$-módulo libre con base finita, entonces la sucesión

$$(\widehat{X}) \qquad \cdots \longrightarrow \widehat{X}_{n-1} \xrightarrow{\widehat{d}_{n+1}} \widehat{X}_n \xrightarrow{\widehat{d}_n} \widehat{X}_{n+1} \longrightarrow \cdots,$$

es exacta, donde cada $\widehat{X}_n$ es un $\mathbb{Z}[G]$-módulo libre con base finita. □

Ahora consideremos dos G-módulos izquierdos C y A. En el producto tensorial, C se considera como un G-módulo derecho definiendo

$$c\sigma := \sigma^{-1}c, \quad c \in C, \sigma \in G.$$

Se sigue que, considerando $C \otimes A$ como un G-módulo izquierdo con: $\sigma(c \otimes a) = (\sigma a) \otimes (\sigma a)$, $c \in C$, $a \in A$ y $\sigma \in G$, se tiene

Proposición 4.5.6. $C \otimes_G A \cong (C \otimes A)_G = \frac{C \otimes A}{I_G(C \otimes A)}$ *y* $\mathrm{Hom}_G(C, A) = \mathrm{Hom}(C, A)^G$.

Demostración. Por definición $C \otimes_G A$, donde C es un G-módulo derecho y A es un G-módulo izquierdo, es F/R_G donde F es el grupo abeliano libre generado por los elementos (c, a) de $C \times A$: $F = \bigoplus_{\substack{c \in C \\ a \in A}} \mathbb{Z}(c, a)$ y R_G es el subgrupo generado por

$$(c + c_1, a) - (c, a) - (c_1, a); \quad (c, a + a_1) - (c, a) - (c, a_1);$$
$$(c\sigma, a) - (c, \sigma a), \quad \sigma \in G.$$

Ahora bien, si consideramos $C \otimes A = C \otimes_{\mathbb{Z}} A$, F es el mismo y $R_{\mathbb{Z}}$ es el subgrupo generado por

$$(c + c_1, a) - (c, a) - (c_1, a); \quad (c, a + a_1) - (c, a) - (c, a_1).$$

Se tiene la sucesión exacta

$$0 \longrightarrow R_G/R_{\mathbb{Z}} \longrightarrow F/R_{\mathbb{Z}} \longrightarrow F/R_G \longrightarrow 0.$$

El grupo $R_G/R_{\mathbb{Z}}$ visto en $F/R_{\mathbb{Z}} = C \otimes A$ es el grupo generado por $\langle (c\sigma \otimes a) - (c \otimes \sigma a) \mid c \in C, a \in A, \sigma \in G \rangle$.

Vemos a C como G-módulo izquierdo: $c\sigma := \sigma^{-1}c$. De esta forma tenemos que $C \otimes_G A = (C \otimes A)/\mathcal{R}$ donde $\mathcal{R} = \langle (\sigma c, a) - (c, \sigma a) \rangle$. Se tiene que

$$(c\sigma, a) - (c, \sigma a) = (\sigma^{-1}c, a) - (c, \sigma a) = (\sigma^{-1} - 1)(c, \sigma a) \in I_G(C \otimes A),$$

de donde se sigue que $C \otimes_G A = \frac{C \otimes A}{I_G(C \otimes A)}$.

Sea $f \in \mathrm{Hom}_G(C, A)$. En particular $f \in \mathrm{Hom}(C, A)$. Ahora G actúa en $\mathrm{Hom}(C, A)$ por $(\sigma \circ f)(c) = \sigma f(\sigma^{-1}c)$. Ahora si $f \in \mathrm{Hom}_G(C, A)$, $f(\sigma^{-1}c) = \sigma^{-1}f(c)$, entonces

$$(\sigma \circ f)(c) = \sigma f(\sigma^{-1}c) = \sigma\sigma^{-1}f(c) = f(c),$$

esto es, $(\sigma \circ f) = f$ de donde se sigue que $f \in \mathrm{Hom}(C, A)^G$.

Recíprocamente, si $f \in \mathrm{Hom}(C, A)^G$, $(\sigma \circ f) = f$, por lo tanto, $f(\sigma c) = (\sigma \circ f)(\sigma c) = (\sigma f)(\sigma^{-1}(\sigma c)) = (\sigma f)(c)$, por lo que $f \in \mathrm{Hom}_G(C, A)$. □

Sea C un $\mathbb{Z}[G]$-módulo libre de rango finito. Por el Teorema 4.5.3 se sigue que $\widehat{C} \otimes A \cong \mathrm{Hom}(C.A)$.

Proposición 4.5.7. *Sea C un $\mathbb{Z}[G]$-módulo libre de rango finito y sea A un grupo abeliano. Entonces la norma $\mathrm{N}\colon (\widehat{C} \otimes A) \longrightarrow (\widehat{C} \otimes A)$ induce un isomorfismo*

$$\mathrm{N}^*\colon (\widehat{C} \otimes A)_G \longrightarrow (\widehat{C} \otimes A)^G.$$

Demostración. Notemos que $\mathbb{Z}[G] \otimes A \cong (\bigoplus_{\sigma\in G} \sigma\mathbb{Z}) \otimes A \cong \bigoplus_{\sigma\in G} \sigma(\mathbb{Z} \otimes A) \cong \bigoplus_{\sigma\in G} \sigma A$. Se sigue que $X := \widehat{C} \otimes A = \bigoplus_{\sigma\in G} \sigma A$.

Sea $a \in X$, $a = (\sigma a_\sigma)_{\sigma\in G} = \sum_{\sigma\in G} \sigma a_\sigma$. Si $a \in X^G$, entonces

$$\tau a = \sum_{\sigma\in G} \tau\sigma a_\sigma = \sum_{\theta\in G} \theta a_{\tau^{-1}\theta} = \sum_{\sigma\in G} \sigma a_{\tau^{-1}\sigma} = \sum_{\sigma\in G} \sigma a_\sigma = a,$$

para toda $\tau \in G$. Se sigue que $a_\sigma = a_{\sigma'}$ para cualesquiera $\sigma, \sigma' \in G$. Por tanto $a_0 = a_\sigma$ es constante para toda $\sigma \in G$. Se sigue que $a = \big(\sum_{\sigma\in G} \sigma\big)a_0 = \mathrm{N}_G\, a_0$. Por tanto $X^G \subseteq \mathrm{N}_G\, X$, lo cual implica que N^* es suprayectiva.

Ahora sea $a \in X$, $a = \sum_{\sigma\in G} \sigma a_\sigma$ con $a_\sigma \in D$. Entonces

$$\mathrm{N}_G\, a = \sum_{\tau\in G} \sum_{\sigma\in G} \sigma a_\sigma = \big(\sum_{\theta\in G} \theta\big)\big(\sum_{\sigma\in G} a_\sigma\big).$$

Por tanto $\mathrm{N}_G\, a = 0 \iff \sum_{\sigma\in G} a_\sigma = 0$ y en este caso se tiene $\sum_{\sigma\in G} \sigma a_\sigma = \sum_{\sigma\in G} \sigma a_\sigma - \sum_{\sigma\in G} 1a_\sigma = \sum_{\sigma\in G} (\sigma - 1)a_\sigma \in I_G X$. Por tanto N^* es inyectiva y es un isomorfismo. □

Como consecuencia, tenemos

Teorema 4.5.8. *Sean C y A dos G-módulos izquierdos con C un $\mathbb{Z}[G]$-módulo libre de rango finito. Entonces existe un isomorfismo $\tau\colon \widehat{C} \otimes_G A \longrightarrow \mathrm{Hom}_G(C, A)$ dado por*

$$[\tau(f \otimes_G a)](c) = \sum_{\sigma\in G} f(\sigma^{-1}c)\sigma a,$$

con $f \in \widehat{C}$, $c \in C$ y $a \in A$.

Demostración. Se había probado que $\widehat{C} \otimes A \cong \mathrm{Hom}(C, A)$ (Teorema 4.5.3) con isomorfismo Φ dado por $\Phi\colon \widehat{C} \otimes A \longrightarrow \mathrm{Hom}(\widehat{\widehat{C}}, A) \cong \mathrm{Hom}(C, A)$,

$$\Phi(f \otimes a)(\xi) = \hat{\xi}(f)a = f(\xi)a.$$

Por otro lado $\mathrm{N}^*\colon (\widehat{C} \otimes A)_G \xrightarrow{\cong} \mathrm{Hom}(C, A)^G = \mathrm{Hom}_G(C, A)$ es un isomorfismo. Se tiene

$$\begin{array}{ccc} (\widehat{C} \otimes A)_G & \xrightarrow[\cong]{\mathrm{N}^*} & (\widehat{C} \otimes A)^G \\ & \overset{\tau}{\searrow} & \downarrow \Phi \\ & & \mathrm{Hom}(C, A)^G = \mathrm{Hom}_G(C, A) \end{array}$$

Entonces $\tau = \Phi \circ \mathrm{N}^*$ es el isomorfismo. Se tiene

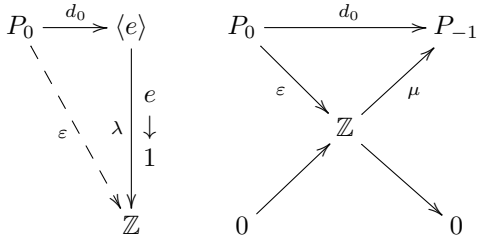
$$\begin{aligned} \tau(f \otimes a)(c) &= \sum_{\sigma \in G} \Phi(\sigma f \otimes \sigma a)(c) = \sum_{\sigma \in G} \hat{c}(\sigma f)\sigma a = \sum_{\sigma \in G} (\sigma f)(c)\sigma a \\ &= \sum_{\sigma \in G} \sigma f(\sigma^{-1}c)\sigma a = \sum_{\sigma \in G} f(\sigma^{-1}c)\sigma a. \end{aligned}$$ □

Definición 4.5.9. Una *resolución completa* P para un grupo finito G es una sucesión exacta

$$(P) \quad \cdots \longrightarrow P_n \xrightarrow{d_n} P_{n-1} \longrightarrow \cdots \longrightarrow P_0 \xrightarrow{d_0} P_{-1} \longrightarrow \cdots \longrightarrow P_{-n} \xrightarrow{d_{-n}} \cdots$$

de módulos P_n que son $\mathbb{Z}[G]$-libres finitamente generados junto con un elemento $e \in (P_{-1})^G$, $e \neq 0$, tal que la imagen de d_0 está generada por e.

Puesto que $\sigma e = e$ para toda $\sigma \in G$, se sigue de que $\operatorname{im} d_0$ es un $\mathbb{Z}$-módulo generado por e. Además como P_{-1} es $\mathbb{Z}$-libre, se tiene $ne \neq 0$ para toda $n \in \mathbb{Z}$, $n \neq 0$. Por tanto d_0 admite una factorización $d_0 = \mu \circ \varepsilon$, donde ε es un G-epimorfismo y μ es un G-monomorfismo dado por $\mu(1) = e$.



Consideremos las sucesiones exactas

$$(P_i) \qquad \cdots \longrightarrow P_n \xrightarrow{d_n} P_{n-1} \xrightarrow{d_{n-1}} \cdots \longrightarrow P_0 \xrightarrow{\varepsilon} \mathbb{Z} \longrightarrow 0$$

$$(P_d) \qquad 0 \longrightarrow \mathbb{Z} \xrightarrow{\mu} P_{-1} \xrightarrow{d_{-1}} \cdots \xrightarrow{d_{-n+2}} P_{-n+1} \xrightarrow{d_{-n+1}} P_{-n} \longrightarrow \cdots$$

La sucesión (P_i) da una resolución proyectiva de $\mathbb{Z}$ con $\mathbb{Z}[G]$-módulos libres finitamente generados. Por el Corolario 4.5.2 y el dual de (P_d): $\widehat{P}_{-n} = \mathrm{Hom}(P_{-n}, \mathbb{Z})$, se tiene que

$$(\widehat{P}_d) \qquad \cdots \longrightarrow \widehat{P}_{-n} \xrightarrow{\widehat{d}_{-n+1}} \widehat{P}_{-n+1} \xrightarrow{\widehat{d}_{-n+2}} \cdots \xrightarrow{\widehat{d}_{-1}} \widehat{P}_{-1} \xrightarrow{\hat{\mu}} \mathbb{Z} \longrightarrow 0$$

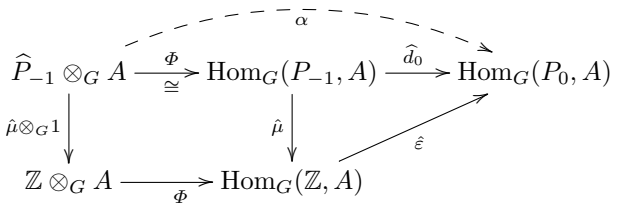
también da una resolución proyectiva por medio de $\mathbb{Z}[G]$-módulos libres finitamente generados. Recíprocamente, dadas dos resoluciones (P_i) y (P'_i) de $\mathbb{Z}$ por $\mathbb{Z}[G]$-módulos finitamente generados, podemos construir una resolución completa empalmando (P_i) y $(\widehat{P}'_i)$ reenumerados adecuadamente.

Dada una resolución completa (P) y un G-módulo izquierdo A, podemos considerar el *complejo*

$$\mathrm{Hom}_G(P, A) = \big\{ \mathrm{Hom}_G(P_n, A) \big\}_{n=-\infty}^{\infty}.$$

Para $n \geq 0$, dejamos el grupo $\mathrm{Hom}_G(P_n, A)$ como está. Para $n < 0$ reemplazamos $\mathrm{Hom}_G(P_n, A)$ por el grupo isomorfo $\widehat{P}_n \otimes_G A$ usando el isomorfismo τ dado en el Teorema 4.5.8.

Veamos el mapeo $\widehat{P}_{-1} \otimes_G A \xrightarrow{\alpha} \mathrm{Hom}_G(P_0, A)$, inducido por $d_0 \colon P_0 \longrightarrow P_{-1}$. Se tiene $d_0 = \mu \circ \varepsilon$ y por tanto obtenemos el diagrama conmutativo



Esto es, α se factoriza:

$$\begin{array}{ccc} \widehat{P}_{-1} \otimes_G A & \xrightarrow{\alpha} & \mathrm{Hom}_G(P_0, A) \\ \downarrow & & \uparrow \\ H_0(G, A) & \xrightarrow{\mathrm{N}^*} & H^0(G, A) \end{array}$$

De esto obtenemos finalmente.

Teorema 4.5.10. *Para cualquier G-módulo izquierdo A, los grupos de cohomología de Tate $\hat{H}^n(G, A)$, $n \in \mathbb{Z}$ se obtiene como $H^n\big(\mathrm{Hom}_G(P, A)\big)$ donde P es cualquier resolución completa de G. Si $f \colon A \longrightarrow B$ es un homomorfismo de G-módulos, entonces los $H^n(f)$ puede ser calculados de $\mathrm{Hom}_G(P, A) \longrightarrow \mathrm{Hom}_G(P, B)$. Si $0 \longrightarrow A \longrightarrow B \longrightarrow C \longrightarrow 0$ es una sucesión exacta de*

G-módulos izquierdos, los mapeos de conexión $\hat{H}^n(G,C) \xrightarrow{\delta} \hat{H}^{n+1}(G,A)$ *pueden ser calculados de la sucesión exacta de resoluciones*

$$0 \longrightarrow \mathrm{Hom}_G(P,A) \longrightarrow \mathrm{Hom}_G(P,B) \longrightarrow \mathrm{Hom}_G(P,C) \longrightarrow 0,$$

como en el Teorema 4.1.13. □

4.6. Resolución canónica

Para $q \geq 1$ consideremos las q-tuplas $(\sigma_1, \ldots, \sigma_q)$ con los σ_i recorriendo el grupo G. Una q-tupla de estas se llama una *q-celdas* con vértices $\sigma_1, \ldots, \sigma_q$. Las q-celdas dan generadores libres de nuestros G-módulos

$$P_q = P_{-q-1} = \bigoplus_{\substack{(\sigma_1,\ldots,\sigma_q)\in \\ \underbrace{G\times\cdots\times G}_{q}}} \mathbb{Z}[G](\sigma_1,\ldots,\sigma_q) \cong \mathbb{Z}[\overbrace{G\times\cdots\times G}^{q+1}].$$

Para $q = 0$, $P_0 = P_{-1} = \mathbb{Z}[G]$ con el $1 \in \mathbb{Z}[G]$ como el generador de la *celda nula o vacía* $(\cdot)$. Sea $\varepsilon\colon P_0 \longrightarrow \mathbb{Z}$, $\varepsilon\big(\sum_{\sigma\in G} a_\sigma \sigma\big) = \sum_{\sigma\in G} a_\sigma$ y $\mu\colon \mathbb{Z} \longrightarrow P_{-1}$, $\mu(n) = n\,\mathrm{N}_G = \sum_{\sigma\in G} n\sigma$ (llamado *coaumentación*).

Los mapeos d_q, están dados por:

$$d_0(1) = \mathrm{N}_G, \tag{4.6.3}$$

$$d_1(\sigma) = \sigma - 1, \tag{4.6.4}$$

$$\begin{aligned} d_q(\sigma_1,\ldots,\sigma_q) &= \sigma_1(\sigma_2,\ldots,\sigma_q) \\ &\quad + \sum_{i=1}^{q-1}(-1)^i(\sigma_1,\ldots,\sigma_{i-1},\sigma_i\sigma_{i+1},\sigma_{i+2},\ldots,\sigma_q) \\ &\quad + (-1)^q(\sigma_1,\ldots,\sigma_{q-1}) \quad \text{para } q>1, \end{aligned} \tag{4.6.5}$$

$$d_{-1}(1) = \sum_{\sigma\in G}(\sigma^{-1}(\sigma) - (\sigma)) \quad \text{para } q=-1, \tag{4.6.6}$$

$$\begin{aligned} d_{-q-1}(\sigma_1,\ldots,\sigma_q) &= \sum_{\sigma\in G}\sigma^{-1}(\sigma,\sigma_1,\ldots,\sigma_q) \\ &\quad + \sum_{\sigma\in G}\sum_{i=1}^{q}(-1)^i(\sigma_1,\ldots,\sigma_{i-1},\sigma_i\sigma,\sigma^{-1},\sigma_{i+1},\ldots,\sigma_q) \\ &\quad + \sum_{\sigma\in G}(-1)^{q+1}(\sigma_1,\ldots,\sigma_q,\sigma) \quad \text{para } q>0. \end{aligned} \tag{4.6.7}$$

Se puede verificar directamente que los mapeos d_q, $q \in \mathbb{Z}$ definidos en (4.6.3, 4.6.4, 4.6.5, 4.6.6, 4.6.7) hacen de la resolución completa una sucesión exacta. Sin embargo, más adelante indicaremos como obtenerlos.

Se tiene que $P_{-q-1} \cong \mathrm{Hom}(P_q, \mathbb{Z}) = \widehat{P}_q$, $q \geq 0$. Ahora, si A es un G-módulo izquierdo, sea $A_q = \mathrm{Hom}_G(P_q, A)$. Los elementos A_q, es decir, los G-homomorfismos $f\colon P_q \longrightarrow A$ se llaman las *q-cadenas* y f está determinado por los valores $\{f(\sigma_1, \ldots, \sigma_q)\}$, $\sigma_1, \ldots, \sigma_q \in G$.

De la sucesión exacta

$$\cdots \xleftarrow{d_{-2}} P_{-2} \xleftarrow{d_{-1}} P_{-1} \xleftarrow{d_0} P_0 \xleftarrow{d_1} P_1 \xleftarrow{d_2} P_2 \xleftarrow{d_3} \cdots$$

se obtiene la sucesión

$$\cdots \xrightarrow{\partial_{-2}} A_{-2} \xrightarrow{\partial_{-1}} A_{-1} \xrightarrow{\partial_0} A_0 \xrightarrow{\partial_1} A_1 \xrightarrow{\partial_2} A_2 \xrightarrow{\partial_3} \cdots$$

donde $\partial_q(f) = f \circ d_q$, $\partial_q\colon A_{q-1} \longrightarrow A_q$. Se tiene $\partial_{q+1} \circ \partial_q = 0$, por lo que $\operatorname{im} \partial_q \subseteq \operatorname{núc} \partial_{q+1}$. Se definen los *$q$-cociclos* Z_q y los *q-cofronteras* B_q por

$$Z_q := \operatorname{núc} \partial_{q+1}, \quad B_q := \operatorname{im} \partial_q, \quad q \in \mathbb{Z}.$$

Definición 4.6.1. Se define el *q-ésimo grupo de cohomología* (de Tate) por

$$H^q(G, A) = Z_q / B_q.$$

$H^q(G, A)$ es el grupo de cohomología de dimensión $q \in \mathbb{Z}$ del G-módulo A o el q-ésimo grupo de cohomología de G con coeficientes en A.

Se tiene que todo elemento de $H^q(G, A)$ es representado por un mapeo $f\colon \underbrace{G \times \cdots \times G}_{q} \longrightarrow A$. Además $A_0 = A_{-1} = \mathrm{Hom}_G(\mathbb{Z}[G], A) \cong A$.

De (4.6.3, 4.6.4, 4.6.5, 4.6.6, 4.6.7) obtenemos

$$\begin{aligned}
\partial_0(f) &= \mathrm{N}_G f, f \in A_{-1} = A,\\
(\partial_1 f)(\sigma) &= \sigma(f) - f, f \in A_0 = A,\\
(\partial_q f)(\sigma_1, \ldots, \sigma_q) &= \sigma_1 f(\sigma_2, \ldots, \sigma_q)\\
&\quad + \sum_{i=1}^{q-1} (-1)^i f(\sigma_1, \ldots, \sigma_{i-1}, \sigma_i\sigma_{i+1}, \sigma_{i+2}, \ldots, \sigma_q)\\
&\quad + (-1)^q f(\sigma_1, \ldots, \sigma_{q-1}) \quad \text{para } f \in A_{q-1}, q \geq 1,\\
(\partial_{-1} f) &= \sum_{\sigma \in G} (\sigma^{-1} f(\sigma) - f(\sigma)) \quad \text{para } f \in A_{-2}\\
(\partial_{-q-1} f)(\sigma_1, \ldots, \sigma_q) &= \sum_{\sigma \in G} \sigma^{-1} f(\sigma, \sigma_1, \ldots, \sigma_q)\\
&\quad + \sum_{\sigma \in G} \sum_{i=1}^{q} (-1)^i f(\sigma_1, \ldots, \sigma_{i-1}, \sigma_i\sigma, \sigma^{-1}, \sigma_{i+1}, \ldots, \sigma_q)\\
&\quad + \sum_{\sigma \in G} (-1)^{q+1} f(\sigma_1, \ldots, \sigma_q, \sigma) \quad \text{para } q \geq 0.
\end{aligned}$$

Así los q-cociclos son los mapeos $f\colon G\times\cdots\times G\longrightarrow A$ con $\partial_{q+1}f=0$ y las q-cofronteras son los mapeos para los cuales existe $g\in A_{q-1}$ con $f=\partial_q g$.

Ahora verificaremos las fórmulas (4.6.3, 4.6.4, 4.6.5, 4.6.6, 4.6.7), particularmente el caso de d_m con $m\leq 0$. Consideremos

$$P_{-q-1}=\bigoplus_{\substack{(\sigma_1,\ldots,\sigma_q)\in\\ G\times\cdots\times G}}\mathbb{Z}[G](\sigma_1,\ldots,\sigma_q).$$

Enumeremos el sistema de $\mathbb{Z}[G]$-generadores de P_q consistente de las q-celdas como $\{\Lambda_i\}$. Esto es, $\{\Lambda_i\}=\{(\sigma_1,\ldots,\sigma_q)\mid \sigma_j\in G, 1\leq j\leq q\}$. Definimos $\{\Lambda_i^*\}$ la base dual de $\{\Lambda_i\}$ por

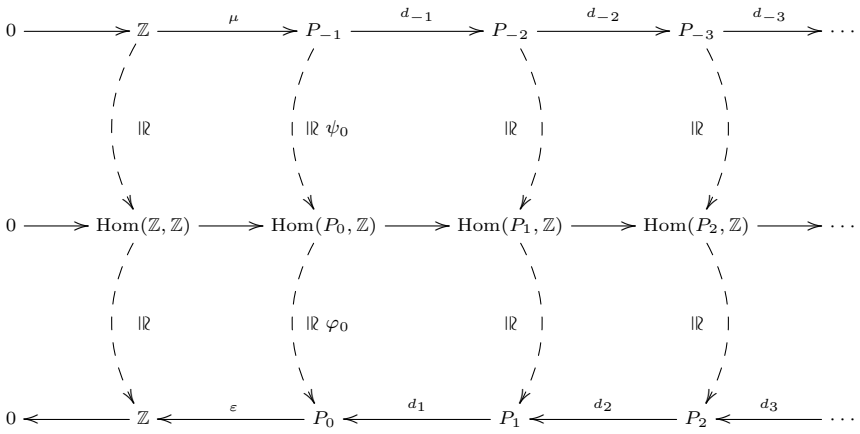
$$\Lambda_i^*(\sigma\Lambda_j)=\begin{cases}1 & \text{si } \sigma=1 \text{ y } i=j\\ 0 & \text{de otra forma.}\end{cases}$$

Se tiene $\Lambda_i^*\in\operatorname{Hom}(P_q,\mathbb{Z})$. Se tiene que $\{\Lambda_i^*\}$ es un sistema de generadores de $\operatorname{Hom}(P_q,\mathbb{Z})$. Esto hace que los G-módulos $\operatorname{Hom}(P_q,\mathbb{Z})$ y P_q sean canónicamente isomorfos. Ahora bien

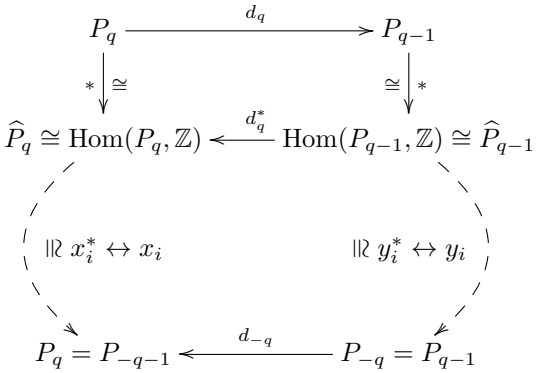
$$P_{-q-1}=P_q\underset{\substack{\uparrow\\ \Lambda_i\leftrightarrow\Lambda_i^*}}{\cong}\operatorname{Hom}(P_q,\mathbb{Z}),$$

$q\geq 0$ y $\mathbb{Z}\cong\operatorname{Hom}(\mathbb{Z},\mathbb{Z})$.

Se tiene



La situación es como sigue para $q\geq 1$:



Por tanto $d_q = d_q^*$ y $d_q^*(f) = f \circ d_q \in \mathrm{Hom}(P_q, \mathbb{Z})$ para $f \in \mathrm{Hom}(P_{q-1}, \mathbb{Z})$.

Sea $\{x_i\}$ el sistema de generadores libres de P_q como el $\mathbb{Z}[G]$-módulo dado por las q-celdas: $\{x_i\}_{i\in I} = \{(\sigma_1, \ldots, \sigma_q) \mid \sigma_i \in G\}$. Entonces el correspondiente sistema de generadores de P_q como $\mathbb{Z}$-módulo es $\{\sigma x_i\}_{\substack{\sigma\in G\\ i\in I}}$. Se tiene que $\{\sigma x_i\}_{\substack{\sigma\in G\\ i\in I}} = \{\sigma(\sigma_1, \ldots, \sigma_q) \mid \sigma, \sigma_i \in G\}$.

Sean $\{y_j\}_{i\in J}$ y $\{\sigma y_j\}_{\substack{\sigma\in G\\ j\in J}}$ las bases correspondientes de P_{q-1}.

Sean

$$d_q x_t = \sum_{\sigma\in G, s} a_{t,\sigma,s}\sigma y_s \quad \text{con } a_{t,\sigma,s} \in \mathbb{Z},$$
$$d_q^* y_l^* = \sum_{\tau\in G, u} b_{l,\tau,u}\tau x_u^* \quad \text{con } b_{l,\tau,u} \in \mathbb{Z}.$$

Se tiene

$$(d_q^* y_l^*)(\theta x_m) = \sum_{\tau,u} b_{l,\tau,u}(\tau x_u^*)(\theta x_m) = \sum_{\tau,u} b_{l,\tau,u}\tau(x^*(\tau^{-1}\theta(x_m))) = b_{l,\theta,m}.$$

Por otro lado

$$\begin{aligned}(d_q^* y_l^*)(\theta x_m) &= y_l^* d_q(\theta x_m) = y_l^*(\theta(d_q(x_m))) = y_l^*\big(\theta\big(\sum_{\sigma,s} a_{m,\sigma,s}\sigma y_s\big)\big)\\ &= y_l^*\big(\sum_{\sigma,s} a_{m,\sigma,s}(\theta\sigma)(y_s)\big) = \sum_{\sigma,s} a_{m,\sigma,s} y_l^*((\theta\sigma)(y_s)) = a_{m,\theta^{-1},l}.\end{aligned}$$

Por tanto se tiene

$$(d_q^* y_l^*)(\theta x_m) = b_{l,\theta,m} = a_{m,\theta^{-1},l}.$$

Poniendo $l\text{“} = \text{”}(\sigma_1, \ldots.\sigma_{q-1})$ y $m\text{“} = \text{”}(\sigma_1', \ldots, \sigma_q')$, se tiene

$$b_{(\sigma_1,\ldots,\sigma_{q-1}),\theta,(\sigma_1',\ldots,\sigma_q')} = a_{(\sigma_1',\ldots,\sigma_q'),\theta^{-1},(\sigma_1,\ldots,\sigma_{q-1})}.$$

Ahora bien, de acuerdo a la ecuación (4.6.5), los coeficientes no cero para las $(q+1)$-celdas son

$$a_{(\mu_1,\ldots,\mu_{q+1}),\mu_1,(\mu_2,\ldots,\mu_{q+1})} = 1, \tag{4.6.8}$$

$$a_{(\mu_1,\ldots,\mu_{q+1}),1,(\mu_1,\ldots,\mu_{i-1},\mu_i\mu_{i+1},\mu_{i+2},\ldots,\mu_{q+1})} = (-1)^i, \quad 1 \leq i \leq q, \tag{4.6.9}$$

$$a_{(\mu_1,\ldots,\mu_{q+1}),1,(\mu_1,\ldots,\mu_q)} = (-1)^{q+1}. \tag{4.6.10}$$

Para (4.6.8), poniendo $(\sigma_1,\ldots,\sigma_q) = (\mu_2,\ldots,\mu_{q+1})$ y $\mu_1 = \tau^{-1}$, se tiene que los $b's$ correspondientes son $\{b_{(\sigma_1,\ldots,\sigma_q),\tau^{-1},(\tau,\sigma_1,\ldots,\sigma_q)}, \tau \in G\}$. Para (4.6.9) ponemos $\theta = 1$ y $(\sigma_1,\ldots,\sigma_q) = (\mu_1,\ldots,\mu_{i-1},\mu_i\mu_{i+1},\mu_{i+2},\ldots,\mu_{q+1})$, se obtiene que los $b's$ son

$$\{b_{(\sigma_1,\ldots,\sigma_q),1,(\sigma_1,\ldots,\sigma_{i-1},\sigma_i\tau,\tau^{-1},\sigma_{i+1},\ldots,\sigma_q)}, \tau \in G\}.$$

Para (4.6.10) se obtiene que los $b's$ correspondientes son

$$\{b_{(\sigma_1,\ldots,\sigma_q),1,(\sigma_1,\ldots,\sigma_q,\tau)}, \tau \in G\}.$$

De esto, se obtiene (4.6.7). Las otras fórmulas se obtienen de manera similar.

4.6.1. Cambio de dimensión

Sean I_G el ideal aumentación y $J_G = \mathbb{Z}[G]/\mathbb{Z}\,\mathrm{N}_G$. Se tienen las sucesiones exactas

$$0 \longrightarrow I_G \longrightarrow \mathbb{Z}[G] \xrightarrow{\varepsilon} \mathbb{Z} \longrightarrow 0,$$
$$0 \longrightarrow \mathbb{Z} \xrightarrow{\Lambda} \mathbb{Z}[G] \longrightarrow J_G \longrightarrow 0.$$

Puesto que $\mathbb{Z}, \mathbb{Z}[G], I_G$ y J_G son todos $\mathbb{Z}$-módulos libres, para un G-módulo A, se tienen las siguientes sucesiones G-exactas (Proposición 4.1.7):

$$\begin{array}{l} 0 \longrightarrow I_G \otimes A \longrightarrow \mathbb{Z}[G] \otimes A \longrightarrow \quad A \quad \longrightarrow 0, \\ 0 \longrightarrow \quad A \quad \longrightarrow \mathbb{Z}[G] \otimes A \longrightarrow J_G \otimes A \longrightarrow 0, \end{array} \tag{4.6.11}$$

puesto que $A \cong \mathbb{Z} \otimes A$.

Como $\mathbb{Z}[G]$ es un G-módulo inducido, $\mathbb{Z}[G]$ es cohomológicamente trivial y por el Teorema 4.3.8 se tienen isomorfismos

$$\mu\colon H^{q-1}(H, J_G \otimes A) \xrightarrow{\cong} H^q(H, A),$$
$$\mu^{-1}\colon H^{q+1}(H, I_G \otimes A) \xrightarrow{\cong} H^q(H, A),$$

para todo $q \in \mathbb{Z}$ y para todo subgrupo $H < G$, donde μ y μ^{-1} son los mapeos de conexión.

Continuamos el proceso, y para cualquier $m \in \mathbb{Z}$ definimos

$$A^m := \overbrace{J_G \otimes \cdots \otimes J_G}^{m} \otimes A \quad \text{para } m \geq 0,$$
$$A^m := \underbrace{I_G \otimes \cdots \otimes I_G}_{-m} \otimes A \quad \text{para } m \leq 0.$$

Se tienen isomorfismos

$$H^{q-m}(H, A^m) \xrightarrow[\mu,\mu^{-1}]{\cong} H^{q-(m-1)}(H, A)^{m-1} \xrightarrow[\mu,\mu^{-1}]{\cong} \cdots \xrightarrow[\mu,\mu^{-1}]{\cong} H^q(H, A),$$

esto es,

$$\mu^m \colon H^{q-m}(H, A^m) \xrightarrow{\cong} H^q(H, A), \quad m \in \mathbb{Z}. \tag{4.6.12}$$

Se usa el isomorfismo (4.6.12) para deducir propiedades de grupos de cohomología de dimensión q a propiedades análogas para cohomología en dimensiones superiores o inferiores. En particular, esta técnica nos permitirá reducir muchas definiciones y demostraciones al caso 0-dimensional que es más fácil de trabajar. Este método se llama *cambio de dimensión*. Se tiene que

$$H^q(G, A) \cong H^0(G, A^q) = (A^q)^G / \operatorname{N}_G A^q.$$

El siguiente resultado, es un ejemplo de como usar el cambio de dimensión.

Teorema 4.6.2. *Sea G un grupo finito de n elementos. Sea A un G-módulo. Entonces $nH^q(H, A) = 0$ para toda $q \in \mathbb{Z}$.*

Demostración. Si $q = 0$, $H^0(G, A) = A^G / \operatorname{N}_G A$, y si $a \in A^G$, $na = \sum_{\sigma \in G} \sigma a \in \operatorname{N}_G A$. Por tanto $nH^0(G, A) = 0$. Se sigue que $nH^q(G, A) = nH^0(G, A^q) = 0$ para toda $q \in \mathbb{Z}$. □

Definición 4.6.3. Si X es un grupo abeliano, X se llama *unívocamente o únicamente divisible* si para toda $n \in \mathbb{N}$ y para toda $a \in X$, la ecuación $nx = a$ tiene una única solución $x \in X$ (formalmente $x = \frac{a}{n}$). Se tiene que X es unívocamente divisible si para toda $n \in \mathbb{N}$ el mapeo $X \longrightarrow X$, $x \longmapsto nx$ es un isomorfismo de grupos,

Ejemplo 4.6.4. El campo de los números racionales $\mathbb{Q}$ es unívocamente divisible. Más generalmente, cualquier campo de característica 0 es unívocamente divisible.

Corolario 4.6.5. *Si A es un G-módulo que es unívocamente divisible, entonces A es cohomológicamente trivial.*

Demostración. Se tiene que $n \operatorname{Id} : A \longrightarrow A$, $a \longmapsto na$ es una biyección para toda $n \in \mathbb{Z}$. Por tanto, si $n = |H|$, $H^q(H, A) = nH^q(H, A) = 0$ para todo $q \in \mathbb{Z}$ y para todo subgrupo $H < G$. □

Aplicando el Corolario 4.6.5 a $\mathbb{Q}$ y a la sucesión exacta de G-módulos triviales $0 \longrightarrow \mathbb{Z} \longrightarrow \mathbb{Q} \longrightarrow \mathbb{Q}/\mathbb{Z} \longrightarrow 0$, obtenemos que $H^q(G, \mathbb{Q}/\mathbb{Z}) \cong H^{q+1}(G, \mathbb{Z})$ para toda $q \in \mathbb{Z}$.

En particular, $H^2(G, \mathbb{Z}) \cong H^1(G, \mathbb{Q}/\mathbb{Z}) \cong \mathrm{Hom}(G, \mathbb{Q}/\mathbb{Z}) \cong \widehat{G} \cong G/G' = G^{\mathrm{ab}}$, donde $\chi(G) = \widehat{G} = \mathrm{Hom}(G, \mathbb{Q}/\mathbb{Z})$ es el *grupo de caracteres* de G.

Por otro lado de la sucesión $0 \longrightarrow I_G \longrightarrow \mathbb{Z}[G] \longrightarrow \mathbb{Z} \longrightarrow 0$, obtenemos $H^{-2}(G, \mathbb{Z}) \cong H^{-1}(G, I_G) \cong I_G/I_G^2 \cong G/G' = G^{\mathrm{ab}}$. Este último isomorfismo está dado por:

$$(\sigma - 1) + I_G^2 \longrightarrow \sigma G' \quad para\ \sigma \in G.$$

En particular $H^{-2}(G, \mathbb{Z}) \cong G^{\mathrm{ab}} \cong H^2(G, \mathbb{Z})$.

Como hicimos notar antes $H^1(G, \mathbb{Z}) = \mathrm{Hom}(G, \mathbb{Z}) = 0$ y $H^{-1}(G, \mathbb{Z}) = \frac{\text{núc}\, \mathrm{N}_G}{I_G \mathbb{Z}} = 0$. Finalmente $H^0(G, \mathbb{Z}) = \mathbb{Z}/n\mathbb{Z} = C_n$, donde $|G| = n$.

De hecho tenemos

$$H^{-q}(G, \mathbb{Z}) \cong \chi\big(H^q(G, \mathbb{Z})\big) = \mathrm{Hom}(H^q(G, \mathbb{Z}), \mathbb{Q}/\mathbb{Z}), \quad \text{para } q > 0,$$

ver [169, Corollary 4-4-7].

4.7. Cambio de grupo

Sea $\varphi\colon G' \longrightarrow G$ un homomorfismo de grupos finitos (aquí G' denota a un grupo finito arbitrario y no al conmutador de G). Si A es un G-módulo, A puede hacerse un G'-módulo de la siguiente forma. Para $\tau' \in G'$ y para $a \in A$, se define $\tau' \circ a := \varphi(\tau') \circ a$. En caso de ser necesario, el G'-módulo A se denotará por $\varphi^* A$.

Si A y B son dos G-módulos y $f\colon A \longrightarrow B$ es un G-homomorfismo, entonces f también es un G'-homomorfismo $f\colon \varphi^* A \longrightarrow \varphi^* B$,

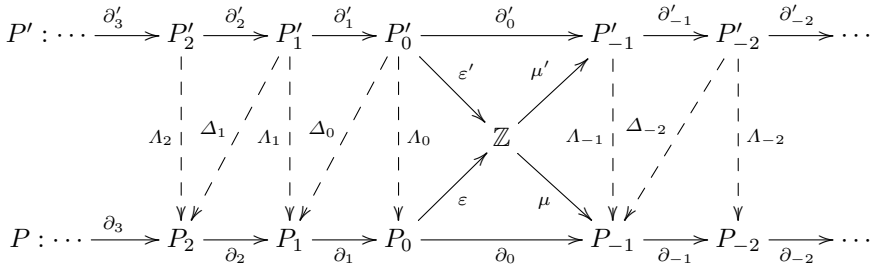
$$f(\tau' a) = f(\varphi(\tau')a) = \varphi(\tau') f(a) = \tau' f(a).$$

Más generalmente, si $\varphi\colon G' \longrightarrow G$ es un homomorfismo de grupos, si A' es un G'-módulo y si $g\colon A \longrightarrow A'$ es un mapeo aditivo, esto es, g es un homomorfismo de grupos abelianos o g es un $\mathbb{Z}$-homomorfismo, entonces φ y g se llaman *compatibles* si

$$g(\varphi(\tau')a) = \tau' g(a) \quad \text{para toda } \tau' \in G'.$$

En otras palabras, si g es un G'-homomorfismo entre $\varphi^* A$ y A'.

Consideremos cualesquiera dos complejos P' y P, esto es, resoluciones completas para G' y para G. Podemos suponer que tanto P' como P son las resoluciones canónicas. Entonces P' y P son resoluciones proyectivas, de hecho libres.



Se tiene que $\partial', \varepsilon', \mu'$ son G'-homomorfismos; $\partial, \varepsilon, \mu$ son G-homomorfismos y por tanto, cuando los módulos P_n son vistos como G'-módulos, $\partial, \varepsilon, \mu$ son también G'-homomorfismos.

Teorema 4.7.1. *Para cualquier homomorfismo $\varphi\colon G' \longrightarrow G$ existen G'-homomorfismos $\Lambda_n\colon P'_n \longrightarrow P_n$, para $n \geq 0$ tales que $\varepsilon \circ \Lambda_0 = \varepsilon'$ y $\partial_{n+1} \circ \Lambda_{n+1} = \Lambda_n \circ \partial'_{n+1}$.*

Demostración. Se tiene que P'_0 es G'-libre y ε es suprayectiva, por lo que existe un G'-homomorfismo $\Lambda_0\colon P'_0 \longrightarrow P_0$ tal que $\varepsilon \circ \Lambda_0 = \varepsilon'$, de hecho, si $\{\xi_i\}$ es G'-base de X'_0 y $\varepsilon'(\xi_i) = n_i \in \mathbb{Z}$, como ε es sobre, existe $\delta_i \in P_0$ con $\varepsilon(\delta_i) = n_i$. Se define $\Lambda_0(\xi_i) := \delta_i$.

Se tiene $\partial_0\Lambda_0\partial'_1 = \mu\varepsilon\Lambda_0\partial'_1 = \mu\varepsilon'\partial'_1 = 0$.

Supongamos que Λ_n ha sido definido para $n \geq 0$ y que $\partial_n\Lambda_n\partial'_{n+1} = 0$. Puesto que P'_{n+1} es G'-libre, P_{n+1} es G'-inducido. Sea $P_{n+1} = \sum_{\sigma\in G'} \sigma X$ y sea $\pi\colon P'_{n+1} \longrightarrow X$ la proyección, esto es, si $a \in P'_{n+1}$, $a = \sum_{\sigma'\in G'} \sigma' b_{\sigma'}$ con $b_{\sigma'} \in X$, entonces $\pi(a) = b_1$. Para $\tau \in G'$, se tiene

$$\begin{aligned}(\tau' \circ \pi)(a) = \tau'\pi((\tau')^{-1}a) &= \tau'\pi\Big(\sum_{\sigma'\in G'} (\tau')^{-1}\sigma' b_{\sigma'}\Big)\\ &= \tau'\pi\Big(\sum_{\theta'\in G'} \theta' b_{\tau'\theta'}\Big) = \tau' b_{\tau'}.\end{aligned}$$

Esto es, $\tau' \circ \pi$ es la proyección de P'_{n+1} en $\tau' X$. Por tanto

$$(\sigma' \circ \pi) \circ (\theta' \circ \pi)(a) = (\sigma' \circ \pi)(\theta' b_{\theta'}) = \begin{cases} 0 & \text{si } \sigma' \neq \theta' \\ \theta' b_{\theta'} & \text{si } \sigma' = \theta' \end{cases} = \delta_{\sigma',\theta'}(\theta' \circ \pi)(a).$$

Se sigue que

$$(\sigma' \circ \pi) \circ (\theta' \circ \pi) = \delta_{\sigma',\theta'}(\theta' \circ \pi).$$

Por otro lado, se tiene que $\mathrm{Id}_{P'_{n+1}}(a) = a = \sum_{\sigma'\in G} \sigma' b_{\sigma'} = \sum_{\sigma'\in G'}(\sigma' \circ \pi)(a)$. Por tanto

$$\mathrm{Id}_{P'_{n+1}} = \sum_{\sigma'\in G'} \sigma' \circ \pi.$$

De esta forma, existe $\pi'_{n+1}(=\pi) \in \mathrm{Hom}(P'_{n+1}, P'_{n+1})$ con $\mathrm{Id}_{P'_{n+1}} = \sum_{\sigma' \in G'} \sigma' \circ \pi'_{n+1}$. Sea $\Lambda_{n+1} := \sum_{\sigma' \in G'} \sigma'(D_n \Lambda_n \partial'_{n+1} \pi'_{n+1})$ donde $D_n \colon P_n \longrightarrow P_{n+1}$ satisface $D_{n-1} \circ \partial_n + \partial_{n+1} \circ D_n = \mathrm{Id}_{P_n}$ (Proposición 4.5.1).

$$\begin{array}{ccccc} P'_{n+1} & \xrightarrow{\pi'_{n+1}} & P'_{n+1} & \xrightarrow{\partial'_{n+1}} & P'_n \\ & \searrow^{\Lambda_{n+1}} & & & \downarrow{\scriptstyle \Lambda_n} \\ & & P_{n+1} & \xleftarrow[D_n]{} & P_n \end{array}$$

Entonces Λ_{n+1} es un G'-homomorfismo y se tiene

$$\begin{aligned} \partial_{n+1}\Lambda_{n+1} &= \sum_{\sigma' \in G'} \partial_{n+1}(\sigma'(D_n \Lambda_n \partial'_{n+1} \pi'_{n+1})) \\ &= \sum_{\sigma' \in G'} (\sigma'(\partial_{n+1} D_n \Lambda_n \partial'_{n+1} \pi'_{n+1})) \\ &\underset{\substack{\partial_{n+1} D_n = \\ 1 - D_{n-1}\partial_n}}{=} \sum_{\sigma' \in G'} \sigma'(\Lambda_n \partial'_{n+1} \pi'_{n+1}) - \sum_{\sigma' \in G'} \sigma'(D_{n-1} \underbrace{\partial_n \Lambda_n \partial'_{n+1}}_{0} \pi'_{n+1}) \\ &= \Lambda_n \partial'_{n+1} \sum_{\sigma' \in G'} \sigma' \pi'_{n+1} - 0 = \Lambda_n \partial'_{n+1} \mathrm{Id}_{P'_{n+1}} = \Lambda_n \partial'_{n+1}. \end{aligned}$$

Esto es, $\partial_{n+1}\Lambda_{n+1} = \Lambda_n \partial'_{n+1}$. Finalmente

$$\partial_{n+1}\Lambda_{n+1}\partial'_{n+2} = \Lambda_n \partial'_{n+1}\partial'_{n+2} = 0. \qquad \square$$

Observación 4.7.2. El proceso del Teorema 4.7.1 no puede ser continuado como está en general para $n < 0$. Sin embargo, cuando $\varphi \colon G' \longrightarrow G$ es un monomorfismo, el proceso puede ser continuado para $n < 0$.

Teorema 4.7.3. *Si $\varphi \colon G' \longrightarrow G$ es un monomorfismo de grupos, entonces existen G' homomorfismos $\Lambda_n \colon P'_n \longrightarrow P_n$ tales que $\varepsilon \circ \Lambda_0 = \varepsilon'$ y $\partial_{n+1} \circ \Lambda_{n+1} = \Lambda_n \circ \partial'_{n+1}$ para toda $n \in \mathbb{Z}$.*

Demostración. Se tiene Λ_0 tal que $\varepsilon \circ \Lambda_0 = \varepsilon'$ y $\partial_0 \Lambda_0 \partial'_1 = 0$. Supongamos inductivamente que para $n \leq 0$ se tiene Λ_n con $\partial_n \Lambda_n \partial'_{n+1} = 0$. Ahora G' se puede considerar como un subgrupo de G, por lo que P_n es G'-libre y en particular es G'-inducido. Por el argumento del Teorema 4.7.1, existe $\pi_n \in \mathrm{Hom}(P_n, P_n)$ tal que $S'(\pi_n) := \sum_{\sigma \in G} \sigma \pi_n = \mathrm{Id}_{P_n}$.

Sea $\Lambda_{n-1} := S'(\pi_{n-1} \partial_n \Lambda_n D'_{n-1}) = \sum_{\sigma \in G} \sigma(\pi_{n-1} \partial_n \Lambda_n D'_{n-1})$, donde $D'_{n+1} \colon P'_n \longrightarrow P'_{n+1}$ satisface $D'_{n-1} \circ \partial'_n + \partial'_{n+1} \circ D'_n = \mathrm{Id}_{P'_n}$. Entonces $\partial_n \circ \Lambda_n = \Lambda_{n-1} \circ \partial'_n$ y $\partial_{n-1} \Lambda_{n-1} \partial'_n = 0$. Además $\mu = \Lambda_{-1} \circ \mu'$. $\square$

Teorema 4.7.4. *Sea $\varphi \colon G' \longrightarrow G$ un homomorfismo de grupos finitos. Sean A y A', un G-módulo y un G'-módulo respectivamente, y sea $g \colon A \longrightarrow A'$*

compatible con φ, es decir, $g(\varphi(\tau')a) = \tau' g(a)$ para toda $\tau' \in G'$ y para toda $a \in A$.

Existe una única familia de homomorfismos de grupos

$$(\varphi, g)_n \colon H^n(G, A) \longrightarrow H^n(G', A'),$$

para $n \geq 0$ (y para $n \in \mathbb{Z}$ si φ es inyectiva) que satisface:

(1) $(1,1)_n = \mathrm{Id}_n$ *para* n.
(2) *Si* $\varphi' \colon G'' \longrightarrow G'$ *es un homomorfismo de grupos finitos,* A'' *es un* G''*-módulo y si* $g' \colon A' \longrightarrow A''$ *es compatible con* φ'*, esto es,* $g'(\varphi'(\tau'')a') = \tau'' g'(a')$ *para toda* $\tau'' \in G''$, $a' \in A'$, *entonces* $(\varphi \circ \varphi', g' \circ g)_n = (\varphi', g')_n \circ (\varphi, f)_n$ *para toda* $n \geq 0$ *(a veces* $n \in \mathbb{Z}$*).*
(3) *Si* $g_1 \colon A \longrightarrow A'$ *es compatible con* φ*, entonces* $(\varphi, g + g_1)_n = (\varphi, g)_n + (\varphi, g_1)_n$.

Demostración. Sea $\Lambda \colon P' \longrightarrow P$ un G'-homomorfismo conmutando con fronteras:

$$\begin{array}{ccc} P'_{n+1} & \xrightarrow{\partial'_{n+1}} & P'_n \\ {\scriptstyle \Lambda_{n+1}}\downarrow & & \downarrow{\scriptstyle \Lambda_n} \\ P_{n+1} & \xrightarrow[\partial_{n+1}]{} & P_n \end{array}$$

$$\partial_{n+1} \circ \Lambda_{n+1} = \Lambda_n \circ \partial'_{n+1}$$

$$\begin{array}{ccc} \mathrm{Hom}_G(P'_n, A') & \xrightarrow{(\partial'_{n+1})^*} & \mathrm{Hom}_G(P'_{n+1}, A') \\ {\scriptstyle (\varphi,g)_n}\downarrow{\scriptstyle \mu_n} & & \downarrow{\scriptstyle \mu_{n+1}} \\ \mathrm{Hom}_G(P_n, A) & \xrightarrow[\partial^*_{n+1}]{} & \mathrm{Hom}_G(P_{n+1}, A) \end{array}$$

Si $\psi \in \mathrm{Hom}_G(P'_n, A')$,

$$\begin{array}{ccc} P'_n & \xrightarrow{\psi} & A' \\ {\scriptstyle \partial'_{n+1}}\uparrow & \nearrow_{\partial^*_{n+1}(\psi)=\psi\circ\partial'_{n+1}} & \\ P_{n+1} & & \end{array} \qquad \begin{array}{ccc} P'_n & \xrightarrow{(\varphi,g)_n(\xi)} & A' \\ {\scriptstyle \Lambda_n}\downarrow & & \uparrow{\scriptstyle g} \\ P_n & \xrightarrow[\xi]{} & A \end{array}$$

Sea $\xi \in \mathrm{Hom}_G(P_n, A)$, $(\varphi, g)_n(\xi) = g \circ \xi \circ \Lambda_n$, $\partial^*_{n+1}(\xi) = \xi \circ \partial_{n+1}$.
Se tiene $\xi \in \mathrm{núc}\, \partial^*_{n+1}$ por lo que $\xi \circ \partial_{n+1} = 0$. Se sigue que

$$\begin{aligned} (\partial'_{n+1})^*((\varphi, g)_n(\xi)) &= (\varphi, g)_n(\xi) \circ \partial'_{n+1} = g \circ \xi \circ \Lambda_n \circ \partial'_{n+1} \\ &= g \circ \underbrace{\xi \circ \partial_{n+1}}_{\| \; 0} \circ \Lambda_{n+1} = 0 \end{aligned}$$

Por tanto $(\varphi, g)_n(\xi) \in \text{núc}\, \partial^*_{n+1}$.

Ahora si $\xi \in \text{im}\, \partial^*_n$, $\xi = \partial^*_n(\nu)$ con $\nu \in \text{Hom}_G(P_{n-1}, A)$ y

$$\begin{aligned}(\varphi, g)_n(\xi) &= g \circ \xi \circ \Lambda_n = g \circ (\partial^*_n(\nu)) \circ \Lambda_n = g \circ \nu \circ \partial_n \circ \Lambda_n \\ &= g \circ \nu \circ \Lambda_{n-1} \circ \partial'_n = (\partial'_n)^*(g \circ \nu \circ \Lambda_{n-1}) \in \text{im}(\partial'_n)^*.\end{aligned}$$

Para la unicidad, sean $\Lambda, \Lambda' \colon P' \longrightarrow P$ dos G'-homomorfismos que conmutan con fronteras. Sea $\Phi := \Lambda - \Lambda'$. Se construirán G'-homomorfismos $\Lambda_n \colon P'_n \longrightarrow P_{n+1}$ tales que

$$\Phi_n = \partial_{n+1}\Delta_n + \Delta_{n-1}\partial'_n. \tag{4.7.13}$$

Sean, en cualquier caso, $n \geq 0$ o $n \in \mathbb{Z}$

$$\Lambda_0 = S'(D_0\Phi_0\pi'_0) = \sum_{\tau' \in G'} \tau' D_0 \Phi_0 \pi'_0 \quad \text{y} \quad \Lambda_{-1} = 0.$$

Entonces

$$\begin{aligned}\partial_1\Lambda_0 &= S'(\underbrace{\partial_1 D_0}_{\substack{\| \\ 1 - D_{-1}\partial_0}} \Phi_0\pi'_0) = S'(\Phi_0\pi'_0) - S'(D_{-1}\partial_0\Phi_0\pi'_0) \\ &= \Phi_0 \underbrace{S'(\pi'_0)}_{\substack{\| \\ 1}} - S'(D_{-1}\mu \underbrace{\varepsilon\Phi_0}_{\substack{\| \\ 0}} \pi'_0) = \Phi_0,\end{aligned}$$

por lo que (4.7.13) es válido para $n = 0$.

Para $n > 0$, procedemos por inducción. Supongamos (4.7.13) cierta n y sea

$$\Delta_{n+1} := S'(D_{n+1}(\Phi_{n+1} - \Delta_n\partial'_{n+1})\pi'_{n+1}), \quad n > 0.$$

Ahora

$$\begin{aligned}\partial_{n+1}(\Phi_{n+1} - \Delta_n\partial'_{n+1}) &= \partial_{n+1}\Phi_{n+1} - \partial_{n+1}\Delta_n\partial'_{n+1} \\ &= \Phi_n\partial'_{n+1} - \partial_{n+1}\Delta_n\partial'_{n+1} \qquad = \\ &\qquad\qquad\qquad\qquad\qquad\qquad \uparrow_{\text{(4.7.13) para } n} \\ &= \partial_{n+1}\Delta_n\partial'_{n+1} + \Delta_{n-1}\underbrace{\partial'_n\partial'_{n+1}}_{0} - \partial_{n+1}\Delta_n\partial'_{n+1} = 0.\end{aligned}$$

Se sigue que

$$\begin{aligned}
\partial_{n+2}\Delta_{n+1} &= S'(\partial_{n+2}D_{n+1}(\Phi_{n+1}-\Delta_n\partial'_{n+1})\pi'_{n+1}) \\
&= \underset{\substack{\uparrow \\ \partial_{n+2}D_{n+1}= \\ 1-D_n\partial_{n+1}}}{} S'((\Phi_{n+1}-\Delta_n\partial'_{n+1})\pi'_{n+1}) \\
&\qquad - S'(D_n \underbrace{\partial_{n+1}(\Phi_{n+1}-\Delta_n\partial'_{n+1})}_{\substack{\| \\ 0}}\pi'_{n+1}) \\
&= S'(\Phi_{n+1}\pi'_{n+1}) - S'((\Delta_n\partial'_{n+1})\pi'_n) \\
&= \Phi_{n+1}S'(\pi'_{n+1}) - \Delta_n\partial'_{n+1}S'(\pi'_n) \\
&= \Phi_{n+1}\cdot 1 - \Delta_n\partial'_{n+1}\cdot 1 = \Phi_{n+1}-\Delta_n\partial'_{n+1}.
\end{aligned}$$

Se sigue que (4.7.13) se cumple para $n+1$.

Por tanto, si $\xi \in \text{núc}\,\partial'_n$, entonces se tiene $\Lambda_n(\xi) - \Lambda'_n(\xi) = \Phi_n(\xi) = \partial_{n+1}\Delta_n(\xi) + \Delta_{n-1}\partial'_n(\xi) = \partial_{n+1}\Delta_n(\xi) \in \text{im}\,\partial_{n+1}$, de donde, $\Lambda_n(\xi) \equiv \Lambda_n(\xi)$ mód $(\text{im}\,\partial_{n+1})$ y por lo tanto $(\varphi, g)_n$ no depende de Λ.

(1), (2) y (3) se verifican directamente. □

Observación 4.7.5. Todo el desarrollo anterior, es con respecto a la cohomología de Tate. Ahora, para H^0 no de Tate, esto es, $H^0(G,A) = A^G$, también se satisface

$$(\varphi, g)_0 \colon H^0(G,A) = A^G \longrightarrow H^0(G',A') = (A')^{G'} :$$

Se tiene para $\tau' \in G'$, $a \in A$, $\tau' g(a) = g(\varphi(\tau')) = g(a)$, por lo tanto $(\varphi, g)_0(A^G) \subseteq (A')^{G'}$.

Ejemplo 4.7.6 (Restricción). Sean G un grupo finito y $H < G$ un subgrupo. Entonces, si $\varphi = i \colon H \longrightarrow G$ es la inyección natural, para A un G-módulo, A es un H-módulo con la misma acción. Entonces

$$(i, \text{Id}_A)_n := \text{res}_n \colon H^n(G,A) \longrightarrow H^n(H,A),$$

se llama *restricción* y como i es inyectiva, el mapeo res_n es válido para toda $n \in \mathbb{Z}$.

A nivel de cadenas $P_H : P_{H,n} = \mathbb{Z}[H^{n+1}]$, $n \geq 0$ y $P_G : P_{G,n} = \mathbb{Z}[G^{n+1}]$, dada una q-cadena de G: $(q \geq 0)$,

$$x \colon \underbrace{G \times G \times \cdots \times G}_{q} \longrightarrow A,$$

$$\text{res}\, x = y \colon \underbrace{H \times H \times \cdots \times H}_{q} \longrightarrow A, \quad y = x|_{H\times\cdots\times H}.$$

También se tiene:

Proposición 4.7.7. *Sean A y B dos G-módulos y $H < G$ un subgrupo de G, G un grupo finito. Sea $f\colon A \longrightarrow B$ un G-homomorfismo. Entonces el diagrama*

$$\begin{array}{ccc} H^q(G,A) & \xrightarrow{H^q(f)} & H^q(G,B) \\ \Big\downarrow{\scriptstyle \mathrm{res}_q} & & \Big\downarrow{\scriptstyle \mathrm{res}_q} \\ H^q(H,A) & \xrightarrow[H^q(f)]{} & H^q(H,B) \end{array}$$

es conmutativo. Notemos que un G-homomorfismo $f\colon A \longrightarrow B$, es también un H-homomorfismo $f\colon A \longrightarrow B$. □

En bajas dimensión, tenemos para $q = 0$, no de Tate, $\mathrm{res}_0\colon H \to G$, $h \mapsto h$, $H^0(G,A) \xrightarrow{\mathrm{res}} H^0(H,A)$, $\mathrm{res}\colon A^G \longrightarrow A^H$, $a \mapsto a$ pues $a \in A^G$ implica $a \in A^H$.

Ahora, para $q = 1$, $\mathrm{res}\colon H^1(G,A) \longrightarrow H^1(H,A)$ está dada de la siguiente forma. Si $f \in Z^1(G,A)$, $f\colon G \longrightarrow A$, $f(\sigma\tau) = \sigma f(\tau) + f(\sigma)$ para todas $\sigma, \tau \in G$. La restricción $f|_H$ satisface la misma relación pero para $\sigma, \tau \in H$. Si $f \in B^1(G,A)$, existe $a \in A$ tal que $f(\sigma) = \sigma a - a$ para toda $\sigma \in G$, en particular, para toda $\sigma \in H$.

Ejemplo 4.7.8 (Inflación). Sea $\varphi = \pi\colon G \longrightarrow G/H$ donde $H \triangleleft G$ (aquí G corresponde a G' de la definición general y G/H corresponde a G). Si A es un G-módulo, A^H es un G/H-módulo. Sea $i : A^H \longrightarrow A$ la inyección natural. A las funciones

$$(\pi, i)_n\colon H^n(G/H, A^H) \longrightarrow H^n(G,A), \quad n \geq 0,$$

se les llama *inflación*. Ahora bien, como π no es monomorfismo, inflación sólo está definida para $n \geq 0$.

A nivel de q-cadenas, inflación se define de la siguiente forma. Sean $q \geq 1$ y $H \triangleleft G$ un subgrupo normal de G. Sea $\sigma\colon \underbrace{G/H \times \cdots \times G/H}_{q} \longrightarrow A^H$ una q-cadena. Se define $\tau\colon \underbrace{G \times \cdots \times G}_{q} \longrightarrow A$ por

$$\tau(g_1, \ldots, g_q) = \sigma(g_1 H, \ldots, g_q H).$$

El mapeo τ es la inflación de σ: $\tau = \inf \sigma$. Se tiene $\partial_{q+1} \circ \inf = \inf \circ \partial_{q+1}$ y por tanto se obtiene el mapeo en cohomología inflación.

Para ver la inflación en bajas dimensiones, procedemos así. Sea $\pi\colon G \longrightarrow G/H$ la proyección natural. Ahora $(A^H)^{G/H} \subseteq A^G$. Por tanto

$$H^0(G/H, A^H) \xrightarrow{\inf} H^0(G,A) = A^G$$

es la inyección natural, en el caso de $q = 0$, tanto de Tate como no de Tate.

Para $q = 1$, si $f \in H^1(G/H, A^H)$, tomando un representante $f \in Z^1(G/H, A^H)$, $f\colon G/H \longrightarrow A^H$ satisface $f(\bar{\sigma}\bar{\tau}) = \bar{\sigma}f(\bar{\tau}) + f(\bar{\sigma})$ para todas $\bar{\sigma}, \bar{\tau} \in G/H$. Entonces $\inf f = \tilde{f}$ satisface $\tilde{f}\colon G \longrightarrow A$, $\tilde{f}(g) := f(gH) = f(\bar{g}) \in A^H \subseteq A$. Se tiene $\tilde{f}(gk) = f(gkH) = f(gHkH) = gH \cdot f(kH) + f(gH)$ el cual está bien definido pues $f(kH) \in A^H$.

Independientemente del criterio general, se puede ver que restricción se podría definir por cambio de dimensión usando si $0 \longrightarrow A \longrightarrow B \longrightarrow C \longrightarrow 0$ es una sucesión exacta de G-módulos, entonces con el mapeo de conexión δ, tenemos el diagrama conmutativo

$$\begin{array}{ccc} H^q(G, C) & \xrightarrow{\delta} & H^{q+1}(G, A) \\ \Big\downarrow{\scriptstyle \mathrm{res}_q} & & \Big\downarrow{\scriptstyle \mathrm{res}_{q+1}} \\ H^q(H, C) & \xrightarrow[\delta]{} & H^{q+1}(H, A) \end{array}$$

para toda $q \in \mathbb{Z}$. Sea $\mu^q\colon H^0(G, A^q) \xrightarrow{\cong} H^q(G, A)$, se tiene el diagrama conmutativo

$$\begin{array}{ccc} H^0(G, A^q) & \xrightarrow{\mu^q} & H^q(G, A) \\ \Big\downarrow{\scriptstyle \mathrm{res}_0} & & \Big\downarrow{\scriptstyle \mathrm{res}_q} \\ H^0(H, A^q) & \xrightarrow[\mu^q]{} & H^q(H, A) \end{array}$$

El caso de inflación es diferente, pues la sucesión exacta respectiva, debería ser: $0 \longrightarrow A^H \longrightarrow B^H \longrightarrow C^G \longrightarrow 0$ pero esta sucesión no es exacta en general. De hecho, la sucesión que es exacta es $0 \longrightarrow A^H \longrightarrow B^H \longrightarrow C^H \longrightarrow H^1(H, A) \longrightarrow \cdots$.

Ahora bien, resulta ser que E. Weiss [168] define un mapeo inflación para índices negativos y se llama *deflación*.

Similarmente al caso de restricción, tenemos:

Proposición 4.7.9. *Sean A y B dos G-módulos y $H \triangleleft G$ un subgrupo normal de G, G un grupo finito. Sea $f\colon A \longrightarrow B$ un G-homomorfismo. Entonces el diagrama*

$$\begin{array}{ccc} H^q(G/H, A^H) & \xrightarrow{H^q(f)} & H^q(G/H, B^H) \\ \Big\downarrow{\scriptstyle \inf_q} & & \Big\downarrow{\scriptstyle \inf_q} \\ H^q(G, A) & \xrightarrow[H^q(f)]{} & H^q(G, B) \end{array}$$

es conmutativo para toda $q \geq 0$. Notemos que un G-homomorfismo $f\colon A \longrightarrow B$, induce un G/H-homomorfismo $f\colon A^H \longrightarrow B^H$. □

Ejemplo 4.7.10 (Corestricción). Sea G un grupo y sea $H < G$, digamos $[G : H] = m$. Sea $G = \cup_{i=1}^{m} \sigma_i H$ la descomposición de G en clases izquierdas de H. Se define $\mathrm{Tr}_{H\to G}\colon A^H \longrightarrow A^G$, $\mathrm{Tr}_{H\to G}(a) = \sum_{i=1}^{m} \sigma_i a$. Esto es, $\mathrm{Tr}_{H\to G}(a) = \mathrm{N}_{G/H}(a)$, aunque entendiendo que H no necesariamente es normal en G.

Si $\{\sigma_i'\}_{i=1}^m$ es otro conjunto de representantes, esto es, $\sigma_i' = \sigma_i h_i$ par algunos $h_i \in H$, entonces $\sigma_i' a = \sigma_i h_i a \underset{\substack{\uparrow \\ a\in A^H}}{=} \sigma a$. Por tanto, $\mathrm{Tr}_{H\to G}(a)$ no depende de los representantes $\{\sigma_i\}_{i=1}^m$.

Si $\theta \in G$, $\theta\sigma_i H = \sigma_{\theta(i)} H$, esto es, $\theta\sigma_i = \sigma_{\theta(i)} h_i$ para alguna $h_i \in H$. Además $\{\sigma_{\theta(i)}\}_{i=1}^m \subseteq \{\sigma_i\}_{i=1}^m$. Si $\sigma_{\theta(i)} = \sigma_{\theta(j)}$, entonces $\sigma_{\theta(i)} = \theta\sigma_i h_i^{-1} = \theta\sigma_j h_j^{-1} = \sigma_{\theta(j)}$. Por tanto $\sigma_i h_i^{-1} = \sigma_j h_j^{-1}$ por lo que $\sigma_i \in \sigma_j H$ de donde se sigue que $\sigma_i = \sigma_j$. Entonces $\tilde{\theta}\colon \{\sigma_i\} \longrightarrow \{\sigma_{\theta(i)}\}$ es una biyección y por tanto

$$\theta\big(\sum_{i=1}^{m} \sigma_i a\big) = \sum_{i=1}^{m} \theta\sigma_i a = \sum_{i=1}^{m} \sigma_{\theta(i)} a = \sum_{i=1}^{m} \sigma_i a,$$

de donde se obtiene que $\mathrm{Tr}_{H\to G}\, a \in A^G$.

Se sigue que

(1) $\mathrm{Tr}_{H\to G}\colon \mathrm{Hom}_H(A, B) \longrightarrow \mathrm{Hom}_G(A, B)$ es un homomorfismo.
(2) Si $f \in \mathrm{Hom}_G(A, B)$, entonces $\mathrm{Tr}_{H\to G}(f) = [G : H]f$.

Sea P una resolución de $\mathbb{Z}[G]$-módulos libres de $\mathbb{Z}$. Entonces P también es una resolución de $\mathbb{Z}[H]$-módulos. Sea $f \in \mathrm{Hom}_H(P_n, A)$, entonces

$$\partial^*\big(\mathrm{Tr}_{H\to G}(f)\big) = \mathrm{Tr}_{H\to G}(f) \circ \partial = \mathrm{Tr}_{H\to G}(f \circ \partial) = \mathrm{Tr}_{H\to G}\big(\partial^*(f)\big).$$

Es decir, $\partial^* \circ \mathrm{Tr}_{H\to G} = \mathrm{Tr}_{H\to G} \circ \partial^*$.

$$\begin{array}{ccc} \mathrm{Hom}_H(P_n, A) & \xrightarrow{\partial^*_{n+1}} & \mathrm{Hom}_H(P_{n+1}, A) \\ \Big\downarrow{\scriptstyle \mathrm{Tr}_{H\to G}} & & \Big\downarrow{\scriptstyle \mathrm{Tr}_{H\to G}} \\ \mathrm{Hom}_G(P_n, A) & \xrightarrow[\partial^*_{n+1}]{} & \mathrm{Hom}_G(P_{n+1}, A) \end{array}$$

Si $f \in \mathrm{núc}\, \partial^*_{n+1}$, entonces $\big(\partial^*_{n+1} \circ \mathrm{Tr}_{H\to G}\big)(f) = \big(\mathrm{Tr}_{H\to G} \circ \partial^*_{n+1}\big)(f) = 0$, es decir, $\mathrm{Tr}_{H\to G}\, f \in \mathrm{núc}\, \partial^*_{n+1}$ y por tanto tenemos homomorfismos

$$H^n(H, A) \xrightarrow{\mathrm{Tr}_{H\to G}} H^n(G, A)$$

para $n \in \mathbb{Z}$.

Este grupo de mapeos se llama *corestricción*. Explícitamente, se tiene para

$$\begin{aligned}\mathrm{cor}_0\colon H^0(H,A) &\longrightarrow H^0(G,A)\\ a+\mathrm{N}_H A &\longrightarrow \mathrm{N}_{G/H}\, a+\mathrm{N}_G A,\\ \mathrm{cor}_{-1}\colon H^{-1}(H,A) &\longrightarrow H^{-1}(G,A)\\ a+I_H A &\longrightarrow a+I_G A \quad \text{para } a\in {}_{\mathrm{N}_H}A \subseteq\in {}_{\mathrm{N}_G}A.\end{aligned}$$

Sea $0 \longrightarrow A \xrightarrow{i} A \xrightarrow{j} C \longrightarrow 0$ una sucesión exacta de G-módulos. Entonces el siguiente diagrama es conmutativo

$$\begin{array}{ccc} H^{-1}(H,C) & \xrightarrow{\delta} & H^0(H,A) \\ {\scriptstyle \mathrm{cor}_{-1}}\downarrow & & \downarrow{\scriptstyle \mathrm{cor}_0} \\ H^{-1}(G,C) & \xrightarrow{\delta} & H^0(G,A) \end{array}$$

De aquí tenemos que la corestricción es la única familia de homomorfismos $\mathrm{cor}_q\colon H^q(H,A) \longrightarrow H^q(G,A)$, $q\in\mathbb{Z}$, tal que:

(1) Si $q=0$, $\mathrm{cor}_0\colon H^0(H,A) \longrightarrow H^0(G,A)$, $a+\mathrm{N}_H A \longrightarrow \mathrm{Tr}_{H\to G}\, a + \mathrm{N}_G A = \mathrm{N}_{G/H}\, a + \mathrm{N}_G A$, $a\in A^H$.
(2) Para cada sucesión G-exacta $0 \longrightarrow A \longrightarrow B \longrightarrow C \longrightarrow 0$, el siguiente diagrama es conmutativo

$$\begin{array}{ccc} H^q(H,C) & \xrightarrow{\delta} & H^{q+1}(H,A) \\ {\scriptstyle \mathrm{cor}_q}\downarrow & & \downarrow{\scriptstyle \mathrm{cor}_{q+1}} \\ H^q(G,C) & \xrightarrow{\delta} & H^{q+1}(G,A) \end{array}$$

Formalmente, $\mathrm{cor}_{q+1} = \delta\circ\mathrm{cor}_q\circ\delta^{-1}$.
El mapeo cor_q está determinado por el diagrama conmutativo

$$\begin{array}{ccc} H^0(H,A^q) & \xrightarrow{\mu^q} & H^q(H,A) \\ {\scriptstyle \mathrm{cor}_0}\downarrow & & \downarrow{\scriptstyle \mathrm{cor}_q} \\ H^0(G,C) & \xrightarrow{\mu^q} & H^q(G,A) \end{array}$$

$\mathrm{cor}_q = \mu^q\circ\mathrm{cor}_0\circ(\mu^q)^{-1}$.

Ejemplo 4.7.11 (Conjugación). Sea $\varphi=\varphi_\sigma\colon G(=G') \longrightarrow G$ dado por $\varphi_\sigma(g)=\sigma g\sigma^{-1}$. Sean A un G-módulo y $\varphi_\sigma^* A(=A)$ es también un G-módulo con acción $gA=\varphi_\sigma(g)a=\sigma g\sigma^{-1}a$.

Sea $f_\sigma\colon A\longrightarrow A$ dada por $f_\sigma(a)=\sigma^{-1}a$. Entonces

$$f_\sigma(\varphi_\sigma(g)a)=f_\sigma(\sigma g\sigma^{-1}a)=\sigma^{-1}(\sigma g\sigma^{-1}a)=g\sigma^{-1}a=gf_\sigma(a)=g\sigma^{-1}a,$$

esto es, $f_\sigma(\varphi_\sigma(g)a) = gf_\sigma(a)$. Por tanto $(\varphi_\sigma, f_\sigma)$ es compatible y puesto que φ_σ es inyectiva, se tienen homomorfismos $(\varphi_\sigma, f_\sigma)_n \colon H^n(G,A) \longrightarrow H^n(G,A)$ para toda $n \in \mathbb{Z}$.

Para $n = 0$, $(\varphi_\sigma, f_\sigma)_0 \colon \mathrm{Id}_{H^0(G,A)} \colon A^G/\,\mathrm{N}_G\, A \longrightarrow A^G/\,\mathrm{N}_G\, a$ y $f_\sigma(a) = \sigma^{-1}a = a$ para toda $a \in A^G$. El diagrama

$$\begin{array}{ccc} H^0(G,A^q) & \xrightarrow{\mu^q} & H^q(G,A) \\ {\scriptstyle (\varphi_\sigma,f_\sigma)_0}\downarrow & & \downarrow{\scriptstyle (\varphi_\sigma,f_\sigma)_q} \\ H^0(G,A^q) & \xrightarrow{\mu^q} & H^q(G,A) \end{array}$$

es conmutativo y $(\varphi_\sigma, f_\sigma)_0 = \mathrm{Id}$ implica que $(\varphi_\sigma, f_\sigma)_q = \mathrm{Id}$ para toda $q \in \mathbb{Z}$.

4.8. Lema de Shapiro, la sucesión inflación-restricción, mapeo de transferencia

Empezamos analizando la composición corestricción-restricción: cor $\circ$ res.

Teorema 4.8.1. *Sea G un grupo finito y sea H un subgrupo, Entonces la composición*

$$H^q(G,A) \xrightarrow{\mathrm{res}} H^q(H,A) \xrightarrow{\mathrm{cor}} H^q(G,A)$$

es el endomorfismo $\mathrm{cor} \circ \mathrm{res} = n(= n \cdot \mathrm{Id})$ *donde* $n = [G : H]$.

Demostración. Si $a \in A^G$, $\mathrm{cor}_0 \circ \mathrm{res}_0(\bar{a}) = \mathrm{cor}_0(a + \mathrm{N}_H\, A) = \sum_{\sigma \in G/H} \sigma a + \mathrm{N}_G\, A = na + \mathrm{N}_G\, A = n\bar{a}$.

Para q general, tenemos

$$\begin{array}{ccc} H^0(G,A^q) & \xrightarrow{\mathrm{cor}_0 \circ \mathrm{res}_0 = n} & H^0(G,A^q) \\ \cong\downarrow{\scriptstyle \mu^q} & & \cong\downarrow{\scriptstyle \mu^q} \\ H^q(G,A) & \xrightarrow{\mathrm{cor}_q \circ \mathrm{res}_q} & H^q(G,A) \end{array}$$

por lo que $\mathrm{cor}_q \circ \mathrm{res}_q = n$ para toda $n \in \mathbb{Z}$. □

Observación 4.8.2. El Teorema 4.8.1 implica que si tomamos $H = \{1\}$, entonces $n = |G|$ y en particular $nH^q(G,A) = 0$ para toda $q \in \mathbb{Z}$.

Sea $f \colon A \longrightarrow B$ es un G-homomorfismo y si $H < G$, los siguientes diagramas son conmutativos

$$\begin{array}{ccc} H^0(G,A) & \xrightarrow{H^0(f)} & H^0(G,B) \\ {\scriptstyle \mathrm{cor}}\uparrow\downarrow{\scriptstyle \mathrm{res}} & & {\scriptstyle \mathrm{cor}}\uparrow\downarrow{\scriptstyle \mathrm{res}} \\ H^q(H,A) & \xrightarrow{H^q(f)} & H^q(H,B) \end{array}$$

Es decir, tanto restricción como restricción conmutan con los homomorfismos en cohomología inducidos de un homomomorfismo de G-módulos.

Ahora bien, los grupos $H^q(G,A)$ son grupos abelianos de torsión pues $nH^q(G,A)=0$ donde $n=|G|$. Por tanto $H^q(G,A)$ es suma directa de sus p-subgrupos de Sylow:

$$H^q(G,A)=\bigoplus_p H^q(G,A)_p,$$

donde $H^q(G,A)_p$ es el p-subgrupo de Sylow de $H^q(G,A)$.

Proposición 4.8.3. *La restricción* $\operatorname{res}\colon H^q(G,A)_p \longrightarrow H^q(G_p,A)$ *es inyectiva y la corestricción* $\operatorname{cor}\colon H^q(G_p,A)\longrightarrow H^q(G,A)_p$ *es biyectiva donde* G_p *es un* p*-subgrupo de Sylow de* G*.*

Demostración. Se tiene $\operatorname{cor}\circ\operatorname{res}=[G:G_p]\operatorname{Id}$ y $\operatorname{mcd}(p,[G:G_p])=1$, entonces el mapeo $H^q(G,A)_p \xrightarrow{\operatorname{cor}\circ\operatorname{res}} H^q(G,A)_p$ es biyectiva. Por tanto, si $x\in H^q(G,A)_p$ es tal que $\operatorname{res}x=0$, $\operatorname{cor}\circ\operatorname{res}x=0$, por tanto res es inyectiva.

Ahora si $|G_p|=p^m$, $p^mH^q(G_p,A)=0$ por lo que $\operatorname{cor}\big(H^q(G_p,A)\big)\subseteq H^q(G,A)_p$:

$$H^q(G,A)_p \xrightarrow{\operatorname{res}} H^q(G_p,A) \xrightarrow{\operatorname{cor}} H^q(G,A)_p.$$
$$\underbrace{\qquad\qquad\qquad\qquad\qquad\qquad}_{\text{biyectiva}}$$

Por tanto, $\operatorname{cor}\big(H^q(G_p,A)\big)=H^q(G,A)_p$. □

Corolario 4.8.4. *Si para cada primo* p *se tiene que* $H^q(G_p,A)=0$ *para algún* p*-subgrupo de Sylow* G_p *de* G*, entonces* $H^q(G,A)=0$*.*

Demostración. Se tiene $\operatorname{res}\colon H^q(G,A)_p\longrightarrow H^q(G_p,A)$ es inyectiva, por lo tanto $H^q(G,A)_p=0$ para toda p. Se sigue que $H^q(G,A)=0$. □

Definición 4.8.5. Sea G un grupo finito y sea $H<G$ un subgrupo de G. Un G-módulo A se llama G/H*-inducido* si $A=\bigoplus_{\sigma\in G/H}\sigma B$ donde B es un H-submódulo de A y σ varía en un conjunto de representantes de clases izquierdas de H en G. Cuando $H=\{1\}$, $G/H=G$ y G/H-inducido significa G-inducido.

Sea $\varphi=i\colon H\longrightarrow G$ la inclusión y sea $g=\pi\colon A\longrightarrow B$ donde $\pi(a)=b_1$ donde $a=\sum_{\sigma_{G/H}}\sigma b_\sigma$. Si $h\in H$,

$$\begin{aligned} g(\varphi(h)a)=\pi(i(h)a)=\pi(ha)&=\pi\Big(\sum_{\sigma\in G/H} h\sigma(hb_\sigma)\Big)\\ &=\pi\Big(h\cdot 1(h(b_1))+\sum_{\substack{\sigma\in G/H\\ \sigma\neq 1}} h\sigma(hb_\sigma)\Big)=h(b_1),\end{aligned}$$

y

$$h \circ g(a) = h\pi(a) = h(b_1),$$

por lo que φ y g son compatibles y tenemos homomorfismos:

$$H^n(G, A) \xrightarrow{(\varphi,g)_n} H^n(H, B), \quad n \in \mathbb{Z}.$$

Proposición 4.8.6. *Sea C un G-módulo. Entonces*

$$\mathrm{Hom}_G(C, A) \underset{\psi}{\cong} \mathrm{Hom}_H(C, B),$$

donde $\psi(f) = \pi \circ f$, $\pi\colon A \longrightarrow B$ con $\pi(a) = b_1$ donde $a = \sum_{\sigma \in G/H} \sigma b_\sigma$. El inverso de ψ es $\psi^{-1}(g) = S_g = \sum_{\sigma \in G/H} \sigma g \sigma^{-1}$.

Demostración. Sea $f \in \mathrm{Hom}_G(C, A)$. Entonces $\pi \circ f\colon C \longrightarrow B$ es un H-homomorfismo. Si $\pi \circ f = 0$, entonces $\pi \circ f(c)$ para toda $c \in C$. Si $f \neq 0$, existiría $f(c) = a \neq 0$. Sea $a = \sum_{\sigma \in G/H} \sigma b_\sigma$ y sea $b_\theta \neq 0$. Entonces

$$\theta^{-1} f(c) = f(\theta^{-1} c) = \theta^{-1} a = \sum_{\sigma \in G/H} \theta^{-1} \sigma b_\sigma = \theta^{-1} \theta b_\theta + \sum_{\substack{\theta \in G/H \\ \sigma \neq \theta}} \theta^{-1} \sigma b_\sigma$$

$$= b_\theta + \sum_{\substack{\sigma \in G/H \\ \sigma \neq \theta}} \theta^{-1} \sigma b_\sigma.$$

Por lo tanto

$$(\pi \circ f)(\theta^{-1} c) = \pi(f(\theta^{-1} c)) = \pi\big(b_\theta + \sum_{\substack{\sigma \in G/H \\ \sigma \neq \theta}} \theta^{-1} \sigma b_\sigma\big) = b_\theta \neq 0.$$

Por tanto ψ es inyectiva.

Sea $g \in \mathrm{Hom}_H(C, B)$ y sea $S_g \in \mathrm{Hom}_G(C, A)$ dada por

$$S_g(c) = \sum_{\sigma \in G/H} \sigma g(\sigma^{-1} c).$$

Si $\sigma' = \sigma h$, esto es, $\sigma' H = \sigma H$ es la misma clase izquierda, entonces

$$\sigma' g((\sigma')^{-1}(c)) = \sigma h g(h^{-1} \sigma^{-1} c) = \sigma h h^{-1} g(\sigma^{-1} c) = \sigma g(\sigma^{-1} c),$$

por lo que $S_g(c)$ está bien definido. Se verifica directamente que $S_g(\theta c) = \theta S_g(c)$ para toda $\theta \in G$ y toda $c \in C$. Por tanto $S_g \in \mathrm{Hom}_G(C, A)$ y $(\pi \circ S_g)(c) = S_g(c)_1 = g(1^{-1} c) = g(c)$ y por tanto $\pi \circ S_g = g$ y ψ es suprayectiva. □

Como corolario, obtenemos el siguiente resultado.

Teorema 4.8.7 (Lema de Shapiro). *Sean G un grupo finito y H un subgrupo de G. Sea A un G–módulo que es G/H–*inducido*, esto es, existe $B \subseteq A$ es un H–módulo tal que*

$$A \cong \bigoplus_{\sigma \in G/H} \sigma B,$$

donde σ corre sobre un conjunto de representantes izquierdos de H en G. Entonces

$$H^n(G, A) \cong H^n(H, B) \quad \textit{para toda } n \in \mathbb{Z}$$

bajo el isomorfismo inducido por

$$H^n(G, A) \xrightarrow{\text{res}} H^n(H, A) \xrightarrow{\bar{\pi}} H^n(H, B),$$

donde $\bar{\pi}$ es inducido por la proyección natural $\pi\colon A \longrightarrow B$ y res *es el mapeo de restricción.*

Demostración. Aplicar lo anterior con $C = P_n$, donde P es una G-resolución completa. □

Teorema 4.8.8 (inflación-restricción). *Sean G un grupo finito, A un G-módulo y $H \triangleleft G$ un subgrupo normal de G. Entonces*

$$0 \longrightarrow H^1(G/H, A^H) \xrightarrow{\text{inf}} H^1(G, A) \xrightarrow{\text{res}} H^1(H, A),$$

es exacta.

Demostración. Para ver la inyectividad de inf, sea $f\colon G/H \longrightarrow A^H$ un 1-cocliclo tal que $\inf f$ es una 1-cofrontera del G-módulo A. Entonces

$$\inf f(\sigma) = f(\sigma H) = \sigma a - a \quad \text{para alguna } a \in A \text{ y para toda } \sigma \in G.$$

Para $\tau \in H$, se tiene $\sigma\tau a - a = \sigma a - a$, por tanto $\tau a = a$ para toda $\tau \in H$. Se sigue que $a \in A^H$. Por lo tanto $f(\sigma H) = \sigma H a - a$ es una 1-cofrontera. Se sigue que inf es inyectiva.

Ahora veamos la exactitud en $H^1(G, A)$. Sea $f\colon G/H \longrightarrow A^H$ un 1-cociclo de A^H. Para $\sigma \in H$, se tiene que

$$\text{res} \circ \inf f(\sigma) = \inf f(\sigma) = f(\sigma H) = f(H) = f(\bar{1}).$$

Ahora $f(\bar{1}) = f(\bar{1} \cdot \bar{1}) = f(\bar{1}) + f(\bar{1})$ de donde obtenemos $f(\bar{1}) = 0$ y por tanto $\text{res} \circ \inf = 0$. En particular $\text{im}\inf \subseteq \text{núc res}$.

Recíprocamente, sea $f\colon G \longrightarrow A$ un 1-cociclo del G-módulo A cuya restricción a H es una 1-cofrontera del H-módulo A:

$$f(\tau) = \tau a - a, \quad a \in A \quad \text{para toda } \tau \in H.$$

Sea $g\colon G \longrightarrow A$, $g(\sigma) = \sigma a - a$ para todo $\sigma \in G$, g es una 1-cofrontera. Entonces $f - g$ es un 1-cociclo $h(\sigma) = f(\sigma) - g(\sigma)$ y h y f están en la misma clase de cohomología y además $h(\tau) = 0$ para $\tau \in H$. Entonces

$$h(\sigma\tau) = h(\sigma) + \sigma h(\tau) = h(\sigma) \quad \text{para toda } \tau \in H$$

y además

$$h(\tau\sigma) = h(\tau) + \tau h(\sigma) = \tau h(\sigma) \quad \text{para toda } \tau \in H.$$

Por tanto $\tau h(\sigma) = h(\sigma)$ para toda $\tau \in H$ y para toda $\sigma \in G$.

Sea $F\colon G/H \longrightarrow A$ dado por $F(\sigma H) = h(\sigma)$. Entonces $f(\sigma H) \in A^H$ y F es un cociclo con $\inf F = h$, lo cual prueba que $\text{núc res} \subseteq \text{im inf}$. El resultado se sigue. □

Para $q \geq 2$ se tiene el análogo siempre y cuando se cumpla que $H^i(H, A) = 0$ para $i = 1, \ldots, q-1$. Esto es,

Teorema 4.8.9. *Sea A un G-módulo y sea $H \triangleleft G$ un subgrupo normal de G. Si $H^i(H, A) = 0$ para $i = 1, \cdots, q-1$ y $q \geq 1$, entonces la sucesión*

$$0 \longrightarrow H^q(G/H, A^H) \xrightarrow{\text{inf}} H^q(G, A) \xrightarrow{\text{res}} H^q(H, A)$$

es exacta.

Demostración. Se probará por inducción en q. El caso $q = 1$ es el Teorema 4.8.8. De la sucesión exacta $0 \longrightarrow \mathbb{Z} \longrightarrow \mathbb{Z}[G] \longrightarrow J_G = \mathbb{Z}[G]/\mathbb{Z} \longrightarrow 0$, se obtiene la sucesión exacta

$$0 \longrightarrow \underset{A \otimes \mathbb{Z}}{A} \longrightarrow \mathbb{Z}[G] \otimes A \longrightarrow J_G \otimes A \longrightarrow 0.$$

Puesto que $H^1(H, A) = 0$, se sigue que la sucesión

$$0 \longrightarrow A^H \longrightarrow \big(\mathbb{Z}[G] \otimes A\big)^H \longrightarrow \big(J_G \otimes A\big)^H \longrightarrow 0$$

es exacta. Por tanto tenemos que el siguiente diagrama es conmutativo.

$$\begin{array}{ccccccc}
0 & \longrightarrow & H^{q-1}(G/H, (J_G \otimes A)^H) & \xrightarrow{\text{inf}} & H^{q-1}(G, (J_G \otimes A)) & \xrightarrow{\text{res}} & H^{q-1}(H, (J_G \otimes A)) \\
 & & \downarrow{\scriptstyle \delta = \mu} & & \downarrow{\scriptstyle \delta = \mu} & & \downarrow{\scriptstyle \delta = \mu} \\
0 & \longrightarrow & H^q(G/H, A^H) & \xrightarrow{\text{inf}} & H^q(G, A) & \xrightarrow{\text{res}} & H^q(H, A)
\end{array}$$

Puesto que $\mathbb{Z}[G] \otimes A$ es tanto G-módulo inducido como H-módulo inducido, los mapeos de conexión $\delta = \mu$ son isomorfismos. Por tanto $H^i(H, (J_G \otimes A)) \cong H^{i+1}(H, A) = 0$ para $i = 1, \cdots, q-2$. Entonces por inducción, la fila superior en el diagrama anterior es exacta, por tanto lo es la fila inferior, probando el resultado. □

El caso que se nos presenta en teoría de campos de clase es que si $K \subseteq L \subseteq M$ es una torre de campos con $q = 2$, M/K y L/K extensiones de Galois, entonces si $G = \mathrm{Gal}(M/K)$, $H = \mathrm{Gal}(M/L)$ y $G/H \cong \mathrm{Gal}(L/K)$ entonces $H^1(H, M^*) = \{1\}$ y por tanto

$$0 \longrightarrow H^2(\mathrm{Gal}(L/K), L^*) \xrightarrow{\inf} H^2(\mathrm{Gal}(M/K), M^*) \xrightarrow{\mathrm{res}} H^2(\mathrm{Gal}(M/L), M^*)$$

es exacta, y en particular se tiene que podemos considerar la contención $H^2(\mathrm{Gal}(L/K), L^*) \subseteq H^2(\mathrm{Gal}(M/K), M^*)$.

Ahora veremos un mapeo importante en teoría de campos de clase, el llamado *mapeo de transferencia*. En alemán, el mapeo de transferencia se llama *Verlagerung*. Primero recrdemos que

$$H^{-2}(G, \mathbb{Z}) \cong G/G' = G^{\mathrm{ab}}.$$

Si $H < G$ tenemos que el mapeo de transferencia, Ver, es el mapeo restricción en dimensión -2: $\mathrm{Ver} := \mathrm{res}_{-2} \colon H^{-2}(G, \mathbb{Z}) \to H^{-2}(H, \mathbb{Z})$, $\mathrm{Ver} \colon G^{\mathrm{ab}} \to H^{\mathrm{ab}}$.

Sea $g \in G$. Sea $\{x_i\}_i$ un conjunto de representantes de las clases derechas módulo $H : G = Hx_1 \cup \ldots \cup Hx_n$. Ahora, para cada índice i, existe un índice $\sigma(i)$ y un elemento $\xi \in H$ tal que $x_i g = \xi x_{\sigma(i)}$, Sea $\xi := \prod_{i=1}^{n}$. Entonces

$$\mathrm{Ver}(gG') = \xi H', \quad \text{esto es,} \quad \mathrm{Ver}(gG') = \Big(\prod_{i=1}^{n} x_i g x_{\sigma(i)}^{-1} \Big) H'.$$

4.9. Producto copa

Uno de los resultados fundamentales en teoría de campos de clase, es el teorema de reciprocidad. El metodo cohomológico para obtener el teorema de reciprocidad es el Teorema de Tate-Nakayama que es un resultado del producto copa.

Para definir el producto copa de manera directa, se hace por medio del producto tensorial a nivel de los valores de cadenas homogéneas. Más precisamente, sean G un grupo finito, A y B dos G-módulos y consideramos $A \otimes B$ como G-módulo: $\sigma(a \otimes b) = \sigma a \otimes \sigma b$, $a \in A, b \in B$ y $\sigma \in G$. Consideremos una resolución P de G y

$$\mathrm{Hom}_G(P_p, A) \times \mathrm{Hom}_G(P_q, B) \xrightarrow{\Cup} \mathrm{Hom}_G(P_{p+q}, A \otimes B)$$

para $p, q \geq 0$, dado por la fórmula

$$(a \Cup b)(g_0, \ldots, g_{p+q}) = a(g_0, \ldots, g_p) \otimes b(g_p, \ldots, g_{p+q}).$$

Para $p = q = 0$, $(a \Cup b)(g_0) = a(g_0) \otimes b(g_0) = (a \otimes b)(g_0)$.

Desarrollamos el producto copa en todas las dimensiones $p, q \in \mathbb{Z}$.

Dados los dos G-módulos A y B, el mapeo $A \times B \longrightarrow A \otimes B$, induce un mapeo bilineal canónico

$$A^G \times B^G \longrightarrow (A \otimes B)^G,$$

que mapea $\mathrm{N}_G\, A \times \mathrm{N}_G\, B$ a $\mathrm{N}_G(A \otimes B)$. Por tanto, se induce un mapeo bilineal

$$H^0(G, A) \times H^0(G, B) \longrightarrow H^0(G, A \otimes B),$$
$$(\bar{a}, \bar{b}) \longmapsto \overline{(a \otimes b)}, \quad \bar{a} = a + \mathrm{N}_G\, A.$$

Definición 4.9.1. El elemento $\overline{a \otimes b} \in H^0(G, A \otimes B)$ se llama el *producto copa*, $\bar{a} \in H^0(G, A)$ y $\bar{b} \in H^0(G, B)$ y se denotará $\bar{a} \Cup \bar{b} = \overline{a \otimes b}$.

Teorema 4.9.2 (Producto copa). *Existe una única familia de mapeos bilineales $\Cup$, llamada el* producto copa *tal que para cualesquiera $p, q \in \mathbb{Z}$ se tiene*

$$\Cup\colon H^p(G, A) \times H^q(G, B) \longrightarrow H^{p+q}(G, A \otimes B)$$

que satisface:

(1) *Si $p = q = 0$, el producto copa está dado por el producto tensorial: $(\bar{a}, \bar{b}) \mapsto \bar{a} \Cup \bar{b} = \overline{a \otimes b}$, $\bar{a} \in H^0(G, A) = A^G/\,\mathrm{N}\, A$, $\bar{b} \in H^0(G, B) = B^G/\,\mathrm{N}\, B$.*

(2) *Si $0 \to A \to B \to C \to 0$ y $0 \to A \otimes D \to B \otimes D \to C \otimes D \to 0$ son sucesiones G-exactas, entonces el siguiente diagrama conmuta:*

$$\begin{array}{ccc} H^p(G, C) \times H^q(G, D) & \xrightarrow{\Cup} & H^{p+q}(G, C \otimes D) \\ {\scriptstyle\delta}\downarrow & \downarrow{\scriptstyle 1} & \downarrow{\scriptstyle\delta} \\ H^{p+1}(G, A) \times H^q(G, D) & \xrightarrow{\Cup} & H^{p+q+1}(G, A \otimes D) \end{array}$$

es decir, $\delta(c \Cup d) = \delta(c) \Cup d$, $c \in H^p(G, C)$, $d \in H^q(G, D)$ con δ los mapeos de conexión.

(3) *Si $0 \to A \to B \to C \to 0$ y $0 \to D \otimes A \to D \otimes B \to D \otimes C \to 0$ son G-exactas, entonces el siguiente diagrama conmuta:*

$$\begin{array}{ccc} H^p(G, D) \times H^q(G, C) & \xrightarrow{\Cup} & H^{p+q}(G, D \otimes C) \\ {\scriptstyle 1}\downarrow & \downarrow{\scriptstyle\delta} & \downarrow{\scriptstyle(-1)^p\delta} \\ H^p(G, D) \times H^{q+1}(G, A) & \xrightarrow{\Cup} & H^{p+q+1}(G, D \otimes A) \end{array}$$

es decir, $\delta(d \Cup c) = (-1)^p\big(d \Cup \delta c\big)$, $d \in H^p(G, D)$, $c \in H^q(G, C)$.

Observación 4.9.3. El factor $(-1)^p$ se debe a la anticonmutatividad del mapeo de conexión δ.

Observación 4.9.4. Lo que se está haciendo es definir un producto copa $H^p(G,A)\times H^q(G,B)\xrightarrow{\Cup} H^{p+q}(G,A\otimes B)$ por medio del diagrama (4.9.14) más adelante y ver que satisface las condiciones (1)–(3) del Teorema 4.9.2. Las condiciones (1)–(3) hace única la posible definición de $\Cup$ por los isomorfismos $H^0(G,A^p)\underset{\mu^p}{\cong} H^p(G,A)$ y de $H^0(G,B^q)\underset{\mu^q}{\cong} H^q(G,B)$. Si cambiamos el isomorfismo $(-1)^{pq}\mu^q$ por otro, obtendríamos otro producto copa con otras condiciones (1)–(3) del Teorema 4.9.2.

Demostración. (Teorema 4.9.2) Como en el caso de los mapeos de restricción, se obtiene el producto copa en general del caso particular $p=0, q=0$ usando el cambio de dimensión.

Se tiene:

$$A^p\otimes B = J_G\otimes\cdots\otimes J_G\otimes A\otimes B = (A\otimes B)^p$$

y

$$A\otimes B^q = A\otimes J_G\otimes\cdots\otimes J_G\otimes B = (J_G\otimes\cdots\otimes J_G)\otimes A\otimes B = (A\otimes B)^q,$$

para A y B dos G-módulos y para $p,q\geq 0$. Similarmente para $p,q\leq 0$ con I_G en lugar de J_G.

Usando el isomorfismo $\mu^m\colon H^{q-m}(G,A^m)\xrightarrow{\cong} H^q(H,A)$, $m\in\mathbb{Z}$, empezando con el caso $p=0$, $q=0$ y obtenemos el producto copa del diagrama

$$\begin{array}{ccc}
H^0(G,A^p)\times H^0(G,B^q) & \xrightarrow[(\bar{x},\bar{y})\to\overline{(x\otimes y)}]{\Cup} & H^0(G,(A\otimes B^q)^p)=H^0(G,A^p\otimes B^q)\\
\cong\downarrow\mu^p \quad \cong\downarrow 1 & & \downarrow\mu^p\\
H^p(G,A)\times H^0(G,B^q) & \xrightarrow[\varphi]{\Cup} & H^p(G,(A\otimes B)^q)=H^p(G,A\otimes B^q)\\
\cong\downarrow 1 \quad \cong\downarrow\mu^q & & \downarrow(-1)^{pq}\mu^q\\
H^p(G,A)\times H^q(G,B) & \xrightarrow[\psi]{\Cup} & H^{p+q}(G,A\otimes B)
\end{array}\tag{4.9.14}$$

Los isomorfismos

$$H^p(G,(A\otimes B)^q)\xrightarrow{(-1)^{pq}\mu^q} H^{p+q}(G,A\otimes B)$$

y

$$H^0(G,(A\otimes B^q)^p)\xrightarrow{\mu^p} H^p(G,(A\otimes B)^q)$$

determinan el producto copa. Si cambiamos los isomorfismos μ^p y $(-1)^{pq}\mu^q$ por algunos otros isomorfismos, el primero dependiendo de p y el segundo de p y de q, obtendríamos otro producto copa. No sabemos de algún otro producto copa que sea útil desde nuestro punto de vista: El Teorema de Reciprocidad

en teoría de campos de clase y la definición de estos isomorfismos como $(-1)^{pq}$ y μ^p de debe a que a nivel de cocadenas queremos el producto tensorial

$$(a \cup b)(g_0, \ldots, g_{p+q}) = a(g_0, \ldots, g_p) \otimes b(g_p, \ldots, g_{p+q})$$

y por lo tanto

$$\partial(a \cup b) = (\partial a \cup b) + (-1)^p (a \cup \partial b).$$

Regresando al diagrama (4.9.14), se tiene que el mapeo φ se obtiene del diagrama superior pues μ^p y $\mu^p \times 1$ son isomorfismos. El mapeo ψ se obtiene del diagrama inferior. Veremos que $\psi = \cup$ es el producto que satisface (2) y (3) del teorema. Además si ψ satisface las condiciones del teorema, este mapeo es únici como consecuencia de (1), (2) y (3).

Antes de probar las condiciones para ψ, veamos $\psi = \cup$ explícitamente en términos de cociclos en los casos $(0, q)$ y $(p, 0)$ y que corresponden a la definición directa en m-cadenas dadas al inicio de la subsección.

Proposición 4.9.5. *Sean a_p y b_q un p-cociclo de A y un q-cociclo de B y $\bar{a}_p$, $\bar{b}_q$ sus clases de cohomología, entonces*

$$\bar{a}_0 \cup \bar{b}_q = \overline{a_0 \otimes b_q} \quad y \quad \bar{a}_p \cup \bar{b}_0 = \overline{a_p \otimes b_0}.$$

Notemos que si $b_q(\sigma_1, \ldots, \sigma_q) \in B$ es un q-cociclo, entonces

$$a_0 \otimes b_q(\sigma_1, \ldots, \sigma_q) \in A \otimes B$$

con $a_0 \in A^G$, es también un q-cociclo.

Demostración. Se puede verificar directamente que $\bar{a}_0 \cup \bar{b}_q$ y $\bar{a}_p \cup \bar{b}_0$ definidos en la proposición satisfacen las condiciones (1), (2) y (3) del teorema para $(0, q)$ y $(p, 0)$ respectivamente, viendo el comportamiento de los cociclos bajo los respectivos mapeos. Finalmente la parte inferior del diagrama (4.9.14) para $p = 0$ y la parte superior para $q = 0$, se sigue que el producto dado por (4.9.14) coincide con lo dado en la proposición. □

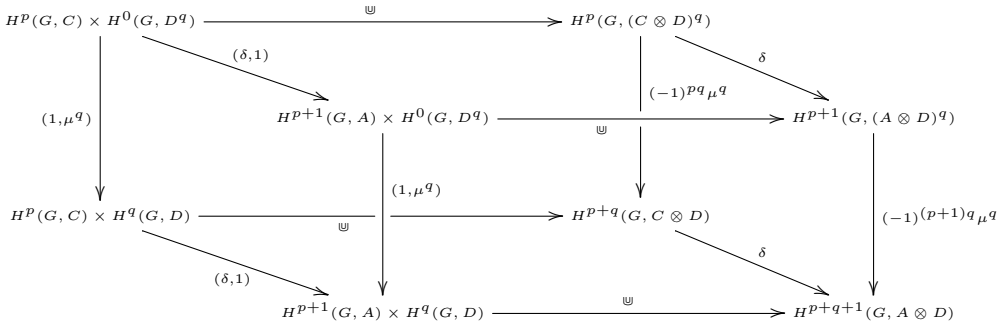
Sean $0 \longrightarrow B \longrightarrow C \longrightarrow 0$ y $0 \longrightarrow A \otimes D \longrightarrow B \otimes D \longrightarrow C \otimes D \longrightarrow 0$ sucesiones G-exactas y similarmente $0 \longrightarrow A \longrightarrow B \longrightarrow C \longrightarrow 0$ y $0 \longrightarrow D \otimes A \longrightarrow D \otimes B \longrightarrow D \otimes C \longrightarrow 0$. Se tienen las siguientes sucesiones G-exactas:

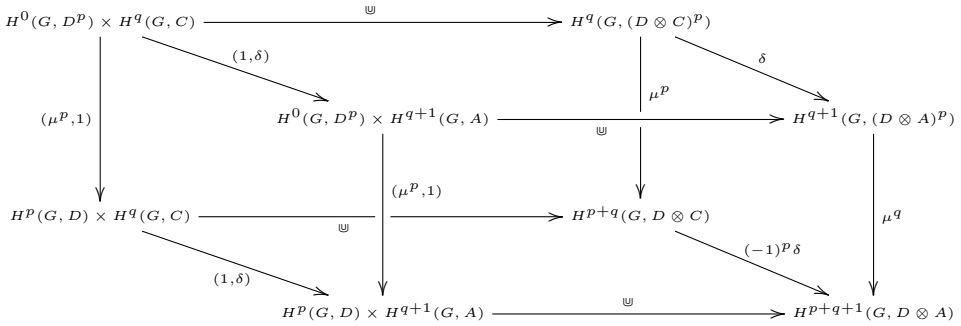
$$0 \longrightarrow A^q \longrightarrow B^q \longrightarrow C^q \longrightarrow 0 \quad \text{y}$$
$$0 \longrightarrow (A \otimes D)^q \longrightarrow (B \otimes D)^q \longrightarrow (C \otimes D)^q \longrightarrow 0$$

y también

$$0 \longrightarrow A^p \longrightarrow B^p \longrightarrow C^p \longrightarrow 0 \quad \text{y}$$
$$0 \longrightarrow (D \otimes A)^p \longrightarrow (D \otimes B)^p \longrightarrow (D \otimes C)^p \longrightarrow 0.$$

Se tienen diagramas:





Las partes (2) y (3) del teorema, son las partes inferiores de los diagramas anteriores.

Es inmediato que los lados izquierdos conmutan. Ahora, los lados derechos se componen de q (resp. p) cuadrados de cohomología de cambio de dimensión por lo que son conmutativos. Las partes frontales y traseras de los diagramas conmutan por la definición del producto copa dado en el diagrama (4.9.14) y finalmente, los cuadrados superiores conmutan por la Proposición 4.9.5. Puesto que los mapeos verticales son biyectivos, la conmutatividad de los cuadros superiores implican la conmutatividad de los cuadros inferiores, lo cual prueba (2) y (3) del teorema. Esto finaliza la prueba. □

Proposición 4.9.6. *Sean $f\colon A\longrightarrow A'$ y $g\colon B\longrightarrow B'$ dos G-homomorfismos y sea $f\otimes g\colon A\otimes A\longrightarrow A'\otimes B'$ el homomorfismo inducido por f y g. Si $\bar{a}\in H^p(G,A)$ y $\bar{b}\in H^q(G,B)$, entonces*

$$\bar{f}(\bar{a})\cup\bar{g}(\bar{b})=\overline{(f\otimes g)}(\bar{a}\cup\bar{b})\in H^{p+q}(G,A'\otimes B').$$

Demostración. La afirmación es equivalente a que el diagrama

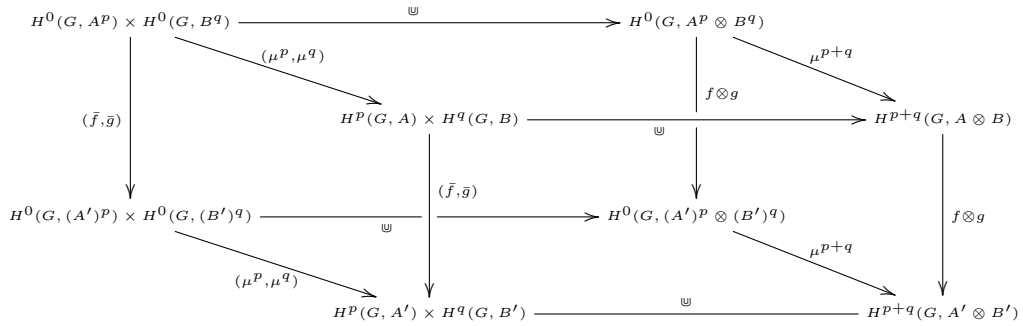
$$\begin{array}{ccc} H^p(G,A)\times H^q(G,B) & \xrightarrow{\cup} & H^{p+q}(G,A\otimes B) \\ \downarrow{\scriptstyle (\bar f,\bar g)} & & \downarrow{\scriptstyle f\otimes g} \\ H^p(G,A')\times H^q(G,B') & \xrightarrow[\cup]{} & H^{p+q}(G,A'\otimes B') \end{array}$$

es conmutativo para todas $p, q \in \mathbb{Z}$.

Para $p = q = 0$, la igualdad se sigue de lo siguiente:

$$\cup(\bar f,\bar g)(\bar a,\bar b) = \bar f(\bar a)\cup \bar g(\bar b) = \overline{f(a)\otimes g(b)},$$
$$(f\otimes g)(\bar a\cup \bar b) = (f\otimes g)(\overline{a\otimes b}) = \overline{f(a)\otimes g(b)}.$$

Para el caso general, consideremos el diagrama



el cual es conmutativo. Los isomorfismos se siguen del hecho de que $A^p\otimes B^q \cong (A\otimes B^q)^p$, etc. □

Proposición 4.9.7. *Sean A, B dos G-módulos y sea $H < G$ un subgrupo de G. Si $\bar a \in H^p(G,A)$ y $\bar b \in H^q(G,B)$, entonces*

$$\operatorname{res}(\bar a\cup \bar b) = \operatorname{res}(\bar a)\cup \operatorname{res}(\bar b) \in H^{p+q}(H, A\otimes B)$$

y

$$\operatorname{cor}(\operatorname{res}(\bar a)\cup \bar b) = \bar a\cup \operatorname{cor}(\bar b) \in H^{p+q}(G, A\otimes B).$$

Demostración. Para $p = q = 0$, la primera fórmula es inmediata. Para la segunda, sean $a \in A^G$, $b \in B^H$, 0-cociclos representando $\bar a$ y $\bar b$. Se tiene

$$\begin{aligned} \operatorname{cor}(\operatorname{res}(\bar a)\cup \bar b) = \operatorname{cor}(a\otimes b + \mathrm{N}_H(A\otimes B)) &= \sum_{\sigma\in G/H} \sigma(a\otimes b) + \mathrm{N}_G(A\otimes B) \\ &= \sum_{\sigma\in G/H} (a\otimes \sigma(b)) + \mathrm{N}_G(A\otimes B) \quad (a \text{ es } G\text{-invariante}) \\ &= a\otimes \Big(\sum_{\sigma\in G/H} \sigma(b)\Big) + \mathrm{N}_G(A\otimes B) = \bar a\cup \operatorname{cor}(\bar b). \end{aligned}$$

El caso general se sigue por cambio de dimensión. □

Similarmente, el siguiente resultado es inmediato para $p = q = 0$ y el caso general se sigue por cambio de dimensión.

Teorema 4.9.8. *Sean* $\bar{a} \in H^p(G, A)$, $\bar{b} \in H^q(G, B)$, $\bar{c} \in H^r(G, C)$. *Entonces*

$$\bar{a} \cup \bar{b} = (-1)^{pq}(\bar{b} \cup \bar{a}) \in H^{p+q}(G, A \otimes B),$$

y

$$(\bar{a} \cup \bar{b}) \cup c = \bar{a} \cup (\bar{b} \cup \bar{c}) \in H^{p+q+r}(G, A \otimes (B \otimes C)). \qquad \square$$

Sean a_p y b_q un p-cociclo de A y un q-cociclo de B respectivamente y sean $\bar{a}_p$, $\bar{b}_q$ sus clases de cohomología en $H^p(G, A)$ y $H^q(G, B)$ respectivamente.

Lema 4.9.9. *Si* $\bar{x}_0 = \bar{a}_1 \cup \bar{b}_{-1} \in H^0(G, A \otimes B)$, *entonces*

$$x_0 = \sum_{\sigma \in G} a_1(\sigma) \otimes \sigma(b_{-1}), \quad \bar{b}_{-1} \in H^{-1}(G, B) = \frac{\text{núc}\, \mathrm{N}_B}{I_G B}.$$

Demostración. Sean $A' := \mathbb{Z}[G] \otimes A$ el G-módulo inducido, $A'' = J_G \otimes A$ y las sucesiones exactas ($A \cong \mathbb{Z} \otimes A$ y si un G-módulo es $\mathbb{Z}$-libre, preserva exactitud como $\mathbb{Z}$-módulos y por tanto como G-módulos)

$$0 \longrightarrow A \longrightarrow A' \longrightarrow A'' \longrightarrow 0,$$
$$0 \longrightarrow A \otimes B \longrightarrow A' \otimes B \longrightarrow A'' \otimes B \longrightarrow 0.$$

Ahora bien $H^1(G, A') = 0 = \frac{Z^1(G,A')}{B^1(G,A')}$ y $A \subseteq A'$, así que existe una 0-cadena $a'_0 \in A'$ con $a_1 = \partial a'_0$ y $a_1(\sigma) = \sigma a'_0 - a'_0$ para toda $\sigma \in G$. Sea $a''_0 \in (A'')^G$ la imagen de a'_0 en A''. El mapeo de conexión δ satisface $\bar{a}_1 = \delta(a''_0)$ y obtenemos por el Teorema 4.9.2 y por (4.6.3)

$$\begin{aligned}
\bar{a}_1 \cup \bar{b}_{-1} &= \delta(\overline{a''_0}) \cup \bar{b}_{-1} = \delta(\overline{a''_0} \cup \bar{b}_{-1}) = \delta(\overline{a''_0 \otimes b_{-1}}) = \partial(\overline{a'_0 \otimes b_{-1}}) \\
&= \overline{\mathrm{N}_G(a'_0 \otimes b_{-1})} = \overline{\sum_{\sigma \in G} \sigma(a'_0) \otimes \sigma(b_{-1})} \underset{\substack{\uparrow \\ a_1(\sigma) = \sigma(a'_0) - a'_0}}{=} \\
&= \overline{\sum_{\sigma \in G} (a_1(\sigma) + a'_0) \otimes \sigma(b_{-1})} = \overline{\sum_{\sigma \in G} (a_1(\sigma) \otimes \sigma(b_{-1})} + \overline{a'_0 \otimes \mathrm{N}_G\, b_{-1}} \\
&= \overline{\sum_{\sigma \in G} (a_1(\sigma) \otimes \sigma(b_{-1}))},
\end{aligned}$$

puesto que $\mathrm{N}_G\, b_{-1} = 0$. $\square$

Tomemos ahora $B = \mathbb{Z}$ e identificamos $A \otimes \mathbb{Z} \xrightarrow{\cong} A$, $a \otimes n \longmapsto na$. Recordemos que $H^{-2}(G, \mathbb{Z}) \cong G/G' \cong G^{\text{ab}}$. Si $\sigma \in G$, sea $\bar{\sigma}$ el elemento de $H^{-2}(G, \mathbb{Z})$ que corresponde a $\sigma G' \in G^{\text{ab}}$.

Lema 4.9.10. $\bar{a}_1 \Cup \bar{\sigma} = \overline{a_1(\sigma)} \in H^{-1}(G, A)$.

Demostración. De la sucesión exacta $0 \longrightarrow A \otimes I_G \longrightarrow A \otimes \mathbb{Z}[G] \longrightarrow A \longrightarrow 0$ y de que $A \otimes \mathbb{Z}[G]$ es cohomológicamente trivial, se sigue que $H^{-1}(G, A) \xrightarrow[\cong]{\delta} H^0(G, A \otimes I_G)$. Por tanto basta probar que $\delta(\bar{a}_1 \Cup \bar{\sigma}) = \delta(\overline{a_1(\sigma)})$.

Usando la definición de δ (ver Corolario 4.3.6), se tiene $\delta(\overline{a_1(\sigma)}) = \bar{x}_0$ con $x_0 = \sum_{\theta \in G} \theta a_1(\sigma) \otimes \theta$.

Por otro lado, bajo el isomorfismo $H^{-2}(G, \mathbb{Z}) \xrightarrow{\delta} H^{-1}(G, I_G)$, el elemento $\bar{\sigma}$ va a $\delta(\bar{\sigma}) = \overline{\sigma - 1}$, por lo que

$$\delta(\bar{a}_1 \Cup \bar{\sigma}) = -(\bar{a}_1 \Cup \delta(\bar{\sigma}) = -\bar{a}_1 \Cup (\overline{\sigma - 1}) = \bar{y}_0.$$

Por el Lema 4.9.9, se tiene

$$y_0 = -\sum_{\theta \in G} a_1(\theta) \otimes \theta(\sigma - 1) = \sum_{\theta \in G} a_1(\theta) \otimes \theta - \sum_{\theta \in G} a_1(\theta) \otimes \theta\sigma.$$

El 1-cociclo $a_1(\theta)$ satisface $a_1(\theta) = a_1(\theta\sigma) - \theta a_1(\sigma)$, por lo que $y_0 = \sum_{\theta \in G} \theta a_1(\sigma) \otimes \theta\sigma$.

Por tanto $y_0 - x_0 = \sum_{\theta \in G} \theta a_1(\sigma) \otimes \theta(\sigma - 1) = \mathrm{N}_G(a_1(\sigma) \otimes (\sigma - 1))$, esto es, $\bar{x}_0 = \bar{y}_0$ y el resultado se sigue. □

Sea $\bar{a}_2 \in H^2(G, A)$. Se obtiene un homomorfismo

$$\varphi = \bar{a}_2 \Cup \_ \colon H^{-2}(G, \mathbb{Z}) \longrightarrow H^0(G, A) (= H^{2-2=0}(G, A \otimes \mathbb{Z})),$$

dada por $\varphi(\bar{\sigma}) = \bar{a}_2 \Cup \bar{\sigma} \in H^0(G, A)$,

$$\varphi \colon G/G' \cong G^{\mathrm{ab}} \longrightarrow A^G / \mathrm{N}_G\, A.$$

Por teoría de campos de clase, se seleccionarán módulos A tales que φ es un isomorfismo de grupos. Esto es, el teorema principal de teoría de campos de clase es $G^{\mathrm{ab}} \cong A^G / \mathrm{N}_G\, A$.

Proposición 4.9.11. *Se tiene* $\bar{a}_2 \Cup \bar{\sigma} = \overline{\sum_{\sigma \in G} a_2(\theta, \sigma)} \in H^0(G, A)$, *donde* $\bar{\sigma} \in G/G'$.

Demostración. Sea $B = \mathbb{Z}[G] \otimes A$ y $C = J_G \otimes A$. Entonces se tiene la sucesión G-exacta $0 \longrightarrow A \longrightarrow B \longrightarrow C \longrightarrow 0$. Ahora bien, por ser B un G-módulo inducido y como $a \in A \subseteq B$, existe una 1-cocadena $b \in B$ con $a_2 = \partial b$, es decir, se tiene

$$a_2(\theta, \sigma) = \theta b(\sigma) - b(\theta\sigma) + b(\theta). \tag{4.9.15}$$

La imagen c de b es un 1-cociclo de C tal que $\bar{a}_2 = \delta(c)$. Por tanto

$$\bar{a}_2 \Cup \bar{\sigma} \underset{\substack{\uparrow \\ \text{definición de} \\ \text{producto copa}}}{\cong} \delta(\bar{c}) \Cup \bar{\sigma} = \delta\big(\bar{c} \Cup \bar{\sigma}\big) \underset{\substack{\uparrow \\ \text{Lema 4.9.10}}}{\cong} \delta\big(\overline{c(\sigma)}\big) = \overline{a_2(\sigma)} = \overline{\partial(b(\sigma))}$$

$$\underset{\substack{\uparrow \\ (4.6.4)}}{\cong} \overline{\sum_{\theta\in G} \theta b(\sigma)} \underset{\substack{\uparrow \\ (4.9.15)}}{\cong} \overline{\sum_{\theta\in G} a_2(\theta,\sigma)} + \overline{\sum_{\theta\in G} b(\theta\sigma) - \sum_{\theta\in G} b(\theta)}$$

$$= \overline{\sum_{\theta\in G} a_2(\theta,\sigma)}. \qquad \square$$

Definimos el cociente de Herbrand para la cohomología de grupos cíclicos finitos. Esta definición se puede extender a endomorfismos.

Definición 4.9.12. Sea A un grupo abeliano y sean f y g dos endomorfismos de A tales que $f\circ g = g\circ f = 0$, esto es, $\operatorname{im} g \subseteq \operatorname{núc} f$ y $\operatorname{im} f \subseteq \operatorname{núc} g$. Entonces se define el *cociente de Herbarand*

$$q_{f,g}(A) = \frac{[\operatorname{núc} f : \operatorname{im} g]}{[\operatorname{núc} g : \operatorname{im} f]}$$

si ambos índices son finitos.

Se tiene que $q_{f,g}(A) = q_{g,f}(A)^{-1}$. Esta definición generaliza la definición anterior de cociente de Herbrand pues si G es cíclico de orden n, generado por σ y si $f = \sigma - 1 = D$ y $g = 1 + \sigma + \cdots + \cdots + \sigma^{n-1} = \mathrm{N}$, $\mathrm{N}\circ D = D \circ N = \sigma^n - 1 = 0$ y $\operatorname{núc} f = A^G$, $\operatorname{im} g = \mathrm{N}_G A$, $\operatorname{núc} g = {}_{\mathrm{N}_G}A$ y $\operatorname{im} D = I_G A$, por lo que

$$h(A) = q_{D,N}(A) = \frac{|H^0(G,A)|}{|H^{-1}(G,A)|} = \frac{|H^2(G,A)|}{|H^1(G,A)|}.$$

También se tiene que si G es un grupo cíclico de orden n y G actúa trivialmente en el grupos abeliano A, entonces

$$h(A) = q_{0.n}(A).$$

Si A es finito, se tiene $q_{f,g}(A) = 1$.

Lema 4.9.13. *Si f, g son dos endomorfismos de un grupo abeliano A con $f\circ g = g\circ f = 0$, entonces $q_{0,fg}(A) = q_{0,f}(A)q_{0,g}(A)$, donde fg denota multiplicación.*

Demostración. El diagrama

$$\begin{array}{ccccccccc}
0 & \longrightarrow & g(A)\cap \operatorname{núc} f & \xrightarrow{\ i\ } & g(A) & \xrightarrow{\ f\ } & (fg)(A) & \longrightarrow & 0 \\
 & & \downarrow{\scriptstyle i} & & \downarrow{\scriptstyle i} & & \downarrow{\scriptstyle i} & & \\
0 & \longrightarrow & \operatorname{núc} f & \xrightarrow{\ i\ } & A & \xrightarrow{\ f\ } & f(A) & \longrightarrow & 0
\end{array}$$

es conmutativo con filas exactas. Por el Lema de la Serpiente, la sucesión

$$0 \longrightarrow \frac{\text{núc}\, f}{g(A) \cap \text{núc}\, f} \longrightarrow \frac{A}{g(A)} \longrightarrow \frac{f(A)}{(fg)(A)} \longrightarrow 0$$

es exacta y por tanto

$$\frac{[A : (fg)(A)]}{[A : f(A)]} = \frac{[A : g(A)]|g(A) \cap \text{núc}\, f|}{|\,\text{núc}\, f|}.$$

Ahora,

$$\frac{\text{núc}\, fg}{\text{núc}\, g} = \frac{g^{-1}(g(A) \cap \text{núc}\, f)}{g^{-1}(0)} \cong g(A) \cap \text{núc}\, f$$

por lo que

$$\frac{[A : (gf)(A)]}{|\,\text{núc}\, gf|} = \frac{[A : g(A)]}{|\,\text{núc}\, g|} \cdot \frac{[A : f(A)]}{|\,\text{núc}\, f|}. \qquad \square$$

Teorema 4.9.14 (Tate). *Sea G un grupo cíclico de orden p, p un número primo y sea A un G-módulo. Si $q_{0,p}(A)$ está definido, entonces $q_{0,p}(A^G)$ y $h(A)$ están también definidos y*

$$h(A)^{p-1} = \frac{q_{0,p}(A^G)^p}{q_{0,p}(A)}.$$

Demostración. Sean σ un generador de G y $D = \sigma - 1$. Consideremos la sucesión exacta $0 \longrightarrow A^G \longrightarrow A \xrightarrow{D} I_G A \longrightarrow 0$.

Puesto que $I_G A$ es un subgrupo y también un grupo cociente de A, se sigue que si $q_{0,p}(A)$ está definido, entonces $q_{0,p}(I_G A)$ también está definido. Por tanto $q_{0,p}(A^G) = \frac{q_{0,p}(A)}{q_{0,p}(I_G A)}$ está definido.

Ahora bien, G actúa trivialmente en A^G por lo que $q_{0,p}(A^G) = h(A^G)$. Se tiene $\mathbb{Z}\,\mathrm{N}_G = \mathbb{Z}\big(\sum_{i=0}^{p-1} \sigma^i\big)$ anula a $I_G A$ y por tanto $I_G A$ es un $/_{\mathfrak{g}\mathfrak{e}}\mathbb{Z}\,\mathrm{N}_G$-módulo. Como anillos tenemos el isomorfismo

$$\mathbb{Z}[G]/\mathbb{Z}\,\mathrm{N}_G \underset{\sigma \leftrightarrow x}{\overset{\cong}{\uparrow}} \mathbb{Z}[x]/\langle 1 + x + \cdots + x^{p-1}\rangle \cong \mathbb{Z}[\zeta_p],$$

el anillo de enteros de $\mathbb{Q}(\zeta_p)$, $\zeta_p = e^{2\pi i/p}$. El isomorfismo está inducido por el mapeo $\sigma \mapsto \zeta_p$. Se tiene que en $\mathbb{Z}[\zeta_p]$, $p = (\zeta_p - 1)^{p-1}u$ con u una unidad de $\mathbb{Z}[\zeta_p]$. Por tanto $p = (\sigma - 1)^{p-1}v$, donde v es una unidad de $\mathbb{Z}[G]/\mathbb{Z}\,\mathrm{N}_G$.

Ahora $v\colon I_G A \longrightarrow I_G A$, $x \longmapsto vx$ es un automorfismo, por lo que $q_{0,v}(I_G A) = 1$. Por tanto

$$q_{0,p}(I_G A) = q_{0,D^{p-1}}(I_G A) q_{0,v}(I_G A) = q_{0,D}(I_G A)^{p-1} = \frac{1}{q_{D,0}(I_G A)^{p-1}}.$$

Ahora, se tiene $\mathrm{N}_G(I_G A) = 0$, por lo que

$$q_{0,p}(I_GA) = \frac{1}{q_{D,0}(I_GA)^{p-1}} = \frac{1}{q_{D,\mathrm{N}}(I_GA)^{p-1}} = \frac{1}{h(I_GA)^{p-1}}.$$

Como $q_{0,p}(A) = q_{0,p}(A^G)q_{0,p}(I_GA)$, se sigue que

$$q_{0.p}(A^G) = h(A^G), \quad q_{0,p}(I_GA) = \frac{1}{h(I_GA)^{p-1}}, \quad q_{0,p}(A) = \frac{q_{0,p}(A^G)}{h(I_GA)^{p-1}}$$

y también

$$h(A)^{p-1} = h(A^G)^{p-1}h(I_GA)^{p-1},$$

por lo que

$$h(A)^{p-1} = \frac{q_{0,p}(A^G)^{p-1}q_{0,p}(A^G)}{q_{0,p}(A)} = \frac{q_{0,p}(A^G)^p}{q_{0,p}(A)}. \qquad \square$$

4.9.1. Cohomología trivial y Teorema de Tate

Recordemos que A es *cohomológicamente trivial* si $H^q(H, A) = 0$ para todo $q \in \mathbb{Z}$ y para todo subgrupo H de G.

Teorema 4.9.15. *Sean G un grupo finito y A un G–módulo. Si existen dos enteros consecutivos q_0, $q_0 + 1$ tales que $H^{q_0}(H, A) = H^{q_0+1}(H, A) = 0$ para todo subgrupo H de G, entonces A es cohomológicamente trivial.*

Demostración. Primero veamos que $H^{q_0-1}(H, A) = H^{q_0+2}(H, A) = \{0\}$ para todo subgrupo de G. Una vez probado esto, el resultado es inmediato.

Para la demostración de lo anterior, aplicamos el cambio de dimensión, es decir, si tenemos lo anterior para $q_0 = 1$, esto es, $H^0(H, A) = H^3(H, A) = 0$ para todo subgrupo H de G, veamos que se cumple para q_0 arbitrario.

Por cambio de dimensión tenemos que $H^1(H, A^{q_0-1}) \cong H^{q_0}(H, A) = 0$ y $H^2(H, A^{q_0-1}) \cong H^{q_0+1}(H, A) = 0$, por lo que $H^{q_0-(q_0-1)}(H, A^{q_0-1}) \cong H^{q_0}(H, A) = 0$ para toda $q_0 \in \mathbb{Z}$.

Así, supongamos que $H^1(H, A) = H^2(H, A) = 0$ para todo subgrupo H de G y queremos probar que

$$H^0(H, A) = H^3(H, A) = 0 \quad \text{para todo } H < G. \tag{4.9.16}$$

Probaremos (4.9.16) por inducción en $|G|$, siendo el caso $G = 1$ trivial. Supongamos probado (4.9.16) para todo subgrupo H de G tal que $H \neq G$. Por tanto, basta probar que $H^0(G, A) = H^3(G, A) = 0$. Si G no es un p-grupo, todos los subgrupos de Sylow de G son propios y satisfacen (4.9.16), por lo que (4.9.16) se sigue para $H = G$ (Corolario 4.8.4).

Supongamos entonces que G es un p-grupo. Sea $H \triangleleft G$ tal que G/H es cíclico de orden p. Por hipótesis de inducción, se tiene $H^0(H, A) = H^3(H, A) = 0$ y $H^1(H, A) = H^2(H, A) = 0$.

Para $q = 1, 2, 3$, $\inf\colon H^q(G/H, A^H) \longrightarrow H^q(G, A)$ es un isomorfismo pues $0 \longrightarrow H^1(G/H, A^H) \xrightarrow{\inf} H^1(G, A) \xrightarrow{\text{res}} H^1(H, A) = 0$ es exacta y como $H^i(H, A) = 0$ para $i = 1, \ldots, q-1$, $0 \longrightarrow H^q(G/H, A^H) \xrightarrow{\inf} H^q(G, A) \xrightarrow{\text{res}} H^q(H, A) = 0$.

De esta forma, obtenemos que $H^1(G, A) = 0$ implica $H^1(G/H, A^H) = 0$ y $H^3(G/H, A^H) = 0$ por ser G/H un grupo cíclico. Ahora bien, $H^2(G, A) = 0$ implica $H^2(G/H, A^H) = 0$, por lo que

$$H^0(G/H, A^H) = 0 = \frac{(A^H)^{G/H}}{\mathrm{N}_{G/H}\, A^H} = \frac{A^G}{\mathrm{N}_{G/H}\, A^H},$$

esto es, $A^G = \mathrm{N}_{G/H}\, A^H \underset{\substack{H^0(H,A)=0 \\ A^H = \mathrm{N}_H A}}{\overset{\uparrow}{\cong}} \mathrm{N}_{G/H}(\mathrm{N}_H\, A) = \mathrm{N}_G\, A$. De esta forma se obtiene que $H^0(G, A) = 0$ y el resultado se sigue. □

Observación 4.9.16. Pueden existir grupos de cohomología $H^{q_0}(G, A) = H^{q_0+1}(G, A) = 0$ pero A no ser cohomológicamente trivial.

Ejemplo 4.9.17. Sean $G = \mathbb{Z}/6\mathbb{Z}$ y $A = \mathbb{Z}/3\mathbb{Z}$ con acción $g \circ a = 2^g a$ donde consideramos a a y a $g \in \mathbb{Z}$ (en particular $3a = 0$, etc. y $0^0 = 1$).

Entonces, $H^{-1}(G, A) = H^0(G, A) = 0$ pero $H^0(H, A) = A \neq 0$, donde $H = \{0, 2, 4\}$.

Teorema 4.9.18. *Si G es un p–grupo finito, donde p es un número primo, y A es un G–módulo sin p–torsión, entonces lo siguiente es equivalente:*

(1) *$H^i(G, A) = H^{i+1}(G, A) = 0$ para dos enteros consecutivos $i, i+1$.*
(2) *A es cohomológicamente trivial.*
(3) *El $\mathbb{F}_p[G]$–módulo A/pA es libre.*

Demostración. [117, Theorem 7.1, Part I], [151, Theorem 6, Ch. IX]. □

Consideremos el producto copa $H^p(G, A) \times H^q(G, B) \xrightarrow{\Cup} H^{p+q}(G, A \otimes B)$ para dos G-módulos, A y B y, como siempre, $A \otimes B = A \otimes_{\mathbb{Z}} B$. Fijemos un elemento $a \in H^p(G, A)$ y consideremos el mapeo $a \Cup \_\colon H^q(G, B) \longrightarrow H^{p+q}(G, A \otimes B)$, $b \longmapsto a \Cup b$ donde $b \in H^q(G, B)$.

Teorema 4.9.19 (axioma de la teoría de campos de clase). *Sea G un grupo finito y sea A un G–módulo tal que para todo subgrupo $H < G$ se tiene*

(1) *$H^{-1}(H, A) = 0$,*
(2) *$H^0(H, A)$ es un grupo cíclico de orden $|H|$.*

Entonces, si a genera $H^0(H, A)$, el producto copa

$$a \Cup \_\colon H^q(G, \mathbb{Z}) \longrightarrow H^q(G, A)$$

es un isomorfismo para toda $q \in \mathbb{Z}$ ($A \cong \mathbb{Z} \otimes A$).

Demostración. Sea $B = A \oplus \mathbb{Z}[G]$. Puesto que $\mathbb{Z}[G]$ es cohomológicamente trivial, se tiene que $H^q(H,B) = H^q(H,A)$ para todo subgrupo $H < G$ y para todo $q \in \mathbb{Z}$.

Puesto que $H^0(G,A) = A^G/\operatorname{N}_G A \cong C_{|H|}$, seleccionamos $a_0 \in A^G$ tal que $a = a_0 + \operatorname{N}_G A$ es un generador de $H^0(G,A)$. El mapeo $f\colon \mathbb{Z} \longrightarrow B$ dado por $m \longmapsto (ma_0, \operatorname{N}_G \cdot m)$ es inyectivo pues el segundo término satisface $\operatorname{N}_G \cdot m = 0 \iff m = 0$.

Sea $\tilde{f}\colon H^q(H,\mathbb{Z}) \longrightarrow H^q(G,B)$ el homomorfismo inducido por f. Sea $\imath\colon A \longrightarrow B$ el encaje $\imath(a) = (a,0)$. Entonces, por ser $\mathbb{Z}[G]$ cohomológicamente trivial, $\imath$ induce el isomorfismo $\bar{\imath}\colon H^q(H,A) \longrightarrow H^q(G,B)$. Recordemos que para x_p, y_q un p-cociclo y un q-cociclo respespectivamente, $\bar{x}_0 \cup \bar{y}_q = \overline{x_0 \otimes y_q}$ y $\bar{x}_p \cup \bar{y}_0 = \overline{x_p \otimes y_0}$, por lo que el diagrama

$$\begin{array}{ccc} H^q(G,\mathbb{Z}) & \xrightarrow{a\cup -} & H^q(G,A) \\ & \searrow^{\bar{f}} & \downarrow{\scriptstyle \bar{\imath}} \\ & & H^q(G,B) \end{array}$$

es conmutativo. Así, es suficiente probar que $\bar{f}$ es biyectivo.

Se tiene que $f\colon \mathbb{Z} \longrightarrow B$ es inyectivo, lo cual da lugar a una sucesión exacta

$$0 \longrightarrow \mathbb{Z} \xrightarrow{f} B \xrightarrow{\varphi} C \longrightarrow 0. \tag{4.9.17}$$

Se tiene $H^{-1}(H,B) = H^{-1}(H,A) = 0$ y $H^1(H,\mathbb{Z}) = 0$ para todo subgrupo $H < G$. Usando el Teorema 4.1.13 y la sucesión exacta (4.9.17) obtenemos

$$\begin{aligned} H^{-1}(H,B) = 0 \longrightarrow H^{-1}(H,C) \longrightarrow H^0(H,\mathbb{Z}) &\xrightarrow{\bar{f}} H^0(H,B) \\ &\xrightarrow{\bar{\varphi}} H^0(H,C) \longrightarrow H^1(H,\mathbb{Z}) = 0. \end{aligned}$$

Para $q = 0$, $H^0(H,\mathbb{Z}) \xrightarrow{\bar{f}} H^0(H,B)$ está dado por

$$\begin{aligned} \bar{f}\colon \mathbb{Z}^H/\operatorname{N}_H \mathbb{Z} \cong \mathbb{Z}/|H|\mathbb{Z} &\longrightarrow H^0(H,A) \\ m &\longmapsto ma_0 \end{aligned}$$

por lo que $\bar{f}$ es un isomorfismo para $q = 0$. Se sigue que $\operatorname{núc} \bar{f} = H^{-1}(H,C) = 0$ e $\operatorname{im} \bar{f} = H^0(H,B) = \operatorname{núc} \varphi$, por lo que $\varphi = 0$

Por tanto, $H^{-1}(H,C) = H^0(H,C) = \{0\}$ para todo subgrupo $H < G$. Por el Teorema 4.9.15, se sigue que C es cohomológicamente trivial. Se sigue de (4.9.17) que $\bar{f}\colon H^q(G,\mathbb{Z}) \longrightarrow H^q(G,B)$ es biyectivo para toda $q \in \mathbb{Z}$ de donde se sigue el resultado. □

Teorema 4.9.20 (Teorema de Tate-Nakayama). *Sea G un grupo finito y A un G–módulo tal que para todo subgrupo $H < G$ se tiene*

(1) $H^1(H,A)=0$ *y*
(2) $H^2(H,A)$ *es cíclico de orden* $|H|$.

Entonces si a *es un generador de* $H^2(G,A)$*, el mapeo*

$$a \cup \_ \colon H^q(G,\mathbb{Z}) \longrightarrow H^{q+2}(G,A)$$

es un isomorfismo donde $\mathbb{Z}$ *es un* G*–módulo con acción trivial.*

Además $\operatorname{res} a \in H^2(H,A)$ *genera al grupo* $H^2(H,A)$ *por lo que tenemos el isomorfismo* $\operatorname{res} a \cup \_ \colon H^q(H,\mathbb{Z}) \longrightarrow H^{q+2}(H,A)$.

Demostración. Consideremos el isomorfismo $\mu^2 \colon H^q(H,A^2) \longrightarrow H^{q+2}(H,A)$. Se tiene $H^{-1}(H,A^2)=H^1(H,A)=0$ y $H^0(H,A^2)$ es cíclico de orden $|H|$. Además, el generador $a \in H^2(G,A)$ es la imagen del generador $\mu^{-2}a \in H^0(G,A^2)$.

Por el Teorema 4.9.2 se tiene el diagrama conmutativo

$$\begin{array}{ccc} H^q(G,\mathbb{Z}) & \xrightarrow{\mu^{-2}a\cup\_} & H^q(G,A^2) \\ {\scriptstyle \mathrm{Id}}\downarrow & & \downarrow{\scriptstyle \mu^2} \\ H^q(G,\mathbb{Z}) & \xrightarrow{a\cup\_} & H^{q+2}(G,A). \end{array}$$

Puesto que $\mu^{-2}a \cup \_$ es una biyección, se sigue del Teorema 4.9.19 que $a \cup \_$ es un isomorfismo.

Ahora bien, puesto que $(\operatorname{cor}\circ\operatorname{res})a=[G:H]a$, el orden del elmento $\operatorname{res} a \in H^2(H,A)$ es divisible por $|H|$, por lo que $\operatorname{res} a$ genera $H^2(H,A)$ por (2). □

Observación 4.9.21. Para la teoría de campos de clase, el caso $q=-2$ en el Teorema de Tate-Nakayama es particularmente importante.

Aplicamos el Teorema de Tate-Nakaya para $q=-2$ y obtenemos en este caso que $H^{-2}(G,\mathbb{Z}) \cong G/G' = G^{\mathrm{ab}}$ de G y el grupo residual nórmico $H^0(G,A)=A^G/\operatorname{N} A$ y un isomorfismo

$$G^{\mathrm{ab}} \xrightarrow{\cong} A^G/\operatorname{N} A.$$

Este isomorfismo es la formulación abstracta del teorema principal en la teoría de campos de clase y se llama la *Ley de Reciprocidad*. El resultado se aplica a los siguientes casos: L/K es una extensión finita de Galois y $G=\operatorname{Gal}(L/K)$

(1) $A=L^*$ donde L/K es una extensión finita de campos locales.
(2) $A=J_L/L^*$ donde J_L/L^* es el *grupo de clases idèles* de un campo global L.
(3) $A=I_L$ donde I_L es el grupo de *clases de ideales o de divisores* de un campo de números o de un campo de funciones congruente.

5

Campos de clase locales

5.1. Cohomología de grupos profinitos

Recordemos, [136, Definición 2.11], que un grupo topológico G se llama *profinito* si G es Hausdorff compacto y tiene una base de vecindades abiertas de la identidad $1 \in G$ consistente de subgrupos normales.

Sean $x \in G$ y V un conjunto abierto con $x \in V$, entonces existe $H \triangleleft G$, H abierto en G, tal que $xH \subseteq V$. Ahora si $\{\xi_i\}_{i\in I}$ es un conjunto de representantes de G/H, $G = \cup_{i\in I}\xi_i H$ y $\xi_i H$ es un conjunto abierto con $\xi H \cap \xi_j H = \emptyset$, para $i \neq j$ y G compacto, por lo que $[G : H] < \infty$ y $H = G\backslash \cup_{\substack{i\in I\\ i\neq 1}} \xi_i H$ es cerrado.

Ahora si $x \neq 1$, existen conjuntos abiertos U y V tales que $1 \in U$, $x \in V$ y $U \cap V = \emptyset$. Sea $N \triangleleft G$, $N \subseteq U$, donde N es un conjunto abierto. Entonces $1 \in N$ y $G = \big(\bigcup_{g\neq N} gN\big) \cup N$. Por tanto $x \in W = \bigcup_{g\neq N} gN$ y $W \cap N = \emptyset$. Se sigue que W y N es una disconexión de G y por tanto la componente conexa de 1 es $\{1\}$ y por tanto G es totalmente disconexo. El recíproco también se cumple.

En resumen, se tiene G es profinito $\iff$ G es compacto, Hausdorff y totalmente disconexo. Además,

$$G = \varprojlim_{\substack{N\triangleleft G\\ N \text{ abierto}}} G/N \qquad ([136, \text{Teorema } 2.1.13])$$

tanto topológica como algebraicamente. Notemos que G/N es finito y que N es abierto.

Si L/K es una extensión de Galois de campos no necesariamente finita, $L = \bigcup_\alpha K(\alpha)$, donde $K(\alpha)/K$ es normal. De hecho, $L = \bigcup_{\alpha\in L} K(\alpha)$, $\alpha \in L$ por lo que α es algebraico y $K(\alpha)/K$ es una extensión finita. Si $\widetilde{K(\alpha)}$ es la cerradura normal de $K(\alpha)/K$, $\widetilde{K(\alpha)} = K(\tilde{\alpha})$ es una extensión finita y $L = \bigcup_{\tilde{\alpha}} K(\tilde{\alpha})$.

Ahora $K(\alpha)/K$ normal, $K(\alpha) = L^H$ con $H \triangleleft \mathrm{Gal}(L/K)$. Damos a G la topología de Krull: una base de vecindades abiertos de $g \in G$ es $\{gH\}_{\substack{H \triangleleft G \\ [G:H]<\infty}}$. Entonces G es compacto y Hausdorff por lo que G es profinito.

En particular, los grupos de Galois son grupos profinitos:

$$G = \mathrm{Gal}(L/K) = \varprojlim_{\substack{N \triangleleft G \\ N \text{ abierto}}} G/N = \varprojlim_{\substack{K(\alpha)/K \\ \text{normal}}} \mathrm{Gal}(K(\alpha)/K)$$

y $L = \bigcup_\alpha K(\alpha) = \varinjlim_\alpha K(\alpha)$.

En otras palabras $\mathrm{Gal}\left(\varinjlim_\alpha K(\alpha)/K\right) = \varprojlim_\alpha \mathrm{Gal}(K(\alpha)/K)$.

Ahora bien, los subgrupos abiertos H de G son de índice finito y por tanto son cerrados y recíprocamente, los subgrupos cerrados de índice finito son abiertos. Se tiene que existen conjuntos subgrupos cerrados que no son de índice finito y por tanto no son abiertos.

Si G es un grupo pro-finito y A es un G-módulo discreto, esto es, A tiene la topología discreta, A es un G-módulo si la acción de G-módulo usual $G \times A \longrightarrow A$ es continua. Esto es equivalente a que $A = \bigcup_N A^N$ donde N recorre los subgrupos abiertos de G.

Definición 5.1.1. Sea $q \geq 0$ y sean $N_1, N_2 \triangleleft G$ subgrupos normales y abiertos de G con $N_1 \subseteq N_2$ y $G/N_1 \longrightarrow G/N_2$ el mapeo natural, $G \cong \varprojlim_N G/N$, $A = \varinjlim_N A^N$. Sea $\inf_{N_2}^{N_1} \colon H^q(G/N_2, A^{N_2}) \longrightarrow H^q(G/N_1, A^{N_1})$ el mapeo inflación. Entonces se define el q-ésimos grupo de cohomología de G en A por

$$H^q(G, A) := \varinjlim_N H^q(G/N, A^N),$$

con respecto a los mapeos inflación.

Usaremos la siguiente notación. Si L/K es una extensión finita de Galois y $G_{L|K} = \mathrm{Gal}(L/K)$, $H^q(G_{L|K}, L^*) = H^q(\mathrm{Gal}(L/K), L^*) =: H^q(L|K)$. Como $H^1(L|K) = \{1\}$, se tiene la sucesión exacta:

$$1 \longrightarrow H^2(L|K) \xrightarrow{\inf_M} H^2(M|K) \xrightarrow{\mathrm{res}_L} H^2(M|L), \quad \text{(Teorema 4.8.9)},$$

con $K \subseteq L \subseteq M$. Puesto que $\inf_M$ es inyectiva, siempre consideraremos $H^2(L|K) \subseteq H^2(M|K)$. Si L recorre todas las extensiones normales y separables de K, $\bigcup_L L = K^{\mathrm{sep}}$ es una cerradura separable de K y ponemos $G_K := \mathrm{Gal}(K^{\mathrm{sep}}/K)$, entonces

$$H^2(G_K, (K^{\mathrm{sep}})^*) =: H^2(\ |K) = \varinjlim_L H^2(L|K) = \bigcup_L H^2(L|K).$$

Definición 5.1.2. El *grupo de Brauer* $\mathrm{Br}(K)$ de un campo K es $\mathrm{Br}(K) = H^2(\ |K) = \bigcup_{\substack{L/K \\ \text{finita Galois}}} H^2(L|K)$.

Sea K'/K una extensión finita de Galois. Sea L/K una extensión finita de Galois y $K' \subseteq L$. La restricción $H^2(\ |K) \xrightarrow{\mathrm{res}_{K'}} H^2(\ |K')$ se define así:

$$\mathrm{res}_{K'}(c) \in H^2(L|K') \subseteq H^2(\ |K').$$

Puesto que la restricción conmuta con inflación, la cual es una inyección, se sigue que $\mathrm{res}_K\, c$ no depende de la elección del campo L.

Proposición 5.1.3. *La sucesión*

$$1 \longrightarrow H^2(K'|K) \xhookrightarrow{i} H^2(\ |K) \xrightarrow{\mathrm{res}_{K'}} H^2(\ |K')$$

es exacta. □

El isomorfismo de Tate-Nakayama: $G^{\mathrm{ab}}_{L|K} \cong A^G/\,\mathrm{N}_{L/K}\, A$ es en cierta forma arbitrario pues depende del generador a de $H^2(G, A)$ seleccionado. Para hacer el mapeo homogéneo con respecto a varias extensiones, la segunda condición del Teorema de Tate-Nakayama, esto es, $H^2(H, A)$ es cíclico de orden $|H|$, se especializa a que hay un isomorfismo entre $H^2(L|K)$ y el grupo cíclico $\left(\frac{1}{[L:K]}\mathbb{Z}\right)/\mathbb{Z}$ el llamado "*mapeo invariante*" $\mathrm{inv}_{L|K}$ que determina un único elemento $u_{L|K} \in H^2(L|K)$ con imagen $\frac{1}{[L:K]} + \mathbb{Z}$, esto es

$$\mathrm{inv}_{L|K} \colon H^2(L|K) \longrightarrow \left(\frac{1}{[L:K]}\mathbb{Z}\right)/\mathbb{Z}, \quad u_{L|K} \longmapsto \frac{1}{[L:K]} + \mathbb{Z}.$$

El elemento $u_{L|K}$ se llama la *clase fundamental de* L/K.

Antes de continuar, veamos algunos ejemplos del grupo de Brauer.

Ejemplo 5.1.4. Si $K = \mathbb{F}_q$ es un campo finito, entonces toda extensión L/K es cíclica, $G = \mathrm{Gal}(L/K)$. Además $H^1(G|L^*) = \{1\}$ y como L^* es finito, el cociente de Herbrand $h(L^*) = 1$, por lo que $H^2(G, L^*) \cong H^0(G, L^*) = \{1\}$, en particular $\mathrm{N}_{L/K}\, L^* = K^*$. Por tanto $\mathrm{Br}(\mathbb{F}_q) = \bigcup_L H^2(L|K) = \bigcup_L \{0\} = \{0\}$. De esta forma obtenemos $\mathrm{Br}(\mathbb{F}_q) = \{0\}$.

Ejemplo 5.1.5. Si $K = \mathbb{R}$, K únicamente tiene dos extensiones algebraicas, $\mathbb{R}$ y $\mathbb{C}$. Por tanto

$$\mathrm{Br}(\mathbb{R}) = H^2(\mathbb{C}|\mathbb{R}) = H^2(G_{L/K}, \mathbb{C}^*) \underset{\substack{\uparrow \\ J\text{conjugación} \\ \text{compleja}}}{\cong} H^2(\{1, J\}, \mathbb{C}^*) = \frac{(\mathbb{C}^*)^{\{1,J\}}}{\{z\bar{z} \mid z \in \mathbb{C}\}}$$

$$= \frac{\mathbb{R}^*}{\mathbb{R}^+} \cong \mathbb{Z}/2\mathbb{Z} \cong \frac{\frac{1}{2}\mathbb{Z}}{\mathbb{Z}} \subseteq \mathbb{Q}/\mathbb{Z}.$$

Ejemplo 5.1.6. El campo de los números complejos no tienen extensiones de Galois propias, por lo tanto $\mathrm{Br}(\mathbb{C}) = \{0\}$. Esto mismo se aplica a cualquier campo algebraicamente cerrado.

Ejemplo 5.1.7. Veremos más adelante que si K es un campo local, entonces $\mathrm{Br}(K) = \mathbb{Q}/\mathbb{Z}$ (Corolario 5.3.5).

Observación 5.1.8. Usaremos el grupo de Brauer de un campo local para hallar un mapeo $\mathrm{inv}_{L|K}\colon H^2(L|K) \longrightarrow \left(\frac{1}{[L:K]}\mathbb{Z}\right)/\mathbb{Z}$ y el elemento $u_{L|K}$ con $\mathrm{inv}_{L|K}(u_{L|K}) = \frac{1}{[L:K]} + \mathbb{Z} \in \mathbb{Q}/\mathbb{Z}$. Este elemento nos dará el mapeo de reciprocidad vía el Teorema de Tate-Nakayam:

$$u_{L|K} \cup \_\colon H^q(G_{L|K}, \mathbb{Z}) \xrightarrow{\cong} H^{q+2}(L|K).$$

Originalmente, el grupo de Brauer fue definido para codificar anillos de división sobre campos, es decir, objetivos no conmutativos, y sirve para hallar la función que nos da la ley de reciprocidad. Este enfoque fue desarrollado por Brauer, Hasse y Noether. De hecho, el grupo de Brauer también describe la correspondencia de los campos de clase para campos globales. El estudio sistemático puede ser consultado en los libros de Serre [151] y de Kato, Kurokawa y Saito [84].

Antes de usar la teoría de cohomología, la teoría de álgebras fue usada para describir la teoría de campos de clase, tanto local como global. Con el uso de la cohomología de grupos, tenemos los mismos resultados de manera mucho más simple. En esta parte describimos la teoría de los grupos de Brauer, pero la descripción del símbolo residual de la norma lo haremos por medio del uso de cohomología. La obtención del símbolo residual de la norma lo haremos en el Teorema 5.3.11.

No daremos detalles de la siguiente discusión. Consideremos E un campo cualquiera. Se define el *grupo de Brauer* $\mathrm{Br}(E)$ de E como el conjunto de clases de E–isomorfismos de anillos de división finito dimensionales sobre E y tales que E es el centro del anillo de división.

En general $\mathrm{Br}(E)$ tiene una estructura de grupo abeliano definido por medio del producto tensorial de álgebras sobre E y es precisamente con esta estructura que se llama *grupo de Brauer*.

Regresamos a nuestro estudio. Consideremos una extensión L/K no ramificada de campos locales. Se tiene $f = [L : K] = [\bar{L} : \bar{K}]$, $e = 1$ y $\mathrm{Gal}(L/K) \cong \mathrm{Gal}(\bar{L}/\bar{K})$. Se tiene un generador de $\mathrm{Gal}(\bar{L}/\bar{K})$ es el *automorfismo de Frobenius* $\varphi_{L|K} \in \mathrm{Gal}(L/K)$ con $\mathrm{Gal}(L/K) \xrightarrow{\cong} \mathrm{Gal}(\bar{L}/\bar{K})$, $\varphi_{L|K} \longmapsto (x \to x^{|\bar{K}|} =: x^{q_K})$, $\bar{K} = \mathbb{F}_{q_K}$ (ver Subsección 2.2).

Se tiene que $\varphi_{L|K}x \equiv x^{q_K} \mod \mathfrak{p}_L$ para toda $x \in \mathcal{O}_L$ y se verifica que $\varphi_{L|K} = \varphi_{M|K}|_L = \varphi_{M|K}G_{M|L} \in G_{L|K}$ con $K \subseteq L \subseteq M$ y $\varphi_{M|L} = \varphi_{M|K}^{[L:K]}$.

Proposición 5.1.9. *Sea L/K una extensión finita de Galois de campos locales con grupo de Galois G. Entonces existe un G-submódulo V de $U_L^{(1)}$ de índice finito (por tanto V también es de índice finito en U_L) tal que V es cohomológicamente trivial.*

Demostración. Sea $\alpha \in L$ tal que $\{\sigma\alpha\}_{\sigma\in G}$ es una base normal de L/K. Sea $a \in K^*$ tal que $a\sigma\alpha \in \mathcal{O}_L$ para toda $\sigma \in G$, esto es, seleccionamos $a \in K^*$ tal que $v_K(a) \geq -v_L(\sigma\alpha)$ para toda $\sigma \in G$. Sea $M := \bigoplus_{\sigma\in G}(a\sigma\alpha)\mathcal{O}_K$. Entonces $M \cong \mathcal{O}_K[G] \cong \mathcal{O}_k \otimes \mathbb{Z}[G]$ es un G-módulo inducido y por tanto cohomológicamente trivial.

Se tiene que $M = \{(a\sigma\alpha\xi_\sigma)_{\sigma\in G} \mid \xi_\sigma \in \mathcal{O}_K\} = \{(m_\sigma)_{\sigma\in G} \mid v_L(m_\sigma) \geq -v_L(a\sigma\alpha)\} = \{(m_\sigma)_{\sigma\in G} \mid v_L(m_\sigma) > -v_L(a\sigma\alpha) - 1\} = \{(m_\sigma)_{\sigma\in G} \mid |m_\sigma|_L < q^{v_L(a\sigma\alpha)+1}\}$. Se sigue que M es abierto en $\mathcal{O}_L$. Puesto que $\mathcal{O}_L$ es compacto, se sigue que $[\mathcal{O}_L : M] < \infty$ y puesto que $\bigcap_{n=1}^{\infty} \pi_K^n \mathcal{O}_L = \{0\}$, existe $m \in \mathbb{N}$ tal que $\pi_K^m \mathcal{O}_L \subseteq M$.

Sea $V_i := 1 + \pi_K^{m+i} M$ el cual es un submódulo de $U_L^{(1)}$ pues $M \subseteq \mathcal{O}_L$. El mapeo $V_i \ni v_i \xrightarrow{\mu} \pi_K^{-m-i}(v_i - 1)$ mód $\pi_K M$ define un mapeo biyectivo $V_i/V_{i+1} \longrightarrow M/\pi_K M$ pues $\operatorname{núc}\mu = V_{i+1}$. Además $V_i/V_{i+1} \cong M/\pi_K M \cong \big(\mathcal{O}_K/\pi_K\big)[G] \cong (\mathcal{O}_K/\pi_K) \otimes \mathbb{Z}[G]$, por lo que tanto V_i/V_{i+1} como $M/\pi_K M$ son finitos y cohomológicamente triviales.

Se tienen sucesiones exactas

$$0 \longrightarrow V_{i-1}/V_i \longrightarrow V_{i-2}/V_i \longrightarrow V_{i-2}/V_{i-1} \longrightarrow 0,$$

donde V_{i-1}/V_i y V_{i-2}/V_{i-1} son finitos y cohomológicamente triviales. Se sigue que V_{i-2}/V_i es finito y cohomológicamente trivial. Por inducción obtenemos que V_1/V_i es finito y cohomológicamente trivial.

Se tiene que $V_1 = \varprojlim_i V_1/V_i$. Por tanto $H^q(H, V_1) = H^q(H, \varprojlim_i V_1/V_i) = \varprojlim_i H^q(H, V_1/V_i) = 0$ para toda $q \in \mathbb{Z}$ y todo subgrupo H de G. De esta froma obtenemos que V_1 es cohomológicamente trivial, $V_1 = 1+\pi_K^{m+1}M$. Finalmente $[U_L^{(1)} : V_1] \leq [\mathfrak{p}_L : \mathfrak{p}_L^{e(m+1)}][\mathcal{O}_L : M] < \infty$, esto es, V_1 es de índice finito en $U_L^{(1)}$, y por tanto también en U_L, y $V = V_1$ es cohomológicamente trivial. □

Como corolario, obtenemos el llamado "*axioma de la teoría de campos de clase locales.*

Teorema 5.1.10 (axioma de la teoría de campos de clase locales). *Sea L/K una extensión cíclica finita de campos locales con grupo de Galois G. Entonces $H^1(G, L^*) = \{1\}$ y $H^0(G, L^*)$ tiene cardinalidad $[L : K] = |G|$.*

Demostración. Por el Teorema 90 de Hilbert se tiene $H^1(G, L^*) = \{1\}$ para G arbitrario, no necesariamente cíclico. Sea $V = V_1$ el submódulo de $U_L^{(1)}$ obtenido en la Proposición 5.1.9. Entonces, por ser V cohmológicamente trivial, $h(V) = 1$. Puesto que $U_L^{(1)}/V$ es finito, $h(U_L^{(1)}/V) = 1$ y puesto que $1 \longrightarrow V \longrightarrow U_L^{(1)} \longrightarrow U_L^{(1)}/V \longrightarrow 1$ es exacta, se sigue que $h(U_L^{(1)}) = 1$. Puesto que $[U_L : U_L^{(n)}] < \infty$ para toda $n \in \mathbb{N}$, se sigue que $h(U_L/U_L^{(n)}) = 1$.

Ahora de la exactitud de la sucesión $1 \longrightarrow U_L^{(n)} \longrightarrow U_L \longrightarrow U_L/U_L^{(n)} \longrightarrow 1$, se obtiene que $h(U_L) = h(U_L^{(n)}) = 1$ para toda $n \in \mathbb{N}$.

Por otro lado, $1 \longrightarrow U_L \longrightarrow L^* \xrightarrow{v_L} \mathbb{Z} \longrightarrow 0$ es exacta y por tanto $h(L^*) = h(\mathbb{Z}) = \frac{|H^0(G,\mathbb{Z})|}{|H^1(G,\mathbb{Z})|} = \frac{|\mathbb{Z}/|G|\mathbb{Z}|}{|\{0\}|} = |G| = [L:K]$. Puesto que $H^1(G,L^*) = 1$, se sigue que $|H^0(G,L^*)| = |G| = [L:K]$ y $H^0(G,L^*) = \frac{(L^*)^G}{\mathrm{N}_{L/K}\, L^*} = \frac{K^*}{\mathrm{N}_{L/K}\, L^*}$. El resultado se sigue. Además, $\left|H^0(G,L^*)\right| = [K^*\colon \mathrm{N}_{L/K}\, L^*] = |G| = [L:K]$. □

Un corolario importante, es el siguiente.

Teorema 5.1.11. *Sea L/K una extensión finita no ramificada de campos locales. Entonces $H^q(G_{L|K}, U_L^{(n)}) = \{1\}$ para toda $q \in \mathbb{Z}$ y para toda $n \in \mathbb{N}\cup\{0\}$. En particular, $\mathrm{N}_{L/K}\, U_L^{(n)} = U_K^{(n)}$ para toda $n \in \mathbb{N} \cup \{0\}$.*

Demostración. Puesto que L/K es no ramificada, se tiene para un elemento primo π_K de K, que

$$v_L(\pi_K) = e(L|K)v_K(\pi_K) = 1 \cdot 1 = 1.$$

Por tanto π_K es un elemento primo de L.

Se tiene la sucesión exacta

$$1 \longrightarrow U_L \longrightarrow L^* \xrightarrow{v_L} \mathbb{Z} \longrightarrow 0.$$

Por otro lado tenemos $H^{-1}(G,\mathbb{Z}) = H^1(G,\mathbb{Z}) = \{0\}$ donde $G = \mathrm{Gal}(L/K)$. Por tanto se obtiene la sucesión en cohomología

$$H^{-1}(G,\mathbb{Z}) = \{0\} \longrightarrow H^0(G,U_L) \longrightarrow H^0(G,L^*) \xrightarrow{\bar{v}_L} H^0(G,\mathbb{Z}) \longrightarrow \cdots,$$

con $\bar{v}_L\colon H^0(G,L^*) = K^*/\,\mathrm{N}_{L/K}\, L^* \longrightarrow \mathbb{Z}/|G|\mathbb{Z} = H^0(G,\mathbb{Z})$, y $\bar{v}_L(\bar{\pi}_K) = \bar{1}$. Por tanto $\bar{v}_L$ es suprayectiva.

Ahora bien, como L/K es cíclica, por el Teorema 5.1.10, obtenemos que $|H^0(G,L^*)| = [L:K] = |H^0(G,\mathbb{Z})|$, de donde se sigue que $\bar{v}_L$ es un isomorfismo. En particular $\mathrm{núc}\,\bar{v}_L = H^0(G,U_L) = \{1\}$. Puesto que $h(U_L) = 1$, se sigue que $H^q(G,U_L) = \{1\}$ para toda $q \in \mathbb{Z}$.

Se tiene la sucesión exacta $1 \longrightarrow U_L^{(1)} \longrightarrow U_L \longrightarrow \tilde{L}^* \longrightarrow 1$. Puesto que $H^{-1}(G,\tilde{L}^*) = \{1\}$ y $h(\tilde{L}^*) = 1$ por $\tilde{L}^*$ finito, se sigue que $\tilde{L}^*$ es cohomológicamente trivial y por tanto $H^q(G,U_L^{(1)}) \cong H^q(G,U_L) = \{1\}$ para toda $q \in \mathbb{Z}$.

En general, para cualquier $n \in \mathbb{N}$, se tiene la sucesión exacta $1 \longrightarrow U_L^{(n+1)} \longrightarrow U_L^{(n)} \longrightarrow \tilde{L} \longrightarrow 0$ y $\tilde{L}$ es cohomológicamente trivial, por lo que $H^q(G,U_L^{(n+1)}) \cong H^q(G,U_L^{(n)}) = \{1\}$ para toda $q \in \mathbb{Z}$ y para toda $n \geq 1$. □

Observación 5.1.12. En general probaremos que $[U_K : \mathrm{N}_{L/K}\, U_L] = e(L|K)$ donde L/K es una extensión abeliana finita de campos locales (ver Corolario 3.4.7).

Consideremos una extensión finita no ramificada de campos locales. Se tiene la sucesión exacta

$$1 \longrightarrow U_L \longrightarrow L^* \xrightarrow{v_L} \mathbb{Z} \longrightarrow 0,$$

y puesto que $H^q(G_{L/K}, U_L) = \{1\}$, $H^q(G_{L/K}, L^*) \cong H^q(G_{L/K}, \mathbb{Z})$. Sea $\bar{v}\colon H^2(G_{L/K}, L^*) \longrightarrow H^2(G_{L/K}, \mathbb{Z})$ el isomorfismo inducido por la valuación.

Ahora, $0 \longrightarrow \mathbb{Z} \longrightarrow \mathbb{Q} \longrightarrow \mathbb{Q}/\mathbb{Z} \longrightarrow 0$ es exacta y $\mathbb{Q}$ es cohomológicamente trivial, de donde obtenemos que el mapeo de conexión $\delta\colon H^q(G_{L/K}, \mathbb{Q}/\mathbb{Z}) \longrightarrow H^{q+1}(G_{L/K}, \mathbb{Z})$ es un isomorfismo. Sea

$$\delta^{-1}\colon H^2(G_{L/K}, \mathbb{Z}) \longrightarrow H^1(G_{L/K}, \mathbb{Q}/\mathbb{Z}) = \mathrm{Hom}(G_{L/K}, \mathbb{Q}/\mathbb{Z}) = \chi(G_{L/K}),$$

el dual de $G_{L/K}$, es decir, el grupo de caracteres de $G_{L/K}$.

Si $\xi \in \chi(G_{L/K})$, se tiene que si $\varphi_{L/K}$ denota al automorfismo de Frobenius de L/K, entonces $\xi(\varphi_{L/K}) \in \left(\frac{1}{[L:K]}\mathbb{Z}\right)/\mathbb{Z} \subseteq \mathbb{Q}/\mathbb{Z}$. Como $\varphi_{L/K}$ genera al grupo $G_{L|K}$, el cual es de orden $[L : K]$, $\chi(G_{L|K}) \underset{\varphi}{\cong} \left(\frac{1}{[L:K]}\mathbb{Z}\right)/\mathbb{Z}$. Esto es, $H^1(G_{L|K}, \mathbb{Q}/\mathbb{Z}) = \chi(G_{L|K}) \xrightarrow{\varphi} \left(\frac{1}{[L:K]}\mathbb{Z}\right)/\mathbb{Z}$. Entonces se define φ para $\xi \in \chi(G_{L|K})$, por $\varphi(\xi) := \xi(\varphi_{L|K})$.

La composición de estos tres isomorfismos nos da el isomorfismo

$$H^2(G_{L|K}, L^*) \xrightarrow{\bar{v}_L} H^2(G_{L|K}, \mathbb{Z}) \xrightarrow{\delta^{-1}} H^1(G_{L|K}, \mathbb{Q}/\mathbb{Z}) \xrightarrow{\varphi} \left(\frac{1}{[L : K]}\mathbb{Z}\right)/\mathbb{Z}.$$

Definición 5.1.13. Se define el *mapeo invariante* para una extensión no ramificada de campos locales L/K

$$\mathrm{inv}_{L|K}\colon H^2(G_{L|K}, L^*) \longrightarrow \left(\frac{1}{[L : K]}\mathbb{Z}\right)/\mathbb{Z},$$

por $\mathrm{inv}_{L|K} = \varphi \circ \delta^{-1} \circ \bar{v}_L$.

Sea K_0 un campo local y sea K_0^{nr} la máxima extensión no ramificada de K_0, es decir, $K_0^{\mathrm{nr}} = \bigcup_L L$, L/K_0 no ramificada.

Definición 5.1.14. El campo K_0^{nr} se llama el *campo de inercia* sobre K_0.

Teorema 5.1.15. *Sean $K_0 \subseteq K \subseteq L \subseteq M \subseteq K_0^{\mathrm{nr}}$. Entonces*

(1) $\mathrm{inv}_{L|K} = \mathrm{inv}_{M|K}\,|_{H^2(L|K)}$.
(2) $\mathrm{inv}_{M|L} \circ \mathrm{res}_L = [L : K]\,\mathrm{inv}_{M|K}$.

Demostración. Para (1), debemos probar que el diagrama

$$\begin{array}{ccc} H^2(L|K) & \xrightarrow{\mathrm{inv}_{L|K}} & \left(\frac{1}{[L:K]}\mathbb{Z}\right)/\mathbb{Z} \subseteq \mathbb{Q}/\mathbb{Z} \\ \Big\downarrow{\scriptstyle i} & & \Big\downarrow{\scriptstyle i} \\ H^2(M|K) & \xrightarrow{\mathrm{inv}_{M|K}} & \left(\frac{1}{[M:K]}\mathbb{Z}\right)/\mathbb{Z} \subseteq \mathbb{Q}/\mathbb{Z} \end{array}$$

es conmutativo. Para ello, se probará que el diagrama

$$\begin{array}{ccccccc}
H^2(L|K) & \xrightarrow{\bar{v}_L} & H^2(G_{L|K},\mathbb{Z}) & \xrightarrow{\delta^{-1}} & H^1(G_{L|K},\mathbb{Q}/\mathbb{Z}) & \xrightarrow{\varphi} & \left(\frac{1}{[L:K]}\mathbb{Z}\right)/\mathbb{Z} \\
\Big\downarrow{\scriptstyle i} & & \Big\downarrow{\scriptstyle \inf} & & \Big\downarrow{\scriptstyle \inf} & & \Big\downarrow{\scriptstyle i} \\
H^2(M|K) & \xrightarrow{\bar{v}_M} & H^2(G_{M|K},\mathbb{Z}) & \xrightarrow{\delta^{-1}} & H^1(G_{M|K},\mathbb{Q}/\mathbb{Z}) & \xrightarrow{\varphi} & \left(\frac{1}{[M:K]}\mathbb{Z}\right)/\mathbb{Z}
\end{array}$$

es conmutativo.

Se verifica que el cuadrado de la izquierda es conmutativo usando la definición de las valuaciones v_L, v_M y del mapeo de inflación inf en los 2-cociclos. Que el cuadro de enmedio es conmutativo se sigue de que inflación y los mapeos de conexión conmutan. Para el cuadro de la derecha, tenemos $\inf\colon H^1(G_{L|K},\mathbb{Q}/\mathbb{Z}) \longrightarrow H^1(G_{M|K},\mathbb{Q}/\mathbb{Z})$ se define en 1-cociclos $Z^1(G_{L|K},\mathbb{Q}/\mathbb{Z}) = \mathrm{Hom}(G_{L|K},\mathbb{Q}/\mathbb{Z})$ (por actuar $G_{L|K}$ en $\mathbb{Q}/\mathbb{Z}$ de manera trivial) así: $\inf(\chi) = \tilde{\chi}$ donde

$$\begin{array}{ccc}
\frac{G_{M|K}}{G_{M|L}} = G_{L|K} & \xrightarrow{\chi} & \mathbb{Q}/\mathbb{Z} \\
\Big\uparrow{\scriptstyle \pi} & \nearrow_{\tilde{\chi}} & \\
G_{M|K} & &
\end{array} \qquad \tilde{\chi}(g) = \chi(gG_{M|L}) = \chi(\bar{g}).$$

Por tanto

$$\begin{aligned}
(\varphi \circ \inf)(\chi) &= \varphi(\tilde{\chi}) = \tilde{\chi}(\varphi_{M|K}), \\
(i \circ \varphi)(\chi) &= i(\varphi(\varphi_{L|K})) = i(\chi(\varphi_{L|K})) = \chi(\varphi_{M|K}|_L) = \tilde{\chi}(\varphi_{M|K}).
\end{aligned}$$

de donde se sigue la conmutatividad del diagrama de la derecha probando (1).

La afirmación en (2) es equivalente a la conmutatividad del diagrama

$$\begin{array}{ccc}
H^2(M|K) & \xrightarrow{\mathrm{inv}_{M|K}} & \left(\frac{1}{[M:K]}\mathbb{Z}\right)/\mathbb{Z} \subseteq \mathbb{Q}/\mathbb{Z} \\
\Big\downarrow{\scriptstyle \mathrm{res}_L} & & \Big\downarrow{\scriptstyle [L:K]} \\
H^2(M|L) & \xrightarrow{\mathrm{inv}_{M|L}} & \left(\frac{1}{[M:L]}\mathbb{Z}\right)/\mathbb{Z} \subseteq \mathbb{Q}/\mathbb{Z}
\end{array}$$

Para esta conmutatividad basta probar la conmutatividad del siguiente diagrama

$$\begin{array}{ccccccc}
H^2(M|K) & \xrightarrow{\bar{v}_M} & H^2(G_{M|K},\mathbb{Z}) & \xrightarrow{\delta^{-1}} & H^1(G_{L|K},\mathbb{Q}/\mathbb{Z}) & \xrightarrow{\varphi} & \left(\frac{1}{[M:K]}\mathbb{Z}\right)/\mathbb{Z} \\
\Big\downarrow{\scriptstyle \mathrm{res}_L} & & \Big\downarrow{\scriptstyle \mathrm{res}} & & \Big\downarrow{\scriptstyle \mathrm{res}} & & \Big\downarrow{\scriptstyle [L:K]} \\
H^2(M|L) & \xrightarrow{\bar{v}_M} & H^2(G_{M|L},\mathbb{Z}) & \xrightarrow{\delta^{-1}} & H^1(G_{M|L},\mathbb{Q}/\mathbb{Z}) & \xrightarrow{\varphi} & \left(\frac{1}{[M:L]}\mathbb{Z}\right)/\mathbb{Z}
\end{array}$$

La conmutatividad del cuadro izquierdo se sigue de la definición de $\bar{v}_M$ y res_L en los 2-cociclos. La conmutatividad del cuadro de enmedio se sigue que res conmuta con los mapeos de conexión. Para el cuadro de la derecha, tenemos

$$\begin{aligned}\mathrm{res}\colon H^1(G_{M|K},\mathbb{Q}/\mathbb{Z}) &\longrightarrow H^1(G_{M|L},\mathbb{Q})/\mathbb{Z}\\ \chi &\xrightarrow{\mathrm{res}} \chi|_{G_{M|L}}\\ (\chi\colon G_{M|K}\longrightarrow\mathbb{Q}/\mathbb{Z}) &\longrightarrow (\chi|_{G_{M|L}}\colon G_{M|L}\longrightarrow\mathbb{Q}/\mathbb{Z})\end{aligned}$$

$$\begin{aligned}(\varphi\circ\mathrm{res})(\chi) &= \varphi\big(\chi|_{G_{M|L}}\big) = \big(\chi|_{G_{M|L}}\big)(\varphi_{M|L}) = \chi(\varphi_{M|L}),\\ [L:K]\varphi(\chi) &= [L:K]\chi(\varphi_{M|K}) = \chi\big(\varphi_{M|K}^{[L:K]}\big) = \chi(\varphi_{M|L}),\end{aligned}$$

de donde se sigue (2). □

Puesto que K_0^{nr} es ma máxima extensión no ramificada de K_0, K_0^{nr} es la máxima extensión no ramificada de cualquier extensión K/K_0 no ramificada, $K^{\mathrm{nr}} = K_0^{\mathrm{nr}}$.

Ahora $\inf\colon H^2(L|K)\longrightarrow H^2(M|K)$ es inyectiva para $K_0\subseteq K\subseteq L\subseteq M\subseteq K_0^{\mathrm{nr}}$, por lo que podemos definir

$$H^2(K^{\mathrm{nr}}|K) = \varinjlim_{L} H^2(L|K) = \bigcup_{L} H^2(L|K).$$

Por el Teorema 5.1.15, se obtiene un mapeo inyectivo:

$$\mathrm{inv}_K\colon H^2(K^{\mathrm{nr}}|K)\longrightarrow\mathbb{Q}/\mathbb{Z}$$

llamado el *morfismo invariante* o *invariante de Hasse*. Además, inv_K es biyectivo pues $\mathbb{Q}/\mathbb{Z} = \bigcup_{n=1}^{\infty}\big(\frac{1}{n}\mathbb{Z}\big)/\mathbb{Z}$ y puesto que para cada $n\in\mathbb{N}$, existe una única extensión no ramificada K_n/K de K de grado n y

$$H^2(K_n|K)\xrightarrow[\cong]{\mathrm{inv}_{K_n|K}}\big(\frac{1}{n}\mathbb{Z}\big)/\mathbb{Z}.$$

Se sigue:

Teorema 5.1.16. *$H^2(K^{\mathrm{nr}}|K)\cong\mathbb{Q}/\mathbb{Z}$.* □

5.2. Símbolo de la norma residual local

Sea L/K una extensión no ramificada finita, por lo que $H^1(G_{L|K},L^*) = \{1\}$ y $H^2(G_{L|K},L^*)\underset{\mathrm{inv}_{L|K}}{\cong}\big(\frac{1}{[L:K]}\mathbb{Z}\big)/\mathbb{Z}\cong\mathbb{Z}/([L\colon K]\mathbb{Z})$ es cíclica de orden $[L:$

$K] = |G_{L|K}|$, por lo que del Teorema de Tate-Nakayama, si $u_{L|K}$ es la clase fundamental de L/K, se obtiene el isomorfismo

$$\begin{aligned}\theta_{L|K} := u_{L|K} \cup \_ \colon H^{-2}(G_{L|K}, \mathbb{Z}) &\longrightarrow H^0(G_{M|K}, L^*)\\ G_{L|K}^{\mathrm{ab}} &\longrightarrow K^*/\operatorname{N}_{L/K} L^*,\end{aligned}$$

llamado el *mapeo de Nakayama* o *isomorfismo de Nakayama*.

El isomorfismo inverso de $\theta_{L|K}$, $\theta_{L|K}^{-1} \colon K^*/\operatorname{N}_{L/K} L^* \longrightarrow G_{L|K}^{\mathrm{ab}} = G_{L|K}$ se llama el *isomorfismo de reciprocidad*. Como consecuencia, tenemos un epimorfismo $(\ , L/K) \colon K^* \longrightarrow G_{L|K}$ con núcleo $\operatorname{N}_{L/K} L^*$ el cual se llama el *símbolo de la norma residual* y se tiene que la sucesión

$$1 \longrightarrow \operatorname{N}_{L/K} L^* \hookrightarrow K^* \xrightarrow{(\ ,L/K)} G_{L|K} \longrightarrow 1$$

es exacta. Notemos que $(a, L/K) = 1 \iff a$ es una norma de L^*.

El siguiente resultado será usado para hallar $(a, L/K)$ explícitamente en el caso no ramificado.

Proposición 5.2.1. *Sean L/K una extensión finita no ramificada de campos locales, $a \in K^*$, $\bar{a} = a \operatorname{N}_{L/K} L^* \in H^0(G_{L|K}, L^*) = H^0(L|K)$. Si $\mu \in \chi(G_{L|K}) = H^1(G_{L|K}, \mathbb{Q}/\mathbb{Z})$ es un caracter de $G_{L|K}$, entonces, si δ denota al mapeo de conexión $\delta \colon H^1(G_{L|K}, \mathbb{Q}/\mathbb{Z}) \longrightarrow H^2(G_{L|K}, \mathbb{Z})$ obtenido de la sucesión exacta $0 \longrightarrow \mathbb{Z} \longrightarrow \mathbb{Q} \longrightarrow \mathbb{Q}/\mathbb{Z} \longrightarrow 0$, se tiene*

$$\mu\big((a, L/K)\big) = \operatorname{inv}_{L|K}\left(\bar{a} \cup \delta\mu\right) \in \Big(\frac{1}{[L:K]}\mathbb{Z}\Big)/\mathbb{Z} \subseteq \mathbb{Q}/\mathbb{Z}.$$

Demostración. Sea $\sigma_a := (a, L/K) \in G_{L|K} \cong H^{-2}(G_{L|K}, \mathbb{Z})$ y sea $\bar{\sigma}_a \in H^{-2}(G_{L|K}, \mathbb{Z})$ el elemento que corresponde a σ_a. Se tiene $\bar{a} = u_{L|K} \cup \bar{\sigma}_a \in H^0(G_{L|K}, L^*)$. Ahora bien, el producto copa es asociativo y conmuta con δ, cualquier mapeo de conexión, por lo que obtenemos

$$\bar{a} \cup \delta\mu = \big(u_{L|K} \cup \bar{\sigma}_a\big) \cup \delta\mu = u_{L|K} \cup \big(\bar{\sigma}_a \cup \delta\mu\big) = u_{L|K} \cup \delta\big(\bar{\sigma}_a \cup \mu\big).$$

Puesto que para $\bar{a}_1 \in H^1(G_{L|K}, \mathbb{Q}/\mathbb{Z})$ y para $\bar{\sigma} \in H^{-2}(G_{L|K}, \mathbb{Z})$ se tiene que $\bar{a}_1 \cup \bar{\sigma} = \overline{a_1(\sigma)} \in H^{-1}(G_{L|K}, \mathbb{Q}/\mathbb{Z})$, se sigue que

$$\bar{\sigma}_a \cup \mu = \mu(\sigma_a) = \frac{r}{n} + \mathbb{Z} \in \Big(\frac{1}{n}\mathbb{Z}\Big)/\mathbb{Z} = H^{-1}(G_{L|K}, \mathbb{Q}/\mathbb{Z}), \quad n = [L:K],$$

para algún r. Ahora, para $\delta \colon H^{-1}(G_{L|K}, \mathbb{Q}/\mathbb{Z}) \longrightarrow H^0(G_{L|K}, \mathbb{Z})$ se obtiene

$$\delta(\mu(\sigma_a)) = n\big(\frac{r}{n} + \mathbb{Z}\big) = r + n\mathbb{Z} \in H^0(G_{L|K}, \mathbb{Z}) = \mathbb{Z}/n\mathbb{Z},$$

pues δ es el mapeo de conexión que manda $\operatorname{núc} \operatorname{N}_n \colon \Big(\mathbb{Q}/\mathbb{Z} \longrightarrow \mathbb{Q}/\mathbb{Z}\Big) = \big\{\frac{r}{n} + \mathbb{Z} \mid 0 \leq r \leq n-1\big\}$ a $H^0(G_{L|K}, \mathbb{Z})$ definido por $\frac{r}{n} + \mathbb{Z} \xrightarrow{\delta} r + n\mathbb{Z}$.

Ahora como el producto copa está dado por el producto tensorial, tenemos que $\bar{a} \cup \delta\mu = u_{L|K} \cup (r + n\mathbb{Z}) = u_{L|K}^r$. Finalmente,

$$\operatorname{inv}_{L|K}\left(\bar{a} \cup \delta\mu\right) = r \cdot \operatorname{inv}_{L|K}(u_{L|K}) = \frac{r}{n} + \mathbb{Z} = \mu(\sigma_a). \qquad \square$$

El siguiente resultado es la expresión explícita para el símbolo de la norma residual en el caso no ramificado.

Teorema 5.2.2. *Sean L/K una extensión finita no ramificada de campos locales y $a \in K^*$. Entonces $(a, L/K) = \varphi_{L|K}^{v_K(a)}$, donde $\varphi_{L|K}$ es el automorfismo de Frobenius de L/K. En particular, si π_K es un elemento primo de K, $(\pi_K, L/K) = \varphi_{L|K}$.*

Demostración. Si $\mu \in \chi(G_{L|K})$, $\delta\mu \in H^2(G_{L|K}, \mathbb{Z}) \cong G_{L|K}^{\mathrm{ab}} = G_{L|K}$, $\bar{a} = a\,\mathrm{N}_{L/K}\,L^* \in H^0(L|K)$. Entonces, por la Proposición 5.2.1, se tiene

$$\mu\big((a, L/K)\big) = \operatorname{inv}_{L|K}\left(\bar{a} \cup \delta\mu\right) = (\varphi \circ \delta^{-1} \circ \bar{v}_K)\big(\bar{a} \cup \delta\mu\big) \underset{\substack{\uparrow \\ v_L = v_K \\ \text{por ser no ramificada}}}{=}$$

$$= (\varphi \circ \delta^{-1})\big(v_K(\overline{a \otimes \delta\mu})\big).$$

Se tiene que los mapeos de la sucesión exacta $0 \longrightarrow \mathbb{Z} \xrightarrow{\iota} \mathbb{Q} \xrightarrow{\pi} \mathbb{Q}/\mathbb{Z} \longrightarrow 0$ son los naturales, y por el Lema de la Serpiente, para $\mu \in H^1(G, \mathbb{Q}/\mathbb{Z}) = \operatorname{Hom}(G, \mathbb{Q}/\mathbb{Z})$, se tiene $\delta\mu = (\iota^{-1} \circ \partial_2^* \circ \pi^{-1})(\mu) = \partial_2^*(\mu) = \mu \circ \partial_2$. Si $a \in K^*$, $\bar{a} = a\,\mathrm{N}_{L/K}\,L^*$, $\bar{a} \cup \delta\mu = \overline{a \otimes \delta\mu}$ está representado por el 2-cociclo $f\colon G \times G \longrightarrow L^*$, $f(\sigma, \tau) = a^{\delta\mu(\sigma,\tau)}$. Por tanto $v_K\big(\overline{a \otimes \delta\mu}\big) = v_K(a^{\delta\mu}) = v_K(a)\delta\mu$.

Por tanto

$$\mu\big((a, L/K)\big) = \varphi \circ \delta^{-1}(v_K(a)\delta\mu) = \varphi(v_K(a)\mu)$$
$$= v_K(a)\mu(\varphi_{L|K}) = \mu\big(\varphi_{L|K}^{v_K(a)}\big).$$

Por tanto, para toda $\mu \in \chi(G_{L|K})$, se tiene que $\mu\big((a, L/K)\big) = \mu\big(\varphi_{L|K}^{v_K(a)}\big)$, de donde se sigue $(a, L/K) = \varphi_{L|K}^{v_K(a)}$. $\square$

Teorema 5.2.3. *Sean K un campo local, π un elemento primo de K y L/K la extensión no ramificada de grado f. Entonces $\mathrm{N}_{L/K}\,L^* = \langle \pi^f \rangle \times U_K$.*

Demostración. Se tiene que $\langle \varphi_{L|K} \rangle = G_{L|K}$, $f = [\tilde{L} : \tilde{K}] = [L : K]$ y $o(\varphi_{L|K}) = f$. Se tiene que $a \in K^*$ pertenece a $\mathrm{N}_{L/K}\,L^* \iff (a, L/K) = \varphi_{L|K}^{v_K(a)} = 1 \iff f | v_K(a) \iff a = u\pi^{lf}$ para alguna $u \in U_K$ y alguna $l \in \mathbb{Z} \iff a \in \langle \pi^f \rangle \times U_K$. $\square$

Se tiene $G_{K^{\mathrm{nr}}|K} = \varprojlim_L G_{L|K}$ donde L recorre las extensiones finitas no ramificadas de K. Para $a \in K^*$ obtendremos $(a, K^{\mathrm{nr}}/K) := \varprojlim_L (a, L/K)$ y obtendremos un homomorfismo $K^* \xrightarrow{(\_, K^{\mathrm{nr}}/K)} G_{K^{\mathrm{nr}}|K}$.

Para ver esto, consideremos $\Lambda_L \colon G_{K^{\mathrm{nr}}|K} \longrightarrow G_{L|K}$ la proyección canónica, esto es, el mapeo de restricción $\sigma \longmapsto \sigma|_L$. Entonces obtenemos

$$\Lambda_L(a, K^{\mathrm{nr}}/K) = (a, K^{\mathrm{nr}}/K)|_L = (a, L/K) = \varphi_{L|K}^{v_K(a)} \in G_{L|K}.$$

Puesto que $\varphi_{L|K} = \varphi_{M|K}|_L$ para $K_0 \subseteq K \subseteq L \subseteq M \subseteq K_0^{\mathrm{nr}}$, el sistema $\{\varphi_{L|K}\}_L$ forma un sistema coherente (sistema compatible) en el sistema proyectivo y obtenemos

$$\varphi_K := \varprojlim_L \varphi_{L|K} \in G_{K^{\mathrm{nr}}|K}.$$

El homomorfismo φ_K se llama el *automorfismo de Frobenius universal de* K y se tiene

$$\varphi_K|_L = \varphi_{L|K}.$$

Teorema 5.2.4. *Si $a \in K^*$, entonces $(a, K^{\mathrm{nr}}/K) = \varphi_K^{v_K(a)}$ y el núcleo del homomorfismo $K^* \xrightarrow{(\_, K^{\mathrm{nr}}/K)} G_{K^{\mathrm{nr}}|K}$ es el grupo de unidades U_K de K.*

Demostración. Para un extensión finita no ramificada L/K, se tiene

$$\Lambda_L(a, K^{\mathrm{nr}}/K) = (a, L/K) = \varphi_{L|K}^{v_K(a)} = \Lambda_L(\varphi_K^{v_K(a)}).$$

Por tanto $(a, K^{\mathrm{nr}}/K) = \varphi_K^{v_K(a)}$ y se tiene $(a, K^{\mathrm{nr}}/K) = \varphi_K^{v_K(a)} = 1 \iff v_K(a) = 0$ pues φ_K es de orden infinito. Finalmente, $v_K(a) = 0 \iff a \in U_K$. □

Observación 5.2.5. El mapeo $(\_, K^{\mathrm{nr}}/K) \colon K^* \longrightarrow G_{K^{\mathrm{nr}}|K}$ no es suprayectivo puesto que $G_{K^{\mathrm{nr}}|K}$ es un grupo profinito y $\operatorname{im}\big((\_, K^{\mathrm{nr}}/K)\big) \cong K^*/U_K \cong \mathbb{Z}$ el cual no es profinito por no ser compacto. Por otro lado, $\langle \varphi_K \rangle$ es denso en $G_{K^{\mathrm{nr}}|K}$ y la completación $\widehat{\langle \varphi_K \rangle} \cong \widehat{\mathbb{Z}} \cong G_{K^{\mathrm{nr}}|K}$.

5.3. Ley de reciprocidad local en general

Sea K_0 un campo local y sea $\Omega := \bar{K}_0$ una cerradura separable de K_0. Para cada extensión normal L/K con $K_0 \subseteq K \subseteq L \subseteq \Omega$, y L/K finita, nuevamente usamos la notación $H^q(L|K) := H^q(G_{L|K}, L^*)$ y $\mathrm{Br}(K) = H^2(\ |K) = \bigcup_{L/K} H^2(L|K)$ donde L recorre las extensions normales, separables y finitas de K. El grupo $\mathrm{Br}(K)$ es el *grupo de Brauer* de K. Sea $G_{K_0} := \mathrm{Gal}(\Omega/K_0)$. Se tiene que $H^1(L|K) = \{1\}$. Veamos que se satisface lo análogo al caso no

ramificado, esto es, para cada extensión normal finita L/K, $L \subseteq \Omega$, existe un isomorfismo $\mathrm{inv}_{L|K}\colon H^2(L|K) \longrightarrow \left(\frac{1}{[L:K]}\mathbb{Z}\right)/\mathbb{Z} \subseteq \mathbb{Q}/\mathbb{Z}$ con las propiedades de que si $K_0 \subseteq K \subseteq L \subseteq M \subseteq \Omega$ es una torre de extensiones normales, M/K_0, entonces:

(1) $\mathrm{inv}_{L|K} = \mathrm{inv}_{M|K}\,|_{H^2(L|K)}$.
(2) Si M/K es normal, entonces $\mathrm{inv}_{M|L} \circ \mathrm{res}_L = [L:K]\,\mathrm{inv}_{M|K}$.

El mecanismo para hacer lo anterior es extender el mapeo invariante para extensiones no ramificadas a extensiones ramificadas.

Primero, probamos un resultado general de campos locales (ver Corolario 3.2.7). Sea K un campo local y sea $m \in \mathbb{N}$. Se define $\mu_m(K) := \{\xi \in K \mid \xi^m = 1\}$ las m-raíces de la unidad contenidas en K.

Proposición 5.3.1. *Sea m tal que $\mathrm{car}\,K \nmid m$ (si $\mathrm{car}\,K = 0$, m es arbitrario). El subgrupo abierto $(K^*)^m$ de K^* tiene índice finito en K^* y $[K^* : (K^*)^m] = mq^{v_K(m)}|\mu_m(K)| = m|m|_{\mathfrak{p}}^{-1}|\mu_m(K)|$ donde el campo residual de K, $\tilde{K}$, satisface $\tilde{K} \cong \mathbb{F}_q$. Además $[U_K : (U_K)^m] = q^{v_K(m)}|\mu_m(K)|$.*

Demostración. Se tiene el cociente de Herbrand $q_{0,m}(K^*) = \frac{[K^*:(K^*)^m]}{[\mu_m(K):1]}$. Puesto que $q_{0,m}$ es multiplicativo, obtenemos

$$q_{0.m}(K^*) = q_{0,m}\big(K^*/U_K\big)q_{0,m}\big(U_K/U_K^{(n)}\big)q_{0,m}(U_K^{(n)}).$$

Ahora bien, $q_{0,m}\big(K^*/U_K\big) = q_{0.m}(\mathbb{Z}) = m$; $q_{0,m}\big(U_K/U_K^{(n)}\big) = 1$ por ser $U_K/U_K^{(n)}$ finito; y, para $n > v_K(m)$,

$$q_{0,m}(U_K^{(n)}\big) = \frac{\big[U_K^{(n)} : \big(U_K^{(n)}\big)^m\big]}{[\{1\} : \{1\}]} = \big[U_K^{(n)} : U_K^{(n+v_K(m))}\big] = q^{v_K(m)},$$

pues $[U_K^{(n)} : U_K^{(n+1)}] = q$ (si $\mathrm{car}\,K = p > 0$, $v_K(m) = 0$ y $n \geq 1$).

Se sigue que $\big[K^* : (K^*)^m\big] = q_{o,m}(K^*)|\mu_m(K)| = m \cdot 1 \cdot q^{v_K(m)} \cdot |\mu_m(K)|$. Además, puesto que $\mu_m(U_K) = \mu_m(K)$, y tomando $n > v_K(m)$,

$$\begin{aligned} q_{0,m}(U_K) &= \frac{\big[U_K : (U_K)^m\big]}{[\mu_m(U_K) : \{1\}]} = \big[U_K : (U_K)^m\big]|\mu_m(K)|^{-1} \\ &= q_{0,m}(U_K/U_K^{(n)})q_{0,m}(U_K^{(n)}) = 1 \cdot q^{v_K(m)}. \end{aligned}$$ □

Para ver que se satisface la segunda condición del Teorema de Tate-Nakayama para tener un isomorfismo en el producto copa, primero vemos una desigualdad.

Proposición 5.3.2 (Segunda desigualdad fundamental). *Sea L/K una extensión normal, separable y finita. Entonces $|H^2(L|K)||[L:K]$.*

Demostración. Primero supongamos que la extensión L/K es cíclica de grado primo $p = [L : K]$. Sabemos que el cociente de Herbrand de L^* es p y como $H^1(L|K) = \{1\}$ se sigue que $|H^2(L|K)| = p = [L : K]$.

Ahora sea L/K normal, separable y finita. Puesto que L/K es una extensión de campos locales, tenemos que $G_{L|K}$ es soluble (Corolario 5.8.7). Por tanto, existe una extensión $K \subseteq K' \subseteq L$, $[K' : K]$ es de orden primo y K'/K es normal. Puesto que $H^1(L|K') = \{1\}$, la sucesión

$$1 \longrightarrow H^2(K'|K) \xrightarrow{\inf} H^2(L|K) \xrightarrow{\text{res}} H^2(L|K'),$$

es exacta. En particular $|H^2(L|K)|\big||H^2(L|K)| \cdot |H^2(K'|K)|$ y por el primer paso, $|H^2(K'|K)| = [K' : K]$. Por inducción, suponemos que $|H^2(L|K)|\big|[L : K']$, de donde obtenemos que $|H^2(L|K)|\big|[L : K'][K' : K] = [L : K]$. □

Teorema 5.3.3. *Si L/K es una extensión normal, separable y finita de campos locales, y si L'/K es la extensión no ramificada de grado $[L : K] = [L' : K]$, entonces $H^2(L|K) = H^2(L'|K) \subseteq H^2(\ |K)$.*

Demostración. Puesto que $|H^2(L'|K)| = [L' : K] = [L : K]$ y $|H^2(L|K)|\big|[L : K]$, basta probar que $H^2(L'|K) \subseteq H^2(L|K)$.

Sea $M := LL'$. Entonces M/K es una extensión de Galois y M/L es no ramificada.

$$\begin{array}{ccc} L' & \text{———} & M = LL' \\ {\scriptstyle \text{no ramificada}}\big| & & \big|{\scriptstyle \text{no ramificada}} \\ K & \text{———} & L \end{array}$$

Sea $c \in H^2(L'|K) \subseteq H^2(M|K)$ pues $H^1(M|L') = \{1\}$ y por tanto $1 \longrightarrow H^2(L'|K) \xrightarrow{\inf} H^2(M|K) \xrightarrow{\text{res}_{L'}} H^2(M|L')$ es exacta.

De la sucesión exacta $1 \longrightarrow H^2(L|K) \xrightarrow{\inf} H^2(M|K) \xrightarrow{\text{res}_L} H^2(M|L)$, se sigue que $c \in H^2(L|K) \iff \text{res}_L(c) = 0$. Ahora bien, se tiene que $\text{res}_L(c) = 1 \iff \text{inv}_{M|L}(\text{res}_L(c)) = 1$ por ser $\text{inv}_{M|L}$ por ser un isomorfismo. El resultado se sigue de

$$\text{inv}_{M|L}(\text{res}_L(c)) = [L : K]\,\text{inv}_{L'|K}(c), \tag{5.3.1}$$

pues como $\text{inv}_{L'|K}(c) \in \left(\frac{1}{[L':K]}\mathbb{Z}\right)/\mathbb{Z} = \left(\frac{1}{[L:K]}\mathbb{Z}\right)/\mathbb{Z}$, se sigue el resultado. La prueba de (5.3.1) se da manera más general en el Lema 5.3.4. □

Lema 5.3.4. *Sea $N|K$ una extensión finita de Galois conteniendo a las dos extensiones L/K y L'/K, con L'/K una extensión no ramificada. Entonces $M = LL'/L$ es no ramificada. Si $c \in H^2(L'|K) \subseteq H^2(N|K)$, entonces $\text{res}_L(c) \in H^2(M|L) \subseteq H^2(N|L)$ y*

$$\text{inv}_{M|L}(\text{res}_L(c)) = [L : K]\,\text{inv}_{L'|K}(c).$$

Demostración. Se tiene que los 2-cociclos de la clase $\mathrm{res}_L(c)$ toman valores en M^* pues $1 \longrightarrow H^2(L'|K) \xrightarrow{\inf} H^2(M|K) \xrightarrow{\mathrm{res}_L} H^2(M|L)$ es exacta y $c \mapsto \inf c = c \mapsto \mathrm{res}_L(c) \in H^2(M|L) = H^2(G_{M|L}, M^*)$.

Por tanto $\mathrm{res}_L(c) \in H^2(M|L)$. Sean f el grado de inercia y e el índice de ramificación de la extensión L/K, la cual no necesariamente es normal. Se extienden las valuaciones v_K y v_L a N. Se tiene $v_L = ev_K$. El mapeo inv es la composición de 3 isomorfismos $\bar{v}_K$, δ^{-1} y φ. La fórmula se seguirá si probamos que el siguiente diagrama es conmutativo:

$$\begin{array}{ccccccc}
H^2(L'|K) & \xrightarrow{\bar{v}_K} & H^2(G_{L'|K}, \mathbb{Z}) & \xrightarrow{\delta^{-1}} & H^1(G_{L'|K}, \mathbb{Q}/\mathbb{Z}) & \xrightarrow{\varphi} & \left(\frac{1}{[L':K]}\mathbb{Z}\right)/\mathbb{Z} \subseteq \mathbb{Q}/\mathbb{Z} \\
\downarrow{\scriptstyle i} & & \downarrow{\scriptstyle \inf} & & \downarrow{\scriptstyle \inf} & & \downarrow{\scriptstyle i} \\
H^2(N|K) & & H^2(G_{N|K}, \mathbb{Z}) & & H^1(G_{N|K}, \mathbb{Q}/\mathbb{Z}) & & \left(\frac{1}{[N:K]}\mathbb{Z}\right)/\mathbb{Z} \subseteq \mathbb{Q}/\mathbb{Z} \\
\downarrow{\scriptstyle \mathrm{res}_L} & & \downarrow{\scriptstyle e\,\mathrm{res}_L} & & \downarrow{\scriptstyle e\,\mathrm{res}_L} & & \downarrow{\scriptstyle [L:K]} \\
H^2(M|L) & \xrightarrow{\bar{v}_L} & H^2(G_{M|L}, \mathbb{Z}) & \xrightarrow{\delta^{-1}} & H^1(G_{M|L}, \mathbb{Q}/\mathbb{Z}) & \xrightarrow{\varphi} & \left(\frac{1}{[M:L]}\mathbb{Z}\right)/\mathbb{Z} \subseteq \mathbb{Q}/\mathbb{Z}
\end{array}$$

donde los mapeos verticales inferiores simplemente mandan las imágenes de los mapeos verticales superiores a los grupos de cohomología inferiores.

El cuadrado de la izquierda es conmutativo simplemente por el comportamiento de los ciclos bajo los mapeos en cuestión. El de enmedio se sigue de que la inflación y la restricción conmutan con los homomorfismos de conexión δ. Finalmente para el cuadrado de la derecha, se tiene $\varphi_{M|L}|_{L'} = \varphi^f_{L'/K}$, donde $f = f(L|K)$ pues si $a \in L'$, entonces $\varphi_{M|L}(a) \equiv a^{|\bar{L}|} \bmod \mathfrak{p}_M = a^{|\bar{K}|^f} \bmod \mathfrak{p}_M = a^{|\bar{K}|^f} \bmod \mathfrak{p}_{L'} = \varphi^f_{L'|K}(a)$.

Sea $\mu \in H^1(G_{L'|K}, \mathbb{Q}/\mathbb{Z})$, entonces

$$\begin{aligned}
[L:K]\varphi(\mu) &= [L:K]\mu\big(\varphi_{L'|K}\big) = ef\mu\big(\varphi_{L'|K}\big) = e\mu\big(\varphi^f_{L'|K}\big) = e\big(\varphi_{M|K}|_{L'}\big) \\
&= e\inf\mu\big(\varphi_{M|L}\big) = e(\mathrm{res}\circ\inf)\mu\big(\varphi_{M|L}\big) = e(\mathrm{res}\circ\inf)\varphi(\mu).
\end{aligned}$$

Por tanto $[L:K]\varphi(\mu) = e(\mathrm{res}\circ\inf)\varphi(\mu)$ lo cual prueba el lema y el Teorema 5.3.3. □

Corolario 5.3.5. *Sea K un campo local. Entonces el grupo de Brauer satisface* $\mathrm{Br}(K) \cong \mathbb{Q}/\mathbb{Z}$.

Demostración. De la Teorema 5.3.3 se sigue que

$$\mathrm{Br}(K) = H^2(\ |K) = H^2(K^{\mathrm{nr}}|K) = \bigcup_{\substack{L/K \\ \text{no ramificas}}} H^2(L|K) \cong \mathbb{Q}/\mathbb{Z}. \qquad \square$$

Definición 5.3.6. Sea L/K una extensión de Galois de campos locales y sea L'/K la extensión no ramificada del mismo grado $[L:K] = [L':K]$, de

tal forma que $H^2(L|K) = H^2(L'|K)$. Se define el *invariante* o *invariante de Hasse* como

$$\mathrm{inv}_{L|K}\colon H^2(L|K) \longrightarrow \Big(\frac{1}{[L:K]}\mathbb{Z}/\mathbb{Z}\Big) \subseteq \mathbb{Q}/\mathbb{Z}$$

por el isomorfismo $\mathrm{inv}_{L|K}(c) := \mathrm{inv}_{L'|K}(c)$, $c \in H^2(L|K) = H^2(L'|K)$.

Teorema 5.3.7. *El invariante de Hasse satisface:*

(1) *Si $K \subseteq L \subseteq M$ es una torre de extensiones de Galois, entonces*

$$\mathrm{inv}_{L|K} = \mathrm{inv}_{M|K}\,|_{H^2(L|K)}.$$

(2) *Si $K \subseteq L \subseteq M$ es una torre de extensiones con M/K de Galois, entonces*

$$\mathrm{inv}_{M|L} \circ \mathrm{res}_L = [L:K]\,\mathrm{inv}_{M|K}\,.$$

Demostración. (1) Sean M'/K y L'/K las extensiones no ramificadas de grados $[M':K] = [M:K]$ y $[L':K] = [L:K]$ respectivamente. Por la unicidad de las extensiones no ramificadas, tenemos $K \subseteq L' \subseteq M'$. Para $c \in H^2(L|K) = H^2(L'|K)$, se tiene

$$\mathrm{inv}_{M|K}(c) = \mathrm{inv}_{M'|K}(c) = \mathrm{inv}_{L'|K}(c) = \mathrm{inv}_{L|K}(c).$$

(2) Consideremos L/K una extensión finita ($K_0 \subseteq K \subseteq L$). Sea $\mathrm{res}_L\colon H^2(\ |K) \longrightarrow H^2(\ |L)$. Si $c \in H^2(\ |K)$, se puede suponer que $c \in H^2(L'|K)$ donde $L'/$ es no ramificada. Así, $M = LL'/L$ es no ramificada y $\mathrm{res}_L(c) \in H^2(M|L) \subseteq H^2(\ |L)$. Por el Lema 5.3.4, $\mathrm{inv}_L(\mathrm{res}_L(c)) = [L:K]\,\mathrm{inv}_K(c)$ lo cual prueba (2). □

Definición 5.3.8. Si L/K es una extensión de Galois, se define la *clase fundamental* $u_{L|K} \in H^2(L|K)$ por

$$\mathrm{inv}_{L|K}(u_{L|K}) = \frac{1}{[L:K]} + \mathbb{Z} \in \Big(\frac{1}{[L:K]}\mathbb{Z}\Big)/\mathbb{Z} \subseteq \mathbb{Q}/\mathbb{Z}.$$

La parte más importante del teorema principal de la teoría de campos de clase, es:

Teorema 5.3.9 (Teorema general de reciprocidad). *Sea L/K es una extensión finita de Galois de campos locales con grupo de Galois G. Entonces, el homomorfismo*

$$u_{L|K} \cup \_\colon H^q(G_{L|K}, \mathbb{Z}) \longrightarrow H^{q+2}(L|K),$$

es biyectivo para todo $q \in \mathbb{Z}$.

Demostración. Para que se cumpla el Teorema de Tate-Nakayama, se debe tener que $H^1(G, L^*) = H^1(L|K) = \{1\}$ y $H^1(H, L^*) = \{1\}$ para todo subgrupo $H < G$ de G, lo cual es simplemente el Teorema 90 de Hilbert.

Veamos la segunda condición. Sea $H < G = \mathrm{Gal}(L/K)$ y sea $E := L^H$. Entonces $[L : E] = |H|$. Sea F'/E la extensión no ramificada de grado $|H|$. Del Teorema 5.3.3 se tiene que $H^2(L|E) = H^2(F'|E)$ el cual es cíclico de orden $|H|$. □

Aplicando el Teorema 5.3.9 para $q = 1, 2$, se obtiene:

Corolario 5.3.10. *Sea L/K una extensión finita de Galois de campos locales. Entonces $H^3(L|K) = \{1\}$ y $H^4(L|K) = \chi(G_{L|K}) = \mathrm{Hom}(G_{L|K}, \mathbb{Q}/\mathbb{Z})$.*

Demostración. Se tiene $H^3(L|K) \cong H^1(G_{L|K}, \mathbb{Z}) = \mathrm{Hom}(G_{L|K}, \mathbb{Q}/\mathbb{Z}) = \{0\}$ por ser $G_{L|K}$ un grupo finito. Por otro lado, tenemos $H^4(L|K) \cong H^2(G_{L|K}, \mathbb{Z}) \cong G_{L|K}^{\mathrm{ab}} \cong H^1(G_{L|K}, \mathbb{Q}/\mathbb{Z}) \cong \mathrm{Hom}(G_{L|K}, \mathbb{Q}/\mathbb{Z}) = \chi(G_{L|K})$. □

Para $q = -2$, se obtiene

Teorema 5.3.11 (Ley local de reciprocidad de Artin). *Para una extensión finita de Galois L/K de campos locales, se tiene el* isomorfismo de Nakayama

$$G_{L|K}^{\mathrm{ab}} \cong H^{-2}(G_{L|K}, \mathbb{Z}) \xrightarrow{u_{L|K} \cup -} H^0(L|K) = K^*/\,\mathrm{N}_{L|K}\, L^*. \qquad \text{□}$$

($\theta_{L|K}$ *mapeo de Nakayama*)

Como consecuencia del Teorema 5.3.11, se tiene una demostración del Corolario 3.4.7.

Proposición 5.3.12. *Si L/K es una extensión abeliana finita de campos locales, se tiene que $e = [U_K : \mathrm{N}_{L/K}\, U_L]$.*

Demostración. Por el Teorema 5.3.11 y el mismo Corolario 3.4.7, se tiene que $ef = [L : K] = [K^* : \mathrm{N}_{L/K}\, L^*] = [U_K : \mathrm{N}_{L/K}\, U_L]f$, de donde se sigue el resultado. □

Corolario 5.3.13. *Sea L/K una extensión finita de Galois de campos locales. Entonces L/K es no ramificada si y sólo si $U_K \subseteq \mathrm{N}_{L/K}\, L^*$.*

Demostración. Si L/K es no ramificada, $U_K = \mathrm{N}_{L/K}\, U_L \subseteq \mathrm{N}_{L/K}\, L^*$.

Recíprocamente, supongamos $U_K \subseteq \mathrm{N}_{L/K}\, L^*$. Para $x \in L^*$, $\mathrm{N}_{L/K}\, x \in U_K$ implica $x \in U_L$. Por tanto $\mathrm{N}_{L/K}\, U_L = U_K$ y $e = [U_K\colon \mathrm{N}_{L/K}\, U_L] = 1$. □

El isomorfismo inverso induce la sucesión exacta:

$$1 \longrightarrow \mathrm{N}_{L/K}\, L^* \hookrightarrow K^* \xrightarrow{(\ ,L/K)} G_{L|K}^{\mathrm{ab}} \longrightarrow 1,$$

donde $(\ ,L/K)$ se llama el *símbolo de la norma residual local*. Se tiene

Teorema 5.3.14. *Sea $K_0 \subseteq K \subseteq L \subseteq M$ una torra de campos locales de tal forma que M/K es finita y de Galois. Los siguientes diagramas son conmutativos*

(a) *Si L/K es normal*

$$\begin{array}{ccc} K^* & \xrightarrow{(\ ,M/K)} & G_{M|K}^{\mathrm{ab}} \\ \| & & \downarrow{\scriptstyle \pi} \\ K^* & \xrightarrow[(\ ,L/K)]{} & G_{L|K}^{\mathrm{ab}} \end{array}$$

es decir, $(\ ,M/K)|_L = (\ ,M/L)$ y donde π es la proyección natural $\mathrm{Gal}(M/K)^{\mathrm{ab}} \xrightarrow{\pi} \mathrm{Gal}(L/K)^{\mathrm{ab}}$, equivalentemente, π es mapeo restricción $\mathrm{Gal}(M/K)^{\mathrm{ab}} \xrightarrow{\mathrm{rest}\,|_L} \mathrm{Gal}(L/K)^{\mathrm{ab}}$, $\sigma \longmapsto \sigma|_L$.

(b)

$$\begin{array}{ccc} K^* & \xrightarrow{(\ ,M/K)} & G_{M|K}^{\mathrm{ab}} \\ \downarrow & & \downarrow{\scriptstyle \mathrm{Ver}} \\ L^* & \xrightarrow[(\ ,M/L)]{} & G_{M|L}^{\mathrm{ab}} \end{array}$$

donde Ver *es el mapeo de transferencia* $\mathrm{Ver}\colon G/G' \longrightarrow H/H'$ *que es*

$$\begin{array}{ccc} \| & & \| \\ G^{\mathrm{ab}} & \longrightarrow & H^{\mathrm{ab}} \end{array}$$

$\mathrm{res}_{-2}\colon H^{-2}(G,\mathbb{Z}) \longrightarrow H^{-2}(H,\mathbb{Z})$.

(c)

$$\begin{array}{ccc} L^* & \xrightarrow{(\ ,M/L)} & G_{M|L}^{\mathrm{ab}} \\ {\scriptstyle \mathrm{N}_{L/K}}\downarrow & & \downarrow{\scriptstyle \kappa} \\ K^* & \xrightarrow[(\ ,M/K)]{} & G_{M|K}^{\mathrm{ab}} \end{array}$$

donde

$$\begin{array}{ccc} \mathrm{Gal}(M/L) & \xhookrightarrow{\ i\ } & \mathrm{Gal}(M/K) \\ {\scriptstyle \pi}\downarrow & & \downarrow{\scriptstyle \pi} \\ \mathrm{Gal}(M/L)^{\mathrm{ab}} & \xrightarrow[\kappa]{} & \mathrm{Gal}(M/K)^{\mathrm{ab}} \end{array}$$

κ inducido por cor_{-2}.

(d) *Si* $\sigma \in \mathrm{Gal}(K_0^{\mathrm{sep}}/K_0) = G_{K_0}$,

$$\begin{array}{ccc} K^* & \xrightarrow{(\ ,M/K)} & G^{\mathrm{ab}}_{M|K} \\ {\scriptstyle\sigma}\downarrow & & \downarrow{\scriptstyle\sigma^*} \\ \sigma K^* & \xrightarrow[(\ ,\sigma M/\sigma K)]{} & G^{\mathrm{ab}}_{\sigma M|\sigma K} \end{array},$$

es decir, $(\sigma a, \sigma M/\sigma K) = \sigma(a, M/K)\sigma^{-1}$ *para* $a \in K^*$ *y donde* $\sigma \in G_{K_0}$, *los mapeos* $K^* \xrightarrow{\sigma} \sigma K^*$ *y* $G^{\mathrm{ab}}_{M|K} \xrightarrow{\sigma^*} G^{\mathrm{ab}}_{\sigma M|\sigma K}$ *son* $a \mapsto \sigma a$ *y* $\tau \mapsto \sigma\tau\sigma^{-1}$.

Demostración.

(a) Sea $\mu \in \chi(G_{L|K}) = H^1(G_{L|K}, \mathbb{Q}/\mathbb{Z})$, $\inf \mu \in H^1(G_{M|K}, \mathbb{Q}/\mathbb{Z})$. Entonces

$$\begin{aligned} \mu(\pi(a, M/K)) &= \inf \mu\big((a, M/K)\big) = \mathrm{inv}_{M|K}\left(\bar{a} \cup \delta(\inf \mu)\right) \\ &= \mathrm{inv}_{M|K}\left(\bar{a} \cup \inf(\delta\mu)\right) = \mathrm{inv}_{M|K}\left(\inf(\bar{a} \cup (\delta\mu))\right) \\ &= \mathrm{inv}_{L|K}(\bar{a} \cup \delta\mu) = \mu((a, L/K)). \end{aligned}$$

Puesto que esto se cumple para toda $\mu \in \chi(G_{L|K})$, se sigue que $\pi(a, M/K) = (a, L/K)$.

(b) y (c) Se seguirán de la conmutatividad de los diagramas

$$\begin{array}{ccccccc} K^* & \longrightarrow & H^0(M|K) & \xleftarrow[\cong]{u_{M|K}\cup\_} & H^{-2}(G_{M|K}, \mathbb{Z}) & \xrightarrow[\gamma]{\cong} & G^{\mathrm{ab}}_{M|K} \\ {\scriptstyle i}\downarrow & & \downarrow{\scriptstyle \mathrm{res}_0} & & \downarrow{\scriptstyle \mathrm{res}_{-2}} & & \downarrow{\scriptstyle \mathrm{Ver}} \\ L^* & \longrightarrow & H^0(M|L) & \xleftarrow[\cong]{u_{M|L}\cup\_} & H^{-2}(G_{M|L}, \mathbb{Z}) & \xrightarrow[\gamma]{\cong} & G^{\mathrm{ab}}_{M|L} \end{array}$$

$$\begin{array}{ccccccc} L^* & \longrightarrow & H^0(M|L) & \xleftarrow[\cong]{u_{M|L}\cup\_} & H^{-2}(G_{M|L}, \mathbb{Z}) & \xrightarrow[\gamma]{\cong} & G^{\mathrm{ab}}_{M|L} \\ {\scriptstyle \mathrm{N}_{L/K}}\downarrow & & \downarrow{\scriptstyle \mathrm{cor}_0} & & \downarrow{\scriptstyle \mathrm{cor}_{-2}} & & \downarrow{\scriptstyle \kappa} \\ K^* & \longrightarrow & H^0(M|L) & \xleftarrow[\cong]{u_{M|K}\cup\_} & H^{-2}(G_{M|K}, \mathbb{Z}) & \xrightarrow[\gamma]{\cong} & G^{\mathrm{ab}}_{M|K} \end{array}$$

La conmutatividad de los cuadros de la izquierda es de inmediata verificación siendo todos los mapeos naturales. La conmutatividad de los cuadros de la derecha es simplemente la definición de Ver y de κ como los mapeos correspondientes a res_{-2} y cor_{-2} bajo los isomorfismos γ. Para los cuadros intermedios, se tiene que si $z \in H^{-2}(G_{M|K}, \mathbb{Z})$ (resp. $z' \in H^{-2}(G_{M|L}, \mathbb{Z})$) por los comportamientos de cor y res con respecto al producto copa, de que

$$\operatorname{res}_0(u_{M|K} \cup z) = \operatorname{res}_0(u_{M|K}) \cup (\operatorname{res}_{-2} z) = u_{M|L} \cup (\operatorname{res}_{-2} z)$$

y respectivamente

$$\operatorname{cor}_0(u_{M|L} \cup z') = \operatorname{cor}_0(\operatorname{res}_0(u_{M|L}) \cup z') = u_{M|K} \cup (\operatorname{cor}_{-2} z').$$

(d) Se quiere ver la conmutatividad del diagrama

$$\begin{array}{ccccccc}
K^* & \longrightarrow & H^0(M|K) & \xleftarrow{u_{M|K} \cup -} & H^{-2}(G_{M|K}, \mathbb{Z}) & \xrightarrow{\cong} & G_{M|K}^{\mathrm{ab}} \\
\downarrow{\scriptstyle \sigma} & & \downarrow{\scriptstyle \sigma^*} & & \downarrow{\scriptstyle \sigma^*} & & \downarrow{\scriptstyle \sigma^*} \\
\sigma K^* & \longrightarrow & H^0(\sigma M|\sigma K) & \xleftarrow{u_{\sigma M|\sigma K} \cup -} & H^{-2}(G_{\sigma M|\sigma K}, \mathbb{Z}) & \xrightarrow{\cong} & G_{\sigma M|\sigma K}^{\mathrm{ab}}
\end{array}$$

Se tiene que $G_{\sigma M|\sigma K} = \sigma G_{M|K} \sigma^{-1}$, por lo que $G_{M|K} \xrightarrow{\sigma^*} G_{\sigma M|\sigma K}$, $\tau \longmapsto \sigma\tau\sigma^{-1}$ es un isomorfismo y por tanto los q-cociclos del grupo $H^q(G_{\sigma M|\sigma K}, \sigma^* A)$, $\sigma^* A = A$, para cualquier G-módulo son de la forma $\sigma^* a_q = \sigma a_q \sigma^{-1}$ donde a_q son los q-cociclos de $H^q(G_{M|K}, A)$. De esto se sigue la conmutatividad del diagrama. □

Proposición 5.3.15. *Sean L/K na extensión de Galois finita de campos locales, $a \in K^*$ y $\bar{a} = a \operatorname{N}_{L/K} L^* \in H^0(L|K)$. Si $\mu \in \chi\big(G_{L|K}^{\mathrm{ab}}\big) = \chi\big(G_{L|K}\big) = H^1(G_{L|K}, \mathbb{Q}/\mathbb{Z})$, se tiene $\mu(a, L/K) = \operatorname{inv}_{L|K}\left(\bar{a} \cup \delta\mu\right) \in \left(\frac{1}{[L:K]}\mathbb{Z}\right)/\mathbb{Z} \subseteq \mathbb{Q}/\mathbb{Z}$.*

Demostración. Se sigue del caso no ramificado. □

Consideremos el símbolo residual de la norma (Teorema de Reciprocidad) en general. Para cada extensión abeliana finita L de K, se tiene el símbolo residual de la norma $K^* \xrightarrow{(\ ,L/K)} G_{L|K}$. Tomando el límite proyectivo sobre todas las extensiones abelianas finitas L/K, $G_K^{\mathrm{ab}} := \varprojlim_{L/K} G_{L|K}$, se obtiene, para cada $a \in K^*$ el elemento $(a, K) := \varprojlim_{L/K} (a, L/K) \in G_K^{\mathrm{ab}}$ el cual es el grupo de Galois de la máxima extensión abeliana de K.

La demostración del siguiente resultado es pospuesto hasta que estudiemos los grupos de Lubin-Tate. De momento presentamos una demostración parcial para el caso $\operatorname{car} K = 0$.

Teorema 5.3.16. *El* símbolo de la norma residual universal *define un monomorfismo continuo $K^* \xrightarrow{\rho_K = (\ ,K)} G_K^{\mathrm{ab}}$.*

Demostración. Se tiene $\rho_K = (\_, K) \colon K^* \longrightarrow G_K^{\mathrm{ab}} = \operatorname{Gal}(K^{\mathrm{sep}}/K)^{\mathrm{ab}}$, $\rho_K(a) = (a, K) := \varprojlim_{\substack{L/K \\ \text{abeliana finita}}} (a, L/K)$.

Se tiene que $\rho_K(a) = 1 \iff (a, L/K) = 1$ para toda extensión L/K abeliana finita $\iff a \in D_K := \bigcap_{L/K} \mathrm{N}_{L/K} L^*$. En general se probará más adelante que $D_K = \{1\}$. Para K de característica 0, se verá que para cada $m \in \mathbb{N}$, $(K^*)^m$ es un grupo de normas, esto es, existe una extensión abeliana finita L_m/K tal que $\mathrm{N}_{L_m/K}(L_m^*) = (K^*)^m$. Se tiene que $[K^* : (K^*)^m] < \infty$ (Proposición 5.3.1). Se sigue que $D_K \subseteq \bigcap_{m=1}^{\infty} (K^*)^m = \{1\}$ (Corolario 3.2.7).

Si H es un subgrupo abierto de G_K^{ab}, H es índice finito, por lo que H es cerrado y H corresponde a una extensión abeliana finita de L/K: $L = (K^{\mathrm{ab}})^H$ y $\rho_K^{-1}(H) = \mathrm{N}_{L/K} L^*$ el cual es cerrado de índice finito en K^*, por lo que es abierto de K^*. Por tanto ρ_K es continua. □

Consideremos en general $a \in K^*$. Se tiene que la restricción de $(a, K) \in G_K^{\mathrm{ab}}$ al campo de inercia K^{nr}/K, K^{nr} la máxima extensión no ramificada de K^{nr}, nos da

$$(a, K)|_{K^{\mathrm{nr}}} = (a, K^{\mathrm{nr}}/K) = \varphi_K^{v_K(a)} \in G_{K^{\mathrm{nr}}|K}$$

donde φ_K es el automorfismo de Frobenius universal. En particular, $\rho_K = (\ , K)$ no es suprayectiva pues $\langle \varphi_K \rangle$ es isomorfo a $\mathbb{Z}$ el cual no es profinito pues no es compacto y de hecho, la completación de $\mathbb{Z}$ es el anillo de Prüfer $\hat{\mathbb{Z}} \cong \prod_p \mathbb{Z}_p$ y $\hat{\mathbb{Z}} \subseteq G_K^{\mathrm{ab}}$.

Antes de enunciar el resultado principal de la teoría de campos de clase local, notamos que cuando estudiamos la teoría de campos de clase global, necesitamos "una ley de reciprocidad para $\mathbb{R}$". Resulta ser $\mathbb{R}$ tiene dos extensiones algebraicas $\{\mathbb{R}, \mathbb{C}\}$. Se tiene $H^2(G_{\mathbb{C}|\mathbb{R}}, \mathbb{C}^*) = H^0(G_{\mathbb{C}|\mathbb{R}}, \mathbb{C}^*) = \mathbb{R}^*/\mathrm{N}_{\mathbb{C}/\mathbb{R}}\, \mathbb{C}^* = \mathbb{R}^*/\mathbb{R}^+ \cong C_2$.

Se tiene que $a \in \mathbb{R}^*$ es norma $\iff a > 0$ y el mapeo invariante

$$\begin{aligned} \mathrm{inv}_{\mathbb{C}|\mathbb{R}} \colon H^2(G_{\mathbb{C}|\mathbb{R}}, \mathbb{C}^*) &\longrightarrow \left(\frac{1}{2}\mathbb{Z}\right)/\mathbb{Z} \\ a\mathbb{R}^+ &\longrightarrow \begin{cases} 1 + \mathbb{Z}, & a > 0, \\ \frac{1}{2} + \mathbb{Z}, & a < 0, \end{cases} \end{aligned}$$

y $(a, \mathbb{C}/\mathbb{R})(\sqrt{-1}) = (\sqrt{-1})^{\operatorname{sgn} a}$, $(a, \mathbb{C}/\mathbb{R})(i) = \begin{cases} i & \text{si } a > 0, \\ i^{-1} = i^3 = -i & \text{si } a < 0. \end{cases}$

El resultado principal de la Teoría de Campos de Clase locales es:

Teorema 5.3.17 (TCCL). *Sea K un campo local o $K \in \{\mathbb{R}, \mathbb{C}\}$. Sea K^{ab} la máxima extensión abeliana de K. Entonces*

(1) *Existe un único homomorfismo continuo*

$$\rho_K \colon K^* \to \mathrm{Gal}(K^{\mathrm{ab}}/K)$$

tal que

(I) *Si L/K es una extensión abeliana finita, ρ_K induce un isomorfismo*

$$K^*/\operatorname{N}_{L/K} L^* \xrightarrow[\psi_{L/K}=(\_,\widetilde{L/K})]{\cong} \operatorname{Gal}(L/K),$$

es decir, $\tilde{\rho}_K = \psi_{L/K}$. Se denota $\psi_{L/K}(a) = (a, L/K)$ por abuso del lenguaje.

(II) *(Relación con los campos finitos). Si el campo residual de K es $\mathbb{F}_q$, se tiene el siguiente diagrama conmutativo*

$$\begin{array}{ccc} K^* & \xrightarrow{\rho_K} & \operatorname{Gal}(K^{\mathrm{ab}}/K) \\ {\scriptstyle \text{valuación}}\downarrow{\scriptstyle v_K = v_{\mathfrak{p}}} & & \downarrow{\scriptstyle \mu} \\ \mathbb{Z} & \xrightarrow[\rho_{\mathbb{F}_q}]{} & \operatorname{Gal}(\mathbb{F}_q^{\mathrm{ab}}/\mathbb{F}_q) \end{array}$$

donde $\rho_{\mathbb{F}_q}$ es el mapeo $n \to \tau^n$ donde τ es el automorfismo de Frobenius y μ es la composición

$$\begin{array}{ccc} \operatorname{Gal}(K^{\mathrm{ab}}/K) & \xrightarrow{\text{rest}} & \operatorname{Gal}(K^{\mathrm{nr}}/K) \cong \operatorname{Gal}(\mathbb{F}_q^{\mathrm{ab}}/\mathbb{F}_q) \\ \sigma & \longmapsto & \sigma|_{K^{\mathrm{nr}}} \end{array}$$

donde K^{nr} es la máxima extensión no ramificada de K (la cual necesariamente tiene que ser abeliana por el Teorema 3.4.5*).*

(2) *Teorema de Existencia La correspondencia $U \longmapsto \rho_K^{-1}(U)$ es una biyección entre el conjunto de subgrupos abiertos de $\operatorname{Gal}(K^{\mathrm{ab}}/K)$ y el conjunto de subgrupos abiertos de índice finito de K^*.*
En particular, si $H \subseteq K^*$ es un subgrupo abierto de índice finito, existe una única extensión abeliana finita L/K tal que $H = \operatorname{N}_{L/K} K^*$. □

Falta probar el Teorema de Existencia, el cual se hará cuando estudiemos los grupos formales de Lubin-Tate. La ley de reciprocidad ya la hemos obtenido Teorema 5.3.11. Como complemento a la ley de reciprocidad presentamos una forma alternativa de obtenerla, sin usar cohomología de grupos. Esta forma alternativa se debe a Jürgen Neukirch [119].

5.4. Isomorfismo de Neukirch

Hay una forma alternativa de obtener el mapeo de Nakayama,

$$\theta_{L/K} \colon \operatorname{Gal}(L/K)^{\mathrm{ab}} \longrightarrow K^*/\operatorname{N}_{L/K} L^*$$

esto es, el inverso del mapeo de reciprocidad. Esta forma alternativa se debe a Jürgen Neukirch [118, 119].

Uno de los problemas en el corazón de la teoría de campos de clase, es la Ley de Reciprocidad y en ella, una de las ideas centrales, es la estrecha relación entre los elementos primos de los campos locales y los automorfismos de Frobenius para extensiones finitas no ramificadas. Más precisamente, si L/K es una extensión finita no ramificada y π es un elemento primo de K, entonces la ley de reciprocidad Artin establece que $(\pi, L/K) = \mathrm{Fr}_{L|K}$ donde, en esta parte, denotará el automorfismo de Frobenius de la extensión L/K.

La idea del automorfismo de Neukirch es que dada una extensión finita de Galois L/K, se debe identificar $\sigma \in \mathrm{Gal}(L/K)$ con extensión de un automorfismo de Frobenius, lo que Neukirch define como "levantamientos de Frobenius", y definir un mapeo $\mathcal{N}_{L/K}$ entre $\mathrm{Gal}(L/K)$ y $K^*/\,\mathrm{N}_{L/K}\, L^*$ identificando σ con la norma $\mathrm{N}_{E/K}\,\pi_E$ de un elemento primo π_E de cierto campo E.

Esta nítida idea funciona a la perfección. El problema es técnico. La idea es relativamente simple y la definición de $\mathcal{N}_{L/K}$ también. Sin embargo la verificación, aunque relativamente elemental, es técnicamente difícil. Hay que verificar que el mapeo está bien definido y que es un homomorfismo. Una vez superado el problema técnico, se obtiene una serie de propiedades funtoriales de este mapeo, importante de por sí para toda la teoría de campos de clase, además que permiten extender el hecho de que $\mathcal{N}_{L/K}$ es en realidad un isomorfismo para extensiones finitas no ramificadas, al caso general de un extensión finita de Galois L/K:

$$\mathcal{N}_{L/K}\colon\ \mathrm{Gal}(L/K)^{\mathrm{ab}} \xrightarrow{\cong} K^*/\,\mathrm{N}_{L/K}\, L^*.$$

En otras palabras, si la equivalencia funciona bien para extensiones no ramificadas, la equivalencia se extiende de manera única a extensiones finitas de Galois arbitrarias.

Neukirch desarrolla la teoría de campos de clase a partir de este isomorfismo ([118, 119]) evitando la cohomología, como fue su trabajo de 1969 ([117]). Aquí hacemos notar que ambos puntos de vista tienen como base las extensiones no ramificadas y en ambos casos se extiende a extensiones finitas de Galois.

El desarrollo del isomorfismo de Neukirch, lo presentamos directamente para campos locales, en lugar de hacerlo para "formación de clases" lo cual es más general.

El desarrollo abstracto del isomorfismo de Neukirch (y de hecho para toda la teoría de campos de clase usando de cohomología de grupos), es como sigue:

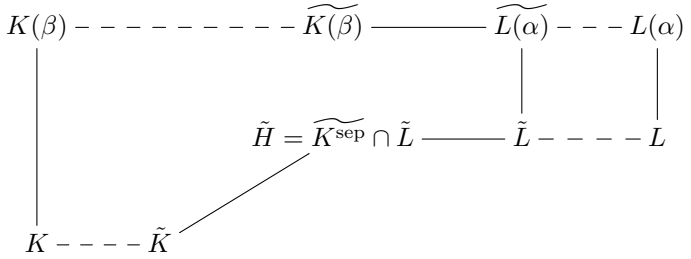
Sea G un grupo profinito y A un G-módulo. Los subgrupos cerrados de G se denotan por G_K y los índices se les consideran campos (G se piensa como $G = \mathrm{Gal}(k^{\mathrm{sep}}/k)$ con k un campo local fijo). De esta forma K juega el papel del campo fijo de G_K: $K := A^{G_K}$ y en particular $G_{k^{\mathrm{sep}}} = \{1\}$ y $G_k = G$ y k juega el papel del campo base. Definimos $K \subseteq L \iff G_L \subseteq G_K$ y el grado de la "extensión" L/K, como $[L\colon K] = [G_K\colon G_L]$. Si $G_L \triangleleft G_K$, L/K se llama extensión o de Galois, etc.

Sea K un campo local y sea K^{sep} una cerradura separable fija de K. Sea K^{nr} la máxima extensión no ramificada de K contenida en K^{sep}. Recordemos que para cada $n \in \mathbb{N}$, existe una única extensión K_n no ramificada de K de grado n y $\text{Gal}(K_n/K) \cong \mathbb{Z}/n\mathbb{Z}$. Por tanto $K^{\text{nr}} = \bigcup_{n=1}^{\infty} K_n$ y $\text{Gal}(K^{\text{nr}}/K) = \text{Gal}\left(\left(\bigcup_{n=1}^{\infty} K_n\right)/K\right) = \text{Gal}\left(\left(\varinjlim_n K_n\right)/K\right) = \varprojlim_n \text{Gal}(K_n/K) = \varprojlim_n \left(\mathbb{Z}/n\mathbb{Z}\right) \cong \hat{\mathbb{Z}}$, el anillo de Prüfer.

Se tiene el mapeo de restricción $\text{rest}_K \colon \text{Gal}(K^{\text{sep}}/K) \longrightarrow \text{Gal}(K^{\text{nr}}/K)$. Cada grupo $\text{Gal}(K_n/K)$ está generado por el automorfismo de Frobenius. De esta forma, $\text{Gal}(K_n/K) = \langle \text{Fr}_{K_n|K} \rangle$ donde, si el campo residual de K es $\mathbb{F}_q$, el campo residual de K_n es $\mathbb{F}_{q^n}$ y el automorfismo de Frobenius es $\text{Fr}_{K_n|K}(\alpha) = \alpha^q$. Entonces $\text{Gal}(K^{\text{nr}}/K)$ está generado topológicamente por $\text{Fr}_K \colon \overline{\mathbb{F}_q} \longrightarrow \mathbb{F}_q$, $\alpha \longrightarrow \alpha^q$ y $\text{Fr}_K|_{K_n} = \text{Fr}_{K_n|K}$, $\text{Gal}(K^{\text{nr}}/K) = \overline{\langle \text{Fr}_K \rangle} \cong \hat{\mathbb{Z}}$.

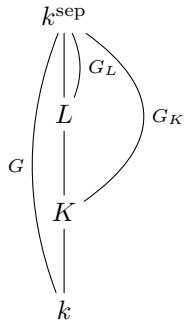
Proposición 5.4.1. *Sea L/K una extensión algebraica. Entonces $L^{\text{nr}} = LK^{\text{nr}}$.*

Demostración. Se tiene que L y $K^{\text{nr}} \subseteq L^{\text{nr}}$, por tanto $LK^{\text{nr}} \subseteq L^{\text{nr}}$. Recordemos que cada extensión finita no ramificada M/E de un campo local E está unívocamente determinada por la extensión de campos residuales, es decir, si $\tilde{M} = \tilde{E}(\tilde{\beta})$, existe $\beta \in \tilde{\beta}$ con $M = E(\beta)$ y $\text{Irr}(x, \beta, E) = \text{Irr}(\bar{x}, \tilde{\beta}, \tilde{E})$ y donde $\tilde{\beta} \in \mathcal{O}_M/\mathfrak{p}_M$, $\tilde{\beta} = \beta + \mathfrak{p}_M$. Por tanto, si probamos que $\tilde{L}^{\text{nr}} = \tilde{K}^{\text{nr}}\tilde{L}$, entonces, dada F/L no ramificada, para cada $\alpha \in F$, $L(\alpha)/L$ es una extensión finita no ramificada, $\widetilde{L(\alpha)} = \tilde{L}(\tilde{\alpha})$ y tenemos $\widetilde{L(\alpha)} = \tilde{L}\widetilde{K(\beta)}$ pues $\widetilde{L(\alpha)} \subseteq \tilde{L}^{\text{nr}} = \tilde{K}^{\text{nr}}\tilde{L}$. Se sigue $K(\beta) \subseteq K^{\text{nr}}$. Se sigue $L(\alpha) = K(\beta)L \subseteq K^{\text{nr}}L$. Por tanto $F \subseteq K^{\text{nr}}L$.



Ahora, $\widetilde{LK^{\text{nr}}} \supseteq \tilde{L}\widetilde{K^{\text{nr}}} = \tilde{L}\widetilde{K^{\text{sep}}} = \tilde{L}\widetilde{L^{\text{sep}}}$ puesto que $\tilde{L}/\tilde{K}$ es separable. Se sigue que $\widetilde{K^{\text{nr}}} = \widetilde{K^{\text{sep}}} = \widetilde{L^{\text{sep}}} = \widetilde{L^{\text{nr}}}$. Por tanto $\widetilde{LK^{\text{nr}}} \supseteq \tilde{L}\widetilde{L^{\text{sep}}} = \widetilde{L^{\text{sep}}} = \widetilde{L^{\text{nr}}}$ de donde obtenemos que $\widetilde{LK^{\text{nr}}} = \widetilde{L^{\text{nr}}}$ y finalmente $LK^{\text{nr}} = L^{\text{nr}}$. □

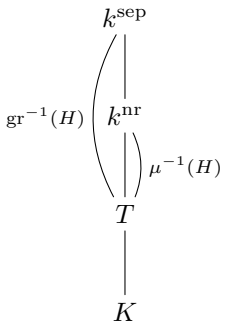
Introducimos alguna notación. Sea k un campo local fijo y sea k^{sep} una cerradura separable fija de k. Todos los campos considerados estarán contenidas en k^{sep} y usualmente serán extensiones finitas de k y por supuesto separables. Sea $G := \text{Gal}(k^{\text{sep}}/k)$. Si K es una extensión de k, sea $G_K := \text{Gal}(k^{\text{sep}}/K)$. Entonces G_K es un subgrupo cerrado de G. Si L/K es una extensión, entonces $[L : K] = [G_K : G_L]$ en caso de ser finita. Se tiene $K = (k^{\text{sep}})^{G_K}$ y $L = (k^{\text{sep}})^{G_L}$.

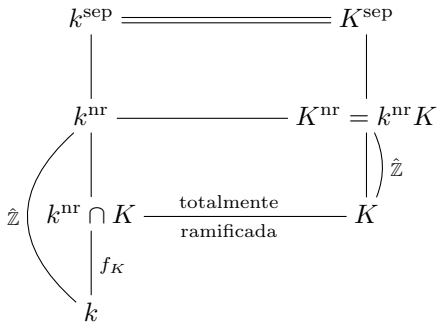


Consideremos $\mathrm{Gal}(K^{\mathrm{nr}}/K) = \overline{\langle \mathrm{Fr}_K \rangle}$. Si $\sigma \in G$, $\sigma|_{k^{\mathrm{nr}}} \in \mathrm{Gal}(k^{\mathrm{nr}}/k) \underset{\mu}{\cong} \hat{\mathbb{Z}}$.

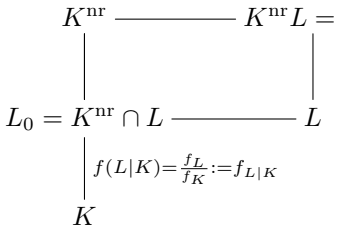
Se tiene que $\sigma|_{k^{\mathrm{nr}}} = \mathrm{Fr}_K^{\alpha_\sigma}$ con $\alpha_\sigma \in \hat{\mathbb{Z}}$. Sea $\mathrm{gr}\colon G \longrightarrow \hat{\mathbb{Z}}$, definido por $\mathrm{gr}(\sigma) := \alpha_\sigma$ el cual es un epimorfismo continuo. De esta forma, si H es un subgrupo cerrado de $\hat{\mathbb{Z}}$, $\mu^{-1}(H)$ es cerrado en $\mathrm{Gal}(k^{\mathrm{nr}}/k)$ y corresponde a un campo T con $k \subseteq T \subseteq k^{\mathrm{nr}}$. Entonces $\mathrm{Gal}(k^{\mathrm{sep}}/T) = \mathrm{gr}^{-1}(H) = G_T$ y $\mathrm{gr}^{-1}(H)$ es un subgrupo cerrado.

Se tiene que $\mathrm{núc}\,\mathrm{gr} = \mathrm{Gal}(k^{\mathrm{sep}}/k^{\mathrm{nr}})$. Se define $\mathrm{gr}_K := \frac{1}{f_K}\,\mathrm{gr}\colon G_K \longrightarrow \hat{\mathbb{Z}}$ y $\mathrm{gr}_K\colon \mathrm{Gal}(K^{\mathrm{nr}}/K) \xrightarrow{\cong} \hat{\mathbb{Z}}$, donde $f_K = f(K|k)$ es el grado de inercia.

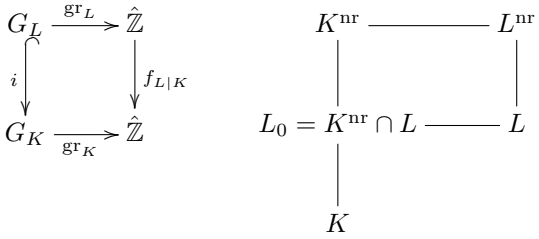




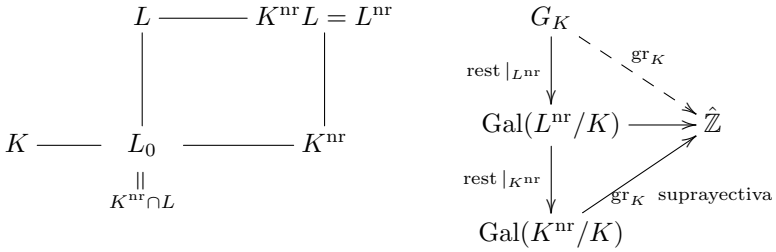
El automorfismo de Frobenius sobre K, Fr_K, el generador topológico de $\mathrm{Gal}(K^{\mathrm{nr}}/K)$ satisface $\mathrm{gr}_K(\mathrm{Fr}_K) = 1$. Si L/K es una extensión finita, se tiene



Si M/N es una extensión no ramificada, $\mathrm{Fr}_{M|N}$ denota al automorfismo de Frobenius de la extensión M/N. De esta forma $\mathrm{Fr}_{L_0|K} = \mathrm{Fr}_K\,|_{L_0}$. Se tiene el diagrama conmutativo

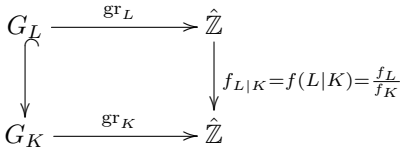


$f_{L|K} \circ \mathrm{gr}_L = \frac{f_L}{f_K} \frac{1}{f_L} \mathrm{gr} = \frac{1}{f_K} \mathrm{gr} = \mathrm{gr}_K = \mathrm{gr}_K \circ i$. En particular $\mathrm{Fr}_L\,|_K = \mathrm{Fr}_K^{f_{L|K}}$. Se tiene

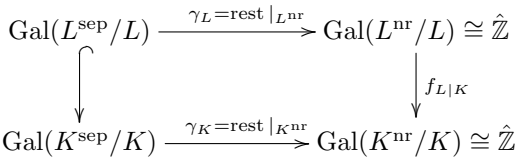


Entonces $\mathrm{gr}_K\colon \mathrm{Gal}(L^{\mathrm{nr}}/K) \longrightarrow \hat{\mathbb{Z}}$ es suprayectiva.

El diagrama



se puede reinterpretar como el diagrama conmutativo

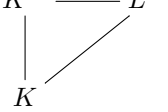


Se define $\Lambda(L^{\mathrm{nr}}/L) = \{\tilde{\sigma} \in \mathrm{Gal}(L^{\mathrm{nr}}/K) \mid \mathrm{gr}_K(\tilde{\sigma}) \in \mathbb{N}\}$. Hacemos notar que se pide que el grado gr_K sea estrictamente positivo. Se tiene que si $\tilde{\sigma} \in \Lambda(L^{\mathrm{nr}}/K)$ y si $n = \mathrm{gr}_K(\tilde{\sigma})$, entonces $\tilde{\sigma}|_{K^{\mathrm{nr}}} = \mathrm{Fr}_K^n$.

La idea central del isomorfismo de Neukirch es, en cierta forma, convertir cualquier elemento en un Frobenius. El resultado siguiente es el que indica el camino a seguir.

Proposición 5.4.2. *El mapeo restricción $\Lambda(L^{\mathrm{nr}}/K) \longrightarrow \mathrm{Gal}(L/K)$, $\tilde{\sigma} \longmapsto \tilde{\sigma}|_L$, es suprayectivo. Si $\sigma = \tilde{\sigma}|_L$, $\tilde{\sigma}$ se llama un* levantamiento de Frobenius *de σ.*

Demostración. Sea $\sigma \in \mathrm{Gal}(L/K)$, entonces $\sigma|_{L_0} = (\mathrm{Fr}_{L_0|K})^n$ para alguna $n \geq 0$. Notemos que $\mathrm{Gal}(L_0/K) = \langle \mathrm{Fr}_{L_0|K} \rangle = \{\mathrm{Fr}_{L_0|K}, \mathrm{Fr}^2_{L_0|K}, \ldots, \mathrm{Fr}^{[L_0:K]}_{L_0|K}\}$, por lo que $n \geq 1$. Sea $\tilde{\mu}$ una extensión de Fr_K a L^{nr}. Se tiene $\mathrm{Gal}(L^{\mathrm{nr}}/K) \overset{\pi}{\twoheadrightarrow} \mathrm{Gal}(K^{\mathrm{nr}}/K)$, $\mathrm{núc}\,\pi = H = \mathrm{Gal}(L^{\mathrm{nr}}/K^{\mathrm{nr}})$ y $\pi(\tilde{\mu}) = \mathrm{Fr}_K$.



Entonces $\tilde{\mu}|_{K^{\mathrm{nr}}} = \mathrm{Fr}_K$, $\tilde{\mu}|_{L_0} = \mathrm{Fr}_K|_{L_0} = \mathrm{Fr}_{L_0|K}$. Por tanto $\sigma\tilde{\mu}^{-n}|_{L_0} = 1$, es decir, $\sigma\tilde{\mu}^{-n}|_L \in \mathrm{Gal}(L/L_0) \cong \mathrm{Gal}(L^{\mathrm{nr}}/K^{\mathrm{nr}})$. En particular, $\sigma\tilde{\mu}^{-n}|_L = \tau|_L$ para algún $\tau \in \mathrm{Gal}(L^{\mathrm{nr}}/K^{\mathrm{nr}})$.

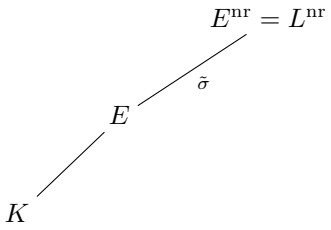
Sea $\tilde{\sigma} = \tau \cdot \tilde{\mu}^n \in \mathrm{Gal}(L^{\mathrm{nr}}/K)$, $\tilde{\sigma}|_L = \tau|_L \cdot \tilde{\mu}^n|_L = \sigma$ y $\tilde{\sigma}|_{K^{\mathrm{nr}}} = \tau|_{K^{\mathrm{nr}}} \cdot \tilde{\mu}^n|_{K^{\mathrm{nr}}} = \mathrm{Fr}^n_K$. Por tanto $\mathrm{gr}_K(\tilde{\sigma}) = n \in \mathbb{N}$ y $\tilde{\sigma}$ es un levantamiento
$\|$
Id
de Frobenius de σ. □

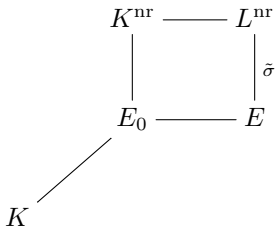
El punto medular de los levantamientos de Frobenius está en el hecho de que resulta que todo elemento $\sigma \in \mathrm{Gal}(L/K)$ puede considerarse "casi" un Frobenius.

Proposición 5.4.3. *Sea $\tilde{\sigma} \in \Lambda(L^{\mathrm{nr}}/K)$ y sea E el campo fijo de $\tilde{\sigma}$. Entonces*

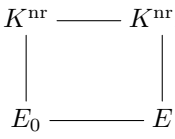
(1) $[E : K] < \infty$.
(2) $f_{E|K} = f(E|K) = \mathrm{gr}_K(\tilde{\sigma})$.
(3) $E^{\mathrm{nr}} = L^{\mathrm{nr}}$.
(4) $\tilde{\sigma} = \mathrm{Fr}_E$.

Demostración.





(2) Sea $E_0 = E \cap K^{\mathrm{nr}}$. Entonces E_0 es el campo fijo de $\tilde{\sigma}|_{K^{\mathrm{nr}}} = \mathrm{Fr}^{\mathrm{gr}_K(\tilde{\sigma})}_K$.
Por tanto $f_{E|K} = f(E|K) = [E_0 : K] = \mathrm{gr}_K(\tilde{\sigma})$.
(1) $[E : E_0] = [K^{\mathrm{nr}}E : K^{\mathrm{nr}}] \leq [L^{\mathrm{nr}} : K^{\mathrm{nr}}] < \infty$. Puesto que



$[E_0 : K] = f_{E_0|K} = f_{E|K} < \infty$,

se sigue que $[E : K] < \infty$.

(3) $\mathrm{Gal}(L^{\mathrm{nr}}/E)$ está generado topológicamente por $\tilde{\sigma}$. En particular $\mathrm{Gal}(L^{\mathrm{nr}}/E)$ es procíclico, esto es, generado topológicamente por un elemento. Puesto $E \subseteq L^{\mathrm{nr}}$, $E^{\mathrm{nr}} \subseteq L^{\mathrm{nr}}$, obtenemos el epimorfismo canónico $\mathrm{Gal}(L^{\mathrm{nr}}/E) \overset{\rho}{\twoheadrightarrow} \mathrm{Gal}(E^{\mathrm{nr}}/E)$ dado por restricción y se tiene $\mathrm{núc}\,\rho = \mathrm{Gal}(L^{\mathrm{nr}}/E^{\mathrm{nr}})$.
Por ser $\mathrm{Gal}(L^{\mathrm{nr}}/E)$ procíclico, $\mathrm{Gal}(L^{\mathrm{nr}}/E)/\mathrm{Gal}(L^{\mathrm{nr}}/E)^n$ es un grupo cíclico de orden n: $\frac{\mathrm{Gal}(L^{\mathrm{nr}}/E)}{\mathrm{Gal}(L^{\mathrm{nr}}/E)^n} = \frac{\overline{\langle\tilde{\sigma}\rangle}}{\overline{\langle\tilde{\sigma}^n\rangle}} \cong \frac{\langle\tilde{\sigma}\rangle}{\langle\tilde{\sigma}^n\rangle}$. De hecho sea $\frac{\mathbb{Z}}{n\mathbb{Z}} \xrightarrow{\varepsilon_n} \frac{\mathrm{Gal}(L^{\mathrm{nr}}/E)}{\mathrm{Gal}(L^{\mathrm{nr}}/E)^n}$ dado por $\varepsilon_n(1 \bmod n) = \tilde{\sigma} \bmod \mathrm{Gal}(L^{\mathrm{nr}}/E)^n$ es un epimorfismo. Tomando la composición inducida por ρ:

$$\frac{\mathbb{Z}}{n\mathbb{Z}} \xrightarrow{\varepsilon_n} \frac{\mathrm{Gal}(L^{\mathrm{nr}}/E)}{\mathrm{Gal}(L^{\mathrm{nr}}/E)^n} \xrightarrow{\tilde{\rho}} \frac{\mathrm{Gal}(E^{\mathrm{nr}}/E)}{\mathrm{Gal}(E^{\mathrm{nr}}/E)^n} \xrightarrow{(\varepsilon_n')^{-1}} \frac{\mathbb{Z}}{n\mathbb{Z}}$$

es un isomorfismo y ρ es un isomorfismo (al tomar límites inversos). Por tanto $\mathrm{Gal}(L^{\mathrm{nr}}/E^{\mathrm{nr}}) = \mathrm{núc}\,\rho = \{1\}$ y $L^{\mathrm{nr}} = E^{\mathrm{nr}}$.

(4) Se tiene $f_{E|K}\,\mathrm{gr}_E(\tilde{\sigma}) = \mathrm{gr}_K(\tilde{\sigma}) \underset{(2)}{=} f_{E|K}$. Por tanto $\mathrm{gr}_K(\tilde{\sigma}) = 1$ y $\tilde{\sigma} = \mathrm{Fr}_E$. □

Consideremos ahora L/K una extensión finita, $L = (k^{\mathrm{sep}})^{G_L}$, $K(k^{\mathrm{sep}})^{G_K}$, $[L:K] = [G_K : G_L]$. Entonces $\mathrm{N}_{L/K}\colon L \longrightarrow K$ dado por $\mathrm{N}\,a = \prod_{\sigma \in G_K/G_L} a^{\sigma}$, donde $\{\sigma\}$ recorre un conjunto de representantes de las clases derechas de G_K/G_L (pues estamos usando la acción por la derecha: a^{σ} en lugar de la acción por la izquierda: σa). Se tiene que si $K \subseteq L \subseteq M$, $\mathrm{N}_{M/K} = \mathrm{N}_{L/K} \circ \mathrm{N}_{M/L}$ y si L/K es Galois, $K = L^{\mathrm{Gal}(L/K)}$.

Definición 5.4.4. Una *valuación de Hensel* con respecto a gr, es un homomorfismo $v\colon k^* \longrightarrow \hat{\mathbb{Z}}$ tal que

(a) $v(k) = \mathcal{Z} \supseteq \mathbb{Z}$ y $\mathcal{Z}/n\mathcal{Z} \cong \mathbb{Z}/n\mathbb{Z}$ para toda $n \in \mathbb{N}$.
(b) $v\big(\mathrm{N}_{K/k}\,K^*\big) = f_K\mathcal{Z}$ para todo campo K, $k \subseteq K \subseteq k^{\mathrm{sep}}$.

Se tiene que una valuación de Hensel, es simplemente una valuación usual de k^{sep}. Dada una valuación de Hensel, $v\colon k^* \longrightarrow \hat{\mathbb{Z}}$, obtenemos el homomorfismo $v_K = \frac{1}{f_K}\big(v \circ \mathrm{N}_{K/k}\big)\colon K^* \longrightarrow \hat{\mathbb{Z}}$ con $\mathrm{im}\,v_K = \mathcal{Z}$.

Proposición 5.4.5. (1) *$v_K = v_{K^\sigma} \circ \sigma$ para $\sigma \in G = \mathrm{Gal}(k^{\mathrm{sep}}/k) = G_k$.*
(2) *Para cada extensión finita de L/K, se tiene el siguiente diagrama conmutativo*

$$\begin{array}{ccc} L^* & \xrightarrow{v_L} & \hat{\mathbb{Z}} \\ {\scriptstyle \mathrm{N}_{L/K}}\downarrow & & \downarrow{\scriptstyle f_{L|K}} \\ K^* & \xrightarrow[v_K]{} & \hat{\mathbb{Z}} \end{array}$$

Demostración. (1) Se tiene que si $\{\tau\}$ es un conjunto completo de representantes de las clases derechas de G_k/G_K, entonces $\{\sigma^{-1}\tau\sigma\}$ es un conjunto completo de representatnes de las clases derechas de $G_k/\sigma^{-1}G_K\sigma = G_k/G_{K^\sigma}$. Por tanto, si $a \in K^*$, se tiene

$$v_{K^\sigma}(a^\sigma) = \frac{1}{f_{K^\sigma}} v\big(\prod_\tau a^{\sigma\sigma^{-1}\tau\sigma}\big) = \frac{1}{f_K} v\big(\big(\underbrace{\prod_\tau a^\tau}_{\in k}\big)^\sigma\big)$$

$$= \frac{1}{f_K} v\big(\mathrm{N}_{K/k}(a)\big) = v_K(a).$$

(2) Si $a \in L^*$, entonces

$$f_{L|K} v_L(a) = f_{L|K} \cdot \frac{1}{f_L} v\big(\mathrm{N}_{L/k}(a)\big) = \frac{1}{f_K} v\big(\mathrm{N}_{K/k}\left(\mathrm{N}_{L/K}(a)\right)\big)$$
$$= v_K\big(\mathrm{N}_{L/K}(a)\big). \qquad \square$$

Observación 5.4.6. Si $f_{L|K} = [L : K]$, es decir, $L_0 = L = K^{\mathrm{nr}} \cap L$, esto es, $L \subseteq K^{\mathrm{nr}}$, entonces por (2), $v_L|_{K^*} = v_K$ pues si $a \in K^*$, $f_{L|K} v_L(a) = [L : K] v_L(a) = v_K\big(\mathrm{N}_{L/K}(a)\big) = v_K\big(a^{[L:K]}\big) = [L : K] v_K(a)$.

En particular, un elemento primo de K^* es un elemento primo de L^* (esto ya nos era conocido y, en este contexto, un elemento primo π_K de K es un elemento con $v_K(\pi_K) = 1$). Por otro lado, si $f_{L|K} = 1$, esto es, $L_0 = K$, si π_L es un elemnto primo de A_L, entonces $\pi_K = \mathrm{N}_{L/K}(\pi_L)$ es un elemento primo de A_K.

5.5. El isomorfismo de Neukirch es el mapeo de Nakayama

Teorema 5.5.1. *Sea L/K una extensión finita no ramificada. Entonces*

$$H^0(\mathrm{Gal}(L/K), L^*) \cong \mathbb{Z}/[L\colon K]\mathbb{Z},$$
$$|H^0(\mathrm{Gal}(L/K), L^*)| = [L\colon K] \quad y$$
$$H^{-1}(\mathrm{Gal}(L/K), L^*) = \{1\}.$$

Demostración. Se tiene que $H^{-1}(\mathrm{Gal}(L/K), L^*) = \{1\}$ por el Teorema 90 de Hilbert. Por otro lado, la sucesión $1 \longrightarrow U_L \longrightarrow L^* \xrightarrow{v_L} \mathbb{Z} \longrightarrow 0$ es una sucesión exacta y $H^n(\mathrm{Gal}(L/K), U_L) = \{1\}$ para toda $n \in \mathbb{Z}$, por tanto $H^n(\mathrm{Gal}(L/K), L^*) \cong H^n(\mathrm{Gal}(L/K), \mathbb{Z})$ para toda $n \in \mathbb{Z}$. En particular, $H^0(\mathrm{Gal}(L/K), L^*) = H^0(\mathrm{Gal}(L/K), \mathbb{Z}) = \mathbb{Z}/[L : K]\mathbb{Z}$. $\square$

Definición 5.5.2 (Mapeo de Neukirch). Sea L/K una extensió finita de Galois. El *mapeo de Neukirch*

$$\mathcal{N}_{L/K}\colon \operatorname{Gal}(L/K) \longrightarrow K^*/\operatorname{N}_{L/K} L^*$$

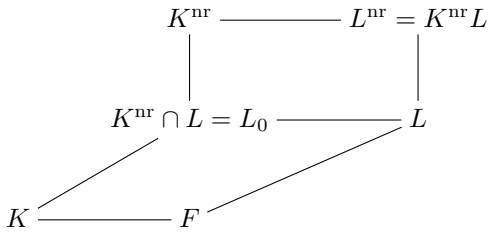
está dado por

$$\mathcal{N}_{L/K}(\sigma) := \operatorname{N}_{E/K}(\pi_E) \text{ mód } \operatorname{N}_{L/K} L^*,$$

donde E es el campo fijo de un levantamiento de Frobenius $\tilde{\sigma} \in \Lambda(L^{\mathrm{nr}}/K)$ de $\sigma \in \operatorname{Gal}(L/K)$ y π_E es un elemento primo de E^*, $v_E(\pi_E) = 1$.

Observación 5.5.3. Se tiene que probar que la definición de $\mathcal{N}_{L/K}(\sigma)$ es independiente de la selección del levantamiento $\tilde{\sigma}$ y del elemento π_E.

Para probar lo anterior, sea $L_0 = K^{\mathrm{nr}} \cap L$. Sea $\mathrm{N} := \operatorname{N}_{L_0/L}$.



Sea $K \subseteq F \subseteq L$ tal que $FL_0 = L$, por ejemplo, $F = L$. Entonces $F_0 = K^{\mathrm{nr}} \cap F = K^{\mathrm{nr}} \cap L \cap F = L_0 \cap F$ y $\mathrm{N}\,|_F = \operatorname{N}_{F/F_0}$. Fijemos una extensión $\varphi \in \Lambda(\tilde{L}/K)$ de Fr_K a L^{nr} y se tiene $\operatorname{N}_{F/K} = \mathrm{N} \circ \mathfrak{N}_F$, donde el homomorfismo $\mathfrak{N}_F\colon F \longrightarrow L$ está definido por

$$\mathfrak{N}_F(a) = \prod_{\eta=0}^{f-1} a^{\varphi^\eta}, \quad f = [F_0 : K].$$

De hecho, $\operatorname{Gal}(F_0/K)$ es un grupo cíclico de orden f y generado por $\operatorname{Fr}_{F_0|K} = \operatorname{Fr}_K|_{F_0}$, por lo que si $a \in F$, se tiene

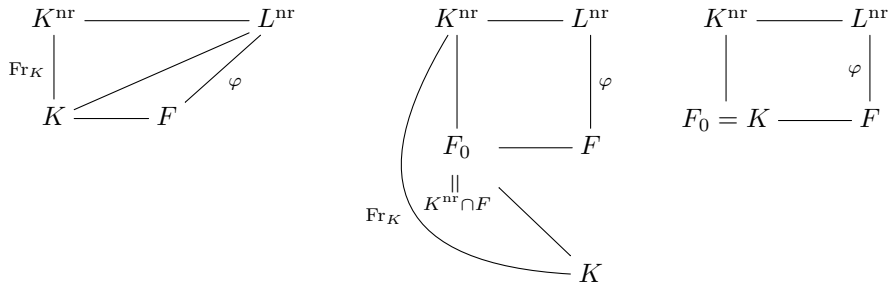
$$\mathrm{N}\left(\mathfrak{N}_F(a)\right) = \prod_{\eta=0}^{f-1} \operatorname{N}_{F/F_0}(a)^{\varphi^\eta} = \operatorname{N}_{F_0/K}\left(\operatorname{N}_{F/F_0}(a)\right) = \operatorname{N}_{F/K}(a).$$

La independencia buscada es consecuencia del siguiente resultado.

Lema 5.5.4. *Sean $\tilde{\sigma}_1, \tilde{\sigma}_2, \tilde{\sigma}_3 \in \Lambda(L^{\mathrm{nr}}/K)$ tales que $\tilde{\sigma}_3 = \tilde{\sigma}_1\tilde{\sigma}_2$. Si $E_i := (L^{\mathrm{nr}})^{\langle \tilde{\sigma}_i \rangle}$ es el campo fijo de $\tilde{\sigma}_i$, $1 \leq i \leq 3$, y si $\pi_i \in E_i$ es un elemento primo de E_i, entonces*

$$\operatorname{N}_{E_3/K}(\pi_3) \equiv \operatorname{N}_{E_1/K}(\pi_1)\operatorname{N}_{E_2/K}(\pi_2) \text{ mód } \operatorname{N}_{L/K} L^*.$$

Demostración. Sea F el campo fijo de φ, el levantamiento de Fr_K a L^{nr}.



Puesto que $\varphi|_{K^{\mathrm{nr}}} = \mathrm{Fr}_K$, $F_0 = K^{\mathrm{nr}} \cap F = K$. Podemos suponer que F y que E_i, $1 \leq i \leq 3$, están contenidos en L, pues si no fuese así, podemos considerar una extensión finita de Galois L'/K contenida en L^{nr} y conteniendo tanto a L como a F, E_1, E_2, E_3 (por ejemplo, la cerradura de Galois L' de $F' := LFE_1E_2E_3/K$). Debido a que $L \subseteq L' \subseteq L^{\mathrm{nr}}$, se tiene que $(L')^{\mathrm{nr}} = L^{\mathrm{nr}}$ y $\tilde{\sigma}_1, \tilde{\sigma}_2, \tilde{\sigma}_3 \in \Lambda((L')^{\mathrm{nr}}/K) = \Lambda(L^{\mathrm{nr}}/K)$ y si probamos que

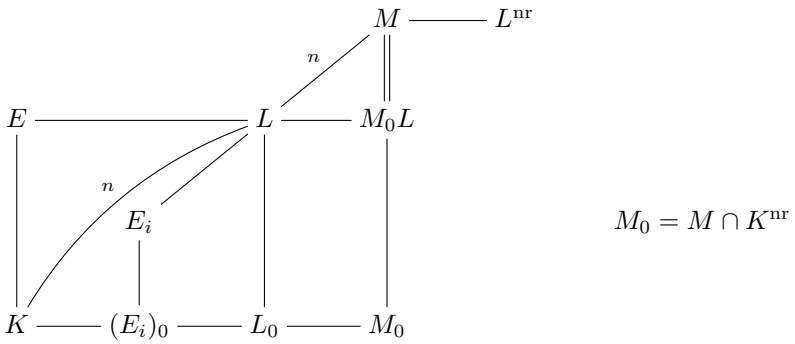
$$\mathrm{N}_{E_3/K}(\pi_3) \equiv \mathrm{N}_{E_1/K}(\pi_1)\,\mathrm{N}_{E_2/K}(\pi_2) \text{ mód } \mathrm{N}_{L'/K}(L')^*,$$

entonces

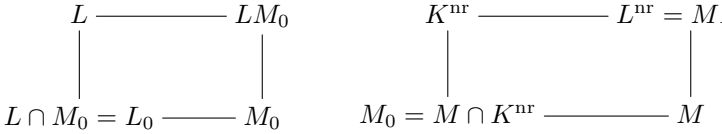
$$N_{E_3/K}(\pi_3) \equiv \mathrm{N}_{E_1/K}(\pi_1)\,\mathrm{N}_{E_2/K}(\pi_2) \text{ mód } \mathrm{N}_{L/K}\,L^*,$$

pues $\mathrm{N}_{L'/K}(L')^* \subseteq \mathrm{N}_{L/K}(L^*)$.

En resumen, podemos suponer que $F, E_i \subseteq L$, $1 \leq i \leq 3$. Sea $n = [L : K]$ y sea M/L la subextensión de L^{nr}/L de grado n, esto es, $[M : L] = n$.



Ahora bien, $M_0 \cap L = M \cap K^{\mathrm{nr}} \cap L \underset{\substack{\uparrow \\ L \subseteq M}}{=} L \cap K^{\mathrm{nr}} = L_0$ y $[M : M_0] = e(M|K) = e(M|L)e(L|K) = e(L|K) = [L : L_0]$, por tanto $[LM_0 : M_0] = [L : L_0] = [M : M_0]$, por lo que $M = LM_0$. Además $[L^{\mathrm{nr}} : K^{\mathrm{nr}}] = [M : M_0]$.



Por tanto $\mathrm{N} = \mathrm{N}_{L/L_0}$ se extiende a N_{M/M_0}. Sean $n_i = \mathrm{gr}_K(\tilde{\sigma}_i)$. Puesto que $\tilde{\sigma}_3 = \tilde{\sigma}_1\tilde{\sigma}_2$, $n_3 = n_1 + n_2$. Sea $\tilde{\sigma}_4 = \varphi^{-n_2}\tilde{\sigma}_1\varphi^{n_2}$ el conjugado de $\tilde{\sigma}_1$ (veremos en un momento para que se hace esta definición), $\mathrm{gr}_K(\tilde{\sigma}_4) = n_4 = n_1 = \mathrm{gr}_K(\tilde{\sigma}_1)$. El campo fijo $L^{\tilde{\sigma}_4} = E_4$ de $\tilde{\sigma}_4$ es el conjugado $E_4 = E_1^{\varphi^{n_2}}$ y $\pi_4 := \pi_1^{\varphi^{n_2}}$ es un elemento primo de E_4. Se tiene que $\mathrm{N}_{E_1/K}(\pi_1) = \mathrm{N}_{E_4/K}(\pi_4)$ y por tanto debemos probar la congruencia

$$N_{E_3/K}(\pi_3) \equiv \mathrm{N}_{E_4/K}(\pi_4)\,\mathrm{N}_{E_2/K}(\pi_2) \text{ mód } \mathrm{N}_{L/K}\,L^*.$$

Sea $\tau_i := \tilde{\sigma}_i^{-1}\varphi^{n_i} \in \mathrm{Gal}(L^{\mathrm{nr}}/K^{\mathrm{nr}}) \cong \mathrm{Gal}(M/M_0)$, se tiene

$$\begin{aligned}\tau_3 = \tilde{\sigma}_3^{-1}\varphi^{n_3} = \big(\varphi^{-n_3}\tilde{\sigma}_3\big)^{-1} &\underset{\substack{\uparrow\\ n_3=n_1+n_2}}{=} \big(\varphi^{-n_1-n_2}\tilde{\sigma}_1\tilde{\sigma}_2\big)^{-1}\\ = \tilde{\sigma}_2^{-1}\tilde{\sigma}_1^{-1}\varphi^{n_1+n_2} = \tilde{\sigma}_2^{-1}\varphi^{n_2}\underbrace{\varphi^{-n_2}\tilde{\sigma}_1^{-1}\varphi^{n_2}}_{\tilde{\sigma}_4^{-1}}\varphi^{n_1} &\underset{\substack{\uparrow\\ n_1=n_4}}{=} \tau_2\tilde{\sigma}_4^{-1}\varphi^{n_4}\\ = \tau_2\tau_4,\end{aligned}$$

por tanto, $\tau_3 = \tau_2\tau_4$ y

$$\begin{aligned}\mathfrak{N}_{E_i}(\pi_i)^{\varphi-1} = \Big(\prod_{\gamma=0}^{[(E_i)_0:K]-1}\pi_i^{\varphi^\gamma}\Big)^{\varphi-1} &= \pi_i^{(\varphi-1)(1+\varphi+\cdots+\varphi^{[(E_i)_0:K]-1})}\\ = \pi_i^{\left(\varphi^{[(E_i)_0:K]}-1\right)} = \pi^{\varphi^{n_i}-1} &\underset{\substack{\uparrow\\ \pi_i\in E_i\\ =(L^{\mathrm{nr}})^{\langle\tilde{\sigma}_i\rangle}}}{=} \pi_i^{\tilde{\sigma}_i^{-1}\varphi^{n_i}-1} = \pi_i^{\tau_i-1},\end{aligned}$$

es decir $\mathfrak{N}(\pi_i)^{\varphi-1} = \pi_i^{\tau_i-1}$.

Sea $A := \mathfrak{N}_{E_3}(\pi_3)\mathfrak{N}_{E_2}(\pi_2)^{-1}\mathfrak{N}_{E_4}(\pi_4)^{-1} \in U_L$, unidad de L pues

$$v_L\big(\mathfrak{N}_{E_i}(\pi_i)\big) = v_L\Big(\prod_{\gamma=0}^{n_i-1}\pi_i^{\varphi^\gamma}\Big) = \sum_{\gamma=0}^{n_i-1}1 = n_i$$

y $v_L(A) = n_3 - n_2 - n_4 = n_3 - n_2 - n_1 = 0$, esto es, $A \in U_L$.

Además $A^{\varphi-1} = \pi_3^{\tau_3-1}\pi_2^{1-\tau_2}\pi_4^{1-\tau_4}$. Ahora bien, por la Proposición 5.4.3 se tiene $L^{\mathrm{nr}} = E_i^{\mathrm{nr}}$ y $E_i \subseteq L \subseteq L^{\mathrm{nr}} = E_i^{\mathrm{nr}}$, esto es, L/E_i es no ramificada, en particular π_i es un elemento primo de L. Se sigue que existen $\varepsilon_2, \varepsilon_3 \in U_L$ con $\pi_2 = \varepsilon_2^{-1}\pi_4$ y $\pi_3 = \varepsilon_3\pi_4$. Sea $\varepsilon_4 = \pi_4^{\tau_2-1} \in U_L$. Se obtiene

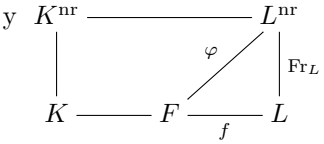
$$(\tau_3-1) + (1-\tau_2) + (1-\tau_4) \underset{\substack{\uparrow\\ \tau_3=\tau_2\tau_4}}{=} (\tau_2-1)(\tau_4-1)$$

y por tanto

$$\begin{aligned}A^{\varphi-1} &= \pi_3^{\tau_3-1}\pi_2^{1-\tau_2}\pi_4^{1-\tau_4} = \varepsilon_3^{\tau_3-1}\pi_4^{\tau_3-1}\varepsilon_2^{\tau_2-1}\pi_4^{1-\tau_2}\pi_4^{1-\tau_4}\\ &= \varepsilon_3^{\tau_3-1}\varepsilon_2^{\tau_2-1}\pi_4^{(\tau_3-1)+(1-\tau_2)+(1-\tau_4)}\\ &= \varepsilon_3^{\tau_3-1}\varepsilon_2^{\tau_2-1}\pi_4^{(\tau_2-1)(\tau_4-1)} = \varepsilon_3^{\tau_3-1}\varepsilon_2^{\tau_2-1}\varepsilon_4^{\tau_4-1}.\end{aligned}$$

Es decir, $A^{\varphi-1}=\prod_{i=2}^{4}\varepsilon_i^{\tau_i-1}$.

Ahora bien, puesto que $F\subseteq L$, se sigue de la Proposición 5.4.3 que $F^{\mathrm{nr}}=L^{\mathrm{nr}}$. Por tanto $F\subseteq L\subseteq L^{\mathrm{nr}}=F^{\mathrm{nr}}$ y L/F es no ramificada. Por tanto $f=[L:F]=f_{L|F}$ y $\varphi^f=\mathrm{Fr}_L$ (recordemos que $\varphi\in\Lambda(L^{\mathrm{nr}}/K)$ es una extensión de Fr_K a L^{nr} y $\mathrm{Gal}(L^{\mathrm{nr}}/F)=\overline{\langle\varphi\rangle}$, $\mathrm{Gal}(L^{\mathrm{nr}}/L)=\overline{\langle\mathrm{Fr}_L\rangle}$).



Ahora M/L es no ramificada por construcción y $H^i(\mathrm{Gal}(M/L),U_M)=0$ para toda $i\in\mathbb{Z}$ y como $A,\varepsilon_i\in U_L$ y $\mathrm{N}_{M/L}U_M=U_L$ pues se tiene $H^0(\mathrm{Gal}(M/L),U_M)=0$, por lo que existen $\tilde{A}_i,\tilde{\varepsilon}_i\in U_M$ con $\mathrm{N}_{M/L}\tilde{A}=A$ y $\mathrm{N}_{M/L}\tilde{\varepsilon}_i=\varepsilon_i$. Por tanto $\mathrm{N}_{M/L}\left(\tilde{A}^{\varphi-1}\right)=\mathrm{N}_{M/L}\left(\prod_{i=2}^{4}\tilde{\varepsilon}_i^{\tau_i-1}\right)$, por lo que existe $x\in U_M$, $\mathrm{N}_{M/L}x=1$ y $\tilde{A}^{\varphi-1}=x\prod_{i=2}^{4}\tilde{\varepsilon}_i^{\tau_i-1}$. Por otro lado $H^{-1}(\mathrm{Gal}(M/K),U_M)=1$ por lo que $\mathrm{núc}\,\mathrm{N}_{M/L}=I_{\mathrm{Gal}(M/K)}U_M$, es decir, $x=\tilde{u}^{\mathrm{Fr}_L-1}$ con $\tilde{u}\in U_M$ y $\mathrm{Fr}_L-1=\varphi^f-1=(\varphi-1)(\varphi^{f-1}+\cdots+\varphi+1)$. Por tanto

$$\tilde{A}^{\varphi-1}=\tilde{u}^{\mathrm{Fr}_L-1}\cdot\prod_{i=2}^{4}\tilde{\varepsilon}_i^{\tau_i-1}=\Big(\prod_{\gamma=0}^{f-1}\tilde{u}^{\varphi^\gamma}\Big)^{\varphi-1}\cdot\prod_{i=2}^{4}\tilde{\varepsilon}_i^{\tau_i-1}.$$

Ahora, $\tau_i\in\mathrm{Gal}(M/M_0)$ ($\tau_i=\tilde{\sigma}_i\varphi^{n_i}\in\mathrm{Gal}(M/M_0)$). Por tanto, considerando que $\mathrm{N}=\mathrm{N}_{L/L_0}$ se extiende a N_{M/M_0}, $M_0\subseteq K^{\mathrm{nr}}$ y por tanto $\varphi-1|_{M_0}=\mathrm{Fr}_K-1$, se sigue que

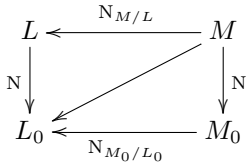
$$\mathrm{N}(\tilde{A}^{\varphi-1})=\mathrm{N}(\tilde{A})^{\varphi-1}=\mathrm{N}(\tilde{A})^{\mathrm{Fr}_K-1}\underset{\mathrm{N}(\tilde{A})\in M_0}{\overset{\uparrow}{=}}$$

$$=\mathrm{N}\Big(\prod_{\gamma=0}^{f-1}\tilde{u}^{\varphi^\gamma}\Big)^{\mathrm{Fr}_K-1}\cdot\underbrace{\prod_{i=2}^{4}\overbrace{\mathrm{N}(\tilde{\varepsilon}_i^{\tau_i})}^{\mathrm{N}(\tilde{\varepsilon}_i)}\mathrm{N}(\tilde{\varepsilon}_i)^{-1}}_{1}=\mathrm{N}\Big(\prod_{\gamma=0}^{f-1}\tilde{u}^{\varphi^\gamma}\Big)^{\mathrm{Fr}_K-1},$$

es decir, $\mathrm{N}(\tilde{A}^{\varphi-1})=\mathrm{N}\left(\prod_{\gamma=0}^{f-1}\tilde{u}^{\varphi^\gamma}\right)^{\mathrm{Fr}_K-1}$.

Se sigue que $\mathrm{N}(\tilde{A})=\mathrm{N}\left(\prod_{\gamma=0}^{f-1}\tilde{u}^{\varphi^\gamma}\right)\cdot y$ con $y\in U_{M_0}$ y $y^{\mathrm{Fr}_K-1}=1$, esto es, $y\in U_K$.

Sea $u:=\mathrm{N}_{M/L}(\tilde{u})$ y recordando que



$\mathrm{N}_{M_0/L_0}\circ\mathrm{N}=\mathrm{N}\circ\mathrm{N}_{M/L}$ y que $\mathrm{N}_{F/K}=\mathrm{N}\circ\mathfrak{N}_F$, se obtiene que

$$
\begin{aligned}
\mathrm{N}(A) &= \mathrm{N}\left(\mathfrak{N}_{E_3}(\pi_3)\mathfrak{N}_{E_2}(\pi_2)^{-1}\mathfrak{N}_{E_4}(\pi_4)^{-1}\right)\\
&= \mathrm{N}_{E_3/K}(\pi_3)\,\mathrm{N}_{E_2/K}(\pi_2)^{-1}\,\mathrm{N}_{E_4/K}(\pi_4)^{-1} \underset{\substack{\uparrow\\ \mathrm{N}=\mathrm{N}_{L/L_0}}}{=} \mathrm{N}\left(\mathrm{N}_{M/L}(\tilde{A})\right)\\
&\underset{\substack{\uparrow\\ \mathrm{N}=\mathrm{N}_{M/M_0}}}{=} \mathrm{N}_{M/M_0}\left(\mathrm{N}_{M/L}(\tilde{A})\right) = \mathrm{N}_{M_0/L_0}(\mathrm{N}(\tilde{A}))\\
&= \mathrm{N}_{M_0/L_0}\left(\mathrm{N}\Big(\prod_{\gamma=0}^{f-1}\tilde{u}^{\varphi^\gamma}\Big)\cdot y\right) \underset{\substack{\uparrow\\ \mathrm{N}_{M_0/L_0}\circ\mathrm{N}\\ =\mathrm{N}\circ\mathrm{N}_{M/L}}}{=} \mathrm{N}\left(\mathrm{N}_{M/L}\Big(\prod_{\gamma=0}^{f-1}\tilde{u}^{\varphi^\gamma}\Big)\right)\underbrace{\mathrm{N}_{M_0/L_0}\,y}_{\substack{\|\\ y^{[M_0:L_0]}}}\\
&\underset{\substack{\uparrow\\ n=[M_0:L_0]}}{=} \mathrm{N}\left(\prod_{\gamma=0}^{f-1}\mathrm{N}_{M/L}\left(\tilde{\mu}\right)^{\varphi^\gamma}\right)\cdot y^n \underset{\substack{\uparrow\\ u=\mathrm{N}_{L/K}(\tilde{u})}}{=} \prod_{\gamma=0}^{f-1}\mathrm{N}(u)^{\varphi^\gamma}\cdot y^n\\
&= \prod_{\gamma=0}^{f-1}\left(\mathrm{N}\circ\mathrm{N}_{M/L}\right)(\tilde{u})^{\varphi^\gamma}y^n = \mathrm{N}\left(\prod_{\gamma=0}^{f-1}u^{\varphi^\gamma}\right)\cdot y^n = \mathrm{N}\circ\mathfrak{N}_L(u)\cdot y^n\\
&= \mathrm{N}_{L/K}(u)\,\mathrm{N}_{L/K}(y)\in \mathrm{N}_{L/K}\,L^*,
\end{aligned}
$$

lo cual prueba el resultado. □

Corolario 5.5.5. *El mapeo de Neukirch,*

$$\mathcal{N}_{L|K}\colon \mathrm{Gal}(L/K)\longrightarrow K^*/\mathrm{N}_{L/K}\,L^*,\quad \mathcal{N}_{L|K}(\sigma):=\mathrm{N}_{F/K}(\pi_F)\ \mathrm{m\acute{o}d}\ \mathrm{N}_{L/K}\,L^*,$$

está bien definido y es un homomorfismo.

Demostración. Sean $\tilde{\sigma}$, $\tilde{\sigma}'$ dos levantamientos de Frobenius de σ. Sean F y F' los campos fijos de $\tilde{\sigma}$ y $\tilde{\sigma}'$ respectivamente y sean $\pi\in F^*$, $\pi'\in (F')^*$ elementos primos. Ordenamos $\tilde{\sigma}$, $\tilde{\sigma}'$ tales que $m=\mathrm{gr}_K(\tilde{\sigma}')-\mathrm{gr}_K(\tilde{\sigma})\geq 0$. Si $m=0$, $\tilde{\sigma}'|_{K^{\mathrm{nr}}}=\tilde{\sigma}|_{K^{\mathrm{nr}}}$ y $\tilde{\sigma}'|_L=\tilde{\sigma}|_L$ de donde obtenemos que $\tilde{\sigma}'=\tilde{\sigma}$ y $\pi'=\pi u$ con $u\in U_F$. Sean M una extensión finita de Galois M/K, $M\subseteq L^{\mathrm{nr}}$ y tal que $L,F\subseteq M$. Puesto que $H^0(\mathrm{Gal}(M/F),U_M)=\{0\}$, existe $\tilde{u}\in U_M$ con $\mathrm{N}_{M/F}(\tilde{u})=u$. Por tanto

$$\mathrm{N}_{F'/K}(\pi')=\mathrm{N}_{F/K}(\pi)\,\mathrm{N}_{M/K}(\tilde{u})\equiv \mathrm{N}_{F/K}(\pi)\ \mathrm{m\acute{o}d}\ \mathrm{N}_{L/K}\,L^*$$

puesto que $\mathrm{N}_{M/K}(\tilde{u})\in \mathrm{N}_{M/K}\,M^*\subseteq \mathrm{N}_{L/K}\,L^*$.

Supongamos ahora que $m>0$. Entonces $\tilde{\tau}=\tilde{\sigma}^{-1}\tilde{\sigma}\in\mathrm{Gal}(L^{\mathrm{nr}}/K)$ es un levantamiento de Frobenius de $1\in\mathrm{Gal}(L/K)$ con $\mathrm{gr}_K(\tilde{\tau})=\mathrm{gr}_K(\tilde{\sigma}')-\mathrm{gr}_K(\tilde{\sigma})=m>0$. Sea M el campo fijo de $\tilde{\tau}$ ($\tilde{\tau}|_L=1$, por lo que $L\subseteq M$) y sea $\pi_M\in M^*$ un elemento primo. Se sigue del Lema 5.5.4

$$\mathrm{N}_{F'/K}(\pi')\underset{\substack{\uparrow\\ \tilde{\sigma}'=\tilde{\sigma}\tilde{\tau}}}{\equiv}\mathrm{N}_{F/K}(\pi)\,\mathrm{N}_{M/K}(\pi_M)\equiv \mathrm{N}_{F/K}(\pi)\ \mathrm{m\acute{o}d}\ \mathrm{N}_{L/K}\,L^*.$$

Esto prueba la independencia de $\mathcal{N}_{L/K}(\pi)(\sigma)$ de la selección del levantamiento $\tilde{\sigma} \in \Lambda(L^{\mathrm{nr}}/K)$ y del elemento primo $\pi_F \in F^*$. Que $\mathcal{N}_{L/K}$ es un homomorfismo se sigue del Lema 5.5.4 puesto que si $\tilde{\sigma}_1, \tilde{\sigma}_2$ son levantamientos de Frobenius de $\sigma_1, \sigma_2 \in \mathrm{Gal}(L/K)$, entonces $\tilde{\sigma}_3 := \tilde{\sigma}_1\tilde{\sigma}_2$ es un levantamiento de Frobenius de $\sigma_3 = \sigma_1\sigma_2$. □

El Teorema de Reciprocidad, el cual asocia a automorfismos de Frobenius elementos primos, es el siguiente resultado.

Teorema 5.5.6. *Si L/K es una subsextensión finita de K^{nr}/K, entonces el inverso del mapeo de reciprocidad*

$$\mathcal{N}_{L|K}\colon \mathrm{Gal}(L/K) \longrightarrow K^*/\,\mathrm{N}_{L/K}\,L^*$$

está dado por $\mathcal{N}_{L|K}(\mathrm{Fr}_{L|K}) = \pi_K \bmod \mathrm{N}_{L/K}\,L^*$ y es un isomorfismo.

Demostración. Se tiene que $\mathrm{Fr}_K \in \Lambda(K^{\mathrm{nr}}/K) = \Lambda(L^{\mathrm{nr}}/K)$ es un levantamiento de Frobenius de $\mathrm{Fr}_{L|K} \in \mathrm{Gal}(L/K)$ y el campo fijo de Fr_K es K. Por tanto $\mathcal{N}_{L|K}(\mathrm{Fr}_{L|K}) \underset{\substack{\uparrow\\ F=K}}{=} \pi_K \bmod \mathrm{N}_{L/K}\,L^*$.

Ahora bien, $H^0(\mathrm{Gal}(L/K), L^*) = \frac{K^*}{\mathrm{N}_{L/K}\,L^*}$ tiene orden $n = [L\colon K]$ el cual también es el orden de $\mathrm{Gal}(L/K)$ y $\pi_K \bmod \mathrm{N}_{L/K}\,L^*$ es un generador de $K^*/\,\mathrm{N}_{L/K}\,L^*$ pues $\pi_K^m = \mathrm{N}_{L/K}(a) \in \mathrm{N}_{L/K}\,L^*$ implica que $m = v_K\big(\mathrm{N}_{L/K}(a)\big) = nv_L(a) \equiv 0 \bmod n$. Por tanto $\mathcal{N}_{L|K}$ es un isomorfismo. □

Observación 5.5.7. Más adelante veremos que $\mathcal{N}_{L|K}$ es un isomorfismo para cualquier extensión abeliana finita L/K, no necesariamente $L \subseteq K^{\mathrm{nr}}$, para lo cual debemos pedir el axioma de campos de clase, es decir lo del Teorema 5.5.1 para cualquier extensión L/K es cíclica.

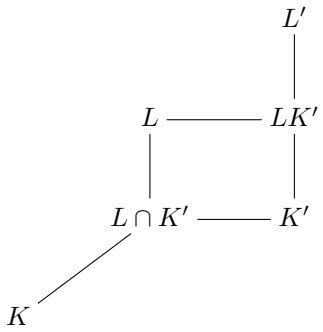
Una de las propiedades fundamentales de $\mathcal{N}_{L|K}$ es que es funtorial.

Teorema 5.5.8. *Sean L/K y L'/K' dos extensiones finitas de Galois de campos locales tales que $K \subseteq K'$ y $L \subseteq L'$. Entonces el diagrama*

$$\begin{array}{ccc} \mathrm{Gal}(L'/K') & \xrightarrow{\mathcal{N}_{L'|K'}} & (K')^*/\,\mathrm{N}_{L'/K'}(L')^* \\ {\scriptstyle \mathrm{rest}\,|_L}\big\downarrow & & \big\downarrow{\scriptstyle \mathrm{N}_{K'/K}} \\ \mathrm{Gal}(L/K) & \xrightarrow{\mathcal{N}_{L|K}} & K^*/\,\mathrm{N}_{L/K}\,L^* \end{array}$$

es conmutativo.

Demostración.



Sean $\sigma' \in \mathrm{Gal}(L'/K')$ y $\sigma = \sigma'|_L$. Si $\tilde{\sigma}' \in \Lambda((L')^{\mathrm{nr}}/K')$ es un levantamiento de Frobenius de σ', entonces $\tilde{\sigma} = \tilde{\sigma}'|_L \in \mathrm{Gal}(L^{\mathrm{nr}}/K)$ es un levantamiento de Frobenius de σ puesto que $\mathrm{gr}_K(\tilde{\sigma}) = f_{K'|K}\,\mathrm{gr}_K(\tilde{\sigma}') \in \mathbb{N}$.

Sea F' el campo fijo de $\tilde{\sigma}'$. Entonces, $F = F' \cap L^{\mathrm{nr}} = F' \cap F^{\mathrm{nr}}$ es el campo fijo de $\tilde{\sigma}$ y puesto que F'/F es totalmente ramificada, $f_{K'|K} = 1$. Por tanto, si $\pi_{F'}$ es un elemento primo de F' y $\pi_F := \mathrm{N}_{F'/F}(\pi_{F'})$ es un elemento primo de F. El teorema se sigue de

$$\begin{aligned}\mathcal{N}_{L|K}(\mathrm{rest}\,|_L\sigma') &= \mathcal{N}_{L|K}\big(\sigma'|_L\big) = \mathrm{N}_{F/K}(\pi_F) = \mathrm{N}_{F/K}\left(\mathrm{N}_{F'/F}(\pi'_F)\right)\\ &= \mathrm{N}_{F'/K}(\pi'_F) = \mathrm{N}_{K'/K}\left(\mathrm{N}_{F'/K'}(\pi'_F)\right)\\ &= \mathrm{N}_{K'/K}\left(\mathcal{N}_{F'|K'}(\sigma')\right).\end{aligned}$$

□

Proposición 5.5.9. *Si L/K es una extensión finita de Galois y $\sigma \in G$, entonces el diagrama*

$$\begin{array}{ccc}\mathrm{Gal}(L/K) & \xrightarrow{\quad\mathcal{N}_{L|K}\quad} & K^*/\,\mathrm{N}_{L/K}\,L^*\\ {\scriptstyle\sigma^*}\downarrow & & \downarrow{\scriptstyle\sigma}\\ \mathrm{Gal}(L^\sigma/K^\sigma) & \xrightarrow{\mathcal{N}_{L^\sigma|K^\sigma}} & (K^\sigma)^*/\,\mathrm{N}_{L^\sigma/K^\sigma}(L^\sigma)^*\end{array}$$

es conmutativa y la flecha izquierda está inducida por conjugación $\tau \longmapsto \sigma^*(\tau) = \sigma^{-1}\tau\sigma$.

Demostración. Sea $\tilde{\tau} \in \Lambda(L^{\mathrm{nr}}/K)$ un levantamiento de Frobenius de $\tau \in \mathrm{Gal}(L/K)$. Sea $\hat{\tau} \in \mathrm{Gal}(k^{\mathrm{sep}}/K)$ una extensión de $\tilde{\tau}$ a k^{sep}. Entonces $\sigma^{-1}\hat{\tau}\sigma$ es un levantamiento de Frobenius de $\sigma^*(\tau)$ puesto que $\mathrm{gr}_{K^\sigma}(\sigma^{-1}\hat{\tau}\sigma) = \mathrm{gr}_K(\hat{\tau}) = \mathrm{gr}_K(\tilde{\tau}) \in \mathbb{N}$.

Sea F el campo fijo de $\tilde{\tau}$. Entonces F^σ es el campo fijo de $\sigma^{-1}\hat{\tau}\sigma|_{(L^\sigma)^{\mathrm{nr}}}$ y si π_F es un elemento primo de F, entonces π_F^σ es un elemento primo de F^σ pues debido a la Proposición 5.4.5 se tiene que $v_K = v_{K^\sigma} \circ \sigma$. Finalmente

$$\mathcal{N}_{F^\sigma|K^\sigma}(\sigma^*(\tau)) = \mathrm{N}_{F^\sigma/K^\sigma}(\pi^\sigma) = \mathrm{N}_{F/K}(\pi)^\sigma = \sigma \circ \mathcal{N}_{L|K}(\tau),$$

es decir, $\mathcal{N}_{F^\sigma|K^\sigma} \circ \sigma^* = \sigma \circ \mathcal{N}_{L|K}$. □

Otra propiedad funtorial de $\mathcal{N}_{L|K}$ está relacionada con el mapeo de transferencia Ver que es res_{-2}. Recordemos como se define el mapeo de transferencia $\mathrm{Ver}\colon G/G' \longrightarrow H/H'$ donde $H < G$ es un subgrupo de índice finito. Sea R un conjunto de representantes de las clases izquierdas de H en G, $G = R \cdot H$, $1 \in R$. Si $\sigma \in G$, para cada $\rho \in R$, se tiene $\sigma\rho = \rho'\sigma_\rho$ con $\sigma_\rho \in H$, $\rho' \in R$. Entonces $\mathrm{Ver}(\sigma \bmod G') = \prod_{\rho\in R} \sigma_\rho \bmod H'$.

Otra descripción de Ver, está dada de la siguiente forma. Sea $\sigma \in G$ y sea $S := \langle\sigma\rangle$ el subgrupo generado por σ. Sea τ recorriendo un sistema de representantes de las clases dobles SxH, esto es, $G = \cup_\tau S\tau H$. Sea $S_\tau := \tau^{-1}S\tau \cap H$ y sea n_τ el mínimo número natural tal que $\sigma_\tau = \tau^{-1}\sigma^{n_\tau} \in H$. Entonces σ_τ genera S_τ y

$$\mathrm{Ver}(\sigma \bmod G') = \prod_\tau \sigma_\tau \bmod H'.$$

Esta última fórmula se obtiene de la anterior tomando como R al conjunto $\{\sigma^i\tau \mid i = 1, \ldots, n_\tau \text{ para toda } n_\tau\}$.

Proposición 5.5.10. *Sea L/K una extensión finita de Galois y sea $K \subseteq K' \subseteq L$. Se tiene un diagrama conmutativo*

$$\begin{array}{ccc} \mathrm{Gal}(L/K')^{\mathrm{ab}} & \xrightarrow{\mathcal{N}_{L|K'}} & (K')^*/\,\mathrm{N}_{L/K'}(L^*) \\ {\scriptstyle \mathrm{Ver}}\uparrow & & \uparrow{\scriptstyle i} \\ \mathrm{Gal}(L/K)^{\mathrm{ab}} & \xrightarrow{\mathcal{N}_{L|K}} & K^*/\,\mathrm{N}_{L/K}(L^*) \end{array}$$

donde i es inducido por la contención $K^* \subseteq (K')^*$.

Demostración. Sean $\mathcal{G} := \mathrm{Gal}(L^{\mathrm{nr}}/K)$ y $\mathcal{H} := \mathrm{Gal}(L^{\mathrm{nr}}/K') \subseteq \mathcal{G}$. Sea $\tilde\sigma$ un levantamiento de Frobenius de $\sigma \in \mathrm{Gal}(L/K)$, F el campo fijo de $\tilde\sigma$ y $S = \mathrm{Gal}(L^{\mathrm{nr}}/F)$. Consideremos la descomposición de las clases dobles $\mathcal{G} = \cup_\tau S\tau\mathcal{H}$. Sean $S_\tau = \tau^{-1}S\tau \cap \mathcal{H}$ y $\tilde\sigma_\tau = \tau^{-1}\tilde\sigma^{n_\tau}\tau \in \mathcal{H}$ como antes.

Sean $G := \mathrm{Gal}(L/K)$, $H := \mathrm{Gal}(L/K') < G$, $\bar S = \langle\sigma\rangle$, $\bar\tau = \tau|_L$ y $\sigma_\tau = \tilde\sigma_\tau|_L$. Entonces $G = \cup_\tau \bar S\bar\tau H$ y por tanto $\mathrm{Ver}(\sigma \bmod G') = \prod_\tau \sigma_\tau (\mathrm{mód}\, H')$.

Para cada τ, sea ω_τ un conjunto completo de representantes de las clases derechas de $\mathcal{H}/S_\tau$. Entonces $\mathcal{H} = \cup_\tau S_\tau\omega_\tau$ y $\mathcal{G} = \cup_{\tau,w_\tau} S\tau\omega_\tau$. Sea F_τ el campo fijo de $\tilde\sigma_\tau$, esto es, el campo fijo de S_τ. Se tiene que $F^\tau = \tau(F)$ es el campo fijo de $\tau^{-1}\tilde\sigma\tau$ de tal forma que F_τ/F^τ es la subextensión de L^{nr}/F^τ de grado n_τ. Sea π_F un elemento primo de F. Por tanto $\pi_{F^\tau} := \pi_F^\tau$ es un elemento primo de F^τ y en consecuencia de F_τ por ser F_τ/F^τ no ramificada. Con la descomposición de clases dobles obtenemos

$$\mathrm{N}_{F/K}(\pi_F) = \prod_{\tau,\omega_\tau} \pi_F^{\tau\omega_\tau} = \prod_\tau \Big(\prod_{\omega_\tau} (\pi_F^\tau)^{\omega_\tau}\Big) = \prod_\tau \mathrm{N}_{F_\tau/K'}(\pi_F^\tau).$$

Puesto que $\tilde\sigma_\tau \in \Lambda(L^{\mathrm{nr}}/K')$ es un levantamiento de Frobenius de $\sigma_\tau \in H = \mathrm{Gal}(L/K')$ se sigue que

$$(i\circ\mathcal{N}_{L|K})(\sigma)=\mathcal{N}_{L|K}(\sigma)=\prod_{\tau}\mathcal{N}_{L|K'}(\sigma_\tau)\equiv\mathcal{N}_{L|K'}\big(\prod_{\tau}\sigma_\tau\big)$$
$$\equiv\mathcal{N}_{L|K'}(\mathrm{Ver}(\sigma \bmod G'))=(\mathcal{N}_{L|K}\circ\mathrm{Ver})(\sigma \bmod G'). \qquad \square$$

Recordemos que si L/K es una extensión cíclica de campos locales. Entonces $H^0(\mathrm{Gal}(L/K),L^*)\cong\mathbb{Z}/[L\colon K]\mathbb{Z}$ y $H^{-1}(\mathrm{Gal}(L/K),L^*)=\{1\}$ (Teorema 5.1.10, Teorema 5.5.1).

Teorema 5.5.11 (Isomorfismo de Neukirch). *Sea L/K una extensión finita de Galois de campos locales. Entonces*

$$\mathcal{N}_{L|K}\colon\ \mathrm{Gal}(L/K)^{\mathrm{ab}}\longrightarrow K^*/\,\mathrm{N}_{L|K}\,L^*$$

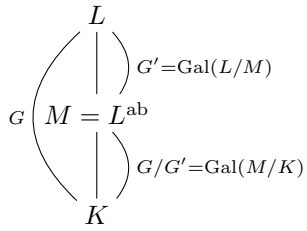
es un isomorfismo.

Demostración. Si M/K es una subextensión de Galois de L/K, entonces por el Teorema 5.5.8, se tiene el diagrama conmutativo

$$\begin{array}{ccccccccc}
1 & \longrightarrow & \mathrm{Gal}(L/M) & \hookrightarrow & \mathrm{Gal}(L/K) & \twoheadrightarrow & \mathrm{Gal}(M/K) & \longrightarrow & 1\\
 & & \downarrow{\scriptstyle \mathcal{N}_{L|M}} & & \downarrow{\scriptstyle \mathcal{N}_{L|K}} & & \downarrow{\scriptstyle \mathcal{N}_{M|K}} & & \\
 & & M^*/\,\mathrm{N}_{L/M}\,L^* & \xrightarrow[\mathrm{N}_{M/K}]{} & K^*/\,\mathrm{N}_{L/K}\,L^* & \longrightarrow & K^*/\,\mathrm{N}_{M/K}\,M^* & \longrightarrow & 1
\end{array} \tag{5.5.2}$$

Este diagrama lo usamos para los tres pasos siguientes para la demostración del resultado.

Paso 1: Podemos suponer que $\mathrm{Gal}(L/K)$ es abeliano. Si probamos el resultado para este caso, y si $M:=L^{\mathrm{ab}}$ es la máxima subextensión abeliana de L/K, entonces $\mathrm{Gal}(L/K)^{\mathrm{ab}}=\mathrm{Gal}(M/K)$ y el subgrupo conmutador $\mathrm{Gal}(L/M)$ de $\mathrm{Gal}(L/K)$ es precisamente el núcleo de $\mathcal{N}_{L|K}$, esto es, $\mathrm{Gal}(L/K)^{\mathrm{ab}}\longrightarrow K^*/\,\mathrm{N}_{L/K}\,L^*$ es inyectivo.



Para ver la suprayectividad, veamos que esta se sigue para extensiones solubles por inducción en el grado del campo. Esto es, en el caso soluble, ya sea $M=L$ o $[L:M]<[L:K]$ y si $\mathcal{N}_{M|K}$ y $\mathcal{N}_{L|M}$ son suprayectivas, entonces por el Lema de la Serpiente aplicada al diagrama (5.5.2), también lo es $\mathcal{N}_{L|K}$. Para

el caso general, sea M el campo fijo de un p-subgrupo de Sylow de $\mathrm{Gal}(L/K)$. En general M/K no es Galois, pero usando la parte izquierda del diagrama (5.5.2), en el cual $\mathcal{N}_{L|K}$ es suprayectiva. Por tanto es suficiente probar que la imagen de $\mathrm{N}_{M/K}$ es el p-subgrupo de Sylow S_p de $K^*/\mathrm{N}_{L/K}\,L^*$, puesto que entonces la imagen de $\mathcal{N}_{L|K}$ contendría los p-subgrupos de Sylow S_p para toda p y por tanto $\mathcal{N}_{L|K}$ será suprayectiva.

Ahora bien, se tiene que el encaje $K^* \subseteq M^*$ induce el homomorfismo natural $i\colon K^*/\mathrm{N}_{L/K}\,L^* \longrightarrow M^*/\mathrm{N}_{L/M}\,L^*$ para el cual $\mathrm{N}_{M/K} \circ i = [M\colon K]$ ($\mathrm{N}_{M/K} \circ i(x) = \mathrm{N}_{M/K}\,x = x^{[M\colon K]}$). Puesto que $\mathrm{mcd}\big([M\colon K], p\big) = 1$, $S_p \xrightarrow{[M:K]} S_p$ es suprayectiva, por lo que S_p está en la imagen de $\mathrm{N}_{M/K}$.

Paso 2: Veamos que podemos suponer que L/K es cíclica. A saber, si M/K recorre las subextensiones cíclicas de L/K, entonces (5.5.2) muestra que el núcleo de $\mathcal{N}_{L|K}$ está contenido en el núcleo del mapeo $\mathrm{Gal}(L/K) \xrightarrow{\psi} \prod_M \mathrm{Gal}(M/K)$. Ahora bien, como L/K es abeliana, se tiene que ψ es inyectiva y por tanto $\mathcal{N}_{L|K}$ es inyectiva.

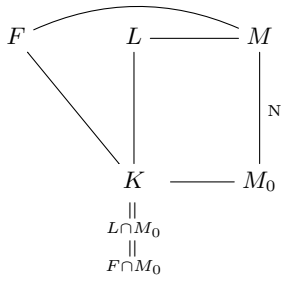
Para ver la suprayectividad, seleccionamos una subextensión cíclica propia M/K de L/K, y la suprayectividad será obtenida por inducción sobre el grado del campo de la misma manera que lo fue en el Paso 1 en el caso soluble.

Paso 3: Sea L/K cíclica. Veamos que podemos suponer que L/K es totalmente ramificada, esto es, $f_{L|K} = 1$. Para ver esta reducción, sea $M = L_0 = K^{\mathrm{nr}} \cap L$ y L/M es totalmente ramificada. Ahora, M/K es no ramificada, por lo que $\mathcal{N}_{M|K}$ es un isomorfismo, Por el Lema de la Serpiente aplicado al diagrama (5.5.2), $\mathrm{N}_{M/K}$ es inyectivo (también esto puede ser deducido por el Teorema 5.1.10, o el Teorema 5.5.1), los grupos de abajo tienen órdenes $[L\colon M], [L\colon K]$ y $[M\colon K]$.

Por tanto, si $\mathcal{N}_{L|K}$ es un isomorfismo, $\mathcal{N}_{L|K}$ lo es. Sea pues L/K cíclica totalmente ramificada, $f_{L|K} = 1$. Sea σ un generador de $\mathrm{Gal}(L/K)$. Puesto que $\mathrm{Gal}(L^{\mathrm{nr}}/K^{\mathrm{nr}}) \cong \mathrm{Gal}(L/K)$.

$$\begin{array}{ccc} K^{\mathrm{nr}} & \text{———} & L^{\mathrm{nr}} \\ \Big| & & \Big| \\ K = L \cap K^{\mathrm{nr}} & \text{———} & L \end{array}$$

Consideremos σ como elemento de $\mathrm{Gal}(L^{\mathrm{nr}}/K^{\mathrm{nr}})$. Por tanto $\tilde{\sigma} := \sigma\,\mathrm{Fr}_L \in \Lambda(L^{\mathrm{nr}}/K)$ es un levantamiento de Frobenius de σ con $\mathrm{gr}_K(\tilde{\sigma}) = 1$. El campo fijo F/K satisface que $F \cap K^{\mathrm{nr}} = K$ y por tanto $f_{F|K} = 1$. Sea $M \subseteq L^{\mathrm{nr}}$ una extensión finita de Galois de K que contiene a F y a L. Sea $\mathrm{N} = \mathrm{N}_{M/M_0}$. Puesto que $f_{F|K} = f_{L|K} = 1$.



$$L \cap M_0 = L \cap M \cap K^{\mathrm{nr}} = L \cap K^{\mathrm{nr}} = L_0 = K,$$

$$F \cap M_0 = F \cap M \cap K^{\mathrm{nr}} = F \cap K^{\mathrm{nr}} = F_0 = K.$$

Por tanto $\mathrm{N}\,|_F = \mathrm{N}_{F/K}$, $\mathrm{N}\,|_L = \mathrm{N}_{L/K}$.

Para la inyectividad de $\mathcal{N}_{L|K}$ debemos probar que si $\mathcal{N}_{L|K}(\sigma^k) = 1$, $0 \leq k < n = [L\colon K]$, entonces $k = 0$. Para este fin consideremos $\pi_F \in F$, $\pi_L \in L$ elementos primos. Puesto que $F, L \subseteq M \subseteq L^{\mathrm{nr}}$, tanto π_F como π_L son elementos primos de M. Sean $\pi_F^k = u\pi_L^k$ con $u \in U_M$. Tenemos

$$\mathcal{N}_{L|K}(\sigma^k) \equiv \mathrm{N}\left(\pi_F^k\right) \equiv \mathrm{N}(u)\,\mathrm{N}\left(\pi_L^k\right) \equiv \mathrm{N}(u) \equiv 1 \text{ mód } \mathrm{N}_{L/K}\, L^*.$$

Por tanto $\mathrm{N}(u) = \mathrm{N}(v)$ con $v \in U_L$. Por tanto $\mathrm{N}(u^{-1}v) = 1$ y por el Teorema 90 de Hilbert existe $a \in M$ con $u^{-1}v = a^{\sigma-1}$. En M, obtenemos $\left(\pi_L^k v\right)^{\sigma-1} = \left(\pi_F^k u^{-1} v\right)^{\tilde{\sigma}-1} \underset{\substack{\uparrow \\ \tilde{\sigma}(\pi_F)=\pi_F}}{=} \left(a^{\sigma-1}\right)^{\tilde{\sigma}-1} = \left(a^{\tilde{\sigma}-1}\right)^{\sigma-1}$.

Se obtiene que si $x := \pi_L^k v a^{1-\tilde{\sigma}}$, $x^{\sigma-1} = 1$ y $x \in K^{\mathrm{nr}}$. Por tanto $x \in K^{\mathrm{nr}} \cap M = M_0$. Ahora bien, $v_{M_0}(x) \in \hat{\mathbb{Z}}$ y $n v_{M_0}(x) \underset{\substack{\uparrow \\ M/M_0 \\ \text{totalmente ramificada}}}{=} v_M(x) = k$, se sigue que $k = 0$. De esta forma hemos obtenido que $\mathcal{N}_{L|K}$ es un mapeo inyectivo.

Finalmente, se tiene que $|H^0(\mathrm{Gal}(L/K), L^*)| = |K^*/\,\mathrm{N}_{L/K}\, L^*| = [L\colon K] = |\,\mathrm{Gal}(L/K)|$, por el axioma de la teoría de campos de clase. Por tanto $\mathcal{N}_{L|K}$ es suprayectiva y es un isomorfismo. □

Tenemos que $\mathcal{N}_{L|K}$ es el inverso del mapeo de reciprocidad

$$(\_, L/K)\colon K^* \longrightarrow \mathrm{Gal}(L/K)^{\mathrm{ab}}$$

con núcleo $\mathrm{N}_{L/K}\, L^*$, el cual es también llamado el símbolo de la norma residual. En particular $\mathcal{N}_{L|K}$ coincide con el mapeo de Nakayama: si $u_{L|K}$ es la clase fundamental de L/K:

$$\theta_{L|K} = u_{L|K} \Cup \_\colon H^{-2}(\mathrm{Gal}(L/K), \mathbb{Z}) \longrightarrow H^0(\mathrm{Gal}(L/K), L^*).$$

Los diagramas conmutativos del Teoremas 5.5.8 y de las Proposiciones 5.5.9 y 5.5.10, se traducen en general de manera inmediata por el hecho de que $\mathcal{N}_{L|K}$ es un isomorfismo y de que $(\_, L/K)/\,\mathrm{N}_{L/K}\, L^* = \mathcal{N}_{L|K}^{-1}$, de la siguiente forma.

Teorema 5.5.12. *Sean L/K y L'/K' extensiones finitas de Galois tales que $K \subseteq K'$ y $L \subseteq L'$ y sea $\sigma \in Gal(k^{\mathrm{sep}}/k)$. Se tienen los diagramas conmutativos*

$$\begin{array}{ccc} (K')^* & \xrightarrow{(\_,L'/K')} & \mathrm{Gal}(L'/K')^{\mathrm{ab}} \\ {\scriptstyle \mathrm{N}_{K'/K}}\downarrow & & \downarrow{\scriptstyle \mathrm{rest}\,|_L} \\ K^* & \xrightarrow{(\_,L/K)} & \mathrm{Gal}(L/K)^{\mathrm{ab}} \end{array}$$

$$\begin{array}{ccc} K^* & \xrightarrow{(\_,L/K)} & \mathrm{Gal}(L/K)^{\mathrm{ab}} \\ {\scriptstyle \sigma}\downarrow & & \downarrow{\scriptstyle \sigma^*} \\ (K^\sigma)^* & \xrightarrow{(\_,L^\sigma/K^\sigma)} & \mathrm{Gal}(L^\sigma/K^\sigma)^{\mathrm{ab}} \end{array}$$

donde $\sigma^*(\tau) = \sigma^{-1}\tau\sigma$. Finalmente, si $K' \subseteq L$, entonces

$$\begin{array}{ccc} (K')^* & \xrightarrow{(\_,L/K')} & \mathrm{Gal}(L/K')^{\mathrm{ab}} \\ \uparrow & & \uparrow{\scriptstyle \mathrm{Ver}} \\ K^* & \xrightarrow{(\_,L/K)} & \mathrm{Gal}(L/K)^{\mathrm{ab}} \end{array}$$

□

Pasando al límite proyectivo, el símbolo de la norma residual se extiende a todas las extensiones de Galois L/K, no necesariamente finitas. Más precisamente, si $\{L_i/K\}$ recorre todas las subextensiones finitas de Galois de L/K, entonces $\mathrm{Gal}(L/K)^{\mathrm{ab}} = \varprojlim_i \mathrm{Gal}(L_i/K)^{\mathrm{ab}}$ y entonces el símbolo de la norma residual $(a, L_i/K)$, con $a \in K^*$, determina un elemento $(a, L/K) \in \mathrm{Gal}(L/K)$ con $(a, L/K)|_{L_i} = (a, L_i/K)$ puesto que tenemos que $(a, L_j/K)|_{L_i} = (a, L_i/K)$ para $L_i \subseteq L_j$ (Teorema 5.5.12). En particular, para la extensión K^{nr}/K, el siguiente resultado describe a $(a, K^{\mathrm{nr}}/K)$.

Teorema 5.5.13. *Se tiene que $\mathrm{gr} \circ (\_, K^{\mathrm{nr}}/K) = v_K$, es decir, en particular*

$$(a, K^{\mathrm{nr}}/K) = \mathrm{Fr}_K^{v_K(a)}.$$

Demostración. Se tiene que $(\pi_K, K^{\mathrm{nr}}/K) = \mathrm{Fr}_K$ pues $(\pi_K, K^{\mathrm{nr}}/K)|_L = (\pi_K, L/K) = \mathrm{Fr}_{L|K} = \mathrm{Fr}_K\,|_L$ para toda subextensión finita L/K de K^{nr}/K y $(u, K^{\mathrm{nr}}/K) = 1$ para $u \in U_K$. Por tanto, si $a = \pi_K^m u$ con $u \in U_K$, se tiene

$$\mathrm{gr}_K(a, K^{\mathrm{nr}}/K) = \mathrm{gr}_K(\mathrm{Fr}_K^m) = m = v_K(a). \qquad \square$$

El Teorema 5.5.13 muestra que la valuación v y, por tanto v_K, es equivalente con la prescripción del símbolo de la norma residual $(\_, K^{\mathrm{nr}}/K)$. Por

tanto, la teoría desarrollada por Neukirch se puede interpretar de la siguiente forma. Si una teoría de campos de clase se desarrolla para $\hat{\mathbb{Z}}$-extensiones K^{nr}/K, entonces, con el axioma de teoría de campos de clase, la teoría se extiende automáticamente, y de manera única, a todas las extensiones abelianas L/K.

5.6. Aplicaciones del TCCL

Regresamos al TCCL. Tenemos las siguientes correspondencias biyectivas:

$$\{\text{extensiones abelianas finitas de } K\} \longleftrightarrow$$
$$\{\text{subgrupos abiertos de } \mathrm{Gal}(K^{\mathrm{ab}}/K)\} \longleftrightarrow$$
$$\{\text{subgrupos abiertos de índice finito en } K^*\}.$$

Las correspondencias están dadas por

$$L \longleftrightarrow \left(\text{núc} : \mathrm{Gal}(K^{\mathrm{ab}}/K) \xrightarrow{\mathrm{rest}\,|_L} \mathrm{Gal}(L/K)\right) \cong \mathrm{Gal}(K^{\mathrm{ab}}/L) \longleftrightarrow$$
$$\longleftrightarrow \text{núc}\left(K^* \xrightarrow{\psi_{L|K}} \mathrm{Gal}(L/K)\right) = \mathrm{N}_{L/K}\, L^*$$

donde la última igualdad proviene del isomorfismo

$$K^*/\,\mathrm{N}_{L/K}\, L^* \xrightarrow[\psi_{L|K}]{\cong} \mathrm{Gal}(L/K).$$

Notemos que en la correspondencia de Galois, los subgrupos abiertos de $\mathrm{Gal}(K^{\mathrm{ab}}/K)$ son de índice finito y por tanto cerrados (ver Observación 5.6.1). En la correspondencia de Galois obtenemos todas las extensiones abelianas de K por medio de todos los subgrupos cerrados.

Observación 5.6.1. Si N es un subgrupo abierto de $\mathrm{Gal}(K^{\mathrm{ab}}/K)$, entonces $\mathrm{Gal}(K^{\mathrm{ab}}/K) = G = \bigcup_{x\in G} Nx$. Como $\{Nx\}_{x\in G}$ es una cubierta abierta de G y G es compacto, existe una subcubierta finita y $G = \bigcup_{i=1}^{m} Nx_i$ por lo que $[G : N] < \infty$, es decir, todo subgrupo abierto de G es de índice finito.

También tenemos que N es cerrado pues si $G = N \bigcup \left(\bigcup_{j=1}^{n} Ny_j\right)$ unión disjunta, entonces $N = G \setminus \left(\bigcup_{j=1}^{n} Ny_j\right)$ el cual es cerrado.

Un subgrupo cerrado de índice finito es abierto, lo cual se demuestra de la misma forma. Sin embargo existen subgrupos cerrados que no son de índice finito y por tanto no son abiertos. Por ejemplo, existe una extensión L de $\mathbb{Q}(\zeta_3)$ tal que $\mathrm{Gal}(L/\mathbb{Q}(\zeta_3)) \cong \mathbb{Z}_3 \times \mathbb{Z}_3 = \langle \sigma, \theta \rangle$ y $\langle \sigma \rangle \cong \mathbb{Z}_3$ es cerrado pero no abierto en G y se tiene $[G : \langle \sigma \rangle] = \infty$.

Corolario 5.6.2. *Sea K un campo local. Entonces hay una correspondencia biyectiva*

$$\{\textit{extensiones abelianas finitas de } K\} \longleftrightarrow \{\textit{subgrupos abiertos de índice finito de } K^*\}$$

la cual está dada de la siguiente forma: a la extensión abeliana finita L/K le corresponde el subgrupo $\mathrm{N}_{L/K} L^*$ de K^* ($L \longleftrightarrow \mathrm{N}_{L/K} L^*$).

Más aún esta correspondencia satisface que si a L le corresponde H ($L \longleftrightarrow H$), entonces $[L : K] = [K^* : H]$ y además si a L' le corresponde H' ($L' \longleftrightarrow H'$), se tiene que $L \supseteq L' \iff H \subseteq H'$. □

Observación 5.6.3. Se tiene que U_K es un conjunto abierto de K^* y además $K^*/U_K \cong \mathbb{Z}$ por lo que U_K no puede corresponder a ninguna extensión abeliana de K pues $\mathbb{Z}$ no es un grupo profinito y por lo tanto no puede ser el grupo de Galois de ninguna extensión.

Notación y definición 5.6.4. El mapeo $\mathrm{rest}_L \circ \rho_K \colon K^* \to \mathrm{Gal}(L/K)$ se llama el *símbolo residual de la norma* o *símbolo residual nórmico* (norm residue symbol en inglés) o *mapeo local de Artin* y se denota $K^* \xrightarrow{(\ ,L/K)} \mathrm{Gal}(L/K)$. Se puede considerar a $(\ ,L/K)$ o a $\psi_{L/K}$ como el símbolo de Artin local o mapeo local de Artin.

Definición 5.6.5. Sea $K = \mathbb{R}$. Se define $U_K^{(0)} = \mathbb{R}^*$ y $U_K^{(1)} = \mathbb{R}^+$. Para $K = \mathbb{C}$, se define $U_K^{(0)} = \mathbb{C}^*$.

5.6.1. Ley de Reciprocidad para $K = \mathbb{R}$ y para $K = \mathbb{C}$.

Proposición 5.6.6. *La ley de reciprocidad se cumple para $K = \mathbb{R}$ y para $K = \mathbb{C}$.*

Demostración. Si $K = \mathbb{R}$, se tiene $\mathbb{R}^{\mathrm{ab}} = \mathbb{C}$ y $\mathbb{R}$ y $\mathbb{C}$ son las únicas dos extensiones abelianas (y de hecho algebraicas) de $\mathbb{R}$. Se tiene que $\mathbb{R}^*$ tiene únicamente dos subgrupos de índice finito los cuales son $\mathbb{R}^+$ y $\mathbb{R}^*$ Además se cumple que $\mathrm{N}_{\mathbb{R}/\mathbb{R}} \mathbb{R}^* = \mathbb{R}^*$ y $\mathrm{N}_{\mathbb{C}/\mathbb{R}} \mathbb{R}^* = \mathbb{R}^+ = (\mathbb{R}^*)^2$.

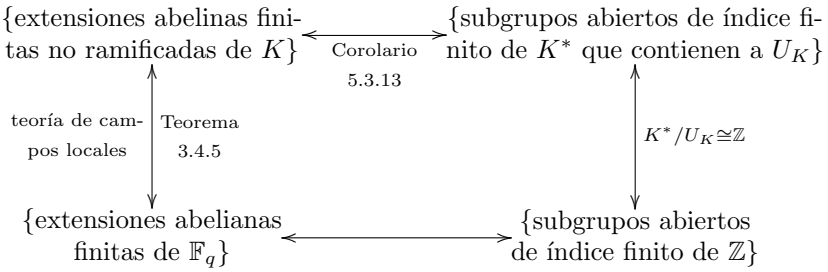
Sea $\rho_{\mathbb{R}} \colon \mathbb{R}^* \longrightarrow \mathrm{Gal}(\mathbb{R}^{\mathrm{ab}}/\mathbb{R}) = \mathrm{Gal}(\mathbb{C}/\mathbb{R}) = \{1, J\}$ dada por

$$\rho_{\mathbb{R}}(x) = \mathrm{sgn}(x) = \begin{cases} 1 & \text{si } x > 0, \\ J = -1 & \text{si } x < 0. \end{cases}$$

Entonces $\rho_{\mathbb{R}}$ cumple las condiciones del Teorema TCCL para $K = \mathbb{R}$.

Si ahora consideramos $K = \mathbb{C}$, $\mathbb{C}$ es la única extensión algebraica de $\mathbb{C}$ y el único subgrupo abierto de índice finito en $\mathbb{C}^*$ es $\mathbb{C}^*$. Por tanto $\rho_{\mathbb{C}} \colon \mathbb{C}^* \longrightarrow \mathrm{Gal}(\mathbb{C}/\mathbb{C}) = \{1\}$, $z \mapsto 1$ satisface las condiciones del Teorema TCCL para $K = \mathbb{C}$. □

Proposición 5.6.7. *Sea K un campo local con campo residual $\mathbb{F}_q$ y valuación $v = v_{\mathfrak{p}}$. Sea $\mathcal{O}_K$ el anillo de valuación de K. Entonces*



(recordemos (Corolario 5.3.13*) que cuando L/K es una extensión abeliana finita no ramificada, $U_K \subseteq \mathrm{N}_{L/K} L^*$, por eso se tiene la correspondencia dada por la flecha vertical del diagrama).* □

Observación 5.6.8. Se tiene que $\rho_K \colon K^* \to \mathrm{Gal}(K^{\mathrm{ab}}/K)$ nos proporciona una biyección entre las extensiones abelianas finitas de L/K y subgrupos abiertos de índice finito en K^*: $L \longleftrightarrow \mathrm{N}_{L/K} L^* (U \longleftrightarrow \rho_K^{-1}(U))$, es decir $K^*/\mathrm{N}_{L/K} L^* \cong \mathrm{Gal}(L/K)$.

Si L está dado, es "fácil" calcular $\mathrm{N}_{L/K} L^*$, pero dado $H < K^*$ con H subgrupo abierto de índice finito, ¿como calcular L tal que $H = \mathrm{N}_{L/K} L^*$?

Ese es el problema que no nos permite dar una descripción explícita de todas las extensiones abelianas finitas de K. Por supuesto, si ρ_K se da explícitamente, resolvemos parcialmente este problema.

Resulta ser que ρ_K es bastante explícito si L/K es no ramificada. De hecho se tiene que si L/K es no ramificada, recordando que estamos en campos locales, entonces $\mathrm{Gal}(L/K) \cong \mathrm{Gal}(\tilde{L}/\tilde{K})$ donde $\tilde{L}$ y $\tilde{K}$ son los campos residuales. Más aún, si $\tilde{K} = \mathbb{F}_q$ y $\tilde{L} = \mathbb{F}_{q^n}$ con $n = [\tilde{L} : \tilde{K}] = [L : K]$, entonces $\rho_K \colon K^* \to \mathrm{Gal}(L/K)$ satisface que $\rho_K(a) = \tau^{v_{\mathfrak{p}}(a)}$ (Teorema 5.2.2), donde τ es el automorfismo de Frobenius de L/K, el cual es el generador de $\mathrm{Gal}(L/K)$ inducido por el automorfismo de Frobenius de $\tilde{L}/\tilde{K}$, es decir, $\tau \colon \tilde{L} \to \tilde{L}$, $\bar{x} \mapsto \bar{x}^q$. Notemos que bajo ρ_K tenemos que si π es un elemento primo de K entonces $\pi \longleftrightarrow \tau$.

De hecho, por TCCL (II). que es el contenido del Teorema 5.2.2, se tiene, $\rho_K(\pi) = \rho_{\mathbb{F}_q}(v_K(\pi)) = \tau$, de donde

$$\mu\rho_K(a) = \rho_K(a)|_{\mathbb{F}_q^{\mathrm{ab}}} = \rho_{\mathbb{F}_q}(v_K(a)) = \tau^{v_K(a)}.$$

Para extensiones ramificadas la historia es muy diferente y se requiere cohomología de grupos para obtenerla. El Teorema de Tate y el grupo de Brauer nos dan el mapeo de Nakayama, esto es, ρ_K^{-1}. Sin embargo, $\psi_{L|K}(a) = (a, L/K)$, el símbolo de la norma residual local o mapeo de Artin local, no es explícito en lo absoluto. Otras aproximaciones para el estudio de ρ_K son por medio de los grupos formales de Lubin-Tate (1965) y también por medio

de álgebras cíclicas (Hasse et. at.). Haremos algo explícito el mapeo local de Artin y obtendremos el Teorema de Existencia en completa generalidad, por medio de los grupos formales de Lubin–Tate en la Sección 5.8.1.

Más aún, los grupos de Lubin–Tate nos permiten encontrar explícitamente la máxima extensión abeliana de un campo local K (Teorema 5.8.67). Podemos considerar este resultado como el análogo al Teorema de Kronecker–Weber para campos locales.

5.7. Teorema de Existencia

De la teoría general de campos locales, tenemos que si L/K es una extensión finita y separable, $\mathrm{N}_{L/K}\colon L^* \longrightarrow K^*$ es continua y $\mathrm{N}_{L/K} L^*$ es un subgrupo cerrado en K^*. Por el Teorema de Reciprocidad, se tiene que L/K es una extensión finita de Galois, entonces $K^*/\mathrm{N}_{L/K} L^* \cong G_{L|K}^{\mathrm{ab}}$ y como $G_{L|K}$ es un grupo finito, $[K^*\colon \mathrm{N}_{L/K} L^*] < \infty$ y por tanto $\mathrm{N}_{L/K} L^*$ es un subgrupo abierto ($\mathrm{N}_{L/K} L^* = K^* \setminus \underbrace{\big(\bigcup_{x \notin \mathrm{N}_{L/K} L^*} x \,\mathrm{N}_{L/K} L^*\big)}_{\text{finita}}$). De hecho, si A es un subgrupo de K^* de índice finito, A es abierto $\iff$ A es cerrado pues $A = K^* \setminus \big(\bigcup_{x \notin A} xA\big)$.

Proposición 5.7.1. *Si* $\operatorname{car} K = 0$*, entonces todo subgrupo de índice finito, es abierto y, por tanto, cerrado.*

Demostración. Tenemos que para $m \in \mathbb{N}$ tal que $\operatorname{car} K \nmid m$, en nuestro caso, $m \in \mathbb{N}$ es arbitrario, $(K^*)^m$ es abierto y de índice finito en K^* (Proposición 5.3.1). Su $H < K^*$, $[K^* : H] = m < \infty$, entonces $(K^*)^m \subseteq H$ y $(K^*)^m$ es un subgrupo abierto. Por tanto $H = \bigcup_{x \in H} x(K^*)^m$ es abierto. □

Observación 5.7.2. Si $\operatorname{car} K = p > 0$, $(K^*)^m$ es abierto para m tal que $\operatorname{car} K \nmid m$. Sin embargo el resultado es falso para $m = p$. Esto es, $(K^*)^p$ no es abierto en K^* pues si lo fuese, existiría $m \in \mathbb{N}$ tal que $U_K^{(m)} \subseteq (K^*)^p$. En particular se tendría que si π es un elemento primo de K, entonces $1+\pi^m = x^p$ para algún $x \in K^*$, por lo que $\pi^m = x^p - 1 = (x-1)^p$ y $m = v_K(\pi^m) = pv_K(x-1)$ y en particular se debería tener que $p|m$ para toda $m \geq m_0$ pues $U_K^{(m)} \subseteq U_K^{(m_0)} \subseteq (K^*)^p$, lo cual es absurdo.

Además, existen subgrupos de índice finito en K^* que no son cerrados y por tanto no son abiertos. Por ejemplo, tenemos que $U_K^{(1)} \cong \mathbb{Z}_p^\infty$. Sea $D = \{(\xi_n)_{n=1}^\infty \in \mathbb{Z}_P^\infty \mid \xi_n = 0 \text{ para casi todo } n\}$. Se tiene que D es denso en $U_K^{(1)}$. Entonces, existe un morfismo no trivial de grupos abelianos $\varphi\colon G \longrightarrow \mathbb{Z}/p\mathbb{Z}$ tal que $D \subseteq \operatorname{núc} \varphi$ y de aquí se deduce que K^* tiene subgrupos no cerrados de índice p.

Por otro lado, se tiene que $(K^*)^p$ es cerrado pues $K^* = \mathbb{Z} \times U_K$ por lo que $(K^*)^p = p\mathbb{Z} \times (U_K)^p$ y $(K^*)^p/(U_K)^p$ es un subgrupo discreto de K^*/U_K el cual es Hausdorff por ser U_K un subgrupo cerrado. Se sigue que $(K^*)^p$ es cerrado en K^* (Lema3.3.8). También se sigue que $(K^*)^p$ no es de índice finito en K^* al ser cerrado pero no abierto.

En el Corolario 5.7.6 probaremos que $D_K = \{1\}$ para K de característica 0. Para ver que $D_K = \text{núc}\,\rho_K = \{1\}$ en el caso $\operatorname{car} K = p > 0$, y que de hecho sirva para cualquier característica, usaremos los grupos de Lubin-Tate para probar que $\langle \pi_K \rangle \times U_K^{(n)}$ es un grupo de normas para toda $n \in \mathbb{N} \cup \{0\}$. Puesto que $\langle \pi_K^f \rangle \times U_K$ es el grupo de normas de la extensión no ramificada de K de grado f, se tiene que

$$D_K \subseteq \big(\langle \pi_K^f \rangle \times U_K\big) \cap \big(\langle \pi_K \rangle \times U_K^{(n)}\big) = \langle \pi_K^f \rangle \cup U_K^{(n)}$$

para toda $f \in \mathbb{N}$ y para toda $n \in \mathbb{N} \cup \{0\}$. Por lo tanto

$$D_K \subseteq \bigcap_{\substack{f \in \mathbb{N} \\ n \in \mathbb{N} \cap \{0\}}} \big(\langle \pi_K^f \rangle \times U_K^{(n)}\big) = \{1\}.$$

En resumen, $\rho_K \colon K^* \longrightarrow G_K^{\text{ab}}$ es un monomorfismo.

El Teorema de Existencia establece que si $H < K^*$ es un subgrupo abierto de índice finito, equivalentemente, un subgrupo cerrado de índice finito, existe una extensión abeliana finita L/K tal que $H = \mathrm{N}_{L/K}\, L^*$, es decir, H es un *grupo de normas*.

Definición 5.7.3. Un *grupo de normas* de K^* es un subgrupo $H < K^*$ de índice finito tal que $H = \mathrm{N}_{L/K}\, L^*$ para alguna extensión abeliana finita L de K.

Teorema 5.7.4. *Si H es un subgrupo de K^* que contiene a un subgrupo de normas, $H \supseteq \mathrm{N}_{L/K}\, L^*$, entonces H es también un grupo de normas y si $H = \mathrm{N}_{M/K}\, M^*$ entonces $M \subseteq L$.*

Demostración. Sea L/K una extensión abeliana tal que $\mathrm{N}_{L/K}\, L^* \subseteq H$, entonces $\rho_K|_L = \psi_{L|K} \colon K^* \longrightarrow G_{L|K}$ es tal que $\text{núc}\,\psi_{L|K} = \mathrm{N}_{L/K}\, L^*$. Como H es abierto y $\psi_{L|K}$ es una biyección entre los grupos H tales que $\mathrm{N}_{L/K}\, L^* \subseteq H \subseteq K^*$ y los subgrupos de $G_{L|K}$, digamos que $\psi_{L|K}(H) = \mathcal{G} < G_{L|K}$, por lo que $\mathcal{G} = G_{L|M}$ para algún campo M (de hecho, $M = L^{\mathcal{G}}$) tal que $K \subseteq M \subseteq L$. Se tiene

$$\psi_{L|K}|_H \colon H \longrightarrow G_{L|K} \quad \text{por tanto} \quad \tilde{\psi}_{L|K} \colon K^*/H \longrightarrow \frac{G_{L|K}}{G_{L|M}} \cong G_{M|K}$$

y

$$H = \text{núc}\,\tilde{\psi}_{L|K} = \mathrm{N}_{M|K}\, M^*.$$

Aquí hemos usado la conmutatividad del diagrama

$$\begin{array}{ccc} K^* & \xrightarrow[\cong]{\psi_{L|K}} & G_{L|K} \\ \| & & \downarrow{\scriptstyle \text{rest}\,|_M} \\ K^* & \xrightarrow[\cong]{\psi_{M|K}} & G_{M|K} \end{array} \qquad \begin{array}{c} \sigma \\ \downarrow \\ \sigma|_M \end{array}$$

□

Proposición 5.7.5. *Sea K un campo local de característica 0. Sea $m \in \mathbb{N}$. Entonces $(K^*)^m$ es un grupo de normas de K^*.*

Demostración. Sea ζ_m una raíz m-primitiva de la unidad. Supongamos primero que $\zeta_m \in K^*$. Para $a \in K^*$, sea $L_a := K(\sqrt[m]{a})$. Sea $L := \bigcup_{a\in K^*} L_a = K\big(\sqrt[m]{K^*}\big)$. Se tiene que L es la máxima extensión abeliana de exponente m (Teorema 2.4.2). Además, por la Teoría de Kummer, tenemos que

$$\begin{aligned} \chi\big(\operatorname{Gal}(L/K)\big) &= \operatorname{Hom}\big(\operatorname{Gal}(L/K), \mathbb{Q}/\mathbb{Z}\big) \\ &= \operatorname{Hom}\big(\operatorname{Gal}(L/K), \langle\zeta_m\rangle\big) \cong K^*/(K^*)^m. \end{aligned}$$

Puesto que $K^*/(K^*)^m$ es finito, $\operatorname{Gal}(L/K)$ es finito y L/K es una extensión finita. Ahora $K^*/\,\mathrm{N}_{L/K}\, L^* \cong \operatorname{Gal}(L/K)$ y $K^*/\,\mathrm{N}_{L/K}\, L^*$ tiene exponente m lo cual implica que $(K^*)^m \subseteq \mathrm{N}_{L/K}\, L^*$ y, por otro lado,

$$[K^* : (K^*)^m] = \big|\chi\big(\operatorname{Gal}(L/K)\big)\big| = \big|\operatorname{Gal}(L/K)\big| = [L\colon K] = [K^*\colon \mathrm{N}_{L/K}\, L^*].$$

Se sigue que $\mathrm{N}_{L/K}\, L^* = (K^*)^m$ y por tanto $(K^*)^m$ es un grupo de normas.

Ahora, si $\zeta_m \notin K^*$, sea $K_1 := K(\zeta_m)$. Por el caso anterior, sea $L_1 := K_1\big(\sqrt[m]{K_1^*}\big)$ y $\mathrm{N}_{L_1/K_1}\, L_1^* = (K_1^*)^m$. Sea L_0 cualquier extensión finita de Galois de K con $L_1 \subseteq L_0$, entonces

$$\begin{aligned} \mathrm{N}_{L_0/K}\, L_0^* = \mathrm{N}_{K_1/K}\big(\mathrm{N}_{L_0/K_1}\, L_0^*\big) &\subseteq \underset{\substack{\uparrow \\ L_1 \subseteq L_0}}{\mathrm{N}_{K_1/K}\big(\mathrm{N}_{L_1/K_1}\, L_1^*\big)} \\ = \mathrm{N}_{K_1/K}\big((K_1^*)^m\big) &\subseteq (K^*)^m. \end{aligned}$$

Puesto que $(K^*)^m$ contiene a un grupo de normas, por el Teorema 5.7.4, $(K^*)^m$ es un grupo de normas. □

Corolario 5.7.6. *Sea K un campo local de característica 0. Entonces el isomorfismo de reciprocidad $\rho_K\colon K^* \longrightarrow \operatorname{Gal}(K^{\mathrm{ab}}/K)$ es un monomorfismo. Esto es,* $\text{núc}\,\rho_K = D_K = \bigcap_{\substack{L/K \text{ abeliana} \\ \text{finita}}} \mathrm{N}_{L/K}\, L^* = \{1\}$.

Demostración. Se tiene $D_K \subseteq \bigcap_{m=1}^{\infty}(K^*)^m = \{1\}$ (Corolario 3.2.7). □

Teorema 5.7.7 (Teorema de Existencia en característica 0). *Sea K un campo local de característica 0. Los grupos de normas de K^* son precisamente los subgrupos abiertos (y por tanto cerrados) de índice finito en K^*.*

Demostración. Si H es un grupo de normas, $H = \mathrm{N}_{L/K} L^*$ con L/K una extensión finita abeliana. Se tiene $[K^*\colon H] = [K^*\colon \mathrm{N}_{L/K} L^*] = [L\colon K] < \infty$ y es cerrado (Teorema 3.3.7), por tanto abierto.

Recíprocamente, si H es un subgrupo abierto de índice finito en K^*, $[K^*\colon H] = m$, entonces $(K^*)^m \subseteq H$ y como $(K^*)^m$ es un grupo de normas, H también lo es (Teorema 5.7.4). □

Notemos que no necesitamos que H sea abierto. De hecho, en la Proposición 5.7.1, vimos que en característica 0, todo subgrupo de índice finito, es abierto y por tanto cerrado.

Teorema 5.7.8. *Sea K un campo local de característica 0. Entonces los grupos de normas son precisamente los grupos que contienen a algún $\langle \pi^f \rangle \times U_K^{(n)}$ para $n \in \mathbb{N} \cup \{0\}$, $f \in \mathbb{N}$.*

Demostración. Se tiene que $\langle \pi^f \rangle \times U_K^{(n)}$ tiene índice finito en K^*:

$$K^* = \langle \pi \rangle \times U_K^{(0)}, \quad [K^*\colon \langle \pi^f \rangle \times U_K^{(n)}] = \begin{cases} f(q-1)q^{n-1} & (n \geq 1), \\ f & (n = 0) \end{cases}$$

y por tanto $\langle \pi^f \rangle \times U_K^{(n)}$ es un grupo de normas. Se sigue que si H contiene a $\langle \pi^f \rangle \times U_K^{(n)}$, H es un grupo de normas.

Recíprocamente, si H es un grupo de normas, H es abierto y como $\{U_K^{(n)}\}_{n \in \mathbb{N} \cup \{0\}}$ es un sistema fundamental de vecindades de 1, existe $n \in \mathbb{N} \cup \{0\}$ con $U_K^{(n)} \subseteq H$. Ahora bien, si $f = [K^*\colon H]$, entonces $\pi^f \in H$ por lo que $\langle \pi^f \rangle \times U_K^{(n)} \subseteq H$. □

Corolario 5.7.9. *Sea $H < K^*$, K un campo local de característica 0. Entonces lo siguiente es equivalente:*

(1) *H es un grupo de normas;*
(2) *H es un subgrupo abierto de índice finito;*
(3) *H es un subgrupo cerrado de índice finito;*
(4) *H es un subgrupo de índice finito.*
(5) *H contiene a $(K^*)^m$ para algún $m \in \mathbb{N}$.*
(6) *H contiene a $\langle \pi \rangle \times U_K^{(n)}$ para algunos $f \in \mathbb{N}$ y $n \in \mathbb{N} \cup \{0\}$.* □

Definición 5.7.10 (Conductor local). Dada una extensión abeliana finita L/K de campos locales, se tiene que $\mathrm{N}_{L/K} L^*$ es un subgrupo abierto pues es cerrado de índice finito (Teorema 3.3.7) y que contiene a 1. Por tanto

$U_K^{(n)} \subseteq \mathrm{N}_{L/K}\, L^*$ para alguna $n \geq 0$ pues $\{U_K^{(n)}\}_{n\in\mathbb{N}}$ es un sistema fundamental de vecindades de 1 (ver Subsección 3.2). Sea n_0 el mínimo entero no negativo tal que $U_K^{(n_0)} \subseteq \mathrm{N}_{L/K}\, L^*$.

Entonces denotamos $n_0 := c_{\mathfrak{p}}$ con $\mathfrak{p} = \mathfrak{p}_K$ el lugar de K. Se define el *conductor local* de L/K por

$$\mathfrak{f}_{L/K} = \mathfrak{f}_{\mathfrak{p}} = \mathfrak{f} = \mathfrak{p}_K^{n_0} = \mathfrak{p}^{n_0} = \mathfrak{p}^{c_{\mathfrak{p}}}.$$

Si L/K es una extensión de campos globales y consideramos las completaciones $L_{\mathfrak{P}}/K_{\mathfrak{p}}$, entonces denotamos $\mathfrak{f}_{L_{\mathfrak{P}}/K_{\mathfrak{p}}} = \mathfrak{f}_{\mathfrak{p}}$.

Teorema 5.7.11. *Una extensión abeliana finita de campos locales L/K es no ramificada $\iff \mathfrak{f}_{L/K} = \mathfrak{f} = 1$, esto es, $\iff c_{\mathfrak{p}} = n_0 = 0$.*

Demostración. Por el Corolario 5.3.13, L/K es no ramificada $\iff U_K \subseteq \mathrm{N}_{L/K}\, L^* \iff n_0 = c_{\mathfrak{p}} = 0$. □

5.7.1. Red de normas y de subcampos

Teorema 5.7.12. *Sean L/K y L'/K' dos extensiones de Galois tales que $K \subseteq K'$ y $L \subseteq L'$. Entonces el siguiente diagrama es conmutativo*

$$\begin{array}{ccc} \mathrm{Gal}^{\mathrm{ab}}(L'/K') & \xrightarrow[\psi_{L'/K'}^{-1}]{} & (K')^*/\,\mathrm{N}_{L'/K'}((L')^*) \\ \Big\downarrow{\scriptstyle \mathrm{rest}_L} & & \Big\downarrow{\scriptstyle \mathrm{N}_{K'/K}} \\ \mathrm{Gal}^{\mathrm{ab}}(L/K) & \xrightarrow[\psi_{L/K}^{-1}]{} & K^*/\,\mathrm{N}_{L/K}(L^*) \end{array}$$

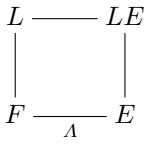
Equivalentemente, tenemos el diagrama conmutativo

$$\begin{array}{ccc} (K')^* & \xrightarrow[\psi_{L'/K'}]{} & \mathrm{Gal}^{\mathrm{ab}}(L'/K') \\ \Big\downarrow{\scriptstyle \mathrm{N}_{K'/K}} & & \Big\downarrow{\scriptstyle \mathrm{rest}_L} \\ K^* & \xrightarrow[\psi_{L/K}]{} & \mathrm{Gal}^{\mathrm{ab}}(L/K) \end{array}$$

Demostración. Es el Teorema 5.5.12. □

Como consecuencia del Teorema 5.7.12 tenemos el siguiente resultado (para el caso global, ver el Teorema6.9.5).

Teorema 5.7.13. *Sea E/F una extensión abeliana finita de campos locales y sea E el campo de clase de $\Lambda \subseteq F^*$, es decir, $\mathrm{N}_{E/F}\, E^* = \Lambda$. Sea L/F una extensión finita y separable. Entonces LE/L es una extensión finita y el grupo de normas correspondiente es $\mathrm{N}_{L/F}^{-1}(\Lambda)$.*



Demostración. Sea $\psi_{EL/L}\colon L^* \longrightarrow \mathrm{Gal}(LE/L)$ el mapeo de Artin. El grupo de normas correspondiente a LE/E es $\mathrm{núc}\,\psi_{LE/L}$, esto es, $L^*/\,\mathrm{núc}\,\psi_{LE/E} \cong \mathrm{Gal}(LE/L)$. Por el Teorema 5.7.12 tenemos $\mathrm{rest}\circ\psi_{LE/L} = \psi_{E/F}\circ \mathrm{N}_{L/F}$. Por tanto

$$\begin{gathered} x \in \mathrm{núc}\,\psi_{LE/E} \iff \psi_{LE/E}(x) = 1 \iff \\ \mathrm{rest}\circ\psi_{LE/E}(x) = 1 = \psi_{E/F}\circ \mathrm{N}_{L/F}(x) \iff \\ \mathrm{N}_{L/F}(x) = \mathrm{núc}\,\psi_{E/F} = \Lambda \iff x \in \mathrm{N}_{L/F}^{-1}(\Lambda). \end{gathered}$$

□

Para probar el Teorema de Existencia en general, primero demostramos el siguiente importante resultado.

Teorema 5.7.14. *Sea K un campo local. Los grupos de normas $H_L := \mathrm{N}_{L/K}\,L^*$ de K^* forman una red y el mapeo $L \longrightarrow H_L$ es una correspondencia biyectiva que cambia contenciones y que de hecho es un isomorfismo de redes entre la red de las extensiones abelianas finitas de K y la red de los grupos de normas de K^*. Por tanto*

(1) $H_{L_1} \supseteq H_{L_2} \iff L_1 \subseteq L_2$;
(2) $H_{L_1L_2} = H_{L_1} \cap H_{L_2}$;
(3) $H_{L_1\cap L_2} = H_{L_1}H_{L_2}$.

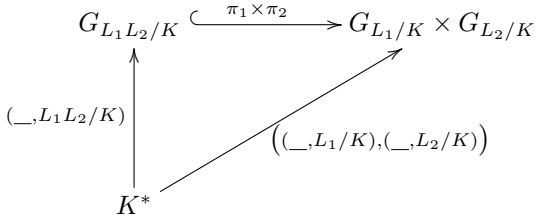
Demostración. Si L_1 y L_2 son dos extensiones abelianas finitas de K entonces se tiene $\mathrm{N}_{L_1L_2/K} = \mathrm{N}_{L_i/K}\,\mathrm{N}_{L_1L_2/L_i}$, $i = 1, 2$, de donde obtenemos que $H_{L_1L_2} \subseteq H_{L_1} \cap H_{L_2}$.

Ahora si $a \in H_{L_1} \cap H_{L_2}$, entonces $(a, L_1L_2/K)|_{L_i} = (a, L_i/K) = 1$, para $i = 1, 2$.

Se tiene el diagrama con filas exactas

$$\begin{array}{ccccccccc} 1 & \longrightarrow & \mathrm{N}_{L_1L_2/K}\left((L_1L_2)^*\right) & \longrightarrow & K^* & \xrightarrow[(a,L_1L_2/K)]{} & G_{L_1L_2/K} & \longrightarrow & 1 \\ & & & & & & \downarrow{\scriptstyle \pi_i=\mathrm{rest}\,|_{L_i}} & & \\ 1 & \longrightarrow & \mathrm{N}_{L_i/K}\,L^* & \longrightarrow & K^* & \xrightarrow[(a,L_i.K)]{} & G_{L_i/K} & \longrightarrow & 1. \end{array}$$

y también tenemos el diagrama conmutativo



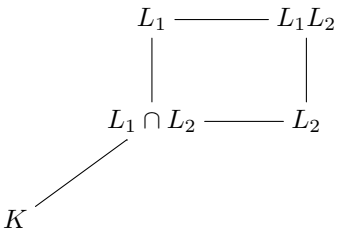
Por lo tanto $(a, L_1L_2/K) = 1$. Así, $a \in H_{L_1L_2}$.

De esta manera se obtiene que $H_{L_1} \cap H_{L_2} = H_{L_1L_2}$.

Ahora $H_{L_1} \supseteq H_{L_2} \iff H_{L_1} \cap H_{L_2} = H_{L_2} = H_{L_1L_2} \iff [L_1L_2 : K] = [L_2 : K] \iff L_1L_2 = L_2 \iff L_1 \subseteq L_2$.

De esta forma tenemos que $L \longrightarrow H_L$ es una biyección que cambia contenciones pues si $H_{L_1} = H_{L_2}$ entonces $H_{L_1L_2} = H_{L_1} \cap H_{L_2} = H_{L_1} = H_{L_2}$ por lo que $L_1L_2 = L_1 = L_2$.

Finalmente, tenemos que $H_{L_i} \subseteq H_{L_1 \cap L_2}$, $i = 1, 2$. Por tanto se sigue que $H_{L_1}H_{L_2} \subseteq H_{L_1 \cap L_2}$.



Ahora $H_{L_i} \subseteq H_{L_1}H_{L_2}$ y H_{L_i} es un subgrupo abierto de K^* de índice finito ya que $K^*/H_{L_i} \cong \mathrm{Gal}(L_i/K)$. Por tanto se sigue que $H_{L_1}H_{L_2}$ es un subgrupo abierto de K^* ya que $H_{L_1}H_{L_2} = \bigcup_{a \in H_{L_2}} aH_{L_1}$ es una unión de conjuntos abiertos (ver también la Observación 5.6.1).

Ahora consideremos la imagen de $H_{L_1}H_{L_2}$ bajo el símbolo residual de la norma del subgrupo correspondiente a las extensiones L_i/K, $i = 1, 2$, las cuales son $(H_{L_1}H_{L_2}, L_i/K)$, $i = 1, 2$, $(\_, L_i/K)\colon K^* \to \mathrm{Gal}(L_i/K)$, la cual corresponde a algún subcampo $K \subseteq T \subseteq L_i$. Notemos que T corresponde al mismo campo tanto de L_1 como de L_2 pues en ambos casos $(\_, L_i/K)$ es la restricción de ρ_K, en otras palabras, T corresponde a $H_{L_1}H_{L_2}$ o, más precisamente, $\rho_K^{-1}\big(\mathrm{Gal}(K^{\mathrm{ab}}/T)\big) = H_{L_1}H_{L_2}$.

Lo anterior implica que $H_{L_1}H_{L_2} = \text{núc}(\_, T/K) = H_T$. Por otro lado $T \subseteq L_1 \cap L_2$, $H_{L_1 \cap L_2} \subseteq H_T = H_{L_1}H_{L_2}$. Se sigue que $H_{L_1 \cap L_2} = H_{L_1}H_{L_2}$. □

Teorema 5.7.15 (limitación de normas local). *Sea L/K una extensión finita y separable de campos locales. Sea $M = L^{\mathrm{ab}}$ la máxima extensión abeliana de K contenida en L. Entonces $\mathrm{N}_{L/K} L^* = \mathrm{N}_{M/K} M^*$.*

Demostración. Se tiene que $\mathrm{N}_{L/K} L^* = \mathrm{N}_{M/K} \mathrm{N}_{L/M} L^* \subseteq \mathrm{N}_{M/K} M^*$.

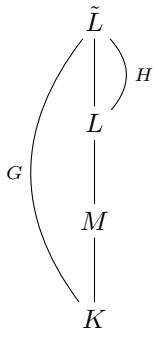
En caso de que L/K sea una extensión de Galois, se tiene que $\mathrm{Gal}(M/K) = \mathrm{Gal}(L/K)^{\mathrm{ab}} = G/[G, G] = G/G'$, donde $G = \mathrm{Gal}(L/K)$. Entonces, por el Teorema de Tate (Teorema 4.9.20), se tiene

$$H^{-2}(G, \mathbb{Z}) \cong G/G' \xrightarrow[\theta]{\cong} (L^*)^G/\mathrm{N}_{L/K} L^* = K^*/\mathrm{N}_{L/K} L^* \cong H^0(G, L^*)$$

y $[K^* : \mathrm{N}_{L/K} L^*] = |G/G'| = [M : K] = [K^* : \mathrm{N}_{M/K} M^*]$ lo que implica que $\mathrm{N}_{L/K} L^* = \mathrm{N}_{M/K} M^*$ y se tiene que $\mu_{L/K}\colon K^* \longrightarrow G/G'$ es el mapeo

inducido por el inverso de θ. De hecho $\mu_{L/K}$ es el mapeo de Artin en el caso abeliano, es decir $\mu_{L/K} = \psi_{L^{\mathrm{ab}}/K}$.

Para el caso general, sea $\tilde{L}$ una extensión finita de Galois de K que contiene a L. Sean $G = \mathrm{Gal}(\tilde{L}/K)$ y $H = \mathrm{Gal}(\tilde{L}/L)$.



Si R es la máxima subextensión abeliana de K contenida en $\tilde{L}$, se tiene $R = \tilde{L}^{G'}$ y $M = R \cap L = \tilde{L}^{G'} \cap \tilde{L}^{H} = \tilde{L}^{G'H}$. Si $a \in \mathrm{N}_{M/K}\, M^*$ se tiene el diagrama conmutativo (Teorema 5.7.12)

$$\begin{array}{ccc} L^* & \xrightarrow{\psi_{\tilde{L}/L}} & H/H' \\ {\scriptstyle \mathrm{N}_{L/K}}\downarrow & & \downarrow{\scriptstyle i} \\ K^* & \xrightarrow{\psi_{\tilde{L}/K}} & G/G' \\ \| & & \downarrow{\scriptstyle \pi} \\ K^* & \xrightarrow{\psi_{M/K}} & G/G'H \end{array}$$

donde i es la inclusión natural, π la proyección y $\psi_{\tilde{L}/L}, \psi_{\tilde{L}/K}, \psi_{M/K}$ los mapeos de Artin, los cuales tienen sentido pues $\tilde{L}/L$ y $\tilde{L}/K$ son extensiones de Galois.

Ahora, puesto que $a \in \mathrm{N}_{M/K}\, M^*$, se tiene $\psi_{M/K}(a) = 1 = \pi \circ \psi_{\tilde{L}/K}(a)$. Por otro lado $\psi_{\tilde{L}/L}$ es suprayectivo y $\psi_{\tilde{L}/K}(a) \in \mathrm{núc}\, \pi = \mathrm{im}\, i$ por lo que existe $b \in L^*$ tal que $\psi_{\tilde{L}/K} \circ (\mathrm{N}_{L/K}\, b) = \psi_{\tilde{L}/K}(a)$. Se sigue que $a/\mathrm{N}_{L/K}\, b \in \mathrm{núc}\, \psi_{\tilde{L}/K} = \mathrm{N}_{\tilde{L}/K}\, \tilde{L}^*$, esto es, existe $c \in \tilde{L}^*$ con $a/\mathrm{N}_{L/K}\, b = \mathrm{N}_{\tilde{L}/K}\, c$ de donde

$$a = \mathrm{N}_{L/K}\, b \cdot \mathrm{N}_{\tilde{L}/K}\, c = \mathrm{N}_{L/K}\, b \cdot \mathrm{N}_{L/K}(\mathrm{N}_{\tilde{L}/L}\, c) = \mathrm{N}_{L/K}(b\, \mathrm{N}_{\tilde{L}/L}\, c) \in \mathrm{N}_{L/K}\, L^*$$

probando que $\mathrm{N}_{M/K}\, M^* = \mathrm{N}_{L/K}\, L^*$. □

5.8. Grupos de ramificación superior y grupos de normas

Sea L/K una extensión de Galois finita de campos locales con grupo de Galois $G = \mathrm{Gal}(L/K)$. Se tiene que $\mathcal{O}_L = \mathcal{O}_K[x]$ para algún $x \in \mathcal{O}_L$ (ver

[151, Ch. III, Section 6, Proposition 12]). Entonces se definen los *grupos de ramificación* por (ver [136, Definición 1.3.4]):

$$G_i := \{\sigma \in G = \mathrm{Gal}(L/K) \mid v_L(\sigma x - x) \geq i+1\}, \quad i \geq -1.$$

Se tiene que $G_{-1} = G$ el cual, en el caso global, corresponde al grupo de descomposición, G_0 es el grupo de inercia y $G = G_{-1} \supseteq G_0 \supseteq G_1 \supseteq \ldots \supseteq G_r \supseteq \ldots$, $G_i \lhd G$ para toda $i \geq -1$ y $G_r = \{1\}$ para r suficientemente grande pues para $\sigma \neq 1$, $\sigma x \neq x$ y $v_K(\sigma x - x) < \infty$.

Se define

$$\imath_G \colon G \longrightarrow \mathbb{Z} \cup \{\infty\},$$

de la siguiente forma: para $\sigma \neq 1$, $\imath_G(\sigma) = v_K(\sigma x - x) \neq \infty$ y $\imath_G(1) = \infty$. Se tiene

$$\imath_G(\sigma) \geq i+1 \iff \sigma \in G_i,$$

lo cual prueba que la definición de G_i no depende de x. Además, puesto que para $\tau \in G$ se tiene $\mathcal{O}_L = \mathcal{O}_K[\tau^{-1}x]$, entonces

$$\begin{aligned}\imath_G(\tau\sigma\tau^{-1}) &= v_K(\tau\sigma\tau^{-1}x - x) = v_K(\tau(\sigma\tau^{-1}x - \tau^{-1}x)) \\ &= v_K(\sigma(\tau^{-1}x) - (\tau^{-1}x)) = \imath_G(\sigma).\end{aligned}$$

Para $\sigma, \tau \in G$ se tiene $(\sigma\tau)(x) - x = \sigma(\tau x) - \tau x + \tau x - x$, de donde

$$\begin{aligned}\imath_G(\sigma\tau) &= v_K((\sigma\tau)x - x) \geq \mathrm{mín}\{v_K(\sigma(\tau x) - (\tau x)), v_K(\tau x - x)\} \\ &= \mathrm{mín}\{\imath_G(\sigma), \imath_g(\tau)\}.\end{aligned}$$

Para un subgrupo $H < G$, sea $E = L^H$. Entonces $\mathrm{Gal}(L/E) = H$.

Proposición 5.8.1. *Para $\sigma \in H$ se tiene $\imath_H(\sigma) = \imath_G(\sigma)$ y $H_i = G_i \cap H$ para toda $i \geq -1$.*

Demostración. Es inmediato pues $v_K(\sigma x - x)$ no depende de H. □

Corolario 5.8.2. *Sea E la máxima subextensión de L no ramificada sobre K, $K \subseteq E \subseteq L$ y sea H el subgrupo correspondiente a E, es decir, $E = L^H$. Entonces $H = G_0$ y los grupos de ramificación de G de índice mayores o iguales a 0 son iguales a aquéllos de H.* □

Notemos que L/E es totalmente ramificada.

Proposición 5.8.3. *Sea $H \lhd G$. Para $\bar{\sigma} \in G/H$ se tiene*

$$\imath_{G/H}(\bar{\sigma}) = \frac{1}{e_{L/K}} \sum_{g \in \bar{\sigma}} \imath_G(g).$$

Demostración. Si $\bar{\sigma} = 1$, $1 \in \bar{\sigma}$ y ambos lados de la igualdad es ∞.

Sea $\bar{\sigma} \neq 1$. Sean $\mathcal{O}_L = \mathcal{O}_K[x]$ y $\mathcal{O}_E = \mathcal{O}_K[y]$. Se tiene

$$e_{L/E}\imath_{G/H}(\bar{\sigma}) = e_{L/K}v_E(\bar{\sigma}y - y) = v_L(\sigma y - y) \quad \text{y} \quad e_G(\sigma) = v_L(\sigma x - x).$$

Se tiene que si σ es un representante de $\bar{\sigma}$, entonces $\bar{\sigma} = \{\sigma\tau \mid \tau \in H\}$. Sean $a := \sigma y - y$ y $b := \prod_{\tau\in H}(\sigma\tau(x) - x)$.

Veamos que $\mathcal{O}_L a = \mathcal{O}_L b$. Una vez probado esto se tendrá $v_L(a) = v_L(b)$ y

$$\begin{aligned} e_{L/E}\imath_{G/H}(\bar{\sigma}) = v_L(a) = v_L(b) &= \prod_{\tau\in H} v_L(\sigma(\tau(x)) - x) \\ &= \sum_{\tau\in H} \imath_G(\sigma\tau) = \sum_{g\in\bar{\sigma}} \imath_G(g). \end{aligned}$$

Sea $f(T) := \mathrm{Irr}(x, T, E) \in E[T]$. Entonces $f(T) = \prod_{\tau\in H}(T - \tau x)$. Entonces $\sigma(f)(T) = \sigma(f(T)) = \prod_{\tau\in H}(T - (\sigma\tau)(x))$.

Puesto que todos los coeficientes de $\sigma f - f$ son divisibles por $\sigma y - y$ debido a que $\mathcal{O}_E = \mathcal{O}_K[y]$ y que por tanto y divide a todos los coeficientes de f, se sigue que $a = \sigma y - y$ divide a $\sigma(f)(x) - f(x) = \sigma(f)(x) = \prod_{\tau\in H}(x - (\sigma\tau)(x)) = \pm b$.

Falta ver que b divide a a. Puesto que $\mathcal{O}_L = \mathcal{O}_K[x]$, escribimos $y = g(x)$ con $g(T) \in \mathcal{O}_K[T]$. Se tiene que el polinomio $g(T) - y \in \mathcal{O}_E[T]$ y x es raíz de $g(T) - y$ por lo que $f(T) \mid g(T) - y$.

Escribamos $g(T) - y = f(T)h(T)$ con $h(T) \in \mathcal{O}_E[T]$. Por tanto $\sigma(g)(x) - \sigma y = \sigma(f)(x)\sigma(h)(x)$.

Ahora bien, $g(T) \in \mathcal{O}_K[T]$, por lo que $\sigma(g)(T) = g(T)$ y $\sigma(g)(x) = g(x) = y$. Se tiene $b = \pm\sigma(f)(x)$. Por tanto $-a = y - \sigma y = \pm b\sigma(h)(x)$, esto es $b \mid a$ de donde se sigue el resultado. □

Corolario 5.8.4. *Si $H = G_j$ para algún $j \geq 0$, entonces*

$$(G/H)_i = G_i/H \quad \textit{para} \quad i \leq j \quad \textit{y} \quad (G/H)_i = \{1\} \quad \textit{para} \quad i \geq j.$$

Demostración. $\{G_i/H\}_{i\leq j}$ es una filtración decreciente de subgrupos de G/H. Para $\bar{\sigma} \in G/H$, $\bar{\sigma} \neq 1$, existe un índice $i < j$ tal que $\bar{\sigma} \in G_i/H$ y $\sigma \notin G_{i+1}/H$. Si $\sigma \in G$ representa a la clase $\bar{\sigma}$, se tiene que $\sigma \in G_i$ y $\sigma \notin G_{i+1}$ de donde se sigue que $\imath_G(\sigma) = i + 1$.

Ahora bien, $H = G_j \subseteq G_0$, lo cual implica que L/E es totalmente ramificada, donde $E = L^H$ y $e_{L/E} = [L : E] = |H|$. Entonces

$$\imath_{G/H}(\bar{\sigma}) = \frac{1}{e_{L/E}} \sum_{g\in\bar{\sigma}} \imath_G(g) \underset{\bar{g}=\bar{\sigma}}{=} \frac{1}{e_{L/E}} \sum_{g\in\bar{\sigma}} \imath_G(\sigma) = \imath_G(\sigma) = i + 1.$$

Esto prueba que las filtraciones $\{G_i/H\}_{i\leq j}$ y $\{(G/H)_i\}_{i\leq j}$ coinciden. Finalmente, tenemos que $(G/H)_j = G_j/H = H/H = \{1\}$ de donde se sigue que $(G/H)_i = \{1\}$ para $i \geq j$. □

Proposición 5.8.5. *Sea $\pi \in \mathcal{O}_L$, $v_L(\pi) = 1$ cualquier elemento primo de L. Sea $\sigma \in G$ y consideremos el mapeo $\sigma \longmapsto \sigma\pi/\pi$. Es mapeo induce, pasando al cociente, un monomorfismo de grupos*

$$G_i/G_{i+1} \overset{\theta_i}{\longhookrightarrow} U_L^{(i)}/U_L^{(i+1)} \cong \mathfrak{p}_L^i/\mathfrak{p}_L^{i+1}.$$

Se tiene que θ_i es independiente de π.

Demostración. Sea π' otro elemento primo de L. Entonces $\pi' = a\pi$ para algún $a \in U_L$. Sea $\sigma \in G$. Entonces

$$\frac{\sigma\pi'}{\pi} = \frac{\sigma\pi}{\pi} \cdot \frac{\sigma u}{u}.$$

Para $\sigma \in G_i$ tenemos $\sigma u - u \in \mathfrak{p}_L^{i+1}$, esto es, $\sigma u/u \equiv 1 \bmod U_L^{(i+1)}$ por lo que θ_i es independiente de π.

Sean $\sigma, \tau \in G_i$, entonces

$$\frac{(\sigma\tau)(\pi)}{\pi} = \frac{\sigma(\tau(\pi))}{\pi} = \frac{\sigma\pi}{\pi} \cdot \frac{\tau\pi}{\pi} \cdot \sigma\Big(\frac{\tau\pi}{\pi}\Big) \cdot \frac{\pi}{\tau\pi} = \frac{\sigma\pi}{\pi} \cdot \frac{\tau\pi}{\pi} \cdot \frac{\sigma v}{v}$$

donde $v = \tau\pi/\pi \in U_L$. Se sigue de lo anterior que $\sigma v/v \equiv 1 \bmod U_L^{(i+1)}$ y por tanto

$$\frac{(\sigma\tau)(\pi)}{\pi} = \frac{\sigma\pi}{\pi} \cdot \frac{\tau\pi}{\pi} \bmod U_L^{(i+1)}$$

lo cual implica que θ_i es un homomorfismo de grupos. Finalmente, si $\sigma \in \operatorname{núc}\theta_i$, $\sigma \mapsto \sigma\pi/\pi \in U_L^{(i+1)}$ por lo que $\sigma \in G_{i+1}$ de donde se sigue que $\bar{\sigma} = 1$. □

Corolario 5.8.6. *Se tiene que G_0/G_1 es un grupo cíclico de orden un divisor de $q-1$ y G_i/G_{i+1} es un p–grupo elemental abeliano para $i \geq -1$. En particular G_1 es un p–grupo. Aquí $q = p^r$ y el campo residual de L es $\mathbb{F}_q$.*

Demostración. Se sigue del hecho de que $G_0/G_1 \subseteq U_L/U_L^{(1)} \cong \mathbb{F}_q^*$ y $G_i/G_{i+1} \subseteq U_L^{(i)}/U_L^{(i+1)} \cong \mathbb{F}_q$ para $i \geq 1$. □

Corolario 5.8.7. *Sea L/K una extensión finita de Galois con grupo de Galois G. Entonces G es un grupo soluble.*

Demostración. Sea G_0 el grupo de inercia de G, $G_0 \triangleleft G$ y G/G_0 es un grupo cíclico pues corresponde a la máxima extensión no ramificada de K contenida en L (Teorema 3.4.5). Del Corolario 5.8.6 se sigue que el grupo G_0 es soluble, de donde se sigue que G es soluble. □

Definición 5.8.8. Si $t \in [-1, \infty)$ definimos $G_t := G_{\lceil t \rceil}$ donde $\lceil t \rceil$ es la función techo, esto es, $\lceil t \rceil$ es el entero más pequeño mayor o igual a t.

Se tiene para $t = -1$, $[G_0 : G_{-1}] := [G_{-1} : G_0]^{-1} = [G : G_0]^{-1}$ y para $-1 < t \leq 0$, $[G_0 : G_t] = 1$.

Sea $g_i = |G_i|$, $i \in \mathbb{Z}$, $i \geq -1$.

Definición 5.8.9. La *función de Herbrand*

$$\varphi = \varphi_{L/K} \colon [-1, \infty) \longrightarrow [-1, \infty)$$

se define por

$$\varphi(u) = \int_0^u \frac{dt}{[G_0 : G_t]} = \frac{1}{g_0}(g_1 + \cdots + g_m + (u - m)g_{m+1})$$

donde $m \leq u \leq m + 1$, $m \in \mathbb{N}$.

En particular se tiene $\varphi(m) + 1 = \frac{1}{g_0} \sum_{i=0}^{m} g_i$.

Notemos que para $u \geq -1$, $u \notin \mathbb{Z}$,

$$\varphi'_{L/K}(u) = \frac{g_{m+1}}{g_0} \quad \text{donde} \quad m < u < m + 1. \tag{5.8.3}$$

Se tiene que φ es continua, lineal, lineal por tramos, creciente y cóncava y por tanto φ es una función biyectiva y continua.

Definición 5.8.10. Sea $\eta = \eta_{L/K} \colon [-1, \infty) \longrightarrow [-1, \infty)$ la inversa de φ: $\eta = \varphi^{-1}$. Se define el *número de ramificación superior* v por

$$G^v := G_{\eta(v)} \quad \text{o, equivalentemente,} \quad G^{\varphi(u)} = G_u$$

y $\varphi(u)$ es el número de ramificación superior.

Se tiene que η es continua, lineal por tramos, creciente y convexa. Además, $\eta(0) = 0$. Si $v = \varphi(u)$ es un entero, entonces $u = \eta(v)$ es también un entero. En efecto, si $m \in \mathbb{Z}$ es tal que $m \leq u \leq m + 1$, entonces

$$g_0 v = g_1 + \cdots + g_m + (u - m)g_{m+1}.$$

Puesto que $G_{m+1} \subseteq G_i$, $0 \leq i \leq m$, $g_{m+1} | g_i$, $0 \leq i \leq m$. Por tanto, puesto que $v \in \mathbb{Z}$, $u - m \in \mathbb{Z}$ y $u \in \mathbb{Z}$. Además

$$\eta(v) = \int_0^v [G^0 : G^w] dw.$$

Una de las razones principales para estudiar los número de ramificación superiores, es que tenemos el siguiente resultado.

Teorema 5.8.11. *Si $H \lhd G$, entonces, para toda $v \in [-1, \infty)$ se tiene*

$$(G/H)^v = G^v H/H.$$

Para probar el Teorema 5.8.11, primero probamos

Proposición 5.8.12. *Se tiene*

$$\varphi_{L/K}(t) = \frac{1}{g_0} \sum_{\sigma \in G} \min\{\imath_G(\sigma), t+1\} - 1.$$

Demostración. Sea $\theta(t) = \frac{1}{g_0} \sum_{\sigma \in G} \min\{\imath_G(\sigma), t+1\} - 1$. Entonces θ es una función continua, lineal por tramos, $\theta(0) = \varphi(0) = 0$. Si $m \geq -1$ es un entero y $m < t < m+1$, entonces se tiene que $t+1 \notin \mathbb{Z}$ y

$$\inf\{\imath_G(\sigma), t+1\} = \imath_G(\sigma) \iff \imath_G(\sigma) < t+1 \iff \imath_G(\sigma) \leq m+1.$$

Sea $\imath_G(\sigma) = i \leq m+1$ $\big($ $\iff$ $\sigma \notin G_{m+1}$ $\big)$, por lo tanto

$$\begin{aligned} \inf\{\imath_G(\sigma), t+1\} = t+1 &\iff \imath_G(\sigma) \geq t+1 \in (m+1, m+2) \\ &\iff \imath_G(\sigma) \geq m+2 \iff \sigma \in G_{m+1}. \end{aligned}$$

Por tanto

$$\begin{aligned} \theta(t) &\underset{\substack{\uparrow \\ m<t<m+1}}{=} \frac{1}{g_0} \sum_{\sigma \in G} \inf\{\imath_G(\sigma), t+1\} - 1 \\ &= \frac{1}{g_0} \sum_{\sigma \in G \setminus G_{m+1}} \inf\{\imath_G(\sigma), t+1\} + \frac{1}{g_0} \sum_{\sigma \in G_{m+1}} \inf\{\imath_G(\sigma), t+1\} - 1 \\ &= \frac{1}{g_0} \sum_{\sigma \in G \setminus G_{t+1}} \imath_G(\sigma) + \frac{|G_{m+1}|}{g_0}(t+1) - 1. \end{aligned}$$

Se sigue que $\theta'(t) = \frac{g_{m+1}}{g_0}$.

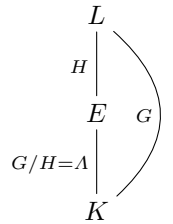
Ahora $\varphi(u) = \int_0^u \frac{dt}{[G:G_t]}$, lo cual implica que

$$\varphi'(t) = \frac{1}{[G:G_t]} = \frac{1}{[G:G_{\lceil t \rceil}]} = \frac{1}{[G:G_{m+1}]} = \frac{g_{m+1}}{g_0} = \theta'(t).$$

De esta forma tenemos que $(\varphi - \theta)'(t) = 0$ para toda $t \in [-1, \infty) \setminus \mathbb{Z}$, $\varphi(0) = \theta(0)$ y $(\varphi - \theta)$ es una función continua. Se sigue que $\varphi(t) = \theta(t)$ para toda $t \in [-1, \infty)$. □

Teorema 5.8.13 (Herbrand). *Sea L/K una extensión finita de Galois de campos locales con grupo $G = \mathrm{Gal}(L/K)$. Sea E/K una subextensión de Galois de L/K con grupo $\Lambda = G/H = \mathrm{Gal}(E/K)$ donde $H = \mathrm{Gal}(L/E)$. Entonces*

$$\frac{G_s H}{H} = \Lambda_t = \left(\frac{G}{H}\right)_t \quad \textit{con} \quad t = \varphi_{L/E}(s).$$



Demostración. Sea $\bar{\sigma} \in \Lambda$ y seleccionaremos una preimagen $\sigma \in G$ que toma el máximo valor $\imath_G(\sigma)$. Esto es, se selecciona $\sigma \in G$ tal que $\imath_G(\sigma) = \sup\{\imath_G(g) \mid g \in \bar{\sigma}\}$. Probaremos que

$$\imath_\Lambda(\bar{\sigma}) = \varphi_{L/E}(\imath_G(\sigma) - 1). \tag{5.8.4}$$

Sea $m = \imath_G(\sigma)$, por lo tanto $\sigma \in H_{m-1}$. Si $\tau \in H$ está en H_{m-1}, entonces $\imath_G(\tau) \geq m$ pues $H_{i-1} = G_{i-1} \cap H$ para toda i (Proposición 5.8.1).

Por tanto $m = \imath_G(\sigma) \geq \imath_G(\tau\sigma) \geq \min\{\imath_G(\tau), \imath_G(\sigma)\} = m$. Se sigue que $\imath_G(\tau\sigma) = m$. Ahora si $\tau \in H$ y $\tau \notin H_{m-1}$, se tiene $\imath_G(\tau) < m$ y $\imath_G(\tau\sigma) = \imath_G(\tau)$. En ambos casos se tiene $\imath_G(\tau\sigma) = \min\{\imath_G(\tau), m\}$.

Aplicando la Proposición 5.8.3 obtenemos

$$\imath_\Lambda(\bar{\sigma}) = \frac{1}{e_{L/E}} \sum_{g \in \bar{\sigma}} \imath_G(g) = \frac{1}{e_{L/E}} \sum_{\tau \in H} \imath_G(\sigma\tau) = \frac{1}{e_{L/E}} \sum_{\tau \in H} \min\{\imath_G(\tau), m\}. \tag{5.8.5}$$

Por otro lado, por la Proposición 5.8.1, se tiene $\imath_G(\tau) = \imath_H(\tau)$ y además $e_{L/E} = |H_0|$. De la Proposición 5.8.12 y de la Ecuación (5.8.5) obtenemos

$$\begin{aligned} \imath_\Lambda(\bar{\sigma}) &= \frac{1}{h_0} \sum_{\tau \in H} \min\{\imath_G(\tau), m\} = \frac{1}{h_0} \sum_{\tau \in H} \min\{\imath_H(\tau), m\} \\ &= \varphi_{L/E}(m-1) + 1 = \varphi_{L/E}(\imath_G(\sigma) - 1) + 1 \end{aligned}$$

la cual es la Ecuación (5.8.4).

Se tiene que si $\bar{\sigma} \in G_s H/H$, entonces existe $\sigma' \in G_s$ tal que $\overline{\sigma'} = \bar{\sigma}$. De la Ecuación (5.8.4) obtenemos

$$\begin{aligned} \bar{\sigma} \in G_s H/H &\iff \imath_G(\sigma) \geq s+1 \iff \imath_G(\sigma) - 1 \geq s \\ \iff \varphi_{L/E}(\imath_G(\sigma) - 1) \geq \varphi_{L/E}(s) &\iff \imath_\Lambda(\sigma') - 1 \geq \varphi_{L/E}(s) \\ &\iff \sigma' \in \Lambda_{\varphi_{L/E}(s)} = \Lambda_t. \end{aligned}$$

□

Proposición 5.8.14. *Sea E/K una subextensión de Galois de L/K. Entonces si $\varphi_{L/K}$ denota la función de Herbrand y $\eta_{L/K} = \varphi_{L/K}^{-1}$, entonces*

$$\varphi_{L/K} = \varphi_{E/K} \circ \varphi_{L/E} \quad y \quad \eta_{L/K} = \eta_{L/E} \circ \eta_{E/K}.$$

Demostración. Tenemos $e_{L/K} = e_{E/K} e_{L/E}$. Del Teorema de Herbrand 5.8.13 se tiene $G_s H/H = G_s/G_s \cap H = G_s/H_s = (G/H)_t$ con $t = \varphi_{L/E}(s)$. Por tanto, puesto que $e_{L/E} = |G_0|$, $e_{E/K} = |(G/H)_0|$ y $e_{L/E} = |H_0|$,

$$\frac{1}{e_{L/K}} |G_s| = \frac{1}{e_{E/K}} \left| \left(\frac{G}{H} \right)_t \right| \cdot \frac{1}{e_{L/E}} |H_s|.$$

Entonces, de la Ecuación (5.8.3) se obtiene

$$\varphi'_{L/K}(s) = \varphi'_{E/K}(t)\cdot\varphi'_{L/E}(s) \underset{\substack{\uparrow\\ t=\varphi_{L/E}(s)}}{=} \varphi'_{E/K}(\varphi_{L/E}(s))\varphi'_{L/E}(s)$$
$$= (\varphi_{E/K}\circ\varphi_{L/E})'(s).$$

Puesto que $\varphi_{L/K}(0) = (\varphi_{E/K}\circ\varphi_{L/E})(0) = 0$, se sigue que

$$\varphi_{L/K} = \varphi_{E/K}\circ\varphi_{L/E}.$$

Tomando las funciones inversas, se sigue que

$$\eta_{L/K} = \varphi^{-1}_{L/K} = (\varphi_{E/K}\circ\varphi_{L/E})^{-1} = \varphi^{-1}_{L/E}\circ\varphi^{-1}_{E/K} = \eta_{L/E}\circ\eta_{E/K}. \qquad \square$$

Con estos resultados, estamos en condiciones de probar el Teorema 5.8.11: si $H \lhd G$, entonces $(G/H)^v = G^vH/H$ para todo $v \geq -1$.

Demostración. (Teorema 5.8.11): Sea $s = \eta_{E/K}(t)$. Usando el Teorema de Herbrand 5.8.13 y la Proposición 5.8.14, obtenemos

$$\frac{G^tH}{H} = \frac{G_{\eta_{L/K}(t)}H}{H} \underset{\substack{\uparrow\\ \text{Herbrand}}}{=} \left(\frac{G}{H}\right)_{\varphi_{L/E}(\eta_{L/K}(t))}$$
$$= \left(\frac{G}{H}\right)_{(\varphi_{L/E}\circ\eta_{L/E}\circ\eta_{E/K})(t)} = \left(\frac{G}{H}\right)_{\eta_{E/K}(t)} = \left(\frac{G}{H}\right)^t. \qquad \square$$

Definición 5.8.15. t se llama *salto superior* si $G^t(L/K) \neq G^{t+\epsilon}(L/K)$ para toda $\epsilon > 0$.

5.8.1. Grupos Formales de Lubin-Tate. Cálculo del símbolo residual de la norma

Nuestra exposición sobre los grupos de Lubin–Tate sigue muy de cerca a [117] el cual es a su vez, una exposición detallada de [102].

En 1965, J. Lubin y J. Tate [102] motivados por la analogía con la teoría de multiplicación compleja en curvas elípticas, mostraron como pueden ser usados los grupos formales sobre campos locales para probar resultados centrales en campos de clase locales. En esta sección introducimos los grupos formales y por medio de ellos daremos las demostraciones de los resultados centrales de la teoría de campos locales. Como ya mencionamos, esta sección está basada en [117, 102] y también en [77].

Los grupos formales son los análogos a las extensiones ciclotómicas del campo $\mathbb{Q}_p$ de los números p–ádicos sobre cualquier campo local. En lugar de las raíces como el núcleo del mapeo $K^* \xrightarrow{n} K^*$, se presenta otra acción y el núcleo son los llamados *puntos de división* los cuales son también las raíces de cierta n–potencia de un mapeo.

Aquí queremos mencionar la gran similitud de los grupos formales con los *módulos de Drinfeld*, y más específicamente con el *módulo de Carlitz* lo cual será evidente a lo largo de esta sección.

Sea K un campo local con valuación v y sea $\mathcal{O}_K$ el anillo de valuación de K, es decir $\mathcal{O}_K = \{x \in K \mid |x|_v \leq 1\} = \{x \in K \mid v(x) \geq 0\} = \bar{B}(1,0)$.

En general, si A es un anillo conmutativo con unidad, el anillo conmutativo de *series formales* en las variables $X_1, \ldots, X_n$ es

$$R = A[[X_1, \ldots, X_n]] = \{f(X_1, \ldots, X_n) = \sum_i a_{i_1,\ldots,i_n} X_1^{i_1} \cdots X_n^{i_n},$$

$a_{i_1,\ldots,i_n} \in A$ y $i = (i_1, \ldots, i_n)$ varía en todos las n–tuplas de enteros $n \geq 0\}$.

Sean $f, g \in R$, $d \in \mathbb{Z}$, $d \geq 0$. Se pone $f \equiv g$ mód gr d si $f - g$ no tiene términos de grado total menores a d.

Si $f \in R$ y $g_1, \ldots, g_n \in A[[Y_1, \ldots, Y_m]]$, se define

$$f \circ (g_1, \ldots, g_n) = f(g_1(Y_1, \ldots, Y_m), \ldots, g_n(Y_1, \ldots, Y_m)) \in A[[Y_1, \ldots, Y_m]].$$

Si A es un anillo topológico, se considera R como anillo topológico de tal forma que el mapeo

$$f = \sum_i a_{i_1,\ldots,i_n} X_1^{i_1} \cdots X_n^{i_n} \longmapsto \{a_{i_1,\ldots,i_n}\}_{\{i_1,\cdots,i_n \geq 0\}} \in \prod_i A$$

define un homomorfismo continuo de R sobre el producto de una cantidad numerable de A indexadas por $i = (i_1, \ldots, i_n)$.

Sea ahora K un campo local y tomemos $\mathcal{O}_K$. Sea π un elemento primo. Sea τ es automorfismo de Frobenius, es decir, el mapeo inducido por $\tau(x) = x^q$ donde $\mathbb{F}_q \cong \mathcal{O}_K/\mathfrak{p}\mathcal{O}_K = \mathcal{O}_K/\pi\mathcal{O}_K$.

Para $f, g \in \mathcal{O}_K[[T]]$ decimos que $f \equiv g$ mód π si $f - g = \sum_{n=0}^{\infty} c_n T^n$ satisface que $\pi | c_n$ para toda $n \in \mathbb{N} \cup \{0\}$, esto es $v(c_n) \geq 1$ para toda n.

Definición 5.8.16. Se define

$$\mathcal{F}_\pi = \{f \in \mathcal{O}_K[[T]] \mid f(T) \equiv \pi T \text{ mód gr } 2 \text{ y } f(T) \equiv T^q \text{ mód } \pi\}.$$

En general, un elemento de $f \in \mathcal{F}_\pi$ es de la forma

$$f(T) = \pi T + \pi a_2 T^2 + \cdots + \pi a_{q-1} T^{q-1} + T^q + \pi T^{q+1} g(T) \text{ con } g(T) \in \mathcal{O}_K[[T]].$$

El elemento más simple de $\mathcal{F}_\pi$ es $f(T) = \pi T + T^q$. Nótese la similitud con el módulo de Carlitz.

Sea $f \in \mathcal{F}_\pi$ arbitrario. Se define

$$f^n(T) = f^{(n)}(T) := (\underbrace{f \circ \cdots \circ f}_{n})(T) = f(f(\cdots(f(T)\cdots))) \in \mathcal{O}_K[[T]]$$

y se define $f^{(0)}(T) = T$.

Definición 5.8.17. Se define $\Lambda_{f,n} = \{\lambda \in \Omega \mid v(\lambda) > 0 \text{ y } f^{(n)}(\lambda) = 0\}$ donde Ω es un cerradura algebraica fija de K.

Definición 5.8.18. Se define el campo $L_{f,n} = K(\Lambda_{f,n})$ para $n = 1, 2, \ldots$ El campo $L_{f,n}$ se llama *el campo de los π^n puntos de división del módulo de Lubin–Tate F_f* el cual definiremos más adelante.

Observación 5.8.19. Se tiene que

$$f^{(n)}(T) = f(f^{(n-1)}(T)) = f^{(n-1)}(T)g_n(T)$$

para algún $g_n(T) \in \mathcal{O}_K[[T]]$. Por tanto $\Lambda_{f,n-1} \subseteq \Lambda_{f,n}$ de donde $L_{f,n-1} \subseteq L_{f,n}$, $n = 1, 2, \ldots$

Definición 5.8.20. Sea $f \in \mathcal{F}_\pi$. Se define $\Lambda_f := \bigcup_{n=1}^{\infty} \Lambda_{f,n}$ y $L_f := K(\Lambda_f) = \bigcup_{n=1}^{\infty} L_{f,n}$.

El objetivo inmediato es probar que $L_{f,n}$ son una especie de campos ciclotómicos, o más precisamente, $L_{f,n}$ es una extensión de tipo ciclotómica de K. Esto es, queremos probar que $L_{f,n}/K$ es una extensión abeliana finita y totalmente ramificada. Más aún, veremos que $\mathrm{N}_{L_{f,n}/K}(L_{f,n}^*) = (\pi) \times U_K^{(n)}$.

El Teorema 5.7.8 también se cumple en característica positivo, por lo que los grupos de normas de K^* son exactamente los grupos conteniendo a algún $(\pi^f) \times U_K^{(n)}$ para $n = 0, 1, \ldots,$ y $f = 1, 2, \ldots$. Como consecuencia, se obtiene el Teorema de Existencia.

La forma en que lo haremos es como sigue. Se usará una serie de potencias para hacer de $\Lambda_{f,n}$ un $\mathcal{O}_K$–módulo de tal forma que la multiplicación de $\Lambda_{f,n}$ por una unidad $u \in \mathcal{O}_K^* = U_K$ produce una permutación de $\Lambda_{f,n}$ la cual induce un automorfismo de $L_{f,n}$ sobre K que resultará ser $(u^{-1}, L_{f,n}/K)$, el símbolo residual de la norma o mapeo de Artin.

Un resultado central para hacer de $\Lambda_{f,n}$ un $\mathcal{O}_K$–módulo, es el siguiente teorema.

Teorema 5.8.21. *Sean $f, g \in \mathcal{F}_\pi$ y $L(X_1, \ldots, X_n) = \sum_{i=1}^n a_i X_i$ una forma lineal con coeficientes en $\mathcal{O}_K$. Entonces existe una única serie de potencias $F(X_1, \ldots, X_n) \in \mathcal{O}_K[[X_1, \ldots, X_n]]$ tal que*

$$F(X_1, \ldots, X_n) \equiv L(X_1, \ldots, X_n) \text{ mód gr } 2,$$
$$f(F(X_1, \ldots, X_n)) = F(g(X_1), \ldots, g(X_n)).$$

Demostración. Pongamos $X := (X_1, \ldots, X_n)$ y $g(X) = (g(X_1), \ldots, g(X_n))$. Sea $F_r(X) \in \mathcal{O}_K[X]$ la serie $F(X_1, \ldots, X_n)$ quitando todos los términos de grado total mayor o igual a r.

Se tiene que si $f(F(X_1, \ldots, X_n)) = F(g_1(X_1), \ldots, g(X_n))$ entonces

$$f(F_r(X)) \equiv F_r(g(X)) \text{ mód gr}(r+1) \quad \text{para toda } r$$

y recíprocamente. De esta forma, $F(X_1, \ldots, X_r)$ es solución si y sólo si

$$F(X) \equiv L(X) \text{ mód gr } 2 \quad \text{y}$$
$$f(F_r(X)) \equiv F_r(g(X)) \text{ mód gr}(r+1) \quad \text{para toda } r. \tag{5.8.6}$$

En otras palabras debemos solucionar la Ecuación (5.8.6) para toda r. Para $r = 1$, definimos $F_1(X) = L(X)$ y se cumple la Ecuación (5.8.6). Notemos que $F_1(X)$ es único.

Supongamos que hemos hallado un único polinomio $F_r(X)$ satisfaciendo la Ecuación (5.8.6). Esto es,

$$f(F_r(X)) \equiv F_r(g(X)) \text{ mód } \mathrm{gr}(r+1).$$

Notemos que si existe $F_{r+1}(X)$ satisfaciendo la Ecuación (5.8.6) mód $\mathrm{gr}(r+2)$ necesariamente se debe tener $F_{r+1}(X) = F_r(X) + \varphi_{r+1}(X)$ donde $\varphi_{r+1}(X)$ es un polinomio homogéneo de grado $r+1$. Veamos que tal $\varphi_{r+1}(X)$ existe y es único.

Si $F_{r+1}(X)$ es solución de la Ecuación (5.8.6), entonces

$$f(F_{r+1}(X)) = f(F_r(X) + \varphi_{r+1}(X)).$$

Sea

$$f(T) = \pi T + \pi a_2 T^2 + \cdots + \pi a_{q-1} T^{q-1} + T^q + \pi T^{q+1} h(T)$$

con $h(T) \in \mathcal{O}_K[[T]]$. Escribamos $f(T) = \sum_{i=1}^{\infty} a_i T^i$ con $a_1 = \pi$, entonces

$$\begin{aligned} f(F_r(X) + \varphi_{r+1}(X)) &= \sum_{i=1}^{\infty} a_i \big(F_r(X) + \varphi_{r+1}(X)\big)^i \\ &= \sum_{i=1}^{\infty} a_i \Big(F_r(X)^i + \sum_{j=1}^{i} \binom{i}{j} F_r(X)^{i-j} \varphi_{r+1}(X)^j\Big) \\ &= \sum_{i=1}^{\infty} a_i F_r(X)^i + \varphi_{r+1}(X)\Big(\sum_{i=1}^{\infty} a_i \sum_{j=1}^{i} \binom{i}{j} F_r(X)^{i-j} \varphi_{r+1}(X)^{j-1}\Big) \\ &= f(F_r(X)) + \varphi_{r+1}(X)\Big(\sum_{i=1}^{\infty} a_i i F_r(X)^{i-1} + \varphi_{r+1}(T) l(T)\Big). \end{aligned}$$

Por tanto

$$f(F_{r+1}(X)) \underset{\substack{\uparrow \\ a_1=\pi}}{\equiv} f(F_r(X)) + \pi \varphi_{r+1}(X) \text{ mód } \mathrm{gr}(r+2).$$

Además $F_{r+1}(g(X)) = F_r(g(X)) + \varphi_{r+1}(g(X))$. Puesto que $g(X) \in \mathcal{F}_\pi$, se tiene

$$\begin{aligned} \varphi_{r+1}(g(x)) = \varphi_{r+1}(g(X_1), \ldots, g(X_n)) &\underset{\substack{\uparrow \\ g(X_i)=\pi X_i + \cdots}}{=} \\ &= \pi^{r+1} \varphi_{r+1}(X) + \text{términos de grado} \geq r+2. \end{aligned}$$

Por tanto

$$F_{r+1}(g(X)) \equiv F_r(g(X)) + \pi^{r+1}\varphi_{r+1}(X) \text{ mód } \mathrm{gr}(r+2).$$

De las congruencias

$$f(F_{r+1}(X)) \equiv f(F_r(X)) + \pi\varphi_{r+1}(X) \text{ mód } \mathrm{gr}(r+2),$$
$$F_{r+1}(g(X)) \equiv F_r(g(X)) + \pi^{r+1}\varphi_{r+1}(X) \text{ mód } \mathrm{gr}(r+2),$$

se sigue que si queremos

$$f(F_{r+1}(X)) \equiv F_{r+1}(g(X)) \text{ mód } \mathrm{gr}(r+2),$$

entonces

$$f(F_r(X)) + \pi\varphi(X) \equiv F_r(g(X)) + \pi^{r+1}\varphi_{r+1}(X) \text{ mód } \mathrm{gr}(r+2),$$

lo cual equivale a

$$\varphi_{r+1}(X) \equiv \frac{f(F_r(X)) - F_r(g(X))}{\pi^{r+1} - \pi} \text{ mód } \mathrm{gr}(r+2).$$

De esta forma, $\varphi_{r+1}(X)$ es único pues es la serie $\frac{f(F_r(X))-F_r(g(X))}{\pi^{r+1}-\pi}$ quitando los términos de grado mayor o igual a $(r+2)$ y la serie $f(F_r(X)) - F_r(g(X))$ no tiene términos de grado diferente a $(r+1)$ por la Ecuación (5.8.6). Ahora bien

$$f(F_r(X)) - F_r(g(X)) \equiv F_r(X)^q - F_r(X^q) \equiv 0 \text{ mód } \pi.$$

Por tanto $\varphi_{r+1}(X) \in \mathcal{O}_K[X]$ y $\varphi_{r+1}(X)$ es homogéneo de grado $(r+1)$. Esto muestra la existencia y la unicidad de $F(X) = \lim_{r\to\infty} F_r(X)$. □

Observación 5.8.22. La demostración del Teorema 5.8.21 de hecho prueba que F es la única serie de potencias en cualquier campo que contenga a $\mathcal{O}_K$ y que satisface las condiciones del Teorema 5.8.21.

Definimos en general *grupos formales* y *módulos formales*.

Sea R es un anillo conmutativo con unidad. Sea $\mathfrak{m} = \langle X\rangle = XR[[X]]$ el ideal generado por X. Entonces $\mathfrak{m} = \{f(X) \in R[[X]] \mid f \equiv 0 \text{ mód gr } 1\}$. Se tiene para $f, g \in \mathfrak{m}$, $(f \circ g)(X) = f(g(X)) \in \mathfrak{m}$. En particular $\mathfrak{m}$ es un semigrupo con la operación $\circ$. Ahora bien, para $f \in \mathfrak{m}$ se tiene $X \circ f = f \circ X = f$, por lo que la identidad del semigrupo es la serie X.

Si para $f, g \in \mathfrak{m}$ satisfacen $f \circ g = g \circ f = X$, escribimos $f = g^{-1}$ y $g = f^{-1}$ y se dice que f es *invertible*.

Proposición 5.8.23. *Se tiene que $f \in \mathfrak{m}$ es invertible si y solamente si $a_1 \in R^*$ donde $f(X) = a_1X + \sum_{i=2}^{\infty} a_iX^i$, esto es, si existe $c \in R$ tal que $a_1c = 1$.*

Demostración. Si $g = f^{-1}$, $(f \circ g)(X) = a_1g(X) + \sum_{j=2}^{\infty} d_jX^j$ con $g(X) = cX + \sum_{j=2}^{\infty} c_jX^j$. Por tanto

$$f(g(X)) = a_1 cX + \sum_{j=2}^{\infty} e_j X^j = X,$$

de donde obtenemos que $a_1 c = 1$.

Recíprocamente, sea $a_1 \in R^*$ y $c_1 = c \in R$ con $a_1 c_1 = 1$. Buscamos $g(X) = \sum_{i=1}^{\infty} c_i X^i$ con $f(g(X)) = X$. Se tiene $f(g(X)) = \sum_{i=1}^{\infty} a_i (g(X))^i$, la cual podemos resolverla de manera recursivo satisfaciendo $f \circ g = X$.

Por la misma razón, existe h tal que $h \circ f = X$. Por tanto

$$h = h \circ X = h \circ f \circ g = X \circ g = g.$$

Obtenemos que $f \circ g = g \circ f = X$. □

Observación 5.8.24. Si $f \circ g = g \circ f = X$ y $f \circ h = h \circ f = X$, entonces $h = h \circ X = h \circ (g \circ f) = (h \circ f) \circ g = X \circ g = g$.

Definición 5.8.25. Sea R un anillo conmutativo con unidad. Una serie formal $F(X, Y) \in R[[X, Y]]$ se llama un *grupo formal* sobre R si

(a) $F(X, Y) \equiv X + Y$ mód gr 2.
(b) $F(F(X, Y), Z) = F(X, F(Y, Z))$ (asociatividad).
(c) $F(X, Y) = F(Y, X)$ (conmutatividad).

En particular se tiene $F(0, 0) = 0$ lo cual implica que las dos series en (b) están bien definidas (pues de otra forma podríamos tener una serie de constantes en R no convergente).

Ejemplos 5.8.26. (1) $F(X, Y) = X + Y$ es un grupo formal llamado el *grupo formal aditivo* y es denotado por $\mathbb{G}_a$.
(2) $F(X, Y) = X + Y + XY = (1 + X)(1 + Y) - 1$ es un grupo formal llamado *grupo formal multiplicativo* y es denotado por $\mathbb{G}_m$.

De la definición de grupo formal, obtenemos $F(X, 0) \equiv X$ mód gr 2, $F(F(X, 0), 0) = F(X, 0)$. De la condición $F(X, 0) \equiv X$ mód gr 2 obtenemos que $f(X) := F(X, 0)$ es invertible, $f^{-1} \in \mathfrak{m} = XR[[X]]$.

Se tiene

$$f(X) = F(X, 0) = F(F(X, 0), 0) = F(f(X), 0) = (f \circ f)(X).$$

Se sigue que $X = (f^{-1} \circ f)(X) = (f^{-1} \circ f \circ f)(X) = f(X)$, esto es, $f(X) = X$. Así, $F(X, 0) = X$. Similarmente se obtiene que $F(0, Y) = Y$. Por tanto

$$F(X, Y) = X + Y + \sum_{i,j=1}^{\infty} c_{i,j} X^i Y^j,$$

es decir, no existen términos de la forma X^i o Y^j con $i, j \geq 2$.

La ecuación $F(X,Y) = 0$ puede resolverse para Y en $\mathfrak{m}$, esto es, existe una única serie $i_F(X) = -X + \sum_{i=2}^{\infty} b_i X^i$ con $b_i \in R$ tal que $F(X, i_F(X)) = F(i_F(X), X) = 0$ (esto lo podemos hacer por recursión).

Notemos que $i_F(X) \equiv -X$ mód gr 2. La serie $i_F(X)$ recibe el nombre de *inversa formal*.

Ejemplos 5.8.27. (1) La inversa formal de $\mathbb{G}_a$ es $i_F(X) = -X$.

(2) La inversa formal de $\mathbb{G}_m$ es $i_F(X) = (1+X)^{-1} - 1 = -X + X^2 - \cdots = \sum_{i=1}^{\infty} (-1)^i X^i$.

Definición 5.8.28. Sea $F(X,Y) \in R[[X,Y]]$ un grupo formal. Para $f, g \in \mathfrak{m}$, definimos

$$f \oplus_F g := F(f(X), g(X)).$$

Entonces $f \oplus_F g \in \mathfrak{m}$ y $\mathfrak{m}$ es un grupo abeliano con respecto a esta operación y el inverso de f es $i_F(f)$. Este grupo abeliano se denota por $\mathfrak{m}_F$.

Ejemplos 5.8.29. (1) $\mathfrak{m}_{\mathbb{G}_a} = \mathfrak{m}$ con la suma.

(2) $\mathfrak{m}_{\mathbb{G}_m} \cong 1 + \mathfrak{m}$ con la multiplicación.

Sea $G(X,Y)$ otro grupo formal sobre R y sea $f \in \mathfrak{m}$ tal que

$$f(F(X,Y)) = G(f(X), f(Y)) \tag{5.8.7}$$

Definición 5.8.30. Si f satisface la Ecuación (5.8.7), f se llama *morfismo* de F en G y se escribe

$$f \colon F \longrightarrow G.$$

Si $F = G$, f se llama *endomorfismo*.

Si f tiene inversa $f^{-1} \in \mathfrak{m}$, $f^{-1} \colon G \longrightarrow F$ es un morfismo de G en F y f se llama *isomorfismo*, $f \colon F \xrightarrow{\cong} G$.

La Ecuación (5.8.7) se escribe

$$f \circ F = G \circ f. \tag{5.8.8}$$

Nótese la similitud con morfismos de módulos de Drinfeld.

Ejemplo 5.8.31. Sea F es un grupo formal. Se define el endomorfismo de F, $[m] \colon F \longrightarrow F$ definido por $[0](X) = 0$, $[m+1](X) = F([m]X, X)$ si $m \geq 0$ y $[m-1](X) = F([m](X), i_F(X))$ si $m \leq 0$.

Este endomorfismo se llama *multiplicación por* m. Si $m \in U_K$, entonces $[m]$ es un isomorfismo.

Definición 5.8.32. Si $F(X_1, \ldots, X_m) \in R[[X_1, \ldots, X_m]]$ y si $f \in \mathfrak{m} = XR[[X]]$ es invertible en $\mathfrak{m}$: $f^{-1} \in \mathfrak{m}$, se define la serie $F^f(X_1, \ldots, X_m) \in R[[X_1, \ldots, X_m]]$ por

$$F^f(X_1, \ldots, X_m) = f \circ F \circ f^{-1} = f(F(f^{-1}(X_1), \ldots, f^{-1}(X_m))). \tag{5.8.9}$$

Si $F(X,Y)$ es un grupo formal sobre R, entonces $G = F^f$ es nuevamente un grupo formal y $f\colon F \xrightarrow{\cong} G$ es un isomorfismo.

Sea

$$\mathrm{Hom}_R(F,G) = \mathrm{Hom}(F,G) = \{f \mid f\colon F \longrightarrow G \text{ es un morfismo}\},$$
$$\mathrm{End}_R(F) = \mathrm{End}(F) = \mathrm{Hom}_R(F,F).$$

Proposición 5.8.33. *Se tiene* $\mathrm{Hom}(F,G)$ *es un subgrupo de* $\mathfrak{m}_G$. *Además* $\mathrm{End}(F)$ *es un anillo con respecto a la suma* $f \oplus_F g$ *y multiplicación* $f \circ g$ *cuya identidad es* X.

Demostración. [77, Lemma 4.1, página 51]. □

Para definir módulos formales, aplicamos el Teorema 5.8.21 a los casos suma y multiplicación por escalar: $L(X,Y) = X + Y$ y $L(X) = aX$ con $a \in \mathcal{O}_K$.

Sea $f \in \mathcal{F}_\pi$ y sea $F_f(X,Y)$ la <u>única</u> solución de

$$\begin{aligned} F_f(X,Y) &\equiv X + Y \text{ mód gr } 2, \\ f(F_f(X,Y)) &= F_f(f(X), f(Y)) \end{aligned} \tag{5.8.10}$$

Notemos que la Ecuación (5.8.10) nos dice que f es un endomorfismo de F_f: $f \circ F_f = F_f \circ f$ (ver Ecuación (5.8.8)).

Para cada $a \in \mathcal{O}_K$ y $f, g \in \mathcal{F}_\pi$, sea la serie $a_{f,g}(T) \in \mathcal{O}_K[[T]]$ la única solución de

$$\begin{aligned} a_{f,g}(T) &\equiv aT \text{ mód gr } 2, \\ f(a_{f,g}(T)) &= a_{f,g}(g(T)). \end{aligned} \tag{5.8.11}$$

Por notación, escribiremos $a_f = a_{f,f}$.

El siguiente teorema probará, entre otras cosas, que F_f es un grupo formal.

Teorema 5.8.34. *Sean* $f, g, h \in \mathcal{F}_\pi$ *y* $a, b \in \mathcal{O}_K$. *Entonces*

(1) $F_f(X,Y) = F_f(Y,X)$.
(2) $F_f(F_f(X,Y),Z) = F_f(X,F_f(Y,Z))$.
(3) $a_{f,g}(F_g(X,Y)) = F_f(a_{f,g}(X), a_{f,g}(Y))$.
(4) $a_{f,g}(b_{g,h}(Z)) = (a \cdot b)_{f,h}(Z)$.
(5) $(a+b)_{f,g}(Z) = F_f(a_{f,g}(Z), b_{f,g}(Z))$.
(6) $(\pi^n)_f(Z) = f^{(n)}(Z)$, $n = 0, 1, 2, \ldots$.

Demostración. Todos estas propiedades se siguen de resolver algún problema específico aplicando el Teorema 5.8.21.

(1) Sea $F(X,Y) = F_f(X,Y)$. Se tiene que

$$F_f(X,Y) \equiv X + Y \text{ mód gr } 2 \equiv Y + X \text{ mód gr } 2 \equiv F_f(Y,X).$$

Además se tiene que $f(F_f(X,Y)) = F_f(f(X), f(Y))$, por tanto

$$f(F_f(Y,X)) \underset{\substack{\uparrow \\ X \leftrightarrow Y}}{=} F_f(f(Y), f(X)).$$

Sea $G(X,Y) = F_f(Y,X)$. Entonces

$$f(G(X,Y)) = f(F_f(Y,X)) = F_f(f(Y), f(X)) = G(f(X), f(Y)).$$

Por unicidad, se tiene $F = G$, esto es, $F_f(X,Y) = G(X,Y) = F_f(Y,X)$.

(2) $F_f(F_f(X,Y),Z) \equiv F_f(X,Y)+Z$ mód gr $2 \equiv X+Y+Z$ mód gr $2 \equiv X + F_f(Y,Z)$ mód gr $2 = F_f(X, F_f(Y,Z))$ mód gr 2.
Sean $F_1(X,Y,Z) = F_f(F_f(X,Y),Z)$, $F_2(X,Y,Z) = F_f(X, F_f(Y,Z))$. Entonces

$$\begin{aligned}
f(F_1(X,Y,Z)) &= f(F_f(F_f(X,Y),Z)) = F_f(f(F_f(X,Y), f(Z))) \\
&= F_f(F_f(f(X), f(Y)), f(Z)) \\
&= F_f(F_f(f(X), f(Y)), f(Z)) \\
&= F_1(f(X), f(Y), f(Z)), \\
f(F_2(X,Y,Z)) &= f(F_f(X, F_f(Y,Z))) \\
&= F_f(f(X), f(F_f(Y,Z))) \\
&= F_f(f(X), F_f(f(Y), f(Z))) = F_2(f(X), f(Y), f(Z)).
\end{aligned}$$

Por tanto

$$\begin{gathered}
F_1(X,Y,Z) \equiv X+Y+Z \text{ mód gr } 2 \equiv F_2(X,Y,Z), \\
f \circ F_1 = F_1 \circ f \quad \text{y} \quad f \circ F_2 = F_2 \circ f.
\end{gathered}$$

Por unicidad tenemos que $F_1 = F_2$.

(3) Sea $H(X,Y)$ la única solución de

$$\begin{aligned}
&H(X,Y) \equiv aX + aY \text{ mód gr } 2, \\
&f(H(X,Y)) = H(g(X), g(Y)).
\end{aligned} \tag{5.8.12}$$

Sea $H_1(X,Y) = F_f(a_{f,g}(X), a_{f,g}(Y))$. Entonces

$$\begin{aligned}
H_1(X,Y) &= F_f(a_{f,g}(X), a_{f,g}(Y)) \equiv a_{f,g}(X) + a_{f,g}(Y) \\
&\equiv aX + aY \text{ mód gr } 2, \\
f(H_1(X,Y)) &= f(F_f(a_{f,g}(X), a_{f,g}(Y))) = F_f(f(a_{f,g}(X)), f(a_{f,g}(Y))) \\
&= F_f(a_{f,g}(g(X)), a_{f,g}(g(Y))) = H_1(g(X), g(Y)).
\end{aligned}$$

Se sigue que $H_1(X,Y,Z)$ es solución de la ecuación (5.8.12).
Sea $H_2(X,Y) = a_{f,g}(F_g(X,Y))$. Entonces

$$\begin{aligned} H_2(X,Y) &= a_{f,g}(F_g(X,Y)) \equiv aF_g(X,Y) \equiv a(X+Y) \text{ mód gr } 2, \\ f(H_2(X,Y)) &= f(a_{f,g}(F(X,Y))) = a_{f,g}(g(F_g(X,Y))) \\ &= a_{f,g}(F_g(g(X),g(Y))) = H_2(g(X),g(Y)). \end{aligned}$$

Se sigue que $H_2(X,Y,Z)$ también es solución de la ecuación (5.8.12). Por la unicidad dada en el Teorema 5.8.21, se sigue que $H_1(X,Y) = H_2(X,Y)$.

(4) Sea $H(Z)$ la solución a

$$H(Z) \equiv abZ \text{ mód gr } 2 \quad \text{y} \quad F(H(Z)) = H(h(Z)). \tag{5.8.13}$$

Sea $H_1(Z) = a_{f,g}(b_{g,h}(Z))$. Entonces

$$\begin{aligned} H_1(Z) &= a_{f,g}(b_{g,h}(Z)) \equiv ab_{g,h}(Z) \equiv abZ \text{ mód gr } 2, \\ f(H_1(Z)) &= f(a_{f,g}(b_{g,h}(Z))) = a_{f,g}(g(b_{g,h}(Z))) \\ &= a_{f,g}(b_{g,h}(h(Z))) = H_1(h(Z)). \end{aligned}$$

Sea ahora $H_2(Z) = (ab)_{f,h}(Z)$. Entonces

$$\begin{aligned} H_2(Z) &= (ab)_{f,h}(Z) \equiv abZ \text{ mód gr } 2, \\ f(H_2(Z)) &= f((ab)_{f,h}(Z)) = (ab)_{f,h}(h(T)) = H_2(h(T)). \end{aligned}$$

Por tanto H_1 y H_2 son soluciones de la ecuación (5.8.13), de donde se sigue que $H_1(Z) = H_2(Z) = H(Z)$.

(5) Sea $H(Z)$ solución a

$$H(Z) \equiv (a+b)Z \text{ mód gr } 2 \quad \text{y} \quad f(H(Z)) = H(g(Z)). \tag{5.8.14}$$

Sea $H_1(Z) = (a+b)_{f,g}(Z)$. Entonces

$$\begin{aligned} H_1(Z) &= (a+b)_{f,g}(Z) \equiv (a+b)Z \text{ mód gr } 2, \\ f(H_1(Z)) &= f((a+b)_{f,g}(Z)) = (a+b)_{f,g}(g(Z)) = H_1(g(Z)). \end{aligned}$$

Sea ahora $H_2(Z) = F_f(a_{f,g}(Z), b_{f,g}(Z))$. Entonces

$$\begin{aligned} H_2(Z) &= F_f(a_{f,g}(Z), b_{f,g}(Z)) \equiv a_{f,g}(Z) + b_{f,g}(Z) \text{ mód gr } 2 \\ &\equiv aZ + bZ \text{ mód gr } 2, \\ f(H_2(Z)) &= f(F_f(a_{f,g}(Z), b_{f,g}(Z))) = F_f(f(a_{f,g}(Z)), f(b_{f,g}(Z))) \\ &= F_f(a_{f,g}(g(Z)), b_{f,g}(g(Z))) = H_2(g(Z)). \end{aligned}$$

Se sigue que $H_1(Z) = H_2(Z)$.

(6) Sea $n \geq 0$ y sea $H^{(n)}(Z)$ la solución a

$$H^{(n)}(Z) \equiv \pi^n Z \text{ mód gr } 2 \quad \text{y} \quad f(H^{(n)}(Z)) = H^{(n)}(f(Z)).$$

Sea $H_1^{(n)}(Z) = (\pi^n)_f(Z)$. Entonces

$$H_1^{(n)}(Z) = (\pi^n)_f(Z) \equiv \pi^n Z \text{ mód gr } 2,$$
$$f(H_1^{(n)}(Z)) = f((\pi^n)_f(Z)) = (\pi^n)_f(f(Z)) = H_1^{(n)}(f(Z)).$$

Sea ahora $H_2^{(n)}(Z) = f^{(n)}(Z)$. Entonces

$$\begin{aligned} H_2^{(n)}(Z) = f^{(n)}(Z) &= f(f^{(n-1)}(Z)) \equiv \pi f^{(n-1)}(Z) \text{ mód gr } 2 \\ &\equiv \pi\pi^{n-1} Z \text{ mód gr } 2, \\ f(H_2^{(n)}(Z)) = f(f^{(n)}(Z)) &= f^{(n)}(f(Z)) = H^{(n)}(f(Z)). \end{aligned}$$

Por tanto se tiene que $H_1(Z) = H_2(Z)$. □

Sea L una extensión algebraica del campo local K. Sea $\mathfrak{p}_L = \{x \in L \mid v_L(x) > 0\}$. Si $x_1, \ldots, x_n \in \mathfrak{p}_L$ y $G(X_1, \ldots, X_n) \in \mathcal{O}_K[[X_1, \ldots, X_n]]$, entonces $G(x_1, \ldots, x_n)$ converge en $K(x_1, \ldots, x_n)$. Si además el término constante de G es 0, $G(x_1, \ldots, x_n) \in \mathfrak{p}_L$.

Una demostración de lo anterior, es como sigue. Como K es completo, $K[x_1, \ldots, x_n] = k(x_1, \ldots, x_n)$ también es completo y si G_d denota a G quitando los términos de grado total $\geq d+1$, entonces

$$\begin{aligned} |G(x_1, \ldots, x_n) - G_d(x_1, \ldots, x_n)| &= \Big| \sum_i a_{i_1,\ldots,i_n} x_1^{i_1} \cdots x_n^{i_n} \Big| \\ &\leq |x_1^{i_1}| \cdots |x_n^{i_n}| \leq c^{i_1+\cdots+i_n} \leq c^{d+1} \xrightarrow[d\to\infty]{} 0, \end{aligned}$$

donde $|x_1|, \ldots, |x_n| \leq c < 1$.

Entonces $\lim_{d\to\infty} G_d(x_1, \ldots, x_n) = G(x_1, \ldots, x_n)$ pues $\{G_d(x_1, \ldots, x_n)\}_d$ es una sucesión de Cauchy. Si $a_{0,\ldots,0} = 0$, claramente $|G_d(x_1, \ldots, x_n)| < 1$ y $G(x_1, \ldots, x_n) \in \mathfrak{p}_L$.

Por esta razón, para $f = g = h$ las propiedades del Teorema 5.8.34, hacen de F_f un $\mathcal{O}_K$*–módulo (de Lie) formal*.

Si en el Teorema 5.8.34 tomamos $f = g = h$ y pensamos $F_f(x, y)$ como la suma y $a_{f,f}$, $a \in \mathcal{O}_K$ como la multiplicación por escalar, entonces tendríamos un $\mathcal{O}_K$–módulo haciendo que las variables X, Y y Z tomen valores de un dominio donde las series convergen (por ejemplo L, una extensión algebraica de K).

Proposición 5.8.35. *Si $f \in \mathcal{F}_\pi$ y L es una extensión algebraica de K, $\mathfrak{p}_L$ es un $\mathcal{O}_K$–módulo con la suma y multiplicación por escalar definidas por:*

$$x \oplus_{F_f} y := F_f(x, y) \quad y \quad a \odot_{F_f} x = a_f(x), \quad x, y \in \mathfrak{p}_L, a \in \mathcal{O}_K.$$

Se denota $\mathfrak{p}_L^{(f)}$ a este $\mathcal{O}_K$–módulo.

Demostración. Es consecuencia inmediata de Teorema 5.8.34. □

Observación 5.8.36. Las propiedades (1) y (2) del Teorema 5.8.34 prueban que $\mathfrak{p}_L^{(f)}$ es un grupo aditivo. Las propiedades (3), (4) y (5) con $f = g = h$, prueban que $\mathfrak{p}_L^{(f)}$ es un $\mathcal{O}_K$–módulo.

El inverso aditivo de x es $(-1)_f(x) = (-1) \odot_{F_f} x$. Es importante distinguir $\mathfrak{p}_L^{(f)}$ de $\mathfrak{p}_L$: ambos son el mismo conjunto y ambos son $\mathcal{O}_K$–módulos pero con diferente acción.

Teorema 5.8.37. *El conjunto de ceros $\Lambda_{f,n}$ de $f^{(n)}(x)$ es un $\mathcal{O}_K$–submódulo de $\mathfrak{p}_{L_{f,n}}^{(f)}$, $n \geq 1$, donde recordemos que $L_{f,n} = K(\Lambda_{f,n})$.*

Más aún, $\Lambda_{f,n}$ son los punto de π^n–torsión del $\mathcal{O}_K$–módulo $\mathfrak{p}_{L_{f,n}}^{(f)}$. Esto es

$$\Lambda_{f,n} = \{\lambda \in \mathfrak{p}_{L_{f,n}} \mid \pi^n \odot_{F_f} \lambda = 0\} = \{\lambda \in \bar{K} \mid \pi^n \odot_{F_f} \ \lambda = 0\}.$$

Demostración. Por definición, tenemos que si $x \in \Lambda_{f,n}$, entonces $x \in \mathfrak{p}_{L_{f,n}}$. Se tiene

$$\begin{aligned} \Lambda_{f,n} &= \{\lambda \in \mathfrak{p}_{L_{f,n}} \mid f^{(n)}(\lambda) = (\pi^n)_f(\lambda) = 0\} \\ &= \{\lambda \in \mathfrak{p}_{L_{f,n}} \mid \pi^n \odot_{F_f} \lambda = 0\} = \text{núc}\, \pi^n. \end{aligned}$$

Por tanto $\Lambda_{f,n}$ es un $\mathcal{O}_K$–módulo. □

Nuevamente hacemos notar la similitud de $\Lambda_{f,n}$ como $\mathcal{O}_K$–módulo y de Λ_M, $M \in R_T = \mathbb{F}_q[T]$ como R_T–módulo (Carlitz).

Ejemplo 5.8.38. Sean $K = \mathbb{Q}_p$ y $f(T) = (T+1)^p - 1 \in \mathcal{F}_p$. Entonces

$$\Lambda_{f,n} = \{\lambda \in \mathbb{Q}_p \mid p^n \odot_{F_f} \lambda = 0\} = \{\lambda \in \bar{\mathbb{Q}}_p \mid f^{(n)}(\lambda) = 0\}.$$

Se tiene $f^{(2)}(T) = f(f(T)) = (f(T)+1)^p - 1 = ((T+1)^p - 1 + 1)^p - 1 = (T+1)^{p^2} - 1$ y en general $f^{(n)}(T) = (T+1)^{p^n} - 1$. Se sigue que

$$\Lambda_{f,n} = \{\lambda \in \bar{\mathbb{Q}}_p \mid (\lambda+1)^{p^n} - 1 = 0\} = \{\zeta_{p^n}^i - 1\}_{i=0}^{p^n-1} \cong \langle \zeta_{p^n} \rangle \cong W_{p^n}.$$

Proposición 5.8.39. *Sean $f, g \in \mathcal{F}_\pi$ y $a \in \mathcal{O}_K$. El mapeo $\lambda \longmapsto a_{g,f}(\lambda)$ da lugar a un homomorfismo de $\mathcal{O}_K$–módulos de $\Lambda_{f,n}$ en $\Lambda_{g,n}$. Este homomorfismo es un isomorfismo si $a \in U_K$. Más precisamente, se tiene $a_{g,f} \colon F_f \longrightarrow F_g$.*

Demostración. Por el Teorema 5.8.34 (3) y (4), se tiene

$$\begin{aligned} \lambda \oplus_{F_f} \mu = F_f(\lambda, \mu) \longmapsto a_{g,f}(F_f(\lambda, \mu)) &= F_g(a_{g,f}(\lambda), a_{g,f}(\mu)) \\ &= a_{g,f}(\lambda) \oplus_{G_f} a_{g,f}(\mu), \end{aligned}$$

y

$$\begin{aligned} b \odot_{F_f} \lambda = b_f(\lambda) \longmapsto a_{g,f}(b_f(\lambda)) &= (ab)_{g,f}(\lambda) = (ba)_{g,f}(\lambda) \\ &= b_{g,g}(a_{g,f}(\lambda)) = b \odot_{G_f} a_{g,f}(\lambda). \end{aligned}$$

Por tanto el mapeo es un homomorfismo de $\mathcal{O}_K$–módulos. Además, si $\lambda \in \Lambda_{f,n}$,

$$\begin{aligned} g^{(n)}(a_{g,f}(\lambda)) &= (\pi^n)_g(a_{g,f}(\lambda)) = (\pi^n a)_{g,f}(\lambda) = (a\pi^n)_{g,f}(\lambda) \\ &= a_{g,f}((\pi^n)_f(\lambda)) = a_{g,f}(f^{(n)}(\lambda)) = a_{g,f}(0) = 0. \end{aligned}$$

Por tanto el homomorfismo manda $\Lambda_{f,n}$ en $\Lambda_{g,n}$.

Ahora si, $a \in U_K$, para $\lambda \in \Lambda_{f,n}$ se tiene

$$(a^{-1})_{f,g}(a_{g,f}(\lambda)) = (a^{-1}a)_{f,f}(\lambda) = 1_f(\lambda) = 1 \odot_{F_f} \lambda = \lambda$$

y para $\mu \in \Lambda_{g,n}$ se tiene

$$(a_{g,f})((a^{-1})_{f,g})(\mu) = (aa^{-1})_{g,g}(\mu) = 1_g(\mu) = 1 \odot_{G_f} \mu = \mu.$$

Se sigue que el homomorfismo $a_{g,f}\colon \Lambda_{f,n} \longrightarrow \Lambda_{g,n}$ tiene como inverso a $(a^{-1})_{f,g}\colon \Lambda_{g,n} \longrightarrow \Lambda_{f,n}$. □

Teorema 5.8.40. *Para cualquier $f \in \mathcal{F}_\pi$, se tiene*

$$\Lambda_{f,n} \cong \mathcal{O}_K/\pi^n\mathcal{O}_K$$

como $\mathcal{O}_K$–módulos.

Demostración. Para cualesquiera $f, g \in \mathcal{F}_\pi$, $1_{g,f}\colon \Lambda_{f,n} \longrightarrow \Lambda_{g,n}$ es un isomorfismo de $\mathcal{O}_K$–módulos. Basta considerar $f(Z) = \pi Z + Z^q \in \mathcal{F}_\pi$.

Se hará por inducción en n. Para $n = 1$, $\Lambda_{f,1}$ es el conjunto de ceros de $f(\lambda) = \pi\lambda + \lambda^q = 0$ el cual es un polinomio separable pues $f'(\lambda) = \pi \neq 0$. Esto es, $\Lambda_{f,1}$ tiene q elementos y por tanto es un espacio vectorial sobre $\mathbb{F}_q$ de dimensión 1. En este caso $\mathbb{F}_q \cong \mathcal{O}_K/\pi\mathcal{O}_K$, de donde se sigue que $\Lambda_{f,1} \cong \mathcal{O}_K/\pi\mathcal{O}_K$.

Supongamos que $\Lambda_{f,n} \cong \mathcal{O}_K/\pi^n\mathcal{O}_K$ como $\mathcal{O}_K$–módulos. Consideremos $\pi_f\colon \Lambda_{f,n+1} \longrightarrow \Lambda_{f,n}$ dada por $\pi_f(\lambda) = \pi \odot_{F_f} \lambda \in \Lambda_{f,n}$ para $\lambda \in \Lambda_{f,n+1}$ pues $f^{(n)}(\pi_f(\lambda)) = f^{(n)}(f(\lambda)) = f^{(n+1)}(\lambda) = 0$.

Puesto que $\operatorname{núc}\pi_f = \Lambda_{f,1}$ y $|\Lambda_{f,n+1}| = q^{n+1}$, $|\Lambda_{f,n}| = q^n$, se tiene la sucesión exacta

$$0 \longrightarrow \Lambda_{f,1} \longrightarrow \Lambda_{f,n+1} \xrightarrow{\pi_f} \Lambda_{f,n} \longrightarrow 0.$$

Otra forma de verificar la suprayectividad de π_f es como sigue. Si $\lambda \in \Lambda_{f,n}$ y μ es una raíz de $f(Z) - \lambda = Z^q + \pi Z - \lambda$, entonces $\lambda = f(\mu)$ y $f^{(n+1)}(\mu) = f^{(n)}(f(\mu)) = 0$ y por tanto $\pi_f(\mu) = f(\mu) = \lambda$ y π_f es suprayectiva.

Sea $\lambda \in \Lambda_{f,n+1} \setminus \Lambda_{f,n}$, entonces $(\pi^n)_f(\lambda) \neq 0$ y $(\pi^{n+1})_f(\lambda) = 0$ por lo que el anulador de λ es $\pi^{n+1}\mathcal{O}_K$. El mapeo $a \longmapsto a \odot_{F_f} \lambda$ da el isomorfismo.

$$\mathcal{O}_K\lambda \cong \mathcal{O}_K/\pi^{n+1}\mathcal{O}_K$$

y $\mathcal{O}_K\lambda \subseteq \Lambda_{f,n+1}$. Puesto que $\left|\mathcal{O}_K/\pi^{n+1}\mathcal{O}_K\right| = |\Lambda_{f,n+1}| = q^{n+1}$, se sigue que $\mathcal{O}_K\lambda = \Lambda_{f,n+1} \cong \mathcal{O}_K/\pi^{n+1}\mathcal{O}_K$. □

Teorema 5.8.41. *Todo automorfismo del $\mathcal{O}_K$–módulo $\Lambda_{f,n}$ es de la forma $u_f\colon \Lambda_{f,n} \longrightarrow \Lambda_{f,n}$ con $u \in U_K$. Se tiene que $u_f = \mathrm{Id}_{\Lambda_{f,n}}$ si y sólo si $u \in U_K^{(n)}$. Por tanto*

$$\mathrm{Aut}_{\mathcal{O}_K}(\Lambda_{f,n}) \cong U_K/U_K^{(n)}.$$

Demostración. Si $\sigma \in \mathrm{Aut}_{\mathcal{O}_K}(\Lambda_{f,n})$ se tiene que, usando el isomorfismo de $\mathcal{O}_K$–módulos $\Lambda_{f,n} \cong \mathcal{O}_K/\pi^n\mathcal{O}_K$, $\sigma \in \mathrm{Aut}_{\mathcal{O}_K}(\mathcal{O}_K/\pi^n\mathcal{O}_K)$. Sea $\tau\colon \mathcal{O}_K \longrightarrow \mathcal{O}_K/\pi^n\mathcal{O}_K$ el epimorfismo natural. Por tanto $\sigma\circ\tau\colon \mathcal{O}_K \longrightarrow \mathcal{O}_K/\pi^n\mathcal{O}_K$ es un epimorfismo de $\mathcal{O}_K$–módulos y para $\xi \in \mathcal{O}_K$ se tiene

$$(\sigma\circ\tau)(\xi) = \xi(\sigma\circ\tau)(1) = \xi\sigma(1 \bmod \pi^n).$$

Se sigue que $\sigma(1 \bmod \pi^n) = a$ genera a $\mathcal{O}_K/\pi^n\mathcal{O}_K$ y por tanto a es unidad.

Se tiene el siguiente diagrama conmutativo

$$\begin{array}{ccc} \mathcal{O}_K/\pi^n\mathcal{O}_K & \xrightarrow{a} & \mathcal{O}_K/\pi^n\mathcal{O}_K \\ \cong\big\downarrow\varphi & & \varphi\big\downarrow\cong \\ \Lambda_{f,n} & \xrightarrow{\sigma} & \Lambda_{f,n} \end{array}$$

donde $\varphi(1 \bmod \pi^n) = \lambda$ es un generador $\Lambda_{f,n}$. Entonces $\sigma(\lambda) = (\varphi a \varphi^{-1})(\lambda) = a \odot_{F_f} \lambda = a_f(\lambda)$.

Ahora $\sigma = \mathrm{Id} \iff \sigma(1 \bmod \pi^n) = a \bmod \pi^n = 1 \bmod \pi^n \iff a - 1 \equiv 0 \bmod \pi^n \iff a \in U_K^{(n)}$. □

Teorema 5.8.42. *El campo $L_{f,n}$ depende únicamente de π y no de la elección de $f \in \mathcal{F}_\pi$. Esto es, para toda $n \geq 1$ y para cualesquiera $f, g \in \mathcal{F}_\pi$, se tiene $K(\Lambda_{f,n}) = K(\Lambda_{g,n})$.*

Demostración. Sean $f, g \in \mathcal{F}_\pi$ y $\lambda \in \Lambda_{f,n}$. Se tiene que $1_{g,f}(Z) \in \mathcal{O}_K[[Z]]$, por tanto $1_{g,f}(\lambda) \in K(\lambda) \subseteq L_{f,n}$. Puesto que $1_{g,f}\colon \Lambda_{f,n} \longrightarrow \Lambda_{g,n}$ es biyectiva, $\Lambda_{g,n} \subseteq L_{f,n}$. Se sigue que $L_{g,n} = K(\Lambda_{g,n}) \subseteq L_{f,n}$. Por simetría tenemos que $L_{f,n} \subseteq L_{g,n}$. □

Definición 5.8.43. Para cualquier $f \in \mathcal{F}_\pi$, se define $L_{\pi,n} := L_{f,n}$ y $L_\pi := \bigcup_{n=1}^{\infty} L_{f,n}$.

Debido al Teorema 5.8.42, se puede suponer que $L_{\pi,n}$ está generado por las raíces de $f^{(n)}(Z)$ donde $f(Z) = \pi Z + Z^q \in \mathcal{F}_\pi$. La extensión $L_{\pi,n}/K$ es una extensión de Galois.

Definición 5.8.44. Se define $G_{\pi,n} := \mathrm{Gal}(L_{\pi,n}/K)$ y $G_\pi = \mathrm{Gal}(L_\pi/K) = \mathrm{Gal}(\bigcup_{n=1}^{\infty} L_{\pi,n}/K) = \varprojlim G_{\pi,n}$.

Consideremos $\sigma \in G_{\pi,n}$ y $\lambda \in \Lambda_{f,n}$. Sea $f(Z) = \pi Z + \sum_{i=1}^{\infty} a_i Z^i$ con $a_i \in \mathcal{O}_K$. Se tiene que $f^{(n)}(Z) = \sum_{j=2}^{\infty} b_j Z^j \in \mathcal{O}_K[[Z]]$ para $n \geq 2$ y $f^{(n)}(\lambda)$ es convergente. Como σ actúa de manera continua en $L_{\pi,n}$,

$$0 = \sigma(0) = \sigma(f^{(n)}(\lambda)) = \sum_{j=2}^{\infty} \sigma(b_j \lambda^j) \underset{\substack{\uparrow \\ b_j \in K}}{=} \sum_{j=2}^{\infty} b_j (\sigma\lambda)^j = f^{(n)}(\sigma\lambda).$$

Por tanto $f^{(n)}(\sigma\lambda) = 0$ y $\sigma\lambda \in \Lambda_{f,n}$.

Puesto que $\mathrm{Aut}_{\mathcal{O}_K}(\Lambda_{f,n}) \cong U_K/U_K^{(n)}$, cada clase $uU_K^{(n)} \in U_K/U_K^{(n)}$ da lugar al automorfismo $\mu_f \colon \Lambda_{f,n} \longrightarrow \Lambda_{f,n}$.

Teorema 5.8.45. *Para cada $\sigma \in G_{\pi,n}$ existe una única clase $u_\sigma U_K^{(n)} = uU_K^{(n)} \in U_K/U_K^{(n)}$ tal que $\sigma(\lambda) = (u_\sigma)_f(\lambda)$, $\lambda \in \Lambda_{f,n}$. El mapeo $\sigma \mapsto u_\sigma U_K^{(n)}$ da lugar a un isomorfismo $G_{\pi,n} \cong U_K/U_K^{(n)}$. Además $L_{\pi,n} = K(\lambda)$ donde* $\mathrm{Irr}(Z, \lambda, K) = \frac{f^{(n)}(Z)}{f^{(n-1)}(Z)}$.

Demostración. Notemos que si $a \in \mathcal{O}_K$ y $\lambda \in \Lambda_{f,n}$ entonces $a \odot_{F_f} \lambda = a_f(\lambda) = \sum_{i=1}^{\infty} c_i \lambda^i \in \mathcal{O}_K[[\lambda]]$ y por tanto

$$\sigma(a \odot_{F_f} \lambda) = \sigma(a_f(\lambda)) = \sigma\Big(\sum_{i=1}^{\infty} c_i \lambda^i\Big) = \sum_{i=1}^{\infty} c_i (\sigma\lambda)^i = a_f(\sigma\lambda) = a \odot_{F_f} (\sigma\lambda).$$

En otras palabras, las acciones de $\mathcal{O}_K$ y de $G_{\pi,n}$ sobre $\Lambda_{f,n}$ conmutan.

Cada $\sigma \in G_{\pi,n}$ induce un automorfismo del $\mathcal{O}_K$–módulo $\Lambda_{f,n}$, esto es, existe $uU_K^{(n)} \in U_K/U_K^{(n)}$ tal que $\sigma\lambda = u_f(\lambda) = u \odot_{F_f} \lambda$ para toda $\lambda \in \Lambda_{f,n}$.

Se tiene el mapeo $G_{\pi,n} \xrightarrow{\varphi} U_K/U_K^{(n)}$, $\sigma \longmapsto u_\sigma U_K^{(n)}$, donde $\sigma\lambda = u_\sigma \odot_{F_f} \lambda$ para toda $\lambda \in \Lambda_{f,n}$.

Como $\Lambda_{f,n}$ genera a $L_{\pi,n}$ sobre K, si $\sigma \in \mathrm{núc}\,\varphi$, entonces $\sigma\lambda = u_f(\lambda) = \lambda$ para toda $\lambda \in \Lambda_{f,n}$, por lo tanto $\sigma = \mathrm{Id}$.

Se tiene que $\big|U_K/U_K^{(n)}\big| = q^{n-1}(q-1)$. Veamos que $|G_{\pi,n}| \geq q^{n-1}(q-1)$. Se tiene $f^{(n)}(Z) = f(f^{(n-1)}(Z)) = f^{(n-1)}(Z)\phi_n(Z)$ con $\phi_n(Z) = (f^{(n-1)}(Z))^{q-1} + \pi \in \mathcal{O}_K[Z]$ (recordemos que $f(Z) = \pi Z + Z^q$).

Ahora $f^{(2)}(Z) = f(f(Z)) = f(Z)^q + \pi f(Z) = (Z^q + \pi Z)^q + \pi(Z^q + \pi Z) = Z^{q^2} + \pi^q Z^q + \pi Z^q + \pi^2 Z$. En general se tiene $f^{(n-1)}(Z) = Z^{q^{n-1}} + \pi(b_{n-2} Z^{q^{n-2}} + \cdots + b_2 Z^{q^2}) + \pi^{n-1} Z$.

Puesto que $\phi_n(Z) = (f^{(n-1)}(Z))^{q-1} + \pi \in \mathcal{O}_K[Z]$, $\phi_n(Z)$ es un polinomio de Eisenstein y por tanto irreducible sobre K. Si λ es una raíz de $\phi_n(Z)$, y por tanto raíz de $f^{(n)}(Z)$, entonces $K(\lambda)$ es una extensión totalmente ramificada de K. Además

$$|G_{\pi,n}| \geq [K(\lambda) : K] = q^{n-1}(q-1) = \mathrm{gr}\,\phi_n(Z) = \mathrm{gr}\,\frac{f^{(n)}(Z)}{f^{(n-1)}(Z)} = \big|U_K/U_K^{(n)}\big|,$$

por tanto $G_{\pi,n} \cong U_K/U_K^{(n)}$ y además $L_{\pi,n} = K(\lambda)$ donde λ es una raíz del polinomio de Eisenstein $\phi_n(Z)$ y $\mathrm{Irr}(Z,\lambda,K) = \phi_n(Z) = \frac{f^{(n)}(Z)}{f^{(n-1)}(Z)}$. □

Hemos demostrado más de lo enunciado:

Teorema 5.8.46. *La extensión $L_{\pi,n}/K$ es una extensión abeliana y totalmente ramificada de grado $q^{n-1}(q-1)$ y es generada por una raíz de*

$$\phi_n(Z) = (f^{(n-1)}(Z))^{q-1} + \pi = \frac{f^{(n)}(Z)}{f^{(n-1)}(Z)}.$$ □

Corolario 5.8.47. *π es una norma de $L_{\pi,n}$ a K.*

Demostración. Se tiene $\phi_n(Z) = \prod_{\sigma\in G_{\pi,n}}(Z-\lambda^\sigma) = (f^{(n-1)}(Z))^{q-1}+\pi$. Por lo tanto $\pi = \prod_{\sigma\in G_{\pi,n}}(-\lambda)^\sigma = \mathrm{N}_{L_{\pi,n}/K}(-\lambda)$ por lo que π es una norma. □

Observación 5.8.48. Todo este desarrollo se basa en un elemento primo $\pi \in \mathcal{O}_K$ fijo. Esto corresponde al caso primo infinito $\mathfrak{p}$ en el caso de campos de funciones, $\mathbb{F}_q(z)$, $\mathfrak{p}$ el polo de x. Así que, debemos estudiar la misma situación cuando tomamos otro elemento primo π'.

Notación 5.8.49. Dado un campo local K, T denotará la máxima extensión no ramificada de K contenida en una cerradura algebraica $\bar{K}$ de K fija. Es decir $T = K^{\mathrm{nr}}$.

Se tiene $\mathrm{Gal}(T/K) \cong \mathrm{Gal}(\overline{\mathbb{F}_q}/\mathbb{F}_q) \cong \hat{\mathbb{Z}}$.

Teorema 5.8.50. *Se tiene $G_\pi \cong U_K$.*

Demostración. Del isomorfismo $G_{\pi,n} \cong U_K/U_K^{(n)}$, se sigue que

$$G_\pi = \mathrm{Gal}(L_\pi/K) \cong \varprojlim G_{\pi,n} \cong \varprojlim U_K/U_K^{(n)} \cong U_K.$$ □

Sea $\tau_K \in \mathrm{Gal}(T/K)$ el automorfismo de Frobenius de T/K, y sea $\bar{\tau}_K$ la única extensión continua de τ_K en la completación $T_{\mathfrak{p}}$ de T en $\bar{K}_{\mathfrak{p}}$, una cerradura algebraica de $K_{\mathfrak{p}}$. Usaremos la notación $\tau = \tau_K = \bar{\tau}_K$. Por definición, τ_K induce el automorfismo $\alpha \mapsto \alpha^q$ en el campo residual $T(\mathfrak{p}_T)$

$$\alpha^\tau = \tau(\alpha) = \alpha^q \text{ mód } \mathfrak{p}_T \quad \text{para toda} \quad \alpha \in \mathcal{O}_T,$$

donde $\mathcal{O}_T$ denota el anillo de enteros de T y $\mathfrak{p}_T$ denota el ideal máximo de $\mathcal{O}_T$.

Usaremos la notación $\bar{T}$ para la completación $T_{\mathfrak{p}_T}$ de T. Se tiene la igualdad de campos residuales $\bar{T}(\mathfrak{p}_T) = \bar{T}_{\mathfrak{p}_{\bar{T}}}(\mathfrak{p}_{\bar{T}})$ el cual denotaremos simplemente por $\bar{T}(\mathfrak{p})$.

Consideremos los endomorfismos

$$\begin{aligned}\tau-1\colon \mathcal{O}_{\bar{T}} &\longrightarrow \mathcal{O}_{\bar{T}}\\ \alpha &\longmapsto (\tau-1)(\alpha)=\tau(\alpha)-\alpha,\\ \tau-1\colon U_{\bar{T}} &\longrightarrow U_{\bar{T}}\\ u &\longmapsto u^{\tau-1}=\tau(u)/u,\end{aligned}$$

donde $U_{\bar{T}}=\{x\in\bar{T}\mid |x|=1\}$. Se tiene el siguiente resultado.

Lema 5.8.51. *Las siguientes sucesiones*

$$\begin{aligned}0\longrightarrow \mathcal{O}_K\longrightarrow \mathcal{O}_{\bar{T}}\xrightarrow{\tau-1}\mathcal{O}_{\bar{T}}\longrightarrow 0,\\ 1\longrightarrow U_K\longrightarrow U_{\bar{T}}\xrightarrow{\tau-1}U_{\bar{T}}\longrightarrow 1,\end{aligned}$$

son exactas. En particular $(\tau-1)\mathcal{O}_{\bar{T}}=\mathcal{O}_{\bar{T}}$ *y* $U_{\bar{T}}^{\tau-1}=U_{\bar{T}}$.

Demostración. Las demostraciones son totalmente paralelas y por tanto la haremos principalmente para $U_{\bar{T}}$.

Puesto que el campo residual $S:=\bar{T}(\mathfrak{p})=\mathcal{O}_{\bar{T}}/\bar{T}_{\mathfrak{p}_{\bar{T}}}\cong\mathcal{O}_T/\mathfrak{p}_T=T(\mathfrak{p})\cong\bar{\mathbb{F}}_q$ es algebraicamente cerrado, los mapeos $\alpha\longmapsto\tau(\alpha)-\alpha$ y $\alpha\longmapsto\alpha^{\tau-1}=\tau(\alpha)/\alpha$ son suprayectivos de $S\longrightarrow S$ y de $S^*\longrightarrow S^*$ respectivamente.

Se tiene

$$U_{\bar{T}}/U_{\bar{T}}^{(1)}\cong S^*=\bar{T}(\mathfrak{p})^*,\quad U_{\bar{T}}^{(n)}/U_{\bar{T}}^{(n+1)}\cong S^+=\bar{T}(\mathfrak{p})^+\quad\text{y}\qquad(5.8.15)$$
$$\mathcal{O}_{\bar{T}}/\mathfrak{p}_{\bar{T}}\cong\mathfrak{p}_{\bar{T}}^n/\mathfrak{p}_{\bar{T}}^{n+1}\cong S^+=\bar{T}(\mathfrak{p})^+.$$

Ahora bien, si $x\in U_{\bar{T}}$ (resp. $x\in\mathcal{O}_{\bar{T}}$), existe $y_1\in T^*(\mathfrak{p})$ (resp. $y_1\in T(\mathfrak{p})^+$) tal que $\bar{x}=\tau\bar{y}_1/\bar{y}_1\in\bar{T}(\mathfrak{p})^*$ (rest. $\bar{x}=\tau\bar{y}_1-\bar{y}_1\in\bar{T}(\mathfrak{p})^+$) donde $\bar{z}=z$ mód $\mathfrak{p}$, por lo que $x=\frac{\tau y_1}{y_1}a_1$ con $y_i\in U_{\bar{T}}$ y $a_1\in U_{\bar{T}}^{(1)}$ (resp. $x=\tau y_1-y_1+a_1$ con $y_1\in\mathcal{O}_{\bar{T}}$, $a_1\in\mathfrak{p}_T$).

De la Ecuación (5.8.15), podemos continuar el proceso y tenemos $a_1=\frac{\tau y_2}{y_2}a_2$, con $y_2\in U_{\bar{T}}^{(1)}$ y $a_2\in U_{\bar{T}}^{(2)}$ (resp. $a_1=\tau y_2-y_2+a_2$ con $y_2\in\mathfrak{p}_{T_{\mathfrak{p}}}$ y $a_2\in\mathfrak{p}_{\bar{T}}^2$). Se sigue que $x=\frac{\tau(y_1y_2)}{y_1y_2}a_2$ (resp. $x=\tau(y_1+y_2)-(y_1+y_2)+a_2$).

En general obtendremos

$$x=\frac{\tau(y_1\cdots y_n)}{y_1\cdots y_n}a_n,\quad y_n\in U_{\bar{T}}^{(n-1)},\quad a_n\in U_{\bar{T}}^{(n)},$$
$$\text{(resp. } x=\tau(y_1+\cdots+y_n)-(y_1+\cdots+y_n)+a_n,\quad y_n\in\mathfrak{p}_{\bar{T}}^{n-1},\quad a_n\in\mathfrak{p}_{\bar{T}}^n).$$

Pasando al límite y puesto que $\bar{T}$ es completo, se obtiene

$$x=\frac{\tau y}{y},y=\prod_{n=1}^{\infty}y_n\in U_{\bar{T}}\quad(\text{resp. } x=\tau y-y,\quad y=\sum_{n=1}^{\infty}y_n\in\mathcal{O}_{\bar{T}})$$

lo cual prueba en ambos caso la suprayectividad de $\tau-1$.

Puesto que $\tau \in \mathrm{Gal}(\bar{T}/K)$ y $U_K \subseteq K$, se tiene que U_K está contenido en el núc$(\tau - 1)$: $U_{\bar{T}} \longrightarrow U_{\bar{T}}$.

Ahora sea $\xi^{\tau-1} = 1$, esto es, $\xi^\tau = \xi$, con $\xi \in U_{\bar{T}}$. Se tiene que $\{0\} \bigcup \bigcup_{m=1}^{\infty} V_m = \{0\} \bigcup V_\infty$ es un conjunto de representantes de $\bar{T}(\mathfrak{p})$, donde $V_m = \{\zeta_{q^{m-1}}^i \mid 0 \leq i \leq q^m - 2\}$, por lo que $\xi = \sum_{n=0}^{\infty} a_n \pi^n$ con $a_n \in \{0\} \bigcup V_\infty$.

Se tiene que $\tau(a_n) = a_n^q$ y $\tau(\xi) = \sum_{n=0}^{\infty} a_n^q \pi^n = \sum_{n=0}^{\infty} a_n \pi^n = \xi$ lo cual implica que $a_n = 0$ o $a_n^{q-1} = 1$ por lo que $a_n \in V_1 = \{\zeta_{q-1}^i \mid 0 \leq i \leq q-2\}$. Se sigue que $\xi \in K \cap U_{\bar{T}} = U_K$ y por tanto

$$1 \longrightarrow U_K \longrightarrow U_{\bar{T}} \xrightarrow{\tau - 1} U_{\bar{T}} \longrightarrow 1$$

es exacta. La demostración de la exactitud de la otra sucesión es similar. □

El Lema 5.8.51 nos permite probar un resultado similar al Teorema 5.8.21 pero ahora con respecto a un cambio en el elemento primo.

Teorema 5.8.52. *Sean π y $\pi' = a\pi$ dos elementos primos de K, $a \in U_K$. Sean $f \in \mathcal{F}_\pi$ y $f' \in \mathcal{F}_{\pi'}$. Entonces existe una serie de potencias $\theta(Z) \in \mathcal{O}_{\bar{T}}[[Z]]$, tal que*

(1) $\theta(Z) \equiv \varepsilon Z$ mód gr 2, $\varepsilon \in U_{\bar{T}}$,
(2) $\theta^\tau(Z) = \theta(a_f(Z))$,
(3) $\theta(F_f(X,Y)) = F_{f'}(\theta(X), \theta(Y))$,
(4) $\theta(b_f(Z)) = b_{f'}(\theta(Z))$ *para toda* $b \in \mathcal{O}_K$,

donde θ^τ denota a la serie obtenida a partir de la de θ aplicando el automorfismo de Frobenius τ a los coeficientes de θ.

Antes de probar el teorema, hagamos la siguiente observación. En general si α y β son dos series en $\mathcal{O}_{\bar{T}}[[Z]]$ y si σ es un automorfismo de $\bar{T}$, entonces $\alpha^\sigma, \beta^\sigma$ representan a las series cuyos coeficientes son obtenidos a partir de α y β aplicando σ a cada uno de los coeficientes, esto es, si $\alpha(Z) = \sum_{i=0}^{\infty} a_i Z^i$, entonces $\alpha^\sigma(Z) = \sum_{i=0}^{\infty} a_i^\sigma Z^i = \sum_{i=0}^{\infty} \sigma(a_i) Z^i$.

Entonces, con cálculos directos, se puede demostrar que $(\alpha \circ \beta)^\sigma = \alpha^\sigma \circ \beta^\sigma$.

Aquí, $\circ$ denota la composición de series. Más precisamente, para dos series $\alpha, \beta \in \mathcal{O}_{\bar{T}}[[Z]]$, $\alpha \circ \beta$ denota $(\alpha \circ \beta)(Z) = \alpha(\beta(Z))$.

Demostración. (Teorema 5.8.52). Por el Lema 5.8.51, se tiene que existe $\varepsilon \in U_{\bar{T}}$ tal que $a = \frac{\tau(\varepsilon)}{\varepsilon}$. Sea $\theta_1(Z) := \varepsilon Z$. Supongamos que se ha construido un polinomio $\theta_n(Z)$ de grado n tal que

$$\theta_n^\tau(Z) \equiv \theta_n(a_f(Z)) \text{ mód } \mathrm{gr}(n+1),$$

Se quiere construir un polinomio $\theta_{n+1}(Z) = \theta_n(Z) + bZ^{n+1}$ que satisfaga

$$\theta_{n+1}^\tau(Z) \equiv \theta_{n+1}(a_f(Z)) \text{ mód } \mathrm{gr}(n+2).$$

Sea $b = \gamma\varepsilon^{n+1}$ para algún γ. Si se tiene el polinomio buscado $\theta_{n+1}(Z)$, entonces

$$\begin{aligned}\theta_n^\tau(Z) - \theta_n(a_f(Z)) &= cZ^{n+1} + \text{ términos de grado mayor,}\\ \theta_{n+1}^\tau(Z) - \theta_{n+1}(a_f(Z)) &= \theta_n^\tau(Z) + \tau(b)Z^{n+1} - \theta_n(a_f(Z)) - b(a_f(Z))^{n+1}\\ &\underset{\substack{\uparrow\\ a_f(Z)=aZ+\cdots}}{=} (c + \tau(b) - ba^{n+1})Z^{n+1}\\ &\qquad + \text{ términos de grado mayor}\end{aligned}$$

Puesto que queremos $\theta_{n+1}^\tau(Z) \equiv \theta_{n+1}(a_f(Z)) \mod \operatorname{gr}(n+2)$, se tiene que se debe satisfacer $c + \tau(b) - ba^{n+1} = 0 = c + \tau(\gamma)\tau(\varepsilon)^{n+1} - \gamma\frac{\varepsilon^{n+1}\tau(\varepsilon)^{n+1}}{\varepsilon^{n+1}}$, por lo que se debe tener

$$c + (\tau(\gamma) - \gamma)\tau(\varepsilon)^{n+1} = 0 \quad \text{o, equivalentemente,} \quad \gamma - \tau(\gamma) = c/\tau(\varepsilon)^{n+1}.$$

Tal γ existe como consecuencia del Lema 5.8.51, de donde obtenemos $\theta_{n+1}(Z)$ y la serie $\theta(Z) = \lim_{n\to\infty}\theta_n(Z)$ la cual satisface la condición

$$\theta^\tau(Z) = \theta(a_f(Z)). \tag{5.8.16}$$

Necesitamos modificar $\theta(Z)$ para satisfacer las condiciones (3) y (4) del teorema.

Para una serie $\psi \in \mathcal{O}_{\bar{T}}$, ψ^{-1} denota la serie inversa de ψ: $\psi \circ \psi^{-1} = \psi^{-1} \circ \psi = \mathrm{Id}$, donde $\mathrm{Id}(Z) = Z$, en caso de existir. Si $\psi(Z) = \delta_1 Z + \sum_{i=2}^{\infty}\delta_i Z^i$ con $\delta_i \in \bar{T}$, $\delta_1 \neq 0$, ψ^{-1} se encuentra sustituyendo directamente.

Ahora bien, $\theta(Z) \equiv \varepsilon Z \mod \operatorname{gr} 2$, $\theta(Z) \in \mathcal{O}_{\bar{T}}[[Z]]$ con $\varepsilon \in U_{\bar{T}}$. Entonces $\theta^{-1}(Z) = \sum_{i=1}^{\infty} c_i Z^i$ debe satisfacer

$$\theta(\theta^{-1}(Z)) = \varepsilon\Big(\sum_{i=1}^{\infty} c_i Z^i\Big) + \sum_{j=2}^{\infty} d_j\Big(\sum_{i=1}^{\infty} c_i Z^i\Big)^j = (\varepsilon c_1)Z + (\varepsilon c_2 + d_2 c_1)Z^2 + \cdots$$

la cual se resuelve para las c_i's de manera recursiva. En particular, puesto que $\varepsilon \in U_{\bar{T}}$, $\theta^{-1}(Z) \in \mathcal{O}_{\bar{T}}[[Z]]$.

Consideremos la serie

$$h = \theta^\tau \circ f \circ \theta^{-1} \in \mathcal{O}_{\bar{T}}[[Z]] \tag{5.8.17}$$

en donde $\circ$ significa composición o evaluación, es decir, $g \circ l(Z) = g(l(Z))$.

De la Ecuación (5.8.16) se obtiene $\theta^\tau = \theta \circ a_f$. Por tanto, de la Ecuación (5.8.17) obtenemos

$$h = \theta^\tau \circ f \circ \theta^{-1} = \theta \circ a_f \circ f \circ \theta^{-1}.$$

Del Teorema 5.8.34 (6) se tiene $f(Z) = (\pi)_f(Z)$. Por tanto

$$h = \theta \circ (a)_f \circ (\pi)_f \circ \theta^{-1} \underset{\substack{\uparrow\\ \text{Teorema 5.8.34 (4)}}}{=} \theta \circ (a\pi)_f \circ \theta^{-1} \underset{\substack{\uparrow\\ a\pi=\pi'}}{=} \theta \circ (\pi')_f \circ \theta^{-1}.$$

Se sigue que

$$h^\tau = \theta^\tau \circ (\pi')_f^\tau \circ \theta^{-\tau} \underset{\substack{\uparrow \\ (5.8.17)}}{=} \theta^\tau \circ (\pi')_f^\tau \circ (a)_f^{-1} \circ \theta^{-1}.$$

Puesto que $\tau \in \mathrm{Gal}(T/K)$, se tiene

$$(\pi')_f^\tau = (\pi')_f = (a\pi)_f = (a)_f \circ (\pi)_f \underset{\substack{\uparrow \\ \text{Teorema 5.8.34 (6)}}}{=} (a)_f \circ f.$$

Se sigue que

$$h^\tau = \theta^\tau \circ (\pi')_f \circ (a)_f^{-1} \circ \theta^{-1} = \theta^\tau \circ (a\pi a^{-1})_f \circ \theta^{-1} = \theta^\tau \circ (\pi)_f \circ \theta^{-1},$$

esto es,

$$h^\tau = \theta^\tau \circ f \circ \theta^{-1} = h$$

por lo que $h \in \mathcal{O}_K$ pues cualquier elemento de $\bar{T}$ fijado por τ pertenece a K debido a que $\mathrm{Gal}(T/K) \cong \mathrm{Gal}(\bar{\mathbb{F}}_q/\mathbb{F}_q) = \overline{\langle \tau \rangle}$.

Por otro lado, puesto que $h = \theta \circ \pi'_f \circ \theta^{-1}$ y que $\theta(Z) \equiv \varepsilon Z$ mód gr 2, se obtiene

$$h(Z) = \theta((\pi')_f(\theta^{-1}(Z))) \equiv \varepsilon \pi' \varepsilon^{-1} Z \equiv \pi' Z \text{ mód gr } 2,$$

y

$$h(Z) = \theta^\tau(f(\theta^{-1}(Z))) \underset{\substack{\uparrow \\ (*)}}{\equiv} \theta^\tau(\theta^{-1}(Z)^q) \underset{\substack{\uparrow \\ \tau = q}}{\equiv} \theta^\tau(\theta^{-\tau}(Z^q)) \equiv Z^q \text{ mód } \pi' \text{ y } \pi$$

donde $(*)$: $f(X) \equiv X^q$ mód π, $f(X) \equiv$ módπ', $f(X) = \sum_{i=1}^\infty \alpha_i Z^i$, $\pi | \alpha_i$ para $i \neq q$ y $\pi' = a^{-1}\pi$ por lo que $\pi' | \alpha_i$ para $i \neq q$.

Por tanto $h \in \mathcal{F}_{\pi'}$. Sea $1_{f',h} \colon F_h \longrightarrow F_{f'}$ y consideramos $\theta_1 = 1_{f',h} \circ \theta$. Entonces

$$\theta_1(Z) = (1_{f',h} \circ \theta)(Z) \equiv \theta(Z) \text{ mód gr } 2 \equiv \varepsilon Z \text{ mód gr } 2,$$
$$\theta_1^\tau = 1_{f',h}^\tau \circ (\theta^\tau(Z)) = 1_{f',h}^\tau(\theta(a_f)(Z)) = (1_{f',h} \circ \theta)(a_f(Z)) = \theta_1(a_f(Z)).$$

Se sigue que θ_1 también satisface (1) y (2) del teorema. Ahora, si $h_1 = \theta_1^\tau \circ f \circ \theta_1^{-1} = 1_{f',h} \circ h = f'$, se tiene

$$f' = \theta_1^\tau \circ f \circ \theta_1^{-1} = \theta_1 \circ \pi'_f \circ \theta^{-1}.$$

Para probar que $\theta_1(F_f(X,Y)) = F_{f'}(\theta(X), \theta(Y))$ basta probar que la serie $F(X,Y) := \theta_1(F_f(\theta_1^{-1}(X), \theta_1^{-1}(Y)))$ satisface la caracterización de $F_{f'}$, esto es:

$$F(X,Y) \equiv X + Y \text{ mód gr } 2 \quad \text{y}$$
$$f'(F(X,Y)) = F(f'(X), f'(Y)).$$

Se tiene que

$$\begin{aligned}
F(X,Y) &= \theta_1(F_f(\theta^{-1}(X),\theta_1^{-1}(Y))) \equiv \varepsilon F_f(\theta_1^{-1}(X),\theta_1^{-1}(Y)) \\
&\equiv \varepsilon(\theta_1^{-1}(X)+\theta_1^{-1}(Y)) \equiv \varepsilon(\varepsilon^{-1}X+\varepsilon^{-1}Y) \\
&\equiv X+Y \text{ mód gr } 2, \\
F(f'(X),f'(Y)) &= \theta_1(F_f(\theta_1^{-1}(f'(X)),\theta_1^{-1}(f'(Y)))) \underset{\substack{\uparrow \\ f'=\theta_1\circ\pi'_f\circ\theta_1^{-1} \\ \theta_1^{-1}\circ f'=\pi'_f\circ\theta_1^{-1}}}{=} \\
&= \theta_1(F_f(\pi'_f(\theta_1^{-1}(X)),\pi'_f(\theta_1^{-1}(Y)))) \\
&= \theta_1(\pi'_f(F_f(\theta_1^{-1}(X),\theta_1^{-1}(Y)))) \underset{\substack{\uparrow \\ \theta_1\circ\pi'_f=f'\circ\theta_1}}{=} \\
&= f'\theta_1(F_f(\theta_1^{-1}(X),\theta_1^{-1}(Y))) = (f'\theta_1 F_f\theta^{-1})(X,Y) \\
&= f'F(X,Y),
\end{aligned}$$

por lo tanto $F = F_{f'}$.

Para probar (4) se necesita $\theta_1 b_f = b_{f'}\theta_1$, $b \in \mathcal{O}_K$.

Sea $H = \theta_1 b_f \theta_1^{-1}$. Se quiere probar que $H = b_{f'}$ y para ello es suficiente probar que H satisface la caracterización de $b_{f'}$, esto es:

$$H(X) \equiv bX \text{ mód gr } 2 \quad \text{y} \quad f(H(X)) = H(f'(X)).$$

Ahora

$$\begin{aligned}
H(X) &= \theta_1 b_f \theta_1^{-1}(X) \equiv (\theta_1 b\theta_1^{-1})(X) \equiv \varepsilon b\varepsilon^{-1}X \equiv bX \text{ mód gr } 2 \\
H(f'(X)) &= \theta_1 b_f \theta_1^{-1} f'(X) \underset{\substack{\uparrow \\ f'=\theta_1\pi'_f\theta_1^{-1}}}{=} \theta_1 b_f \theta_1^{-1}\cdot\theta_1\pi'_f\theta_1^{-1}(X) \\
&= (\theta_1 b_f \pi'_f \theta_1^{-1})(X) = \theta_1((b\pi')_f\theta_1^{-1})(X) = (\theta_1\pi'_f b_f\theta_1^{-1})(X) \\
&= \theta_1\pi'_f\theta_1^{-1}\theta_1 b_f\theta_1^{-1}(X) \underset{\substack{\uparrow \\ \theta_1\pi'_f\theta_1^{-1}=f'}}{=} f'(H(X)).
\end{aligned}$$

Por tanto $H = b_{f'}$ y se tiene (4). □

La importancia del Teorema 5.8.52 es el siguiente teorema.

Teorema 5.8.53. *Sean π y $\pi' = a\pi$ dos elementos primos en K, $a \in U_K$ y sean $f \in \mathcal{F}_\pi$, $f' \in \mathcal{F}_{\pi'}$. Entonces el mapeo $\lambda \longmapsto \theta(\lambda)$ da lugar a un isomorfismo de $\mathcal{O}_K$–módulos*

$$\Lambda_{f,n} \cong \Lambda_{f',n}$$

para toda $n \in \mathbb{N}$.

Por el Teorema 5.8.40 ya sabíamos que

$$\Lambda_{f,n} \cong \mathcal{O}_K/\pi^n\mathcal{O}_K = \mathcal{O}_K/(\pi')^n\mathcal{O}_K \cong \Lambda_{f',n}.$$

La afirmación del teorema es que el mapeo dado por θ es un isomorfismo.

Demostración. Si $\lambda \in \Lambda_{f,n}$, entonces

$$(f')^{(n)}(\theta(\lambda)) = (\pi')_f^{(n)}(\theta(\lambda)) = \theta((a^n\pi^n)_f)(\lambda) = \theta(a^n f^{(n)}(\lambda)) = \theta(0) = 0,$$

por tanto $\lambda \in \Lambda_{f',n}$. Se sigue que $\lambda \longmapsto \theta(\lambda)$ manda $\Lambda_{f,n}$ en $\Lambda_{f',n}$.

Por (3) y (4) del Teorema 5.8.52, se tiene

$$\theta(\lambda \oplus_{F_f} \mu) = \theta(F_f(\lambda,\mu)) = F_{f'}(\theta(\lambda),\theta(\mu)) = \theta(\lambda) \oplus_{F_{f'}} \theta(\mu),$$
$$\theta(a \odot_{F_f} \lambda) = \theta(a_f(\lambda)) = a_{f'}\theta(\lambda) = a \odot_{F_{f'}} \theta(\lambda).$$

Por tanto θ es un homomorfismo de $\mathcal{O}_K$–módulos de $\Lambda_{f,n}$ en $\Lambda_{f',n}$.

Veamos que θ es 1–1. Sea $\theta(\lambda) = 0$, $\lambda \in \Lambda_{f,n}$. Ahora

$$\theta(\lambda) = \varepsilon\lambda + \sum_{i=0}^{\infty} \alpha_i \lambda^i = 0.$$

Si $\lambda \neq 0$ esto implicaría que $0 = \varepsilon + \lambda\big(\sum_{i=2}^{\infty} \alpha_i \lambda^{i-2}\big)$ lo cual implicaría que $\theta(\varepsilon) = 0 = \theta(\lambda)\theta\big(-\sum_{i=2}^{\infty} \alpha_i \lambda^{i-2}\big)$.

Lo anterior no es posible pues ε es una unidad y θ es una serie invertible.

Puesto que $\Lambda_{f,n} \cong \mathcal{O}_K/\pi^n\mathcal{O}_K \cong \mathcal{O}_K/(\pi')^n\mathcal{O}_K \cong \Lambda_{f',n}$ tienen la misma cardinalidad, θ es suprayectiva y por tanto θ es un isomorfismo. □

Observación 5.8.54. Para dos elementos primos π y π' de K, los campos $L_{\pi,n}$ y $L_{\pi',n}$ pueden ser diferentes. Sin embargo, se tiene que $TL_{\pi,n} = TL_{\pi',n}$. Esto es el contenido de la Proposición 5.8.56.

Primero probamos el siguiente lema.

Lema 5.8.55. *Sea $K \subseteq F \subseteq K^{\text{sep}}$, K^{sep} una cerradura separable de K. Entonces F es un conjunto cerrado en K^{sep}.*

Demostración. Sea $H := \text{Gal}(K^{\text{sep}}/F)$. Entonces H fija a todo elemento de F y por tanto fija a todo elemento de la cerradura $\bar{F}$ de F en K^{sep} por continuidad. Por tanto

$$F \subseteq \bar{F} \subseteq (K^{\text{sep}})^H = F.$$ □

Proposición 5.8.56. *Si π y π' son dos elementos primos de K y T es la máxima extensión abeliana no ramificada de K, entonces*

$$TL_{\pi,n} = TL_{\pi',n}.$$

Demostración. Por el Teorema 5.8.53 se tiene que si $\lambda \in \Lambda_{f,n}$, entonces $\theta(\lambda) = \varepsilon\lambda + \sum_{i=2}^{\infty} \alpha_i \lambda^i \in \bar{T}(\lambda)$. Por lo tanto

$$\bar{T}(\Lambda_{f',n}) = \bar{T}(\theta(\Lambda_{f,n})) \subseteq \bar{T}(\Lambda_{f,n}) = \bar{T}(\theta^{-1}(\Lambda_{f',n})) \subseteq \bar{T}(\Lambda_{f',n}).$$

Por lo tanto $\overline{TL}_{\pi,n} = \overline{TL}_{\pi',n}$.

Por el Lema 5.8.55, se sigue que $T(\Lambda_{\pi,n}) = T(\Lambda_{\pi',n})$, de donde obtenemos que $TL_{\pi,n} = TL_{\pi',n}$. □

Por otro lado, puesto que T/K es no ramificada y $L_{\pi,n}/K$ es totalmente ramificada, T y $L_{\pi,n}$ son linealmente disjuntos sobre K y

$$\begin{aligned} \mathrm{Gal}(TL_{\pi,n}/K) &\cong \mathrm{Gal}(T/K) \times \mathrm{Gal}(L_{\pi,n}/K) = \mathrm{Gal}(T/K) \times G_{\pi,n} \\ &\cong \mathrm{Gal}(\mathbb{F}_q^{\mathrm{ab}}/\mathbb{F}_q) \times G_{\pi,n} \cong \hat{\mathbb{Z}} \times (U_K/U_K^{(n)}). \end{aligned} \tag{5.8.18}$$

Sea $\rho_\pi \colon K^* \longrightarrow \mathrm{Gal}(TL_{\pi,n}/K)$ el siguiente homomorfismo. Para $a = u\pi^m \in K^*$ con $u \in U_K$, $m \in \mathbb{Z}$. Entonces

$$\begin{aligned} \rho_\pi(a)|_T &:= \tau_K^m \in \mathrm{Gal}(T/K), \quad \tau_K \text{ el automorfismo de Frobenius,} \\ \rho_\pi(a)|_{L_{\pi,n}} &:= \sigma_u \in G_{\pi,n}, \end{aligned}$$

donde σ_u es el automorfismo de $L_{\pi,n}$ que bajo el isomorfismo $G_{\pi,n} \cong U_K/U_K^{(n)}$, σ_u corresponde a la clase $u^{-1}U_K^{(n)}$. En otras palabras $\rho_\pi(a)|_{L_{\pi,n}}$ está determinado por

$$\rho_\pi(a)(\lambda) = (u^{-1})_f(\lambda) = u^{-1} \odot_{F_f} \lambda, \quad \lambda \in \Lambda_{f,n}.$$

El objetivo central de los grupos formales para nosotros, es probar que ρ_π es precisamente el símbolo residual de la norma $(\_, K)$, esto es, ρ_π es el mapeo de reciprocidad.

Teorema 5.8.57. *Para $a \in K^*$ se tiene*

$$\rho_\pi(a) = (a, K)|_{TL_{\pi,n}} = \rho_K|_{TL_{\pi,n}}(a).$$

Demostración. Se tiene que los elementos primos de K^* generan K^*, por lo que basta probar el teorema para elementos primos. Sea $a = \pi$ un elemento primo de K. Entonces

$$\rho_\pi(\pi)|_T = \tau = (\pi, T/K) = (\pi, K)|_T$$

como consecuencia del Teorema 5.2.2 pues T/K es no ramificada.

Ahora, por el Corolario 5.8.47, π es una norma de $L_{\pi,n}$ a K. Por el Teorema 5.3.17, $(\pi, L_{\pi,n}/K) = (\pi, K)|_{L_{\pi,n}} = 1$. Se tiene $\pi = 1 \cdot \pi$, por lo que

$$\rho_\pi(\pi)|_{L_{\pi,n}} = \sigma_1 = \mathrm{Id}_{L_{\pi,n}} = (\pi, K)|_{L_{\pi,n}} = 1.$$

Se sigue que $\rho_\pi(\pi) = (\pi, K)|_{TL_{\pi,n}}$.

Ahora sea $\pi' = u\pi$ con $u \in U_K$ otro elemento primo de K. Se tiene $TL_{\pi,n} = TL_{\pi',n}$ y por el Teorema 5.2.2

$$\rho_\pi(\pi')|_T = \tau = (\pi', T/K) = (\pi', K)|_T.$$

Puesto que π' es una norma de $L_{\pi',n}$ a K, se tiene que $(\pi', K)|_{L_{\pi',n}} = (\pi', L_{\pi',n}/K) = \mathrm{Id}_{L_{\pi',n}}$. Así debemos verificar que $\rho_\pi(\pi')|_{L_{\pi',n}} = \mathrm{Id}_{L_{\pi',n}}$. Esto equivale a ver que $\rho_\pi(\pi')(\mu) = \mu$ para toda $\mu \in \Lambda_{f',n}$ con $f' \in \mathcal{F}_{\pi'}$.

Sabemos del Teorema 5.8.53 que $\Lambda_{f',n} = \theta(\Lambda_{f,n})$. Por tanto debemos probar que $\rho_\pi(\pi')(\theta(\lambda)) = \theta(\lambda)$ para toda $\lambda \in \Lambda_{f,n}$.

Se tiene que $\rho_\pi(\pi') = \rho_\pi(u\pi) = \rho_\pi(u) \circ \rho_u(\pi)$. Para $\lambda \in \Lambda_{f,n}$, $\rho_\pi(\pi)(\lambda) = \lambda$, $\rho_\pi(\pi)|_T = \tau$, $\rho_\pi(u)|_T = \mathrm{Id}_T$.

Extendemos $\rho_\pi(\pi)|_T$ y $\rho_\pi(u)|_T$ continuamente a $\bar{T}$ y usando el Teorema 5.8.52

$$\begin{aligned}\rho_\pi(\pi')(\theta(\lambda)) &= (\rho_\pi(u) \circ \rho_\pi(\pi))(\theta(\lambda)) = \rho_\pi(u)(\rho_\pi(\pi)(\theta(\lambda))) \\ &= \rho_\pi(u)(\theta^\tau(\lambda)) = (\rho_\pi(u) \circ \theta^\tau)(\lambda) = \theta^\tau(\rho_\pi(u))(\lambda) \\ &= \theta^\tau((u^{-1})_f(\lambda)) = \theta((u)_f(u^{-1})_f(\lambda)) = \theta(\lambda). \qquad \square\end{aligned}$$

De esta forma se puede describir el símbolo de la norma residual $(\_, L_{\pi,n}/K)$ de la extensión abeliana y totalmente ramificada $L_{\pi,n}$:

Teorema 5.8.58. *Sea $a = u\pi^m \in K^*$, $u \in U_K$ y $m \in \mathbb{Z}$. Entonces*

$$(a, L_{\pi,n}/K)(\lambda) = (u^{-1})_f(\lambda) \quad \textit{para toda } \lambda \in \Lambda_{f,n} \subseteq L_{\pi,n}.$$

El grupo de normas de la extensión $L_{\pi,n}/K$ es el grupo $(\pi) \times U_K^{(n)}$.

Demostración. Se tiene del Teorema 5.8.57 que $(a, L_{\pi,n}/K)(\lambda) = \rho_\pi(a)(\lambda)$. Por tanto $(a, K)(\lambda) = (a, L_{\pi,n}/K)(\lambda) = \rho_\pi(a)(\lambda) = (u^{-1})_f(\lambda)$.

En consecuencia, $a \in \mathrm{N}_{L_{\pi,n}/K}(L_{\pi,n}^*) \iff (a, L_{\pi,n}/K)(\lambda) = (u^{-1})_f(\lambda) = \lambda$ para toda $\lambda \in \Lambda_{f,n}$. Por el Teorema 5.8.41, $(u^{-1})_f = \mathrm{Id} \iff u^{-1} \in U_K^{(n)} \iff u \in U_K^{(n)} \iff a \in (\pi) \times U_K^{(n)}$. $\square$

El siguiente ejemplo es el origen del uso de los grupos formales en teoría local de campos locales.

Ejemplo 5.8.59 (Ver el Ejemplo 5.8.38). Sea $K = \mathbb{Q}_p$ el campo de los números p–ádicos. Entonces p es un elemento primo en K. Sea $f \in \mathcal{F}_p$ definido por

$$f(Z) = (1+Z)^p - 1 = pZ + \binom{p}{2}Z^2 + \binom{p}{3}Z^3 + \cdots + pZ^{p-1} + Z^p.$$

En nuestro caso, $q = p$. Se tiene

$$f^{(2)}(Z) = f(f(Z)) = (1+f(Z))^p - 1 = (1+(1+Z)^p - 1)^p - 1 = (1+Z)^{p^2} - 1$$

y en general $f^{(n)}(Z) = (1+Z)^{p^n} - 1$. El conjunto de ceros de $f^{(n)}(Z)$ son $\{\lambda = \xi - 1 \mid \xi \text{ es } p^n\text{–raíz de } 1\}$. Por tanto $L_{p,n} = \mathbb{Q}_p(\zeta_{p^n})$, es decir, $\lambda = \zeta_{p^n}^j - 1$, $0 \leq j \leq p^n - 1$.

Sea $a = up^m \in \mathbb{Q}_p^*$, u una unidad y ζ_{p^n} una p^n–raíz primitiva de la unidad. Entonces

$$(a, \mathbb{Q}_p(\zeta_{p^n})/\mathbb{Q}_p)(\zeta_{p^n}) = \zeta_{p^n}^r$$

donde $r \in \mathbb{N}$ tal que $r \equiv u^{-1} \mod p^n$.

En efecto, si $\lambda = \zeta_{p^n} - 1 \in \Lambda_{f,n}$, se tiene que $ru \equiv 1 \mod p^n$ y por los Teoremas 5.8.58 y 5.8.41 se tiene

$$(a, \mathbb{Q}_p(\zeta_{p^n})/\mathbb{Q}_p)(\lambda) = (u^{-1})_f(\lambda) = r_f(\lambda).$$

Por otro lado si $g(Z) = (1+Z)^r - 1$ se tiene

$$\begin{aligned} g(Z) &= (1+Z)^r - 1 = rZ + \cdots + Z^r \equiv rZ \mod \operatorname{gr} 2 \quad \text{y} \\ f(g(Z)) &= f((1+Z)^r - 1) = ((1+Z)^r)^p - 1 = (1+Z)^{rp} - 1 \\ &= (1+Z)^{pr} - 1 = ((1+Z)^p)^r - 1 = g((1+Z)^p - 1) = g(f(Z)). \end{aligned}$$

Por tanto $g(Z)$ satisface las condiciones que definen $r_f(Z)$, esto es $r_f(Z) = (1+Z)^r - 1$.

Se sigue que

$$\begin{aligned} (a, \mathbb{Q}_p(\zeta_{p^n})/\mathbb{Q}_p)(\zeta_{p^n}) &= (a, \mathbb{Q}_p(\zeta_{p^n})/\mathbb{Q}_p)(\lambda + 1) = r_f(\lambda) + 1 \\ &= r_f(\zeta_{p^n} - 1) + 1 = (\zeta_{p^n} - 1 + 1)^r - 1 + 1 = \zeta_{p^n}^r. \end{aligned}$$

Por ser el origen de lo presentado en esta sección, enunciamos el Ejemplo 5.8.59 como un teorema.

Teorema 5.8.60. *Sean $K = \mathbb{Q}_p$, $a = up^m \in \mathbb{Q}_p^*$ con u una unidad, ζ_{p^n} una raíz p^n–primitiva de 1. Entonces el símbolo de la norma residual de $\mathbb{Q}_p(\zeta_{p^n})/\mathbb{Q}_p$ está dado por*

$$(a, \mathbb{Q}_p(\zeta_{p^n})/\mathbb{Q}_p)(\zeta_{p^n}) = \zeta_{p^n}^r$$

donde $r \equiv u^{-1} \mod p^n$, $r \in \mathbb{N}$. □

Observación 5.8.61. Usando el teorema de existencia podemos dar otra demostración del Teorema 5.7.15. Sea $H = \mathrm{N}_{L/K} L^*$. Por el teorema de existencia, existe una extensión abeliana finita M/K tal que $\mathrm{N}_{M/K} M^* = H$. Por el Teorema 5.7.13, el grupo de normas correspondiente a la extensión abeliana LM/L es $\mathrm{N}_{L/K}^{-1} H = \mathrm{N}_{L/K}^{-1} \mathrm{N}_{L/K} L^* = L^*$. Por tanto $\mathrm{N}_{LM/L}(LM)^* = L^* = \mathrm{N}_{L/L} L^*$ de donde se sigue que $LM = L$ lo cual equivale a que $M \subseteq L$. Finalmente si N/K es abeliana y $K \subseteq M \subseteq N \subseteq L$, entonces $H = \mathrm{N}_{L/K} L^* \subseteq \mathrm{N}_{N/K} N^* \subseteq \mathrm{N}_{M/K} M^* = H$, de donde se sique que $N = M$ y por tanto M es la máxima extensión abeliana de K contenida en L.

Para finalizar la teoría local de campos de clase, únicamente resta probar que todo subgrupo abierto de índice finito en K^* es un subgrupo de normas.

El Teorema 5.2.3 prueba que los grupos de las extensiones no ramificadas son $(\pi^f) \times U_K$. Para las extensiones abelianas totalmente ramificadas se tiene

Teorema 5.8.62. *Los grupos de normas de las extensiones abelianas finitas L/K totalmente ramificadas son exactamente los grupos que contienen a algún grupo*

$$(\pi) \times U_K^{(n)}$$

con π un elemento primo de K y $n \in \mathbb{N} \cup \{0\}$.

Demostración. Como el grupo de normas de $L_{\pi,n}$ es $(\pi) \times U_K^{(n)}$, un subgrupo que contiene a $(\pi) \times U_K^{(n)}$ corresponde a un subcampo L con $K \subseteq L \subseteq L_{\pi,n}$ y por tanto L/K es abeliana y totalmente ramificada.

Ahora sea L/K totalmente ramificada. Entonces $L = K(\lambda)$ con λ una raíz de un polinomio Eisenstein

$$X^e + \cdots + \pi = 0,$$

donde π es un elemento primo de K el cual es la norma del elemento $\pm\lambda$. Se sigue que $(\pi) \subseteq \mathrm{N}_{L/K} L^*$. Ahora bien, puesto que $\mathrm{N}_{L/K}(L^*)$ es un subgrupo abierto en K^*, existe $n \in \mathbb{N} \cup \{0\}$ tal que $U_K^{(n)} \subseteq \mathrm{N}_{L/K} L^*$. Se sigue que $(\pi) \times U_K^{(n)} \subseteq \mathrm{N}_{L/K} L^*$. □

Corolario 5.8.63. *Si L/K es una extensión abeliana finita totalmente ramificada, entonces L/K está contenida en algún $L_{\pi,n}$.* □

Teorema 5.8.64. *El grupo $(\pi^f) \times U_K^{(n)}$ es el grupo de normas del campo $K_f L_{\pi,n}$ donde K_f/K es la extensión no ramificada de K de grado f.*

Demostración. Se tiene

$$\begin{aligned}(\pi^f) \times U_K^{(n)} &= ((\pi^f) \times U_K) \cap ((\pi) \times U_K^{(n)}) = (\mathrm{N}_{K_f/K} K_f^*) \cap (\mathrm{N}_{L_{\pi,n}/K} L_{\pi,n}^*) \\ &= \mathrm{N}_{K_f L_{\pi,n}/K}(K_f L_{\pi,n})^*\end{aligned}$$

por los Teorema 5.2.3 y 5.7.14. □

Teorema 5.8.65. *Los grupos de normas de K^* son precisamente los grupos conteniendo a algún $(\pi^f) \times U_K^{(n)}$ con $n = 0, 1, 2, \ldots, f = 1, 2, \ldots$, donde π es un elemento primo de K.*

Demostración. Cada grupo $(\pi^f) \times U_K^{(n)}$ tiene índice finito en $K^* = (\pi) \times U_K$ pues

$$\frac{K^*}{(\pi^f) \times U_K^{(n)}} \cong \frac{(\pi) \times U_K}{(\pi^f) \times U_K^{(n)}} \cong \frac{(\pi)}{(\pi^f)} \times \frac{U_K}{U_K^{(n)}}$$

el cual es cardinalidad $f \cdot q \cdot (q^{n-1}-1)$. Además $(\pi^f) \times U_K^{(n)}$ es un grupo abierto en K^*. Por otro lado, por el Teorema 5.8.64, $(\pi^f) \times U_K^{(n)}$ es un grupo de normas.

Por tanto, si H es un subgrupo que contiene a uno de estos grupos, H es un grupo de normas (ver la demostración del Teorema 5.7.14).

Recíprocamente, si H es un grupo de normas, entonces H es un subgrupo abierto de K^* de índice finito. Entonces $1 \in H$ y $\{U_K^{(n)}\}_{n=0}^{\infty}$ es un sistema fundamental de vecindades de 1, existe $n \in \mathbb{N} \cup \{0\}$ con $U_K^{(n)} \subseteq H$. Finalmente, al ser H de índice finito en K^*, existe f tal que $\pi^f \in H$. Se sigue que $(\pi^f) \times U_K^{(n)} \subseteq H$. □

Corolario 5.8.66. *Se tiene que*

$$D_K := \bigcap_{\substack{L/K \\ \textit{finita y abeliana}}} \mathrm{N}_{L/K}\, L^* = \{1\}$$

y $\rho_K \colon K^* \longrightarrow G_K^{\mathrm{ab}}$ *es un monomorfismo.*

Demostración. Se tiene $\{1\} \subseteq D_K \subseteq \bigcap_{f,n} \left(\langle \pi_K^f \rangle \times U_K^{(n)}\right) = \{1\}$. □

Teorema 5.8.67. *Sea T la máxima extensión no ramificada de K. Sean π un elemento primo de K, $f \in \mathcal{F}_\pi$, $\Lambda_f = \bigcup_{n=1}^{\infty} \Lambda_{f,n}$, $L_\pi = \bigcup_{n=1}^{\infty} L_{\pi,n} = K(\Lambda_f)$ y $G_\pi = \mathrm{Gal}(L_\pi/K)$. Entonces el campo TL_π es independiente de π y es la máxima extensión abeliana de K, $K^{\mathrm{ab}} = TL_\pi$. En particular*

$$G_K^{\mathrm{ab}} = \mathrm{Gal}(K^{\mathrm{ab}}/K) = G_{T/K} \times G_\pi \cong \hat{\mathbb{Z}} \times U_K.$$

Si $a = u\pi^m \in K^*$ con $u \in U_K$, entonces el símbolo de la norma residual $(a, K_=\rho_K(a)$ está dado por

$$(a,K)|_T = \tau^m, \quad (a,K)(\lambda) = (u^{-1})_f(\lambda) \quad \textit{para } \lambda \in \Lambda_f.$$

Demostración. Por el Teorema 5.8.65 los grupos de normas son los grupos conteniendo a algún $(\pi^f) \times U_K^{(n)}$, el cual es, por el Teorema 5.8.64, el grupo de normas de $L_{\pi,n}K_f$.

Así, si L/K es una extensión abeliana finita, existen $n \in \mathbb{N} \cup \{0\}$, $f \in \mathbb{N}$ tales que $(\pi^f) \times U_K^{(n)} \subseteq \mathrm{N}_{L/K}\, L^*$ lo cual implica que $L^* \subseteq L_{\pi,n}K_f$ con $K_f \subseteq T$. Se sigue que $L^* \subseteq L_\pi T$ y $L_\pi T$ es la máxima extensión abeliana de K.

Puesto que $G_K^{\mathrm{ab}} = G_{T/K} \times G_\pi$, el símbolo de la norma residual está determinad por

$$(a,K)|_T = \tau^m \quad \text{y} \quad (a,K)(\lambda) = (u^{-1})_f(\lambda) \quad \text{para } \lambda \in \Lambda_f.$$

Finalmente, por el Teorema 5.8.50 tenemos que $G_\pi \cong U_K$. □

Corolario 5.8.68 (Teorema de Kronecker–Weber local). *La máxima extensión abeliana de $\mathbb{Q}_p$ es*

$$\mathbb{Q}_p^{\mathrm{ab}} = \bigcup_{n=1}^{\infty} \mathbb{Q}_p(\zeta_n) = \mathbb{Q}_p(\zeta_\infty).$$

Demostración. Las extensiones abelianas no ramificadas de $\mathbb{Q}_p$ corresponden a las extensiones finitas de $\mathbb{F}_p$ y estas con $\mathbb{F}_p(\zeta_n)$ con $\mathrm{mcd}(n,p)=1$. Esto es

$$T = \bigcup_{\substack{n=1 \\ \mathrm{mcd}(n,p)=1}}^{\infty} \mathbb{Q}_p(\zeta_n).$$

Por ora lado $L_{p,n} = \mathbb{Q}(\zeta_{p^n})$ por lo cual $L_\pi = \bigcup_{n=1}^{\infty} \mathbb{Q}_p(\zeta_{p^n}) = \mathbb{Q}_p(\zeta_{p^\infty})$ de donde se sigue el resultado. □

Teorema 5.8.69 (Teorema de Existencia). *Sea K un campo local. Entonces la correspondencia $L \longrightarrow H_L := \mathrm{N}_{L/K} L^* \subseteq K^*$ nos da un isomorfismo de redes que cambia contenciones entre la red de extensiones abelianas finitas L/K y la red de subgrupos abiertos de índice finito de K^*. Todo subgrupo que contenga a un grupo de normas es a su vez un grupo de normas.*

En particular, si K es un campo local, entonces las siguientes condiciones sobre un subgrupo H de K^*, son equivalentes:

(1) *H es abierto y de índice finito en K^*.*
(2) *H es un grupo de normas.*
(3) *H contiene a algún grupo $\langle \pi_K^f \rangle \times U_K^{(n)}$ para algunos $f \in \mathbb{N}$ y $n \in \mathbb{N} \cup \{0\}$.*

Observación 5.8.70. El Teorema 5.8.69 es de existencia pues dado una subgrupo abierto de índice finito V de K^*, existe una única extensión abeliana finita L/K tal que $K^*/\mathrm{N}_{L/K} L^* \xrightarrow[(\_,L/K)]{\cong} \mathrm{Gal}(L/K)$, esto es, $\mathrm{N}_{L/K} L^* = V$.

Demostración. (Teorema 5.8.69). Teoremas 5.7.14, 5.8.64 y 5.8.65. □

Observación 5.8.71. Para otra demostración del Teorema de Existencia en característica 0 se puede consultar Teorema 5.7.7, [119, Theorem 3.1, Ch. III Section 3, página 43]; [117, Theorem 6.2, Ch. II, Section 6, página]. Para característica $p > 0$, se puede consultar [151, Ch. XIV, Section 6, página 218].

Observación 5.8.72. Notemos que L/K es no ramificada $\iff$ $U_K \subseteq \mathrm{N}_{L|K} L^*$. En efecto, si L/K es no ramificada, entonces $\mathrm{N}_{L/K} L^* = \langle \pi_K^f \rangle \times U_K$ con $f = [L : K]$. Recíprocamente, si $U_K \subseteq \mathrm{N}_{L/K} L^*$ y si $f = [K^* : \mathrm{N}_{L/K} L^*]$, entonces $\pi_K^f \in \mathrm{N}_{L/K} L^*$ y por tanto $\langle \pi_K^f \rangle \times U_K \subseteq \mathrm{N}_{L/K} L^*$. Por tanto L está contenida en la extensión no ramificada de K de grado f (y de hecho, es igual).

5.8.2. Grupos de ramificación, grupos de descomposición y grupos formales

Todos los resultados presentados aquí sin demostración, así como la teoría general de grupos de ramificación pueden ser consultados en [151, Ch. IV].

En esta parte desarrollamos lo expuesto en la Subsección 5.8. Sea L/K una extensión finita de Galois con grupo $G = \mathrm{Gal}(L/K)$. Recordemos que $\varphi\colon [-1,\infty) \longrightarrow [-1,\infty)$ dada por $\varphi(u) = \int_0^u \frac{dt}{[G:G_t]}$ donde $G_t := G_{\lceil t \rceil}$ es una función biyectiva y sea η la función inversa. Entonces se define para $v \in [-1,\infty)$

$$G^v := G_{\eta(v)} \quad \text{o} \quad G^{\varphi(u)} := G_u.$$

Proposición 5.8.73. *Sea K un campo local y sea $L_{\pi,n} = K(\Lambda_{f,n})$ el campo de los puntos de π^n–división de un módulo de Lubin–Tate para π. Entonces*

$$G_i(L_{\pi,n}/K) = \mathrm{Gal}(L_{\pi,n}/L_{\pi,m}) \quad \textit{para } q^{m-1} \leq i \leq q^m - 1.$$

Demostración. Se tiene que el símbolo de la norma residual proporciona un isomorfismo $U_K/U_K^{(n)} \longrightarrow \mathrm{Gal}(L_{\pi,n}/K)$ (Teorema 5.8.45). Por tanto se tiene

$$\mathrm{Gal}(L_{\pi,n}/L_{\pi,m}) \cong \frac{\mathrm{Gal}(L_{\pi,n}/K)}{\mathrm{Gal}(L_{\pi,m}/K)} \cong \frac{U_K/U_K^{(n)}}{U_K/U_K^{(m)}} \cong \frac{U_K^{(m)}}{U_K^{(n)}},$$

y por tanto

$$\mathrm{Gal}(L_{\pi,n}/L_{\pi,m}) = (U_K^{(m)}, L_{\pi,n}/K).$$

Lo que se quiere probar es que para $q^{m-1} \leq i \leq q^m - 1$, $G_i(L_{\pi,n}/K) = (U_K^{(m)}, L_{\pi,n}/K)$.

Sea $\sigma \in G_1(L_{\pi,n}/K)$ y sea $\sigma = (u^{-1}, L_{\pi,n}/K)$ para algún u. El mapeo $(\_, L_{\pi,n}/K)\colon U_K/U_K^{(n)} \xrightarrow{\cong} \mathrm{Gal}(L_{\pi,n}/K)$ manda el p–subgrupo de Sylow $U_K^{(1)}/U_K^{(n)}$ de $U_K/U_K^{(n)}$ (recordemos que $\left|U_K/U_K^{(n)}\right| = q^{n-1}(q-1)$ y $\left|U_K^{(1)}/U_K^{(n)}\right| = q^{n-1}$) sobre el p–subgrupo de Sylow de $\mathrm{Gal}(L_{\pi,n}/K)$, el cual es $G_1(L_{\pi,n}/K)$. En particular $u \in U_K^{(1)}$.

Escribamos $u = 1 + \varepsilon\pi^l$ con $\varepsilon \in U_K$ y $l \geq 1$. Sea $\lambda \in \Lambda_{f,n}$ un generador como $\mathcal{O}_K$–módulos, esto es, $\lambda \in \Lambda_{f,n} \setminus \Lambda_{f,n-1}$. Entonces

$$\begin{aligned}\lambda^\sigma = (u^{-1}, L_{\pi,n}/K)(\lambda) &\underset{\substack{\uparrow \\ \text{Teorema 5.8.67}}}{=} (u)_f(\lambda) = (1 \oplus_{F_f} \varepsilon\pi^l)_f(\lambda) \\ &= 1 = F_f(\lambda, [\varepsilon\pi^l]_f(\lambda)).\end{aligned}$$

Si $l \geq n$, $\sigma = 1$ por lo que $\lambda^\sigma - \lambda = 0$ y $v_{L_{\pi,n}}(\lambda) = \infty$. Si $l < n$ entonces $\lambda_{n-l} := (\pi^m)_f(\lambda)$ es un elemento primo $L_{\pi,n-l}$.

Se tiene $(\varepsilon\pi^l)_f(\lambda) = (\varepsilon)_f(\pi^l)_f(\lambda) = (\varepsilon)_f(\lambda_{n-l})$.

Puesto que $L_{\pi,n}/L_{\pi,n-l}$ es totalmente ramificada de grado q^l, se tiene que $v_{L_{\pi,n}}(\lambda^{q^l}) = q^l v_{L_{\pi,n}}(\lambda) = q^l \cdot 1 = q^l$ y $v_{L_{\pi,n}}(\lambda_{n-l}) = e(L_n/L_{n-l}) v_{L_{\pi,n}}(\lambda_{n-l}) = q^l \cdot 1 = q^l$, por tanto existe $\varepsilon_0 \in U_{L_n}$ tal que

$$[\varepsilon]_{F_f}(\lambda_{n-l}) = [\varepsilon\pi^l]_{F_f}(\lambda) = \varepsilon_0 \lambda^{q^l}.$$

De las identidades $F_f(X,0) = X$, $F_f(0,Y) = Y$ (ver después de la Definición 5.8.25), se obtiene que

$$F_f(X,Y) = X + Y + XYG(X,Y) \quad \text{con } G(X,Y) \in \mathcal{O})K[[X,Y]].$$

De esta forma obtenemos

$$\lambda^\sigma - \lambda = F_f(\lambda, \varepsilon_0 \lambda^{q^l}) - \lambda = \varepsilon_0 \lambda^{q^l} + a\lambda^{q^l+1} \quad \text{con } a \in \mathcal{O}_{L_{\pi,n}}.$$

Por lo tanto

$$\imath_{L_{\pi,n}/K}(\sigma) = v_{L_{\pi,n}}(\lambda^\sigma - \lambda) = \begin{cases} q^l & \text{si } l < n \\ \infty & \text{si } l \geq n. \end{cases}$$

Consideremos $q^{m-1} \leq i \leq q^m - 1$ y $u \in U_K^{(m)}$. Entonces $l \geq m$, esto es, $\imath_{L_{\pi,n}/K}(\sigma) \geq q^l \geq i+1$ y de esta forma $\sigma \in G_i(L_{\pi,n}/K)$.

Esto demuestra que $(U_K^{(m)}, L_{\pi,n}/K) \subseteq G_i(L_{\pi,n}/K)$.

Recíprocamente, si $\sigma \in G_i(L_{\pi,n}/K)$ y $\sigma \neq \mathrm{Id}$, entonces $\imath_{L_{\pi,n}/K}(\sigma) = q^m > i \geq q^{m-1}$, esto es, $l \geq m$ por lo que $u \in U_K^{(m)}$ lo que demuestra que $G_i(L_{\pi,n}/K) \subseteq (U_K^{(m)}, L_{\pi,n}/K)$. □

Un resultado interesante es ver que tipo de saltos superiores tienen las extensiones abelianas.

Teorema 5.8.74 (Hasse–Arf). *Sea L/K una extensión abeliana finita de campos locales. Entonces los saltos de la filtración superior $\{G^t(L/K)\}_{t\geq -1}$ son enteros.*

Demostración. Sea E/K la máxima subextensión $K \subseteq E \subseteq L$ no ramificada. Entonces $G^t(L/E) = G^t(L/K)$ para $t > -1$ debido a que $\eta_{E/K}(s) = s$ donde $\eta_{E/K}$ es la inversa de la función de Herbrand. Por tanto

$$\eta_{L/K}(s) = \eta_{L/E}(\eta_{E/K}(s)) = \eta_{L/E}(s).$$

Se sigue que podemos suponer que L/K es totalmente ramificada.

Sea π_L un elemento primo de L. Entonces $\pi := \mathrm{N}_{L/K}(\pi_L)$ es un elemento primo de K. Por otro lado, existe $m \in \mathbb{N}$ tal que $(\pi) \times U_K^{(m)} \subseteq \mathrm{N}_{L/K} L^*$. Se sigue que L está contenida en el campo de clase de $(\pi) \times U_K^{(m)}$ el cual corresponde a $L_{\pi,m}$. Si t_0 es un salto de $\{G^t(L/K)\}_t$ entonces, por el Teorema

5.8.11, t_0 es un salto de $\{G^t(L_{\pi,m}/K)_t$. Por lo tanto podemos suponer $L = L_{\pi,m}$.

De la Proposición 5.8.73 los saltos de $\{G_s(L_{\pi,m}/K)\}_s$ son los números $q^l - 1$, $0 \leq l \leq m-1$ con la excepción de que cuando $q = 2$, 0 no es un salto.

Para calcular los saltos $\{G^t(L_{\pi,m}/K)\}_t$ calculamos $\varphi_{L_{\pi,m}/K}(q^l - 1) = l$, $l = 0, 1, \ldots, m-1$ lo cual prueba el teorema. □

El siguiente es el resultado central de los grupos de ramificación superior con la teoría de clase de campos locales.

Teorema 5.8.75. *Sea L/K una extensión abeliana finita de campos locales. Entonces el símbolo residual de la norma*

$$(\ \ , L/K)\colon K^* \longrightarrow \mathrm{Gal}(L/K)$$

manda el grupo $U_K^{(n)}$, $n \geq 0$, sobre el n–ésimo grupo de ramificación superior $G^n(L/K)$:

$$(U_K^{(n)}, L/K) = G^n(L/K), n \geq 0.$$

Demostración. Si E es la máxima extensión no ramificada de K contenida en L: $K \subseteq E \subseteq L$, entonces $G^n(L/K) = G^n(L/E)$. Por el Teorema 5.1.11 y el Teorema 5.7.12 se tiene

$$(U_E^{(n)}, L/E) = (\mathrm{N}_{E/K}\, U_E^{(n)}, L/K) = (U_K^{(n)}, L/K).$$

Por tanto, podemos, sustituir L/K por L/E y por ende podemos suponer que L/K es totalmente ramificada. Procediendo como en el Teorema de Hasse–Arf, Teorema 5.8.74, se tiene que $L \subseteq L_{\pi,m}$ para alguna $m \in \mathbb{N}$ y sin pérdida de generalidad podemos suponer $L = L_{\pi,m}$.

Ahora, por el Teorema 5.8.62 y la Proposición 5.8.73, se tiene

$$\mathrm{Gal}(L_{\pi,m}/L_{\pi,l}) = G_i(L_{\pi,m}/K)$$

para $q^{l-1} \leq i \leq q^l - 1$. Puesto que la función de Herbrand φ satisface $\varphi_{L_{\pi,m}/K}(q^l - 1) = l$, obtenemos

$$(U_K^{(l)}, L_{\pi,m}/K) = G_{q^l-1}(L_{\pi,m}/K) = G^l(L_{\pi,m}/K). \qquad \square$$

El Teorema 5.8.75 nos proporciona una forma de calcular el conductor local.

Corolario 5.8.76. *Sea L/K una extensión abeliana finita de campos locales y sea $\mathfrak{f}_{L/K} = \mathfrak{f}$ el conductor de la extensión L/K. Sea n tal que $G_n(L/K) \neq \{1\}$ y $G_{n+1}(L/K) = \{1\}$, $n \geq 1$. Entonces $\mathfrak{f} = \mathfrak{p}^{c_\mathfrak{p}}$ donde*

$$c_\mathfrak{p} = 1 + \varphi_{L/K}(n) = \frac{1}{g_0}(g_0 + g_1 + \cdots + g_n).$$

En otras palabras, el conductor local pudo haber sido definido como

$$\mathfrak{f} = \mathfrak{p}^{1+\varphi_{L/K}(n)}$$

donde $G_n(L/K) \neq \{1\}$ *y* $G_{n+1}(L/K) = \{1\}$.

Demostración. Por el Teorema 5.8.75 se tiene

$$\begin{aligned} U_K^{(m)} \subseteq \mathrm{N}_{L/K}\, L^* &\iff (U_K^{(m)}, L/K) = 1 \iff G^m(L/K) = \{1\} \\ &\iff G_{\eta_{L/K}(m)}(L/K) = \{1\}. \end{aligned}$$

Se sigue que $G_n(L/K) \neq \{1\}$ y $G_{n+1}(L/K) = \{1\}$ si y solamente si $U_K^{(\varphi_{L/K}(n))} \nsubseteq \mathrm{N}_{L/K}\, L^*$ y $U_K^{(1+\varphi_{L/K}(n))} \subseteq \mathrm{N}_{L/K}\, L^*$. □

Terminamos esta sección estudiando la descomposición en extensiones abelianas de campos locales.

Teorema 5.8.77. *Sea* L/K *una extensión abeliana finita de campos locales. Sean* e *y* f *el índice de ramificación y el grado de inercia. Entonces*

$$e = [U_K : \mathrm{N}_{L/K}\, U_L] \quad y \quad f = o(\pi_K \bmod U_K\, \mathrm{N}_{L/K}\, L^*),$$

donde π_K *es un elemento uniformizador de* K.

Demostración. El Corolario 5.3.12 prueba que $e = [U_K : \mathrm{N}_{L/K}\, U_L]$. Otra demostración es consecuencia del Teorema 5.8.75:

$$(U_K, L/K) = G_0(L/K) \cong \frac{U_K\, \mathrm{N}_{L/K}\, L^*}{\mathrm{N}_{L/K}\, L^*} \cong \frac{U_K}{U_K \cap \mathrm{N}_{L/K}\, L^*} = \frac{U_K}{\mathrm{N}_{L/K}\, U_L}.$$

Ahora bien, $ef = [L : K] = [K^* : \mathrm{N}_{L/K}\, L^*]$. Notemos que

$$\frac{U_K\, \mathrm{N}_{L/K}\, L^*}{\mathrm{N}_{L/K}\, L^*} \cong \frac{U_K}{\mathrm{N}_{L/K}\, L^* \cap U_K} = \frac{U_K}{\mathrm{N}_{L/K}\, U_L}.$$

Se sigue que $f = \frac{[L:K]}{e} = \frac{[K^* : \mathrm{N}_{L/K}\, L^*]}{[U_K\, \mathrm{N}_{L/K}\, L^* : \mathrm{N}_{L/K}\, L^*]} = [K^* : U_K\, \mathrm{N}_{L/K}\, L^*]$. Puesto que $K^* = (\pi_K) \times U_K$, obtenemos

$$\frac{K^*}{U_K\, \mathrm{N}_{L/K}\, L^*} = \frac{(\pi_K) U_K\, \mathrm{N}_{L/K}\, L^*}{U_K\, \mathrm{N}_{L/K}\, L^*} = \langle \pi_K \bmod U_K\, \mathrm{N}_{L/K}\, L^* \rangle.$$

Se sigue $f = [K^* : U_K\, \mathrm{N}_{L/K}\, L^*] = o(\pi_K \bmod U_K\, \mathrm{N}_{L/K}\, L^*)$. □

6

Campos de clase globales

Definición 6.0.1. Un *campo global* K es o bien una extensión finita de $\mathbb{Q}$ o bien un campo de funciones con campo de constantes $\mathbb{F}_q$, el campo finito de $q = p^r$ elementos.

Las extensión finitas de $\mathbb{Q}$ son el caso de característica 0 y los llamaremos *campos numéricos*. Los campos de funciones son el caso de característica $p > 0$ y los llamaremos *campos de funciones*.

Observación 6.0.2. En el caso de campos de funciones no hay lugares infinitos.

Sea K un campo global. Sea $\mathfrak{p}$ un lugar de K. Usaremos la notación $\mathfrak{p}|\infty$ para $\mathfrak{p}$ un lugar infinito (arquimediano) y $\mathfrak{p} \nmid \infty$ si $\mathfrak{p}$ es un lugar finito.

Si $\mathfrak{p}$ es un lugar finito, sea $\mathcal{O}_\mathfrak{p} = \{x \in K \mid v_\mathfrak{p}(x) \geq 0\}$ el anillo de valuación de $\mathfrak{p}$ y $v_\mathfrak{p}$ es la valuación asociada. La completación de K en un lugar finito o infinito se denotará por $K_\mathfrak{p}$.

Si $\mathfrak{p}$ es finito, $\mathrm{N}(\mathfrak{p})$ va a denotar la *norma absoluta* de $\mathfrak{p}$, esto es $\mathrm{N}(\mathfrak{p}) = \left|\mathcal{O}_\mathfrak{p}/\mathfrak{p}\right|$.

Se tiene que si $\mathbb{F}_p$ es el campo primo de $\mathcal{O}_\mathfrak{p}/\mathfrak{p}$ y $f_\mathfrak{p} = \left[\mathcal{O}_\mathfrak{p}/\mathfrak{p} : \mathbb{F}_p\right]$, entonces $\mathrm{N}(\mathfrak{p}) = p^{f_\mathfrak{p}} = q_\mathfrak{p}$.

Para el valor absoluto $|\ |_\mathfrak{p}$ asociado a $\mathfrak{p}$, seleccionamos el número $0 < c < 1$ como $c = p^{-f_\mathfrak{p}} = \mathrm{N}(\mathfrak{p})^{-1} = \frac{1}{\left|\mathcal{O}_\mathfrak{p}/\mathfrak{p}\right|} = q_\mathfrak{p}^{-1}$. De esta foma, tenemos que si $a \in K$, $a \neq 0$,

$$|a|_\mathfrak{p} = p^{-f_\mathfrak{p} v_\mathfrak{p}(a)} = q_\mathfrak{p}^{-v_\mathfrak{p}(a)} \quad \text{y} \quad |0|_\mathfrak{p} = 0.$$

Si $\mathfrak{p}$ es un lugar finito, denotamos por $U_\mathfrak{p} = U_{K_\mathfrak{p}}$ al grupo de unidades de $K_\mathfrak{p}$. Si $\mathfrak{p}$ es un lugar infinito, entonces $K_\mathfrak{p} = \mathbb{R}$ o $\mathbb{C}$. Si $\mathfrak{p}$ es real, es decir si $K_\mathfrak{p} = \mathbb{R}$ y si $\sigma\colon K \to \mathbb{R} = K_\mathfrak{p}$ es el encaje asociado a $\mathfrak{p}$, entonces $|a|_\mathfrak{p} := |\sigma a|$, $a \in K$, donde $|\ |$ denota el valor absoluto usual de $\mathbb{R}$.

Si $\mathfrak{p}$ es complejo, $K_\mathfrak{p} = \mathbb{C}$, si σ es uno de los dos encajes conjugados $\sigma\colon K \to \mathbb{C} = K_\mathfrak{p}$, ponemos $|a|_\mathfrak{p} := \|\sigma a\|^2$ para $a \in K$, donde $\|\ \|$ es el valor absoluto usual de $\mathbb{C}$.

6.1. Repaso de resultados básicos de campos globales

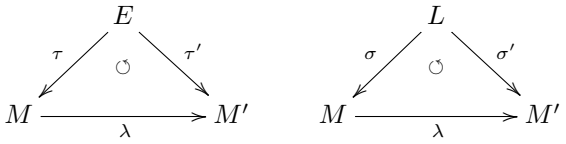
6.1.1. Composición de campos

Sean E y L dos campos cualesquiera de la misma característica, esto es, el campo primo, $\mathbb{F}_p$ o $\mathbb{Q}$, es el mismo para ambos campos. Nos preguntamos, ¿qué significa la composición de E y L?

Supongamos primero que existe un campo Ω tal que $E, L \subseteq \Omega$. Entonces la composición es simplemente el mínimo subcampo de Ω que contiene tanto a E como a L. Sin embargo, si no tenemos un tal campo Ω, debemos construir un campo (mínimo) que contenga tanto a E como a L.

Definición 6.1.1. Sea K un campo arbitrario y sean E/K y L/K dos extensiones de K (por ejemplo, K podría ser el campo primo). Una *composición* de E y L sobre K, es una terna (M, τ, σ) donde M es un campo que contiene a K, $\tau\colon E \to M$ y $\sigma\colon L \to M$, τ y σ son monomorfismos de campos tales que $\tau|_K = \sigma|_K = \mathrm{Id}_K$ y M está generado por $\tau(E)$ y $\sigma(L)$.

Definición 6.1.2. Dos composiciones (M, τ, σ), (M', τ', σ') de E/K y L/K se llaman *equivalentes* si existe un isomorfismo $\lambda\colon M \longrightarrow M'$ tal que $\lambda \circ \tau = \tau'$ y $\lambda \circ \sigma = \sigma'$.



Ser equivalentes, es una relación de equivalencia. Estudiaremos en el caso en que L/K es finita, $[L : K] < \infty$ y E/K es arbitraria, las diferentes clases de equivalencia.

Sean $[L : K] = n < \infty$ y (M, τ, σ) una composición de E y L. Sean $E' = \tau(E)$, $L' = \sigma(L)$ y

$$E'L' = \Big\{ \sum_{i=1}^{r} e_i l_i \mid e_i \in E', l_i \in L', r \in \mathbb{N} \Big\} \subseteq M,$$

entonces $E'L'$ es una subálgebra sobre K. Ahora bien, $E'L'$ es un dominio entero. Sea $\{\alpha_1, \ldots, \alpha_n\}$ una base de L/K. Entonces $\{\sigma(\alpha_1), \ldots, \sigma(\alpha_n)\}$ genera a $E'L'$ sobre E'. Puesto que E' es un campo, $E'L'$ es un campo (recordemos que si F es un campo y D es un dominio entero con $\dim_F D < \infty$, entonces D es un campo). Se sigue que $E'L' = M$.

Sea $\theta\colon E \otimes_K L \longrightarrow M$ definido por $\theta(e \otimes_K l) = \tau(e)\sigma(l)$. Entonces θ es un K-epimorfismo y $M \cong (E \otimes_K L)/\operatorname{núc}\theta$. Como M es un campo, $\operatorname{núc}\theta = \mathfrak{M}$ es un ideal maximal. Ahora bien $K \cong K \otimes_K K$ y $\theta|_K = \mathrm{Id}_K$ por lo que $\mathfrak{M} \cap K = \{0\}$.

Los homomorfismos

$$E \xrightarrow{\ i\ } E \otimes_K L, \qquad i(e) = \tau(e) \otimes_K 1,$$
$$L \xrightarrow{\ j\ } E \otimes_K L, \qquad j(l) = 1 \otimes_K \sigma(l),$$

son monomorfismos pues $(\theta \circ i)(E) = \tau(E)$ y $(\theta \circ j)(L) = \sigma(L)$. Por tanto $\mathfrak{M} \cap E = \mathfrak{M} \cap L = \{0\}$.

Teorema 6.1.3. *Las clases de equivalencia de las composiciones E con L sobre K, están en correspondencia biyectiva con los ideales maximales de la K-álgebra $E \otimes_K L$. En particular, la composición de campos siempre existe.*

Demostración. Ya vimos que cada composición corresponde a un ideal maximal. Reciprocamente, si $\mathfrak{M}$ es un ideal maximal de $E \otimes_K L$, definimos $M = (E \otimes_K L)/\mathfrak{M}$ el cual es un campo. Sean

$$i\colon E \longrightarrow (E \otimes_K L)/\mathfrak{M}, \quad i(e) = (e \otimes_K 1) + \mathfrak{M} \quad \text{y}$$
$$j\colon L \longrightarrow (E \otimes_K L)/\mathfrak{M}, \quad j(l) = (1 \otimes_K l) + \mathfrak{M}.$$

Puesto que $\mathfrak{M}$ no contiene unidades, i y j son inyectivas y M está generado por $i(E)$ y $j(L)$. Además $i|_K = j|_K = \mathrm{Id}_K$. Se sigue que M es una composición de E y L.

Ahora sean (M, τ, σ) y (M', τ', σ') dos composiciones donde

$$M \cong (E \otimes_K L)/\mathfrak{M} \quad \text{y} \quad M' \cong (E \otimes_K L)/\mathfrak{M}'.$$

Si M y M' son equivalentes, existe un isomorfismo $\lambda\colon M \to M'$ con $\lambda \circ \tau = \tau'$ y $\lambda \circ \sigma = \sigma'$. Sea $\sum_{i=1}^r e_i \otimes_K l_i \in \mathfrak{M}$. Entonces se tiene que si $\sum_{i=1}^r \tau(e_i)\sigma(l_i) = 0$ en M entonces

$$\lambda\Big(\sum_{i=1}^r \tau(e_i)\sigma(l_i)\Big) = \sum_{i=1}^r (\lambda \circ \tau)(e_i)(\lambda \circ \sigma)(l_i) = \sum_{i=1}^r \tau'(e_i)\sigma'(l_i) = 0$$

en M' por lo que $\sum_{i=1}^r e_i \otimes_K l_i \in \mathfrak{M}'$. Se sigue que $\mathfrak{M} \subseteq \mathfrak{M}'$ y como ambos son maximales, se tiene $\mathfrak{M} = \mathfrak{M}'$.

Recíprocamente, sean $\mathfrak{M} = \mathfrak{M}'$. Si θ y θ' son los isomorfismos de $(E \otimes_K L)/\mathfrak{M}$ y de $(E \otimes_K L)/\mathfrak{M}'$ a M y M' respectivamente, entonces

$$\begin{array}{ccc} (E \otimes_K L)/\mathfrak{M} & = & (E \otimes_K L)/\mathfrak{M}' \\ \downarrow{\scriptstyle \theta} & & \downarrow{\scriptstyle \theta'} \\ M & \xrightarrow[\theta' \circ \theta^{-1}]{} & \mathfrak{M}' \end{array}$$

y $\lambda := \theta' \circ \theta^{-1}$ es un isomorfismo de M y M', y

$$\tau = \theta \circ i, \quad \tau' = \theta' \circ i = \theta' \circ \theta^{-1} \circ \theta \circ i = \lambda \circ \tau,$$
$$\sigma = \theta \circ j, \quad \sigma' = \theta' \circ j = \theta' \circ \theta^{-1} \circ \theta \circ j = \lambda \circ \sigma,$$

por lo que M y M' son extensiones equivalentes. □

Teorema 6.1.4. *Sean T un campo y A un álgebra sobre T tal que A es de dimemsión finita sobre T y A tiene unidad. Entonces A tiene un número finito de ideales maximales.*

Demostración. Sea $\dim_T A = n < \infty$ y sean $\mathfrak{M}_1, \ldots, \mathfrak{M}_r$ r ideales maximales de A distintos. Sea $\mathfrak{N} = \bigcap_{i=1}^r \mathfrak{M}_i$. Entonces $A/\mathfrak{N} \cong \bigoplus_{i=1}^r A/\mathfrak{M}_i$. Ahora bien, $A/\mathfrak{N}$ y $A/\mathfrak{M}_i$, $1 \leq i \leq r$, son T-álgebras y

$$n = \dim_T A \geq \dim_T A/\mathfrak{N} = \sum_{i=1}^r A/\mathfrak{M}_i \geq r,$$

de donde se sigue que $r \leq n$. □

Corolario 6.1.5. *Si K es cualquier campo y E/K y L/K son dos extensiones de K con $[L : K] = n < \infty$, entonces el número de composiciones de E y L sobre K es menor o igual n y en particular este número es finito.*

Demostración. Si $\{\alpha_1, \ldots, \alpha_n\}$ es una base de L/K, $\{1 \otimes_K \alpha_1, \ldots, 1 \otimes_K \alpha_n\}$ genera a $E \otimes_K L$ sobre E y $\dim_E(E \otimes_K L) \leq \dim_K L = n$. El resultado se sigue pues $A = E \otimes_K L$ es una E-álgebra. □

Consideremos ahora $L = K(\theta)$ una extensión simple y sea $f(x) = \mathrm{Irr}(\theta, x, K) \in K[x]$. Sea $f(x) = p_1(x)^{e_1} \cdots p_r(x)^{e_r} \in E[x]$ la descomposición de $f(x)$ como producto de polinomios irreducibles de $E[x]$. Entonces

$$\begin{aligned} E \otimes_K L = E \otimes_K K(\theta) &\cong E \otimes_K \big(K[x]/\langle f(x)\rangle\big) \cong \big(E \otimes_K K[x]\big)/\langle f(x)\rangle \\ &\cong (E[x])/\langle f(x)\rangle \cong \bigoplus_{i=1}^r \big(E[x]/\langle p_i^{e_i}(x)\rangle\big). \end{aligned}$$

Los ideales maximales de $E \otimes_K L$ están dados por

$$\langle p_1(x)\rangle/\langle f(x)\rangle, \ldots, \langle p_r(x)\rangle/\langle f(x)\rangle$$

y por tanto todas las composiciones inequivalentes de E y L sobre K son $\Big\{E[x]/\langle p_i(x)\rangle\Big\}_{i=1}^r$.

Se tiene $\dim_E(E \otimes_K L) = \mathrm{gr}\, f(x) = \sum_{i=1}^r e_i \,\mathrm{gr}\, p_i(x) = [L : K]$. Si L/K es una extensión separable, se tiene que e_i, $1 \leq i \leq r$ y

$$E \otimes_K L \cong \bigoplus_{i=1}^r E[x]/\langle p_i(x)\rangle \cong \bigoplus_{i=1}^r E(\theta_i)$$

donde θ_i es una raíz de $p_i(x)$ y $E \otimes_K L$ es la suma directa de las composiciones de E y L sobre K y estas composiciones son $\big\{E(\theta_i)\big\}_{i=1}^r$.

De esta forma, si suponemos que $f(x)$ es separable y enumeramos las raíces de $f(x)$ en E, entonces

$$f(x) = \prod_{i=1}^{r} p_i(x) = \prod_{i=1}^{r} \big(\prod_{j=1}^{m_i} (x - \theta_{ij}) \big)$$

con $p_i(x) = \prod_{j=1}^{m_i}(x-\theta_{ij})$. Se tiene que $E(\theta_{ij})$ y $E(\theta_{ij'})$ son equivalentes pues θ_{ij} y $\theta_{ij'}$ son conjugados sobre E.

En resumen, E y L tienen $n = [L : K]$ composiciones con r clases inequivalentes. Las r clases inequivalentes tienen $m_1, \ldots, m_r$ elementos respectivamente.

Ejemplo 6.1.6. Sea $K = \mathbb{Q}$, $E = \mathbb{R}$ y sea $L = K(\theta)$ con $\theta^3 = d$ con $d \in \mathbb{Q}$ que no es cubo de $\mathbb{Q}$. Entonces

$$x^3 - d = (x - \theta)(x^2 + \theta x + \theta^2)$$

con $\theta^3 = d$ y $\theta \in \mathbb{R}$. Las raíces de $x^2+\theta x+\theta^2 \in \mathbb{R}[x]$ son $\theta_1 = \zeta_3\theta$ y $\theta_2 = \zeta_3^{-1}\theta$. Hay dos composiciones inequivalentes de L con $\mathbb{R}$, a saber $\mathbb{R}(\theta) = \mathbb{R}$ y los encajes conjugados $\{\mathbb{R}(\zeta_3\theta) = \mathbb{C}, \mathbb{R}(\zeta_3^{-1}\theta) = \mathbb{C}\}$.

Ejemplo 6.1.7. Sean $K = \mathbb{Q}_p$ con p un número primo tal que $p \equiv 1 \bmod n$ con $n \in \mathbb{N}$, $n \geq 3$. Sea ζ_n una raíz n-ésima primitiva de la unidad y sea $L = \mathbb{Q}(\zeta_n)$. Entonces p se descompone totalmente en L/K. Se tiene que $\zeta_n \in \mathbb{Q}_p$: $\zeta_n^p = \zeta_n$ pues $p \equiv 1 \bmod n$ por lo que $\zeta_n \in \mathbb{F}_p$. Por tanto $x^n - 1 \in \mathbb{F}_p[x]$ se factoriza en factores lineales y por el Lema de Hensel, ζ_n tiene un levantamiento a $\mathbb{Q}_p$

De esta forma tenemos que si $\psi_n(x) = \prod_{\mathrm{mcd}(a,n)=1}(x - \zeta_n^a) = \mathrm{Irr}(\zeta_n, x, \mathbb{Q})$ y $\prod_{\mathrm{mcd}(a,n)=1}(x-\zeta_n^a)$ es la factorización de irreducibles de $\psi_n(x)$ en $\mathbb{Q}_p[x]$, se sigue que las composiciones inequivalentes de $\mathbb{Q}(\zeta_n)$ con $\mathbb{Q}_p$ son precisamente $\big\{\mathbb{Q}_p(\zeta_n^a)\big\}_{\mathrm{mcd}(a,n)=1}$, esto es, $\mathbb{Q}_p(\zeta_n^a) = \mathbb{Q}_p(\zeta_n) = \mathbb{Q}_p$ pero son inequivalentes.

En resumen, hay $\varphi(n)$ composiciones de $\mathbb{Q}(\zeta_n)$ y $\mathbb{Q}_p$ sobre $\mathbb{Q}$ inequivalentes y todos ellos son iguales $\mathbb{Q}_p$.

Sea K un campo global y sea v un valor absoluto de K y K_v la completación de K en v. El valor absoluto v se extiende de manera única a K_v: Si $\{x_n\}_{n=1}^{\infty}$ es una sucesión de Cauchy en K, $\bar{v}\big(\{x_n\}\big) := \lim\limits_{n\to\infty} v(x_n)$, $\bar{v}|_K = v$. Equivalentemente, $\big|\{x_n\}\big|_v = \lim\limits_{n\to\infty} |x_n|_v$. Se denota nuevamente por v la extensión a K_v.

Sea ahora L/K una extensión finita y separable de campos globales y sea v un valor absoluto de K. Sea K_v la completación de K en v. Entonces si M es una composición de L con K_v sobre K, denotada de momento como LK_v, se tiene que LK_v es un campo que es una extensión finita de K_v y por tanto v se extiende de manera única a un valor absoluto ω en LK_v. Denotemos $L_\omega = LK_v$ con $\omega|_K = v$ y L_ω es completo.

De esta forma, $LK_v \subseteq \bar{K}_v$ pues LK_v es una extensión finita de K_v. Esta composición es (L_ω, τ, ι), $\tau\colon L \longrightarrow L_\omega \subseteq \bar{K}_v$ y ι es el encaje natural $\iota : K_v \longrightarrow L_\omega \subseteq \bar{K}_v$, $\iota|_K = \mathrm{Id}_K$, esto es $\iota(K_v) = K_v$ dentro de $\bar{K}_v$. Se tiene $L_\omega = \tau(L)K_v$ con τ un encaje de L en $\bar{K}_v$.

Recíprocamente, si ω es un valor absoluto de L con $\omega|_K \sim v$, podemos normalizar ω de tal forma que $\omega|_K = v$. Entonces, si L_ω es la completación de L con respecto a ω y si K_ω es la cerradura de K en L_ω, K_ω es completo y por tanto $K_\omega = K_v$ puesto que K es denso en K_ω. Además, $L, K_v \subseteq L_\omega$ por lo que LK_v, la composición de L y K_v, está contenida en L_ω y L es denso en L_ω por lo que LK_v es denso y cerrado en L_ω (por ser completo). Se sigue que $LK_v = L_\omega$.

De esta forma, hemos obtenido, todas las completaciones L_ω con $\omega|_K = v$ son las composiciones de L con K_v sobre K, es decir:

$$\left\{\tau(L)K_v\right\}_{\tau: L \to \bar{K}_v}.$$

Además, $\left|\{\sigma : L \to \bar{K}_v\}\right| = [L : K]_s = [L : K]$, donde $[L : K]_s$ denota el grado de separabilidad de la extensión L/K y $|\ |_v$ se extiende de manera única $|\ |_{\tilde{v}}$ a K_v y como todas las composiciones de L con K_v sobre K están contenidas en una extensión finita C de K_v, la extensión de $|\ |_{\tilde{v}}$ a C es única, denotada nuevamente por $|\ |_v$. De esta forma, los valores absolutos ω de L con $\omega|_K = v$ pueden definirse como $|\alpha|_\omega = |\sigma\alpha|_v$ donde $\alpha \in L$ y con $\sigma : L \hookrightarrow \bar{K}_v$. En este caso se tiene $L_\omega = \sigma(L)K_v$.

Dados dos encajes $\tau, \sigma : L \longrightarrow \bar{K}_v$, veremos cuando $\tau(L)K_v$ y $\sigma(L)K_v$ tienen el mismo valor absoluto.

Recordemos que dos valores absolutos $|\ |_1$ y $|\ |_2$ en un campo E se llaman *equivalentes* si para $x \in E$, se tiene

$$|x|_1 < 1 \iff |x|_2 < 1.$$

Equivalentemente, $|a|_1 < |b|_1 \iff |a|_2 < |b|_2$.

Si $|\ |$ es cualquier valor absoluto en E y $s \in \mathbb{R}$, $s > 0$, entonces $|\ |$ y $|\ |^s$ son equivalentes. Recíprocamente, se tiene

Teorema 6.1.8. *Si $|\ |_1$ y $|\ |_2$ son equivalentes en E, entonces existe $s \in \mathbb{R}$, $s > 0$ con $|\ |_1^s = |\ |_2$.*

Demostración. Si $|\ |_1$ es trivial, $|\ |_2$ es también trivial y recíprocamente (recordemos que $|\ |$ es *trivial* significa que $|x| = 1$ para todo $x \neq 0$).

Sea $0 < |a_0|_2 < 1$. Sea $a \in E$, $a \neq 0$ y sea $\mathcal{A} = \{(n, m) \in \mathbb{N}^2 \mid |a_0|_2^n < |a|_2^m\}$. Por tanto, si $(n, m) \in \mathcal{A}$, $|a_0|_2^n < |a|_2^m$ de donde se sigue que $n \log |a_0|_2 < m \log |a|_2$. Como $\log |a_0|_2 < 0$, $(n, m) \in \mathcal{A} \iff \frac{n}{m} > \frac{\log |a|_2}{\log |a_0|_2}$.

Como $|\ |_1$ es equivalente $|\ |_2$, se tiene $(n, m) \in \mathcal{A} \iff \frac{n}{m} > \frac{\log |a|_1}{\log |a_0|_1}$. Se sigue que $\frac{\log |a|_2}{\log |a_0|_2} = \frac{\log |a|_1}{\log |a_0|_1}$. Por tanto $\frac{\log |a|_2}{\log |a|_1} = \frac{\log |a_0|_2}{\log |a_0|_1}$ y $\frac{\log |a|_2}{\log |a|_1}$ es independiente de a.

Sea $s := \frac{\log |a|_2}{\log |a|_1}$. Entonces $|a|_1^s = |a|_2$ para toda $a \in E$, $a \neq 0$ y $s \in \mathbb{R}$, $s > 0$ pues como $|\ |_1$ y $|\ |_2$ son equivalentes, $\log |a_0|_1 < 0$ y $\log |a_0|_2 < 0$, por lo que $s = \frac{\log |a_0|_2}{\log |a_0|_1} > 0$. □

Teorema 6.1.9. *Sea v un valor absoluto no trivial en un campo E y sea F/E una extensión. Si ω y ω' son dos extensiones de v a F, esto es, $\omega|_F = \omega'|_F = v$, y ω y ω' son equivalentes, entonces $\omega = \omega'$.*

Demostración. Se tiene que $|\ |_\omega^s = |\ |_{\omega'}$, $s \in \mathbb{R}$, $s > 0$. Puesto que si $a_0 \in E$, con $|a_0|_v \neq 1$, entonces $|a_0|_\omega = |a_0|_v = |a_0|_{\omega'} = |a_0|_\omega^s$, de donde se sigue que $s = 1$. □

En otras palabras, si ω y ω' son dos valores absolutos de F no iguales que extienden a v, entonces ω y ω' no son equivalentes.

Regresando a $|\ |_v$, un valor absoluto de K, y $|\ |_v$ se extiende de manera única $|\ |_{\tilde{v}}$ a K_v. Entonces, si $L_\omega = \sigma(L)K_v$ y $L_{\omega'} = \tau(L)K_v$, para $\sigma, \tau : L \longrightarrow \bar{K}_v$ y para $\alpha \in L$, $|\alpha|_\omega = |\sigma\alpha|_v$ y $|\alpha|_{\omega'} = |\tau\alpha|_v$. Por tanto ω y ω' son equivalentes si y sólo si $|\sigma\alpha|_v = |\tau\alpha|_v$, esto es, dan el mismo valor absoluto en L.

Sea ahora $\sigma : L \longrightarrow \bar{K}_v$, $\bar{K}_v$ una cerradura separable de K_v, un encaje. Entonces $\sigma(L) \cong L$ y $\sigma(L)K_v/K_v$ es una extensión finita. Entonces $\sigma(L)K_v$ es una completación de L, digamos L_σ. Esto es, σ se identifica con una completación de L, L_σ "$=$" L_ω con $\omega|_{K_v} = v$.

Definición 6.1.10. Sea K un campo global. Los *valores absolutos canónicos* de K estan dados de la siguiente forma: Si $\mathfrak{p}$ es finito, $\mathcal{O}_\mathfrak{p}/\mathfrak{p} = K(\mathfrak{p}) \cong \mathbb{F}_{q_\mathfrak{p}}$, entonces seleccionamos $c = q_\mathfrak{p}^{-1}$ para el valor absoluto:

$$|x|_\mathfrak{p} = q_\mathfrak{p}^{-v_\mathfrak{p}(x)}, \quad \mathrm{N}(\mathfrak{p}) = q_\mathfrak{p}.$$

Si $\mathfrak{p}$ es infinito, $K_\mathfrak{p} \cong \mathbb{R}$ o $\mathbb{C}$, si $\sigma : K \longrightarrow K_\mathfrak{p}$, entonces

$$|x|_\mathfrak{p} = |\sigma x|_\mathbb{R} = |\sigma x| \text{ usual si } \mathfrak{p} = \mathbb{R} \text{ y } |x|_\mathfrak{p} = \|\sigma x\|_\mathbb{C}^2 = \|\sigma x\|_\mathbb{C}^2 \text{ en } \mathbb{C} \text{ si } \mathfrak{p} = \mathbb{C}$$

pues en un lugar complejo consiste de 2 encajes σ y $\bar{\sigma}$ con $\sigma \neq \bar{\sigma}$.

El conjunto de los valores absolutos canónicos se dontará por $\mathcal{M}_K$. Se tiene que $\mathfrak{p}, \mathfrak{p}' \in \mathcal{M}_K$, $\mathfrak{p} \neq \mathfrak{p}'$, entonces $|\ |_\mathfrak{p}$ y $|\ |_{\mathfrak{p}'}$ dan diferentes topologías en K.

Dado un valor absoluto ω de L, $\omega|_K = v$, L_ω/K_v es una extensión finita. Ahora si $\sigma : L_\omega \longrightarrow \bar{K}_v$ es uno de los $[L_\omega : K_v] = [L_\omega : K_v]_s$ encajes, $\sigma|_{K_v} = \mathrm{Id}_{K_v}$. Entonces $\sigma(L) \subseteq \sigma(L_\omega)$ y $\sigma(L)K_v = \sigma(L_\omega)$ por el argumento dado anteriormente.

Teorema 6.1.11. *Sea K un campo global, $v \in \mathcal{M}_K$ y L/K una extensión finita y separable. Se tiene que dos encajes $\sigma, \tau : L \longrightarrow \bar{K}_v$ sobre K, $\sigma|_K = \tau|_K = \mathrm{Id}_K$, dan lugar al mismo valor absoluto en L si y sólo si son conjugados sobre K_v, lo cual significa que existe un isomorfismo $\lambda : \sigma(L)K_v \longrightarrow \tau(L)K_v$ tal que $\lambda|_{K_v} = \mathrm{Id}_{K_v}$. En otras palabras, los encajes dan lugar al mismo valor absoluto si y sólo si las composiciones $\sigma(L)K_v$ y $\tau(L)K_v$ de L y K_v sobre ya sea K o sobre K_v, son equivalentes.*

Demostración. Dado cualquier encaje $\theta : L \longrightarrow \bar{K}_v$, entonces para $\beta \in K$, $\theta(\beta) \in \theta(L)$ y $\theta(L)K_v/K_v$ es una extensión finita.

La extensión de v a $\theta(L)K_v$ es única y si ponemos $\theta(L)K_v = L_\omega$, ω la extensión de v a L_ω, entonces

$$|\beta|_\theta = |\theta\beta|_\omega = |\,\mathrm{N}_{L_\omega/K_v}(\theta\beta)|^{1/n_\omega},$$

donde $n_\omega = [L_\omega : K_v]$. Sean σ y τ conjugados, $\sigma(L)K_v = L_\omega$, $\tau(L)K_v = L_{\omega'}$, $\lambda : L_\omega \longrightarrow L_{\omega'}$ isomorfismo y $\lambda|_{K_v} = \mathrm{Id}_{K_v}$, entonces

$$\begin{gathered}\mathrm{N}_{L_\omega/K_v}(\sigma\beta) = \mathrm{N}_{L_{\omega'}/K_v}(\lambda\sigma\beta) = \mathrm{N}_{L_{\omega'}/K_v}(\tau\beta),\\ |\beta|_\omega = |\,\mathrm{N}_{L_\omega/K_v}(\sigma\beta)|^{1/n_\omega} = |\,\mathrm{N}_{L_{\omega'}/K_v}(\tau\beta)|^{1/n_{\omega'}} = |\beta|_{\omega'} \quad \text{y}\\ n_\omega = [L_\omega : K_v] = [L_{\omega'} : K_v] = n_{\omega'}.\end{gathered}$$

Se sigue que $|\beta|_\omega = |\beta|_{\omega'}$.

Recíprocamente, supongamos que los valores absolutos son los mismos. Ahora $\tau(L)$ y $\sigma(L)$ son isomorfos a L sobre K. Sea $\lambda : \tau(L) \longrightarrow \sigma(L)$ un isomorfismo sobre K. Veremos que λ se puede extender de $\tau(L)K_v$ a $\sigma(L)K_v$ sobre K_v.

Se tiene que $\tau(L)$ es denso en $\tau(L)K_v$, por lo que dado $x \in \tau(L)K_v$ puede ser escrito como $x = \lim\limits_{n\to\infty} \tau x_n$ con $x_n \in L$. Ahora bien, como los valores absolutos inducidos por τ y por σ son el mismo, se sigue que $\{\lambda\tau x_n\} = \{\sigma x_n\}$ converge a un elemento de $\sigma(L)K_v$. Denotemos este elemento por λx. Se verifica que λx es independiente de $\{\tau x_n\}$ y que $\lambda : \tau(L)K_v \longrightarrow \sigma(L)K_v$ es un isomorfismo que deja fija a K_v. □

Con este resultado, podemos enumerar las extensiones de v a L, una fórmula ya muy conocida.

Corolario 6.1.12. *Sea L/K una extensión finita y separable de grado n de campos globales y $v \in \mathcal{M}_K$. Para cada valor absoluto ω de L, sea $n_\omega = [L_\omega : K_v]$ el grado de campos locales (o de $\mathbb{R}$ o de $\mathbb{C}$). Entonces $\sum_{\omega|v} n_\omega = n$.*

Demostración. Se tiene que $n = [L : K] = [L : K]_s$ es el número de encajes $\sigma : L \longrightarrow \bar{K}_v$, $\sigma|_K = \mathrm{Id}_K$. Además $[L_\omega : K_v] = n_\omega$ es el número de encajes $L_\omega \longrightarrow \bar{K}_v$ y todos ellos son conjugados sobre K_v y por tanto dan lugar al mismo valor absoluto. Se sigue que $n = \sum_{\omega|v} n_\omega = \sum_{\omega|v} e_\omega f_\omega$. □

Corolario 6.1.13. *Sean K un campo global y L/K una extensión finita y separable. Sea $\alpha \in L$. Entonces, si $v \in \mathcal{M}_K$, se tiene*

$$\prod_{\omega|v} |\alpha|_\omega^{n_\omega} = |\,\mathrm{N}_{L/K}(\alpha)|_v,$$

con $n_\omega = [L_\omega : K_v]$.

Demostración. La extensión del valor absoluto de K_v a L_ω está dado por $|\alpha|_\omega = |\,\mathrm{N}_{L_\omega/K_v}(\alpha)|^{1/n_\omega}$. Por tanto, si A_ω es la clase de conjugación de ω, se tiene

$$|\alpha|_\omega^{n_\omega} = |\,\mathrm{N}_{L_\omega/K_v}(\alpha)| = \Big|\prod_{\sigma\in A_\omega}\sigma\alpha\Big|_v,$$
$$\prod_{\omega|v}|\alpha|_\omega^{n_\omega} = \prod_{\omega|v}\Big|\prod_{\sigma\in A_\omega}\sigma\alpha\Big| = \Big|\prod_{\sigma}\sigma\alpha\Big|_v,$$

donde σ recorre los $[L:K]$ encajes $\sigma : L \longrightarrow \bar{K}$. Se sigue que $\prod_{\omega|v}|\alpha|_\omega^{n_\omega} = \big|\,\mathrm{N}_{L/K}\,\alpha\big|_v$. □

Corolario 6.1.14. *Sea L/K una extensión finita y separable de campos globales. Entonces $v \in \mathcal{M}_K$ se tiene*

$$\mathrm{N}_{L/K}(\alpha) = \prod_{\omega|v}\mathrm{N}_{L_\omega/K_v}(\alpha) \quad y \quad \mathrm{Tr}_{L/K}(\alpha) = \sum_{\omega|v}\mathrm{Tr}_{L_\omega/K_v}(\alpha)$$

para $\alpha \in L$.

Demostración. Se tiene que si $\mathcal{A}_\omega = \{\sigma : L_\omega \longrightarrow \bar{K}_v \mid \sigma|_{K_v} = \mathrm{Id}_{K_v}\}$ y $\mathcal{A}'_\omega = \{\sigma|_L \mid \sigma \in \mathcal{A}_\omega\}$, entonces $\bigcup_{\omega|v}\mathcal{A}'_\omega = \{\sigma : L \longrightarrow \bar{K} \mid \sigma|_K = \mathrm{Id}_K\}$ de donde se sigue el resultado. □

Proposición 6.1.15. *Sea $K \in \{\mathbb{Q}, \mathbb{F}_q(T)\}$. Entonces*

$$\prod_{v\in\mathcal{M}_K}|\alpha|_v = 1.$$

para toda $\alpha \in K^*$.

Demostración. Sea $\alpha = \gamma p_1^{a_1}\cdots p_r^{a_r}$ con $\{p_1,\ldots,p_r\}$ ya sea números primos distintos si $K = \mathbb{Q}$ o polinomios mónicos irreducibles distintos si $K = \mathbb{F}_q(T)$ y $\gamma = \pm 1$ en el caso numérico y $\gamma \in \mathbb{F}_q^*$ en el caso de campos de funciones.

Entonces si $K = \mathbb{Q}$,

$$|\alpha|_v = \begin{cases} p_i^{-a_i} & \text{si } v = p_i, \\ 1 & \text{si } v \notin \{p_1,\ldots,p_r\} \text{ y } v \text{ es finito}, \\ |\alpha| & \text{el valor absoluto usual si } v = \infty, \end{cases}$$

y si $K = \mathbb{F}_q$, entonces

$$|\alpha|_v = \begin{cases} q^{-a_i\,\mathrm{gr}\,p_i} & \text{si } v = p_i, \\ 1 & \text{si } v \notin \{p_1,\ldots,p_r\} \text{ y } v \text{ es finito}, \\ q^{\mathrm{gr}\,\alpha} & \text{si } v = \mathfrak{p}_\infty,\ v = 1/T \text{ es el primo infinito}. \end{cases}$$

Se sigue que

$$\prod_{v\in\mathcal{M}_K} |\alpha|_v = \begin{cases} \prod_{i=1}^r p_i^{-a_i}\cdot(p_1^{a_1}\cdots p_r^{a_r}) = 1 & \text{si } K=\mathbb{Q}, \\ q^{-\sum_{i=1}^r a_i \operatorname{gr} p_i}\cdot q^{\sum_{i=1}^r a_i \operatorname{gr} p_i} = 1 & \text{si } K=\mathbb{F}_q. \end{cases}$$

□

Teorema 6.1.16 (Producto de los valores absolutos). *Sea L cualquier campo global. Entonces para $\alpha\in L^*$, se tiene*

$$\prod_{\omega\in\mathcal{M}_L} |\alpha|_\omega = 1.$$

Demostración. Si L es un campo de funciones, sabemos que para $\alpha\in L^*$ $\operatorname{gr}\alpha = \operatorname{gr}(\alpha)_L = 0$ donde $(\alpha)_L$ denota al divisor principal de α, $\operatorname{gr}\alpha = \sum_{\mathfrak{p}\in\mathcal{M}_L}\operatorname{gr}\mathfrak{p}\cdot v_{\mathfrak{p}}(\alpha)$ y $|\alpha|_{\mathfrak{p}} = q^{-\operatorname{gr}\mathfrak{p}\cdot v_{\mathfrak{p}}(\alpha)}$. Por tanto $\prod_{\mathfrak{p}\in\mathcal{M}_L}|\alpha|_{\mathfrak{p}} = q^{-\operatorname{gr}\alpha} = q^0 = 1$.

Ahora damos otra demostración que funciona para cualquier campo global. Si L es campo de funciones, por ser $\mathbb{F}_q$ un campo perfecto, L es una extensión finita y separable de algún $\mathbb{F}_q(T)$.

Para L cualquier campo global, denotamos $n_\omega = [L_\omega : K_v]$ donde $\omega\in\mathbb{P}_L$ y $\omega|_K = v\in\mathbb{P}_K$ y donde $K\in\{\mathbb{Q},\mathbb{F}_q(T)\}$ según sea el caso. Sabemos que $\prod_{\omega|v}|\alpha|_\omega^{n_\omega} = \big|\operatorname{N}_{L/K}(\alpha)\big|_v$, Corolario 6.1.13.

Ahora bien ω es la única extensión de v a L_ω, sin embargo $|\alpha|_\omega = \big|\operatorname{N}_{L_\omega/K_v}(\alpha)\big|_v^{1/n_\omega}$ no está normalizada pues $\operatorname{gr}\omega = f_\omega\operatorname{gr}v$ donde $f_\omega = f(\omega|v)$.

Si v es un lugar finito (es decir, no arquimediano), se tiene que el campo residual de K_v es $\mathbb{F}_{q^{\operatorname{gr}v}}$ y el de L_ω es $\mathbb{F}_{q^{\operatorname{gr}\omega}}$. Por otro lado $\operatorname{gr}\omega = f(\omega|v)\operatorname{gr}v$ donde $n_\omega = [L_\omega:K_v] = f(\omega|v)e(\omega|v)$. Además $v_{L_\omega}(\alpha) = \frac{1}{f(\omega|v)}v_{K_v}\big(\operatorname{N}_{L_\omega/K_v}(\alpha)\big)$ (Corolario 3.1.15), por lo que

$$\begin{aligned}\big|\operatorname{N}_{L_\omega/K_v}(\alpha)\big|_v &= q^{-\operatorname{gr}v\cdot v_{K_v}(\operatorname{N}_{L_\omega/K_v}(\alpha))} = q^{-\operatorname{gr}v\cdot f(\omega|v)\cdot v_{L_\omega}(\alpha)} \\ &= q^{-\operatorname{gr}\omega\cdot v_{L_\omega}(\alpha)} = \|\alpha\|_\omega\end{aligned}$$

normalizada. Esto es, el valor absoluto normalizado de α en L_ω es $\|\alpha\|_\omega = \big|\operatorname{N}_{L_\omega/K_v}(\alpha)\big|_v$.

Se sigue que, para v un valor absoluto no arquimediano,

$$\prod_{\omega|v}\|\alpha\|_\omega = \big|\prod_{\omega|v}\operatorname{N}_{L_\omega/K_v}(\alpha)\big|_v = \big|\operatorname{N}_{L/K}(\alpha)\big|_v.$$

Para el caso arquimediano, tenemos que si ω, v son ambos reales o ambos complejos, $L_\omega = K_v$ y $\operatorname{N}_{L_\omega/K_v}(\alpha) = \alpha$ y

$$\big|\operatorname{N}_{L_\omega/K_v}(\alpha)\big|_\omega = |\alpha|_v = \begin{cases}|\alpha|^2 & \text{si } w \text{ y } v \text{ son complejos,}\\ |\alpha| & \text{si } w \text{ y } v \text{ son reales.}\end{cases}$$

Si v es real y ω es complejo, $\mathrm{N}_{L_\omega/K_v}(\alpha) = \alpha\bar{\alpha} = |\alpha|^2$ y $\left|\mathrm{N}_{L_\omega/K_v}(\alpha)\right|_\omega = \left|\mathrm{N}_{L_\omega/K_v}(\alpha)\right|^2$. Entonces, en el caso arquimediano, también tenemos que $|\alpha|_\omega = \left|\mathrm{N}_{L_\omega/K_v}(\alpha)\right|_v$.

Se sigue que para cualquier valor absoluto v se tiene

$$\prod_{\omega\in\mathcal{M}_L} |\alpha|_\omega = \prod_{v\in\mathcal{M}_K} \left|\mathrm{N}_{L/K}(\alpha)\right| = 1. \qquad \square$$

Sea S un conjunto finito no vacío de lugares de un campo global K, S conteniendo a los primos arquimedianos en característica 0. Sea $K^S := \{a \in K^* \mid v_\mathfrak{p}(a) = 0$ (es decir, $|a|_\mathfrak{p} = 1)$ para todo $\mathfrak{p} \notin S\}$. K^S se llama *el grupo de las S-unidades*. Si K es un campo numérico y S consiste exactamente de los lugares arquimedianos de K, entonces K^S son las unidades de K, esto es, $K^S = \mathcal{O}_K^*$ donde $\mathcal{O}_K$ es el anillo de enteros de K.

Se tiene el siguiente resultado, cuya demostración presentamos más adelante.

Teorema 6.1.17 (Teorema de las unidades de Dirichlet). *Se tiene que, como grupo,*

$$K^S \cong \begin{cases} W_K \times \mathbb{Z}^{|S|-1} & \text{si } \operatorname{car} K = 0, \\ \mathbb{F}_q^* \times \mathbb{Z}^{|S|-1} & \text{si } \operatorname{car} K = p > 0, \end{cases}$$

donde W_K son las raíces de unidad en K.

El grupo de divisores (característica $p > 0$) o de ideales fraccionarios (característica 0), según sea el caso, se denotará por D_K y en característica p tenemos $D_{K,0} = \{\mathfrak{a} \in D_K \mid \operatorname{gr}\mathfrak{a} = 0\}$. Si $P_K = \{(\alpha) \mid \alpha \in K^*\}$ denota a los divisores o ideales fraccionarios principales, tenemos los grupos de clases de divisores o de ideales fraccionarios $D_K/P_K =: I_K$ y $D_{K,0}/P_K = I_{K,0}$. Se tiene que I_K es finito cuando K es campo numérico y es infinito en el caso de campos de funciones. Por otro lado $I_{K,0}$ es finito (K un campo de funciones).

Usaremos la siguiente notación. Sea $\mathfrak{p}$ un lugar,

$$U_\mathfrak{p} = \begin{cases} \text{grupo de unidades de } K_\mathfrak{p} \text{ si } \mathfrak{p} \text{ es finito}, \\ K_\mathfrak{p}^* \text{ si } \mathfrak{p} \text{ es infinito}. \end{cases}$$

Como vimos anteriormente, $\sum_{\mathfrak{P}|\mathfrak{p}} [L_\mathfrak{P} : K_\mathfrak{p}] = [L : K]$.

Si L/K es una extensión finita de Galois y $\sigma \in G_{L|K}$, entonces para $\mathfrak{P}|\mathfrak{p}$, entonces $\sigma\mathfrak{P}|\mathfrak{p}$ y $L_\mathfrak{P} \xrightarrow[\cong]{\sigma} L_{\sigma\mathfrak{P}}$ es un isomorfismo sobre $K_\mathfrak{p}$. De hecho, si $\alpha \in L_\mathfrak{P}$, existe una sucesión en L, $\alpha = \lim\limits_{n\to\infty} x_n$, $x_n \in L$, σx_n converge $L_{\sigma\mathfrak{P}}$ a $\sigma\alpha$ pues el valor absoluto (no normalizado) satisface

$$\begin{aligned} |\alpha - x_n|_\mathfrak{P} &= \left|\mathrm{N}_{L_\mathfrak{P}/K_\mathfrak{p}}(\alpha - x_n)\right|^{1/[L_\mathfrak{P}:K_\mathfrak{p}]} \\ &= \left|\mathrm{N}_{L_\mathfrak{P}/K_\mathfrak{p}}(\sigma\alpha - \sigma x_n)\right|^{1/[L_\mathfrak{P}:K_\mathfrak{p}]} = |\sigma\alpha - \sigma x_n|_{\sigma\mathfrak{P}}. \end{aligned}$$

Si $\mathfrak{P} = \sigma\mathfrak{P}$, $L_{\mathfrak{P}} \xrightarrow{\sigma} L_{\mathfrak{P}}$ es un automorfismo y $\sigma \in G_{L_{\mathfrak{P}}|K_{\mathfrak{p}}} = D_{L/K}(\mathfrak{P}|\mathfrak{p})$, $|D_{L/K}(\mathfrak{P}|\mathfrak{p})| = e(\mathfrak{P}|\mathfrak{p})f(\mathfrak{P}|\mathfrak{p})$ y $h(L/K) = \big|G_{L|K}/D_{L/K}(\mathfrak{P}|\mathfrak{p})\big|$.

Con respecto a la Teoría de Kummer (Teorema 2.4.2), obtenemos la siguiente información aritmética

Teorema 6.1.18. *Sea K un campo global que contiene una n-ésima raíz primitiva de la unidad ζ_n, donde $p \nmid n$, y p es la característica de K. Sean $L = K\big(\sqrt[n]{\Delta}\big)$, una extensión finita de Kummer de K, y $\mathfrak{p}$ un primo de K. Entonces:*

(1) *$\mathfrak{p}$ se descompone totalmente en $L \iff \Delta \subseteq (K_{\mathfrak{p}}^*)^n$.*
(2) *Si $\mathfrak{p}$ es finito y $\mathfrak{p} \nmid n$, entonces $\mathfrak{p}$ es no ramificado en $L \iff$ existe un conjunto de generadores de $\Delta/(K^*)^n$ que son unidades en $\mathfrak{p}$. En otras palabras, $\Delta \subseteq U_{\mathfrak{p}} \cdot (K^*)^n$.*

Demostración. (1): Se tiene que $\mathfrak{p}$ se descompone totalmente en $L/K \iff L_{\mathfrak{P}} = K_{\mathfrak{p}}$ para todo $\mathfrak{P}|\mathfrak{p}$, $L_{\mathfrak{P}} = K_{\mathfrak{p}}\big(\sqrt[n]{\Delta}\big) = K_{\mathfrak{p}} \iff \sqrt[n]{\Delta} \subseteq K_{\mathfrak{p}}^* \iff \Delta \subseteq (K_{\mathfrak{p}}^*)^n$.

(2): Sea $\mathfrak{P}|\mathfrak{p}$. Supongamos $\mathfrak{p}$ no ramificado. Se tiene que $L_{\mathfrak{P}}/K_{\mathfrak{p}}$ es no ramificada si el grupo de valores de la valuación de $L_{\mathfrak{P}}$ es el mismo que el de $K_{\mathfrak{p}}$. Sea δ uno de los generadores de Δ. Puesto que $\delta = (\delta^{1/n})^n$ en $L_{\mathfrak{P}}$, su valuación es un n-múltiplo de un valor: $v_{\mathfrak{P}}(\delta) = nv_{\mathfrak{P}}(\sqrt[n]{\delta})$ y $v_{\mathfrak{P}}(\delta) = e(\mathfrak{P}|\mathfrak{p})v_{\mathfrak{p}}(\delta) = v_{\mathfrak{p}}(\delta)$. Por tanto se tiene que $v_{\mathfrak{p}}(\delta) = rn$ para alguna $r \in \mathbb{Z}$. Sea $\pi \in K$, $v_{\mathfrak{p}}(\pi) = 1$. Entonces $v_{\mathfrak{p}}\big(\delta(\pi^{-r})^n\big) = 0$ y $(\pi^{-r})^n$ es una n-potencia, por lo que $\delta(\pi^{-r})^n$ es tambíen un generador y es una $\mathfrak{p}$-unidad.

Recíprocamente, supongamos que $\Delta/(K^*)^n$ tiene generadores δ que son unidades en $\mathfrak{p}$. Es suficiente probar que $K(\sqrt[n]{\delta})/K$ es no ramificada para $\delta \in \Delta$. Se tiene que $\alpha = \sqrt[n]{\delta}$ satisface $f(x) = x^n - \delta$ y $f'(\alpha) = n\alpha^{n-1}$ es primo relativo a $\mathfrak{p}$. Entonces $\mathfrak{p}$ no divide al diferente local y por tanto es no ramificado. □

6.1.2. Teoría de Kummer aditiva o de Artin-Schreier-Witt

La teoría de Kummer aditiva es necesaria en nuestro enfoque para probar la segunda desigualdad fundamental. Únicamente requerimos estudiar las extensiones abelianas de un campo global de funciones de exponente p. El tratamiento de exponente p^n se puede hacer cambiando las extensiones de Artin-Schreier por extensiones usando vectores de Witt. Los vectores de Witt pueden ser consultados en [136, Capítulo 12]. Aquí presentamos únicamente las extensiones de exponente p para simplificar la presentación, en el entendido que la teoría es inmediatamente generalizable para extensiones de exponente p^n para cualquier $n \in \mathbb{N}$ cambiando la operación $\wp(x) = x^p - x$ o $\wp(x) = x^q - x$ por $\wp(\vec{x}) = \vec{x}^p \overset{\bullet}{-} \vec{x}$ o $\wp(\vec{x}) = \vec{x}^q \overset{\bullet}{-} \vec{x}$, $\mathbb{F}_p$ por $W_n(\mathbb{F}_p) \cong \mathbb{Z}/p^n\mathbb{Z}$, etc.

Sea K un campo de característica $p > 0$ y sea L/K una extensión abeliana ya sea finita o infinita, de exponente p, esto es, $\sigma^p = 1$ para toda $\sigma \in G = \mathrm{Gal}(L/K)$. Podemos usar a $\mathbb{F}_p$ como el grupo de valores para los caracteres de G, esto es, $\chi(G) = \mathrm{Hom}(G, \mathbb{F}_p)$. Un caracter $\mu \in \chi(G)$ satisface

$$\mu(\sigma\tau) = \mu(\sigma) + \mu(\tau) = \mu(\sigma) + \sigma\mu(\tau),$$

por lo que μ es un cociclo aditivo $Z^1(G, K)$. Ahora bien, $H^1(G, L) = \{0\}$, por lo que existe $\alpha \in L$ tal que $\mu(\sigma) = (1 - \sigma)\alpha$ para toda $\sigma \in G$.

Sea $\wp : L \longrightarrow L$ el operador de Artin-Schreier $\wp(\beta) = \beta^p - \beta$. Se tiene que $\mathrm{núc}\, \wp = \{\beta \in L \mid \beta^p - \beta = 0\} = \mathbb{F}_p$ y $\wp(\sigma\beta) = \sigma\wp(\beta)$ para toda $\beta \in L$. Se tiene que

$$0 \longrightarrow \mathbb{F}_p \longrightarrow L \xrightarrow{\wp} \wp(L) \longrightarrow 0,$$

es una sucesión G-exacta. En cohomología obtenemos la sucesión exacta

$$L^G = K \xrightarrow{\wp} \wp(L)^G = \wp(L) \cap K \xrightarrow{\delta} H^1(G, \mathbb{F}_p) \longrightarrow H^1(G, L) = \{0\}.$$

Ahora bien, $H^1(G, \mathbb{F}_p) = \mathrm{Hom}(G, \mathbb{F}_p) \cong \chi(G)$. Por tanto

$$\frac{\wp(L) \cap K}{\wp(K)} \cong \chi(G).$$

El isomorfismo anterior está dado por el mapeo de conexión δ. Si $a + \wp(K) \in \frac{\wp(L)\cap K}{\wp(K)}$, formalmente, se tiene

$$\begin{array}{ccc} H^0(G, L) & \longleftarrow & H^0(G, \wp(L)) \\ \wp^{-1}(a) & \longleftarrow & a \\ \Big\downarrow \partial & & \\ H^1(G, \mathbb{F}_p) & \longleftarrow & H^1(G, L) \end{array}$$

Por tanto $\delta(a + \wp(K)) = \mu_a \in \chi(G)$ donde $\mu_a(\sigma) = \wp^{-1}a - \sigma(\wp^{-1}a)$. Ahora bien, $\wp^{-1}a = b$ significa $\wp b = a = b^p - b$ por lo que $\sigma(b) = b - \mu_a(\sigma)$ con $\mu_a(\sigma) \in \mathbb{F}_p$.

Sea N la máxima extensión de Artin-Schreier sobre K. Entonces $\wp(L) \subseteq \wp(N) \cap K \subseteq K$. Si tuviésemos $\wp(N) \cap K \neq K$, existiría $a \in K$ con $\wp^{-1}a \notin N$ y $N(\wp^{-1}a)$ sería una extensión de Artin-Schreier conteniendo propiamente a N. Por tanto $\wp(N) \cap K = K$.

Sea $G = \mathrm{Gal}(N/K)$. Entonces $K/\wp(K) \cong H^1(G, \mathbb{F}_p) \cong \chi(G)$. Tenemos un isomorfismo de redes que preserva contenciones entre la red de extensiones de Artin-Schreier y la red de subgrupos de K que contienen a $\wp(K)$.

Si L corresponde al subgrupo Λ, entonces

(a) $\Lambda = \wp(L) \cap K$: Si $a \in K$, $a \in \Lambda \iff \mu_a(\sigma) = 0$ ($\mu_a \in \chi\big(\mathrm{Gal}(N/K)\big)$ para $\sigma \in \mathrm{Gal}(N/L) \iff \sigma(\wp^{-1}a) = \wp^{-1}a$ para $\sigma \in \mathrm{Gal}(N/L) \iff \wp^{-1}a \in L \iff a \in \wp(L)$.

(b) $L = K(\wp^{-1}(\Lambda))$: Si $\sigma \in G = \mathrm{Gal}(N/K)$ entonces $\sigma \in \mathrm{Gal}(N/L) \iff \mu_a(\sigma) = 0$ para $a \in \Lambda \iff \sigma(\wp^{-1}a) = \wp^{-1}a$ para $a \in \Lambda \iff \sigma|_{K(\wp^{-1}(\Lambda))} = \mathrm{Id}_{K(\wp^{-1}(\Lambda))} \iff \sigma \in \mathrm{Gal}(N/K(\wp^{-1}(\Lambda)))$.

De esta forma, hemos probado:

Teorema 6.1.19. *Sea K un campo de característica $p > 0$. Existe una correspondencia entre los subgrupos aditivos Λ de K que contienen a $\wp^{-1}(K)$ y las extensiones abelianas L/K de exponente p. La correspondencia está dada por $\Lambda \longleftrightarrow L_\Lambda = K(\wp^{-1}(\Lambda))$. Además $\chi(\mathrm{Gal}(N/K)) \cong \frac{\wp(L)\cap K}{\wp(K)}$.* □

6.2. Anillo de adèles y grupo de idèles

Tanto los *adèles* como los *idèles* son un caso especial de la siguiente construcción de los llamados "productos directos restringidos".

Definición 6.2.1 (Productos directos restringidos). Sea $\{v\}$ una familia de índices y para cada v sea G_v un grupo abeliano localmente compacto, esto es, cada $x \in G_v$ tiene una vecindad compacta. Para casi todo índice v, sea H_v un subgrupo abierto compacto de G_v. Entonces el *producto directo restringido* de los G_v con respecto a los H_v es el subgrupo G de $\mathcal{G} := \prod_v G_v$ consistente de los elementos de $\mathcal{G}$ cuyas todas las componentes, salvo un número finito, pertenecen a H_v:

$$G = \{(x_v)_v \in \mathcal{G} \mid x_v \in H_v \text{ para casi toda } v\}.$$

Si S es un conjunto finito de índices que incluye a todos los índices v tales que H_v no está definido, entonces se define $G_S := \prod_{v\in S} G_v \times \prod_{v\notin S} H_v$.

Entonces G_S es el producto directo de grupos localmente compactos, por lo que G_S es localmente compacto en la topología producto. Se tiene que G_S es un conjunto abierto de G y G es localmente compacto.

Se tiene $G_v \hookrightarrow G$, $g_v \longrightarrow (\ldots, 1, \ldots, 1, g_v, 1 \ldots, 1, \ldots)$ el cual es un monomorfismo de grupos.

Definición 6.2.2. Los *adèles* de un campo global K, $\mathbb{A}_K$, es el producto restringido de $\{K_v\}_{v\in\mathbb{P}_K}$ con respecto a $\{\mathcal{O}_v\}_{v \text{ finito}}$.

Los *idèles* de un campo global K, J_K, es el producto directo restringido de $\{K_v^*\}_{v\in\mathbb{P}_K}$ con respecto a $\{\mathcal{O}_v^* = U_v\}_{v \text{ finito}}$.

Como veremos más adelante, la topología de $\mathbb{A}_K$ restringida a J_K no es la misma topología de J_K.

Veamos explícitamente los adèles o reparticiones en un campo global K. Un adèle es una familia $\vec{\alpha} = (\alpha_\mathfrak{p})_{\mathfrak{p}\in\mathbb{P}_K} = (\alpha_v)_{v\in\mathbb{P}_K}$, donde $\mathbb{P}_K$ denota el conjunto de lugares (valores absolutos) de K, $\alpha_\mathfrak{p} \in K_\mathfrak{p}$ para toda $\mathfrak{p}$ y $\alpha_\mathfrak{p} \in \mathcal{O}_\mathfrak{p}$ para casi todo $\mathfrak{p}$ finito. Indistintamente usaremos $\mathbb{P}_K$ y $\mathcal{M}_K$, esto es,

siempre supondremos, a menos que se indique lo contrario, que todos los valores absolutos estarán normalizados (de manera canónica).

De esta forma, $\mathbb{A}_K$ denota al anillo de los adèles con las operaciones entrada por entrada y la topología de $\mathbb{A}_K$ está dada por la base de vecindades abiertas de $\vec{0}$ consistente de los conjuntos $\prod_{v\in S} V_v \times \prod_{v\notin S} \mathcal{O}_v$ donde $S \subseteq \mathbb{P}_K$ es un conjunto finito y V_v es un conjunto abierto de K_v y donde $0 \in V_v$ para $v \in S$.

Ahora bien el *grupo de idèles* de un campo global K está formado por los vectores $\vec{\alpha} = (\alpha_{\mathfrak{p}})_{\mathfrak{p}\in\mathbb{P}_K} = (\alpha_v)_{v\in\mathbb{P}_K}$ donde $\alpha_{\mathfrak{p}} \in K_{\mathfrak{p}}^*$ para toda $\mathfrak{p} \in \mathbb{P}_K$ y $|\alpha_{\mathfrak{p}}|_{\mathfrak{p}} = 1$, equivalentemente, $v_{\mathfrak{p}}(\alpha_{\mathfrak{p}}) = 0$, esto es, $\alpha_{\mathfrak{p}} \in \mathcal{O}_{\mathfrak{p}}^* = U_{\mathfrak{p}}$, para casi toda $\mathfrak{p} \in \mathbb{P}_K$.

El conjunto de idèles J_K forma un grupo con la multiplicación entrada por entrada y la topología de J_K está dada por el sistema de vecindades abiertas de $\vec{1}$ consiste de los subconjuntos de la forma del tipo $\prod_{v\in S} W_v \times \prod_{v\notin S} U_v$ donde $S \subseteq \mathbb{P}_K$ es un conjunto finito, W_v es un conjunto abierto de K_v^* donde $1 \in W_v$ para $v \in S$ y $U_v = \mathcal{O}_v^*$ son las unidades. Recordemos que definimos $U_v = \begin{cases} \mathcal{O}_{K_{\mathfrak{p}}}^* = \mathcal{O}_{\mathfrak{p}}^* & \text{si } v \text{ es finito,} \\ K_v^* & \text{si } v \text{ es infinito} \end{cases}$.

Notemos en particular que $U_K := \prod_{\mathfrak{p}\in\mathbb{P}_K} U_{\mathfrak{p}}$ es un conjunto abierto de J_K.

Observación 6.2.3. El grupo de unidades de $\mathbb{A}_K$ es J_K pues $\vec{\alpha} \in \mathbb{A}_K^*$ si para toda $v \in \mathbb{P}_K$, existe $\beta_v \in K_v$ con $\alpha_v\beta_v = 1$. Como $\alpha_v \in \mathcal{O}_v$ para casi toda v, $\alpha_v \in \mathcal{O}_v^*$ para toda v. Esto es $\mathbb{A}_K^* = J_K$.

Definición 6.2.4. Los *idèles principales* son los elementos de J_K de la forma $(\ldots, x, \ldots, x, \ldots)$ con $x \in K^*$.

Los *adèles principales* son los adèles de la forma $(\ldots, x, \ldots, x, \ldots)$ con $x \in K$.

La siguiente definición es el concepto central de la teoría global de campos de clase.

Definición 6.2.5. El *grupo de clases de idèles* C_K se define por J_K/K^* donde $K^* \xhookrightarrow{\mu} J_K$, $\mu(\vec{x}) = (\ldots, x, \ldots, x \ldots)$, esto es, $\mu(\vec{x})_v = x$ para toda $v \in \mathbb{P}_K$.

Los elementos de C_K los denotaremos por $\tilde{\vec{\alpha}}$ donde $\vec{\alpha} \in J_K$ es el representante del elemento de C_K.

Notación 6.2.6. Dado $\mathfrak{p} \in \mathbb{P}_K$, donde K es un campo global, $\mathfrak{p}|\infty$ significa que $\mathfrak{p}$ es arquimediano y $\mathfrak{p} \nmid \infty$ significa que $\mathfrak{p}$ es un primo finito.

Definición 6.2.7 (Valor absoluto de idèles). Se define el *valor absoluto* de J_K por $\| \ \| : J_K \longrightarrow \mathbb{R}^+ = \{x \in \mathbb{R} \mid x > 0\}$, por

$$\|\vec{\alpha}\| := \prod_{v\in\mathbb{P}_K} |\alpha_v|_v.$$

El valor absoluto está bien definido pues $|\alpha_v|_v = 1$ para casi toda v. Además es fácil verificar que el valor absoluto es un mapeo continuo, donde $\mathbb{R}^+$ tiene la topología usual de los números reales y la imágen de $\| \ \|$ tiene la topología inducida.

Se tiene que si $\vec{\alpha}$ y $\vec{\beta}$ están en la misma clase de equivalencia en C_K, entonces existe $x \in K^*$ tal que $\vec{\alpha} = x\vec{\beta}$ y como $\|x\| = 1$, se sigue que $\|\vec{\alpha}\| = \|\vec{\beta}\|$ por lo que se puede definir $\|\tilde{\vec{\alpha}}\|$ por

$$\|\tilde{\vec{\alpha}}\| = \|\vec{\alpha}\|.$$

Ahora bien, núc$\| \ \| = \{\vec{\alpha} \in J_K \mid \|\vec{\alpha}\| = \prod_{v \in \mathbb{P}_K} |\alpha_v|_v = 1\} =: J_{K,0}$. Se tiene que $K^* \subseteq J_{K,0}$.

Definición 6.2.8. El grupo $J_{K,0}$ recibe el nombre de *idèles de grado* 0 y el grupo $C_{K,0} := J_{K,0}/K^*$ recibe el nombre de *grupo de clases de idèles de grado* 0.

Si K es un campo de funciones, entonces $\|\vec{\alpha}\| = q^{-\operatorname{gr}\vec{\alpha}}$, es decir,

$$J_{K,0} = \{\vec{\alpha} \in J_K \mid \operatorname{gr}\vec{\alpha} = \sum_{\mathfrak{p} \in \mathbb{P}_K} \operatorname{gr}_{\mathfrak{p}} \alpha_{\mathfrak{p}} = 0\},$$

donde $\operatorname{gr}_{\mathfrak{p}} \alpha_{\mathfrak{p}} = \operatorname{gr}\mathfrak{p} \cdot v_{\mathfrak{p}}(\alpha_{\mathfrak{p}})$, $\operatorname{gr}\mathfrak{p} := \big[\mathcal{O}_{\mathfrak{p}}/\mathfrak{p} : \mathbb{F}_q\big]$, $\mathbb{F}_q$ el campo de constantes de K.

Para K un campo global, se tiene

$$C_K/C_{K,0} \cong J_K/J_{K,0} \cong \operatorname{im}\| \ \| =: \Delta$$
$$\cong \begin{cases} \mathbb{R}^+ & \text{si } K \text{ es numérico,} \\ q^{\mathbb{Z}} = \{q^n \mid n \in \mathbb{Z}\} \cong \mathbb{Z} & \text{si } K \text{ es campo de funciones} \end{cases}.$$

Veremos más adelante con detalle que las sucesiones exactas

$$1 \longrightarrow J_{K,0} \longrightarrow J_K \longrightarrow \Delta \longrightarrow 1, \qquad 1 \longrightarrow C_{K,0} \longrightarrow C_K \longrightarrow \Delta \longrightarrow 1,$$

se escinden tanto algebraica como topológicamente, es decir, tenemos que

$$C_K \cong C_{K,0} \times \Delta \qquad \text{y} \qquad J_K \cong J_{K,0} \times \Delta$$

tanto algebraica como topológicamente, donde $\Delta = \mathbb{R}^+$ si K es numérico y $\Delta \cong \mathbb{Z}$ si K es de funciones. La topología inducida de im$\| \ \|$ en $\mathbb{Z}$ es la topología discreta (Teorema 6.8.1).

La conexión de los idèles con los divisores y de varios grupos relacionados, nos la da la siguiente definición.

Definición 6.2.9. Sea K un campo global, J_K el grupo de idèles y D_K el grupo de divisores o de ideales fraccionarios. Se define el epimorfismo

$$\Lambda : J_K \longrightarrow D_K, \qquad \Lambda(\vec{\alpha}) = \mathfrak{a}_{\vec{\alpha}} = \prod_{\substack{\mathfrak{p} \in \mathbb{P}_K \\ \mathfrak{p} \nmid \infty}} \mathfrak{p}^{v_{\mathfrak{p}}(\alpha_{\mathfrak{p}})}.$$

Se tiene que

$$\text{núc}\,\Lambda = U_K := \prod_{\mathfrak{p}\in\mathbb{P}_K} U_{\mathfrak{p}} = \{\vec{\alpha}\in J_K \mid v_{\mathfrak{p}}(\alpha_{\mathfrak{p}}) = 0 \text{ para todo } \mathfrak{p} \text{ finito}\}$$
$$= \begin{cases} \prod_{\mathfrak{p}|\infty} K_{\mathfrak{p}}^* \times \prod_{\mathfrak{p}\nmid\infty} U_{\mathfrak{p}} & \text{si } K \text{ es numérico,} \\ \\ \prod_{\mathfrak{p}} U_{\mathfrak{p}} & \text{si } K \text{ es de funciones} \end{cases}.$$

Cuando K es campo de funciones, se tiene $\Lambda(J_{K,0}) = D_{K,0}$ y $U_K \subseteq J_{K,0}$. Entonces se tiene

$$\frac{J_K}{U_K} \cong D_K \text{ (K campo global)}, \qquad \frac{J_{K,0}}{U_K} \cong D_{K,0} \text{ (K campo de funciones)}.$$

Si K es campo numérico, se tiene $\Lambda(J_{K,0}) = D_K = D_{K,0}$. También tenemos para cualquier K campo global que $\Lambda(K^*) = P_K = \{(x)_K \mid x \in K^*\}$. Se sigue que

$$\Lambda : J_K/K^* \longrightarrow D_K/P_K \qquad \text{y} \qquad \text{núc}\,\Lambda = U_K K^*/K^*,$$
$$\Lambda : J_{K,0}/K^* \longrightarrow D_{K,0}/P_K \qquad \text{y} \qquad \text{núc}\,\Lambda = U_K K^*/K^*.$$

En particular, tenemos

$$J_K/U_K K^* \cong D_K/P_K = I_K \text{ grupo de clases de divisores},$$
$$J_{K,0}/U_K K^* \cong D_{K,0}/P_K = I_{K,0} \text{ grupo de clases de divisores de grado 0}.$$

Si K es numérico, $D_K/P_K = D_{K,0}/P_K = I_K = I_{K,0}$ es el grupo de clases y $h_K = |I_K| < \infty$. En el caso de K campo de funciones $h_K = |I_{K,0}|$ es finito y $I_K \cong I_{K,0} \oplus \mathbb{Z}$ es infinito.

6.2.1. Algo de topología para los idèles

Sea K un campo global. Se tiene que J_K es Hausdorff: si $\vec{\alpha} \neq \vec{\beta}$, entonces $\alpha_v \neq \beta_v$ para algún v y K_v^* es Hausdorff (simplemente por ser espacio métrico). Sean U y V conjuntos abiertos de K_v^*, $\alpha_v \in U, \beta_v \in V$ y $U \cap V = \emptyset$. Sean U_0 y V_0 dos abiertos de J_K con la componente de U_0 en v igual a U y la componente en v en V_0 igual a V y $\vec{\alpha} \in U_0$ y $\vec{\beta} \in V_0$ y $U_0 \cap V_0 = \emptyset$.

Sea $S_\infty = \{\mathfrak{p} \in \mathbb{P}_K \mid \mathfrak{p}|\infty\}$ el conjunto de los lugares arquimedianos de K y sea $S = S_\infty \cup \{v_0\}$ un conjunto no vacío finito de lugares. Ahora, cada K_v^* es localmente compacto. Sea V_v un abierto de K_v^* con $\bar{V}_v$ compacto y tal que $1 \in V_v$. Entonces $\vec{1} \in W = \prod_{v\in S} V_v \times \prod_{v\notin S} U_v$ y U_v es compacto. Por tanto W es una vecindad de $\vec{1}$ con cerradura compacta y por tanto J_K es localmente compacto.

Veamos a continuación una propiedad de J_K que nos es indispensable para probar el teorema de existencia. La propiedad en discusión es que si K es un

campo de funciones, J_K es totalmente disconexo y en general si K es un campo global $J_K^{\text{fin}} := \{\vec{\alpha} \in J_K \mid \alpha_v = 1 \text{ para } v|\infty\}$ es totalmente disconexo.

En efecto, sean $\vec{\alpha}, \vec{\beta} \in J_K^{\text{fin}}$ con $\vec{\alpha} \neq \vec{\beta}$. Existe v_0 finito con $\alpha_{v_0} \neq \beta_{v_0}$. Entonces $\alpha_{v_0}, \beta_{v_0} \in K_{v_0}^*$ y como $K_{v_0}^*$ es totalmente disconexo, existen V_0, W_0 abiertos de $K_{v_0}^*$, $K_{v_0}^* = V_0 \cup W_0$, $V_0 \cap W_0 = \emptyset$ y $\alpha_{v_0} \in V_0$, $\beta_{v_0} \in W_0$. Por tanto $\left(V_0 \times \prod_{v \neq v_0} K_v^*\right) \cap \left(W_0 \times \prod_{v \neq v_0} K_v^*\right) = \emptyset$ y el resultado se sigue.

En resumen, tenemos

Proposición 6.2.10. *Sea K un campo global, entonces J_K es Hausdorff, localmente compacto y J_K^{fin} es totalmente disconexo, donde $J_K^{fin} = \{\vec{\alpha} \mid \alpha_v = 1$ para $v|\infty\}$.* □

Corolario 6.2.11. *Si K es un campo de funciones, entonces C_K y $C_{K,0}$ son totalmente disconexos.*

Demostración. Se tiene que la proyección natural $J_K \twoheadrightarrow C_K$ es un mapeo continuo, suprayectivo y J_K es totalmente disconexo. □

Observación 6.2.12. Se tendrá que el mapeo global de reciprocidad $\rho_K : C_K \longrightarrow \text{Gal}(K^{\text{ab}}/K) = G_K^{\text{ab}}$, tiene núcleo $\mathfrak{N}_K$ que es la componente conexa de $\vec{1}$ en C_K. Por tanto ρ_K resultará ser inyectiva en el caso de campos de funciones. En el caso de campos numéricos la estructura de $\mathfrak{N}_K$ fue hallada por Tate. En el caso numérico, ρ_K es suprayectiva y no inyectiva.

Proposición 6.2.13. *Para cualquier campo global K, el subgrupo $C_{K,0}$ es cerrado de C_K. Si K es de funciones, entonces $C_{K,0}$ también es abierto. Si K es numérico, $C_{K,0}$ no es abierto en C_K.*

Demostración. Primero supongamos que K es de funciones. Entonces $U := \prod_{v \in \mathbb{P}_K} U_v$ es abierto en J_K por lo que $\tilde{U} := UK^*/K^*$ es abierto en C_K y además $\tilde{U} \subseteq C_{K,0}$. Si $\tilde{\vec{\alpha}} \in C_{K,0}$, entonces $\tilde{\vec{\alpha}}\tilde{U} \subseteq C_{K,0}$ probando que $C_{K,0}$ es abierto. El mismo argumento prueba que si $\tilde{\vec{\beta}} \notin \tilde{U}$, entonces $\tilde{\vec{\beta}}\tilde{U} \cap C_{K,0} = \emptyset$ probando que $C_{K,0}$ es cerrado.

De lo anterior obtenemos que $\text{gr} : C_K \longrightarrow \mathbb{Z}$, donde $\mathbb{Z}$ es considerado con la topología discreta, es una función continua pues $\text{gr}^{-1}(\{0\}) = C_{K,0}$ es tanto abierto como cerrado.

Si K es numérico, tenemos que si $\varphi := \| \ \|$, entonces φ es continua y $\{1\} \in \mathbb{R}^+$ es cerrado, por lo que $C_{K,0} = \varphi^{-1}(\{1\})$ es cerrado en C_K.

Es claro en el caso numérico que toda vecindad de $\tilde{\vec{1}}$ contiene elementos de valor absoluto diferente de 1 por lo que $C_{K,0}$ no es abierto. □

Corolario 6.2.14. *Si K es cualquier campo global, se tiene que C_K no es compacto.*

Demostración. Primero consideremos K numérico. Sea $\varphi = \| \ \|$ el valor absoluto de C_K. Sea $\{U_i\}_{i\in I}$ una cubierta abierta de $\mathbb{R}^+$ que no tenga subcubiertas finitas. Entonces $\left\{\varphi^{-1}(U_i)\right\}_{i\in I}$ es una cubierta abierta de C_K sin subcubiertas finitas.

Si K es de funciones, sea $\tilde{\vec{\alpha}}_1$ de grado 1. Entonces $\bigcup_{n\in\mathbb{Z}} \tilde{\vec{\alpha}}_1^n C_{K,0}$ es una cubierta abierta de C_K sin subcubiertas finitas. □

Proposición 6.2.15. *Se tiene para un campo global K que $K^* \subseteq J_K$ es un subgrupo discreto de J_K. En particular, K^* es cerrado en J_K.*

Demostración. Sea $S \subseteq \mathbb{P}_K$ un conjunto finito y no vacío de lugares conteniendo los lugares arquimedianos. Sea V la vecindad de $\vec{1}$ en J_K definido por $\vec{\alpha} \in V \iff |\alpha_v - 1|_v < 1$ para toda $v \in S$ y $|\alpha_v|_v = 1$ para toda $v \notin S$. Si $x \in K^*$, $x \neq 1$ se tiene que $\prod_{v\in\mathbb{P}_K} |x-1|_v = 1$. Si $x \in V$ se tendría que $|x-1|_v < 1$ para $v \in S$ y para $v \notin S$, $\max\{|x|_v, 1\} = \max\{1,1\} = 1$ y $|x-1|_v \leq \max\{|x|_v, 1\} = 1$. Se seguiría que

$$\prod_{v\in\mathbb{P}_K} |x-1|_v = \prod_{v\in S} |x-1|_v \cdot \prod_{v\notin S} |x-1|_v \leq \prod_{v\in S} |x-1|_v < 1.$$

Esta contradicción a la fórmula del producto prueba que $x \notin V$. Por tanto $V \cap K^* = \{1\}$ y por tanto K^* es discreto.

Por el Lema 3.3.8, K^* es cerrado pues J_K es Hausdorff. □

Observación 6.2.16. De manera similar, se prueba que K es un subgrupo discreto de $\mathbb{A}_K$

Observación 6.2.17. Se tiene que $\mathbb{A}_K^* = J_K$ (Observación 6.2.3), pero la topología de J_K no es la inducida por $\mathbb{A}_K$.

Ejemplo 6.2.18. Sea $K = \mathbb{Q}$. Sea $\vec{x}_p$ el adèle cuya p-componente es p y cuya v-componente es 1 para $v \neq p$. Veamos que $\vec{x}_p \xrightarrow[p\to\infty]{} \vec{1}$ en la topología de $\mathbb{A}_\mathbb{Q}$.

Sea V un abierto básico conteniendo a $\vec{1}$. Puesto que $V = \prod_{v\in S} W_v \times \prod_{v\notin S} \mathcal{O}_v$, W_v abierto de K_v para $v \in S$. Entonces, existe p_0 un número primo tal que para toda $p \geq p_0$ se tiene que $p \notin S$. De esta forma, tenemos que $p \in \mathcal{O}_p = \mathbb{Z}_p$. Se sigue que $\vec{x}_p \in V$ para toda $p \geq p_0$ y por tanto $\lim_{p\to\infty} \vec{x}_p = \vec{1}$.

Si la inversión fuese continua en $\mathbb{A}_\mathbb{Q}$, entonces la sucesión $\vec{x}_p^{-1}$ convergería a $\vec{1}^{-1} = \vec{1}$, sin embargo, si V es un conjunto abierto conteniendo a $\vec{1}$, entonces para toda $p \geq p_0$, $p^{-1} \notin \mathcal{O}_p = \mathbb{Z}_p$. Por tanto $\vec{x}_p^{-1} \notin V$ para toda $p \geq p_0$.

Esto prueba que el mapeo $\vec{x} \longrightarrow \vec{x}^{-1}$ no es continua en la topología de $\mathbb{A}_\mathbb{Q}$ restringida a $\mathbb{A}_\mathbb{Q}^* = J_\mathbb{Q}$. La razón es que p^{-1} no es unidad en $\mathbb{Z}_p$ y que $p \to \infty$.

Ahora bien, en la topología de J_K, donde K es un campo global arbitrario, sea $\varphi : J_K \longrightarrow J_K$ dada por $\varphi(\vec{\alpha}) = \vec{\alpha}^{-1}$. Sea $\mathcal{W} = \prod_{v\in S} W_v \times \prod_{v\notin S} U_v$ un abierto básico de J_K, por tanto $\varphi^{-1}(\mathcal{W}) = \prod_{v\in S} W_v^{-1} \times \prod_{v\notin S} U_v^{-1}$ y si W_v es

abierto en K_v^*, entonces W_v^{-1} es abierto en K_v^* por ser K_v^* un grupo topológico y además $U_v^{-1} = U_v$, por lo que φ^{-1} es un abierto en J_K y φ es continua.

Por tanto J_K es un grupo topológico. Se puede probar que la topología dada a J_K está dada de la siguiente forma: Sea $\mu : J_K \hookrightarrow \mathbb{A}_K \times \mathbb{A}_K$ dada por $\mu(\vec{\alpha}) = \left(\vec{\alpha}, \frac{1}{\vec{\alpha}}\right)$. Entonces los abiertos de J_K son $\mu(J_K) \cap (V \times W)$ donde V y W son conjuntos abiertos de $\mathbb{A}_K$.

Lema 6.2.19. *Sea K un campo global y sea L/K una extensión finita y separable. Entonces*

$$\mathbb{A}_K \otimes_K L \cong \mathbb{A}_L$$

algebraica y topológicamente. En esta correspondencia, tenemos que $K \otimes_K L = L \subseteq \mathbb{A}_K \otimes_K L$ donde $K \subseteq \mathbb{A}_K$ se inyecta en $L \subseteq \mathbb{A}_L$.

Demostración. Primero estableceremos el isomorfismo como espacios topológicos. Sea $\{\alpha_1, \ldots, \alpha_n\}$ base de L/K y sea v que recorre los valores absolutos finitos normalizados de K. Se tiene que, $\mathbb{A}_K \otimes_K L$ con la topología del producto tensorial, es el producto restringido de

$$K_v \otimes_K L = K_v\alpha_1 \oplus \cdots \oplus K_v\alpha_n \tag{6.2.1}$$

con respecto a

$$\mathcal{O}_K\alpha_1 \oplus \cdots \oplus \mathcal{O}_v\alpha_n. \tag{6.2.2}$$

Ahora bien, se tiene

$$K_v \otimes_K L = L_{\omega_1} \oplus \cdots \oplus L_{\omega_r}, \tag{6.2.3}$$

donde $\omega_1, \ldots, \omega_r$ son los valores absolutos que son extensiones de v y bajo esta identificación de (6.2.1) con (6.2.3), se identifica (6.2.2) con $\mathcal{O}_{\omega_1} \oplus \cdots \oplus \mathcal{O}_{\omega_r}$. Así, el producto restringido de $\mathbb{A}_K \otimes_K L$ con respecto a $K_v \otimes_K L$ es isomorfo topológicamente al producto restringido de los L_ω con respecto a $\mathcal{O}_\omega$. Este isomorfismo también es algebraico. □

Corolario 6.2.20. *Sea $\mathbb{A}_K^+$ la parte aditiva de $\mathbb{A}_K$. Entonces*

$$\mathbb{A}_L^+ \cong \underbrace{\mathbb{A}_K^+ \oplus \cdots \oplus \mathbb{A}_K^+}_{n=[L:K]}.$$

En este isomorfismo se tiene $L \subseteq \mathbb{A}_L^+$, el subgrupo de los adèles principales, se manda en $K \oplus \cdots \oplus K$.

Demostración. Para $x \in L$, $x \neq 0$, $x\mathbb{A}_K^+ \subseteq \mathbb{A}_L^+$ y $x\mathbb{A}_K \cong \mathbb{A}_K^+$ como grupos topológicos. Por tanto

$$\mathbb{A}_L^+ \cong \mathbb{A}_K^+ \otimes_K L \cong \alpha_1\mathbb{A}_K^+ \oplus \cdots \oplus \alpha_n\mathbb{A}_K^+ \cong \mathbb{A}_K^+ \oplus \cdots \oplus \mathbb{A}_K^+.$$ □

Del Corolario 6.2.14, tenemos que $J_K/K^* = C_K$ no es compacto. Sin embargo, para los adèles, tenemos:

Teorema 6.2.21. *K es discreto en $\mathbb{A}_K$ y $\mathbb{A}_K^+/K$ es compacto en la topología cociente.*

Demostración. Por el Corolario 6.2.20, basta probar el teorema para $K = \mathbb{Q}$ en el caso numérico y para $K = \mathbb{F}_q(T)$ en el caso de campos de funciones.

Denotamos por ∞ al valor absoluto usual si $K = \mathbb{Q}$ y por el valor absoluto a $\frac{1}{T}$ si $K = \mathbb{F}_q(T)$. Sea $W \subseteq \mathbb{A}_K^+$ el conjunto definido por $W = \{\vec{\alpha} \in \mathbb{A}_K^+ \mid |\alpha_\infty|_\infty \leq \frac{1}{2}, |\alpha_v|_v \leq 1 \text{ para todo } v \neq \infty\}$. Veamos que $\mathbb{A}_K^+ = K + W$.

Sea $\vec{\alpha} \in \mathbb{A}_K^+$. Para cada $v \neq \infty$, sea $v = p \in \mathbb{Z}$ un número primo o $p \in R_T^+$, donde R_T^+ denota al conjunto de los polinomios mónicos irreducibles de $R_T = \mathbb{F}_q[T]$. Podemos hallar $r_v = r_p = z_p/p^{x_p}$ con $x_p \in \mathbb{Z}$ o R_T y y $x_p \in \mathbb{Z}$, $x_p \geq 0$ tal que

$$|\alpha_v - r_v|_v = |\alpha_p - r_p|_p \leq 1.$$

Puesto que $\vec{\alpha} \in \mathbb{A}_K^+$, se tiene $r_v = 0$ para casi toda v. Sea $r := \sum_{v \neq \infty} r_v$. Se tiene $|\alpha_v - r|_v \leq 1$ para toda $v \neq \infty$.

Sea $s \in \mathbb{Z}$ o $s \in R_T$ con $|\alpha_\infty - r - s|_\infty \leq \frac{1}{2}$. Sea $\vec{\beta} = \vec{\alpha} - (r + s)$, $\vec{\alpha} = \vec{\beta} + (r + s)$. Se tiene $\beta_v = \alpha_v - (r + s)$, $|\beta_v|_v = |\alpha_v - (r + s)|_v \leq$ máx$\{|\alpha_v - r|_v, |s|_v\} \leq 1$ para toda $v \neq \infty$. Además $|\beta|_\infty = |\alpha_\infty - r - s|_\infty \leq \frac{1}{2}$.

Se tiene que $W \twoheadrightarrow \mathbb{A}_K^+/K$ es un epimorfismo continuo y W es compacto, de donde se sigue que $\mathbb{A}_K^+/K$ es compacto. □

Corolario 6.2.22. *Sea K un campo global. Existe $W_0 \subseteq \mathbb{A}_K$ compacto con $W_0 := \{\vec{\xi} \in \mathbb{A}_K \mid |\xi_v|_v \leq \delta_v \text{ para toda } v \in \mathbb{P}_K \text{ y } \delta_v = 1 \text{ para casi toda } v\}$ y tal que $\mathbb{A}_K = W_0 + K$.*

Demostración. Se sigue inmediatamente de la demostración del Teorema 6.2.21. □

6.2.2. Medida de Haar

Sea G un grupo topológico localmente compacto. Entonces, salvo una constante positiva, existe una única medida no trivial μ en los subgrupos de Borel, esto es, los elementos del álgebra de Borel que es la generada por los conjuntos abiertos de G, la cual es numerablemente aditiva y tal que satisface lo siguiente:

(1) μ es invariante bajo translaciones por la izquierda: $\mu(gS) = \mu(S)$ para toda $g \in G$ y para todo conjunto de Borel S.
(2) μ es finita en conjuntos compactos $T \subseteq G$: $\mu(T) < \infty$ para T compacto.
(3) μ es regular por fuera para todo subgrupo de Borel: $\mu(S) = \text{ínf}\{\mu(U) \mid S \subseteq U, U \text{ abierto}\}$.

(4) μ es regular por dentro para conjuntos abiertos U: $\mu(U) = \sup\{\mu(T) \mid T \subseteq U, T \text{ compacto}\}$.

Se puede probar que $\mu(U) > 0$ para todo conjunto abierto U de G con U no vacío. En particular, si G es compacto, $\mu(G) < \infty$ y se puede normalizar para que $\mu(G) = 1$.

De igual manera, se puede definir un única medida (salvo constantes positivas) por la derecha. Sin embargo estas dos medidas no coinciden en general.

Proposición 6.2.23. *Sea K un campo global. Existe una constante $C > 0$ que depende únicamente de K con la siguiente propiedad: si $\vec{\alpha} \in \mathbb{A}_K$ satisface*

$$\prod_v |\alpha_v|_v > C, \tag{6.2.4}$$

entonces existe $\beta \in K$, $\beta \neq 0$ tal que $|\beta|_v \leq |\alpha|_v$ para toda $v \in \mathbb{P}_K$.

Demostración. Primero consideremos cualquier constante $C > 0$ y un idèle $\vec{\alpha}$ que satisface (6.2.4). Puesto que para casi toda v se tiene $|\alpha_v|_v \leq 1$, entonces se sigue que $|\alpha_v|_v = 1$ para casi toda v pues de lo contrario, si para v finito se tiene $|\alpha_v|_v < 1$ entonces $|\alpha_v|_v \leq q_v^{-1}$ y por tanto si tuviésemos esta situación para una infinidad de primos finitos v, entonces $\prod_v |\alpha_v|_v = 0$.

Sean c_0 la medida de Haar μ de $\mathbb{A}_K^+/K$ y c_1 es la medida de Haar del conjunto $A = \{\vec{\gamma} \mid |\gamma_v|_v \leq \frac{1}{10}$ si $v|\infty$ y $|\gamma_v|_v \leq 1$ si $v \nmid \infty\}$. Se tiene que por ser $\mathbb{A}_K^+/K$ compacto, lo mismo que A pues el número de $v|\infty$ es finito, entonces $0 < c_0 < \infty$ y $0 < c_1 < \infty$. Veamos que $C = \frac{c_0}{c_1}$ satisfacen las condiciones de la propisición.

Sea $\vec{\alpha}$ que satisface (6.2.4) con $C = \frac{c_0}{c_1}$. El conjunto $T := \{\vec{\gamma} \mid |\gamma_v|_v \leq \frac{1}{10}|\alpha_v|_v, V| \, |, |\tau_v|_v \leq |\alpha_v|_v, v \nmid \infty\}$ tiene medida igual a $c_1 \cdot \prod_v |\alpha_v|_v > c_1 C = C_0 = \mu\big(\mathbb{A}_K^+/K\big)$. Se sigue que el epimorfismo natural $\mathbb{A}_K^+ \twoheadrightarrow \mathbb{A}_K^+/K$ debe tener dos elementos distintos $\vec{\tau}', \vec{\tau}''$ en T con la misma imágen debido a que $\mu(T) > \mu\big(\mathbb{A}_K^+/K\big)$, y por tanto $\vec{\tau}' - \vec{\tau}'' = \beta \in K$. Por tanto,

$$|\beta|_v = |\tau_v' - \tau_v''|_v \leq |\alpha_v|_v$$

para toda v. □

Corolario 6.2.24. *Sea v_0 un valor absoluto normalizado y sean $\delta_v > 0$ dados para $v \neq v_0$ tales que $\delta_v = 1$ para casi toda v. Entonces existe $\beta \in K$ con $\beta \neq 0$ con $|\beta_v|_v \leq \delta_v$ para todo $v \neq v_0$.*

Demostración. Seleccionamos $\alpha_v \in K_v$ con $0 < |\alpha_v|_v \leq \delta_v$ y $|\alpha_v|_v = 1$ si $\delta_v = 1$. Sea $\alpha_{v_0} \in K_{v_0}$ tal que $\prod_{v \in \mathbb{P}_K} |\alpha_v|_v > C$. Por la Proposición 6.2.23 tenemos que existe $\beta \in K$, $\beta \neq 0$ que satisface lo requerido. □

A continuación presentamos el teorema de aproximación fuerte. Una versión para campos de funciones se puede encontrar en [136, Teorema 8.3.8] cuya demostración usa el Teorema de Riemann-Roch y donde el campo de funciones es arbitrario y no únicamente global. El resultado que ahora presentamos es válido para cualquier campo global.

Teorema 6.2.25 (Teorema de aproximación fuerte). *Sea K un campo global y sea v_0 cualquier valor absoluto de K. Sea V el producto restringido de los K_v con respecto a $\mathcal{O}_v$ para toda $v \neq v_0$. Entonces K es denso en V.*

En otras palabras, dados $S = \{v_1, \ldots, v_n\} \subseteq \mathbb{P}_K$ con $v_0 \notin S$, $\epsilon_1, \ldots, \epsilon_n > 0$ y $\vec{\alpha} \in \mathbb{A}_K$, entonces existe $\beta \in K$ con

$$|\beta - \alpha_{v_i}|_{v_i} < \epsilon_i, \quad 1 \leq i \leq n \quad y \quad |\beta|_v \leq 1 \quad \text{para toda } v \notin S \cup \{v_0\}.$$

Demostración. Existe $W \subseteq \mathbb{A}_K$ con $\{\vec{\xi} \mid |\xi_v|_v \leq \delta_v \text{ y } \delta_v = 1 \text{ para casi toda } v\}$ y con $\mathbb{A}_K = K + W$ (Corolario 6.2.22). Del Corolario 6.2.24 tenemos que existe $\lambda \in K$, $\lambda \neq 0$ tal que

$$\begin{aligned} |\lambda|_v &< \delta_v^{-1}\epsilon \quad v \in S, \\ |\lambda|_v &\leq \delta_v^{-1}, \quad v \notin S, v \neq v_0, \end{aligned}$$

con $\epsilon = \text{mín}\{\epsilon_1, \ldots, \epsilon_n\}$.

Dada $\vec{\alpha} \in \mathbb{A}_K$, si $\vec{\gamma} := \lambda^{-1}\vec{\alpha}$, existe $\vec{\xi} \in W$ tal que $\vec{\gamma} = \vec{\xi} + \nu$ para algún $\nu \in K$. Se sigue que $\vec{\alpha} = \lambda\vec{\xi} + \lambda\nu$. Por tanto $\mathbb{A}_K = \lambda W + K$.

Sea $\vec{\mu} \in \mathbb{A}_K$ definido por: $(\vec{\mu})_{v_i} = \alpha_{v_i}$, $1 \leq i \leq n$ y $(\vec{\mu})_v = 0$ para $v \notin S$. Sean $\vec{\xi} \in W$ y $\beta \in K$ tales que $\vec{\mu} = \lambda\vec{\xi} + \beta$. Se tiene

$$\begin{aligned} &|\beta - \alpha_{v_i}|_{v_i} = |\lambda\xi_{v_i}|_{v_i} \leq |\lambda|_{v_i}\delta_{v_i} < \epsilon \quad \text{y} \\ &|\beta - \alpha_v|_v = |\beta|_v = |\lambda\xi_v|_v = |\lambda|_v|\xi_v|_v \leq \delta_v^{-1}\delta_v = 1, v \notin S \cup \{v_0\}. \end{aligned}$$ □

Lema 6.2.26. *El subgrupo $J_{K,0}$ es cerrado en $\mathbb{A}_K$ en la topología de $\mathbb{A}_K$. Por otro lado, las topologías inducidas, tanto de $\mathbb{A}_K$ como de J_K en $J_{K,0}$.*

Demostración. Sea $\vec{\alpha} \in \mathbb{A}_K$ tal que $\vec{\alpha} \notin J_{K,0}$. Debemos hallar una vecindad W de $\vec{\alpha}$ con $W \cap J_{K,0} = \emptyset$. Se tiene $|\alpha_v|_v \leq 1$ para casi toda $v \in \mathbb{P}_K$ y por tanto el producto infinito $C := \prod_{v \in \mathbb{P}_K} |\alpha_v|_v \in \{x \in \mathbb{R} \mid x \geq 0\}$ puesto que en la serie $\sum_v \log|\alpha_v|_v$ se tiene que $\log|\alpha_v|_v \leq 0$ para casi toda v, esto es, $\sum_v \log|\alpha_v|_v \neq \infty$.

(a) Caso en que $C < 1$. Puesto que $\vec{\alpha}$ es un adèle, únicamente un número finito de lugares de K satisfacen que $|\alpha_v|_v \geq 1$. Puesto que $C < 1$, existe un conjunto finito S de lugares de K tal que si $|\alpha_v|_v \geq 1$, entonces $v \in S$ y se tiene además $\prod_{v \in S} |\alpha_v|_v < 1$. Sea $W := \{\vec{\xi} \mid |\xi_v - \alpha_v|_v < \epsilon, v \in S, |\xi_v|_v \leq 1, v \notin S\}$ con ϵ suficientemente pequeño. Se tiene que si $\vec{\xi} \in W$, entonces

$$\prod_{v \in \mathbb{P}_K} |\xi_v|_v = \prod_{v \in S} |\xi_v|_v \cdot \prod_{v \notin S} |\xi_v|_v \leq \prod_{v \in S} \left(|\alpha_v|_v + \epsilon\right) < 1.$$

Se sigue que $W \cap J_{K,0} = \emptyset$ y $\vec{\alpha} \in W$.

(b) Caso en que $C \geq 1$. Puesto que $\vec{\alpha} \notin J_{K,0}$, $C > 1$. Probemos primero que, en este caso, $\vec{\alpha} \in J_K$. Para v finito, si $|x|_v < 1$, entonces $|x|_v \leq \frac{1}{q_v} = q_v^{-1}$, q_v la cardinalidad del campo residual de K_v.

De esta forma, existe un conjunto finito S de lugares, tales que si $v \notin S$, entonces $|\alpha_v|_v = 1$ o $|\alpha_v|_v \leq \frac{1}{2}$ pues como $\vec{\alpha}$ es un adèle, $|\alpha_v|_v \leq 1$ para $v \notin S$ ($\alpha_v \in \mathcal{O}_v$).

Puesto que $\prod_{v \in \mathbb{P}_K} |\alpha_v|_v$ converge a $C > 0$ ($C \geq 1$), $|\alpha_v|_v \xrightarrow[v \to \infty]{} 1$. Por tanto, para un número finito de lugares v, se tiene $|\alpha_v|_v \leq \frac{1}{2}$. Así, agregando un número finito de lugares, podemos tomar S tal que $|\alpha_v|_v = 1$ para toda $v \notin S$ y por tanto $\vec{\alpha} \in J_K$ pues $\alpha_v \neq 0$ para todo $v \in \mathbb{P}_K$ y $C > 1$.

Ampliando nuevamente S en caso de ser necesario, podemos suponer que si $v \notin S$ y $|\alpha_v|_v < 1$ entonces $|\alpha_v|_v < (2C)^{-1}$ pues el número de lugares de grado menor o igual a n es finito y $q_v = q^{n_v}$, por lo que tomamos $\frac{1}{q_v} < \frac{1}{2C}$. Nuevamente, ampliando S, podemos suponer que

$$1 < \prod_{v \in S} |\alpha_v|_v < 2C.$$

Para $\epsilon > 0$ pequeño, si $|\xi_v - \alpha_v|_v < \epsilon$ para $v \in S$ se tiene

$$-\epsilon + |\alpha_v|_v < |\xi_v|_v < \epsilon + |\alpha_v|_v \quad \text{y}$$
$$\prod_{v \in S} \big(|\alpha_v|_v - \epsilon\big) < \prod_{v \in S} |\xi_v|_v < \prod_{v \in S} \big(\epsilon + |\alpha_v|_v\big).$$

Tomamos ϵ suficientemente pequeño de tal forma que

$$\prod_{v \in S} \big(|\alpha_v|_v - \epsilon\big) > 1 \quad \text{y} \quad \prod_{v \in S} \big(\epsilon + |\alpha_v|_v\big) < 2C.$$

Así, sea $W := \{\vec{\xi} \mid |\xi_v - \alpha_v|_v < \epsilon, v \in S \text{ y } |\xi_v|_v \leq 1, v \notin S\}$. Si $\vec{\xi} \in W$, $\|\vec{\xi}\| \neq 1$ pues si $v \notin S$, $|\xi_v|_v = 1$ o $|\xi_v|_v < (2C)^{-1}$. Así, si existe $v_0 \notin S$ con $|\xi_{v_0}|_{v_0} < (2C)^{-1}$, entonces

$$\|\vec{\xi}\| = \prod_{v \in S} |\xi_v|_v \cdot |\xi_{v_0}|_{v_0} \cdot \prod_{v \notin S \cup \{v_0\}} |\xi_v|_v < 2C \cdot \frac{1}{2C} \cdot 1 = 1,$$

esto es $\|\vec{\xi}\| < 1$.

Si para toda $v \notin S$, $|\xi_v|_v = 1$, $\|\vec{\xi}\| = \prod_{v \in S} |\xi_v|_v > 1$. Por tanto $\|\vec{\xi}\| \neq 1$ y $\vec{\xi} \notin J_{K,0}$, $\vec{\alpha} \in W$ abierto en $\mathbb{A}_K$ y $W \cap J_{K,0} = \emptyset$. Por tanto $J_{K,0}$ es cerrado en $\mathbb{A}_K$.

Sea $\vec{\alpha} \in J_{K,0}$, en particular $\alpha_v \in \mathcal{O}_v^* \subseteq \mathcal{O}_v$ para casi toda v. Una vecindad de $\vec{\alpha}$ en $\mathbb{A}_K$ es una vecindad de la forma $\vec{\alpha} + W$ con $W = \prod_{v \in S} V_v \times \prod_{v \notin S} \mathcal{O}_v$ con S un conjunto finito y V_v un conjunto abierto de K_v. Queremos hallar un

conjunto $W_0 = \prod_{v\in T} X_v \times \prod_{v\notin T} \mathcal{O}_v^*$ con X_v un conjunto abierto de K_v^*, T un conjunto finito, y tal que se tenga $\vec{\alpha}W_0 \subseteq \vec{\alpha} + W$, $\vec{\alpha}W_0$ es una vecindad de $\vec{\alpha}$ en J_K.

Pongamos $W = \prod_v Y_v$. Sea $W_0 = \prod_v X_v$. Se necesita $\alpha_v x_v = \alpha_v + y_v$, lo cual es equivalente a que $x_v = 1 + \alpha_v^{-1} y_v \in (1 + \alpha_v^{-1} Y_v) \cap K_v^*$. Esto es, $X_v \subseteq (1 + \alpha_v^{-1} Y_v) \cap K_v^*$ para toda v. Como $1 + \alpha_v^{-1} Y_v$ es abierto en K_v, se tiene que $(1+\alpha_v^{-1} Y_v) \cap K_v^*$ es abierto en K_v^* para toda v y además claramente $(1 + \alpha_v^{-1} Y_v) \cap K_v^* \neq \emptyset$.

Por otro lado, se tiene $\alpha_v \in \mathcal{O}_v^*$ y $Y_v = \mathcal{O}_v$ para casi toda v. Se sigue que $(1 + \alpha_v^{-1} Y_v) = 1 + \mathcal{O}_v = \mathcal{O}_v$ para casi toda v. Podemos definir $X_v = (1 + \alpha_v^{-1} Y_v) \cap \mathcal{O}_v^* = \mathcal{O}_v^*$ para casi toda v y $X_v = (1 + \alpha_v^{-1} Y_v) \cap K_v^*$ para el resto. De esto se sigue que la $\mathbb{A}_K$-topología de $J_{K,0}$ contiene a la J_K-topología.

Recíprocamente, sea ahora H una J_K-vecindad de $\vec{\alpha}$. Entonces H contiene una J_K-vecindad de la forma $|\xi_v - \alpha_v|_v < \epsilon$ para $v \in S$ y $|\xi_v|_v = 1$ para $v \notin S$ y donde S contiene a todos los v arquimedianos: $v|\infty$ y a todos los v tales que $|\alpha_v|_v \neq 1$. Puesto que $\vec{\alpha} \in J_{K,0}$, se tiene $\|\vec{\alpha}\| = \prod_v |\alpha_v|_v = 1$. Se tiene que para $v \notin S$, si $|\xi_v|_v < 1$, entonces $|\xi_v|_v \leq \frac{1}{2}$ por ser v un lugar finito. Sea ϵ tal que para $\vec{\xi} \in J_{K,0} \cap H$ se tiene $|\xi_v - \alpha_v|_v < \epsilon$ para $v \in S$ y $|\xi_v|_v \leq 1$ para $v \notin S$ de tal forma que se satisface

$$\prod_{v\in S} |\xi_v|_v < \prod_{v\in S} \left(|\alpha_v|_v + \epsilon\right) < 2.$$

Entonces $|\xi_v|_v = 1$ para $v \notin S$ pues de lo contrario existiría $v \notin S$ con $|\xi_v|_v \leq \frac{1}{2}$ y por tanto

$$1 = \|\vec{\xi}\| = \prod_v |\xi_v|_v = \prod_{v\in S} |\xi_v|_v \cdot \prod_{v\notin S} |\xi_v|_v < 2 \cdot \frac{1}{2} = 1,$$

lo cual es absurdo. Se sigue que $\xi_v \in \mathcal{O}_v^*$. Por tanto $H \cap J_{K,0}$ contiene una $\mathbb{A}_K$-vecindad de $\vec{\alpha}$ de $J_{K,0}$, esto es, contiene a $\vec{\alpha} + H_0$, $H_0 := \prod_{v\in S} V_v \times \prod_{v\notin S} \mathcal{O}_v$. □

Teorema 6.2.27. *Sea K un campo global. Se tiene que el grupo $C_{K,0} = J_{K,0}/K^*$ es compacto con respecto a la topología cociente.*

Demostración. Por el Lema 6.2.26 es suficiente hallar un conjunto $W \subseteq \mathbb{A}_K$ compacto en la topología de $\mathbb{A}_K$ tal que la proyección natural $W \cap J_{K,0} \twoheadrightarrow J_{K,0}/ * K$ sea suprayectiva.

Sea $W = \{\vec{\xi} \in \mathbb{A}_K \mid |\xi_v|_v \leq |\alpha_v|_v\}$ donde $\vec{\alpha}$ es cualquier idèle de norma mayor a la constante C de la Proposición 6.2.23. Se tiene que W es compacto. Sea $\vec{\beta} \in J_{K,0}$. Se tiene que

$$\|\vec{\beta}^{-1}\vec{\alpha}\| = \|\vec{\beta}^{-1}\|\|\vec{\alpha}\| > 1 \cdot C = C,$$

por lo que existe $\mu \in K^*$ tal que

$$|\mu|_v \leq |\beta_v^{-1}\alpha_v|_v \quad \text{para toda } v.$$

Se sigue que $\mu\vec{\beta} \in W$ y $\mu\vec{\beta} \longmapsto \mu\vec{\beta}$ mód $K^* = \vec{\beta}$ mód K^*. □

Sea K un campo numérico y sea $\Lambda : J_K \longrightarrow D_K$ dada por $\Lambda(\vec{\alpha}) = \mathfrak{a}_{\vec{\alpha}} = \prod_{\mathfrak{p}\nmid\infty} \mathfrak{p}^{v_\mathfrak{p}(\alpha_\mathfrak{p})}$, donde D_K, el grupo de ideales fraccionarios, tiene la topología discreta. Se tiene $\Lambda(K^*) = P_K$ y $D_K/P_K = I_K$ es el grupo de clases de K. Puesto que hay al menos un lugar arquimediano, Λ induce un epimorfismo continuo $J_{K,0}/K^* \xrightarrow{\tilde{\Lambda}} I_K$.

Similarmente, si K es un campo de funciones y $I_{K,0}$ denota el grupo de clases de divisores de grado 0,

$$J_{K,0}/K^* \xrightarrow{\tilde{\Lambda}} I_{K,0}$$

es un epimorfismo continuo donde $D_{K,0}$ tiene la topología discreta. Se sigue que I_K en el caso numérico y $I_{K,0}$ en el caso de campos de funciones son compactos y discretos, por lo tanto finitos.

Teorema 6.2.28. *Si K es un campo numérico y I_K es el grupo de clases de K, $I_K = D_K/P_K$ es finito.*

Si K es un campo de funciones y $I_{K,0} = D_{K,0}/P_K$ es el grupo de clases de divisores de grado 0 de K, entonces $I_{K,0}$ es finito. □

Definición 6.2.29. Sea S un conjunto finito de lugares de un campo global que contiene a los primos infinitos. Se define el *grupo de los S-idèles* por

$$J_{K,S} = \prod_{v\in S} K_v^* \times \prod_{v\notin S} \mathcal{O}_v^* = \prod_{v\in S} K_v^* \times \prod_{v\notin S} U_v.$$

Se tiene $J_K = \bigcup_{S \text{ finito}} J_{K,S}$.

Proposición 6.2.30. *Si K es un campo numérico y $S = S_\infty = \{v \in \mathbb{P}_K \mid v|\infty\}$, entonces $J_K/J_{K,S_\infty} = D_K$ y $J_K/J_{K,S_\infty}K^* \cong D_K/P_K \cong I_K$.*

Demostración. Nuevamente usamos el epimorfismo $\Lambda : J_K \longrightarrow D_K$, $\Lambda(\vec{\alpha}) = \mathfrak{a}_{\vec{\alpha}} = \prod_{\mathfrak{p}\nmid\infty} \mathfrak{p}^{v_\mathfrak{p}(\alpha_\mathfrak{p})}$ y se tiene que núc $\Lambda = J_{K,S_\infty}$ de donde $D_K \cong J_K/J_{K,S_\infty}$.

Similarmente, $\tilde{\Lambda} : J_K \xrightarrow{\Lambda} D_K \xrightarrow{\pi} D_K/P_K = I_K$ es un epimorfismo y

$$\vec{\alpha} \in \text{núc}\,\tilde{\Lambda} \iff \prod_{\mathfrak{p}\nmid\infty} \mathfrak{p}^{v_\mathfrak{p}(\alpha_\mathfrak{p})} \in P_K,$$

$$\text{esto es,} \quad \prod_{\mathfrak{p}\nmid\infty} \mathfrak{p}^{v_\mathfrak{p}(\alpha_\mathfrak{p})} = (x) = \prod_{\mathfrak{p}\nmid\infty} \mathfrak{p}^{v_\mathfrak{p}(x)}, \quad x \in K^*$$

$$\iff v_\mathfrak{p}(\alpha_\mathfrak{p}) = v_\mathfrak{p}(x) \quad \text{para toda} \quad \mathfrak{p} \nmid \infty$$

$$\iff v_\mathfrak{p}(\alpha_\mathfrak{p} x^{-1}) = 0 \quad \text{para toda} \quad \mathfrak{p} \nmid \infty$$

$$\iff \vec{\alpha}x^{-1} \in J_{K,S_\infty} \iff \vec{\alpha} \in J_{K,S_\infty}K^*.$$

Por tanto núc $\tilde{\Lambda} = J_{K,S_\infty}K^*$. □

Teorema 6.2.31. *Sea K un campo global. Existe S, un conjunto finito suficientemente grande tal que $J_K = J_{K,S}K^*$ y*

$$C_K = J_K/K^* = J_{K,S}K^*/K^* \cong J_{K,S}/(J_{K,S} \cap K^*).$$

Demostración. Primero consideremos el caso de K de un campo numérico. Se tiene que $I_K = D_K/P_K$ es finito. Sean $\mathfrak{a}_1, \ldots, \mathfrak{a}_n$ ideales que representen a todos los elementos de I_K. Tomando la descomposición de los ideales $\mathfrak{a}_1, \ldots, \mathfrak{a}_n$ en producto de primos, se obtiene un número finito de ideales primos $\mathfrak{p}_1, \ldots, \mathfrak{p}_s$ que son los diversos divisores primos de los ideales $\mathfrak{a}_i$'s.

Sea S cualquier conjunto finito que contenga a $\{\mathfrak{p}_1, \ldots, \mathfrak{p}_s\}$ y a los primos $\mathfrak{p}|\infty$. Sea $\Lambda_0 : J_K/J_{K,S_\infty} \xrightarrow{\cong} D_K$. Sea $\vec{\alpha} \in J_K$, $\Lambda_0(\vec{\alpha}) = \mathfrak{a} = \prod_{\mathfrak{p}\nmid\infty} \mathfrak{p}^{v_\mathfrak{p}(\alpha_\mathfrak{p})} \in \mathfrak{a}_i \cdot P_K$ para algún i. Esto es, $\mathfrak{a} = \mathfrak{a}_i \cdot (x)$ con $(x) \in P_K$, $x \in K^*$. Se tiene que

$$\vec{\alpha'} = \vec{\alpha} \cdot x^{-1} \xrightarrow{\Lambda_0} \mathfrak{a}' = \prod_{\mathfrak{p}\nmid\infty} \mathfrak{p}^{v_\mathfrak{p}(\vec{\alpha'})} = \prod_{\mathfrak{p}\nmid\infty} \mathfrak{p}^{v_\mathfrak{p}(\alpha_\mathfrak{p})-v_\mathfrak{p}(x)} = \mathfrak{a} \cdot (x)^{-1} = \mathfrak{a}_i.$$

Ahora, las componentes primas de $\mathfrak{a}_i$ pertenecen a S, por lo que $v_\mathfrak{p}(\mathfrak{a}') = v_\mathfrak{p}(\alpha'_\mathfrak{p}) = 0$ para $\mathfrak{p} \notin S$. Se sigue que $\vec{\alpha'} \in J_{K,S}$, de donde $\vec{\alpha} = \vec{\alpha'} \cdot x \in J_{K,S}K^*$ y $J_K = J_{K,S}K^*$.

Ahora consideremos el caso de un campo de funciones con campo de constantes $\mathbb{F}_q$. Sea v_0 un primo cualquiera de $\mathbb{P}_K$. Sea $\mathcal{O}_K := \bigcap_{\mathfrak{p}\neq v_0} \mathcal{O}_\mathfrak{p} = \{x \in K \mid v_\mathfrak{p}(x) \geq 0 \text{ para toda } \mathfrak{p} \neq v_0\}$. Entonces, por el Teorema de Riemann-Roch, existe $T \in K$ cuyo único polo de T es v_0. Se sigue que $\mathcal{O}_K$ es la cerradura entera de $\mathbb{F}_q[T]$ en K y $\mathcal{O}_K$ es un dominio Dedekind.

Sean $\mathcal{D}_K$ el grupo de ideales fraccionarios de $\mathcal{O}_K$ y $\mathcal{P}_K$ el subgrupo de ideales principales de $\mathcal{D}_K$. Entonces $\mathcal{D}_K/\mathcal{P}_K$ es un grupo finito ([136, Corolario 10.1.14]). Sea

$$\Lambda_{v_0} : J_K/J_{K,\{v_0\}} \longrightarrow \mathcal{D}_K, \qquad \Lambda_{v_0}(\bar{\vec{\alpha}}) = \prod_{\mathfrak{p}\neq v_0} \mathfrak{p}^{v_\mathfrak{p}(\alpha_\mathfrak{p})},$$

el cual es un isomorfismo y $\Lambda_{v_0}(\bar{K^*}) = \mathcal{P}_K$. Por tanto $J_K/J_{K,\{v_0\}}K^* \cong \mathcal{D}_K/\mathcal{P}_K$ es finito. A partir de este punto, se procede como en el caso numérico. □

Ahora consideremos nuevamente un campo global de funciones. Recordemos que el epimorfismo Λ nos induce un epimorfismo continuo y $C_{K,0} = J_{K,0}/K^* \twoheadrightarrow J_{K,0}/U_K K^* \cong I_{K,0}$ y puesto que $C_{K,0}$ es compacto, $I_{K,0}$ es compacto y discreto, por tanto finito. Esto mismo es obtenido en [136, Teorema 10.1.5] por otros métodos.

Definición 6.2.32. Sea S un conjunto finito no vacío de lugares de un campo global K conteniendo a los lugares infinitos en el caso de ser K numérico. Sea $K^S = \{x \in K^* \mid v_\mathfrak{p}(x) = 0 \text{ para toda } \mathfrak{p} \notin S\} = K^* \cap J_{K,S}$ el grupo de las S-unidades de K.

Proposición 6.2.33. *Sea K un campo global de funciones. Existe S, un conjunto de lugares suficientemente grande, tal que $J_{K,0} = J_{K,S,0}K^*$ donde*

$$\begin{aligned} J_{K,S,0} &= J_{K,S} \cap J_{K,S} \\ &= \{\vec{\alpha} \in J_K \mid \operatorname{gr} \vec{\alpha} = 0 \text{ y } v_{\mathfrak{p}}(\alpha_{\mathfrak{p}}) = 0 \text{ para casi toda } \mathfrak{p} \in S\}. \end{aligned}$$

Demostración. Análoga a la del Teorema 6.2.31. □

Cuando K es numérico y $S = S_\infty$ es el conjunto de los lugares arquimedianos, $K^{S_\infty} = E_K = \mathcal{O}_K^*$ las unidades del anillo de enteros $\mathcal{O}_K$ de K.

Se tiene que K^S es el grupo de elementos invertibles de los S-enteros de K: $\mathcal{O}_{K,S} = \{x \in K \mid v_{\mathfrak{p}}(x) \geq 0 \text{ para toda } \mathfrak{p} \notin S\} = \bigcap_{\mathfrak{p} \notin S} \mathcal{O}_{\mathfrak{p}}$, el cual es un dominio Dedekind.

Sea V^s un espacio real de dimensión finita s: $V^s = \bigoplus_{i=1}^s \mathbb{R}v_i$. Una *red* es un subgrupo abeliano libre de V^s de rango s y tal que una $\mathbb{Z}$-base de este subgrupo es una $\mathbb{R}$-base de V^s.

Lema 6.2.34. *Sea S un conjunto finito no vacío de lugares de un campo global K conteniendo a los lugares arquimedianos cuando K es un campo numérico. Sea $V := \{f : S \longrightarrow \mathbb{R}\} \cong \mathbb{R}^s$ que es un $\mathbb{R}$-espacio vectorial s dimensional, en donde $s = |S|$, Sea $\lambda : K^s \longrightarrow V$ dada por $\lambda(a) = f_a$ donde $f_a(v) = \log |a|_v$, esto es, $\lambda : a \longmapsto \big(\log |a|_{v_1}, \ldots, \log |a|_{v_s}\big) \in \mathbb{R}^s$, donde $S = \{v_1, \ldots, v_s\}$.*

Entonces $\operatorname{núc} \lambda$ *es un subgrupo finito de K^S y su imagen es una red generando el $\mathbb{R}$-espacio vectorial V_0 que consiste de las $f \in V$ tales que $\sum_{v \in S} f(v) = 0$.*

Demostración. Si c y C son constantes con $0 < c < C$, entonces $\{\eta \in K^S \mid c \leq |\eta|_v \leq C \text{ para toda } v \in S\}$ es la intersección de un subconjunto compacto de J_K con el grupo discreta K^*, esto es, es compacto y discreto por lo que es finito.

En particular, $\{x \in K^* \mid |x|_v = 1 \text{ para toda } v \in \mathbb{R}\}$ es finito y forma un grupo multiplicativo por lo que es el grupo de las raíces de unidad de K.

Se sigue que $\operatorname{núc} \lambda$ es finito.

Para ver la imagen de λ, notemos que se definir λ por una fórmula análoga en los S-idèles $J_{K,S}$, esto es $J_{K,S} \longrightarrow \mathbb{R}^s$, $\vec{\alpha} \longmapsto \big(\log |\alpha_{v_1}|_{v_1}, \ldots, \log |\alpha_{v_s}|_{v_s}\big)$ y la imagen de $J_{K,S,0} = J_{K,S} \cap J_{K,0}$ genera el $\mathbb{R}$-espacio vectorial consistente de las f satisfaciendo $\sum_{v \in S} f(v) = 0$ que es de dimensión $s - 1$, pues para un idèle $\vec{\alpha}$ en $J_{K,S,0}$ se tiene $\|\vec{\alpha}\| = \sum_{v \in S} |\alpha_v|_v = 1$.

El grupo $\lambda(K^S)$ es discreto puesto que hay un número finito de elementos $\eta \in K^S$ con $1/2 < |\eta|_v < 2$ para toda $v \in S$. Ahora, $J_{K,S,0}/K^S$ es un subgrupo abierto, por tanto cerrado, en $J_{K,0}/K^* = C_{K,0}$ el cual es compacto. Se sigue que $J_{K,S,0}/K^S$ es compacto y por lo tanto el epimorfismo $J_{K,S,0}/K^S \overset{\lambda}{\twoheadrightarrow} \lambda(J_{K,S,0})/\lambda(K^S)$ implica que $\lambda(J_{K,S,0})/\lambda(K^S)$ es compacto. Se sigue que $\lambda(K^S)$ genera a V_0. □

Como corolario, obtenemos el teorema de las unidades de Dirichlet.

Teorema 6.2.35 (Teorema de las Unidades de Dirichlet). *Sea K un campo global y sea S un conjunto finito no vacío de lugares de K conteniendo a los primos infinitos. Entonces, como grupos, se tiene $K^S \cong W_K \times \mathbb{Z}^{s-1}$ donde W_K son las raíces de unidad en K y $s = |S|$.* □

Nuestro objeto de estudio es el grupo de clases de idèles $C_K = J_K/K^*$ donde K es un campo global. Si L/K es una extensión finita y separable, se define el encaje $J_K \xrightarrow{\mu} J_L$, definido por $\mu(\vec{\alpha})_{\mathfrak{P}} := \alpha_{\mathfrak{p}}$ donde $\mathfrak{P}|\mathfrak{p}$, esto es, si $\mu(\vec{\alpha}) = \vec{\beta} \in J_L$, las componentes de $\vec{\beta}$ están dadas por los provenientes de K: $\beta_{\mathfrak{P}} = \alpha_{\mathfrak{P}|_K}$. En particular, si $\beta_{\mathfrak{P}} = \beta_{\mathfrak{P}'}$ si $\mathfrak{P}|_K = \mathfrak{P}'|_K = \mathfrak{p}$.

Si L/K es una extensión de Galois y $G = \mathrm{Gal}(L/K) = G_{L|K}$, entonces G actúa en J_L de manera natural: si $\sigma \in G$, σ define un isomorfismo $\sigma : L_{\sigma^{-1}\mathfrak{P}} \longrightarrow L_{\mathfrak{P}}$. Por tanto, si $\vec{\beta} \in J_L$, $\sigma\vec{\beta} \in J_L$ está definido por $(\sigma\vec{\beta})_{\mathfrak{P}} := \sigma\beta_{\sigma^{-1}\mathfrak{P}} \in L_{\mathfrak{P}}, \beta_{\sigma^{-1}\mathfrak{P}} \in L_{\sigma^{-1}\mathfrak{P}}$, esto es, $\beta_{\sigma^{-1}\mathfrak{P}} \in L_{\sigma^{-1}\mathfrak{P}}$ es la $\sigma^{-1}\mathfrak{P}$-componente de $\vec{\beta}$. Notemos qe $(\sigma\vec{\beta})_{\mathfrak{P}}$ es no unidad en $L_{\mathfrak{P}} \iff (\vec{\beta})_{\sigma^{-1}\mathfrak{P}}$ es no unidad. Por tanto, cuando pasamos a ideales o divisores bajo el mapeo $\Lambda : J_L \longrightarrow D_L$, $\Lambda(\vec{\beta}) = \prod_{\mathfrak{P}\nmid\infty} \mathfrak{P}^{v_{\mathfrak{P}}(\beta_{\mathfrak{P}})}$, el mapeo $\sigma : \vec{\beta} \longrightarrow \sigma\beta$ es el mapeo

$$\begin{aligned}\Lambda(\sigma\vec{\beta}) = \mathfrak{a}_{\sigma\vec{\beta}} &= \prod_{\mathfrak{P}\nmid\infty} \mathfrak{P}^{v_{\mathfrak{P}}((\sigma\vec{\beta})_{\mathfrak{P}})} = \prod_{\mathfrak{P}\nmid\infty} \mathfrak{P}^{v_{\mathfrak{P}}(\sigma\beta_{\sigma^{-1}\mathfrak{P}})} \\ &= \underset{\substack{\mathfrak{P}'=\sigma^{-1}\mathfrak{P} \\ \sigma\mathfrak{P}'=\mathfrak{P}}}{\uparrow} \prod_{\mathfrak{P}'\nmid\infty} (\sigma\mathfrak{P}')^{v_{\sigma\mathfrak{P}'}(\sigma\beta_{\mathfrak{P}'})} = \prod_{\mathfrak{P}'\nmid\infty} (\sigma\mathfrak{P}')^{v_{\mathfrak{P}'}(\beta_{\mathfrak{P}'})} \\ &= \sigma\mathfrak{a}_{\vec{\beta}} = \sigma\Lambda(\vec{\beta}).\end{aligned}$$

Esto es

$$\Lambda(\sigma\vec{\beta}) = \mathfrak{a}_{\sigma\vec{\beta}} = \sigma\mathfrak{a}_{\vec{\beta}} = \sigma\Lambda(\vec{\beta}).$$

Teorema 6.2.36. *Sea L/K una extensión finita de Galois de campos globales con $G = \mathrm{Gal}(L/K)$. Entonces $J_L^G = J_K$.*

Demostración. Al considerar $J_K \subseteq J_L$, todas las componentes de $\vec{\alpha}$ en J_L son las mismas en todo $\{\mathfrak{P}\}_{\mathfrak{P}|\mathfrak{p}}$ y G únicamente las permuta. Mas precisamente, sea $\sigma \in G$, $\sigma : L_{\sigma^{-1}\mathfrak{P}} \longrightarrow L_{\mathfrak{P}}$ es un $K_{\mathfrak{p}}$-isomorfismo para $\mathfrak{P}|\mathfrak{p}$ y si $\vec{\alpha} \in J_K$ considerado en J_L, entonces

$$(\sigma\vec{\alpha})_{\mathfrak{P}} = \sigma\alpha_{\sigma^{-1}\mathfrak{P}} = \sigma\alpha_{\mathfrak{P}} = \alpha_{\mathfrak{P}} \in K_{\mathfrak{p}}.$$

Por tanto $\sigma\vec{\alpha} = \vec{\alpha}$.

Ahora sea $\vec{\beta} \in J_L$ con $\sigma\vec{\beta} = \vec{\beta}$ para toda $\sigma \in G$. Por tanto, $(\sigma\vec{\beta})_{\mathfrak{P}} = \sigma\beta_{\sigma^{-1}\mathfrak{P}} = \beta_{\mathfrak{P}}$ para todos los primos $\mathfrak{P} \in \mathbb{P}_L$. Ahora, el grupo de descomposición $D(\mathfrak{P}|\mathfrak{p})$ de $\mathfrak{P}/\mathfrak{p}$ de K, es isomorfo al grupo de Galois de la

extensión $L_{\mathfrak{P}}/K_{\mathfrak{p}}$. Para $\sigma \in D(\mathfrak{P}|\mathfrak{p})$ se tiene $\sigma^{-1}\mathfrak{P} = \mathfrak{P}$ y puesto que $\beta_{\mathfrak{P}} = \sigma\beta_{\sigma^{-1}\mathfrak{P}} = \sigma\beta_{\mathfrak{P}}$, se sigue que $\beta_{\mathfrak{P}} \in K_{\mathfrak{p}}$ para todo primo $\mathfrak{P}|\mathfrak{p}$.

Para $\sigma \in G$ arbitrario, $(\sigma\vec{\beta})_{\mathfrak{P}} = \beta_{\mathfrak{P}} = (\sigma\vec{\beta})_{\sigma^{-1}\mathfrak{P}} = \beta_{\sigma^{-1}\mathfrak{P}} \in K_{\mathfrak{p}}$, es decir, los dos lugares $\mathfrak{P}$ y $\sigma^{-1}\mathfrak{P}$ sobre $\mathfrak{p}$ tienen la misma componente $\beta_{\mathfrak{P}} = \beta_{\sigma^{-1}\mathfrak{P}} \in K_{\mathfrak{p}}$ por lo que $\vec{\beta} \in J_K$. Por tanto $J_L^G \subseteq J_K$ y $J_K = J_L^G$. □

En general el mapeo $I_{K,0} \longrightarrow I_{L,0}$ no es inyectivo, es decir, un ideal o divisor que no es principal en $D_{K,0}$ puede ser principal en $D_{L,0}$. Este fenómeno no sucede para los idèles.

Proposición 6.2.37. *Sea L/K un extensión finita y separable de campos globales. Entonces $L^* \cap J_K = K^*$.*

En particular, si $\vec{\alpha} \in J_K$ es un idèle de K que es principal en J_L, entonces $\vec{\alpha}$ es principal en K.

Demostración. Es inmediato que $K^* \subseteq L^* \cap J_K$. Sea $\tilde{L}$ una extensión finita de Galois que contiene a L y sea $\tilde{G} = \mathrm{Gal}(\tilde{L}/K)$. Entonces $J_K, J_L \subseteq J_{\tilde{L}}$. Si $\vec{\alpha} \in \tilde{L}^* \cap J_K$, entonces $\vec{\alpha} \in J_{\tilde{L}}^{\tilde{G}}$, es decir, $\sigma\vec{\alpha} = \vec{\alpha}$ para toda $\sigma \in \tilde{G}$. Ahora, puesto que $\vec{\alpha} \in \tilde{L}^*$, se tiene que $\vec{\alpha} \in (\tilde{L}^*)^{\tilde{G}} = K^*$, por lo tanto, $\tilde{L}^* \cap J_K = K^*$. Se sigue que $L^* \cap J_K \subseteq \tilde{L}^* \cap J_K = K^*$. □

Corolario 6.2.38. *El encaje $\mu : J_K \longrightarrow J_L$ induce un monomorfismo $\tilde{\mu} : C_K = J_K/K^* \longrightarrow J_L/L^* = C_L$ donde L/K es cualquier extensión finita y separable de campos globales.*

Demostración. Se tiene que $\tilde{\mu}(\vec{\alpha}K^*) = \vec{\alpha}L^*$ es un homomorfismo. Si $\tilde{\mu}(\vec{\alpha}K^*) = \vec{\alpha}L^* = 1$, es decir, $\vec{\alpha} \in L^*$, por lo que $\vec{\alpha} \in L^* \cap J_K = K^*$. Se sigue que $\vec{\alpha}K^* = 1$ y $\tilde{\mu}$ es inyectiva. □

En adelante, si $K \subseteq L$, entonces consideramos $C_K \subseteq C_L$ de manera natural.

Teorema 6.2.39. *Sea L/K un extensión finita de Galois de campos globales con $G = \mathrm{Gal}(L/K)$. Entonces C_L es de manera natural un G-módulo y $C_L^G = C_K$.*

Demostración. Si $\vec{\beta}L^* \in C_L$, $\vec{\beta} \in J_L$, se define $\sigma(\vec{\beta}L^*) := \sigma\vec{\beta}\cdot L^*$. La definición es independiente del representante $\vec{\beta} \in J_L$ de $\vec{\beta}L^* \in C_L$ y C_L es un G-módulo.

Se tiene la sucesión G-exacta

$$1 \longrightarrow L^* \longrightarrow J_L \longrightarrow C_L \longrightarrow 1,$$

de donde se sigue la sucesión exacta en cohomología

$$1 \longrightarrow (L^*)^G = K^* \longrightarrow J_L^G = J_K \longrightarrow C_L^G \longrightarrow H^1(G, L^*) = \{1\}.$$

Por tanto $C_L^G \cong J_K/K^* = C_K$. □

6.3. Cohomología de J_L

Sea L/K una extensión finita de Galois de campos globales con grupo de Galois $G = \mathrm{Gal}(L/K) = G_{L|K}$. Sean S un conjunto finito de primos de K y $\bar{S} = \{\mathfrak{P} \in \mathbb{P}_L \mid \mathfrak{P}|_K \in S\}$. Se denota $J_{L,\bar{S}} = J_{L,S}$ y se hablará de los S-idèles de L en lugar de los $\bar{S}$-idèles. Así

$$J_{L,S} = \prod_{\substack{\mathfrak{P}|\mathfrak{p} \\ \mathfrak{p}\in S}} L_{\mathfrak{P}}^* \times \prod_{\substack{\mathfrak{P}|\mathfrak{p} \\ \mathfrak{p}\notin S}} U_{\mathfrak{P}} = \prod_{\mathfrak{p}\in S}\prod_{\mathfrak{P}|\mathfrak{p}} L_{\mathfrak{P}}^* \times \prod_{\mathfrak{p}\notin S}\prod_{\mathfrak{P}|\mathfrak{p}} U_{\mathfrak{P}}.$$

Sean

$$J_L^{\mathfrak{p}} := \prod_{\mathfrak{P}|\mathfrak{p}} L_{\mathfrak{P}}^* \quad \text{y} \quad U_L^{\mathfrak{p}} := \prod_{\mathfrak{P}|\mathfrak{p}} U_{\mathfrak{P}}$$

subgrupos de J_L en donde las componentes de $J_L^{\mathfrak{p}}$ y de $U_L^{\mathfrak{p}}$ en primos $\mathfrak{P} \nmid \mathfrak{p}$ son iguales a 1.

Como G permuta los lugares $\mathfrak{P}$ con $\mathfrak{P}|\mathfrak{p}$, se tiene que $J_L^{\mathfrak{p}}$ y $U_L^{\mathfrak{p}}$ son G-módulos. Se tiene $J_{L,S} = \prod_{\mathfrak{p}\in S} J_L^{\mathfrak{p}} \times \prod_{\mathfrak{p}\notin S} U_L^{\mathfrak{p}}$.

6.3.1. Norma de idéles

Sea L/K una extensión finita y separable de campos globales.

Definición 6.3.1. La *norma* $\mathrm{N}_{L/K}$ de J_L a J_K se define de la siguiente forma: Sea M la cerradra normal de L/K y sean $G = \mathrm{Gal}(M/K)$ y $H = \mathrm{Gal}(M/L)$. Entonces $J_L = J_M^H$. Sea G/H el conjunto de las clases izquierdas de H en G. Entonces

$$\mathrm{N}_{L/K}\,\vec{\alpha} = \prod_{\sigma\in G/H} \sigma\vec{\alpha}, \quad \vec{\alpha} \in J_L.$$

Se tiene que $\mathrm{N}_{L/K}$ no depende de los representantes $\sigma \in G/H$ pues J_L esta fijo bajo H.

Para $\tau \in G$, se tiene

$$\tau\,\mathrm{N}_{L/K}\,\vec{\alpha} = \prod_{\sigma\in G/H} \tau\sigma\vec{\alpha} = \prod_{\sigma\in G/H} \sigma\vec{\alpha} = \mathrm{N}_{L/K}\,\vec{\alpha},$$

por tanto $\mathrm{N}_{L/K}\,\vec{\alpha} \in J_K$.

Se tiene que $\mathrm{N}_{L/K}\,L^* \subseteq K^*$, es decir, $\mathrm{N}_{L/K}$ manda idèles principales en idèles principales. En particular $\mathrm{N}_{L/K}$ induce $\mathrm{N}_{L/K} : C_L \longrightarrow C_K$.

Teorema 6.3.2. *Si L/K es una extensión finita y separable de campos globales, las componentes locales de $\mathrm{N}_{L/K}\,\vec{\alpha} \in J_L$ están dadas por:*

$$\left(\mathrm{N}_{L/K}\,\vec{\alpha}\right)_{\mathfrak{p}} = \prod_{\mathfrak{P}|\mathfrak{p}} \mathrm{N}_{L_{\mathfrak{P}}/K_{\mathfrak{p}}}\,\alpha_{\mathfrak{P}}.$$

En particular si L/K es una extensión finita y abeliana, definimos para $\vec{\alpha} \in J_L$

$$\mathrm{N}_{L/K}\,\vec{\alpha} = \vec{\beta} \in J_K \quad \textit{donde} \quad \beta_{\mathfrak{p}} = \prod_{\mathfrak{P}|\mathfrak{p}} \mathrm{N}_{L_{\mathfrak{P}}/K_{\mathfrak{p}}}\,\alpha_{\mathfrak{P}}.$$

Si L/K es una extensión abeliana finita, entonces la norma $\mathrm{N}_{L/K} : J_L \longrightarrow J_K$ es un mapeo abierto y por tanto, la norma inducida en las clases de idèles $\mathrm{N}_{L/K} : C_L \longrightarrow C_K$ es un mapeo abierto.

Demostración. Sea M/K la cerradura normal de L/K y sea $G = \mathrm{Gal}(M/K)$ y $H = \mathrm{Gal}(M/L)$. Para cada primo $\mathfrak{p}$ de K, sea $\mathfrak{q}_{\mathfrak{p}}$ un primo fijo de M sobre $\mathfrak{p}$ y sea $\mathfrak{P}_{\mathfrak{p}} = \mathfrak{q}_{\mathfrak{p}}|_L$. Sea $G_{\mathfrak{q}_{\mathfrak{p}}} = \mathrm{Gal}(M_{\mathfrak{q}_{\mathfrak{p}}}/K_{\mathfrak{p}}) \subseteq G$ y sea $\{\sigma_i\}$ un conjunto completo de representantes de las clases dobles $H\tau G_{\mathfrak{q}_{\mathfrak{p}}}$, es decir, $G = \cup_i H\sigma_i G_{\mathfrak{q}_{\mathfrak{p}}}$.

Entonces $\mathfrak{P}_i := \mathfrak{q}_i|_L = (\sigma_i\mathfrak{q}_{\mathfrak{p}})|_L$ es un conjunto completo de primos de L sobre $\mathfrak{p}$. Para cada i, sea $\{\tau_{ij}\}$ un conjunto completo de representantes derechos de las clases de $G_{\mathfrak{q}_{\mathfrak{p}}} \cap H^{\sigma_i}$ en $G_{\mathfrak{q}_{\mathfrak{p}}}$, donde $H^{\sigma_i} := \sigma_i^{-1}H\sigma_i$. Entonces

$$G_{\mathfrak{q}_{\mathfrak{p}}} = \cup_j \big(G_{\mathfrak{q}_{\mathfrak{p}}} \cap H^{\sigma_i}\big)\tau_{ij} \quad \text{y} \quad G = \cup_{i,j} H\sigma_i\tau_{ij} = \cup_{i,j}\tau_{ij}^{-1}\sigma_i^{-1}H,$$

y $G_{\mathfrak{q}_{\mathfrak{p}}} \cap H_i$ es el grupo de descomposición de $\mathfrak{q}_{\mathfrak{p}}$ sobre $\sigma_i^{-1}L$.

Sea $\vec{\alpha} \in J_L$, considered como un idèle de M. Entonces

$$\begin{aligned}\mathrm{N}_{L/K}(\vec{\alpha})_{\mathfrak{p}} = \mathrm{N}_{L/K}(\vec{\alpha})_{\mathfrak{q}_{\mathfrak{p}}} &= \prod_{i,j}(\tau_{ij}^{-1}\sigma_i^{-1}\vec{\alpha})_{\mathfrak{q}_{\mathfrak{p}}} = \prod_{i,j}\tau_{ij}^{-1}(\sigma_i^{-1}\vec{\alpha})_{\mathfrak{q}_{\mathfrak{p}}} \\ &= \prod_i \mathrm{N}_{(\sigma_i^{-1}L)_{\mathfrak{q}_{\mathfrak{p}}}/K_{\mathfrak{p}}}\big((\sigma_i^{-1}\vec{\alpha})_{\mathfrak{q}_{\mathfrak{p}}}\big).\end{aligned}$$

El isomorfismo $\sigma_i : \sigma_i^{-1}L \longrightarrow L$ induce a su vez un $K_{\mathfrak{p}}$-isomorfismo $\sigma_i : (\sigma_i^{-1}L)_{\mathfrak{q}_{\mathfrak{p}}} \longrightarrow L_{\mathfrak{q}_i} = L_{\mathfrak{P}_i}$ que manda $(\sigma_i^{-1}\vec{\alpha})_{\mathfrak{q}_{\mathfrak{p}}}$ a $\alpha_{\mathfrak{q}_i} = \alpha_{\mathfrak{P}_i}$. Por tanto

$$\big(\mathrm{N}_{L/K}(\vec{\alpha})\big)_{\mathfrak{p}} = \prod_i \mathrm{N}_{L_{\mathfrak{P}_i}/K_{\mathfrak{p}}}(\vec{\alpha})_{\mathfrak{P}_i} = \prod_{\mathfrak{P}|\mathfrak{p}} \mathrm{N}_{L_{\mathfrak{P}}/K_{\mathfrak{p}}}(\alpha_{\mathfrak{P}}).$$

Veamos que la norma es abierta. Sean V un conjunto abierto de J_L y $\vec{\alpha} \in V$. Sea $W = \prod_{\mathfrak{P}} W_{\mathfrak{P}}$ una vecindad de $\vec{1}$ con $\vec{\alpha}\cdot W \subseteq V$. Podemos suponer que $W = \prod_{\mathfrak{P}|\infty} W_{\mathfrak{P}} \times \prod_{\mathfrak{P}\nmid\infty} W_{\mathfrak{P}}$ con $W_{\mathfrak{P}} \subseteq L_{\mathfrak{P}}^*$ un abierto para $\mathfrak{P}$ un primo infinito y $W_{\mathfrak{P}} = U_{\mathfrak{P}}^{(m_{\mathfrak{P}})}$ si $\mathfrak{P}$ es un primo finito y donde $m_{\mathfrak{P}} = 0$ para casi toda $\mathfrak{P}$. Ahora bien, $U_{\mathfrak{P}}^{(m_{\mathfrak{P}})}$ es compacto, abierto y cerrado (Proposiciones 3.2.1 y 3.2.2) y como $\mathrm{N}_{L_{\mathfrak{P}}/K_{\mathfrak{p}}}$ es continua, se tiene que $\mathrm{N}_{L_{\mathfrak{P}}/K_{\mathfrak{p}}}(U_{\mathfrak{P}}^{(m)})$ es compacto y de índice finito en $U_{\mathfrak{p}}^{(m)}$ por lo que $\mathrm{N}_{L_{\mathfrak{P}}/K_{\mathfrak{p}}}(U_{\mathfrak{P}}^{(m)})$ es abierto y cerrado. Por tanto, para cada m, existe un n_m tal que $\mathrm{N}_{L_{\mathfrak{P}}/K_{\mathfrak{p}}}\,U_{\mathfrak{P}}^{(m)} \supseteq U_{\mathfrak{p}}^{(n_m)}$ por ser $\{U_{\mathfrak{p}}^{(n)}\}_{n=0}^{\infty}$ un sistema fundamental de vecindades de $1 \in K_{\mathfrak{p}}^*$ (Corolario 3.2.4).

Si $\mathfrak{p}$ es infinito, se tiene $\mathrm{N}_{L_{\mathfrak{P}}/K_{\mathfrak{p}}}\,L_{\mathfrak{P}}^* \supseteq \mathbb{R}^+$. Sea $\vec{\beta} = \mathrm{N}_{L/K}\,\vec{\alpha}$ y sea $W' = \prod_{\mathfrak{p}} W'_{\mathfrak{p}}$ tal que $W'_{\mathfrak{p}} \subseteq \mathbb{R}^+$ y tal que $\mathrm{N}_{L_{\mathfrak{P}}/K_{\mathfrak{p}}}\,W_{\mathfrak{P}} \supseteq W'_{\mathfrak{p}}$ si $\mathfrak{p}$ es infinito y $W_{\mathfrak{p}} = U_{\mathfrak{p}}^{(n_{\mathfrak{p}})}$ con $\mathrm{N}_{L_{\mathfrak{P}}/K_{\mathfrak{p}}}\,U_{\mathfrak{P}}^{(m_{\mathfrak{P}})} \supseteq U_{\mathfrak{p}}^{(n_{\mathfrak{p}})}$ para $\mathfrak{p}$ finito. Entonces

$$\vec{\beta}\cdot W' \subseteq \mathrm{N}_{L/K}\left(\vec{\alpha}\cdot W\right) \subseteq \mathrm{N}_{L/K}\, V.$$

Por tanto $\mathrm{N}_{L/K}$ es un mapeo abierto. □

Proposición 6.3.3. *Sea L/K una extensión abeliana finita de campos globales. Sea $\mathfrak{P}$ un primo de L sobre el primo $\mathfrak{p}$. Entonces*

$$H^q(G, J_L^{\mathfrak{p}}) \cong H^q(G_{\mathfrak{P}}, L_{\mathfrak{P}}^*) \quad y \quad H^q(G, U_L^{\mathfrak{p}}) \cong H^q(G_{\mathfrak{P}}, U_{\mathfrak{P}}) \quad \text{para toda } q \in \mathbb{Z},$$

donde $G_{\mathfrak{P}}$ es el grupo de descomposición de $\mathfrak{P}$ sobre K y se tiene $G_{\mathfrak{P}} \cong \mathrm{Gal}(L_{\mathfrak{P}}/K_{\mathfrak{p}})$.

Si $\mathfrak{p}$ es un primo finito de K no ramificado en L, entonces $H^q(G, U_L^{\mathfrak{p}}) = 1$ para toda $q \in \mathbb{Z}$.

Demostración. Los isomorfismos se siguen del Lema de Shapiro, Teorema 4.8.7: $L_{\mathfrak{P}}^*$ y $U_{\mathfrak{P}}$ son $G_{\mathfrak{P}}$-módulos y se tiene

$$J_L^{\mathfrak{p}} = \prod_{\mathfrak{P}|\mathfrak{p}} L_{\mathfrak{P}}^* \cong \bigoplus_{\sigma \in G/G_{\mathfrak{P}}} \sigma L_{\mathfrak{P}}^* \quad \text{y} \quad U_L^{\mathfrak{p}} = \prod_{\mathfrak{P}|\mathfrak{p}} U_{\mathfrak{P}} \cong \bigoplus_{\sigma \in G/G_{\mathfrak{P}}} \sigma U_{\mathfrak{P}}.$$

Cuando $\mathfrak{p}$ es no ramificado en L/K, $\mathfrak{p}$ es no ramificado en $L_{\mathfrak{P}}/K_{\mathfrak{p}}$, por lo tanto $H^q(G_{\mathfrak{P}}, U_{\mathfrak{P}}) = \{1\}$ para toda $q \in \mathbb{Z}$ (Teorema 5.1.11). □

Observación 6.3.4. Si $\pi : J_L^{\mathfrak{p}} \longrightarrow L_{\mathfrak{P}}^*$ es la proyección $\pi(\vec{\alpha}) = \alpha_{\mathfrak{P}}$, el isomorfismo por $H^q(G, J_L^{\mathfrak{p}}) \cong H^q(G_{\mathfrak{P}}, L_{\mathfrak{P}}^*)$ está dado por

$$H^q(G, J_L^{\mathfrak{p}}) \xrightarrow{\text{res}} H^q(G_{\mathfrak{P}}, J_L^{\mathfrak{p}}) \xrightarrow{\bar{\pi}} H^q(G_{\mathfrak{P}}, L_{\mathfrak{P}}^*).$$

Si S es un conjunto finito de lugares de K, se tiene

$$H^q(G, J_{L,S}) \cong \prod_{\mathfrak{p}\in S} H^q(G, J_L^{\mathfrak{p}}) \times \prod_{\mathfrak{p}\notin S} H^q(G, U_L^{\mathfrak{p}}).$$

Cuando S contiene a todos los primos ramificados en L, entonces por la Proposición 6.3.3 se obtiene $H^q(G, J_{L,S}) = \prod_{\mathfrak{p}\in S} H^q(G_{\mathfrak{P}}, L_{\mathfrak{P}}^*)$ donde $\mathfrak{P}$ es cualquier primo de L dividiendo a $\mathfrak{p}$ primo de K (pues para $\mathfrak{p} \notin S$, $\mathfrak{p}$ es no ramificado y $H^q(G, U_L^{\mathfrak{p}}) = \{1\}$).

Ahora $J_L = \bigcup_S J_{L,S} = \varinjlim_S J_{L,S}$ y

$$H^q(G, J_L) \cong H^q(G, \varinjlim_S J_{L,S}) \cong \varinjlim_S H^q(G, J_{L,S}) \cong \bigoplus_{\mathfrak{p}} H^q(G_{\mathfrak{P}}, L_{\mathfrak{P}}^*),$$

y donde S varía sobre todos los conjuntos finitos de K que contienen a todos los primos ramificados. Hemos probado

Teorema 6.3.5. *Sea L/K una extensión finita de Galois de campos globales. Para cada primo de $\mathfrak{p}$ de K, sea $\mathfrak{P}$ un primo de L sobre $\mathfrak{p}$. Sea S cualquier conjunto finito de primos de K que contiene a todos los primos ramificados en L. Entonces*

$$H^q(G, J_{L,S}) \cong \prod_{\mathfrak{p}\in S} H^q(G_{\mathfrak{P}}, L_{\mathfrak{P}}^*),$$
$$H^q(G, J_L) \cong \bigoplus_{\mathfrak{p}\in \mathbb{P}_K} H^q(G_{\mathfrak{P}}, L_{\mathfrak{P}}^*). \qquad \square$$

Observación 6.3.6. Del resultado del Teorema 6.3.5 se obtiene que la cohomología de J_L se puede calcular por medio de los grupos de cohomología local $H^q(G_{\mathfrak{P}}, L_{\mathfrak{P}}^*)$.

Observación 6.3.7. El isomorfismo $H^q(G, J_L) \cong \bigoplus_{\mathfrak{p}} H^q(G_{\mathfrak{P}}, L_{\mathfrak{P}}^*)$ está dado por las proyecciones $H^q(G, J_L) \longrightarrow H^q(G_{\mathfrak{P}}, L_{\mathfrak{P}}^*)$, es decir, la composición de los mapeos

$$H^q(G, J_L) \xrightarrow{\text{res}} H^q(G_{\mathfrak{P}}, J_L) \xrightarrow{\bar{\pi}} H^q(G_{\mathfrak{P}}, L_{\mathfrak{P}}^*),$$

donde $\bar{\pi}$ está inducido por la proyección natural $J_L \xrightarrow{\pi} L_{\mathfrak{P}}^*$, $\vec{\alpha} \longmapsto \alpha_{\mathfrak{P}}$.

Las proyecciones anteriores mapean cada $c \in H^q(G, J_L)$ a su $\mathfrak{p}$-componente $c_{\mathfrak{p}} \in H^q(G_{\mathfrak{P}}, L_{\mathfrak{P}}^*)$. Por tanto el Teorema 6.3.5 dice que c está unívocamente determinada por sus componentes locales $c_{\mathfrak{p}}$ y como es suma directa, $c_{\mathfrak{p}} = 1$ para casi toda $\mathfrak{p}$. Para dimensiones $q > 0$ el mapeo $c \longrightarrow c_{\mathfrak{p}}$ puede ser descrito como sigue. Dado $c \in H^q(G, J_L)$, seleccionamos un cociclo $\beta(\sigma_1, \ldots, \sigma_q)$ representando a c. Esta es una función del grupo a $G \times \ldots \times G$ con valores en J_L. Restringimos la función a $G_{\mathfrak{P}} \times \cdots \times G_{\mathfrak{P}}$ y tomamos la $\mathfrak{P}$-componente $\beta_{\mathfrak{P}}(\sigma_1, \ldots, \sigma_q)$ del idèle $\beta(\sigma_1, \ldots, \sigma_q)$. La función resultante de $G_{\mathfrak{P}} \times \cdots G_{\mathfrak{P}}$ a $L_{\mathfrak{P}}^*$ es un cociclo y su clase de cohomología $c_{\mathfrak{p}} \in H^q(G_{\mathfrak{P}}, L_{\mathfrak{P}}^*)$ es la $\mathfrak{p}$-componente de c.

Proposición 6.3.8. *Sea $K \subseteq L \subseteq M$ una torre de campos globales con M/K y L/K extensiones finitas y de Galois. Sea $\mathfrak{q}|\mathfrak{P}|\mathfrak{p}$ primos de M, L y de K respectivamente. Entonces*

(1) $(\inf_M c)_{\mathfrak{p}} = \inf_{M_{\mathfrak{q}}}(c_{\mathfrak{p}}), \quad c \in H^q(G_{L|K}, J_L), \quad q \geq 1,$
(2) $(\text{res}_L\, c)_{\mathfrak{P}} = \text{res}_{L_{\mathfrak{P}}}(c_{\mathfrak{p}}), \quad c \in H^q(G_{M|K}, J_M), \quad q \in \mathbb{Z},$
(3) $(\text{cor}_K\, c)_{\mathfrak{p}} = \sum_{\mathfrak{P}|\mathfrak{p}} \text{cor}_{K_{\mathfrak{p}}}(c_{\mathfrak{P}}), \quad c \in H^q(G_{M|L}, J_M), \quad q \in \mathbb{Z},$

donde en (2) *y en* (3) *es suficiente suponer que M/K es de Galois.*

Demostración. En la fórmula (3), para cada $\mathfrak{P}|\mathfrak{p}$, podemos seleccionar $\mathfrak{q}$ en M con $\mathfrak{q}|\mathfrak{P}$, pero entonces las corestricciones $\text{cor}_{K_{\mathfrak{p}}}(c_{\mathfrak{P}})$ pertenecen a distintos grupos de cohomología $H^q(G_{M_{\mathfrak{q}}|K_{\mathfrak{p}}}, M_{\mathfrak{q}}^*)$. Sin embargo podemos identificar todos estos elementos como sigue. Si $\mathfrak{q}$ y $\mathfrak{q}'$ son dos lugares de M sobre $\mathfrak{p}$, existe $\sigma \in G_{M|K}$ tal que $\mathfrak{q}^\sigma = \mathfrak{q}'$ y $M_{\mathfrak{q}}^* \xrightarrow{\sigma} M_{\mathfrak{q}^\sigma}^*$ induce un isomorfismo natural $H^q(G_{M_{\mathfrak{q}}|K_{\mathfrak{p}}}, M_{\mathfrak{q}}^*) \cong H^q(G_{M_{\mathfrak{q}}|K_{\mathfrak{p}}}, M_{\mathfrak{q}^\sigma}^*)$.

De esta forma seleccionamos, para cada $\mathfrak{P}|\mathfrak{p}$ un $\mathfrak{q}|\mathfrak{P}$ y cada $\mathrm{cor}_{K_\mathfrak{p}}(c_\mathfrak{P}) \in H^q(G_{M_\mathfrak{q}|K_\mathfrak{p}}, M_\mathfrak{q}^*)$ y la suma se realiza en $H^q(G_{M_\mathfrak{q}|K_\mathfrak{p}}, M_\mathfrak{q}^*)$.

Para la demostración de la proposición, se tiene que el mapeo de restricción que se obtiene cuando pasamos a las componentes locales, conmuta con los mapeos inf, res y cor. Esta afirmación puede verificarse a nivel de cociclos para inf y res si $q \geq 1$, y para cor si $q = -1, 0$. El caso general se sigue por cambio de dimensión. □

Teorema 6.3.9 (Teorema de la norma para idèles). *Sea L/K una extensión finita de Galois de campos globales. Entonces un idèle $\vec{\alpha} \in J_K$ es la norma de un idèle $\vec{\beta} \in J_L$ si y sólo si cada componente $\alpha_\mathfrak{p} \in K_\mathfrak{p}^*$ es norma de un elemento $\beta_\mathfrak{P} \in L_\mathfrak{P}^*$ con $\mathfrak{P}|\mathfrak{p}$, es decir, si y sólo si es una norma local para toda completación.*

Demostración. Se tiene $H^0(G, J_L) = \frac{J_L^G}{\mathrm{N}_{L/K} J_L} = \frac{J_K}{\mathrm{N}_{L/K} J_L}$ y $H^0(G_\mathfrak{P}, L_\mathfrak{P}^*) = \frac{K_\mathfrak{p}^*}{\mathrm{N}_{L_\mathfrak{P}/K_\mathfrak{p}} L_\mathfrak{P}^*}$. Por el Teorema 6.3.5,

$$H^0(G, J_L) \cong \frac{J_K}{\mathrm{N}_{L/K} J_L} \cong \bigoplus_\mathfrak{p} \frac{K_\mathfrak{p}^*}{\mathrm{N}_{L_\mathfrak{P}/K_\mathfrak{p}} L_\mathfrak{P}} = \bigoplus_\mathfrak{p} H^0(G_\mathfrak{P}, L_\mathfrak{P}^*),$$

donde para cada $\mathfrak{p}$ se selecciona un $\mathfrak{P}$ con $\mathfrak{P}|\mathfrak{p}$.

Si $\vec{\alpha} \in J_K$, el isomorfismo anterior manda la clase $\vec{\alpha}\,\mathrm{N}_{L/K} J_L = \tilde{\vec{\alpha}}$ a las componentes $\tilde{\alpha}_\mathfrak{p} = \alpha_\mathfrak{p}\,\mathrm{N}_{L_\mathfrak{P}/K_\mathfrak{p}} L_\mathfrak{P}^*$. Se sigue $\tilde{\vec{\alpha}} = 1 \iff \tilde{\alpha}_\mathfrak{p} = 1$ para toda $\mathfrak{p}$, es decir, $\vec{\alpha} \in \mathrm{N}_{L/K} J_L \iff \alpha_\mathfrak{p} \in \mathrm{N}_{L_\mathfrak{P}/K_\mathfrak{p}} L_\mathfrak{P}^*$ para toda $\mathfrak{p} \in \mathbb{P}_K$. □

El teorema de la norma para idèles es un análogo al teorema de la norma de Hasse que establece que si L/K es una extensión cíclica finita de campos globales y si $x \in K^*$, entonces x es norma de L^* si y sólo si x es norma local para toda completación (ver Corolario 6.6.21).

Se tiene que si $x \in K^* \subseteq J_K$, entonces $x \in \mathrm{N}_{L/K} J_L \iff x \in \mathrm{N}_{L_\mathfrak{P}/K_\mathfrak{p}} L_\mathfrak{P}^*$ para toda $\mathfrak{p}$, sin embargo no sabemos que $\vec{\beta}$ sea principal, es decir, si $\vec{\beta} = y \in L^*$. En otras palabras, si $x \in K$ es norma para todas las completaciones, x es norma de idèle $\vec{\beta}$ pero no necesariamente de un idèle principal.

Corolario 6.3.10. *Sea L/K una extensión finita y de Galois de campos globales. Entonces se tiene $H^1(G, J_L) = H^3(G, J_L) = \{1\}$. Además, si S es un conjunto finito de lugares que contiene a los primos ramificados y a los primos infinitos, entonces $H^1(G, J_{L,S}) = \{1\}$.*

Demostración. Se sigue de que $H^1(G_{L_\mathfrak{P}|K_\mathfrak{p}}, L_\mathfrak{P}^*) = H^3(G_{L_\mathfrak{P}|K_\mathfrak{p}}, L_\mathfrak{P}^*) = \{1\}$ (Corolario 5.3.10). □

Corolario 6.3.11. *Se tiene que*

$$H^2(G, J_L) \cong \bigoplus_{\mathfrak{p} \in \mathbb{P}_K} \Big(\big(\frac{1}{[L_\mathfrak{P} : K_\mathfrak{p}]}\, \mathbb{Z} \big)/\mathbb{Z} \Big).$$

Demostración. Del Teorema de Tate-Nakayama (Teorema 4.9.20), se tiene

$$H^2(G_{\mathfrak{P}}, L_{\mathfrak{P}}^*) \cong H^0(G_{\mathfrak{P}}, \mathbb{Z}) \cong \frac{\mathbb{Z}}{|G_{\mathfrak{P}}|\mathbb{Z}} \cong \frac{\left(\frac{1}{[L_{\mathfrak{P}}:K_{\mathfrak{p}}]}\ \mathbb{Z}\right)}{\mathbb{Z}},$$

y

$$H^2(G, J_L) \cong \bigoplus_{\mathfrak{p}\in\mathbb{P}_K} H^2(G_{\mathfrak{P}}, L_{\mathfrak{P}}^*). \qquad \square$$

6.4. Grupo de Brauer para campos globales

Puesto que para cualquier extensión finita de Galois L/K de campos globales se tiene $H^1(G_{L|K}, J_L) = \{1\}$, se sigue que $H^2(G_{L|K}, J_L) \subseteq H^2(G_{M|K}, J_M)$ para $K \subseteq L \subseteq M$ una torre de extensiones finitas de Galois, la cual se obtiene como consecuencia de la sucesión exacta inflación-restricción.

Sea $\Omega = K^{\text{sep}}$. Puesto que $J_\Omega = \varinjlim_L J_L = \bigcup_{L/K} J_L$ se obtiene que

$$H^2(G_{\Omega|K}, J_\Omega) = \bigcup_L H^2(G_{L|K}, J_L)$$

y que para $K \subseteq L \subseteq M$ extensiones finitas de Galois,

$$H^2(G_{L|K}, J_L) \subseteq H^2(G_{M|K}, J_M) \subseteq H^2(G_{\Omega|K}, J_\Omega).$$

Por la teoría local, se tiene que el grupo de Brauer $\text{Br}(E)$ de un campo local E satisface que $\text{Br}(E) = \bigcup_F H^2(G_{F|E}, F^*)$ donde F/E recorre las extensiones no ramificadas (Teorema 5.3.3). En el caso global veremos que $\text{Br}(K) = \bigcup_L H^2(G_{L|K}, L^*)$ donde L recorre las extensiones cíclicas ciclotómicas de K si K es un campo numérico y las extensiones de constantes de K si K es un campo de funciones. En otras palabras, $L \in \{\text{subcampos de } K(\zeta_n) \mid K(\zeta_n)/K \text{ es cíclica}\}$ o $L \in \{K\mathbb{F}_{q^n} \mid n \in \mathbb{N}\}$.

Lema 6.4.1. *Sean K un campo global, S un conjunto finito de primos de K y $m \in \mathbb{N}$. Entonces existe una extensión cíclica ciclotómica o una extensión de constantes L/K con la propiedad:*

- $m|[L_{\mathfrak{P}} : K_{\mathfrak{p}}]$ *para toda* $\mathfrak{p} \in S$, $\mathfrak{p}$ *finito,*
- $[L_{\mathfrak{P}} : K_{\mathfrak{p}}] = 2$ *para toda* $\mathfrak{p} \in S$, $\mathfrak{p}$ *real.*

Demostración. Supongamos que hemos probado el lema para los casos especiales $K_0 = \mathbb{Q}$ en el caso numérico y para $K_0 = K$ para campos de funciones. Entonces aplicamos el lema para los casos especiales, encontrando M/K_0 una extensión totalmente imaginaria (caso numérico) cíclica ciclotómica o una extensión de constantes en el caso de campos de funciones, tal que para cada

primo $\mathfrak{p}$ de K_0 en S, $\mathfrak{p}$ finito, hay un primo $\mathfrak{P}$ de M para el cual el grado $[M_{\mathfrak{P}} : (K_0)_{\mathfrak{p}}]$ es divisible por $m \cdot [K : K_0]$.

Entonces $L := KM$ satisface las propiedades requeridas para L/K.

Ahora, para $K = K_0$, el lema se cumple pues podemos realizar lo anterior debido a la descomposición de primos en campos ciclotómicos en el caso numérico, o debido a que en el caso de campos de funciones, en las extensiones de constantes, todo primo es eventualmente inerte. □

Teorema 6.4.2. *Sea K un campo global. Entonces*

$$\mathrm{Br}(K) = \bigcup_L H^2(G_{L|K}, L^*) \quad y \quad H^2(G_\Omega|K, J_\Omega) = \bigcup_L H^2(G_{L|K}, J_L),$$

donde L/K recorre las extensiones cíclicas ciclotómicas finitas en el caso numérico y las extensiones de constantes finitas en caso de campos de funciones.

Demostración. Sea $c \in H^2(G_{\Omega|K}, J_\Omega)$, digamos $c \in H^2(G_{L|K}, J_M)$. Sea m el orden de c y sea S un conjunto finito de primos de K para los cuales las componentes $c_{\mathfrak{p}}$ de c son distintas de 1. Sea L/K una extensión como en el Lema 6.4.1 con $m|[L_{\mathfrak{P}} : K_{\mathfrak{p}}]$ si $\mathfrak{p} \in S$, $\mathfrak{p}$ finito y $[L_{\mathfrak{P}} : K_{\mathfrak{p}}] = 2$ para $\mathfrak{p} \in S$ real.

Sea $N := ML$. Entonces

$$H^2(G_{M|K}, J_M), H^2(G_{L|K}, J_L) \subseteq H^2(G_{N|K}, J_N).$$

Veremos que $c \in H^2(G_{L|K}, J_L)$. Puesto que la sucesión

$$1 \longrightarrow H^2(G_{L|K}, J_L) \xrightarrow{\inf} H^2(G_{N|K}, J_N) \xrightarrow{\mathrm{res}_L} H^2(G_{N|K}, J_N)$$

es exacta, es suficiente probar que $\mathrm{res}_L\, c = 1$.

Por teoría local, junto el Teorema 6.3.5 y la Proposición 6.3.8, se tiene que $\mathrm{res}_L\, c = 1 \iff (\mathrm{res}_L\, c)_{\mathfrak{P}} = \mathrm{res}_{L_{\mathfrak{P}}}\, c_{\mathfrak{p}} = 1$ para toda $\mathfrak{P} \in \mathbb{P}_L \iff \mathrm{inv}_{N_{\mathfrak{q}}|L_{\mathfrak{P}}}(\mathrm{res}_{L_{\mathfrak{P}}}\, c_{\mathfrak{p}}) = [L_{\mathfrak{P}} : K_{\mathfrak{p}}] \cdot \mathrm{inv}_{N_{\mathfrak{q}}|K_{\mathfrak{p}}}\, c_{\mathfrak{p}} = \mathrm{inv}_{N_{\mathfrak{q}}|K_{\mathfrak{p}}}\, c_{\mathfrak{p}}^{[L_{\mathfrak{P}}:K_{\mathfrak{p}}]} = 0$ para toda $\mathfrak{p} \in \mathbb{P}_K \iff c_{\mathfrak{p}}^{[L_{\mathfrak{P}}:K_{\mathfrak{p}}]} = 1$ para toda $\mathfrak{p} \in S$.

Esta última condición se cumple puesto que $c_{\mathfrak{p}}^m = 1$ y $m|[L_{\mathfrak{P}} : K_{\mathfrak{p}}]$ para toda $\mathfrak{p} \in S$ finito y $[L_{\mathfrak{P}} : K_{\mathfrak{p}}] = 2$ para todo $\mathfrak{p} \in S$ real.

Se sigue que $H^2(G_{\Omega|K}, J_\Omega) = \bigcup_L H^2(G_{L|K}, J_L)$.

Para probar que $\mathrm{Br}(K) = \bigcup_L H^2(G_{L|K}, L^*)$ se hace exactamente lo mismo, sustituyendo, para un campo E, J_E por E^*. □

6.5. Primera desigualdad fundamental

Esta primera desigualdad establece que si L/K es una extensión cíclica de grado n de campos globales, entonces

$$[C_K : \mathrm{N}_{L/K}\, C_L] \geq n.$$

Es importante mencionar, que la primera desigualdad únicamente será válida para extensiones abelianas y no para otro tipo de extensiones, incluyendo las de Galois no abelianas. Esto se puede ver en el Teorema 6.9.7. La segunda desigualdad es válida para extensiones finitas de Galois arbitrarias.

Teorema 6.5.1. *Sea L/K una extensión cíclica de grado n de campos globales. Entonces el cociente de Herbrand de C_L, satisface*

$$h(C_L) = \frac{|H^0(G, C_L)|}{|H^1(G, C_L)|} = n,$$

donde $G = \mathrm{Gal}(L/K)$ es el grupo de Galois de la extensión L/K.

En particular,

$$|H^0(G, C_L)| = |H^2(G, C_L)| = [C_K : \mathrm{N}_{L/K}\, C_L] = n \cdot |H^1(G, C_L)| \geq n.$$

Demostración. Sea L/K una extensión cíclica de campos de funciones. Sea $U_L := \prod_{\mathfrak{P}} U_{\mathfrak{P}}$ y consideremos el grupo $J_{L,0}$. Entonces U_L, $L^* \subseteq J_{L,0}$, por lo cual $U_L L^* \subseteq J_{L,0}$. Se tiene

$$h(C_L) = h(J_L/L^*) = h(J_L/J_{L,0})h(J_{L,0}/U_L L^*)h(U_L L^*/L^*).$$

Consideremos la sucesión exacta $1 \longrightarrow J_{L,0} \longrightarrow J_L \xrightarrow{\mathrm{gr}} \mathbb{Z} \longrightarrow 0$, por lo que $J_L/J_{L,0} \cong \mathbb{Z}$ y $h(J_L/J_{L,0}) = h(\mathbb{Z}) = n$.

Ahora $\Lambda : J_{L,0} \longrightarrow D_{L,0} \overset{\pi}{\twoheadrightarrow} I_{L,0}$ y $\mathrm{núc}\, \Lambda = U_L$. Por tanto $D_{L,0} \cong J_{L,0}/U_L$. Además $\mathrm{núc}\, \pi = P_L = \Lambda(L^*)$, de donde obtenemos $J_{L,0}/U_L L^* \cong I_{L,0}$ el cual es finito por lo que $h(J_{L,0}/U_L L^*) = h(I_{L,0}) = 1$.

Ahora, $U_L L^*/L^* \cong U_L/U_L \cap L^*$. Se tiene que $U_L \cap L^* = \mathbb{F}_q^*$, donde $\mathbb{F}_q$ es el campo de constantes de L y por ende $h(U_L \cap L^*) = 1$.

Por otro lado $U = \prod_{\mathfrak{p} \in \mathbb{P}_K} \prod_{\mathfrak{P}|\mathfrak{p}} U_{\mathfrak{P}}$ y $\sigma\big(\prod_{\mathfrak{P}|\mathfrak{p}} U_{\mathfrak{P}}\big) = \prod_{\mathfrak{P}|\mathfrak{p}} U_{\mathfrak{P}}$ para toda $\sigma \in G$.

Del Lema de Shapiro, obtenemos $H^r(G, \prod_{\mathfrak{P}|\mathfrak{p}} U_{\mathfrak{P}}) \cong H^r(G_{\mathfrak{P}}, U_{\mathfrak{P}})$. Por teoría de campos de clase locales tenemos que $h(G_{\mathfrak{P}}, U_{\mathfrak{P}}) = 1$ (ver la demostración del Teorema 5.1.10). De hecho $|H^0(G_{\mathfrak{P}}, U_{\mathfrak{P}})| = |H^1(G_{\mathfrak{P}}, U_{\mathfrak{P}})| = e_{\mathfrak{P}}$ y $e_{\mathfrak{P}} = 1$ para casi toda $\mathfrak{P}$ (Corolario 3.4.7 y Teoremas 5.1.11 y 5.8.77).

Por tanto $|H^0(G, U_L)| = |H^1(G, U_L)| = \prod_{\mathfrak{P}} e_{\mathfrak{P}}$ y por tanto $h(U_L) = 1$ y $h(U_L/U_L \cap L^*) = h(U_L)h(U_L \cap L^*)^{-1} = 1$. De esta forma obtenemos $h(C_L) = n \cdot 1 \cdot 1 = n$.

Ahora consideremos una extensión de campos numéricos. Sea S un conjunto finito de primos de K tal que

1.- S contiene a los primos infinitos y a los primos ramificados.
2.- $J_L = J_{L,S} L^*$.
3.- $J_K = J_{K,S} K^*$.

Entonces $C_L = J_{L,S}L^*/L^* \cong J_{L,S}/L^S$, donde $L^S = J_{L,S} \cap L^*$ es el grupo de las S-unidades, $L^S = \{x \in L^* \mid v_{\mathfrak{P}}(x) = 0 \text{ para toda } \mathfrak{P} \notin S\}$ y $h(C_L) = h(J_{L,S})h(L^S)^{-1}$. Podemos considerar que $h(J_{L,S})$ es la parte local de $h(C_L)$ y que $h(L^S)$ es la parte global de $h(C_L)$.

Se va a probar que $h(L^S) = \frac{1}{n}\prod_{\mathfrak{p}\in S} n_{\mathfrak{p}}$ donde $n_{\mathfrak{p}} = [L_{\mathfrak{P}} : K_{\mathfrak{p}}]$ y donde $\mathfrak{P}$ es un primo fijo de L que divide a $\mathfrak{p}$, $n_{\mathfrak{p}} = |D_{L/K}(\mathfrak{P}|\mathfrak{p})| = |G_{\mathfrak{P}}| = |\operatorname{Gal}(L_{\mathfrak{P}}/K_{\mathfrak{p}})|$ donde $D_{L/K}(\mathfrak{P}|\mathfrak{p})$ es el grupo de descomposición.

Sea $s = |\bar{S}| = |\{\mathfrak{P} \in \mathbb{P}_L \mid \mathfrak{P}|_K \in S\}|$ y para cada $\mathfrak{P} \in \bar{S}$ sea $e_{\mathfrak{P}}$ un símbolo formal. Definimos $E^s := \bigoplus_{\mathfrak{P}\in\bar{S}} \mathbb{R}e_{\mathfrak{P}}$ como el espacio vectorial sobre los reales de dimensión s con base $\{e_{\mathfrak{P}} \mid \mathfrak{P} \in \bar{S}\}$. El grupo $G = \operatorname{Gal}(L/K)$ actúa en E^s por $\sigma(e_{\mathfrak{P}}) = e_{\sigma\mathfrak{P}}$ para $\sigma \in G$.

Sea M una red en E^s, esto es, M es un subgrupo abeliano libre de E^s de rango s y tal que una $\mathbb{Z}$-base de este subgrupo es una $\mathbb{R}$-base de E^s. Supongamos que M es invariante bajo G, es decir, $\sigma M \subseteq M$ para toda $\sigma \in G$. Veremos que existe una subred M_0 de M de índice finito que tiene una $\mathbb{Z}$-base $\{y_{\mathfrak{P}} \mid \mathfrak{P} \in \bar{S}\}$ tal que $\sigma y_{\mathfrak{P}} = y_{\sigma\mathfrak{P}}$.

Para esto tomemos la norma infinita $\| \ \|_\infty$ de E^s con respecto a las coordenadas relativas a la base $\{e_{\mathfrak{P}} \mid \mathfrak{P} \in \bar{S}\}$. Esto es, $\|\sum_{\mathfrak{P}\in\bar{S}} d_{\mathfrak{P}}e_{\mathfrak{P}}\|_\infty = \text{máx}_{\mathfrak{P}\in\bar{S}}\{|d_{\mathfrak{P}}|\}$. Puesto que M es una red, existe N tal que para cada $x \in E^s$, existe $y \in M$ con $\|x - y\|_\infty < N$. Para cada $\mathfrak{p} \in S$, sea $\mathfrak{P}_0 \in \bar{S}$ un primo fijo de L sobre $\mathfrak{p}$. Sean $t \in \mathbb{R}$, $t > s \cdot n \cdot N$ y $z_{\mathfrak{P}_0} \in M$ tal que $\|te_{\mathfrak{P}} - z_{\mathfrak{P}_0}\|_\infty < N$.

Para $\mathfrak{P}|\mathfrak{p}$, sea $y_{\mathfrak{P}} := \sum_{\sigma\mathfrak{P}_0=\mathfrak{P}} \sigma z_{\mathfrak{P}_0}$. Sea $M_0 = \bigoplus_{\mathfrak{P}\in\bar{S}} \mathbb{Z}y_{\mathfrak{P}}$. Para $\tau \in G$, se tiene

$$\tau y_{\mathfrak{P}} = \sum_{\sigma\mathfrak{P}_0=\mathfrak{P}} \tau\sigma z_{\mathfrak{P}_0} \underset{\substack{\rho=\tau\sigma \\ \uparrow \\ \rho\mathfrak{P}_0=\tau\sigma\mathfrak{P}_0=\tau\mathfrak{P}}}{=} \sum_{\rho\mathfrak{P}_0=\tau\mathfrak{P}} \rho z_{\mathfrak{P}_0} = y_{\tau\mathfrak{P}}.$$

Debemos ver que $\{y_{\mathfrak{P}} \mid \mathfrak{P} \in \bar{S}\}$ es linealmente independiente sobre $\mathbb{R}$. Sea $\sum_{\mathfrak{P}\in\bar{S}} c_{\mathfrak{P}}y_{\mathfrak{P}} = 0$ con $c_{\mathfrak{P}} \in \mathbb{R}$. Si algún $c_{\mathfrak{P}} \neq 0$, definimos $r = \text{máx}\{|c_{\mathfrak{P}}| \mid \mathfrak{P} \in \bar{S}\} > 0$. Por tanto tenemos $\sum_{\mathfrak{P}\in\bar{S}} \frac{c_{\mathfrak{P}}}{\pm r}y_{\mathfrak{P}} = 0$. Podemos suponer que $|c_{\mathfrak{P}}| \leq 1$ para toda $\mathfrak{P} \in \bar{S}$ y $c_{\mathfrak{P}'} = 1$ para algún $\mathfrak{P}'$.

Sea $z_{\mathfrak{P}_0} = te_{\mathfrak{P}_0} + b_{\mathfrak{P}_0}$ con $b_{\mathfrak{P}_0}$ un vector tal que $\|b_{\mathfrak{P}_0}\|_\infty < N$. Entonces

$$y_{\mathfrak{P}} = \sum_{\sigma\mathfrak{P}_0=\mathfrak{P}} \sigma z_{\mathfrak{P}_0} = t \sum_{\sigma\mathfrak{P}_0=\mathfrak{P}} e_{\sigma\mathfrak{P}_0} + b'_{\mathfrak{P}}$$

con $\|b'_{\mathfrak{P}}\|_\infty \leq n \cdot N$. Por tanto

$$y_{\mathfrak{P}} = tm_{\mathfrak{P}}e_{\mathfrak{P}} + b'_{\mathfrak{P}} \quad \text{con} \quad m_{\mathfrak{P}} = |\{\sigma \in G \mid \sigma\mathfrak{P}_0 = \mathfrak{P}\}| = |D_{L/K}(\mathfrak{P}_0|\mathfrak{p})| = n_{\mathfrak{p}}.$$

Se sigue que $0 = \sum_{\mathfrak{P}} c_{\mathfrak{P}}y_{\mathfrak{P}} = t\sum_{\mathfrak{P}} c_{\mathfrak{P}}m_{\mathfrak{P}}e_{\mathfrak{P}} + b'$ con $\|b'\|_\infty \leq s \cdot n \cdot N$. De esta forma, se tiene

$$\sum_{\mathfrak{P}} c_{\mathfrak{P}} m_{\mathfrak{P}} e_{\mathfrak{P}} = -\frac{b'}{t},$$

$$\Big\| \sum_{\mathfrak{P}} c_{\mathfrak{P}} m_{\mathfrak{P}} e_{\mathfrak{P}} \Big\|_\infty = \max_{\mathfrak{P}} |c_{\mathfrak{P}} m_{\mathfrak{P}}| \geq c_{\mathfrak{P}'} m_{\mathfrak{P}'} = m_{\mathfrak{P}'} \geq 1 \quad \text{y}$$

$$\Big\| -\frac{b'}{t} \Big\|_\infty = \frac{1}{t}\|b'\|_\infty < 1, \quad \text{de donde obtenemos} \quad m_{\mathfrak{P}'} \leq \frac{1}{t}\|b'\|_\infty < 1,$$

lo cual es una contradicción, probando que M_0 satisface lo requerido.

Sea $\mu : L^S \longrightarrow E^s$ dada por $\mu(x) = \sum_{\mathfrak{P}\in\bar{S}} \log|x|_{\mathfrak{P}} \cdot e_{\mathfrak{P}}$. La imagen es una red $s-1$ dimensional con núcleo finito (Teorema 6.1.17).

Para $\sigma \in G$, se tiene

$$\mu(\sigma x) = \sum_{\mathfrak{P}} \log|\sigma x|_{\mathfrak{P}} e_{\mathfrak{P}} = \sum_{\mathfrak{P}} \log|x|_{\sigma^{-1}\mathfrak{P}} \underbrace{\sigma e_{\sigma^{-1}\mathfrak{P}}}_{\| \; e_{\mathfrak{P}}}$$

$$= \sigma\big(\sum_{\mathfrak{P}} \log|x|_{\sigma^{-1}\mathfrak{P}} e_{\sigma^{-1}\mathfrak{P}}\big) = \sigma\mu(x),$$

por lo que μ es un G-homomorfismo.

Sea $e_0 := \sum_{\mathfrak{P}\in\bar{S}} e_{\mathfrak{P}}$. Entonces e_0 y $\mu(L^S)$ generan una red s-dimensional M en E^s. Puesto que $\mathbb{Z}e_0$ es G-isomorfo a $\mathbb{Z}$, de la sucesión exacta

$$0 \longrightarrow \mathbb{Z}e_0 \longrightarrow M \longrightarrow M/\mathbb{Z}e_0 \longrightarrow 0$$

y de que $M/\mathbb{Z}e_0 \cong \mu(L^s)$ deducimos que

$$h(L^s) = h(\mu(L^s)) = h(\mathbb{Z})^{-1} \cdot h(M) = \frac{1}{n} h(M).$$

Sea M_0 la subred de M de índice finito en M como antes. Entonces

$$M_0 \cong \bigoplus_{\mathfrak{p}\in S} \bigoplus_{\mathfrak{P}|\mathfrak{p}} \mathbb{Z}y_{\mathfrak{P}} \cong \bigoplus_{\mathfrak{p}\in S} M_0^{\mathfrak{p}} \quad \text{y} \quad M_0^{\mathfrak{p}} = \bigoplus_{\mathfrak{P}|\mathfrak{p}} \mathbb{Z}y_{\mathfrak{P}} = \bigoplus_{\sigma\in G/G_{\mathfrak{P}}} \sigma\big(\mathbb{Z}y_{\mathfrak{P}_0}\big).$$

Por el Lema de Shapiro, se tiene

$$h(M_0^{\mathfrak{p}}) = h(G_{\mathfrak{P}}, \mathbb{Z}y_{\mathfrak{P}_0}) = |G_{\mathfrak{P}}| = n_{\mathfrak{p}}$$

y como M/M_0 es finito, $h(M) = h(M_0)$, lo que implica que

$$h(L^S) = \frac{1}{n} h(M) = \frac{1}{n} \prod_{\mathfrak{p}\in S} h(G_{\mathfrak{P}}, \mathbb{Z}y_{\mathfrak{P}_0}) = \frac{1}{n} \prod_{\mathfrak{p}\in S} n_{\mathfrak{p}}.$$

Ahora

$$H^q(G, J_{L,S}) = \prod_{\mathfrak{p}\in S} H^q(G_{\mathfrak{P}}, L_{\mathfrak{P}}^*), \quad \text{por tanto}$$

$$h(G, J_{L,S}) = \prod_{\mathfrak{p}\in S} \underbrace{h(G_{\mathfrak{P}}, L_{\mathfrak{P}}^*)}_{\| \; G_{\mathfrak{p}}} = \prod_{\mathfrak{p}\in S} |G_{\mathfrak{p}}| = \prod_{\mathfrak{p}\in S} n_{\mathfrak{p}}.$$

Se sigue que

$$h(C_L) = h(J_{L,S})h(L^s)^{-1} = \Big(\prod_{\mathfrak{p}\in S} n_{\mathfrak{p}}\Big) \cdot \frac{n}{\Big(\prod_{\mathfrak{p}\in S} n_{\mathfrak{p}}\Big)} = n. \qquad \square$$

Corolario 6.5.2 (Caso especial del teorema de densidad de Chebotarev). *Sea L/K una extensión cíclica de campos globales de grado una potencia de un primo $n = p^m$. Entonces existe una infinidad de primos de K que no se descomponen totalmente en L. Como consecuencia tenemos que hay una infinidad de primos totalmente inertes en L/K.*

Demostración. Supongamos primero que L/K es cíclica de grado p. Sea S el conjunto de primos de K que no se descomponen en L/K. Si S fuese finito se probará que $\mathrm{N}_{L/K} C_L = C_K$ lo que contradice que $[C_K : \mathrm{N}_{L/K} C_L] \geq p$.

Sea $\vec{\alpha} \in J_K$. Por el teorema de aproximación, tenemos que existe $a \in K^*$ tal que $(\vec{\alpha}a^{-1})_{\mathfrak{p}} = \alpha_{\mathfrak{p}} a^{-1}$ está contenido en el subgrupo abierto $\mathrm{N}_{L_{\mathfrak{P}}/K_{\mathfrak{p}}} L_{\mathfrak{P}}^*$ de $K_{\mathfrak{p}}^*$ (es abierto por el teorema de existencia para campos locales) para toda $\mathfrak{p} \in S$.

Para $\mathfrak{p} \notin S$, $\mathfrak{p}$ se descompone totalmente en L/K y por tanto $L_{\mathfrak{P}} = K_{\mathfrak{p}}$ y por tanto $(\vec{\alpha}a^{-1})_{\mathfrak{p}} \in \mathrm{N}_{L_{\mathfrak{P}}/K_{\mathfrak{p}}} L_{\mathfrak{P}}^* = K_{\mathfrak{P}}^*$. Entonces $(\vec{\alpha}a^{-1})_{\mathfrak{p}} = \alpha_{\mathfrak{p}} a^{-1}$ es una norma local para toda $\mathfrak{p} \in \mathbb{P}_K$. Por tanto $\vec{\alpha}a^{-1}$ es una norma de un idèle $\vec{\beta}$ de L (Teorema 6.3.9). Por tanto $\vec{\alpha} = \big(\mathrm{N}_{L/K}\, \vec{\beta}\big) \cdot a \in \big(\mathrm{N}_{L/K}\, J_L\big) \cdot K^*$. Se sigue que $\tilde{\vec{\alpha}} \in \mathrm{N}_{L/K} C_L$ y $C_K = \mathrm{N}_{L/K} C_L$.

Ahora sea L/K cíclica de grado p^m y sea M la única subextensión de grado p: $[M : K] = p$. Hay una infinidad de primos inertes en M/K, lo que implica que hay una infinidad de primos no totalmente descompuestos en L.

Finalmente, si $\mathfrak{p}$ es inerte en M/K, entonces $\mathfrak{p}$ es totalmente inerte en L/K pues si $G_{\mathfrak{P}}$ es el grupo de descomposición de $\mathfrak{P}|\mathfrak{p}$ y como la extensión L/K consiste de una única torre de extensiones de grado p (por ser la extensión cícica), se tiene que $\mathrm{Gal}(L/M) \subsetneqq G_{\mathfrak{P}}$ puesto que $\mathfrak{p}$ es inerte en M/K. Por tanto $G_{\mathfrak{P}} = \mathrm{Gal}(L/K)$ y $\mathfrak{p}$ es totalmente inerte en L/K. $\square$

Corolario 6.5.3. *Sea L/K es cualquier extensión finita y separable de campos globales con $L \neq K$. Entonces hay una infinidad de primos $\mathfrak{p}$ de K que no se descomponen totalmente en L/K. En otras palabras, si $L_{\mathfrak{P}} = K_{\mathfrak{p}}$ para casi toda $\mathfrak{p}$, entonces $L = K$.*

Demostración. Si $\tilde{L}$ es la cerradura de Galois de L/K, entonces un primo de K se descompone totalmente en L si y solamente si se descompone totalmente en $\tilde{L}$. Por tanto, podemos suponer que L/K es una extensión de Galois.

Sea $H < G$ un subgrupo cíclico de orden una potencia de un número primo, $|H| = p^m$ y sea $M := L^H$. Entonces hay una infinidad de primos de M que no se descomponen totalmente en L. Se sigue el resultado. $\square$

Observación 6.5.4. El Corolario 6.5.3 es un caso particular del Teorema de densidad de Chebotarev el cual establece que en cualquier extensión finita de Galois de campos globales, todas las posibles descomposiciones posibles de primos, tienen densidad positiva.

Teorema 6.5.5. *Sea $L = K_1 \cdots K_r/K$ una extensión abeliana p-elemental de campos globales, donde p es un número primo. Se tiene* $\mathrm{Gal}(L/K) \cong C_p^r = C_p \times \cdots \times C_p$. *Entonces existe una infinidad de primos $\mathfrak{p}$ de K que son inertes en K_1/K y son totalmente descompuestos en K_i/K para toda $i \geq 2$.*

Demostración. Se tiene que $L/K_2 \cdots K_r$ es cíclica de grado p. Sea $\mathfrak{q}$ un primo de $K_2 \cdots K_r$ que permanece primo en L y tal que $\mathfrak{q}|_K = \mathfrak{p}$ es no ramificado. De esta forma se tiene $L_\mathfrak{q}/(K_2 \cdots K_r)_\mathfrak{q}$ es cíclica de grado p. Por otro lado, $L_\mathfrak{q}/K_\mathfrak{p}$ es un grupo cíclico puesto que $\mathfrak{p}$ es no ramificado y $\mathrm{Gal}(L_\mathfrak{q}/K_\mathfrak{p})$ es isomorfo al grupo de Galois de los campos residuales los cuales son campos finitos.

Puesto que $\mathrm{Gal}(L/K) \cong C_p^r$, se tiene que $[L_\mathfrak{q} : K_\mathfrak{p}] \leq p$ y, por otro lado, como $[L_\mathfrak{q} : K_\mathfrak{p}] \geq [L_\mathfrak{q} : (K_2 \cdots K_r)_\mathfrak{q}] = p$, se sigue que $(K_2 \cdots K_r)_\mathfrak{q} = K_\mathfrak{p}$ por lo que $\mathfrak{p}$ se descompone totalmente en $K_2 \cdots K_r/K$. Además $\mathfrak{p}$ es inerte en K_1/K pues $f_\mathfrak{p}(L|K) = p$. □

Otra consecuencia de la primera desigualdad es el teorema de F.K. Schmidt.

Teorema 6.5.6 (F. K. Schmidt). *Sea K un campo global de funciones. Entonces existe un divisor de K de grado* 1.

Demostración. Sea $\mathrm{gr} : D_K \longrightarrow \mathbb{Z}$ y sea $\mathrm{gr}(D_K) = \rho\mathbb{Z}$ para algún $\rho \in \mathbb{N}$. Sea $k = \mathbb{F}_q$ el campo de constantes de K. Sea $k_1 := \mathbb{F}_{q^\rho}$ la extensión de k de grado ρ y sea $K_1 = Kk_1$ la extensión de constantes. Para cada primo $\mathfrak{p}$ de K, el campo residual $K(\mathfrak{p}) \cong \mathbb{F}_{q^{\mathrm{gr}\,\mathfrak{p}}}$ contiene a k_1 pues $\rho | \mathrm{gr}\,\mathfrak{p}$. Por tanto, si $\mathfrak{P}|\mathfrak{p}$, con $\mathfrak{P}$ primo en K_1, entonces $(K_1)_\mathfrak{P} = K_\mathfrak{p}$ puesto que $(K_1)_\mathfrak{P} = K_\mathfrak{p} \cdot k_1 = K_\mathfrak{p}$, esto es, todo primo de K se descompone totalmente en K_1 de donde se sigue que $\mathbb{F}_{q^\rho} = \mathbb{F}_q$ y que $\rho = 1$. □

6.6. Segunda desigualdad fundamental

La segunda desigualdad será válida para cualquier extensión finita de Galois de campos globales. Por otro lado, la primera desigualdad únicamente es válida para extensiones abelianas. Esto dirá más adelante que si L/K es una extensión finita y separable de campos globales, entonces

$$[C_K : \mathrm{N}_{L/K}\, C_L] = [L : K] \iff L/K \text{ es abeliana.}$$

La segunda desigualdad establece que si L/K es una extensión finita de Galois de campos globales, entonces $[C_K : \mathrm{N}_{L/K}\, C_L] \big| [L : K]$.

Reduciremos este problema para probar que es suficiente probar la desigualdad para una extensión L/K cíclica de grado primo l.

Lema 6.6.1. *Si E/K es cualquier extensión finita y separable, entonces $[C_K : \mathrm{N}_{E/K}\, C_E]$ es finita y divide a una potencia de $m = [E : K]$.*

Demostración. Sea L/K la cerradura normal de E/K. Entonces se tiene $\mathrm{N}_{L/K}\, C_L \subseteq \mathrm{N}_{E/K}\, C_E$. Por tanto

$$[C_K : \mathrm{N}_{L/K}\, C_L] = [C_K : \mathrm{N}_{E/K}\, C_E][\mathrm{N}_{E/K}\, C_E : \mathrm{N}_{L/K}\, C_L].$$

Si probamos que $[C_K : \mathrm{N}_{L/K}\, C_L]$ es finita, entonces $[C_K : \mathrm{N}_{E/K}\, C_E]$ es finita, por lo tanto, para la finitud, basta considerar el caso cuando E/K es de Galois.

Sea pues E/K Galois. Sea S un conjunto finito de primos incluyendo a los arquimedianos, a los primos ramificados y suficientemente grande tal que $J_K = J_{K,S}K^*$ y $J_E = J_{E,S}E^*$ (por ser E/K normal). Entonces

$$K^*\, \mathrm{N}_{E/K}\, J_E = K^*\, \mathrm{N}_{E/K}\, E^* \cdot \mathrm{N}_{E/K}\, J_{E,S} = K^*\, \mathrm{N}_{E/K}\, J_{E,S}.$$

Por tanto

$$\begin{aligned}
[J_K : K^*\, \mathrm{N}_{E/K}\, J_E] &= [K^* J_{K,S} : K^*\, \mathrm{N}_{E/K}\, J_{E,S}] \leq [J_{K,S} : \mathrm{N}_{E/K}\, J_{E,S}] \\
&= \Big[\prod_{v\in S} K_v^* \times \prod_{v\notin S} U_v : \prod_{v\in S}\prod_{\omega|v} \mathrm{N}_{E_\omega/K_v}\, E_\omega^* \times \prod_{v\notin S}\prod_{\omega|v} U_\omega \Big] \\
&\underset{\substack{\uparrow \\ v\notin S \Rightarrow v \\ \text{no ramificado}}}{=} \Big[\prod_{v\in S} K_v^* \times \prod_{v\in S} U_v : \prod_{v\in S}\prod_{\omega|v} \mathrm{N}_{E_\omega/K_v}\, E_\omega^* \times \prod_{v\notin S} U_v \Big] \\
&\underset{\substack{\uparrow \\ E/K \text{ Galois}}}{\leq} \prod_{v\in S} [K_v^* : \mathrm{N}_{E_\omega/K_v}\, E_\omega^*] \underset{\substack{\uparrow \\ \text{Teorema de} \\ \text{reciprocidad local}}}{=} \prod_{v\in S} [E_\omega : K_v] \\
&= \prod_{v\in S} n_v < \infty.
\end{aligned}$$

Esto prueba la finitud.

Ahora, el índice de la norma divide a una potencia de grado $m = [E : K]$, la extensión siendo normal o no, pues si $\vec{\alpha} \in C_K$, $\vec{\alpha}^m = \mathrm{N}_{E/K}\, \vec{\alpha} \in \mathrm{N}_{E/K}\, C_E$, lo que implica $C_K/\,\mathrm{N}_{E/K}\, C_E$ es subgrupo de $\big(\mathbb{Z}/m\mathbb{Z}\big)^r$ para algún $r \in \mathbb{N}$. □

Lema 6.6.2. *Sea $K \subseteq F \subseteq E$ dos extensiones finitas. Entonces*

(a) $[C_K : \mathrm{N}_{F/K}\, C_F] \big| [C_K : \mathrm{N}_{E/K}\, C_E]$.
(b) $[C_K : \mathrm{N}_{E/K}\, C_E] \big| [C_K : \mathrm{N}_{F/K}\, C_F] \cdot [C_F : \mathrm{N}_{E/F}\, C_E]$.

Por tanto, si la desigualdad se presenta en los pasos de la torre, se tiene la desigualdad en la torre misma.

Demostración. Se tiene

$$[C_K : \mathrm{N}_{E/K}\, C_E] = [C_K : \mathrm{N}_{F/K}\, C_F][\mathrm{N}_{F/K}\, C_F : \mathrm{N}_{F/K}(\mathrm{N}_{E/F}\, C_E)]$$

lo cual prueba (a).

Ahora, el mapeo $C_F \longrightarrow \mathrm{N}_{F/K}\, C_F$, $\vec{\alpha} \longmapsto \mathrm{N}_{F/K}\, \vec{\alpha}$, es un homomorfismo. Se tiene el epimorfismo inducido

$$\frac{C_F}{\mathrm{N}_{E/F}\, C_E} \xrightarrow{\mathrm{N}_{F/K}} \frac{\mathrm{N}_{F/K}\, C_F}{\mathrm{N}_{F/K}\left(\mathrm{N}_{E/F}\, C_E\right)} = \frac{\mathrm{N}_{F/K}\, C_F}{\mathrm{N}_{E/K}\, C_E},$$

por lo que $[\mathrm{N}_{F/K}\, C_F : \mathrm{N}_{F/K}(\mathrm{N}_{E/F}\, C_E)]$ divide a $[C_F : \mathrm{N}_{E/F}\, C_E]$ de donde se sigue (b). □

Corolario 6.6.3. *Si la segunda desigualdad se cumple para todas las extensiones cíclicas de grado primo, entonces se cumple para todas las extensiones de Galois.*

Demostración. Sea L/K una extensión de Galois y sea l un número primo. Sea E el campo fijo de L de un l-subgrupo de Sylow del grupo $G = \mathrm{Gal}(L/K)$. Se tiene que L/E es una torre de extensiones cíclicas de grado l y la desigualdad se cumple en L/E por el Lema 6.6.2, esto es $[C_E : \mathrm{N}_{L/E}\, C_L] \big| [L : E]$.

Por otro lado $[C_K : \mathrm{N}_{E/K}\, C_E]$ divide a una potencia $[E : K]$ y por tanto es primo relativo a l. Ahora, por el Lema 6.6.2, se tiene que

$$[C_K : \mathrm{N}_{L/K}\, C_L] \big| [C_K : \mathrm{N}_{E/K}\, C_E][C_E : \mathrm{N}_{L/E}\, C_L],$$

por lo que para cada número primo l, la l-contribución de $[C_K : \mathrm{N}_{L/K}\, C_L]$ divide a $[L : E]$ y por tanto a $[L : K]$. La desigualdad se sigue para L/K. □

Corolario 6.6.4. *Si l un número primo con $l \neq p$ donde p es la característica de K, es suficiente probar la segunda desigualdad para extensiones cíclicas de K de orden l suponiendo que una l-raíz primitiva ζ_l de la unidad está en K.*

Demostración. Sea L/K una extensión cíclica de grado l. Entonces

$$[C_K : \mathrm{N}_{L/K}\, C_L] \big| [C_K : \mathrm{N}_{L(\zeta_l)/K}\, C_{L(\zeta_l)}] \quad \text{y}$$
$$[C_K : \mathrm{N}_{L(\zeta_l)/K}\, C_{L(\zeta_l)}] \big| [C_K : \mathrm{N}_{K(\zeta_l)/K}\, C_{K(\zeta_l)}] \cdot [C_{K(\zeta_l)} : \mathrm{N}_{L(\zeta_l)/K(\zeta_l)}\, C_{L(\zeta_l)}].$$

Además $[C_K : \mathrm{N}_{K(\zeta_l)/K}\, C_{K(\zeta_l)}]$ es primo relativo a l pues $[K(\zeta_l) : K] | l - 1$ y $[C_K : \mathrm{N}_{L/K}\, C_L]$ es una potencia de l y divide a $[C_{K(\zeta_l)} : \mathrm{N}_{L(\zeta_l)/K(\zeta_l)}\, C_{L(\zeta_l)}]$, una extensión cíclica de grado primo de un campo que contiene a ζ_l. □

6.6.1. Segunda desigualdad para extensiones de Kummer

Sea K un campo global que contiene a las n-raíces de la unidad, $\zeta_n \in K$ y donde n es una potencia de un número primo diferente a la característica p de K. Sea L/K una extensión de Galois con grupo de Galois $\mathrm{Gal}(L/K) \cong (\mathbb{Z}/n\mathbb{Z})^r$.

Sea S un conjunto finito no vacío de lugares de K conteniendo a los primos infinitos, a los primos que dividen a n, a los primos ramificados en L y suficientemente grande tal que $J_K = J_{K,S}K^*$. Sea $s = |S|$.

Proposición 6.6.5. *Se tiene que $s \geq r$ y que existe un conjunto T de $s - r$ primos de K, disjunto de S, tal que $L = K(\sqrt[n]{\Delta})$ donde Δ es el núcleo del homomorfismo $K^S \longrightarrow \prod_{\mathfrak{p}\in T} K_{\mathfrak{p}}^*/(K_{\mathfrak{p}}^*)^n$.*

Demostración. Se tiene que $L = K(\sqrt[n]{D})$ donde $D = (L^*)^n \cap K^*$ por la Teoría de Kummer, Teorema 2.4.2. Si $x \in D$, entonces $K_{\mathfrak{p}}(\sqrt[n]{x})/K_{\mathfrak{p}}$ es no ramificado para todo $\mathfrak{p} \notin S$. Por tanto $x = u_{\mathfrak{p}} y_{\mathfrak{p}}^n$ con $u_{\mathfrak{p}} \in U_{\mathfrak{p}}$ y $y_{\mathfrak{p}} \in K_{\mathfrak{p}}^*$.

Definimos $y_{\mathfrak{p}} = 1$ para $\mathfrak{p} \in S$ de tal forma que se define un idèle $\vec{y}$ que se puede escribir $\vec{y} = \vec{\alpha} \cdot z$ con $\vec{\alpha} \in J_{K,S}$, $z \in K^*$. Ahora bien

$$xz^{-n} = u_{\mathfrak{p}} y_{\mathfrak{p}}^n z^{-n} = u_{\mathfrak{p}} \alpha_{\mathfrak{p}}^n z^n z^{-n} = u_{\mathfrak{p}} \alpha_{\mathfrak{p}}^n \in U_{\mathfrak{p}}$$

para toda $\mathfrak{p} \notin S$, de tal forma que $xz^{-n} \in J_{K,S} \cap K^* = K^S$, por lo que $xz^{-n} \in \Delta := (L^*)^n \cap K^S$. Por tanto $D = \Delta(K^*)^n$ (pues claramente, $\Delta \subseteq D$), de donde $L = K(\sqrt[n]{\Delta})$.

El campo $M := K(\sqrt[n]{K^S})$ contiene a L puesto que $\Delta \subseteq K^S$. Nuevamente, por Teoría de Kummer, tenemos $\mathrm{Gal}(M/K) \cong \mathrm{Hom}\left(K^S/(K^S)^n, \langle\zeta_n\rangle\right)$. Puesto que K^S tiene rango finito $s - 1$ (Teorema 6.1.17) y contiene a $\langle\zeta_n\rangle$, se tiene que $K^S/(K^S)^n \cong (\mathbb{Z}/n\mathbb{Z})^s$. Por tanto $\mathrm{Gal}(M/K) \cong (\mathbb{Z}/n\mathbb{Z})^n$ y como $\frac{\mathrm{Gal}(M/K)}{\mathrm{Gal}(M/L)} \cong \mathrm{Gal}(L/K) \cong (\mathbb{Z}/n\mathbb{Z})^r$, se tiene que $r \leq s$ y $\mathrm{Gal}(M/L) \cong (\mathbb{Z}/n\mathbb{Z})^{s-r}$.

Sean $\{\sigma_1, \ldots, \sigma_{s-r}\}$ una $(\mathbb{Z}/n\mathbb{Z})$-base de $\mathrm{Gal}(M/L)$, M_i el campo fijo de σ_i, $M_i = M^{\langle\sigma_i\rangle}$ y $L = \bigcap_{i=1}^{s-r} M_i$. Para cada $1 \leq i \leq s - r$, sea $\mathfrak{P}_i$ un primo de M_i totalmente inerte en M/M_i y tal que $\mathfrak{p}_i := \mathfrak{P}_i|_K \notin S$. Además, seleccionamos estos primos $\mathfrak{p}_i$ distintos. Esto se puede hacer por el Corolario 6.5.2.

Puesto que $\mathfrak{p}_i \notin S$, se tiene que $\mathfrak{p}_i$ es no ramificado en M/K pues $M = K(\sqrt[n]{K^S})$ y por tanto $\mathfrak{p}_i$ es no ramficado en cada $K(\sqrt[n]{x})$, $x \in K^S$. Sea Z_i el campo de descomposición del único primo $\mathfrak{q}_i$ de M sobre $\mathfrak{P}_i$, $1 \leq i \leq s - r$ en M/K. Como $\mathfrak{P}_i$ es totalmente inerte en M/M_i, se tiene $Z_i \supseteq M_i$. Por otro lado, el grupo de descomposición $D_i = D_{M/K}(\mathfrak{q}_i|\mathfrak{p}_i)$ es cíclico pues $\mathfrak{p}_i$ es no ramificado. Puesto que $D_i \subseteq \mathrm{Gal}(M/K) = \left(\mathbb{Z}/n\mathbb{Z}\right)^s$, D_i tiene exponente n de donde se sigue que D_i es de orden un divisor de n. Por tanto $Z_i \subseteq M_i$. En resumen, M_i es el campo de descomposición de $\mathfrak{q}_i$ en M/K.

Sea $T := \{\mathfrak{p}_1, \ldots, \mathfrak{p}_{s-r}\}$. Puesto que $L = \bigcap_{i=1}^{s-r} M_i$, se tiene que L/K es la máxima subextensión de M/K en el cual todos los primos $\mathfrak{p}_1, \ldots, \mathfrak{p}_{s-r}$ son totalmente descompuestos. Por tanto, si $x \in K^S$, se tiene

$$x \in \Delta \iff K(\sqrt[n]{x}) \subseteq L \iff K_{\mathfrak{p}_i}(\sqrt[n]{x}) = K_{\mathfrak{p}_i}, \quad i = 1, \ldots, s-r$$
$$\iff x \in (K^*_{\mathfrak{p}_i})^n, \quad i = 1, \ldots, s-r,$$

probando que Δ es el núcleo del mapeo natural

$$K^S \longrightarrow \prod_{i=1}^{s-r} K^*_{\mathfrak{p}_i}/(K^*_{\mathfrak{p}_i})^n, \quad x \longmapsto \prod_{i=1}^{s-r} x \text{ mód } (K^*_{\mathfrak{p}_i})^n. \qquad \square$$

Lema 6.6.6. *Sean S y T como en la Proposición* 6.6.5 *y sean*

$$J_K(S,T) := \prod_{\mathfrak{p}\in S}(K^*_{\mathfrak{p}})^n \times \prod_{\mathfrak{p}\in T} K^*_{\mathfrak{p}} \times \prod_{\mathfrak{p}\notin(S\cup T)} U_{\mathfrak{p}},$$

y

$$C_K(S,T) := J_K(S,T)K^*/K^*.$$

Entonces $J_K(S,T) \cap K^* = (K^{S\cup T})^n$.

Demostración. Es inmediato de $(K^{(S\cup T)})^n \subseteq J_K(S,T) \cap K^*$. Sea $y \in J_K(S,T) \cap K^*$ y sea $N = K(\sqrt[n]{y})$. Para probar que $N = K$ basta probar que $C_K = \mathrm{N}_{N/K} C_N$ pues por la primera desigualdad, se tiene $[C_K : \mathrm{N}_{N/K} C_N] \geq [N : K]$.

Sea $\tilde{\vec{\alpha}} \in C_K = J_{K,S}K^*/K^*$ y sea $\vec{\alpha}$ un representante de $\tilde{\vec{\alpha}}$. El mapeo $K^S \longrightarrow \prod_{\mathfrak{p}\in T} U_{\mathfrak{p}}/(U_{\mathfrak{p}})^n$ es sobre pues Δ es su núcleo y se tiene $|K^S/\Delta| = \frac{|K^S/(K^S)^n|}{|\Delta/(K^S)^n|} = \frac{n^s}{|\mathrm{Gal}(L/K)|} = n^{s-r}$, $|U_{\mathfrak{p}}/(U_{\mathfrak{p}})^n| = \frac{n}{n_{\mathfrak{p}}} = n$, donde $n_{\mathfrak{p}} = q^{-v_{\mathfrak{p}}(n)} = 1$, (Proposición 5.3.1) y por tanto $\left|\prod_{\mathfrak{p}\in T} U_{\mathfrak{p}}/(U_{\mathfrak{p}})^n\right| = n^{s-r}$.

Por tanto existe $x \in K^S$ con $\alpha_{\mathfrak{p}} = xu^n_{\mathfrak{p}}$ con $u_{\mathfrak{p}} \in U_{\mathfrak{p}}$ para $\mathfrak{p} \in T$. El idèle $\vec{\beta} = \vec{\alpha}x^{-1}$ pertenece a la misma clase $\vec{\alpha}$ y veremos que $\vec{\beta} \in \mathrm{N}_{N/K} J_N$. Para esto, por el teorema de la norma de idèles, Teorema 6.3.9, necesitamos que cada componente $\beta_{\mathfrak{p}}$ sea una norma de $N_{\mathfrak{P}}/K_{\mathfrak{p}}$. Para $\mathfrak{p} \in S$ esto se cumple puesto que $y \in (K^*_{\mathfrak{p}})^n$ por lo que $N_{\mathfrak{P}} = K_{\mathfrak{p}}$. Para $\mathfrak{p} \in T$ esto se cumple pues $\beta_{\mathfrak{p}} = u^n_{\mathfrak{p}}$ es una n-potencia.

Para $\mathfrak{p} \in S \cup T$, $\beta_{\mathfrak{p}}$ es una unidad y $N_{\mathfrak{P}}/K_{\mathfrak{p}}$ es no ramificada, por lo que $\mathrm{N}_{N_{\mathfrak{P}}/K_{\mathfrak{p}}} U_{\mathfrak{P}} = U_{\mathfrak{p}}$ (Teoremas 5.1.11 y 6.1.18). Por tanto $C_K = \mathrm{N}_{N/K} C_N$ de donde se sigue que $N = K$ y por tanto $y \in (K^*)^n \cap J_K(S,T) \subseteq \left(K^{(SUT)}\right)^n$. De esta forma obtenemos que $J_K(S,T) \cap K^* = \left(K^{(S\cup T)}\right)^n$. $\square$

Teorema 6.6.7. *Con las notaciones anteriores, se tiene que $\mathrm{N}_{L/K} C_L \supseteq C_K(S,T)$ y $[C_K : C_K(S,T)] = [L : K]$.*

En particular, $[C_K : \mathrm{N}_{L/K} C_L] \big| [C_K : C_K(S,T)] = [L : K]$.

Cuando L/K es cíclica, esto es, $r = 1$, entonces $\mathrm{N}_{L/K} C_L = C_K(S,T)$ y $[C_K : \mathrm{N}_{L/K} C_L] = [L : K]$.

Demostración. Se tiene la sucesión exacta

$$1 \longrightarrow \frac{J_{K,S\cup T} \cap K^*}{J_K(S,T) \cap K^*} \longrightarrow \frac{J_{K,S\cup T}}{J_{K(S,T)}} \twoheadrightarrow \frac{J_{K,S\cup T}K^*}{J_K(S,T)K^*} \longrightarrow 1.$$

Puesto que $J_{K,S\cup T}K^* = J_K$, el orden del último grupo es

$$[J_{K,S\cup T}K^* : J_K(S,T)K^*] = \left[J_K/K^* : J_K(S,T)K^*/K^*\right] = [C_K : C_K(S,T)].$$

El orden del primer grupo es

$$[J_{K,S\cup T} \cap K^* : J_K(S,T) \cap K^*] = [K^{S\cup T} : (K^{S\cup T})^n] = n^{s+s-r} = n^{2s-r},$$

pues $\langle \zeta_n \rangle \subseteq K^{S\cup T}$. El orden del grupo intermedio es

$$\begin{aligned}[J_{K,S\cup T} : J_K(S,T)] &= \prod_{\mathfrak{p}\in S}[K_\mathfrak{p}^* : (K_\mathfrak{p}^*)^n] \underset{\text{Proposición 5.3.1}}{\overset{\uparrow}{=}} \prod_{\mathfrak{p}\in S}\frac{n^2}{|n|_\mathfrak{p}} \\ &= n^{2s}\prod_{\mathfrak{p}\in S}|n|_\mathfrak{p}^{-1} \underset{\substack{\mathfrak{p}\in S\Rightarrow \mathfrak{p}\nmid n\Rightarrow \\ |n|_\mathfrak{p}=q^{-v_K(n)}=q^0=1}}{\overset{\uparrow}{=}} n^{2s}.\end{aligned}$$

Se sigue que $[C_K : C_K(S,T)] = \frac{n^{2s}}{n^{2s-r}} = n^r = [L : K]$.

Ahora veremos que $C_K(S,T) \subseteq \mathrm{N}_{L/K}\, C_L$. Sea $\vec{\alpha} \in J_K(S,T)$. Por el Teorema 6.3.9, $\vec{\alpha} \in \mathrm{N}_{L/K}\, J_L \iff \alpha_\mathfrak{p} \in \mathrm{N}_{L_\mathfrak{P}/K_\mathfrak{p}}\, L_\mathfrak{P}^*$ para toda $\mathfrak{p} \in \mathbb{P}_K$. Si $\mathfrak{p} \in S$, puesto que $\alpha_\mathfrak{p} \in (K_\mathfrak{p}^*)^n$, se tiene que es norma $K_\mathfrak{p}(\sqrt[n]{K_\mathfrak{p}^*})$ por Teoría de Kummer para campos locales (Proposición 5.7.5), y por tanto de $K_\mathfrak{p}(\sqrt[n]{\Delta})$, $\Delta = \text{núc}\left(K^S \longrightarrow \prod_{\mathfrak{p}\in T} K_\mathfrak{p}^*/(K_\mathfrak{p}^*)^n\right)$ pues $K_\mathfrak{p}(\sqrt[n]{\Delta}) \subseteq K_\mathfrak{p}(\sqrt[n]{K_\mathfrak{p}^*})$.

Para $\mathfrak{p} \in T$, por el Lema 6.6.6, $\Delta \subseteq (K_\mathfrak{p}^*)^n$ de tal forma que $\mathfrak{p}$ se descompone totalmente y $L_\mathfrak{P} = K_\mathfrak{p}$.

Para $\mathfrak{p} \notin S\cup T$, $\alpha_\mathfrak{p}$ es una unidad y $L_\mathfrak{P} = K_\mathfrak{p}(\sqrt[n]{\Delta})$ es no ramificada sobre $K_\mathfrak{p}$ y $\mathrm{N}_{L_\mathfrak{P}/K_\mathfrak{p}}\, U_\mathfrak{P} = U_\mathfrak{p}$.

Por tanto $J_K(S,T) \subseteq \mathrm{N}_{L/K}\, J_L$ de donde $C_K(S,T) \subseteq \mathrm{N}_{L/K}\, C_L$. Por tanto $[C_K : \mathrm{N}_{L/K}\, C_L] \leq [C_K : C_K(S,T)] = n^r$.

Cuando L/K es cíclica, es decir, cuando $r = 1$, entonces, como consecuencia de la primera desigualdad

$$n = [L : K] \leq [C_K : \mathrm{N}_{L/K}\, C_L] \leq [C_K : C_K(S,T)] = [L : K] = n,$$

de donde se sigue que $\mathrm{N}_{L/K}\, C_L = C_K(S,T)$ y $[C_K : \mathrm{N}_{L/K}\, C_L] = [L : K]$. □

Esto prueba la segunda desigualdad para campos numéricos.

6.6.2. Segunda desigualdad para campos de funciones

Ahora, sea K un campo global de funciones de característica $p > 0$.

Definición 6.6.8. Sea E cualquier campo. Una *derivación* en E es un mapeo $D : E \longrightarrow E$, tal que

- $D(x+y) = D(x) + D(y)$ para cualesquiera $x, y \in E$,
- $D(xy) = xD(y) + yD(x)$ para cualesquiera $x, y \in E$.

Con $x = y = 1$ obtenemos $D(1) = 0$ y si $y = x^{-1}$ con $x \neq 0$, se obtiene $D(x^{-1}) = -x^{-2}D(x)$.

Sea $P_n = \{x \in E \mid D^n(x) = 0\}$. P_n es un subgrupo aditivo de E. Se define, $D^0 = \mathrm{Id}_E$, $P_0 = \{0\}$.

Notación 6.6.9. El operador aditivo $E \longrightarrow E$, $x \longmapsto xy$ se denota ya sea simplemente por y o por μ_y: $\mu_y(x) = xy$. De esta forma Dy significa el operador producto y seguido de D y $D(y)$ significa el efecto que D tiene en el elemento y.

Definición 6.6.10. Un elemento $x \in E$ es una *derivada logarítmica* en E si existe $y \in E$ tal que $x = \frac{D(y)}{y}$ y x es *la derivada logarítmica* de y.

Lema 6.6.11. *Un elemento $x \in E$ es la derivada logarítmica de un elemento $y \in P_n \setminus P_{n-1}$, $n > 0$, si y solamente si la n-potencia del operador $D + x$ aplicada a 1 es igual 0 y la $(n-1)$-potencia aplicada a 1, es diferente a 0:*

$$(D+x)^n(1) = 0 \quad y \quad (D+x)^{n-1}(1) \neq 0,$$

o, equivalentemente,

$$(D+\mu_x)^n(1) = 0 \quad y \quad (D+\mu_x)^{n-1}(1) \neq 0.$$

Demostración. Sea $x = \frac{D(y)}{y}$ para alguna $y \in E^*$. Se tiene

$$\begin{aligned}(D+\mu_x)(z) &= D(z) + xz = D(z) + \frac{D(y)}{y}z \\ &= y^{-1}D(zy) = y^{-1}D\mu_y(z) = y^{-1}Dy(z).\end{aligned}$$

Esto es, $D + \mu_x = y^{-1}D\mu_y$ y por tanto, para $n \geq 0$, tenemos

$$(D+x)^n = (D+\mu_x)^n = y^{-1}D^n\mu_y.$$

Sea $y \in P_n \setminus P_{n-1}$. Entonces $(D+\mu_x)^n(1) = y^{-1}D^n\mu_y(1) = y^{-1}D^n(y) = 0$ y de manera análoga, tenemos $(D+\mu_x)^{n-1}(1) \neq 0$.

Recíprocamente, supongamos que $(D+\mu_x)^n(1) = 0$ y que $(D+\mu_x)^{n-1}(1) \neq 0$. Definimos $y^{-1} := (D+\mu_x)^{n-1}(1)$. Entonces $(D+\mu_y)(y^{-1}) = 0 = -y^{-2}D(y) + xy^{-1}$, por lo que $x = \frac{D(y)}{y}$. Ahora bien, $D + \mu_x = y^{-1}Dy = y^{-1}D\mu_y$ y $(D+\mu_x)^{n-1}(1) = y^{-1}D^{n-1}(y) \neq 0$ y similarmente $y^{-1}D^n(y) = 0$. Por tanto $y \in P_n \setminus P_{n-1}$. □

Consideremos un campo E con la propiedad de que para cada $x \in E$, exista $n_x \in \mathbb{N}$ con $D^{n_x}(x) = 0$, esto es, $E = \bigcup_{n=0}^{\infty} P_n$. Sea $F \subseteq E$ un subcampo tal que $D(F) \subseteq F$. Entonces, del Lema 6.6.11 se sigue que para $x \in F$, se tiene que x es una derivada logarítmica en $F \iff x$ es un derivada logarítmica en E. De hecho, si $x \in F$ es la derivada logarítmica de un elemento $y \in P_n \setminus P_{n-1}$, entonces x es la derivada logarítmica de z donde $z^{-1} = (D + \mu_x)^{n-1}(1)$, el cual es un elemento de F pues $D(F) \subseteq F$.

La situación anterior se presenta en el siguiente caso. Sea K un campo de característica $p > 0$ y $E = K((t))$ el campo de las series formales de Laurent con la derivada usual con respecto a t: $D\big(\sum_{n=m}^{\infty} a_n t^n\big) = \sum_{n=m}^{\infty} n a_n t^{n-1} = \sum_{n=m-1}^{\infty} (n+1) a_{n+1} t^n$. Entonces se tiene que $D^p = 0$.

Corolario 6.6.12. *Sea $E = K((t))$ las series de Laurent de característica $p > 0$ y sea F un subcampo de E estable bajo la derivación $D := \frac{d}{dt}$, $D(F) \subseteq F$. Un elemento $x \in F$ es la derivada logarítmica en F si y solamente si es una derivada logarítmica en E.* □

Sea K un campo de funciones global de característica $p > 0$. Sean $k_0 = \mathbb{F}_q$ el campo de constantes de K y $\mathbb{F}_p$ es el campo primo. Sea $K_{\mathfrak{p}}$ la completación de K con respecto al primo $\mathfrak{p}$. Sea $K(\mathfrak{p})$ el campo residual de $K_{\mathfrak{p}}$, $\mathbb{F}_q \subseteq K(\mathfrak{p})$ por ser $\mathbb{F}_q$ perfecto y $K_{\mathfrak{p}}$ es de manera natural isomorfo a $K(\mathfrak{p})((t))$ donde t es un elemento uniformizador, $v_{\mathfrak{p}}(t) = 1$.

Puesto que $\mathbb{F}_q$ es perfecto, se puede tomar $t \in K$ que sea un elemento separador, esto es $K/\mathbb{F}_q(t)$ es separable ([160, Corollary 8.2.11 y Remark 8.4.9]). Sea Tr la traza de $K(\mathfrak{p})$ a $\mathbb{F}_p$. Sea $\operatorname{Res}(xdy)$ el residuo de la diferencial local xdy calculado con respecto a un parámetro uniformizador.El residuo no depende del parámetro ([160, Theorem 9.3.9 y Definition 9.3.10]).

Definimos un pareo local de la siguiente forma. Para $x, y \in K_{\mathfrak{p}}$, sea

$$\int_{\mathfrak{p}} xdy := \operatorname{Tr}(\operatorname{Res} xdy). \tag{6.6.5}$$

Si $x \in K_{\mathfrak{p}}$ y $y \in K_{\mathfrak{p}}^*$, se define

$$\varphi_{\mathfrak{p}}(x, y) = \int_{\mathfrak{p}} x \frac{dy}{y} = \int_{\mathfrak{p}} x \frac{\frac{dy}{dt}}{y} dt.$$

Se verifica que

$$\begin{aligned} \varphi_{\mathfrak{p}}(x + x', y) &= \varphi_{\mathfrak{p}}(x, y) + \varphi_{\mathfrak{p}}(x', y), \\ \varphi_{\mathfrak{p}}(x, yy') &= \varphi_{\mathfrak{p}}(x, y) + \varphi_{\mathfrak{p}}(x, y'), \end{aligned}$$

por lo que se tiene un pareo de los grupos $K_{\mathfrak{p}}$ (aditivo) y $K_{\mathfrak{p}}^*$ (multiplicativo) con valores en el grupo aditivo $\mathbb{F}_p$. Si x es entero en $K_{\mathfrak{p}}$, esto es, $v_{\mathfrak{p}}(x) \geq 0$ y y es una unidad en $K_{\mathfrak{p}}^*$, es decir, $v_{\mathfrak{p}}(y) = 0$, entonces $x\frac{dy}{y}$ tiene residuo 0. Esto muestra la continuidad del pareo: $\varphi_{\mathfrak{p}}^{-1}(0) \supseteq \mathcal{O}_{\mathfrak{p}} \times U_{\mathfrak{p}}$.

Lema 6.6.13. *Sea $x \in \mathcal{O}_{\mathfrak{p}}$. Entonces $\varphi_{\mathfrak{p}}(x,y) = 0 \iff p | v_{\mathfrak{p}}(y)$ o $x = \wp(z)$ para algún $z \in K_{\mathfrak{p}}$, donde $\wp$ es el operador de Artin-Schreier: $\wp(z) = z^p - z$.*

Demostración. Sea $x = a_0 + a_1 t + \cdots$, $a_i \in K(\mathfrak{p})$, $y = t^n \varepsilon$, $\varepsilon \in U_{\mathfrak{p}}$. Entonces $\varphi_{\mathfrak{p}}(x, \varepsilon) = 0$. Por tanto

$$\varphi_{\mathfrak{p}}(x,y) = \varphi_{\mathfrak{p}}(x,t^n) = \int_{\mathfrak{p}} x \frac{dt^n}{t} = n \int_{\mathfrak{p}} x \frac{dt}{t} = n \operatorname{Tr}(a_0).$$

Se sigue que tener $\varphi_{\mathfrak{p}}(x,y) = 0$ es equivalente con $p|n$ o $\operatorname{Tr}(a_0) = 0$ y debemos probar que $\operatorname{Tr}(a_0) = 0$ es equivalente con la existencia de un z tal que $x = \wp(z) = z^p - z$, $z \in K_{\mathfrak{p}}$.

Primero supongamos que $x = z^p - z$. Si la serie de Laurent para z tiene polos, estos polos serían dominantes en z^p y entonces x no podría ser entero: Sea b el término constante de z, por lo que $a_0 = b^p - b$. Sea σ el automorfismo de Frobenius de $K(\mathfrak{p})/\mathbb{F}_p$: $\sigma c = c^p$. De esta forma, $a_0 = (\sigma - 1)b$ lo cual es equivalente $\operatorname{Tr} a_0 = 0$ pues $H^n(\operatorname{Gal}(K(\mathfrak{p})/\mathbb{F}_p), K(\mathfrak{p})) = 0$, en particular, $H^1(\operatorname{Gal}(K(\mathfrak{p})/\mathbb{F}_p), K(\mathfrak{p})) = 0$, o simplemente, $\operatorname{Tr} a_0 = \operatorname{Tr} \sigma b - \operatorname{Tr} b = 0$ pues σb y b son conjugado.

Recíprocamente, si $\operatorname{Tr}(a_0) = 0$, entonces por la misma razón anterior, $a_0 = (\sigma - 1)b = \wp(b)$ para algún $b \in K(\mathfrak{p})$. Sea $x - a_0 = x_1 = a_1 t + a_2 t^2 + \cdots$ y sea $z_1 = -(x_1 + x_1^p + x_1^{p^2} + \cdots)$. La serie converge en la topología de $K_{\mathfrak{p}}$ y se obtiene $x_1 = z_1^p - z_1 = \wp(z_1)$ y por tanto $x = a_0 + x_1 = \wp(b) + \wp(z_1) = \wp(b + z_1)$ y el resultado se sigue. □

6.6.3. Un pareo global

La traza Tr definida en el pareo local (6.6.5), se puede descomponer como $\operatorname{Tr} = \operatorname{Tr}_{K(\mathfrak{p})/\mathbb{F}_p} = \operatorname{Tr}_{\mathbb{F}_q/\mathbb{F}_p} \circ \operatorname{Tr}_{K(\mathfrak{p})/\mathbb{F}_q}$. Sea $\mathbb{A}_K$ el anillo de adèles. Sea $\mathfrak{p}$ un primo y sea t un elemento separador para K y $v_{\mathfrak{p}}(t) = 1$. Sea

$$\lambda(\vec{\xi}) = \sum_{\mathfrak{p}} \operatorname{Tr}_{\mathfrak{p}}(\operatorname{Res}_{\mathfrak{p}}(\xi_{\mathfrak{p}} dt)),$$

con $\operatorname{Tr}_{\mathfrak{p}} = \operatorname{Tr}_{K(\mathfrak{p})/\mathbb{F}_q}$, $\vec{\xi} \in \mathbb{A}_K$ y $\lambda(\vec{\xi}) \in \mathbb{F}_q$. Si $|\xi_{\mathfrak{p}}|_{\mathfrak{p}}$ es suficientemente pequeño en todos los primos donde t tiene polos y $\xi_{\mathfrak{p}}$ es una unidad en los demás primos, se tiene $\lambda(\vec{\xi}) = 0$ pues $\operatorname{Res}_{\mathfrak{p}}(\xi_{\mathfrak{p}} dt) = 0$ para toda $\mathfrak{p}$. En particular λ es una función continua sobre $\mathbb{A}_K$. Por el Teorema de los residuos ([160, Theorem 9.3.14]), $\lambda(x) = 0$ para toda $x \in K$, donde x es el adèle principal. En otras palabras, λ es un diferencial sobre K. Sea

$$\oint \vec{\xi} dt = \operatorname{Tr}_{\mathbb{F}_q/\mathbb{F}_p}(\lambda(\vec{\xi})) = \sum_{\mathfrak{p}} \int_{\mathfrak{p}} \xi_{\mathfrak{p}} dt.$$

Lema 6.6.14. *Si $\vec{\xi} \in \mathbb{A}_K$ es tal que $\oint \xi x dt = \operatorname{Tr}_{\mathbb{F}_q/\mathbb{F}_p}(\lambda(\vec{\xi} x)) = 0$ para toda $x \in K$, entonces $\vec{\xi} \in K$.*

Demostración. Podemos reemplazar x por αx por cualquier $\alpha \in \mathbb{F}_q$ y obtenemos $\mathrm{Tr}_{\mathbb{F}_q/\mathbb{F}_p}(\alpha \cdot \lambda(\vec{\xi}x)) = 0$. Si $\lambda(\vec{\xi}x) \neq 0$, tendríamos $\mathrm{Tr}_{\mathbb{F}_q/\mathbb{F}_p}(\mathbb{F}_q) = 0$ lo cual no se cumple pues $\mathbb{F}_q/\mathbb{F}_p$ es separable. Por tanto $\lambda(\vec{\xi}x) = 0$ para toda $x \in K$.

Se tiene que, para $x \in K$, si μ es una diferencial, $x\mu$ es una diferencial donde $(x\mu)(\vec{\alpha}) := \mu(\vec{\alpha}x)$. Si seleccionamos $\mu_0 \neq 0$, puesto que las diferenciales es un espacio de dimensión 1 sobre K, toda diferencial es de la forma $x\mu_0$. Ahora $\lambda \neq 0$ y $(x\lambda)(\vec{\xi}) = \lambda(\vec{\xi}x) = 0$, es decir $\mu(\vec{\xi}) = 0$ para toda diferencial μ. Veamos que necesariamente $\vec{\xi} \in K$, esto es,

$$\bigcap_{\mu \text{ diferencial}} \text{núc}\, \mu = \bigcap_{\mathfrak{a} \text{ divisor}} (K + \mathfrak{X}_K(\mathfrak{a}^{-1})) = K.$$

Sea $\vec{\alpha} \xrightarrow[\delta]{} \lambda(\vec{\xi}\vec{\alpha})$. Se verifica que δ es una diferencial ($\lambda(\vec{\xi}x) = \delta(x) = 0$ para toda $x \in K$). Por tanto existe $\beta \in K$ tal que $\delta = \beta\lambda$, es decir, $\lambda(\vec{\xi}\vec{\alpha}) = \delta(\vec{\alpha}) = \beta\lambda(\vec{\alpha}) = \lambda(\beta\vec{\alpha})$. Por tanto $\lambda_{\mathfrak{P}}(\vec{\xi}\vec{\alpha}) = \lambda_{\mathfrak{P}}(\beta\vec{\alpha})$ para toda $\mathfrak{P} \in \mathbb{P}_K$ lo cual implica $\lambda_{\mathfrak{P}}((\xi_{\mathfrak{P}} - \beta)\alpha_{\mathfrak{P}}) = 0$ para toda $\alpha_{\mathfrak{P}}$. Por tanto $\xi_{\mathfrak{P}} - \beta = 0$ para toda $\mathfrak{P} \in \mathbb{P}_K$, de donde se sigue $\vec{\xi} = \beta \in K$. □

Sea t un elemento separador de $K/\mathbb{F}_q$, es decir, $K/\mathbb{F}_q(t)$ es separable, el cual existe por ser $\mathbb{F}_q$ perfecto ([160, Corollary 8.2.11]).

Lema 6.6.15. *Para cada $\mathfrak{p} \in \mathbb{P}_K$, sea $t_{\mathfrak{p}}$ un elemento primo de $K_{\mathfrak{p}}$. Entonces $\frac{dt}{dt_{\mathfrak{p}}}$ es unidad para casi toda $\mathfrak{p}$.*

Demostración. Tenemos que el divisor de la diferencial dt en K es $(dt)_K = \mathfrak{D}_{K/k(t)} \operatorname{con}_{\mathbb{F}_q(t)/K} \mathcal{P}_\infty^{-2}$, donde $\mathcal{P}_\infty$ es el polo de x en $\mathbb{F}_q(t)$. En particular $v_{\mathfrak{p}}((dt)_K) = 0$ para casi toda $\mathfrak{p}$.

Veamos que si $t_{\mathfrak{p}}$ es un elemento primo en $\mathfrak{p}$, entonces si en $K_{\mathfrak{p}}$, $\frac{dt}{dt_{\mathfrak{p}}} = \sum_{m=n} a_m t_{\mathfrak{p}}^m$ con $a_n \neq 0$, se tiene que $v_{\mathfrak{p}}((dt)_K) = n$. Una vez probado lo anterior, se seguirá que $\frac{dt}{dt_{\mathfrak{p}}}$ es una unidad para casi toda $\mathfrak{p}$.

Nos referimos a [160, Subsection 9.3] donde se ve la relación entre las diferenciales $\alpha d\beta$ (de Hasse) y las diferenciales ω de Weil. Esto es [160, Theorem 9.3.15]: Dada $\alpha d\beta$, se define $\omega : \mathfrak{X}_K (= \mathbb{A}_K) \longrightarrow \mathbb{F}_q$ por

$$\omega(\vec{\xi}) = \sum_{\mathfrak{p} \in \mathbb{P}_K} \operatorname*{Res}_{\mathfrak{p}}(\xi_{\mathfrak{p}} \alpha d\beta) \quad \text{y se tiene} \quad \omega^{\mathfrak{p}}(\vec{\xi}) = \operatorname*{Res}_{\mathfrak{p}} \xi_{\mathfrak{p}} \alpha d\beta.$$

En la demostración del Theorem 9.3.15 de [160] se obtiene que el exponente local del divisor $(\omega)_K$, es precisamente $v_{\mathfrak{p}}(\alpha d\beta)$. En nuestro caso, $dt = \frac{dt}{dt_{\mathfrak{p}}} dt_{\mathfrak{p}}$ y $v_{\mathfrak{p}}(dt) = v_{\mathfrak{p}}\big(\frac{dt}{dt_{\mathfrak{p}}}\big)$. □

Ahora sea $\vec{\alpha} \in J_K$. Sea $\vec{\beta}$ dada por $\beta_{\mathfrak{p}} = \frac{1}{\alpha_{\mathfrak{p}}} \frac{d\alpha_{\mathfrak{p}}}{dt} = \frac{1}{\alpha_{\mathfrak{p}}} \frac{d\alpha_{\mathfrak{p}}}{dt_{\mathfrak{p}}} \big(\frac{dt}{dt_{\mathfrak{p}}}\big)^{-1}$. Entonces $\beta_{\mathfrak{p}} \in \mathcal{O}_K$ para casi toda $\mathfrak{p}$ y por tanto $\beta \in \mathbb{A}_K$. Usamos la notación $\vec{\beta} = \frac{1}{\vec{\alpha}} \frac{d\vec{\alpha}}{dt}$.

Sea $\varphi : K \times J_K \longrightarrow \mathbb{F}_p$ el pareo dado por

$$\varphi(x,\vec{\alpha}) = \oint x\frac{1}{\vec{\alpha}}\frac{d\vec{\alpha}}{dt}dt = \sum_{\mathfrak{p}}\int_{\mathfrak{p}} x\frac{1}{\alpha_{\mathfrak{p}}}\frac{d\alpha_{\mathfrak{p}}}{dt}dt = \sum_{\mathfrak{p}}\int_{\mathfrak{p}} x\frac{d\alpha_{\mathfrak{p}}}{\alpha_{\mathfrak{p}}}$$
$$= \sum_{\mathfrak{p}}\varphi_{\mathfrak{p}}(x,\alpha_{\mathfrak{p}}) = \sum_{\mathfrak{p}}\mathrm{Tr}(\mathrm{Res}\,\frac{x}{\alpha_{\mathfrak{p}}}d\alpha_{\mathfrak{p}}). \tag{6.6.6}$$

Considerando K y $\mathbb{F}_p$ con la topología discreta, se tiene que si $\alpha_{\mathfrak{p}}$ está muy cerca de 1, entonces $\frac{d\alpha_{\mathfrak{p}}}{\alpha_{\mathfrak{p}}}$ está muy cerca de 0 y viendo las componentes de los integrandos locales, se sigue la continuidad en J_K. Por tanto el pareo en (6.6.6) es un pareo continuo.

Lema 6.6.16. *El núcleo en J_K del pareo* (6.6.6) *es $J_K^p K^*$ y el núcleo en K es $\wp(K) = \{z^p - z \mid z \in K\}$.*

Notemos que cada elemento de K tiene período p y que $J_K/K^*J_K^p$ es compacto y de hecho, isomorfo a C_K/C_K^p. Más precisamente, se tiene $C_K \cong C_{K,0} \times A$, $A \subseteq \mathbb{R}^+$, $C_K^p \cong C_{K,0}^p \times A^p$ y $C_{K,0}$ es compacto, $A \cong \mathbb{Z}$ por lo que $C_K/C_K^p \cong C_{K,0}/C_{K,0}^p \times \mathbb{Z}/p\mathbb{Z}$ es compacto.

Demostración. Si $\vec{\alpha}$ está en el núcleo en J_K, entonces $\vec{\xi} = \frac{1}{\vec{\alpha}}\frac{d\vec{\alpha}}{dt} \in \mathbb{A}_K$ satisface $\oint \vec{\xi}x dt = 0$ para toda $x \in K$, por lo que $\vec{\xi} = y \in K$ pues $\omega(\vec{\xi}) = 0$ para toda diferencial de K (Lema 6.6.14).

Tomando la componente $\mathfrak{p}$ de y ($y_{\mathfrak{p}} = y$), que tenga a $t \in K$ como uniformizador local, entonces $y = \frac{1}{\alpha_{\mathfrak{p}}}\frac{d\alpha_{\mathfrak{p}}}{dt}$ y por tanto y es una derivada logarítmica en $K_{\mathfrak{p}}$. Puesto que $K \subseteq K_{\mathfrak{p}}$, y K es estable bajo diferenciación puesto que $t \in K$, y ya que $y \in K$, el Corolario 6.6.12 prueba que y es derivada logarítmica en K:

$$y = \frac{1}{z}\frac{dz}{dt}, \qquad z \in K.$$

Obtenemos

$$\vec{\xi} = \frac{1}{\vec{\alpha}}\frac{d\vec{\alpha}}{dt} = \frac{1}{z}\frac{dz}{dt} = y.$$

Sea $\vec{\gamma} = z^{-1}\vec{\alpha}$. Entonces $\frac{d\vec{\gamma}}{dt} = -z^{-2}\frac{dz}{dt}\vec{\alpha} + z^{-1}\frac{d\vec{\alpha}}{dt} = 0$. Por tanto $\frac{d\gamma_{\mathfrak{p}}}{dt} = 0$ para toda $\mathfrak{p}$ lo cual implica que cada componente es una p-potencia por lo que $\vec{\gamma} \in J_K^p$ y por tanto $\vec{\alpha} \in J_K^p K^*$.

Por otro lado, tanto J_K^p como K^* claramente pertenecen al núcleo del mapeo φ, K^* puesto que $\lambda(\vec{\xi}) = \sum_{\mathfrak{p}} \mathrm{Tr}_{\mathfrak{p}}(\mathrm{Res}_{\mathfrak{p}}(\xi_{\mathfrak{p}}dt))$ es una diferencial. Se sigue que el núcleo de $\varphi(x,\vec{\alpha})$ en J_K es $J_K^p K^*$.

Ahora sea $x = z^p - z$. Sea $\vec{\xi} \in J_K$. Por el teorema de aproximación, existe $y \in K$ tal que $y\vec{\xi}$ está muy cercano a 1 en todos los lugares en donde x tiene un polo. Sea $\mathfrak{p}$ un polo de x. Entonces

$$\varphi_{\mathfrak{p}}(x, y\vec{\xi}) = \int_{\mathfrak{p}} x\frac{d(y\xi_{\mathfrak{p}})}{y\xi_{\mathfrak{p}}}.$$

Sea π un primo en $\mathfrak{p}$. Se tiene

$$x\frac{d(y\xi_{\mathfrak{p}})}{y\xi_{\mathfrak{p}}} = x\frac{d(y\xi_{\mathfrak{p}})}{\pi}\Big(\frac{y\xi_{\mathfrak{p}}}{\pi}\Big)^{-1},$$
$$y\xi_{\mathfrak{p}} = 1+\pi^n b, \quad d(y\xi_{\mathfrak{p}}) = n\pi^{n-1}bd\pi,$$

así que

$$\frac{d(y\xi_{\mathfrak{p}})}{\pi} = n\pi^{n-2}bd\pi, \quad \Big(\frac{y\xi_{\mathfrak{p}}}{\pi}\Big)^{-1} = \pi^{-1}(1-\pi^n b+\cdots) = \pi^{-1}-\pi^{n-1}b+\cdots,$$
$$\frac{d(y\xi_{\mathfrak{p}})}{\pi}\Big(\frac{y\xi_{\mathfrak{p}}}{\pi}\Big)^{-1} = n\pi^{n-2}+\cdots, \quad x\frac{d(y\xi_{\mathfrak{p}})}{\pi}\Big(\frac{y\xi_{\mathfrak{p}}}{\pi}\Big)^{-1} = n\pi^{n-2-m}+\cdots$$

donde $x = \frac{x_0}{\pi^m}$. Por tanto, con $n \geq 2+m$, se tiene $\operatorname{Res} x\frac{d(y\xi_{\mathfrak{p}})}{y\xi_{\mathfrak{p}}} = 0$. Se sigue que $\varphi_{\mathfrak{p}}(x, y\vec{\xi}) = 0$ para todo lugar $\mathfrak{p}$ que es polo de x.

Ahora, como y está en el núcleo de J_K. Entonces

$$\varphi(x,\vec{\xi}) = \sum_{\mathfrak{p}} \varphi_{\mathfrak{p}}(x, y\vec{\xi}) = \sum_{\mathfrak{q}} \varphi_{\mathfrak{q}}(x, y\xi_{\mathfrak{q}}),$$

donde $\mathfrak{q}$ varía sobre los primos donde x no tiene polos y por tanto x es un entero local. Por el Lema 6.6.13 se tiene que $\varphi_{\mathfrak{q}}(x, y\xi_{\mathfrak{q}}) = 0$ pues $x = z^p - z$. Se sigue que x está en el núcleo de K bajo el pareo φ.

Recíprocamente, supongamos que x está en el núcleo de K. Entonces, $\varphi(x,\vec{\xi}) = 0$ para toda $\vec{\xi} \in J_K$, en particular para los idèles $\vec{\xi}_{\mathfrak{p}}$ que únicamente una componente $\neq 1$, esto es, $(\vec{\xi}_{\mathfrak{p}})_{\mathfrak{q}} = \begin{cases} 1 & \text{si } \mathfrak{q} \neq \mathfrak{p}, \\ \xi_{\mathfrak{p}} & \text{si } \mathfrak{q} = \mathfrak{p} \end{cases}$, se tiene $\varphi(x,\vec{\xi}_{\mathfrak{p}}) = \varphi_{\mathfrak{p}}\big(x, (\vec{\xi}_{\mathfrak{p}})_{\mathfrak{p}}\big) = 0$. Por tanto $\varphi_{\mathfrak{p}}(x,\xi_{\mathfrak{p}}) = 0$ para toda $\xi_{\mathfrak{p}} \in K_{\mathfrak{p}}$.

Sea $\mathfrak{p}$ un primo que no es polo de x. En ese primo, se puede aplicar el Lema 6.6.13 y se tiene $x = z_{\mathfrak{p}}^p - z_{\mathfrak{p}}$ con algún $z_{\mathfrak{p}} \in K_{\mathfrak{p}}$.

Se tiene que $\mathfrak{p}$ se descompone en $K\big(\wp^{-1}x\big)/K$ pues $\big(K(\wp^{-1}x)\big)_{\mathfrak{p}} = \big(K(z_{\mathfrak{p}})\big)_{\mathfrak{p}} = K_{\mathfrak{p}}$ o, simplemente, $Y^p - Y - x = \prod_{i=0}^{p-1}(Y - z_{\mathfrak{p}} - i)$ se descompone totalmente módulo $\mathfrak{p}$, por lo tanto $\mathfrak{p}$ se descompone totalmente ([136, Teorema 10.3.16]).

Como esto se cumple para toda $\mathfrak{p}$, como consecuencia del Corolario 6.5.3, se sigue que $K(\wp^{-1}x) = K$ por lo que $x = z^p - z$, $z \in K$. □

6.6.4. Grupo de Galois de la máxima *p*-extensión elemental abeliana de *K*

Esta extensión es $L = K(\wp^{-1}(K))$. Sea $\mathcal{G} = \operatorname{Gal}(L/K)$. El grupo asociado a L es $A = \wp^{-1}(K)$. El pareo es $(\alpha,\sigma) = (\sigma-1)\alpha$. A se mapea en K por el mapeo $\alpha \mapsto \wp\alpha$. La imagen de A es K. Se puede ver como el pareo $K \times \mathcal{G} \xrightarrow{[\_,\_]} \mathbb{F}_p$ donde $[x,\sigma] = (\sigma-1)(\wp^{-1}(x))$, $x \in K$, $\sigma \in \mathcal{G}$.

El núcleo en K es $\wp(K)$, el mismo que el del pareo $\varphi(x,\vec{\xi})$. El núcleo en $\mathcal{G}$ es $\{1\}$. Con este pareo, se tiene $\mathcal{G} \cong \widehat{\left(K/\wp(K)\right)} = \mathrm{Hom}(K/\wp(K), \mathbb{F}_p)$ donde $K/\wp(K)$ tiene la topología discreta. Con el pareo $\varphi(x,\vec{\xi})$, el grupo $J_K/J_K^p K^*$ es naturalmente isomorfo al mismo grupo $\widehat{K/\wp(K)}$.

Se tiene un isomorfismo natural

$$\mathcal{G} \cong J_K/J_K^p K^* = C_K/C_K^p.$$

Si $\sigma \in \mathcal{G}$ es la imagen del idèle $\vec{\alpha}$ bajo este isomorfismo, entonces debemos tener $\varphi(x,\vec{\alpha}) = [x,\sigma] = (\sigma - 1)(\wp^{-1}(x))$.

Denotamos este elemento $\sigma \in \mathcal{G}$ por $\sigma_{\vec{\alpha}}$. Esto es, el isomorfismo $\mathcal{G} \cong J_L/J_K^p K^*$ lo describimos por $\mu : J_L \xrightarrow{\mu} \mathcal{G}$, $\mu(\vec{\alpha}) := \sigma_{\vec{\alpha}}$ y donde $\mathrm{núc}\,\mu = J_K^p K^*$. La ecuación anterior describe el efecto de $\sigma_{\vec{\alpha}}$ en los generadores de L, una descripción que determina $\sigma_{\vec{\alpha}}$ completamente:

$$\sigma_{\vec{\alpha}} : \wp^{-1}(x) \longrightarrow \wp^{-1}(x) + \varphi(x,\vec{\alpha}), \tag{6.6.7}$$

donde φ es el pareo global $\varphi : \mathcal{G} \times L \longrightarrow \mathbb{F}_p$, y si $\vec{\alpha} \in J_K$ se mapea a $\sigma_{\vec{\alpha}} \in \mathcal{G}$ bajo μ, tenemos que (6.6.7) se lee $\sigma_{\vec{\alpha}}(z) = z + \varphi(x,\vec{\alpha})$ con $\varphi(x,\vec{\alpha}) \in \mathbb{F}_p$ y donde $z^p - z = x$.

De esta forma, hemos probado

Teorema 6.6.17. *El mapeo dado en* (6.6.7) *es un isomorfismo bicontinuo entre* $J_K/J_K^p K^* \cong C_K/C_K^p$ *y el grupo de Galois de la máxima extensión abeliana* L *de* K *de exponente* p. □

6.6.5. Demostración de la 2nda. desigualdad en característica $p > 0$

Sea M/K una extensión cíclica de grado p de campos globales de funciones. Como M es subcampo de la máxima p-extensión elemental abeliana de K, $L = K(\wp^{-1}(K))$, M está determinado por un subgrupo abierto $\mathcal{H}$ de $\mathcal{G} = \mathrm{Gal}(L/K)$ de índice p, $\mathcal{H} = \mathrm{Gal}(L/M)$, $[\mathcal{G} : \mathcal{H}] = p$.

El grupo de normas $K^* \,\mathrm{N}_{M/K}\, J_M$ es un subgrupo abierto de J_K (Teorema 6.3.2): todos los idèles en un vecindad suficientemente pequeña de 1 son normas, y es de índice finito en J_K, pues $J_K/K^* \,\mathrm{N}_{M/K}\, J_M \cong C_K/\,\mathrm{N}_{M/K}\, C_M$ y si $\Lambda = C_{K,0} \cap \mathrm{N}_{M/K}\, C_M$, entonces Λ es abierto en $C_{K,0}$. Como $C_{K,0}$ es compacto, se sigue que $[C_{K,0} : \Lambda] < \infty$. Puesto que el campo de constantes de M es $\mathbb{F}_{q^\nu}$ con $\nu \in \{1,p\}$, se tiene que $\Delta = \mathrm{N}_{M/K}\, C_M \cap \mathbb{Z} \neq \{0\}$ de donde se sigue que $\mathbb{Z}/\Delta$ es un grupo finito y por tanto $[C_K : \mathrm{N}_{M/K}\, C_M] < \infty$.

Por la primera desigualdad, se tiene que

$$[C_K : \mathrm{N}_{M/K}\, C_M] = [J_K : K^* \,\mathrm{N}_{M/K}\, J_M] \geq p = [M : K].$$

La imagen de este grupo bajo el isomorfismo del Teorema 6.6.17 (el epimorfismo μ) es cierto subgrupo abierto $\mathcal{H}'$ de $\mathcal{G}$. Esquemáticamente, tenemos:

$$K^* \, \mathrm{N}_{M/K} \, J_M \rightsquigarrow \mathcal{H}', \qquad M \rightsquigarrow \mathcal{H}.$$

El índice de $\mathcal{H}'$ en $\mathcal{G}$ es finito y mayor o igual p. Se tiene que $\mathcal{H}'$ determina cierto subcampo E/K de L/K el cual es la composición de campos cíclicos de grado p y cada uno de estos campos se quedan fijos bajo $\mathcal{H}'$, $E = L^{\mathcal{H}'}$.

A cada subcampo cíclico M'/K de grado p que sea diferente a M, daremos un elemento de $\mathcal{H}'$ que no deja fijo a todos los elementos de M'. Esto probará que $\mathcal{H}' = \mathcal{H}$ y probará completamente la segunda desigualdad puesto que el índice de $\mathcal{H}$ en $\mathcal{G}$ es p.

Más precisamente, si $[M' : K] = p$ con M'/K abeliana y $M' \neq M$, se probará que $M \not\subseteq L^{\mathcal{H}'}$ y en consecuencia, como $L^{\mathcal{H}'} \neq K$, entonces $L^{\mathcal{H}'} \subseteq M = L^{\mathcal{H}}$ por lo que $\mathcal{H} \subseteq \mathcal{H}'$ y $p = [\mathcal{G} : \mathcal{H}] = [\mathcal{G} : \mathcal{H}'][\mathcal{H}' : \mathcal{H}] \geq [\mathcal{G} : \mathcal{H}'] \geq p$. Por tanto obtendremos que $p = [\mathcal{G} : \mathcal{H}] = [\mathcal{G} : \mathcal{H}']$ y $\mathcal{H} = \mathcal{H}'$.

Por el Teorema 6.5.5, existe un primo (de hecho, una infinidad) $\mathfrak{p}$ en K que se descompone en M/K y es inerte en M'/K. Si $K' = K(\wp^{-1}(x))$ se puede seleccionar $\mathfrak{p}$ que no sea polo de x. Sea $\vec{\alpha}_{\mathfrak{p}} \in J_K$ que tiene en la componente $\mathfrak{p}$ un elemento primo de $K_{\mathfrak{p}}$ y las demás componentes son 1.

Se tiene que $(\vec{\alpha}_{\mathfrak{p}})_{\mathfrak{p}} \in K_{\mathfrak{p}}$ es norma de de $M_{\mathfrak{P}}$, $\mathfrak{P}|\mathfrak{p}$, pues $\mathfrak{p}$ se descompone en M/K y por tanto $M_{\mathfrak{P}} = K_{\mathfrak{p}}$. Las demás componentes son 1 y por tanto son normas locales. Del Teorema 6.3.9, se tiene que $\vec{\alpha}_{\mathfrak{p}}$ es una norma de algún elemento de J_M. Se sigue que $\sigma_{\vec{\alpha}_{\mathfrak{p}}} \in \mathcal{H}'$. Ahora, calculamos $\varphi(x, \vec{\alpha}_{\mathfrak{p}}) = \varphi_{\mathfrak{p}}(x, (\vec{\alpha}_{\mathfrak{p}})_{\mathfrak{p}})$.

Como $\mathfrak{p}$ no se descompone en M', se tiene que $x \notin \wp(K_{\mathfrak{p}})$. Ahora $(\vec{\alpha}_{\mathfrak{p}})_{\mathfrak{p}}$ es un elemento primo, por tanto de valuación 1 y en particular no es divisible por p. Por el Lema 6.6.16, se tiene que $\varphi(x, \vec{\alpha}_{\mathfrak{p}}) \neq 0$. Esto significa, de acuerdo a (6.6.7), que $\sigma_{\vec{\alpha}_{\mathfrak{p}}}$ mueve $\wp^{-1}(x)$:

$$\sigma_{\vec{\alpha}_{\mathfrak{p}}}(\wp^{-1}(x)) = \wp^{-1}(x) + \varphi_{\mathfrak{p}}(x, (\vec{\alpha}_{\mathfrak{p}})_{\mathfrak{p}}) \neq \wp^{-1}(x),$$

y por tanto no es la identidad en M'.

Teorema 6.6.18 (Segunda desigualdad fundamental). *Para cualquier extensión finita de Galois L/K de campos globales, se tiene que*

$$[C_K : \mathrm{N}_{L/K} \, C_L] \big| [L : K]. \qquad \square$$

Como consecuencia de la primera y de la segunda desigualdad obtenemos.

Teorema 6.6.19. *Si L/K es una extensión finita cíclica de grado primo p de campos globales, $H^0(G, C_L) \cong H^2(G, C_L) \cong G = \mathrm{Gal}(L/K)$ y $H^1(G, C_L) = 1$.*

Demostración. Se obtuvo de la primera desigualdad que $h(G, C_L) = p = [L : K]$, por tanto $|H^0(G, C_L)| \geq p$ y por la segunda desigualdad que $|H^0(G, C_L)| = [C_K : \mathrm{N}_{L/K} \, C_L] \leq p$. Se sigue que $|H^0(G, C_L)| = p$ y $|H^1(G, C_L)| = 1$.

Ahora bien, puesto que $H^0(G, C_L)$ tiene orden primo p, es cíclico lo mismo que G, por lo que $H^0(G, C_L) \cong H^2(G, C_L) \cong G$. $\square$

Teorema 6.6.20. *Si L/K es una extensión finita de Galois de campos globales con grupo de Galois $G = \mathrm{Gal}(L/K)$, entonces se tiene $H^1(G, C_L) = \{1\}$.*

Demostración. Si L/K es cíclica, entonces por la primera desigualdad, se tiene $|H^0(G, C_L)| \geq [L : K]$ y por la segunda desigualdad $|H^0(G, C_L)| \leq [L : K]$, de donde $|H^0(G, C_L)| = [L : K] = h(G, C_L) = \frac{|H^0(G,C_L)|}{|H^1(G,C_L)|}$ por lo que $|H^1(G, C_L)| = 1$. Se sigue que $H^1(G, C_L) = \{1\}$.

Sea G arbitrario de orden $n = [L : K]$. Por inducción suponemos que $H^1(H, C_L) = \{1\}$ para toda extensión L/K de Galois con grupo H y de orden menor a n.

Si G no es una p-potencia, para todo p-subgrupo de Sylow S_p de G, se tiene $H^1(S_p, C_L) = \{1\}$. Del Corolario 4.8.4 se sigue que $H^1(G, C_L) = \{1\}$.

Sea ahora $|G| = p^m$ con p un número primo y $m \geq 1$. Si $m = 1$ ya se tiene el resultado. Sea $m \geq 2$. Sea $H \lhd G$ de índice p y sea $K \subseteq M \subseteq L$ con $H = \mathrm{Gal}(L/M)$. Por hipótesis de inducción tenemos $H^1(H, C_L) = \{1\} = H^1(G/H, C_M)$. De la sucesión inflación-restricción

$$1 \longrightarrow H^1(G/H, C_M) \xrightarrow{\inf} H^1(G, C_L) \xrightarrow{\mathrm{res}} H^1(H, C_L),$$

se sigue que $H^1(G, C_L) = \{1\}$. □

Corolario 6.6.21 (Teorema de la norma de Hasse). *Sea L/K una extensión cíclica finita de campos globales. Entonces un elemento $x \in K^*$ es norma de un elemento de L^* si y solamente si x en un norma local para toda completación $L_{\mathfrak{P}}/K_{\mathfrak{p}}$, $\mathfrak{p} \in \mathbb{P}_K$, $\mathfrak{P}|\mathfrak{p}$.*

Demostración. La sucesión exacta de G-módulos

$$1 \longrightarrow L^* \longrightarrow J_L \longrightarrow C_L \longrightarrow 1,$$

da en cohomología la sucesión exacta

$$H^{-1}(G, C_L) = \{1\} \longrightarrow H^0(G, L^*) \xrightarrow{\tilde{\theta}} H^0(G, J_L) \cong \bigoplus_{\mathfrak{p}} H^0(G_{\mathfrak{P}}, L_{\mathfrak{P}}),$$

por lo que $\tilde{\theta}$ es inyectivo.

Como $H^0(G, L^*) \cong K^*/\,\mathrm{N}_{L/K}\, L^*$ y $H^0(G, J_L) \cong \bigoplus_{\mathfrak{p}} K_{\mathfrak{p}}^*/\,\mathrm{N}_{L_{\mathfrak{P}}/K_{\mathfrak{p}}}\, L_{\mathfrak{P}}^*$, se tiene que el homomorfismo

$$\begin{aligned} K^* &\xrightarrow{\theta} \bigoplus_{\mathfrak{p}} K_{\mathfrak{p}}^*/\,\mathrm{N}_{L_{\mathfrak{P}}/K_{\mathfrak{p}}}\, L_{\mathfrak{P}}^*, \\ x &\longmapsto \bigoplus_{\mathfrak{p}} x \text{ mód } \mathrm{N}_{L_{\mathfrak{P}}/K_{\mathfrak{p}}}\, L_{\mathfrak{P}}^*, \end{aligned}$$

tiene núcleo $K^* \bigcap \left(\bigcap_{\mathfrak{p}} \mathrm{N}_{L_{\mathfrak{P}}/K_{\mathfrak{p}}}\, L_{\mathfrak{P}}^* \right) = \mathrm{N}_{L/K}\, L^*$, de donde se sigue el resultado. □

Observación 6.6.22. El teorema de Hasse únicamente es válido para extensiones cíclicas de campos globales. La demostración del Corolario 6.6.21 es únicamente válida para extensiones cíclicas pues estamos usando que $H^{-1}(G, C_L) = H^1(G, C_L) = \{1\}$ lo cual es falso en general para extensiones no cíclicas.

Teorema 6.6.23. *Sea L/K una extensión finita de Galois de campos globales con grupo $G = G_{L|K}$. Entonces el orden de $H^2(G, C_L)$ es un divisor de $[L : K]$.*

Demostración. Lo probamos por inducción en $n = [L : K]$. Si $n = 1$ o p, con p un número primo ya se tiene (Teorema 6.6.19). Sea n un número natural que no es 1 ni primo. Supongamos el resultado para toda extensión de grado menor a n. Si n no es potencia de un primo, entonces para cada subgrupo de Sylow S_p de G, se tiene $|H^2(S_p, C_L)|\big|n_p = |S_p|$. Sea $H^2(G, C_L)_p$ el p-subgrupo de Sylow de $H^2(G, C_L)$, entonces la restricción $H^2(G, C_L)_p \xrightarrow{\text{res}} H^2(S_p, C_L)$ es inyectiva (Proposición 4.8.3). Por tanto, $|H^2(G, C_L)_p|\big||H^2(S_p, C_L)|\big|n_p$ y como $H^2(G, C_L) \cong \bigoplus_{\mathfrak{p}} H^2(S_p, C_L)$ se sigue que $|H^2(G, C_L)|\big|\prod_p n_p = n$.

Sea G un p-grupo, $|G| = p^m$, $m \geq 2$. Sea $H \lhd G$ de índice p. Entonces $|H| = \frac{n}{p}$ y tomando en cuenta que $H^1(G, C_L) = \{1\}$, tenemos la sucesión inflación-restricción

$$1 \longrightarrow H^2(G/H, C_L^H) \xrightarrow{\text{inf}} H^2(G, C_L) \xrightarrow{\text{res}} H^2(H, C_L),$$

la cual es exacta.

Ahora puesto que $|G/H| = p$ se tiene que G/H es cíclico, y se tiene $H^2(G/H, C_L^H) \cong H^0(G/H, C_L^H) \cong G/H$ ($C_L^H = C_M$ donde $M = L^H$). Por tanto $\frac{|H^2(G,C_L)|}{p}|H^2(H, C_L)|\big|\frac{n}{p}$. Se sigue que $|H^2(G, C_L)|\big|n = [L : K]$. □

Observación 6.6.24. Del Teorema 6.6.23 no se obtiene nuestro objetivo de probar que $H^2(G, C_L)$ es cíclico de orden $[L : K]$.

Teorema 6.6.25 (Axioma de la teoría de campos de clases globales). *Sea L/K una extensión cíclica finita de campos globales, entonces*

$$|H^i(G_{L|K}, C_L)| = \begin{cases} [L : K], & i \equiv 0 \text{ mód } 2, \\ 1, & i \equiv 1 \text{ mód } 2. \end{cases}$$

Demostración. El resultado se sigue de que $h(G_{L|K}, C_L) = n = [L : K] = \frac{|H^0(G_{L|K}, C_L)|}{|H^1(G_{L|K}, C_L)|}$ y $H^1(G_{L|K}, C_L) = \{1\}$ por tanto $|H^0(G_{L|K}, C_L)| = [L : K]$. □

Para tener el teorema de reciprocidad, el objetivo será probar que si L/K es una extensión abeliana finita de campos globales, entonces C_L satisface las condiciones del teorema de Tate-Nakayama:

(I) $H^1(G, C_L) = \{1\}$,

(II) $H^2(G, C_L)$ es cíclica de orden $|G| = [L : K]$,

donde $G = \mathrm{Gal}(L/K) = G_{L|K}$.

Empezaremos por definir el mapeo invariante

$$H^2(G_{L|K}, C_L) \longrightarrow \Big(\frac{1}{[L:K]}\mathbb{Z}\Big)/\mathbb{Z}.$$

Como de costumbre, para cada $\mathfrak{p} \in \mathbb{P}_K$ seleccionaremos únicamente un primo $\mathfrak{P} \in \mathbb{P}_L$ con $\mathfrak{P}|\mathfrak{p}$.

Para cada extensión $L_\mathfrak{P}/K_\mathfrak{p}$, $\mathrm{Gal}(L_\mathfrak{P}/K_\mathfrak{p}) \cong G_\mathfrak{P} \subseteq G_{L|K}$ donde $G_\mathfrak{P}$ es el grupo de descomposición $D(\mathfrak{P}|\mathfrak{p})$, se tiene el isomorfismo invariante

$$\mathrm{inv}_{L_\mathfrak{P}|K_\mathfrak{p}} : H^2(G_{L_\mathfrak{P}|K_\mathfrak{p}}, L_\mathfrak{P}^*) \longrightarrow \Big(\frac{1}{[L_\mathfrak{P} : K_\mathfrak{p}]}\mathbb{Z}\Big)/\mathbb{Z} \subseteq \Big(\frac{1}{[L:K]}\mathbb{Z}\Big)/\mathbb{Z},$$

y cada $\mathrm{inv}_{L_\mathfrak{P}|K_\mathfrak{p}}$ es la composición de tres isomorfismos, ver Definición 5.1.13. Se tiene $H^2(G_{L|K}, J_L) \cong \bigoplus_\mathfrak{p} H^2(G_{L_\mathfrak{P}|K_\mathfrak{p}}, L_\mathfrak{P}^*)$, el cual es un grupo infinito.

Definición 6.6.26. Sea $c \in H^2(G_{L|K}, J_L)$. Descomponemos c así: $c = \oplus_\mathfrak{p} c_\mathfrak{p}$, $c_\mathfrak{p} \in H^2(G_{L_\mathfrak{P}|K_\mathfrak{p}}, L_\mathfrak{P}^*)$. Se define

$$\mathrm{inv}_{L|K} : H^2(G_{L|K}, J_L) \longrightarrow \Big(\frac{1}{[L:K]}\mathbb{Z}\Big)/\mathbb{Z},$$

por

$$\mathrm{inv}_{L|K}\, c := \sum_\mathfrak{p} \mathrm{inv}_{L_\mathfrak{P}|K_\mathfrak{p}}\, c_\mathfrak{p},$$

donde $c_\mathfrak{p}$ es la componente en $\mathfrak{p}$ de $c \in H^2(G_{L|K}, J_L) \cong \bigoplus\limits_{\mathfrak{p}\in\mathbb{P}_K} H^2(G_{L_\mathfrak{P}|K_\mathfrak{p}}, L_\mathfrak{P}^*)$.

Notemos que $c_\mathfrak{p} = 1$ para casi toda $\mathfrak{p}$ y por tanto $\mathrm{inv}_{L_\mathfrak{P}|K_\mathfrak{p}}\, c_\mathfrak{p} = 0$ para casi toda $\mathfrak{p}$.

Proposición 6.6.27. *Si $M \supseteq L \supseteq K$ son extensiones de Galois de K de campos globales, entonces*

(a) $\mathrm{inv}_{M|K}\, c = \mathrm{inv}_{L|K}\, c, \quad c \in H^2(G_{L|K}, J_L) \subseteq H^2(G_{M|K}, J_M)$ *bajo el mapeo de inflación puesto que* $H^1(G_{M|K}, J_M) = \{1\}$.
(b) $\mathrm{inv}_{M|L}(\mathrm{res}_L\, c) = [L : K] \cdot \mathrm{inv}_{M|K}\, c, \quad c \in H^2(G_{M|K}, J_M)$.
(c) $\mathrm{inv}_{M|K}(\mathrm{cor}_K\, c) = \mathrm{inv}_{M|L}\, c, \quad c \in H^2(G_{M|L}, J_M)$.

Para (b) *y* (c) *únicamente se requiere que M/K sea de Galois.*
En otras palabras, los siguientes diagramas son conmutativos:

(b)
$$\begin{array}{ccc} H^2(G_{M|L}, J_M) & \xrightarrow{\mathrm{inv}_{M|L}} & \Big(\frac{1}{[M:L]}\mathbb{Z}\Big)/\mathbb{Z} \\ \uparrow{\scriptstyle \mathrm{res}_L} & & \uparrow{\scriptstyle [L:K]} \\ H^2(G_{M|K}, J_M) & \xrightarrow{\mathrm{inv}_{M|K}} & \Big(\frac{1}{[M:K]}\mathbb{Z}\Big)/\mathbb{Z} \end{array}$$

(c)
$$\begin{array}{ccc} H^2(G_{M|L}, J_M) & \xrightarrow{\text{inv}_{M|L}} & \left(\frac{1}{[M:L]}\mathbb{Z}\right)/\mathbb{Z} \\ \Big\downarrow{\scriptstyle \text{cor}_K} & & \Big\downarrow{\scriptstyle j \text{ encaje}} \\ H^2(G_{M|K}, J_M) & \xrightarrow{\text{inv}_{M|K}} & \left(\frac{1}{[M:K]}\mathbb{Z}\right)/\mathbb{Z} \end{array}$$

Si $J = J_{K^{\text{sep}}} = \varinjlim_L J_L$ *y* $C = C_{K^{\text{sep}}} = \varinjlim_L C_L = J/(K^{\text{sep}})^*$ *donde el límite se toma sobre todas las extensiones finitas de Galois* L/K*, entonces obtenemos un mapeo*

$$\text{inv} : H^2(K, J) \longrightarrow \mathbb{Q}/\mathbb{Z},$$

con $H^2(K, J) = H^2(\text{Gal}(K^{\text{sep}}/K), J)$*, con la inclusión* $H^2(G_{L|K}, J_L) \longrightarrow H^2(G_{M|K}, J_M)$*, para* $K \subseteq L \subseteq M$*.*

Demostración. La proposición se sigue del comportamiento de los invariantes locales con respecto a los mapeos de inclusión, restricción y corestricción.

(a) Sea $c \in H^2(G_{L|K}, J_L)$, entonces

$$\text{inv}_{M|K}\, c = \sum_{\mathfrak{p}} \text{inv}_{M_\mathfrak{q}|K_\mathfrak{p}}\, c_\mathfrak{p} = \sum_{\mathfrak{p}} \text{inv}_{L_\mathfrak{P}|K_\mathfrak{p}}\, c_\mathfrak{p} = \text{inv}_{L|K}\, c,$$

donde $\mathfrak{q}$ es cualquier primo sobre $\mathfrak{P}$.

(b) Sea $c \in H^2(G_{M|K}, J_M)$ y $\mathfrak{P}$ recorriendo los primos de L. Entonces

$$\begin{aligned} \text{inv}_{M|L}(\text{res}_L\, c) &= \sum_{\mathfrak{P}} \text{inv}_{M_\mathfrak{q}|L_\mathfrak{P}}(\text{res}_L\, c)_\mathfrak{P} = \sum_{\mathfrak{P}} \text{inv}_{M_\mathfrak{q}|L_\mathfrak{P}}(\text{res}_{L_\mathfrak{P}}\, c_\mathfrak{p}) \\ &= \sum_{\mathfrak{P}} [L_\mathfrak{P} : K_\mathfrak{p}] \cdot \text{inv}_{M_\mathfrak{q}|K_\mathfrak{p}}\, c_\mathfrak{p} \\ &= \sum_{\mathfrak{p}} \sum_{\mathfrak{P}|\mathfrak{p}} [L_\mathfrak{P} : K_\mathfrak{p}] \cdot \text{inv}_{M_\mathfrak{q}|K_\mathfrak{p}}\, c_\mathfrak{p}, \end{aligned}$$

con $\mathfrak{q}|_L = \mathfrak{P}$ y $\mathfrak{P}|_K = \mathfrak{p}$.
Se tiene que $\text{inv}_{M_\mathfrak{q}|K_\mathfrak{p}}\, c_\mathfrak{p}$ son independientes del primo $\mathfrak{q}$ sobre el $\mathfrak{P}$ seleccionado, pues si $\mathfrak{P}_1$ es otro primo de L, el $K_\mathfrak{p}$-isomorfismo canónica $L_\mathfrak{P} \xrightarrow{\cong} L_{\mathfrak{P}_1}$ da un isomorfismo canónico $H^2(G_{L_\mathfrak{P}|K_\mathfrak{p}}, L_\mathfrak{P}^*) \xrightarrow{\cong} H^2(G_{L_{\mathfrak{P}_1}|K_\mathfrak{p}}, L_{\mathfrak{P}_1}^*)$ y el cual preserva el invariante. Por otro lado, tenemos $\sum_{\mathfrak{P}|\mathfrak{p}} [L_\mathfrak{P} : K_\mathfrak{p}] = [L : K]$, por lo que

$$\begin{aligned} \text{inv}_{M|L}(\text{res}_L\, c) &= \sum_{\mathfrak{p}} \Big(\sum_{\mathfrak{P}|\mathfrak{p}} [L_\mathfrak{P} : K_\mathfrak{p}] \Big) \text{inv}_{M_\mathfrak{q}|K_\mathfrak{p}}\, c_\mathfrak{p} \\ &= [L : K] \sum_{\mathfrak{p}} \text{inv}_{M_\mathfrak{q}|K_\mathfrak{p}}\, c_\mathfrak{p} = [L : K]\, \text{inv}_{M|L}\, c. \end{aligned}$$

(c) Para $c \in H^2(G_{M|L}, J_M)$, se tiene que

$$\begin{aligned}\operatorname{inv}_{M|K}(\operatorname{cor}_K c) &= \sum_{\mathfrak{p}} \operatorname{inv}_{M_\mathfrak{q}|K_\mathfrak{p}}(\operatorname{cor}_K c)_\mathfrak{p} \\ &= \sum_{\mathfrak{p}} \sum_{\mathfrak{P}|\mathfrak{p}} \operatorname{inv}_{M_\mathfrak{q}|K_\mathfrak{p}}(\operatorname{cor}_{K_\mathfrak{p}} c_\mathfrak{P}) \\ &= \sum_{\mathfrak{p}} \sum_{\mathfrak{P}|\mathfrak{p}} \operatorname{inv}_{M_\mathfrak{q}|L_\mathfrak{P}} c_\mathfrak{P} = \operatorname{inv}_{M|L}(c). \qquad \square\end{aligned}$$

Observación 6.6.28. Se tiene todo para poder aplicar el teorema de Tate-Nakayama, excepto que $\operatorname{inv}_{L|K} : H^2(G_{L|K}, J_L) \longrightarrow \left(\frac{1}{[L:K]}\mathbb{Z}\right)/\mathbb{Z}$ no es un isomorfismo (el primer grupo es infinito y el segundo finito). Para hacer de esto un isomorfismo, necesitamos pasar de J_L a $J_L/L^* = C_L$.

Definición 6.6.29. Sea L/K una extensión abeliana finita de campos globales. Para cada $\mathfrak{p} \in \mathbb{P}_K$, fijamos un $\mathfrak{P} \in \mathbb{P}_L$ con $\mathfrak{P}|_K = \mathfrak{p}$. Sea $\vec{\alpha} \in J_K$, entonces definimos el mapeo

$$[\vec{\alpha}, L/K] := \prod_{\mathfrak{p} \in \mathbb{P}_K} (\alpha_\mathfrak{p}, L_\mathfrak{P}/K_\mathfrak{p}) \in G_{L|K}.$$

Aquí, $(\alpha_\mathfrak{p}, L_\mathfrak{P}/K_\mathfrak{p}) \in G_\mathfrak{P}$ para toda $\mathfrak{p} \in \mathbb{P}_K$ y $(\alpha_\mathfrak{p}, L_\mathfrak{P}/K_\mathfrak{p}) = 1$ para casi toda $\mathfrak{p}$ y consideramos $G_\mathfrak{P} = G_{L_\mathfrak{P}|K_\mathfrak{p}} \subseteq G_{L|K}$. Se tiene que $\alpha_\mathfrak{p}$ es una unidad para casi todo $\mathfrak{p}$ y el número de primos ramificados es finito, por lo que $(\alpha_\mathfrak{p}, L_\mathfrak{P}/K_\mathfrak{p}) = 1$, para casi toda $\mathfrak{p}$.

El producto es independiente del orden de los factores pues el grupo $G_{L|K}$ es abeliano. A la extensión $L_\mathfrak{P}/K_\mathfrak{p}$ la denotamos $L_\mathfrak{p}/K_\mathfrak{p}$ para enfatizar que para cada $\mathfrak{p} \in \mathbb{P}_K$ seleccionamos únicamente un primo $\mathfrak{P} \in \mathbb{P}_L$ con $\mathfrak{P}|\mathfrak{p}$.

Proposición 6.6.30. *Sea L/K una extensión abeliana finita de campos globales, $\vec{\alpha} \in J_K$ y denotamos $(\vec{\alpha}) := \vec{\alpha}\,\mathrm{N}_{L/K} J_L \in H^0(G_{L|K}, J_L)$. Si $\mu \in \chi(G_{L|K}) = H^1(G_{L|K}, \mathbb{Q}/\mathbb{Z})$, entonces*

$$\mu\big([\vec{\alpha}, L/K]\big) = \operatorname{inv}_{L|K}\big((\vec{\alpha}) \Cup \delta\mu\big) \in \Big(\frac{1}{[L:K]}\mathbb{Z}\Big)/\mathbb{Z},$$

$(\vec{\alpha}) \in H^0(G_{L|K}, J_L)$, $\delta\mu \in H^2(G_{L|K}, \mathbb{Z})$, $\big((\vec{\alpha}) \Cup \delta\mu\big) \in H^2(G_{L|K}, J_L)$.

Demostración. El resultado es consecuencia de la fórmula análoga que relaciona el símbolo de la norma residual local $(\_, L_\mathfrak{P}/K_\mathfrak{p})$ con el invariante local $\operatorname{inv}_{L_\mathfrak{P}|K_\mathfrak{p}}$.

Sea $\mu_\mathfrak{p}$ la restricción de μ a $G_{L_\mathfrak{P}|K_\mathfrak{p}}$ y sea $(\alpha_\mathfrak{p}) = \alpha_\mathfrak{p}\,\mathrm{N}_{L_\mathfrak{P}/K_\mathfrak{p}} L_\mathfrak{P}^*$. Entonces

$$\mu\big([\vec{\alpha}, L/K]\big) = \sum_{\mathfrak{p}} \mu_\mathfrak{p}(\alpha_\mathfrak{p}, L_\mathfrak{p}|K_\mathfrak{p}) = \sum_{\mathfrak{p}} \operatorname{inv}_{L_\mathfrak{P}|K_\mathfrak{p}}\big((\alpha_\mathfrak{p}) \Cup \delta\mu_\mathfrak{p}\big).$$

Además, se tiene que $\big((\alpha_\mathfrak{p}) \Cup \delta\mu_\mathfrak{p}\big) \in H^2(G_{L_\mathfrak{P}|K_\mathfrak{p}}, L_\mathfrak{P}^*)$ son las componentes locales de $(\vec{\alpha}) \Cup \delta\mu \in H^2(G_{L|K}, J_L)$, únicamente necesitamos notar que $\alpha_\mathfrak{p} \cdot \delta\mu_\mathfrak{p}(\sigma,\tau)$ (resp. $\vec{\alpha} \cdot \delta\mu(\sigma,\tau)$) es un 2-cociclos de la clase $\big((\alpha_\mathfrak{p}) \Cup \delta\mu_\mathfrak{p}\big)$ (resp. $\big((\vec{\alpha}) \Cup \delta\mu\big)$). Por tanto

$$\mu\big([\vec{\alpha}, L/K]\big) = \mathrm{inv}_{L|K}\,\big((\vec{\alpha}) \Cup \delta\mu\big). \qquad \square$$

Cuando queramos definir $\mathrm{inv}_{L|K}$ en C_L, el siguiente resultado es de capital importancia. De la sucesión exacta

$$1 \longrightarrow L^* \longrightarrow J_L \longrightarrow C_L \longrightarrow 1,$$

obtenemos del hecho de que $H^1(G_{L|K}, C_L) = \{1\}$ que el homomorfismo $H^2(G_{L|K}, L^*) \longrightarrow H^2(G_{L|K}, J_L)$ es inyectivo. Con esto en mente, usaremos que $H^2(G_{L|K}, L^*) \subseteq H^2(G_{L|K}, J_L)$.

Teorema 6.6.31. *Sea L/K una extensión finita de Galois de campos globales. Si $c \in H^2(G_{L|K}, L^*)$, entonces* $\mathrm{inv}_{L|K}\, c = 0$.

Demostración. La demostración está basada en la descripción explícita del símbolo de la norma residual y de la fórmula del producto.

Sea L/K una extensión finita de Galois de campos globales. Sea $K_0 = \mathbb{Q}$ o $K_0 = K$, dependiendo de si K es numérico o de funciones. Sea M una extensión de Galois de K_0 que contiene a L. Entonces

$$c \in H^2(G_{L|K}, L^*) \subseteq H^2(G_{M|L}, M^*) \subseteq H^2(G_{M|K}, J_M),$$
$$\mathrm{cor}_{K_0}\, c \in H^2(G_{M|K_0}, M^*) \text{ y } \mathrm{inv}_{L|K}\, c = \mathrm{inv}_{M|K}\, c = \mathrm{inv}_{M|K_0}(\mathrm{cor}_{K_0}\, c).$$

Por tanto, para probar que $\mathrm{inv}_{L|K}\, c = 0$, es suficiente considerar el caso $K = K_0$.

Por la estructura del grupo de Brauer, existe una extensión L_0/K_0 con L_0 cíclica ciclotómica o de constantes, con $c \in H^2(G_{L_0|K_0}, L_0^*)$. En el caso numérico podemos suponer que L/K_0 es cíclica ciclotómica y que L/K_0 es extensión de constantes en el caso de campos de funciones.

Sea μ un generador del grupo cíclico $\chi(G_{L|K_0}) = H^1(G_{L|K_0}, \mathbb{Q}/\mathbb{Z})$. Entonces, $\delta\mu$ es un generaodr de $H^2(G_{L|K_0}, \mathbb{Z})$. Por el teorema de Tate, se tiene que

$$\_ \Cup \delta\mu : H^0(G_{L|K_0}, L^*) \longrightarrow H^2(G_{L|K_0}, L^*)$$

es una biyección. Por tanto todo elemento $c \in H^2(G_{L|K_0}, L^*)$ tiene la forma $c = (a) \Cup \delta\mu$ con $(a) = a\,\mathrm{N}_{L|K_0}\, L^* \in H^2(G_{L|K_0}, L^*)$, $a \in K_0^*$. De la Proposición 6.6.30 se tiene

$$\mathrm{inv}_{L|K_0}\, c = \mathrm{inv}_{L|K_0}\,\big((a) \Cup \delta\mu\big) = \mu\big([a, L/K_0]\big).$$

Por tanto necesitamos probar $[a, L/K_0] = \prod_{\mathfrak{p} \in \mathbb{P}_K} (a_\mathfrak{p}, L_\mathfrak{P}/(K_0)_\mathfrak{p}) = 1$.

Como L es ciclotómica $L \subseteq K_0(\zeta_n)$ para alguna n (ambos casos). El automorfismo $[a, L/K_0]$ es precisamente la restricción de $[a, K_0(\zeta_n)/K_0]$ a L (Teorema 5.3.14).

Por tanto, es suficiente probar que $[a, K_0(\zeta_n)/K_0] = 1$ para $a \in K_0^*$. Puesto que $K_0(\zeta_n)$ está generado por raíces de unidad de órdenes una potencia de un número primo, es suficiente probar que $[a, K_0(\zeta_n)/K_0] = 1$ para estos generadores. Por tanto, podemos suponer que $n = l^m$ con l un número primo.

Sea ζ una raíz l^m-primitiva de la unidad. Si $l = 2$ y $K_0 = \mathbb{Q}$, podemos suponer $m \geq 2$. Las completaciones de $K_0(\zeta_n)/K_0$ son $(K_0)_\mathfrak{p}(\zeta)/(K_0)_\mathfrak{p}$ la cual es no ramificada para $l \neq p = \mathfrak{p}$ y totalmente ramificada para $l = p = \mathfrak{p}$ caso $K_0 = \mathbb{Q}$ y $l \neq p$ y no ramificada siempre para los campos de funciones. Para $\mathfrak{p}$, el primo infinito real, $(K_0)_\mathfrak{p}(\zeta)/(K_0)_\mathfrak{p}$ significa $\mathbb{C}/\mathbb{R}$.

Se debe probar que para $a \in K_0^*$,

$$[a, K_0(\zeta)/K_0] = \prod_\mathfrak{p} (a, (K_0)_\mathfrak{p}(\zeta)/(K_0)_\mathfrak{p}) = 1.$$

Se tiene que $K_0(\zeta)/K_0$ es no ramificada excepto si $K_0 = \mathbb{Q}$, $\mathfrak{p} = l$ o $\mathfrak{p} = \mathcal{P}_\infty$ el valor absoluto usual de $\mathbb{Q}$. Para cualquier otro $\mathfrak{p}$, por ser la extensión no ramificada,

$$(a, (K_0)_\mathfrak{p}(\zeta)/(K_0)_\mathfrak{p}) = \varphi_\mathfrak{p}^{v_\mathfrak{p}(a)},$$

donde $\varphi_\mathfrak{p}$ es el Frobenius y por tanto

$$(a, (K_0)_\mathfrak{p}(\zeta)/(K_0)_\mathfrak{p})(\zeta) = \varphi_\mathfrak{p}^{v_\mathfrak{p}(a)}(\zeta).$$

El campo residual tiene $q_\mathfrak{p}$-elementos, donde

$$q_\mathfrak{p} = \begin{cases} p & \text{si } K_0 \text{ es numérico,} \\ q^{\operatorname{gr}\mathfrak{p}} & \text{si } K_0 \text{ es de funciones.} \end{cases}$$

Por tanto

$$(a, (K_0)_\mathfrak{p}(\zeta)/(K_0)_\mathfrak{p})(\zeta) = \zeta^{q_\mathfrak{p}^{v_\mathfrak{p}(a)}}.$$

Consideremos K_0 campo de funciones. Entonces

$$(a, (K_0)_\mathfrak{p}(\zeta)/(K_0)_\mathfrak{p})(\zeta) = \zeta^{q^{v_\mathfrak{p}(a)\operatorname{gr}\mathfrak{p}}}.$$

Se sigue

$$\prod_\mathfrak{p} (a, (K_0)_\mathfrak{p}(\zeta)/(K_0)_\mathfrak{p})(\zeta) = \prod_\mathfrak{p} \zeta^{q^{v_\mathfrak{p}(a)\operatorname{gr}\mathfrak{p}}} = \zeta^{q^s},$$

donde

$$s = \sum_{\mathfrak{p}} v_{\mathfrak{p}}(a) \operatorname{gr} \mathfrak{p} = \operatorname{gr} a = 0.$$

De esta forma

$$[a, K_0(\zeta)/K_0](\zeta) = \zeta^{q^0} = \zeta.$$

Esto prueba que $[a, K_0(\zeta)/K_0] = 1$ para K_0 un campo de funciones.

Ahora sea $K_0 = \mathbb{Q}$. Para $p \neq l, \mathcal{P}_\infty$, se tiene

$$(a, \mathbb{Q}_p(\zeta)/\mathbb{Q}_p) = \varphi^{v_p(a)} \quad \text{y} \quad (a, \mathbb{Q}_p(\zeta)/\mathbb{Q}_p)(\zeta) = \zeta^{\varphi^{v_p(a)}}.$$

Usando los grupos de Lubin-Tate, Ejemplos 5.8.38 y 5.8.59, se tiene, para $p = l$, $\zeta = \zeta_{p^m} = \zeta_{l^m}$, que

$$(a, \mathbb{Q}_p(\zeta)/\mathbb{Q}_p)(\zeta) = \zeta^r,$$

donde $r \equiv u^{-1} \operatorname{mód} p^m$ y donde $a = up^n$, $u \in U_p$. Entonces $r \equiv u^{-1} \equiv a^{-1} p^{v_p(a)} \operatorname{mód} p^m$.

Para $p = \mathcal{P}_\infty$, el automorfismo $(a, \mathbb{C}/\mathbb{R})$ es bien la identidad o bien conjugación compleja, dependiendo de si $a > 0$ o $a < 0$ respectivamente. Por tanto

$$(a, \mathbb{Q}_p(\zeta)/\mathbb{Q}_p)(\zeta) = \zeta^{\operatorname{sig} a}.$$

donde $\operatorname{sig}(a) = \begin{cases} 1 & \text{si } a > 0, \\ -1 & \text{si } a < 0. \end{cases}$ Se sigue que

$$[a, \mathbb{Q}(\zeta)/\mathbb{Q}](\zeta) = \prod_p (a, \mathbb{Q}_p(\zeta)/\mathbb{Q}_p)(\zeta) = \zeta^{\operatorname{sig} a \cdot \prod_{p \neq l} p^{v_p(a)} \cdot r},$$

Ahora

$$\operatorname{sig} a \cdot \prod_{p \neq l} p^{v_p(a)} \cdot r \equiv \operatorname{sig} a \cdot \prod_{p \neq l} p^{v_p(a)} \cdot l^{v_l(a)} \cdot a^{-1} = \frac{1}{\prod_p |a|_p} = 1 \operatorname{mód} l^m.$$

Se sigue que $[a, \mathbb{Q}(\zeta)/\mathbb{Q}](\zeta) = \zeta$ lo cual implica que $[a, \mathbb{Q}(\zeta)/\mathbb{Q}] = 1$. □

Corolario 6.6.32. *Sea L/K una extensión abeliana finita de campos globales y sea $\Omega = K^{\text{sep}}$. Entonces, si $a \in K^*$ es un idèle principal, se tiene $[a, L/K] = 1$ y $[a, \Omega/K] = 1$.* □

Con este resultado tenemos que $H^2(G_{L|K}, L^*) \subseteq \text{núc inv}_{L|K}$ donde $\text{inv}_{L|K} : H^2(G_{L|K}, J_L) \longrightarrow \left(\frac{1}{[L:K]}\mathbb{Z}\right)/\mathbb{Z}$ y donde L/K es una extensión abeliana finita de campos globales. Todavía queda pendiente averiguar exactamente cual es el núcleo de $\text{inv}_{L|K}$ y si $\text{inv}_{L|K}$ es suprayectiva.

Para el caso cíclico, se tiene

Proposición 6.6.33. *Si L/K es una extensión cíclica finita de campos globales, entonces*

$$1 \longrightarrow H^2(G_{L|K}, L^*) \xrightarrow{\inf} H^2(G_{L|K}, J_L) \xrightarrow{\mathrm{inv}_{L|K}} \Big(\frac{1}{[L:K]}\mathbb{Z}\Big)/\mathbb{Z} \longrightarrow 0$$

es una sucesión exacta.

En particular $\mathrm{inv}_{L|K}$ *es suprayectiva y* $\mathrm{núc}\,\mathrm{inv}_{L|K} = H^2(G_{L|K}, L^*)$.

Demostración. Para ver la suprayectividad de $\mathrm{inv}_{L|K}$, supongamos primero que $[L:K] = l^r$ con l un número primo. Se tiene que $\frac{1}{[L:K]} + \mathbb{Z}$ genera $\Big(\frac{1}{[L:K]}\mathbb{Z}\Big)/\mathbb{Z}$ por lo que es suficiente hallar $c \in H^2(G_{L|K}, J_L)$ tal que $\mathrm{inv}_{L|K}\, c = \frac{1}{[L:K]} + \mathbb{Z}$.

Como L/K es una extensión cíclica de orden l^r, existe $\mathfrak{p}_0 \in K$ totalmente inerte en L. Por tanto, para $\mathfrak{P}_0 \in \mathbb{P}_L$ sobre $\mathfrak{p}_0$, se tiene que $[L_{\mathfrak{P}_0} : K_{\mathfrak{p}_0}] = [L : K]$. Por el teorema de reciprocidad local, existe $c_{\mathfrak{p}_0} \in H^2(G_{L_{\mathfrak{P}_0}|K_{\mathfrak{p}_0}}, L^*_{\mathfrak{P}_0})$ con $\mathrm{inv}_{L_{\mathfrak{P}_0}|K_{\mathfrak{p}_0}}\, c_{\mathfrak{p}_0} = \frac{1}{[L_{\mathfrak{P}_0}:K_{\mathfrak{p}_0}]} + \mathbb{Z} = \frac{1}{[L:K]} + \mathbb{Z}$.

Sea $c_{\mathfrak{p}} = 1$ para todo $\mathfrak{p} \neq \mathfrak{p}_0$. De $H^2(G_{L|K}, J_L) \cong \bigoplus_{\mathfrak{p}} H^2(G_{L_{\mathfrak{P}}|K_{\mathfrak{p}}}, L^*_{\mathfrak{P}})$, consideremos $c = (\ldots, 1, c_{\mathfrak{p}_0}, 1, \ldots) \in H^2(G_{L|K}, J_L)$. Entonces

$$\mathrm{inv}_{L|K}\, c = \sum_{\mathfrak{p}} \mathrm{inv}_{L_{\mathfrak{P}}|K_{\mathfrak{p}}}\, c_{\mathfrak{p}} = \mathrm{inv}_{L_{\mathfrak{P}_0}|K_{\mathfrak{p}_0}}\, c_{\mathfrak{p}_0} = \frac{1}{[L:K]} + \mathbb{Z}.$$

Ahora sea $[L:K] = n = p_1^{r_1} \cdots p_s^{r_s}$ su descomposición en primos. Para cada $1 \leq i \leq s$, existe $K \subseteq L_i \subseteq L$, $[L_i : K] = p_i^{r_i}$. Sea

$$\frac{1}{n} = \frac{n_1}{p_1^{r_1}} + \cdots + \frac{n_s}{p_s^{r_s}}.$$

Existe $c_i \in H^2(G_{L_i|K}, J_{L_i})$ con $\mathrm{inv}_{L_i|K}\, c_i = \mathrm{inv}_{L|K}\, c_i = \frac{n_i}{p_i^{r_i}} + \mathbb{Z}$.

Sea $c = c_1 \cdots c_s \in H^2(G_{L|K}, J_L)$. Entonces

$$\mathrm{inv}_{L|K}\, c = \sum_{i=1}^{s} \mathrm{inv}_{L|K}\, c_i = \sum_{i=1}^{s} \frac{n_i}{p_i^{r_i}} + \mathbb{Z} = \frac{1}{n} + \mathbb{Z}.$$

Se sigue que $\mathrm{inv}_{L|K}$ es suprayectiva para toda extensión cíclica.

Puesto que $H^2(G_{L|K}, L^*) \subseteq \mathrm{núc}\,\mathrm{inv}_{L|K}$, para probar la igualdad, basta probar que $H^2(G_{L|K}, J_L)/H^2(G_{L|K}, L^*)$ es de orden menor o igual a $\frac{1}{[L:K]} = \big|\big(\frac{1}{[L:K]}\mathbb{Z}\big)/\mathbb{Z}\big|$.

Ahora bien, de la sucesión exacta $1 \longrightarrow L^* \longrightarrow J_L \longrightarrow C_L \longrightarrow 1$ y puesto que $H^1(G_{L|K}, C_L) = 1$, obtenemos en cohomología la sucesión exacta

$$1 \longrightarrow H^2(G_{L|K}, L^*) \longrightarrow H^2(G_{L|K}, J_L) \longrightarrow H^2(G_{L|K}, C_L).$$

Por tanto

$$\Big|\frac{H^2(G_{L|K}, J_L)}{H^2(G_{L|K}, L^*)}\Big| \Big| \big|H^2(G_{L|K}, C_L)\big| \Big| [L:K]. \qquad \square$$

Observación 6.6.34. Sería afortunado que tuviésemos que $\mathrm{inv}_{L|K}$ fuese suprayectiva en general, pero esto es falso. Para que cada elemento de $\left(\frac{1}{[L:K]}\mathbb{Z}\right)/\mathbb{Z}$ esté en la imagen del mapeo $\mathrm{inv}_{L|K}$, es necesario agregar a L una extensión cíclica.

Consideramos $H^2(G_{\Omega|K}, J_\Omega) = \bigcup_L H^2(G_{L|K}, J_L)$, donde L recorre a las extensiones finitas de Galois de K. Para extensiones de Galois, $K \subseteq L \subseteq M$, se tiene $H^2(G_{L|K}, J_L) \subseteq H^2(G_{M|K}, J_M)$.

$$\uparrow \inf$$

Ahora, el mapeo invariante inv se puede extender de $H^2(G_{L|K}, J_L)$ a $H^2(G_{M|K}, J_M)$ y por ende se obtiene el homomorfismo

$$\mathrm{inv}_K : H^2(G_{\Omega|K}, J_\Omega) \longrightarrow \mathbb{Q}/\mathbb{Z}$$

y donde $\mathrm{inv}_K\,|_L = \mathrm{inv}_{L|K} : H^2(G_{L|K}, J_L) \longrightarrow \left(\frac{1}{[L:K]}\mathbb{Z}\right)/\mathbb{Z} \subseteq \mathbb{Q}/\mathbb{Z}$.

Para cada $m \in \mathbb{N}$, existe L_m/K cíclica de grado m y tal que $\left(\frac{1}{m}\mathbb{Z}\right)/\mathbb{Z} \subseteq \mathrm{im}(\mathrm{inv}_K)$, lo cual implica que $\mathbb{Q}/\mathbb{Z} \subseteq \mathrm{im}(\mathrm{inv}_K)$.

Teorema 6.6.35. *El homomorfismo* $\mathrm{inv}_K : H^2(G_{\Omega|K}, J_\Omega) \longrightarrow \mathbb{Q}/\mathbb{Z}$ *es suprayectivo.* □

Ahora bien, el grupo de Brauer de K, $\mathrm{Br}(K)$, satisface que $\mathrm{Br}(K) = \bigcup_L H^2(G_{L|K}, L^*)$ donde L recorre las extensiones finitas de Galois de K. Para cada primo $\mathfrak{p}$ de K, seleccionamos un valor absoluto fijo en Ω, entonces este valor absoluto determina a su vez un primo $\mathfrak{P}$ de cada extensión de Galois L/K sobre $\mathfrak{p}$ y se tiene que el grupo de Brauer del campo local $K_\mathfrak{p}$ es tal que

$$\mathrm{Br}(K_\mathfrak{p}) = \bigcup_L H^2(G_{L_\mathfrak{P}|K_\mathfrak{p}}, L_\mathfrak{P}^*).$$

Se tiene

$$\begin{aligned} H^2(G_{L|K}, L^*) \longrightarrow H^2(G_{L|K}, J_L) &\cong \bigoplus_\mathfrak{p} H^2(G_{L_\mathfrak{P}|K_\mathfrak{p}}, L_\mathfrak{P}^*) \\ &\xrightarrow{\mathrm{inv}_{L|K}} \left(\frac{1}{[L:K]}\mathbb{Z}\right)/\mathbb{Z} \end{aligned}$$

y tomando el límite directo, en este caso la unión, obtenemos el homomorfismo canónico

$$\mathrm{Br}(K) \longrightarrow H^2(G_{\Omega|K}, J_\Omega) \cong \bigoplus_\mathfrak{p} \mathrm{Br}(K_\mathfrak{p}) \xrightarrow{\mathrm{inv}_{L|K}} \mathbb{Q}/\mathbb{Z},$$

donde $\mathrm{inv}_K = \sum_\mathfrak{p} \mathrm{inv}_{K_\mathfrak{p}}$, $\mathrm{inv}_{K_\mathfrak{p}} : \mathrm{Br}(K_\mathfrak{p}) \longrightarrow \mathbb{Q}/\mathbb{Z}$.

Teorema 6.6.36 (Brauer-Hasse-Noether). *Sea K un campo global. Se tiene*

(1) *Sea* $\mathrm{Br}(K) \longrightarrow \mathrm{Br}(K_\mathfrak{p})$, $\alpha \longmapsto \alpha_\mathfrak{p}$, *el mapeo canónico para cada lugar* $\mathfrak{p}$ *de* K. *Entonces* $\alpha_\mathfrak{p} = 0$ *para casi toda* $\mathfrak{p}$ *y en particular* $\mathrm{Br}(K) \longrightarrow \prod_\mathfrak{p} \mathrm{Br}(K_\mathfrak{p})$, $\alpha \longmapsto (\alpha_\mathfrak{p})_\mathfrak{p}$ *pertenece a* $\bigoplus_\mathfrak{p} \mathrm{Br}(K_\mathfrak{p})$.

(2) **Teorema principal de Hasse en la teoría de álgebras**
La sucesión $0 \longrightarrow \mathrm{Br}(K) \longrightarrow \bigoplus_\mathfrak{p} \mathrm{Br}(K_\mathfrak{p}) \xrightarrow{\xi} \mathbb{Q}/\mathbb{Z} \longrightarrow 0$ *es exacta, donde* $\xi\big((\alpha_\mathfrak{p})_\mathfrak{p}\big) = \sum_\mathfrak{p} \mathrm{inv}_\mathfrak{p}(\alpha_\mathfrak{p})$.
Notemos que $\bigoplus_\mathfrak{p} \mathrm{Br}(K_\mathfrak{p}) = \bigoplus_{\mathfrak{p}\ real} \frac{\left(\frac{1}{2}\mathbb{Z}\right)}{\mathbb{Z}} \bigoplus \bigoplus_{\mathfrak{p}\nmid\infty} \mathbb{Q}/\mathbb{Z}$.

Demostración. Los grupos $\mathrm{Br}(K)$, $\bigoplus_\mathfrak{p} \mathrm{Br}(K_\mathfrak{p}) \cong H^2(G_{\Omega|K}, J_\Omega)$ y $\mathbb{Q}/\mathbb{Z}$ son las respectivas uniones de $H^2(G_{L|K}, L^*)$, $\bigoplus_\mathfrak{p} H^2(G_{L_\mathfrak{P}|L_\mathfrak{p}}, L_\mathfrak{P}^*) \cong H^2(G_{L|K}, J_L)$ y $\left(\frac{1}{[L:K]}\mathbb{Z}\right)/\mathbb{Z}$ y donde L/K recorre las extensiones cíclicas finitas de K. Para cada L/K cíclica finita, se tiene que la sucesión

$$1 \longrightarrow H^2(G_{L|K}, L^*) \longrightarrow H^2(G_{L|K}, J_L) \xrightarrow{\mathrm{inv}_{L|K}} \Big(\frac{1}{[L:K]}\mathbb{Z}\Big)/\mathbb{Z} \longrightarrow 0$$

es exacta. El resultado se sigue tomando los límites directos (en nuestro caso uniones). □

Corolario 6.6.37 (Ley de reciprocidad de Hasse). *Sean los homomorfismos* $\mathrm{Br}(K) \xrightarrow{i} \bigoplus_\mathfrak{p} \mathrm{Br}(K_\mathfrak{p})$ *y* $\bigoplus_\mathfrak{p} \mathrm{Br}(K_\mathfrak{p}) \xrightarrow{\xi} \mathbb{Q}/\mathbb{Z}$, *entonces* $\psi = \xi \circ i = 0$, *esto es,* $\psi : \mathrm{Br}(K) \longrightarrow \mathbb{Q}/\mathbb{Z}$, $\psi(\alpha) = \sum_\mathfrak{p} \mathrm{inv}_{K_\mathfrak{p}}\, \alpha = 0$. □

6.7. Ley de reciprocidad

Consideremos la sucesión exacta $1 \longrightarrow L^* \longrightarrow J_L \xrightarrow{\pi} C_L \longrightarrow 1$.

Proposición 6.7.1. *Sea* L/K *una extensión cíclica finita de campos globales. Entonces* $\tilde{\pi} : H^2(G_{L|K}, J_L) \longrightarrow H^2(G_{L|K}, C_L)$ *es suprayectiva.*

Demostración. De la sucesión exacta, se obtiene en cohomología

$$H^1(G_{L|K}, C_L) = 1 \longrightarrow H^2(G_{L|K}, L^*) \longrightarrow H^2(G_{L|K}, J_L) \xrightarrow{\tilde{\pi}}$$
$$\xrightarrow{\tilde{\pi}} H^2(G_{L|K}, C_L) \longrightarrow H^3(G_{L|K}, L^*) \cong H^1(G_{L|K}, L^*) = 1.$$

Por tanto $\tilde{\pi}$ es suprayectiva. □

Nos gustaría definir en general para $\bar{c} \in H^2(G_{L|K}, C_L)$ y $c \in H^2(G_{L|K}, J_L)$ donde $\bar{c} = \tilde{\pi} c$,

$$\operatorname{inv}_{L|K} \bar{c} = \operatorname{inv}_{L|K} c \in \Big(\frac{1}{[L:K]}\mathbb{Z}\Big)/\mathbb{Z}.$$

Tenemos que la definición es independiente de la preimagen c pues 2 preimágenes cualesquiera difieren únicamente de un elemento en $H^2(G_{L|K}, L^*)$ pero cualquier elemento de este último grupo tiene invariante 0. Notemos que en general que se tiene

$$1 \longrightarrow H^2(G_{L|K}, L^*) \longrightarrow H^2(G_{L|K}, J_L) \xrightarrow{\tilde{\pi}} H^2(G_{L|K}, C_L) \longrightarrow$$
$$\longrightarrow H^3(G_{L|K}, L^*) \longrightarrow H^3(G_{L|K}, J_L) = \{1\}.$$

Se sigue que $\tilde{\pi}$ es suprayectiva si y solamente si $H^3(G_{L|K}, L^*) = \{1\}$ pero esto no se cumple en general. De hecho, si L/K es una extensión de Galois de grado n y m es el mínimo común múltiplo de todos los grados locales $n_{\mathfrak{p}} = [L_{\mathfrak{P}} : K_{\mathfrak{p}}]$, entonces $H^3(G_{L|K}, L^*)$ es un grupo cíclico de orden n/m ([7, Chap. 7, Theorem 12]).

Por tanto, no todo elemento $\bar{c} \in H^2(G_{L|K}, C_L)$ proviene de un elemento $c \in H^2(G_{L|K}, J_L)$ y no podemos definir $\operatorname{inv}_{L|K} \bar{c}$ como nos hubiera gustado.

Para poder definir un mapeo invariante para una extensión finita de Galois L/K, se procede de manera parecida para el caso de los grupos $H^2(G_{L|K}, J_L)$. Se tiene que el homomorfismo

$$H^2(G_{L|K}, J_L) \xrightarrow{\tilde{\pi}} H^2(G_{L|K}, C_L)$$

conmuta con los homomorfismos inf y res, esto es, si $K \subseteq L \subseteq M$ son extensiones finitas de Galois, entonces se tiene

$$\tilde{\pi} \circ \inf_M = \inf_M \circ \tilde{\pi} \quad \text{y} \quad \tilde{\pi} \circ \operatorname{res}_L = \operatorname{res}_L \circ \tilde{\pi}$$

y en la segunda fórmula, únicamente se necesita que M/K sea de Galois.

Notación 6.7.2. Sea L/K una extensión finita de Galois de campos globales. Entonces denotamos $H^q(L|K) = H^q(G_{L|K}, C_L)$. El grupo C_L jugará el papel global de L^* en el caso local.

Puesto que $H^1(L|K) = \{1\}$, las extensiones L/K forman una familia como en el caso local con C_L en lugar de L^*. Como de costumbre, cuando $K \subseteq L \subseteq M$, la inflación es inyectiva: $H^2(L|K) \xrightarrow{\inf} H^2(M|K)$ y supondremos que $H^2(L|K) \subseteq H^2(M|K)$. Si $\Omega = K^{\text{sep}}$ tenemos el límite directo

$$H^2(\Omega|K) = \varinjlim_L H^2(L|K),$$

donde L varía sobre las extensiones finitas de Galois de K y usaremos que $H^2(L|K) \subseteq H^2(\Omega|K)$ vía el mapeo inflación. De esta forma se tiene

$$H^2(\Omega|K) = \bigcup_L H^2(L|K),$$

y si $K \subseteq L \subseteq M$ son extensiones de Galois, entonces $H^2(L|K) \subseteq H^2(M|K) \subseteq H^2(\Omega|K)$.

De manera similar como en el caso local, tenemos:

Teorema 6.7.3. *Sea L/K una extensión finita de Galois de campos globales de grado n. Sea N/K una extensión cíclica de grado n. Entonces*

$$H^2(N|K) = H^2(L|K) \subseteq H^2(\Omega|K).$$

Demostración. Sea $M := NL$. Como N/K es cíclica, M/L es cíclica de orden un divisor de n.

$$\begin{array}{ccc} N & \text{——} & M = NL \\ {\scriptstyle n}\big| & & \big| \\ K & \text{————} & L \end{array}$$

Sea $\bar{c} \in H^2(N|K) \subseteq H^2(M|K)$. De la sucesión exacta

$$1 \longrightarrow H^2(L|K) \xrightarrow{\text{inf}} H^2(M|K) \xrightarrow{\text{res}} H^2(M, L),$$

se tiene que un elemento $\bar{c} \in H^2(M|K)$ es un elemento de $H^2(L|K)$ si y solamente si $\text{res}_L \bar{c} = 1$. Puesto que N/K es cíclica, el homomorfismo $H^2(G_{N|K}, J_L) \xrightarrow{\tilde{\pi}} H^2(N|K)$ es suprayectivo. Por tanto, existe $c \in H^2(G_{N|K}, J_L) \subseteq H^2(G_{M|K}, J_M)$ con $\tilde{\pi}c = \bar{c}$. Como $\tilde{\pi}$ conmuta con inflación, la cual es de hecho un inclusión, y también con restricción, se tiene

$$\text{res}_L \bar{c} = \text{res}_L(\tilde{\pi}c) = \tilde{\pi}(\text{res}_L c).$$

Por tanto, $\text{res}_L \bar{c} = 1 \iff \text{res}_L c \in \text{núc}\, \tilde{\pi} = H^2(G_{M|L}, M^*)$. Puesto que M/L es cíclica, $\text{res}_L c \in H^2(G_{M|L}, M^*) \iff \text{inv}_{M|L}(\text{res}_L c) = 0$. Ahora bien,

$$\text{inv}_{M|L}(\text{res}_L c) = [L : K] \cdot \text{inv}_{M|K} c = [N : K] \cdot \text{inv}_{N|K} c = 0.$$

Se sigue que $H^2(N|K) \subseteq H^2(L, K)$.

Puesto que $H^1(N|K) = \{1\}$ y $H^3(G_{N|K}, N^*) \cong H^1(G_{N|K}, N^*) = \{1\}$, se tiene la sucesión exacta en cohomología

$$1 \longrightarrow H^2(G_{N|K}, N^*) \longrightarrow H^2(G_{N|K}, J_N) \longrightarrow H^2(N|K) \longrightarrow 1,$$

y donde $|H^2(N|K)| = [N : K] = [L : K]$ pues N/K es una extensión cíclica (Teorema 6.6.25). Por otro lado, $|H^2(L|K)|$ divide a $[L : K]$ (Teorema 6.6.18). Por tanto $H^2(N|K) = H^2(L|K)$. □

Corolario 6.7.4. *Se tiene* $H^2(\Omega|K) = \bigcup_{L/K \text{ cíclica}} H^2(L|K)$.

Demostración. Es consecuencia de Teorema 6.7.3 y de que para toda $n \in \mathbb{N}$, existe una extensión cíclica L/K de grado n. □

Consideremos $K \subseteq L \subseteq M$ extensiones finitas de Galois. Ahora bien, al conmutar $\tilde{\pi} : H^2(G_{L|K}, J_L) \longrightarrow H^2(L|K)$ con restricción y con inflación, usando esto último, $\tilde{\pi}$ se extiende de manera canónica a $\tilde{\pi} : H^2(G_{M|K}, J_M) \longrightarrow H^2(M|K)$ y de esta forma obtenemos un homomorfismo

$$\tilde{\pi} : H^2(G_{\Omega|K}, J_\Omega) \longrightarrow H^2(\Omega|K),$$

cuya restricción a los grupos $H^2(G_{L|K}, J_L)$ son los homorfismos $\tilde{\pi}$ originales: $\tilde{\pi} : H^2(G_{L|K}, J_L) \longrightarrow H^2(L|K)$. Estos últimos no son suprayectivos en general pero, se tiene de cualquier forma el siguiente resultado:

Teorema 6.7.5. *El homomorfismo*

$$\tilde{\pi} : H^2(G_{\Omega|K}, J_\Omega) \longrightarrow H^2(\Omega|K)$$

es suprayectivo.

Demostración. Si $\bar{c} \in H^2(\Omega|K)$, entonces existe una extensión L/K cíclica finita tal que $\bar{c} \in H^2(L|K)$. Puesto que para extensiones cíclicas finitas

$$\tilde{\pi} : H^2(G_{L|K}, J_L) \longrightarrow H^2(L|K)$$

es suprayectiva, $\bar{c} = \tilde{\pi}c$ para alguna $c \in H^2(G_{L|K}, J_L) \subseteq H^2(G_{\Omega|K}, J_\Omega)$. □

Con este resultado, podemos obtener clases invariantes para los elementos de $H^2(\Omega, K) = \bigcup_L H^2(L|K)$ a partir del mapeo invariante de las clases de cohomología del grupo de idèles. De hecho, del homomorfismo

$$\mathrm{inv}_K : H^2(G_{\Omega|K}, J_\Omega) \longrightarrow \mathbb{Q}/\mathbb{Z},$$

el cual es suprayectivo, obtenemos:

Definición 6.7.6. Si $\bar{c} \in H^2(\Omega|K)$ y $\bar{c} = \tilde{\pi}c$, $c \in H^2(G_{\Omega|K}, J_\Omega)$, se define $\mathrm{inv}_K \bar{c} := \mathrm{inv}_K c \in \mathbb{Q}/\mathbb{Z}$.

Veamos que la definición es independiente de la preimagen c seleccionada. Si d es otra preimagen de $\bar{c}$ en $H^2(G_{\Omega|K}, J_\Omega)$, $\bar{c} = \tilde{\pi}d$, entonces podemos escoger L/K una extensión de Galois con $c, d \in H^2(G_{L|K}, J_L) \subseteq H^2(G_{\Omega|K}, J_\Omega)$ y podemos agrandar L en caso de ser necesario de tal forma que $\bar{c} \in H^2(L|K)$. Ahora bien, $\bar{c} = \tilde{\pi}c = \tilde{\pi}d$ por lo que c y d difieren por elemento de $\mathrm{núc}\,\tilde{\pi}$, $\tilde{\pi} : H^2(G_{L|K}, J_L) \longrightarrow H^2(L|K)$ y por tanto de un elemento de $H^2(G_{L|K}, L^*) = \mathrm{núc}\,\tilde{\pi}$, pero este elemento tiene invariante 0. Por tanto $\mathrm{inv}_K \bar{c}$ está bien definido.

Con esta definición de $\mathrm{inv}\,\bar{c}$, obtenemos un epimorfismo

$$\mathrm{inv}_K : H^2(\Omega|K) \longrightarrow \mathbb{Q}/\mathbb{Z}.$$

La restricción de inv_K a L, $\mathrm{inv}_K|_L$, donde L/K es una extensión finita de Galois, $\mathrm{inv}_K|_L = \mathrm{inv}_{L|K} : H^2(L|K) \longrightarrow \left(\frac{1}{[L:K]}\mathbb{Z}\right)/\mathbb{Z}$ puesto que los órdenes de los elementos de $H^2(L|K)$ dividen a $[L:K]$, y por lo tanto son mapeados al único subgrupo $\left(\frac{1}{[L:K]}\mathbb{Z}\right)/\mathbb{Z}$ de $\mathbb{Q}/\mathbb{Z}$ de orden $[L:K]$.

Teorema 6.7.7. *Cuando $\bar{c} = \tilde{\pi}c$, $\bar{c} \in H^2(L|K)$, $c \in H^2(G_{L|K}, J_L)$, entonces* $\mathrm{inv}_{L|K}\,\bar{c} = \mathrm{inv}_{L|K}\,c$.

Para el caso general, tenemos: Sean L/K una extensión finita de Galois de campos globales y $\Omega = K^{\mathrm{sep}}$. Entonces los mapeos invariantes

$$\mathrm{inv}_K : H^2(\Omega|K) \longrightarrow \mathbb{Q}/\mathbb{Z},$$
$$\mathrm{inv}_{L|K} : H^2(L|K) \longrightarrow \Big(\frac{1}{[L:K]}\mathbb{Z}\Big)/\mathbb{Z},$$

son isomorfismos.

Demostración. Se tiene que es suficiente verificar que $\mathrm{inv}_{L|K}$ es biyectiva pues como $H^2(L|K) = H^2(N|K)$ para N/K cíclica con $[N:K] = [L:K]$, se tiene que si $\{N_n\}_{n=1}^{\infty}$ es una colección tal que N_n/K es cíclica de grado n, $H^2(\Omega|K) = \bigcup_{n=1}^{\infty} H^2(N_n|K)$ y $\mathrm{inv}_K\left(H^2(N_n,K)\right) = \left(\frac{1}{n}\mathbb{Z}\right)/\mathbb{Z}$, $\mathbb{Q}/\mathbb{Z} = \bigcup_{n=1}^{\infty}\left(\frac{1}{n}\mathbb{Z}\right)/\mathbb{Z}$.

Sea L/K dada y N/K cíclica con $[N:K] = [L:K]$. Por tanto $H^2(L|K) = H^2(N|K)$. Si $\alpha \in \left(\frac{1}{[L:K]}\mathbb{Z}\right)/\mathbb{Z}$, existe $c \in H^2(G_{N|K}, J_N)$ con $\mathrm{inv}_{N|K}\,c = \alpha$. Sea $\bar{c} = \tilde{\pi}c \in H^2(N|K) = H^2(L|K)$ Entonces $\mathrm{inv}_{L|K}\,\bar{c} = \mathrm{inv}_{N|K}\,\bar{c} = \mathrm{inv}_{N|K}\,c = \alpha$. Por tanto $\mathrm{inv}_{L|K}$ es suprayectiva. Ahora bien, $|H^2(L|K)|\big|[L:K] = \left|\left(\frac{1}{[L:k]}\mathbb{Z}\right)/\mathbb{Z}\right|$. Por tanto $\mathrm{inv}_{L|K}$ es biyectiva. □

Para enunciar el resultado principal de la teoría global de campos de clase, damos una definición que pudimos haber dado antes de desarrollar la teoría local de campos de clase, pero, en ese punto, por razones de claridad, preferimos dar directamente los resultados para campos locales.

6.7.1. Formación de clases

Sea G un grupo profinito, es decir, G es compacto con la topología de los subgrupos normales (topología de Krull), es decir, una base de vecindades abiertas de la identidad 1 de G consiste de los subgrupos de G que son normales y de índice finito o, equivalentemente, G es compacto, Hausdorff y totalmente disconexo.

Sea $\{G_K \mid K \in X\}$ la familia de todos los subgrupos cerrados de G. Los subgrupos abiertos son los subgrupos cerrados de índice finito.

Enumeramos cada uno de los subgrupos cerrados G_K con el índice K que llamaremos *campo* y formalmente nos referimos a K como el "*campo fijo de*

G_K". El campo K_0, con $G_{K_0} = G$ se llama el *campo base* y denotamos por $\Omega = K^{\text{sep}}$ el campo tal que $G_\Omega = \{1\}$.

Escribimos formalmene $K \subseteq L$ o L/K si $G_L \subseteq G_K$ y al par L/K lo llamamos *extensión de campos*. La extensión L/K se llama *finita* si G_L es abierto en G_K (es de índice finito) y ponemos $[L : K] := [G_K : G_L]$ y lo llamamos el *grado de la extensión*. Si G_L es normal en G_K, la extensión L/K se llama *normal* o *de Galois* . En este caso se define *el grupo de Galois* de L/K por $\text{Gal}(L/K) = G_{L|K} := G_K/G_L$.

Si $K \subseteq L \subseteq M$ son dos extensiones de Galois, se define la *restricción a* L de $\sigma \in \text{Gal}(M/K)$ por

$$\sigma|_L = \sigma \text{ mód } \text{Gal}(M/L) \in \text{Gal}(L/K).$$

La extensión se llama *cíclica, abeliana, nilpotente, soluble, simple*, etc. si L/K es de Galois y $\text{Gal}(L/K)$ es cíclica, abeliana, nilpotente, soluble, simple, etc.

Se define $K = \bigcap_i K_i$ (intersección) si G_K es topológicamente generado por los subgrupos G_{K_i} y $K = \prod_i K_i$ (composición) si $G_K = \bigcap_i G_{K_i}$. Si $G_{L'} = \sigma^{-1} G_i \sigma$, $\sigma \in G$, escribimos $L' = L^\sigma = \sigma(L)$.

De esta forma, de cada grupo profinito G obtenemos una teoría de Galois formal.

Definición 6.7.8. Sean G un grupo profinito y A un G-módulo con A dotado de la topología discreta y tal que satisface cualquiera de las tres siguientes condiciones equivalentes:

(a) La acción $G \times A \longrightarrow A$, $(\sigma, a) \longmapsto \sigma a$ es continua.
(b) Para cada $a \in A$, el estabilizador $\{\sigma \in G \mid \sigma a = a\}$ es abierto en G.
(c) $A = \bigcup_U A^U$ donde U recorre todos los subgrupos abiertos de G.

Entonces el par (G, A) se llama una *formación*. A puede tener otra topología que no sea la discreta, pero para (a) se considerará A con la topología discreta.

Ejemplo 6.7.9. Si G es el grupo de Galois de la extensión de campos E/F, entonces G actúa en E^* y el par (G, E^*) es una formación. Aquí, para $F \subseteq N \subseteq E$, $G_N = \text{Gal}(E/N)$ (si G es finito, G tiene la topología discreta).

Sea (G, A) una formación, A escrito multiplicativamente. Se define $A_K = A^{G_K} = \{a \in A \mid \sigma a = a \text{ para toda } \sigma \in G_K\}$.

Ejemplo 6.7.10. Sean K_0 un campo local y $\Omega = K_0^{\text{sep}}$. Entonces $A_K = K^*$.

Ejemplo 6.7.11. Sean K_0 un campo global y $\Omega = K_0^{\text{sep}}$. Entonces $A_K = C_K$.

Dada una formación (G, A) consideramos para una extensión de Galois L/K los grupos de cohomología del $G_{L|K}$-módulo A_L.

Definición 6.7.12. Una formación (G, A) se llama una *formación de clases* si satisface las siguientes condiciones:

Axioma I: $H^1(L|K) = H^1(G_{L|K}, A_L) = \{1\}$ para cada extensión finita de Galois L/K (formación de campos).

Axioma II: Para toda extensión finita de Galois L/K, existe un isomorfismo

$$\mathrm{inv}_{L|K} : H^2(L|K) = H^2(G_{L|K}, A_L) \longrightarrow \big(\frac{1}{[L:K]}\mathbb{Z}\big)/\mathbb{Z}$$

llamado el *mapeo invariante* con las siguientes propiedades:

(a) Si $K \subseteq L \subseteq M$ es una torre de extensiones finitas de Galois, entonces

$$\mathrm{inv}_{L|K} = \mathrm{inv}_{M|K}\,|_{H^2(L|K)}.$$

(b) Si $K \subseteq L \subseteq M$ es una torre de extensiones con M/K finita de Galois, entonces

$$\mathrm{inv}_{M|L} \circ \mathrm{res}_L = [L:K] \cdot \mathrm{inv}_{M|K}$$

$$\begin{array}{ccc} H^2(M|K) & \xrightarrow{\mathrm{inv}_{M|K}} & \Big(\frac{1}{[M:K]}\mathbb{Z}\Big)/\mathbb{Z} \\ \Big\downarrow{\scriptstyle \mathrm{res}_L} & & \Big\downarrow{\scriptstyle \cdot[L:K]} \\ H^2(M|L) & \xrightarrow[\mathrm{inv}_{M|L}]{} & \Big(\frac{1}{[M:L]}\mathbb{Z}\Big)/\mathbb{Z} \end{array}$$

Si (G, A) es una formación de clases, se tienen

Teorema 6.7.13 (Principal). *Sea L/K una extensión finita de Galois. Entonces el mapeo $u_{L|K} \cup_{\_} : H^q(G_{L|K}, \mathbb{Z}) \longrightarrow H^{q+2}(L|K)$ con $u_{L|K} \in H^2(L|K)$ la* clase fundamental *($\mathrm{inv}_{L|K}(u_{L|K}) = \frac{1}{[L:K]} + \mathbb{Z} \in \big(\frac{1}{[L:K]}\mathbb{Z}\big)/\mathbb{Z} \subseteq \mathbb{Q}/\mathbb{Z}$) es un isomorfismo para toda $q \in \mathbb{Z}$.* □

Teorema 6.7.14 (Ley general de reciprocidad). *Sea L/K una extensión finita de Galois, $u_{L|K} \cup_{\_} : H^{-2}(G_{L|K}, \mathbb{Z}) \longrightarrow H^0(L|K)$ nos da un isomorfismo canónico (mapeo de Nakayama):*

$$\theta_{L|K} : G_{L|K}^{\mathrm{ab}} \longrightarrow A_K / \mathrm{N}_{L/K} A_L.$$ □

Se obtienen todos los resultados derivados de cohomología que obtuvimos para los campos locales pues si K_0 es un campo local, $\Omega = K_0^{\mathrm{sep}}$, $G = \mathrm{Gal}(\Omega/K_0)$ y $A = \Omega^*$, entonces (G, A) es una formación de clases.

Para obtener estos resultados para cualquier otra formación de clases, las demostraciones se obtienen sustituyendo Ω^* por el otro A y $\mathrm{Gal}(\Omega/K_0)$ por el otro G.

Lo que queremos obtener es que si K es un campo global y $\Omega = K^{\text{sep}}$, $G = \text{Gal}(\Omega/K)$, entonces (G, C_Ω), C_Ω el grupo de clases de idèles de Ω: $C_\Omega = \bigcup_L C_L$, donde L recorre todas las extensiones finitas y separables de K, es una formación de clases.

Se tiene que (G, C_Ω) es una formación.

Teorema 6.7.15. *La formación (G, C_Ω) es una formación de clases con respecto al mapeo invariante $\text{inv}_K : H^2(\Omega|K) \longrightarrow \mathbb{Q}/\mathbb{Z}$ definido en la Definición* 6.7.6.

Demostración. Debemos verificar los Axiomas I y II de la Definición 6.7.12:

Axioma I: $H^1(L|K) = H^1(G_{L|K}, C_L) = \{1\}$ para toda extensión de Galois finita (Teorema 6.6.20).

Axioma II: Para cada extensión de Galois finita tenemos el isomorfismo $\text{inv}_{L|K} : H^2(L|K) \longrightarrow \left(\frac{1}{[L:K]}\mathbb{Z}\right)/\mathbb{Z}$ (Teorema 6.7.7).

(a): Si $K \subseteq L \subset M$ son dos extensiones finitas de Galois de K y $\bar{c} \in H^2(L|K)$, entonces $\bar{c} \in H^2(M|K)$ y $\text{inv}_{M|K}\, \bar{c} = \text{inv}_{L|K}\, \bar{c}$ pues $\text{inv}_{M|K}$ y $\text{inv}_{L|K}$ están definidas por restricción de inv_K a $H^2(M, K)$ y $H^2(L, K) \subseteq H^2(M|K)$, respectivamente.

(b): Sean $K \subseteq L \subseteq M$ dos extensiones de K con M/K extensión finita de Galois. Si $\bar{c} \in H^2(M|K)$, entonces $\text{res}_L\, \bar{c} \in H^2(M|L)$. Para la demostración de la fórmula

$$\text{inv}_{M|K}(\text{res}_L\, \bar{c}) = [L : K]\, \text{inv}_{M|L}\, \bar{c}$$

usamos la fórmula análoga para el grupo de idèles: existe $c \in H^2(G_{\Omega|K}, J_\Omega)$ con $\tilde{\pi}c = \bar{c}$ donde podemos suponer que hay una extensión finita de Galois N/K que contiene a M, $K \subseteq L \subseteq M \subseteq N$, tal que $c \in H^2(G_{N|K}, J_N)$. De la fórmulas de la Proposición 6.6.27 y usando al mapeo inflación como inclusión tenemos

$$\begin{aligned}\text{inv}_{M|L}(\text{res}_L\, c) &= \text{inv}_{N|L}(\text{res}_L\, \tilde{\pi}c) = \text{inv}_{N|L}(\tilde{\pi}\, \text{res}_L\, c) = \text{inv}_{N|L}(\text{res}_L\, c)\\ &= [L : K] \cdot \text{inv}_{N|K}\, c = [L : K] \cdot \text{inv}_{N|K}\, \tilde{\pi}c\\ &= [L : K] \cdot \text{inv}_{M|K}\, \bar{c}.\end{aligned}$$

□

Con este resultado podemos aplicar los resultados obtenidos para campos locales a los campos globales.

Sea $u_{L|K} \in H^2(L|K)$ la *clase fundamental* de la extensión de Galois L/K que está unívocamente por la fórmula $\text{inv}_{L|K}\, u_{L|K} = \frac{1}{[L:K]} + \mathbb{Z}$. Obtenemos el resultado general:

Teorema 6.7.16. *Sea L/K una extensión finita de Galois de campos globales. El homomorfismo del producto copa con la clase fundamental*

$$u_{L|K} \cup \_ : H^q(G_{L|K}, \mathbb{Z}) \longrightarrow H^{q+2}(L|K)$$

es biyectiva para toda $q \in \mathbb{Z}$. □

De esto obtenemos:

Corolario 6.7.17. *Sea L/K una extensión finita de Galois de campos globales. Entonces $H^3(L|K) = \{1\}$ y $H^4(L|K) \cong \chi(G_{L|K})$.* □

Para $q = -2$, obtenemos

Teorema 6.7.18 (Ley de reciprocidad de Artin). *Sea L/K una extensión finita de Galois de campos globales. El mapeo del producto copa con la clase fundamental*

$$G_{L|K}^{\mathrm{ab}} \cong H^{-2}(G_{L|K}|\mathbb{Z}) \xrightarrow{u_{L|K} \cup \_} H^0(L|K) = C_K/\,\mathrm{N}_{L/K}\, C_L,$$

nos da un isomorfismo canónico, es decir el mapeo de reciprocidad *entre la abelianización $G_{L|K}^{\mathrm{ab}}$ del grupo de Galois $G_{L|K}$ de L/K y el grupo residual de las normas $C_K/\,\mathrm{N}_{L/K}\, C_L$ del grupo de clases de idèles C_K (mapeo de Nakayama):*

$$\theta_{L|K} \colon G_{L|K}^{\mathrm{ab}} \longrightarrow C_K/\,\mathrm{N}_{L/K}\, C_L.$$

El inverso del mapeo $\theta_{L|K}$ es el inducido por el homomorfismo

$$\psi_{L|K} = (\ , L/K) : C_K \longrightarrow G_{L|K}^{\mathrm{ab}}$$

con núcleo $\mathrm{N}_{L/K}\, C_L$ y recibe el nombre del símbolo de la norma residual (global) *o* mapeo de reciprocidad (global)*.*

La sucesión

$$1 \longrightarrow \mathrm{N}_{L/K}\, C_L \longrightarrow C_K \xrightarrow{(\ , L/K)} G_{L|K}^{\mathrm{ab}} \longrightarrow 1,$$

es exacta. □

Puesto que el mapeo invariante es compatible con el mapeo inflación (que es una inclusión) y con el mapeo restricción, el símbolo de la norma residual, se comporta como en el caso local:

Teorema 6.7.19. *Sean $K \subseteq L \subseteq M$ dos extensiones finitas de campos globales con M/K de Galois. Entonces, los siguientes diagramas son conmutativos*

(a) *Si L/K es de Galois, entonces*

$$\begin{array}{ccc} C_K & \xrightarrow{(\_,M/K)} & G^{\mathrm{ab}}_{M|K} \\ {\scriptstyle \mathrm{Id}}\downarrow & & \downarrow{\scriptstyle \pi} \\ C_K & \xrightarrow{(\_,L/K)} & G^{\mathrm{ab}}_{L|K} \end{array} \qquad \begin{array}{c} \pi : \mathrm{Gal}(M/K) \longrightarrow \mathrm{Gal}(L/K) \cong \\ \cong \dfrac{\mathrm{Gal}(M/K)}{\mathrm{Gal}(M/L)}, \\ \sigma \longmapsto \sigma|_L \end{array}$$

Aquí se tiene $(\tilde{\vec{\alpha}}, L/K) = \pi(\tilde{\vec{\alpha}}, M/K) \in G^{\mathrm{ab}}_{L|K}$, $\tilde{\vec{\alpha}} \in C_K$.

(b)

$$\begin{array}{ccc} C_K & \xrightarrow{(\_,M/K)} & G^{\mathrm{ab}}_{M|K} \\ {\scriptstyle \iota}\downarrow & & \downarrow{\scriptstyle \mathrm{Ver}} \\ C_L & \xrightarrow{(\_,M/L)} & G^{\mathrm{ab}}_{M|L} \end{array}$$

Esto es, $(\tilde{\vec{\alpha}}, M/L) = \mathrm{Ver}(\tilde{\vec{\alpha}}, M/K) \in G^{\mathrm{ab}}_{M|L}$, $\tilde{\vec{\alpha}} \in C_K$, *donde el mapeo de transferencia* Ver *está inducido por restricción:*

$$G^{\mathrm{ab}}_{M|K} \cong H^{-2}(G_{M|K}, \mathbb{Z}) \xrightarrow{\mathrm{res}} H^{-2}(G_{M|L}, \mathbb{Z}) \cong G^{\mathrm{ab}}_{M|L}$$

y ι es el encaje natural.

(c)

$$\begin{array}{ccc} C_L & \xrightarrow{(\_,M/L)} & G^{\mathrm{ab}}_{M|L} \\ {\scriptstyle \mathrm{N}_{L|K}}\downarrow & & \downarrow{\scriptstyle \kappa} \\ C_K & \xrightarrow{(\_,M/K)} & G^{\mathrm{ab}}_{M|K} \end{array}$$

Es decir, $(\mathrm{N}_{L|K}\,\tilde{\vec{\alpha}}, M/K) = \kappa\big((\tilde{\vec{\alpha}}, M/L)\big) \in G^{\mathrm{ab}}_{M|K}$ *para* $\tilde{\vec{\alpha}} \in C_L$ *y donde κ es el encaje natural* $\kappa : G^{\mathrm{ab}}_{M|L} \longrightarrow G^{\mathrm{ab}}_{M|K}$.

(d)

$$\begin{array}{ccc} C_K & \xrightarrow{(\_,M/K)} & G^{\mathrm{ab}}_{M|K} \\ {\scriptstyle \sigma}\downarrow & & \downarrow{\scriptstyle \sigma^*} \\ C_{\sigma K} & \xrightarrow{(\_,\sigma M/\sigma K)} & G^{\mathrm{ab}}_{\sigma M|\sigma K} \end{array}$$

Es decir, $\big(\sigma\tilde{\vec{\alpha}}, \sigma M/\sigma K\big) = \sigma\big(\tilde{\vec{\alpha}}, M/K\big)\sigma^{-1}$ *para* $\tilde{\vec{\alpha}} \in C_K$, *donde para* $\sigma \in G := G_{\Omega|K_0}$ *los mapeos* $C_K \xrightarrow{\sigma} C_{\sigma K}$ *y* $G^{\mathrm{ab}}_{M|K} \xrightarrow{\sigma^*} G^{\mathrm{ab}}_{\sigma M|\sigma K}$ *están inducidas por* $\vec{\alpha} \longmapsto \sigma\vec{\alpha}$ *y* $\tau \longmapsto \sigma\tau\sigma^{-1}$. □

Definición 6.7.20. Sea K un campo global. Un subgrupo H de C_K se llama *grupo de normas* si existe una extensión finita de Galois L/K tal que $H = \mathrm{N}_{L/K}\, C_L$. En este caso denotamos $H = \mathcal{N}_L = \mathrm{N}_{L/K}\, C_L$.

6.7.2. Ley de reciprocidad vía el isomorfismo de Neukirch

Aquí presentamos otra forma de obtener el mapeo de Nakayama, usando ahora el isomorfismo de Neukirch.

Hicimos el desarrollo para campos locales, sin embargo, el desarrollo vale para cualquier formación, junto con una función grado y un axioma sobre los grupos de cohomología. Veremos que (G_Ω, C_Ω) satisface esta condición, donde K es un campo global, Ω una cerradura separable, $\Omega = K^{\text{sep}}$ y $C_\Omega = \bigcup_L C_L$, L/K variando en las extensiones finitas de Galois. Entonces (G_Ω, C_Ω) es una formación.

Necesitamos un epimorfismo continuo llamado *grado*: $\text{gr} : G = G_\Omega \longrightarrow \hat{\mathbb{Z}}$.

Empezamos por usar la Definición 6.6.29. Sea $\vec{\alpha} \in J_L$, L/K una extensión finita de Galois de campos globales:

$$[\vec{\alpha}, L/K] = \langle \vec{\alpha}, L/K \rangle := \prod_{\mathfrak{p} \in \mathbb{P}_K} (\alpha_\mathfrak{p}, L_\mathfrak{p}/K_\mathfrak{p}),$$

donde $(\_, L_\mathfrak{p}/K_\mathfrak{p})$ son los mapeos de reciprocidad local y donde para cada $\mathfrak{p} \in \mathbb{P}_K$ seleccionamos un único $\mathfrak{P} \in \mathbb{P}_L$ con $\mathfrak{P}|\mathfrak{p}$ y $L_\mathfrak{p} = L_\mathfrak{P}$.

Teorema 6.7.21. *Si L/K y L'/K' son dos extensiones finitas abelianas de campos globales, tales que $K \subseteq K'$ y $L \subseteq L'$, entonces el diagrama*

$$\begin{array}{ccc} J_{K'} & \xrightarrow{[\_, L'/K']} & G^{\text{ab}}_{L'|K'} \\ {\scriptstyle \text{N}_{K'/K}}\downarrow & & \downarrow{\scriptstyle \text{rest}} \\ J_K & \xrightarrow[[\_, L/K]]{} & G^{\text{ab}}_{L|K} \end{array} \qquad \begin{array}{c} \sigma \\ \downarrow \\ \sigma|_L \end{array}$$

es conmutativo.

En otras palabras, si $\vec{\alpha} \in J_{K'}$,

$$[\text{N}_{K'/K}\, \vec{\alpha}, L/K] = [\vec{\alpha}, L'/K']|_L.$$

Demostración. Se tiene para $\vec{\alpha} \in J_{K'}$,

$$(\alpha_\mathfrak{q}, L'_\mathfrak{q}/K'_\mathfrak{q})|_{L_\mathfrak{p}} = \big(\text{N}_{K'_\mathfrak{q}/K_\mathfrak{p}}(\alpha_\mathfrak{q}), L_\mathfrak{p}/K_\mathfrak{p}\big),$$

con $\mathfrak{q} \in \mathbb{P}_{K'}$, $\mathfrak{q}|\mathfrak{p}$, $\mathfrak{p} \in \mathbb{P}_K$.

Ahora $(\text{N}_{K'/K}\, \vec{\alpha})_\mathfrak{p} = \prod_{\mathfrak{q}|\mathfrak{p}} \text{N}_{K'_\mathfrak{q}/K_\mathfrak{p}}(\alpha_\mathfrak{q})$ por lo que

$$\begin{aligned} [\text{N}_{K'/K}\, \vec{\alpha}, L/K] &= \prod_\mathfrak{p} \big((\text{N}_{K'/K}\, \vec{\alpha})_\mathfrak{p}, L_\mathfrak{p}/K_\mathfrak{p}\big) = \prod_\mathfrak{p} \prod_{\mathfrak{q}|\mathfrak{p}} \big(\text{N}_{K'_\mathfrak{q}/K_\mathfrak{p}}(\alpha_\mathfrak{q}), L_\mathfrak{p}/K_\mathfrak{p}\big) \\ &= \prod_\mathfrak{q} (\alpha_\mathfrak{q}, L'_\mathfrak{q}/K'_\mathfrak{q})|_L = [\vec{\alpha}, L'/K']|_L. \end{aligned}$$

□

Se tiene el homomorfismo

$$[\_, L/K] : J_K \longrightarrow \mathrm{Gal}(L/K)$$

para una extensión abeliana arbitraria L/K, la cual podría ser de grado infinito, por medio de las restricciones $[\_, L/K]|_{L'} := [\_, L'/K]$ donde L' recorre las subextensiones finitas de L/K.

En otras palabras, si $\vec{\alpha} \in J_K$, consideramos $[\vec{\alpha}, L'/K] \in G_{L'|K}$ que forma parte del límite proyectivo $\varprojlim_{L'} G_{L'|K} = G_{L|K}$ y $[\vec{\alpha}, L/K] = \varprojlim_{L'}[\vec{\alpha}, L'/K]$ es este elemento después de identificar $G_{L|K}$ con $\varprojlim_{L'} G_{L'|K}$. La igualdad

$$[\vec{\alpha}, L/K] = \prod_{\mathfrak{p}} (\alpha_{\mathfrak{p}}, L_{\mathfrak{p}}/K_{\mathfrak{p}})$$

permanece válida en el sentido de que el producto infinito del lado derecho converge a $[\vec{\alpha}, L/K]$ en el grupo topológico $G_{L|K}$. Más precisamene, si L'/K es finita, el conjunto $S_{L'} = \{\mathfrak{p} \mid (\alpha_{\mathfrak{p}}, L'_{\mathfrak{p}}/K_{\mathfrak{p}}) \neq 1\}$ es finito y se pueden considerar a los elementos

$$\xi_{L'} := \prod_{\mathfrak{p} \in S_{L'}} (\alpha_{\mathfrak{p}}, L_{\mathfrak{p}}/K_{\mathfrak{p}}) \in G_{L|K}.$$

Sea $[\vec{\alpha}, L/K] \cdot G_{L|M}$ una vecindad abierta básica de $[\vec{\alpha}, L/K]$, esto es, M/K es una subextensión finita de L/K. Entonces $\sigma_{L'} \in [\vec{\alpha}, L/K] \cdot G_{L/M}$ para toda $L' \supseteq M$ pues

$$\sigma_{L'}|_M = \prod_{\mathfrak{p}} (\alpha_{\mathfrak{p}}, M_{\mathfrak{p}}/K_{\mathfrak{p}}) = [\vec{\alpha}, M/K] = [\vec{\alpha}, L/M]|_M,$$

lo cual prueba que $[\vec{\alpha}, L/K]$ es el único punto de acumulación de $\{\sigma_{L'}\}$. Se sigue que el teorema anterior sigue compliéndose para extensiones infinitas L y L' de K y K' respectivamente.

El siguiente resultado está relacionado con la teoría de Iwasawa.

Teorema 6.7.22. *Sea Ω la máxima extensiones abeliana de $\mathbb{Q}$, es decir, (Kronecker-Weber) $\Omega = \bigcup_{n=1}^{\infty} \mathbb{Q}(\zeta_n)$ es el campo generado por las raíces de unidad. Sea T el subgrupo de torsión de $\mathrm{Gal}(\Omega/\mathbb{Q})$, es decir, todos los elementos de orden finito de $\mathrm{Gal}(\Omega/\mathbb{Q})$. Sea $\tilde{\mathbb{Q}} = \Omega^T$ el campo fijo de T. Entonces $\mathrm{Gal}(\tilde{\mathbb{Q}}/\mathbb{Q}) \cong \hat{\mathbb{Z}}$.*

Demostración. Se tiene

$$\mathrm{Gal}(\Omega/\mathbb{Q}) = \mathrm{Gal}\left(\varinjlim_n \mathbb{Q}(\zeta_n)/\mathbb{Q}\right) \cong \varprojlim_n \mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q}) \cong \varprojlim_n \left(\mathbb{Z}/n\mathbb{Z}\right)^* = \hat{\mathbb{Z}}^*.$$

Ahora, se tiene $\hat{\mathbb{Z}} \cong \prod_{p \text{ primo}} \mathbb{Z}_p$ y $\mathbb{Z}_p^* \cong \mathbb{Z}_p \times \mathbb{Z}/(p-1)\mathbb{Z}$ para $p \neq 2$ y $\mathbb{Z}_2^* \cong \mathbb{Z}_2 \times \mathbb{Z}/2\mathbb{Z}$. Por tanto

$$\mathrm{Gal}(\Omega/\mathbb{Q}) \cong \hat{\mathbb{Z}}^* \cong \hat{\mathbb{Z}} \times \hat{T}, \quad \text{donde} \quad \hat{T} \cong \prod_{p\neq 2} \mathbb{Z}/(p-1)\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}.$$

Por tanto el grupo de torsión T de $\mathrm{Gal}(\Omega/\mathbb{Q})$ es isomorfo al grupo de torsión $\hat{T}$. Se tiene que $\bigoplus_{p\neq 2} \mathbb{Z}/(p-1)\mathbb{Z} \bigoplus \mathbb{Z}/2\mathbb{Z} \subseteq \hat{T}$, y que la cerradura $\bar{T}$ de T es isomorfo a $\hat{T}$.

Se sigue que $\tilde{\mathbb{Q}} = \mathbb{Q}^T = \mathbb{Q}^{\bar{T}}$, $\mathrm{Gal}(\tilde{\mathbb{Q}}/\mathbb{Q}) \cong \mathrm{Gal}(\Omega/\mathbb{Q})/\bar{T} \cong \hat{\mathbb{Z}}$. □

Procediendo como en el caso de campos locales, fijemos un isomorfismo $\mathrm{Gal}(\tilde{\mathbb{Q}}/\mathbb{Q}) \cong \hat{\mathbb{Z}}$. En el caso de campos de funciones, consideremos $K_0 = \mathbb{F}_q(T)$ y para $n \in \mathbb{N}$, sea $k_n = K_0\mathbb{F}_{q^n}$ la extensión de constantes. Entonces si $R := \bigcup_{n=1}^{\infty} k_n$, se tiene

$$\begin{aligned}\mathrm{Gal}(R/K_0) &= \mathrm{Gal}\Big(\bigcup_{n=1}^{\infty} k_n/K_0\Big) \cong \mathrm{Gal}\Big(\varinjlim_n k_n/K_0\Big)\\ &\cong \varprojlim_n \mathrm{Gal}(k_n/K_0) \cong \varprojlim_n \mathbb{Z}/n\mathbb{Z} \cong \hat{\mathbb{Z}}.\end{aligned}$$

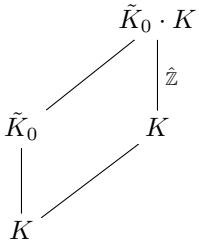
Para considerar ambos casos, sea $K_0 \in \{\mathbb{Q}, \mathbb{F}_q(T)\}$ y $\tilde{K}_0 \in \{\tilde{\mathbb{Q}}, R\}$. Tenemos un epimorfismo continuo

$$\mathrm{gr}_{K_0} : \mathrm{Gal}_{K_0^{\mathrm{sep}}} \longrightarrow \hat{\mathbb{Z}} \cong \mathrm{Gal}(\tilde{K}_0/K_0),$$

donde $G_{K_0^{\mathrm{sep}}} = \mathcal{G} = \mathrm{Gal}(K_0^{\mathrm{sep}}/K_0)$. Para K/K_0 una extensión finita y separable, sea $f_K := [K \cap \tilde{K}_0 : K_0]$ y obtenemos un epimorfismo

$$\mathrm{gr}_K := \frac{1}{f_K}\,\mathrm{gr}_{K_0} : G_K \longrightarrow \hat{\mathbb{Z}},$$

que determina la $\hat{\mathbb{Z}}$-extensión $\tilde{K} := K \cdot \tilde{K}_0$ de K.



Podemos llamar a $\tilde{K}/K$ la $\hat{\mathbb{Z}}$-extensión ciclotómica de K.

El elemento de $\mathrm{Gal}(\tilde{K}/K)$ que se mapea a $1 \in \hat{\mathbb{Z}}$ bajo el isomorfismo gr_K lo denotamos, como en el caso local, por Fr_K, el "*Frobenius*", esto es, $\mathrm{gr}_K(\mathrm{Fr}_K) = 1$ y por $\mathrm{Fr}_{L|K} = \mathrm{Fr}_K\,|_L$ en caso de que L/K es una subextensión finita de $\tilde{K}/K$. Este elemento $\mathrm{Fr}_{L|K}$ no debe confundirse con el automorfismo de Frobenius de primos de L.

Para el G_{K_0}-módulo A tomamos $C_\Omega = \bigcup_K C_K$ donde K recorre las extensiones finitas y separables de K_0 y se tiene $A_K = C_K$. Definimos el homomorfismo

$$v_K : J_K \longrightarrow \tilde{\mathbb{Z}}$$

como $v_K := \mathrm{gr}_K \circ [\_, \tilde{K}/K]$, $J_K \xrightarrow{[\_,\tilde{K}/K]} \mathrm{Gal}(\tilde{K}/K) \xrightarrow{\mathrm{gr}_K} \hat{\mathbb{Z}}$.

Teorema 6.7.23. *Para cada idèle principal $a \in K^*$, se tiene $[a, \tilde{K}/K] = 1$.*

Demostración. La prueba está contenida en la demostración del Teorema 6.6.31. □

Corolario 6.7.24. *El grado $v_K : J_K \longrightarrow \hat{\mathbb{Z}}$ induce $v_K : C_K \longrightarrow \hat{\mathbb{Z}}$.* □

Proposición 6.7.25. *El homomorfismo $v_K : C_K \longrightarrow \hat{\mathbb{Z}}$ es suprayectivo en el caso numérico y $v_K(C_K) = \mathbb{Z}$ en el caso de campos de funciones y es una* valuación henseliana *con respecto a gr_K, es decir*

(a) $v_K(C_\Omega) = \mathcal{Z} \supseteq \mathbb{Z}$ *y* $\mathcal{Z}/n\mathcal{Z} \cong \mathbb{Z}/n\mathbb{Z}$ *para toda* $n \in \mathbb{N}$.
(b) $v_K(\mathrm{N}_{L/K_0} C_L) = f_L\mathcal{Z}$ *para toda extensión finita y separable* L/K_0.

Demostración. Primero veamos que v_K es suprayectivo. Sea L/K una subextensión finita de $\tilde{K}/K$, entoces el mapeo

$$[\ , L/K] = \prod_{\mathfrak{p}} (\ , L_\mathfrak{p}/K_\mathfrak{p}) : J_K \longrightarrow G_{L|K}$$

es suprayectivo pues de hecho, debido a que $(\ , L_\mathfrak{p}/K_\mathfrak{p}) : K_\mathfrak{p}^* \longrightarrow \mathrm{Gal}(L_\mathfrak{p}/K_\mathfrak{p})$ es suprayectivo, $[J_K, L/K]$ contiene a todos los subgrupos de descomposición $\mathrm{Gal}(L_\mathfrak{p}/K_\mathfrak{p})$. Por tanto, todos los primos $\mathfrak{p}$ de K son totalmente descompuestos en el campo fijo M de $[J_K, L/K]$. Se sigue que $M = K$ (Corolario 6.5.2). Obtenemos que $[J_K, L/K] = \mathrm{Gal}(L/K)$.

Se sigue $[J_K, \tilde{K}/K] = [C_K, \tilde{K}/K]$ es denso en $\mathrm{Gal}(\tilde{K}/K)$.

En el caso numérico, $C_K \cong C_{K,0} \times \mathbb{R}^+$. Si $x \in \mathbb{R}^+$, entonces $[x, \tilde{K}/K]|_L = [x, L/K]$. Sea $[L : K] = n$. Existe $y \in \mathbb{R}^+$ con $y^n = x$ por lo que

$$[x, L/K] = [y^n, L/K] = [y, L/K]^n = 1,$$

por tanto $[x, \tilde{K}/K] = 1$ y $[\mathbb{R}^+, \tilde{K}/K] = 1$. Se sigue que $[C_K, \tilde{K}/K] = [C_{K,0}, \tilde{K}/K]$ es denso y como $C_{K,0}$ es compacto, se tiene que

$$[C_K, \tilde{K}/K] = [C_{K,0}, \tilde{K}/K] = \mathrm{Gal}(\tilde{K}/K),$$

por lo que $v_K = \mathrm{gr}_K \circ [\ , \tilde{K}/K]$ es suprayectiva en el caso numérico y denso en el caso de campos de funciones.

En el caso de campos de funciones, $\tilde{K}/K$ son las extensiones de constantes por lo que $(\alpha_\mathfrak{p}, \tilde{K}_\mathfrak{p}/K_\mathfrak{p}) = \mathrm{Fr}_{\tilde{K}_\mathfrak{p}|K_\mathfrak{p}}^{v_\mathfrak{p}(\alpha_\mathfrak{p})}$. Por tanto, $[C_K, \tilde{K}/K] = \langle \mathrm{Fr}_{K|K_0} \rangle \cong \mathbb{Z}$.

Ahora $v_K(C_K) = \begin{cases} \hat{\mathbb{Z}}, & \operatorname{car} K = 0, \\ \mathbb{Z}, & \operatorname{car} K = p \end{cases}$, por lo que se satisface (a) ($\mathcal{Z} = \hat{\mathbb{Z}}$ o $\mathbb{Z}$).

Para (b), se tiene que

$$\begin{aligned} v_K(\mathrm{N}_{L/K}\, C_L) &= v_K(\mathrm{N}_{L/K}\, J_L) = f_{L|K} \operatorname{gr}_L[J_L, \tilde{L}/L] \\ &= f_{L|K} v_L(C_L) = f_{L|K}\mathcal{Z}. \end{aligned}$$ □

Observación 6.7.26. Los grupos de clases de idèles C_K satisfacen el axioma de los campos de clase y se tiene que el par

$$(\operatorname{gr}_{K_0} : G_{K_0} \longrightarrow \hat{\mathbb{Z}}, \qquad v_{K_0} : C_{K_0} \longrightarrow \hat{\mathbb{Z}})$$

satisface todas las condiciones de teoría de campos de clase. Si K/K_0 es una extensión finita y separable, entonces por el Teorema 6.7.21 se tiene que el homomorfismo $v_K = \operatorname{gr}_K \circ [\ , \tilde{K}/K] : C_K \longrightarrow \hat{\mathbb{Z}}$ satisface

$$v_K = \frac{1}{f_K} \operatorname{gr} \circ [\ , \tilde{K}_0/K_0] \circ \mathrm{N}_{K/K_0} = \frac{1}{f_K} v_{K_0} \circ \mathrm{N}_{K/K_0},$$

que es precisamente el mapeo inducido por la valuación henseliana v_{K_0} en el sentido de la teoría de campos de clase locales.

Por tanto, hemos obtenido el teorema de reciprocidad global de Artin.

Teorema 6.7.27 (Ley global de reciprocidad de Artin). *Para toda extensión finita de Galois L/K de campos globales, tenemos un isomorfismo canónico (*isomorfismo global de Neukirch*):*

$$\mathfrak{N}_{L/K} : \operatorname{Gal}(L/K)^{\mathrm{ab}} \xrightarrow{\cong} C_K / \mathrm{N}_{L/K}\, C_L.$$ □

El invesrso de $\mathfrak{N}_{L/K}$ da un epimorfismo

$$(\ , L/K) : C_K \longrightarrow \operatorname{Gal}(L/K)^{\mathrm{ab}}$$

con núcleo $\mathrm{N}_{L/K}\, C_L$. El mapeo $(\ , L/K)$ es el símbolo de la norma residual global.

6.7.3. Teorema principal de la teoría de campos de clase globales

Regresamos a nuestra exposición principal. A continuación enunciamos el teorema principal de la teoría global de campos de funciones.

Teorema 6.7.28 (Teorema principal de la teoría global de campos de clase, TCCG). *Sea K un campo global. Entonces*

(1) *Existe un único homomorfismo continuo*

$$\rho_K = (\ ,K)\colon C_K \longrightarrow \mathrm{Gal}(K^{\mathrm{ab}}/K) \quad o$$
$$\rho_K = (\ ,L)\colon J_K \longrightarrow \mathrm{Gal}(K^{\mathrm{ab}}/K), \quad K^* \subseteq \mathrm{núc}\,\rho_K)$$

tal que para todo lugar $\mathfrak{p}$ *de* K *el siguiente diagrama es conmutativo:*

$$\begin{array}{ccc} K_{\mathfrak{p}}^* & \xrightarrow{\rho_{K_{\mathfrak{p}}}} & \mathrm{Gal}(K_{\mathfrak{p}}^{\mathrm{ab}}/K_{\mathfrak{p}}) \\ {\scriptstyle\theta}\downarrow & \circlearrowleft & \downarrow{\scriptstyle\mathrm{rest}} \\ C_K & \xrightarrow[\rho_K]{} & \mathrm{Gal}(K^{\mathrm{ab}}/K) \end{array}$$

donde

$$\theta = \pi \circ \lceil\ \rceil_{\mathfrak{p}}\colon K_{\mathfrak{p}}^* \xrightarrow{\lceil\ \rceil_{\mathfrak{p}}} J_K \xrightarrow{\pi} J_K/K^* = C_K,$$
$$x_{\mathfrak{p}} \mapsto (\ldots,1,1x_{\mathfrak{p}},1,1,\ldots) \mapsto (\ldots,1,1,x_{\mathfrak{p}},1,1,\ldots) \bmod K^*$$

y rest *es la restricción* $\sigma \longrightarrow \sigma|_{K^{\mathrm{ab}}}$.
El mapeo $\rho_K = (\ ,K)$ *se llama el* mapeo de reciprocidad.

(2) *Si* $K \subseteq E \subseteq L$ *con* L/K *una extensión abeliana finita, se tiene el siguiente diagrama conmutativo*

$$\begin{array}{ccc} C_E & \xrightarrow{\rho_E} & \mathrm{Gal}(L/E) \\ {\scriptstyle \mathrm{N}_{E/K}}\downarrow & & \downarrow{\scriptstyle\mu} \\ C_K & \xrightarrow[\rho_K]{} & \mathrm{Gal}(L/K) \end{array}$$

donde μ *es el encaje natural.*

(3) *Para cualquier extensión abeliana finita* L *de* K, ρ_K *induce un isomorfismo*

$$C_K/\,\mathrm{N}_{L/K}\,C_L \xrightarrow[\psi_{L/K}=(\ ,L/K)]{\cong} \mathrm{Gal}(L/K)$$
$$\uparrow{\scriptstyle Artin}$$

donde $\psi_{L/K} = (\ ,L/K)$ *es el mapeo de Artin o símbolo de la norma residual global:* $\psi_{L/K} = \tilde{\rho}_K\colon J_K \twoheadrightarrow \mathrm{Gal}(L/K)$, $\mathrm{núc}\,\psi_{L/K} = K^*\,\mathrm{N}_{L/K}\,J_L$ *y donde* $\mathrm{N}_{L/K}\colon C_L \longrightarrow C_K$ *es la norma inducida por la norma de los grupos de idèles:*

$$\vec{y} = (y_{\mathfrak{P}})_{\mathfrak{P}\in\mathbb{P}_L} \in J_L \xrightarrow{\mathrm{N}_{L/K}} \Big(\prod_{\mathfrak{P}|\mathfrak{p}} \mathrm{N}_{L_{\mathfrak{P}}/K_{\mathfrak{p}}}\, y_{\mathfrak{P}}\Big)_{\mathfrak{p}\in\mathbb{P}_K} \in J_K.$$

Esto es, si $\vec{\alpha} \bmod L^* \in C_L$, *entonces se define* $\mathrm{N}_{L/K}(\vec{\alpha} \bmod L^*) = \mathrm{N}_{L/K}(\vec{\alpha}) \bmod K^*$ *y se tiene* $\mathrm{N}_{L/K}(C_L) = \mathrm{N}_{L/K}(J_L)K^*/K^*$.
Además $\mathrm{N}_{L/K}$ *es una función abierta.*

(4) $H \longrightarrow \rho_K^{-1}(H)$ *es una biyección entre el conjunto de todos los subgrupos abiertos de* $\mathrm{Gal}(K^{\mathrm{ab}}/K)$ *y el conjunto de todos los subgrupos abiertos de índice finito de* C_K*. En particular* ρ_K *es una función densa.*

(5) = (4) **Teorema de Existencia** *Para cada subgrupo abierto* H *de índice finito en* C_K*, existe una única extensión abeliana finita* L/K *tal que* $\mathrm{N}_{L/K}\, C_L = H$*.*

(6) *Si* L/K *es una extensión abeliana finita y* S *es el conjunto de lugares ramificados en* L/K *más los primos infinitos, entonces para* $\vec{x} \in J_K$*, sea* $(\vec{x})^S := \prod_{\mathfrak{p}\notin S} \mathfrak{p}^{v_{\mathfrak{p}}(x_{\mathfrak{p}})} \in D_K^S$ *el grupo de los divisores (o ideales fraccionarios) primos relativos a* S*, es decir,* $D_K^S = D_K/\langle S\rangle$*, entonces* $\tilde{\rho}_K(\vec{x}) = \psi_{L/K}((\vec{x})^S)$*, donde* $\psi_{L/K}$ *es el mapeo de Artin, para* $\vec{x} \in J_K^S := \{\vec{y} \in J_K \mid y_{\mathfrak{q}} = 1 \text{ para } \mathfrak{q} \in S\}$ *(es decir,* ρ_K *evaluado en idèles con componente* 1 *en los primos ramificados y en los primos infinitos, coincide con el mapeo usual de Artin (o símbolo de Artin)) en ideales. Más precisamente, se tiene*

$$\tilde{\rho}(\vec{x}) = \psi_{L/K}((\vec{x})^S) = \psi_{L/K}\Big(\prod_{\mathfrak{p}\notin S} \mathfrak{p}^{v_{\mathfrak{p}}(x_{\mathfrak{p}})}\Big) = \prod_{\mathfrak{p}\notin S} \left(\frac{L/K}{\mathfrak{p}}\right)^{v_{\mathfrak{p}}(x_{\mathfrak{p}})}. \quad \square$$

Como corolario, se tiene

Corolario 6.7.29. *Sea* K *un campo global. Entonces existe una correspondencia biyectiva*

$$\{\textit{extensiones abelianas finitas de } K\} \longleftrightarrow \{\textit{subgrupos abiertos de índice finito de } C_K\}$$

donde la correspondencia está dada por $L \longrightarrow \mathrm{N}_{L/K}\, C_L \subseteq C_K$*. Si* $L \longleftrightarrow H$*, entonces* $[L : K] = [C_K : H]$ *y si* $L' \longleftrightarrow H'$*, entonces* $L \supseteq L' \iff H \subseteq H'$*.* $\square$

Teorema 6.7.30. *Sea* K *un campo global y sea* H *un subgrupo de* C_K*. Si* H *contiene a un grupo de normas, entonces* H *mismo es un grupo de normas.*

Demostración. Sea L/K una extensión abeliana finita tal que $\mathrm{N}_{L/K}\, C_L \subseteq H$. Entonces $H = \bigcup_{\text{finita}} x\, \mathrm{N}_{L/K}\, C_L$ y como $\mathrm{N}_{L/K}\, C_L$ es abierto, H es abierto. Sea $\psi_{L/K}$ el isomorfismo de Artin

$$\psi_{L/K} : C_K/\,\mathrm{N}_{L/K}\, C_L \longrightarrow \mathrm{Gal}(L/K).$$

Sea $\psi_{L/K}\big(H/\,\mathrm{N}_{L/K}\, C_L\big) = \mathrm{Gal}(L/M)$. Por tanto

$$\tilde{\psi}_{L/K} : C_K/H \cong \frac{C_K/\,\mathrm{N}_{L/K}\, C_L}{H/\,\mathrm{N}_{L/K}\, C_L} \longrightarrow \frac{\mathrm{Gal}(L/K)}{\mathrm{Gal}(L/M)} \cong \mathrm{Gal}(M/K).$$

Por tanto $\tilde{\psi}_{L/K} = \psi_{M/K} : C_K/\,\mathrm{N}_{M/K}\, C_M \longrightarrow \mathrm{Gal}(M/K)$ es el isomorfismo de Artin y $H = \mathrm{N}_{M/K}\, C_M$ es un grupo de normas. $\square$

Definición 6.7.31. Si $H = \mathrm{N}_{L/K} C_L$, donde L/K es una extensión abeliana finita de campos globales, se dice que L es el *campo de clase asociado a* H

Veamos la versión global de la correspondencia $L \longleftrightarrow \mathrm{N}_{L/K} C_L$.

Teorema 6.7.32. *Sea K un campo global. Para una extensión abeliana finita L/K, denotamos $\mathcal{N}_L = \mathrm{N}_{L/K} C_L$.*

Sean L_1, L_2 dos extensiones abelianas finitas de K. Entonces

(1) $L_1 \subseteq L_2 \iff \mathcal{N}_{L_1} \supseteq \mathcal{N}_{L_2}$.
(2) $\mathcal{N}_{L_1 L_2} = \mathcal{N}_{L_1} \cap \mathcal{N}_{L_2}$
(3) $\mathcal{N}_{L_1 \cap L_2} = \mathcal{N}_{L_1} \mathcal{N}_{L_2}$.

Demostración. (1) $\Longrightarrow$) Si $L_1 \subseteq L_2$, entonces

$$\mathcal{N}_{L_2} = \mathrm{N}_{L_2/K} C_{L_2} = \mathrm{N}_{L_1/K} \mathrm{N}_{L_2/L_1} C_{L_2} \subseteq \mathrm{N}_{L_1/K} C_{L_1} = \mathcal{N}_{L_1}.$$

(2) Se tiene para $i = 1, 2$, $L_i \subseteq L_1 L_2$. Por la parte (1), $\mathcal{N}_{L_1 L_2} \subseteq \mathcal{N}_{L_1} \cap \mathcal{N}_{L_2}$.

Recíprocamente, si $\tilde{\vec{\alpha}} \in \mathcal{N}_{L_1} \cap \mathcal{N}_{L_2}$ se tiene que

$$\psi_{L_i/K}(\tilde{\vec{\alpha}}) = (\tilde{\vec{\alpha}}, L_i/K) = \mathrm{rest}_{L_i} \circ \rho_K(\tilde{\vec{\alpha}}) \in \mathrm{Gal}(L_i/K) \cong C_K/\mathcal{N}_{L_i}.$$

Por tanto $\psi_{L_i/K}(\vec{\alpha}) = 1$, $i = 1, 2$. Se tiene el monomorfismo

$$\theta\colon \mathrm{Gal}(L_1 L_2/K) \hookrightarrow \mathrm{Gal}(L_1/K) \times \mathrm{Gal}(L_2/K), \quad \sigma \longmapsto (\sigma|_{L_1}, \sigma|_{L_2}).$$

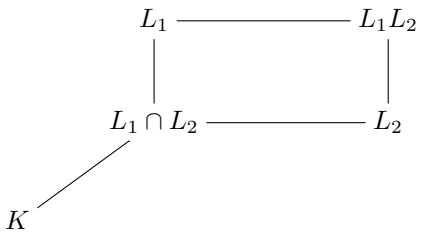
Sea

$$\sigma = (\tilde{\vec{\alpha}}, L_1 L_2/K) \xrightarrow{\theta} (\sigma|_{L_1}, \sigma|_{L_2}) = (\psi_{L_1/K}(\tilde{\vec{\alpha}}), \psi_{L_2/K}(\tilde{\vec{\alpha}})) = (1, 1)$$

por lo que $\psi_{L_1 L_2/K}(\tilde{\vec{\alpha}}) = 1$. Se sigue que $\tilde{\vec{\alpha}} \in \mathcal{N}_{L_1 L_2}$ lo cual implica que $\mathcal{N}_{L_1} \cap \mathcal{N}_{L_2} \subseteq \mathcal{N}_{L_1 L_2}$ y por tanto $\mathcal{N}_{L_1} \cap \mathcal{N}_{L_2} = \mathcal{N}_{L_1 L_2}$.
(1) $\Longleftarrow$) Sea ahora $\mathcal{N}_{L_2} \subseteq \mathcal{N}_{L_1}$. Entonces $\mathcal{N}_{L_1} \cap \mathcal{N}_{L_2} = \mathcal{N}_{L_1 L_2} = \mathcal{N}_{L_2}$. Por tanto

$$[L_1 L_2 : K] = |C_K/\mathcal{N}_{L_1 L_2}| = |C_K/\mathcal{N}_{L_2}| = [L_2 : K].$$

Se sigue que $L_1 L_2 = L_2$ de donde se sigue que $L_1 \subseteq L_2$.
(3) Se tiene que $L_1 \cap L_2 \subseteq L_i$, $i = 1, 2$. Por tanto $\mathcal{N}_{L_i} \subseteq \mathcal{N}_{L_1 \cap L_2}$, $i = 1, 2$. Se sigue que $\mathcal{N}_{L_1} \mathcal{N}_{L_2} \subseteq \mathcal{N}_{L_1 \cap L_2}$.



Ahora bien, $\mathcal{N}_{L_i} \subseteq \mathcal{N}_{L_1}\mathcal{N}_{L_2} =: H$, $i = 1, 2$, donde H es un subgrupo de índice finito en C_K pues $H = \bigcup_{\text{finito}} \mathcal{N}_{L_i} x$.

Sea T el campo que corresponde a H. Entonces $T \subseteq L_1$ y $T \subseteq L_2$ por lo que $T \subseteq L_1 \cap L_2$ lo cual implica $\mathcal{N}_{L_1 \cap L_2} \subseteq \mathrm{N}_{T/K} C_T = H = \mathcal{N}_{L_1}\mathcal{N}_{L_2}$ con lo cual se sigue que $\mathcal{N}_{L_1 \cap L_2} = \mathcal{N}_{L_1}\mathcal{N}_{L_2}$. □

Teorema 6.7.33 (Hasse). *Sea L/K una extensión abeliana finita de campos globales. Entonces, para $\vec{\alpha} \in J_L$, $\tilde{\vec{\alpha}} \in C_L = J_L/L^*$ se tiene*

$$[\vec{\alpha}, L/K] = (\vec{\alpha}, L/K) = \prod_{\mathfrak{p}} (\alpha_{\mathfrak{p}}, L_{\mathfrak{p}}/K_{\mathfrak{p}}) \quad y$$

$$[\tilde{\vec{\alpha}}, L/K] = (\tilde{\vec{\alpha}}, L/K) = \psi_{L/K}(\tilde{\vec{\alpha}}) = \prod_{\mathfrak{p}} (\alpha_{\mathfrak{p}}, L_{\mathfrak{p}}/K_{\mathfrak{p}}).$$

Demostración. Puesto que $(\ , L/K)$ es el símbolo de la norma residual, aplicamos la Proposición 5.2.1, que fue demostrada para campos locales, pero como hicimos notar, vale para cualquier formación de clase, y se tiene que si $\tilde{\vec{\alpha}} := \tilde{\vec{\alpha}}\, \mathrm{N}_{L/K} C_L \in H^0(L|K)$, entonces para todo caracter $\mu \in \chi(G_{L|K}) = H^1(G_{L|K}, \mathbb{Q}/\mathbb{Z})$, se tiene

$$\mu\big((\tilde{\vec{\alpha}}, L/K)\big) = \mathrm{inv}_{L|K}\left((\tilde{\vec{\alpha}}) \cup \delta\mu\right).$$

Por otro lado, por la Proposición 6.6.30, se tiene

$$\mu\big([\vec{\alpha}, L/K)]\big) = \mathrm{inv}_{L|K}\left((\vec{\alpha}) \cup \delta\mu\right),$$

donde $(\vec{\alpha}) := \vec{\alpha}\, \mathrm{N}_{L/K} J_L \in H^0(G_{L|K}, J_L)$. El homomorfismo

$$H^q(G_{L|K}, J_L) \xrightarrow{\tilde{\pi}} H^q(G_{L|K}, C_L)$$

mapea $(\vec{\alpha}) \in H^q(G_{L|K}, J_L)$ a $\tilde{\vec{\alpha}} \in H^0(G_{L|K}, C_L)$, y por tanto mapea $(\vec{\alpha}) \cup \delta\mu \in H^2(G_{L|K}, J_L)$ a $(\tilde{\vec{\alpha}}) \cup \delta\mu \in H^2(G_{L|K}, C_L) = H^2(L|K)$.

Por tanto $\tilde{\pi}\big((\tilde{\vec{\alpha}}) \cup \delta\mu\big) = (\tilde{\vec{\alpha}}) \cup \delta\mu$.

Por el Teorema 6.7.7, obtenemos

$$\mu\big((\tilde{\vec{\alpha}}, L/K)\big) = \mathrm{inv}_{L|K}\left((\vec{\alpha}) \cup \delta\mu\right) = \mathrm{inv}_{L|K}\left((\vec{\alpha}) \cup \delta\mu\right) = \mu\big([\vec{\alpha}, L/K]\big),$$

y puesto que esto es para todo caracter $\mu \in \chi(G_{L|K})$, se sigue que

$$\big(\tilde{\vec{\alpha}}, L/K\big) = [\vec{\alpha}, L/K] = \prod_{\mathfrak{p}} (\alpha_{\mathfrak{p}}, L_{\mathfrak{p}}/K_{\mathfrak{p}}).$$ □

El teorema de Hasse provee de varios resultados de gran importancia para la teoría global de campos de clase.

Corolario 6.7.34. *Sea K un campo global. Para $\alpha_{\mathfrak{p}} \in K_{\mathfrak{p}}^*$, sea $\lceil \alpha_{\mathfrak{p}} \rceil_{\mathfrak{p}} = (\ldots, 1, 1, \alpha_{\mathfrak{p}}, 1, 1, \ldots)$ el idèle cuya $\mathfrak{p}$-componente es $\alpha_{\mathfrak{p}}$ y las demás componentes son 1. Entonces $\big(\lceil \alpha_{\mathfrak{p}} \rceil_{\mathfrak{p}}, L/K\big) = (\alpha_{\mathfrak{p}}, L_{\mathfrak{p}}/K_{\mathfrak{p}})$.*

En particular el diagrama

$$\begin{array}{ccc} K_{\mathfrak{p}}^* & \xrightarrow{(\ ,L_{\mathfrak{p}}/K_{\mathfrak{p}})} & \mathrm{Gal}(L_{\mathfrak{p}}/K_{\mathfrak{p}}) \\ {\scriptstyle \lceil\ \rceil_{\mathfrak{p}}}\downarrow & & \downarrow{\scriptstyle \iota} \\ C_K & \xrightarrow[(\ ,L/K)]{} & \mathrm{Gal}(L/K) \end{array}$$

donde ι es el encaje natural, es conmutativo. Pasando al límite, se tiene que

$$\begin{array}{ccc} K_{\mathfrak{p}}^* & \xrightarrow{\rho_{K_{\mathfrak{p}}}} & \mathrm{Gal}(K_{\mathfrak{p}}^{\mathrm{ab}}/K_{\mathfrak{p}}) \\ {\scriptstyle \pi \circ \lceil\ \rceil_{\mathfrak{p}}}\downarrow & & \downarrow{\scriptstyle \iota} \\ C_K & \xrightarrow[\rho_K]{} & \mathrm{Gal}(K^{\mathrm{ab}}/K) \end{array}$$

es un diagrama conmutativo. Esto es el contenido de (1) *del Teorema* 6.7.28.

Demostración. Se tiene

$$\big(\lceil \alpha_{\mathfrak{p}} \rceil_{\mathfrak{p}}, L/K\big) = \prod_{\mathfrak{q}} \Big(\big(\lceil \alpha_{\mathfrak{p}} \rceil_{\mathfrak{p}}\big)_{\mathfrak{q}}, L_{\mathfrak{q}}/K_{\mathfrak{q}}\Big) = (\alpha_{\mathfrak{p}}, L_{\mathfrak{p}}/K_{\mathfrak{p}}). \qquad \square$$

Corolario 6.7.35. *Sea L/K una extensión abeliana finita de campos globales. Para $\vec{\alpha} \in J_K$, si S es el conjunto es el conjunto de los primos de K ramificados en L y de los primos infinitos, se tiene que*

$$\tilde{\rho}_K(\vec{\alpha}) = \psi_{L/K}\big((\vec{\alpha})^S\big) = \psi_{L/K}\Big(\prod_{\mathfrak{p} \notin S} \mathfrak{p}^{v_{\mathfrak{p}}(\alpha_{\mathfrak{p}})}\Big) = \prod_{\mathfrak{p} \notin S} \left(\frac{L|K}{\mathfrak{p}}\right)^{v_{\mathfrak{p}}(\alpha_{\mathfrak{p}})}.$$

Este es el contenido de (6) *del Teorema* 6.7.28.

Demostración. Es inmediato del hecho de que $\left(\frac{L|K}{\mathfrak{p}}\right) = \varphi_{\mathfrak{p}} = (\pi_{\mathfrak{p}}, L_{\mathfrak{p}}/K_{\mathfrak{p}})$ donde $\mathfrak{p}$ es no ramificado ni infinito, $\varphi_{\mathfrak{p}}$ es el Frobenis y $\pi_{\mathfrak{p}}$ es un elemento primo en $\mathfrak{p}$. $\square$

Corolario 6.7.36. *Si $x \in K^*$ es un idèle principal de un campo global, entonces $(x, L/K) = 1$.*

Demostración. Se tiene $(x, L/K) = [x, L/K] = 1$. $\square$

Corolario 6.7.37. *Sea L/K una extensión abeliana finita de campos globales. Entonces*

$$\mathrm{N}_{L/K}\, C_L \cap K_{\mathfrak{p}}^* = \mathrm{N}_{L_{\mathfrak{p}}/K_{\mathfrak{p}}}\, L_{\mathfrak{p}}^*,$$

donde consideramos $K_{\mathfrak{p}}^* \subseteq C_K$ bajo el monomorfismo $K_{\mathfrak{p}}^* \overset{\lceil\ \rceil_{\mathfrak{p}}}{\hookrightarrow} J_K \overset{\pi}{\to} J_K/K^* = C_K$.

En particular, las extensiones locales derivadas de una extensión global, corresponden a las componentes locales del grupo de normas global.

Demostración. Si $\alpha_{\mathfrak{p}} \in \mathrm{N}_{L_{\mathfrak{p}}/K_{\mathfrak{p}}}\, L_{\mathfrak{p}}^*$ entonces $\big(\lceil\alpha_{\mathfrak{p}}\rceil_{\mathfrak{p}}, L/K\big) = (\alpha_{\mathfrak{p}}, L_{\mathfrak{p}}/K_{\mathfrak{p}}) = 1$ por lo que $\lceil\alpha_{\mathfrak{p}}\rceil_{\mathfrak{p}} \in \mathrm{N}_{L/K}\, C_L$, esto es, $\mathrm{N}_{L_{\mathfrak{p}}/K_{\mathfrak{p}}}\, L_{\mathfrak{p}}^* \subseteq \mathrm{N}_{L/K}\, C_L$ y obviamente $\mathrm{N}_{L_{\mathfrak{p}}/K_{\mathfrak{p}}}\, L_{\mathfrak{p}}^* \subseteq K_{\mathfrak{p}}^*$ por lo que $\mathrm{N}_{L_{\mathfrak{p}}/K_{\mathfrak{p}}}\, L_{\mathfrak{p}}^* \subseteq \mathrm{N}_{L/K}\, C_L \cap K_{\mathfrak{p}}^*$.

Recíprocamente, sea $\tilde{\vec{\alpha}} \in \mathrm{N}_{L/K}\, C_L \cap K_{\mathfrak{p}}^*$. Entonces $\tilde{\vec{\alpha}}$ está representado por un idèle $\vec{\alpha} = \mathrm{N}_{L/K}\, \vec{\beta}$ con $\vec{\beta} \in J_L$ y también por un idèle $\lceil a_{\mathfrak{p}}\rceil_{\mathfrak{p}}$, $a_{\mathfrak{p}} \in K_{\mathfrak{p}}^*$. Por tanto existe $x \in K^*$ tal que $\lceil a_{\mathfrak{p}}\rceil_{\mathfrak{p}} \cdot x = \mathrm{N}_{L/K}\, \vec{\beta}$. Para cualquier $\mathfrak{q} \neq \mathfrak{q}$, x es una norma de $L_{\mathfrak{q}}/K_{\mathfrak{q}}$ pues si $\mathfrak{Q}$ y $\mathfrak{Q}'$ son primos en L sobre $\mathfrak{q}$, entonces $\mathrm{N}_{L_{\mathfrak{Q}}/K_{\mathfrak{q}}}\, L_{\mathfrak{Q}}^* = \mathrm{N}_{L_{\mathfrak{Q}'}/K_{\mathfrak{q}}}\, L_{\mathfrak{Q}'}^*$ por lo que $x \in \prod_{\mathfrak{Q}|\mathfrak{q}} \mathrm{N}_{L_{\mathfrak{Q}}/K_{\mathfrak{q}}}\, L_{\mathfrak{Q}}^* = \mathrm{N}_{L_{\mathfrak{q}}/K_{\mathfrak{q}}}\, L_{\mathfrak{q}}^*$. Puesto que

$$(x, L/K) = \prod_{\mathfrak{q}} (x, L_{\mathfrak{q}}/K_{\mathfrak{q}}) = (x, L_{\mathfrak{p}}/K_{\mathfrak{p}}) = 1,$$

se sigue que x es una norma de $L_{\mathfrak{p}}/K_{\mathfrak{p}}$. Puesto que $\lceil a_{\mathfrak{p}}\rceil_{\mathfrak{p}} \cdot x$ es norma de un idèle, por el Teorema 6.3.9, $\lceil a_{\mathfrak{p}}\rceil_{\mathfrak{p}} x$ es norma local para toda completación $L_{\mathfrak{p}}/K_{\mathfrak{p}}$. Se sigue que $\lceil a_{\mathfrak{p}}\rceil_{\mathfrak{p}} \in \mathrm{N}_{L_{\mathfrak{p}}/K_{\mathfrak{p}}}\, L_{\mathfrak{p}}^*$, por tanto, $\tilde{\vec{\alpha}} = \lceil a_{\mathfrak{p}}\rceil_{\mathfrak{p}} \in \mathrm{N}_{L_{\mathfrak{p}}/K_{\mathfrak{p}}}\, L_{\mathfrak{p}}^*$ probando que $\mathrm{N}_{L/K}\, C_L \cap K_{\mathfrak{p}}^* \subseteq \mathrm{N}_{L_{\mathfrak{p}}/K_{\mathfrak{p}}}\, L_{\mathfrak{p}}^*$. □

Corolario 6.7.38. *Sea L/K una extensión abeliana finita de campos globales. Entonces $\mathrm{N}_{L/K}\, C_L$ es cerrado en C_K y por tanto es abierto.*

Demostración. Sea $\tilde{\vec{\alpha}} \notin \mathrm{N}_{L/K}\, C_L$. Por tanto existe $\mathfrak{p} \in \mathbb{P}_K$ tal que $\alpha_{\mathfrak{p}} \notin \mathrm{N}_{L_{\mathfrak{p}}/K_{\mathfrak{p}}}\, L_{\mathfrak{p}}^*$ pues $\mathrm{N}_{L/K}\, C_L \cap K_{\mathfrak{p}}^* = \mathrm{N}_{L_{\mathfrak{p}}/K_{\mathfrak{p}}}\, L_{\mathfrak{p}}^*$. Como $\mathrm{N}_{L_{\mathfrak{p}}/K_{\mathfrak{p}}}\, L_{\mathfrak{p}}^*$ es cerrado, existe U conjunto abierto de $K_{\mathfrak{p}}^*$ tal que $\alpha_{\mathfrak{p}} \in U$ y $U \cap \mathrm{N}_{L_{\mathfrak{p}}/K_{\mathfrak{p}}}\, L_{\mathfrak{p}}^* = \emptyset$.

Sea W cualquier abierto de C_K con $\tilde{\vec{\alpha}} \in W$ de la forma $W = U \times \prod_{\mathfrak{q}\neq\mathfrak{p}} V_{\mathfrak{q}}$. Entonces $\mathrm{N}_{L/K}\, C_K \cap W = \emptyset$ pues $\mathrm{N}_{L_{\mathfrak{p}}/K_{\mathfrak{p}}}\, L_{\mathfrak{p}}^* \cap U = \emptyset$. Se sigue que $\mathrm{N}_{L/K}\, C_L$ es cerrado en C_K. □

Podemos usar límites y obtener el *símbolo universal de la norma residual*. Para un campo global K y una extensión abeliana finita, tenemos el homomorfismo $C_K \xrightarrow{(\ ,L/K)} \mathrm{Gal}(L/K)$. Se tiene $\bigcup_{\substack{L \text{ abeliana} \\ \text{finita de } K}} L = K^{\mathrm{ab}}$ es la máxima extensión abeliana de K. Se tiene

$$G_K^{\mathrm{ab}} = \mathrm{Gal}(K^{\mathrm{ab}}/K) = \mathrm{Gal}(\varinjlim_{L} L/K) \cong \varprojlim_{L} \mathrm{Gal}(L/K)$$

donde L recorre todas las extensiones abelianas finitas de K.

Para $\tilde{\tilde{\alpha}} \in C_K$, obtenemos

$$\left(\tilde{\tilde{\alpha}}, K\right) := \varprojlim_{L} \left(\tilde{\tilde{\alpha}}, L/K\right) \in G_K^{\mathrm{ab}}$$

formado por los elementos compatibles $\left\{\left(\tilde{\tilde{\alpha}}, L/K\right) \in G_{L|K}\right\}_L$. Por tanto obtenemos

$$C_K \xrightarrow{(\ \ ,K)} G_K^{\mathrm{ab}}$$

y el núcleo de $(\ ,K)$ es $\bigcap_{\substack{L/K \text{ abeliana} \\ \text{finita}}} \mathrm{N}_{L/K} C_L = \mathfrak{N}_K = \text{núc}(\_, K)$ y la imagen es densa en G_K^{ab}. De hecho, se tiene que $(\ \ ,K)$ es suprayectivo en el caso numérico y $\mathfrak{N}_K$ es la componente conexa de $\tilde{\tilde{1}} \in C_K$. En el caso de campos de funciones, $\mathfrak{N}_K = \{1\}$, es decir $(\ ,K)$ es inyectiva pero no suprayectiva. Esto lo veremos más adelante.

En el caso local tenemos $K_{\mathfrak{p}}^* \xrightarrow{(\ ,K_{\mathfrak{p}})} G_{K_{\mathfrak{p}}}^{\mathrm{ab}} \subseteq G_K^{\mathrm{ab}}$, donde $(\ ,K_{\mathfrak{p}})$ es el símbolo universal de la norma residual local y pasando a los límites, obtenemos para $\tilde{\tilde{\alpha}} \in C_K$, $\left(\tilde{\tilde{\alpha}}, K\right) = \prod_{\mathfrak{p}} (\alpha_{\mathfrak{p}}, K_{\mathfrak{p}})$.

Teorema 6.7.39. *Sea K un campo global. El símbolo universal de la norma residual $\rho_K : C_K \longrightarrow G_K^{\mathrm{ab}} = \mathrm{Gal}(K^{\mathrm{ab}}/K)$ es un mapeo continuo. Este es el contenido de* (1) *del Teorema* 6.7.28.

Demostración. Sea U una vecindad abierta de $1 \in G_K^{\mathrm{ab}}$, esto es, U es un subgrupo abierto de G_K^{ab} de índice finito. Sea L el campo fijo de U: $L = (K^{\mathrm{ab}})^U$, L/K es una extensión abeliana finita. Sea $\vec{\alpha} \in J_K$. Si $\mathfrak{p} \in \mathbb{P}_K$ es no ramificado en L y $\alpha_{\mathfrak{p}}$ es una unidad, $(\alpha_{\mathfrak{p}}, L_{\mathfrak{p}}/K_{\mathfrak{p}}) = 1$. Por tanto, si $\mathfrak{p}$ es no ramificado, $(U_{\mathfrak{p}}, K) \subseteq U$. Ahora, si $\mathfrak{p} \in \mathbb{P}_K$ es ramificado, se sigue de la teoría local, Teorema 5.3.16, que existe una vecindad $V_{\mathfrak{p}}$ de $1 \in K_{\mathfrak{p}}^*$ tal que $(V_{\mathfrak{p}}, L_{\mathfrak{p}}/K_{\mathfrak{p}}) = 1$. De esta forma obtenemos que $(V_{\mathfrak{p}}, K) \subseteq U$.

Sea $V = \prod_{\substack{\mathfrak{p} \text{ no} \\ \text{ramificado}}} U_{\mathfrak{p}} \times \prod_{\substack{\mathfrak{p} \\ \text{ramificado}}} V_{\mathfrak{p}}$, entonces V es una vecindad abierta de $\vec{1} \in J_K$ y $(V, K) \subseteq U$. Puesto que C_K tiene la topología cociente y $(K^*, K) = 1$, se sigue la continuidad. □

6.8. Teorema de existencia

Hemos obtenido una biyección entre las extensiones abelianas finitas de K, K un campo global, y los grupos de normas de C_K. El teorema de existencia, nos caracteriza estos grupos.

Recordemos las estructuras topológicas que hemos obtenido:

- J_K es un grupo Hausdorff localmente compacto (Proposición 6.2.10).
- C_K es un grupo Hausdorff localmente compacto (Proposición 6.2.10).

- K^* es discreto y por tanto cerrado en J_K (Proposición 6.2.15).
- $C_{K,0}$ es cerrado en C_K para K global. Si K es de funciones, $C_{K,0}$ también es abierto en C_K (Proposición 6.2.13).
- $C_{K,0}$ es compacto (Teorema 6.2.27).
- El epimorfismo canónico $J_K \longrightarrow C_K$ es continuo y manda conjuntos abiertos en conjuntos abiertos.
- $\lceil\ \rceil_{\mathfrak{p}} : K_{\mathfrak{p}}^* \longrightarrow C_K$ es un monomorfismo continuo.
- Si K es de funciones, C_K y $C_{K,0}$ son totalmente disconexos (Corolario 6.2.11).

Ahora veamos con más detalle los mapeos norma y grado en campos globales. Ver Definicion 6.2.7 para las propiedades fundamentales de estos mapeos.

Sea $\|\ \| : J_K \longrightarrow \mathbb{R}^+$ el mapeo norma

$$\|\vec{\alpha}\| = \prod_{\mathfrak{p}\in\mathbb{P}_K} |\alpha_{\mathfrak{p}}|_{\mathfrak{p}},$$

con todos los valores absolutos $|\ |_{\mathfrak{p}}$ normalizados. Notemos que la imagen de $\|\ \|$ es $\mathbb{R}^+$ en el caso numérico y $\{q^n \mid n \in \mathbb{Z}\}$ en el caso de campos de funciones, donde $\mathbb{F}_q$ es el campo de constantes de K. Esto se debe al Teorema de Schmidt, Teorema 6.5.6, que establece la existencia de un divisor de grado 1, como detallamos un poco más adelante.

Ahora bien, $\{q^n \mid n \in \mathbb{Z}\} \xrightarrow[\log_q]{\cong} \mathbb{Z}$ es un isomorfismo de grupos y de espacios topológicos, ambos con la topología discreta.

Para K un campo de funciones, la función grado gr es simplemente $\operatorname{gr} := \log_q \circ \|\ \|$, esto es,

$$\operatorname{gr} : J_L \longrightarrow \mathbb{Z}, \quad \operatorname{gr}\vec{\alpha} = \log_q(\|\vec{\alpha}\|) = \sum_{\mathfrak{p}} \operatorname{gr}\alpha_{\mathfrak{p}} = \sum_{\mathfrak{p}} \operatorname{gr}\mathfrak{p}\cdot v_{\mathfrak{p}}(\alpha_{\mathfrak{p}}).$$

Se tiene que $\operatorname{núc}\|\ \| = \operatorname{núc}\operatorname{gr} = J_{K,0}$.

Recordemos que tanto $\|\ \|$ como gr son funciones continuas. Puesto que $\|x\| = 1$ para $x \in K^*$ (y además $\operatorname{gr} x = 0$ si K es campo de funciones), se tienen los mapeos inducidos

$$\begin{aligned} \|\ \| : C_K &\longrightarrow \mathbb{R}^+, \quad K \text{ un campo global,} \\ \operatorname{gr} : C_K &\longrightarrow \mathbb{Z}, \quad K \text{ un campo de funciones,} \end{aligned}$$

y $\operatorname{núc}\|\ \| = \operatorname{núc}\operatorname{gr} = C_{K,0}$. Notemos que, por el Teorema de Schmidt, Teorema 6.5.6, que gr es suprayectiva.

Las sucesiones exactas de homomorfismos continuos

$$\begin{aligned} 1 \longrightarrow J_{K,0} &\xhookrightarrow{\imath} J_K \xrightarrow{\|\ \|} \Lambda \longrightarrow 1, \\ 1 \longrightarrow J_{K,0} &\xhookrightarrow{\imath} J_K \xrightarrow{\operatorname{gr}} \Lambda \longrightarrow 1, \\ 1 \longrightarrow C_{K,0} &\xhookrightarrow{\jmath} C_K \xrightarrow{\|\ \|} \Lambda \longrightarrow 1, \\ 1 \longrightarrow C_{K,0} &\xhookrightarrow{\jmath} C_K \xrightarrow{\operatorname{gr}} \Lambda \longrightarrow 1, \end{aligned}$$

donde $\Lambda = \begin{cases} \mathbb{R}^+ & \text{si } K \text{ es numérico,} \\ \mathbb{Z} & \text{si } K \text{ es campo de funciones,} \end{cases}$ y gr está definido únicamente si K es campo de funciones, se escinden. Más precisamente, primero consideremos K campo numérico, $\Lambda = \mathbb{R}^+$. Sea $\mathfrak{p}$ un lugar infinito de K y consideremos $\mathbb{R}^+ \subseteq K_\mathfrak{p}$. Sea $\varphi : \mathbb{R}^+ \longrightarrow J_K$ o C_K donde $\varphi(x) = (\ldots, 1, 1, x, 1, 1, \ldots)$ es el idèle o la clase de idèle, donde la entrada en $\mathfrak{p}$ es x y las demás entradas son 1. Entonces φ es continuo, donde consideramos a $\mathbb{R}^+$ con la topología inducida por la topología usual de $\mathbb{R}$ y se tiene $\| \ \| \circ \varphi = \mathrm{Id}_{\mathbb{R}^+}$. También, sea $\psi : J_K \longrightarrow J_{K,0}$ (o $\psi : C_K \longrightarrow C_{K,0}$), donde $\psi(\vec{\alpha})$ es el idèle donde todas las entradas $\mathfrak{q}$ distintas de $\mathfrak{p}$ son $\alpha_\mathfrak{q}$ y su entrada en $\mathfrak{p}$ es $\frac{\alpha_\mathfrak{p}}{\|\vec{\alpha}\|}$. Entonces ψ es continua y $\psi \circ \imath = \mathrm{Id}_{J_{K,0}}$ (o $\mathrm{Id}_{C_{K,0}}$).

Ahora, si K es un campo de funciones, $\Lambda = \mathbb{Z}$. Veamos que debemos considerar $\mathbb{Z}$ con la topología discreta. Sea $\vec{\beta}$ un idèle fijo de grado 1, el cual existe por el Teorema de Schmidt. La topología de $\mathbb{Z}$ debe corresponder a la topología de $\{\vec{\beta}^n\}_{n\in\mathbb{Z}}$ con la topología inducida por la topología usual de J_K. Esto se sigue del hecho de que $U = \prod_{v\in\mathbb{P}_K} U_v$ es abierto en J_K y de que $\vec{\beta}U \cap \{\vec{\beta}^n\}_{n\in\mathbb{Z}} = \{\vec{\beta}\}$.

Sea $\mu : \mathbb{Z} \longrightarrow J_K$ dada por $\mu(n) = \vec{\beta}^n$. Entonces μ es continua y $\mathrm{gr} \circ \mu = \mathrm{Id}_\mathbb{Z}$. También tenemos $\delta : J_K \longrightarrow J_{K,0}$ dada por $\delta(\vec{\alpha}) = \vec{\beta}^{-\,\mathrm{gr}\,\vec{\alpha}}\vec{\alpha}$. Entonces δ es continua y $\delta \circ \jmath = \mathrm{Id}_{J_{K,0}}$. Similarmente para C_K.

Teorema 6.8.1. *Se tienen isomorfismos tanto algebraicos como topológicos*

$$C_K \xrightarrow[\nu]{\cong} C_{K,0} \times \mathbb{R}^+, \quad \textit{si } K \textit{ es numérico,}$$
$$C_K \xrightarrow[\eta]{\cong} C_{K,0} \times \mathbb{Z}, \quad \textit{si } K \textit{ es de funciones,}$$

donde

$$\nu(\tilde{\vec{\alpha}}) = (\psi(\tilde{\vec{\alpha}}), \|\tilde{\vec{\alpha}}\|) \quad y \quad \eta(\tilde{\vec{\alpha}}) = (\tilde{\vec{\beta}}^{-\,\mathrm{gr}\,\tilde{\vec{\alpha}}} \cdot \tilde{\vec{\alpha}}, \mathrm{gr}\,\tilde{\vec{\alpha}}),$$

y donde $\mathbb{R}^+$ tiene la topología inducida por la topología usual de $\mathbb{R}$ y donde $\mathbb{Z}$ tiene la topología discreta. □

Observación 6.8.2. No existe un subgrupo distinguido de representantes de C_K en $C_K/C_{K,0}$. En el caso numérico, es un lugar infinito $\mathfrak{p}$, y en el caso de campos de funciones, es una clase de idèle de grado 1, $\vec{\beta}$. Esto lo veremos de manera más clara en el caso de campos de funciones.

Los grupos $\prod_{\mathfrak{p}\in S} W_\mathfrak{p} \times \prod_{\mathfrak{p}\notin S} U_\mathfrak{p} \subseteq J_K$ es un sistema fundamental de vecindades, donde S es un conjunto finito de lugares y $W_\mathfrak{p}$ pertenece a un sistema de vecindades de la identidad de $K_\mathfrak{p}^*$.

6.8.1. Extensiones de constantes

Sea K un campo global de funciones con campo de constantes $\mathbb{F}_q$. Sean $\mathfrak{p} \in \mathbb{P}_K$ y $K_\mathfrak{p}$ la completación de K en $\mathfrak{p}$. Sea $\mathbb{F}_{q_\mathfrak{p}}$ el campo residual de $K_\mathfrak{p}$ el cual es el mismo que el de K en $\mathfrak{p}$: $\mathbb{F}_{q_\mathfrak{p}} \cong \mathcal{O}_\mathfrak{p}/\mathfrak{p}$. Se tiene que $q_\mathfrak{p} = q^{\operatorname{gr}\mathfrak{p}}$.

Teorema 6.8.3. *Sea L/K la extensión de constantes de grado n, esto es, $L = K\mathbb{F}_{q^n}$. Entonces si escribimos $C_K \cong C_{K,0} \times \mathbb{Z}$, se tiene que $\mathrm{N}_{L/K} C_L = C_{K,0} \times n\mathbb{Z}$.*

Demostración. Del Teorema de Schmidt tenemos que $\operatorname{gr} : C_K \longrightarrow \mathbb{Z}$ es suprayectiva. Se tiene que la extensión L/K es no ramificada por lo que $L_\mathfrak{p}/K_\mathfrak{p}$ es no ramificada. Se sigue que $\alpha_\mathfrak{p} \in K_\mathfrak{p}^*$ se tiene

$$(\alpha_\mathfrak{p}, L_\mathfrak{p}/K_\mathfrak{p}) = \mathrm{Fr}_{L_\mathfrak{p}|K_\mathfrak{p}}^{v_\mathfrak{p}(\alpha_\mathfrak{p})},$$

donde $\mathrm{Fr}_{L_\mathfrak{p}|K_\mathfrak{p}}$ es el automorfismo de Frobenius correspondiente a $L_\mathfrak{p}/K_\mathfrak{p}$.

Puesto que L/K es cíclica, digamos $\mathrm{Gal}(L/K) = \langle \mathrm{Fr}_{L|K} \rangle$, donde se tiene $\langle \mathrm{Fr}_{L|K}^{\operatorname{gr}\mathfrak{p}} \rangle \cong \mathrm{Gal}(L(\mathfrak{P})/K(\mathfrak{p}))$. Se sigue que

$$\mathrm{Fr}_{L_\mathfrak{p}|K_\mathfrak{p}} = \mathrm{Fr}_{L|K}^{\operatorname{gr}\mathfrak{p}} \quad \text{y} \quad \mathrm{Fr}_{L_\mathfrak{p}|K_\mathfrak{p}}^{v_\mathfrak{p}(\alpha_\mathfrak{p})} = \mathrm{Fr}_{L|K}^{\operatorname{gr}\mathfrak{p}\cdot v_\mathfrak{p}(\alpha_\mathfrak{p})}.$$

Se sigue que si $\vec{\alpha} \in J_K$, entonces

$$(\vec{\alpha}, L/K) = \prod_{\mathfrak{p}\in\mathbb{P}_K} (\alpha_\mathfrak{p}, L_\mathfrak{p}/K_\mathfrak{p}) = \prod_{\mathfrak{p}} \mathrm{Fr}_{L|K}^{\operatorname{gr}\mathfrak{p}\cdot v_\mathfrak{p}(\alpha_\mathfrak{p})} = \mathrm{Fr}_{L|K}^{\sum_\mathfrak{p} \operatorname{gr}\mathfrak{p}\cdot v_\mathfrak{p}(\alpha_\mathfrak{p})} = \mathrm{Fr}_{L|K}^{\operatorname{gr}\vec{\alpha}}.$$

Por tanto $(\vec{\alpha}, L/K) = 1 \iff n | \operatorname{gr}\vec{\alpha}$, de donde obtenemos $\mathrm{N}_{L/K} C_L = \text{núc}(\_, L/K) = C_{K,0} \times n\mathbb{Z}$. Además, se verifica que $\mathrm{Gal}(L/K) \cong \frac{C_K}{\mathrm{N}_{L/K} C_L} = \frac{C_{K,0}\times\mathbb{Z}}{C_{K,0}\times n\mathbb{Z}} \cong \frac{\mathbb{Z}}{n\mathbb{Z}}$. □

Más adelante probaremos (Teorema 6.8.37)

Teorema *Sea L/K una extensión abeliana finita de campos de funciones globales. Sea $\mathbb{F}_q$ el campo de constantes de K. Sea*

$$d := \text{mín}\{n \in \mathbb{N} \mid \textit{existe } \vec{\alpha} \in \mathrm{N}_{L/K} J_L \textit{ con } \operatorname{gr}\vec{\alpha} = n\}.$$

Entonces $\mathbb{F}_{q^d}$ es el campo de constantes de L.

6.8.2. Teorema de existencia en característica 0

Definición 6.8.4. Sea S un conjunto finito de primos de un campo global K. Sean $U_{K,S} := \{\vec{\alpha} \in J_L \mid \alpha_\mathfrak{p} = 1 \text{ para } \mathfrak{p} \in S,\ \alpha_\mathfrak{p} \in U_\mathfrak{p} \text{ para } \mathfrak{p} \notin S\} \subseteq J_{K,S} = \prod_{\mathfrak{p}\notin S} U_\mathfrak{p} \times \prod_{\mathfrak{p}\in S} K_\mathfrak{p}^*$ y $\bar{U}_{K,S} := U_{K,S}K^*/K^* \subseteq C_{K,S}$.

Se tiene que $\bar{U}_{K,S}$ no es abierto pero, puesto que $U_{\mathfrak{p}}$ es cerrado en $K_{\mathfrak{p}}^*$, se tiene que $\bar{U}_{K,S}$ es cerrado en C_K. Las vecindades fundamentales $\prod_{\mathfrak{p}\notin S} U_{\mathfrak{p}} \times \prod_{\mathfrak{p}\in S} W_{\mathfrak{p}}$ de 1, contienen a $U_{K,S}$.

Primero probamos un resultado de teoría de grupos que se usa frecuentemente en el cálculo de diversos de índices en subgrupos de idèles y de subgrupos de clases de idèles.

Proposición 6.8.5. *Sea G un grupo abeliano y sean X, Y, Z subgrupos de G tales que $Y \subseteq X$. Entonces el epimorfismo natural $\mu : X/Y \longrightarrow XZ/YZ$ tiene núcleo $\frac{X\cap YZ}{Y} \cong \frac{X\cap Z}{Y\cap Z}$.*

Demostración. Es inmediato que μ es un epimorfismo y que $\operatorname{núc}\mu = \frac{X\cap YZ}{Y}$. Consideremos ahora $X \cap Z \overset{\imath}{\longhookrightarrow} X \cap YZ \overset{\pi}{\twoheadrightarrow} \frac{X\cap YZ}{Y}$, $\varphi := \pi \circ \imath$.

Si $\alpha \in X \cap Z$, $\varphi(\alpha) = \alpha \bmod Y$. Sea $\beta \in X \cap YZ$, es decir, $\beta = yz$ con $\beta \in X$, $y \in Y$, $z \in Z$. Entonces $z = y^{-1}\beta \in Z \cap X$. Se sigue que $\varphi(z) = z \bmod Y = y^{-1}\beta \bmod Y = \beta \bmod Y$, por lo que φ es un epimorfismo y $\operatorname{núc}\varphi = (X \cap Z) \cap Y = Y \cap Z$, de donde se obtiene el resultado. □

Corolario 6.8.6. *Si G un grupo abeliano y si X, Y, Z son subgrupos de G tales que $Y \subseteq X$, entonces*

$$[XZ : YZ] = \frac{[X : Y]}{[X \cap Z : Y \cap Z]}.$$ □

Un resultado fundamental para el teorema de existencia para campos numéricos, y cierta familia de campos de funciones, es el siguiente teorema que tiene como base fundamental la teoría de Kummer.

Teorema 6.8.7. *Sea K un campo numérico que contiene a las n-raíces de la unidad. Si K es un campo de funciones de característica $p > 0$, se supone que $p \nmid n$. Sea S un conjunto finito de primos de K tal que*

- *S contiene a todos los primos infinitos y a todos los primos encima de los primos que dividen a n (esta última condición es vacía en el caso de campos de funciones).*
- *$J_K = J_{K,S}K^*$.*

Entonces $C_K^n \bar{U}_{K,S}$ es el grupo de normas de la extensión de Kummer $L = K\big(\sqrt[n]{K^S}\big)/K$.

Demostración. Por teoría de Kummer y por el teorema de las unidades de Dirichlet, tenemos que $\chi(G_{L|K}) \cong \big((L^*)^n \cap K^*\big)/(K^*)^n = (K^S)(K^*)^n/(K^*)^n = K^S/(K^S)^n$ y que K^S es finitamente generado de rango $s - 1 = |S| - 1$ y contiene a las n-raíces de unidad, por lo que $K^S/(K^S)^n \cong C_n^s$.

Por tanto $G_{L|K} \cong C_n^s$.

Para $\tilde{\tilde{\alpha}}^n \in C_K^n$, se tiene $\big(\tilde{\tilde{\alpha}}^n, L/K\big) = \big(\tilde{\tilde{\alpha}}, L/K\big)^n = 1$. Por tanto $\tilde{\tilde{\alpha}}^n \in \mathrm{N}_{L/K} C_L = \operatorname{núc}(\_, L/K)$.

Ahora sea $\tilde{\vec{\alpha}} \in U_{K,S}$. Para probar que $\vec{\alpha} \in \mathrm{N}_{L/K} J_L$, se debe obtener que para cada $\alpha_\mathfrak{p}$ es norma local de $L_\mathfrak{p}/K_\mathfrak{p}$, $L_\mathfrak{p} = K_\mathfrak{p}\big(\sqrt[n]{K^S}\big)/K_\mathfrak{p}$ para toda $\mathfrak{p} \in \mathbb{P}_K$.

Para $\mathfrak{p} \in S$, $\alpha_\mathfrak{p} = 1$ por lo que $\alpha_\mathfrak{p}$ es norma local. Para $\mathfrak{p} \notin S$, $\alpha_\mathfrak{p} \in U_\mathfrak{p}$. Se seguirá que $\alpha_\mathfrak{p}$ será norma si $\mathfrak{p}$ es no ramificado. Ahora bien, todo $a \in K^S$ es una unidad para $\mathfrak{p} \notin S$ y puesto que n es primo relativo a la característica $\operatorname{car} K(\mathfrak{p})$ del campo residual para $\mathfrak{p} \notin S$, la ecuación $x^n - a = 0$ es separable sobre $K(\mathfrak{p})$ por lo que $K_\mathfrak{p}(\sqrt[n]{a})/K_\mathfrak{p}$ es no ramificada, Teorema 6.1.18.

Se sigue que $\bar{U}_{K,S} \subseteq \mathrm{N}_{L/K} C_L$ y $C_K^n \bar{U}_{K,S} \subseteq \mathrm{N}_{L/K} C_L$. Ahora bien, por la ley de reciprocidad, se obtiene $[C_K : \mathrm{N}_{L/K} C_L] = |\operatorname{Gal}(L/K)| = [K^S : (K^S)^n] = n^s$.

Por otro lado, se tiene:

$$[C_K : C_K^n \bar{U}_{K,S}] = [J_{K,S}K^* : J_{K,S}^n U_{K,S} K^*] \underset{\substack{\uparrow \\ \text{Corolario 6.8.6}}}{=} \frac{[J_{K,S} : J_{K,S}^n U_{K,S}]}{[J_{K,S} \cap K^* : J_{K,S}^n U_{K,S} \cap K^*]} = \frac{A}{B}, \tag{6.8.8}$$

donde $A = [J_{K,S} : J_{K,S}^n U_{K,S}] = \prod_{\mathfrak{p}\in S} [K_\mathfrak{p}^* : (K_\mathfrak{p}^*)^n]$. La última igualdad se debe a que el mapeo $J_{K,S} \longrightarrow \prod_{\mathfrak{p}\in S} K_\mathfrak{p}^*/(K_\mathfrak{p}^*)^n$, $\vec{\alpha} \longmapsto \prod_{\mathfrak{p}\in S} \alpha_\mathfrak{p}(K_\mathfrak{p}^*)^n$ es un epimorfismo y el núcleo consiste de los idèles $\vec{\alpha} \in J_{K,S}$ tales que $\alpha_\mathfrak{p} \in (K_\mathfrak{p}^*)^n$ para $\mathfrak{p} \in S$. Estos últimos son precisamente los idèles $J_{K,S}^n U_{K,S}$.

Ahora bien, se tiene que $[K_\mathfrak{p}^* : (K_\mathfrak{p}^*)^n] = n q^{v_\mathfrak{p}(n)} |\mu_n(K_\mathfrak{p})| = n|n|_\mathfrak{p}^{-1} |\mu_n(K_\mathfrak{p})|$ con $q = |K(\mathfrak{p})|$ (Proposición 5.3.1). Puesto que $|n|_\mathfrak{p} = 1$ para $\mathfrak{p} \notin S$, se tiene

$$A = [J_{K,S} : J_{K,S}^n U_{K,S}] = \prod_{\mathfrak{p}\in S} [K_\mathfrak{p}^* : (K_\mathfrak{p}^*)^n] = \prod_{\mathfrak{p}\in S} n \cdot |n|_\mathfrak{p}^{-1} \cdot n$$
$$= \prod_{\mathfrak{p}\in S} n^2 \cdot |n|_\mathfrak{p}^{-1} = n^{2s} \prod_{\mathfrak{p}} |n|_\mathfrak{p}^{-1} = n^{2s} \cdot 1 = n^{2s}.$$

Para $B = [J_{K,S} \cap K^* : J_{K,S}^n U_{K,S} \cap K^*]$, se tiene que $J_{K,S} \cap K^* = K^S$ y $J_{K,S}^n U_{K,S} \cap K^* = (K^S)^n$. Para verificar esta última desigualdad, notemos en primer lugar que se tiene $(K^S)^n \subseteq J_{K,S}^n U_{K,S} \cap K^*$ y para la otra contención, si $x \in J_{K,S}^n U_{K,S} \cap K^*$, entonces $x = \vec{\alpha}^n u$ con $\vec{\alpha} \in J_{K,S}$ y $u \in U_{K,S}$. Formamos el campo $K(\sqrt[n]{x})$ y probaremos que $K(\sqrt[n]{x}) = K$.

Si $\vec{\beta} \in J_{K,S}$, $\vec{\beta}$ es una norma de algún idèle de $K(\sqrt[n]{x})$: de hecho, si $\mathfrak{p} \in S$, entonces $\beta_\mathfrak{p} \in K_\mathfrak{p}^*$ es una norma pues $K_\mathfrak{p}(\sqrt[n]{x}) = K(\sqrt[n]{\alpha_\mathfrak{p}^n}) = K_\mathfrak{p}$. Si $\mathfrak{p} \notin S$, $\beta_\mathfrak{p} \in U_\mathfrak{p}$ y $K_\mathfrak{p}(\sqrt[n]{x}) = K_\mathfrak{p}(\sqrt[n]{u_\mathfrak{p}})/K_\mathfrak{p}$ pues $\mathfrak{p} \nmid n$, y por tanto $\mathfrak{p}$ es no ramificado. Puesto que $J_K = J_{K,S}K^*$, hemos probado que

$$\mathrm{N}_{K(\sqrt[n]{x})/K} C_{K(\sqrt[n]{x})} = C_K,$$

lo que implica, por la ley de reciprocidad, que $K(\sqrt[n]{x}) = K$.

De esta forma $\sqrt[n]{x} = y \in K^*$, $x = y^n \in (K^*)^n \cap K^S = (K^S)^n$. Por tanto $B = [J_{K,S} \cap K^* : J_{K,S}^n U_{K,S} \cap K^*] = [K^S : (K^S)^n] = n^s$.

Se sigue que

$$[C_K : C_K^n \bar{U}_{K,S}] = \frac{A}{B} = \frac{n^{2s}}{n^s} = n^s = [C_K : \mathrm{N}_{L/K}\, C_L]$$

y por tanto $\mathrm{N}_{L/K}\, C_L = C_K^n \bar{U}_{K,S}$. □

Corolario 6.8.8. *Sea K, ya sea un campo numérico o un campo global de funciones con* $\operatorname{car} K = p \nmid n$. *Sean S y n como antes y no suponemos que K contenga a las n-raíces de unidad. Entonces $C_K^n \bar{U}_{K,S}$ es un grupo de normas.*

Demostración. Sea $K' = K(\zeta_n)$ con ζ_n una n-raíz primitiva de la unidad. Sea S' el conjunto de primos de K' que contienen a todos los primos sobre los de S y suficientemente grande tal que $J_{K'} = J_{K',S'}(K')^*$. Entonces $C_{K'}^n \bar{U}_{K',S'}$ es el grupo de normas de una extensión de Galois L' de K'. Sea L la mínima extensión de Galois de K conteniendo a L'. Se sigue que

$$\begin{aligned}\mathrm{N}_{L/K}\, C_L &= \mathrm{N}_{K'/K}(\mathrm{N}_{L'/K'}(\mathrm{N}_{L/L'}(C_L))) \subseteq \mathrm{N}_{K'/K}(\mathrm{N}_{L'/K}(C_{L'})) \\ &= \mathrm{N}_{K'/K}(C_{K'}^n \bar{U}_{K',S'}) = (\mathrm{N}_{K'/K}\, C_{K'})^n \cdot \mathrm{N}_{K'/K}\, \bar{U}_{K',S'} \subseteq C_K^n \bar{U}_{K,S}.\end{aligned}$$

Esto es, $C_K^n \bar{U}_{K,S}$ contiene a un subgrupo de normas, por lo que $C_K^n \bar{U}_{K,S}$ también es a su vez. un grupo de normas. □

A continuación probamos el teorema de existencia, esencialmente en característica 0. Más adelante daremos otra demostración.

Teorema 6.8.9 (Teorema de existencia en característica 0). *Sea K un campo numérico. Los grupos de normas de C_K son exactamente los subgrupos cerrados de índice finito en C_K.*

Demostración. Sea $\mathcal{N}_L = \mathrm{N}_{L/K}\, C_L \subseteq C_K$ un grupo de normas de una extensión finita y normal, es decir, de Galois, L/K. Se tiene, por la ley de reciprocidad que $[C_K : \mathcal{N}_L] = |G_{L|K}^{\mathrm{ab}}| < \infty$.

Ahora bien, la norma $\mathrm{N}_{L/K} : C_L \longrightarrow C_K$ es una función continua y $C_K \cong C_{K,0} \times \Gamma_K$, $C_L = C_{L,0} \times \Gamma_L$ con Γ_K y $\Gamma_L \cong \mathbb{R}^+$. Consideremos el mapeo de escisión $\varphi : \mathbb{R}^+ \longrightarrow C_K$ definido como sigue. Sea $\mathfrak{p}$ cualquier primo infinito de K y sea $\lceil\ \rceil_{\mathfrak{p}} : K_{\mathfrak{p}}^* \longrightarrow C_K$ el encaje natural. Se tiene que $\mathbb{R}^+ \subseteq K_{\mathfrak{p}}^*$ es un subgrupo.

Si $\mathfrak{p}$ es real $\lceil\ \rceil_{\mathfrak{p}} : \mathbb{R}^+ \longrightarrow C_K$ es la inyección deseada pues $\|\lceil x \rceil_{\mathfrak{p}}\| = |x|_{\mathfrak{p}} = x \in \mathbb{R}^+$. Si $\mathfrak{p}$ es complejo, entonces $\|\lceil x \rceil_{\mathfrak{p}}\| = |x|_{\mathfrak{p}} = x^2$ y tomamos el mapeo $x \longmapsto \lceil \sqrt{x} \rceil_{\mathfrak{p}}$.

Se tiene que la inyección $\varphi : \mathbb{R}^+ \longrightarrow C_K$ nos da un conjunto completo de representantes de $C_K / C_{K,0}$. Por tanto, podemos suponer que $\Gamma_K = \Gamma_L \subseteq C_L$. Se sigue que

$$\mathrm{N}_{L/K}\, C_L = \mathrm{N}_{L/K}\, C_{L,0} \times \mathrm{N}_{L/K}\, \Gamma_L = \mathrm{N}_{L/K}\, C_{L,0} \times \Gamma_K^{[L:K]} = \mathrm{N}_{L/K}\, C_{L,0} \times \Gamma_K.$$

La imagen del grupo compacto $C_{L,0}$ en C_K es compacto, por tanto cerrado y, puesto que $\mathit{\Gamma}_K \subseteq C_K$ es también cerrado, $\mathrm{N}_{L/K}\, C_L = \mathcal{N}_L$ es cerrado en C_K. Esta misma conclusión está dada en el Corolario 6.7.38.

Recíprocamente, sea $\mathcal{N} \subseteq C_K$ un subgrupo cerrado de índice finito: $[C_K : \mathcal{N}] = n$. Se sigue que $C_K^n \subseteq \mathcal{N}$. Por otro lado, $\mathcal{N}$ es también un subgrupo abierto y por ende contiene a algún subgrupo de la forma $\bar{U}_{K,S}$. Puesto que $C_K^n \bar{U}_{K,S}$ es un grupo de normas para S suficientemente grande y como $C_K^n \bar{U}_{K,S} \subseteq \mathcal{N}$, $\mathcal{N}$ es a su vez, un grupo de normas. □

Observación 6.8.10. La demostración del teorema de existencia 6.8.9 sigue cumpliéndose para campos de funciones tales que $\operatorname{car} K = p \nmid n = [C_K : \mathcal{N}]$. El caso general de campos de funciones lo daremos más adelante y requiere otro tratamiento.

6.8.3. Normas universales

Definición 6.8.11. Sea K un campo global. Se define el grupo de *normas universales* como

$$\mathfrak{N}_K := \bigcap_L \mathrm{N}_{L/K}\, C_L,$$

donde L recorre todas las extensiones abelianas finitas de K.

Sea $\rho_K : C_K \longrightarrow G_K^{\mathrm{ab}} = \mathrm{Gal}(K^{\mathrm{ab}}/K)$ el símbolo universal de la norma residual, esto es, $\rho_K = (\_, K)$.

Teorema 6.8.12. *Se tiene*

$$\text{núc}\, \rho_K = \mathfrak{N}_K = \bigcap_{\substack{L/K \text{ abeliana} \\ \text{finita}}} \mathcal{N}_L = \bigcap_{\substack{L/K \text{ abeliana} \\ \text{finita}}} \mathrm{N}_{L/K}\, C_L.$$

Demostración. Para $\tilde{\vec{\alpha}} \in C_K$, se tiene $\rho_K\big(\tilde{\vec{\alpha}}\big) = \varprojlim_L \rho_K|_L\big(\tilde{\vec{\alpha}}\big) = \varprojlim_L \big(\tilde{\vec{\alpha}}, L/K\big)$. Por tanto

$$\begin{aligned}
\tilde{\vec{\alpha}} \in \text{núc}\, \rho_L &\iff \big(\tilde{\vec{\alpha}}, L/K\big) = 1 \text{ para toda extensión } L/K \text{ abeliana finita} \\
&\iff \tilde{\vec{\alpha}} \in \mathcal{N}_L = \mathrm{N}_{L/K}\, C_L \text{ para toda extensión } L/K \text{ abeliana finita} \\
&\iff \tilde{\vec{\alpha}} \in \bigcap_L \mathrm{N}_{L/K}\, C_L \text{ para } L/K \text{ extensión abeliana finita.}
\end{aligned}$$

□

Recordemos que para cualquier extensión abeliana finita E/F de campos globales ($K \subseteq F \subseteq E \subseteq K^{\mathrm{ab}}$), con E/K finita, se tiene que $\mathrm{N}_{E/F}\, C_E$ es cerrado y abierto en C_F (Corolario 6.7.38).

Lema 6.8.13. *Sea K un campo global, E/K una extensión finita con $E \subseteq K^{\mathrm{ab}}$. Sea $K \subseteq F \subseteq E$. Entonces* $\text{núc}\, \mathrm{N}_{E/F} = \mathrm{N}_{E/F}^{-1}(1)$ *es un subgrupo compacto de C_E.*

Demostración. Se tiene $C_E \cong C_{E,0} \times \Lambda$ donde

$$\Lambda = \begin{cases} \mathbb{R}^+ & \text{si } E \text{ es numérico,} \\ \mathbb{Z} & \text{si } E \text{ es de funciones.} \end{cases}$$

Sea $[E:F] = n$, $\mathrm{N}_{E/F}\,\Lambda = n\Lambda \cong \Lambda$ y por tanto $\mathrm{núc}\,\mathrm{N}_{E/F}\,|_\Lambda = \{1\}$.

Se tiene el diagrama conmutativo con filas exactas

$$\begin{array}{ccccccccc} 1 & \longrightarrow & C_{E,0} & \xrightarrow{\imath} & C_E & \xrightarrow{\| \ \|} & \Lambda & \longrightarrow & 1 \\ & & \downarrow{\scriptstyle \mathrm{N}_0} & \circlearrowleft & \downarrow{\scriptstyle \mathrm{N}} & \circlearrowleft & \downarrow{\scriptstyle \mathrm{N}_1} & & \\ 1 & \longrightarrow & C_{F,0} & \xrightarrow{\imath} & C_F & \xrightarrow{\| \ \|} & \Lambda & \longrightarrow & 1 \end{array}$$

donde $\mathrm{N}_0 = \mathrm{N}_{E/F}\,|_{C_{E,0}}$, $\mathrm{N} = \mathrm{N}_{E/F}$, $\mathrm{N}_1 = \mathrm{N}_{E/F}\,|_\Lambda$. Del Lema de la Serpiente, obtenemos la sucesión exacta

$$\begin{aligned} 1 \longrightarrow \mathrm{núc}\,\mathrm{N}_0 \longrightarrow \mathrm{núc}\,\mathrm{N} \longrightarrow 1 \longrightarrow C_{F,0}/\,\mathrm{N}_{E/F}\,C_{E,0} \longrightarrow \\ \longrightarrow C_F/\,\mathrm{N}_{E/F}\,C_E \longrightarrow \Lambda/n\Lambda \longrightarrow 1. \end{aligned}$$

Se sigue que $\mathrm{núc}\,\mathrm{N} = \mathrm{núc}\,\mathrm{N}_0$ y que $C_F/\,\mathrm{N}_{E/F}\,C_E \cong C_{F,0}/\,\mathrm{N}_{E/F}\,C_{E,0} \times \Lambda/n\Lambda$. Además $\Lambda/n\Lambda \cong \begin{cases} 1 & \text{si } E \text{ es numérico} \\ \mathbb{Z}/n\mathbb{Z} & \text{si } E \text{ es de funciones.} \end{cases}$

Ahora bien, $\mathrm{núc}\,\mathrm{N} = \mathrm{núc}\,\mathrm{N}_0 < C_{E,0}$ el cual es compacto y $\mathrm{núc}\,\mathrm{N}_0$ es cerrado, por lo que $\mathrm{núc}\,\mathrm{N}$ es compacto. □

Teorema 6.8.14. *Sea E/F una extensión de campos globales tal que $[E : K] < \infty$ y $E \subseteq K^{\mathrm{ab}}$. Entonces $\mathfrak{N}_F = \mathrm{N}_{E/F}\,\mathfrak{N}_E$.*

Demostración. Primero veamos que $\mathrm{N}_{E/F}\,\mathfrak{N}_E \subseteq \mathfrak{N}_F$. Consideremos $\tilde{\vec{\alpha}} \in \mathfrak{N}_E = \bigcap_L \mathrm{N}_{L/E}\,C_L$, donde L recorre a las extensiones abelianas finitas de E. Para cada tal L, existe $\tilde{\vec{\beta}}_L$ tal que $\tilde{\vec{\alpha}} = \mathrm{N}_{L/E}\,\tilde{\vec{\beta}}_L$.

Ahora consideremos M cualquier extensión abeliana finita de F. Se tiene

$$\mathrm{N}_{ME/F}\,C_{ME} = \mathrm{N}_{M/F}\,\mathrm{N}_{ME/M}\,C_{ME} \subseteq \mathrm{N}_{M/F}\,C_M.$$

Por tanto $\mathrm{N}_{ME/F}\,C_{ME} \cap \mathrm{N}_{M/F}\,C_M = \mathrm{N}_{ME/F}\,C_{ME}$ y $ME \supseteq E$. Esto es,

$$\mathfrak{N}_F = \bigcap_{L \supseteq F} \mathrm{N}_{L/F}\,C_L = \bigcap_{L \supseteq E} \mathrm{N}_{L/F}\,C_L.$$

Se sigue que para $L \supseteq E$, $\mathrm{N}_{E/F}\,\tilde{\vec{\alpha}} = \mathrm{N}_{E/F}\,\mathrm{N}_{L/E}\,\tilde{\vec{\beta}}_L = \mathrm{N}_{L/F}\,\tilde{\vec{\beta}}_L \in \mathrm{N}_{L/F}\,C_L$. Por tanto

$$\mathrm{N}_{E/F}\,\tilde{\vec{\alpha}} \in \bigcap_{L \supseteq E} \mathrm{N}_{L/F}\,C_L = \mathfrak{N}_F \quad \text{y} \quad \mathrm{N}_{E/F}\,\mathfrak{N}_E \subseteq \mathfrak{N}_F.$$

Ahora veamos que $\mathfrak{N}_F \subseteq \mathrm{N}_{E/F}\,\mathfrak{N}_E$. Sea $\tilde{\vec{\alpha}} \in \mathfrak{N}_F$. Para cada $L \supseteq E$, sea $\mathcal{T}_L := \mathrm{N}_{L/E}\,C_L \cap \mathrm{N}_{E/F}^{-1}(\tilde{\vec{\alpha}}) = \{\tilde{\vec{\beta}} \in C_E \mid \tilde{\vec{\beta}} \in \mathrm{N}_{L/E}\,C_L \text{ y } \mathrm{N}_{E/F}\,\tilde{\vec{\beta}} = \tilde{\vec{\alpha}}\}$.

Verificaremos que $\bigcap_{L\supseteq E} \mathcal{T}_L \neq \emptyset$ y en este caso, si $\tilde{\vec{\gamma}} \in \bigcap_{L\supseteq E} \mathcal{T}_L$, entonces $\tilde{\vec{\gamma}} \in \bigcap_{L\supseteq E} \mathrm{N}_{L/E}\,C_L = \mathfrak{N}_E$ y $\mathrm{N}_{E/F}\,\tilde{\vec{\gamma}} = \tilde{\vec{\alpha}}$ y por tanto $\tilde{\vec{\alpha}} \in \mathrm{N}_{E/F}\,\mathfrak{N}_E$ mostrando que $\mathfrak{N}_F \subseteq \mathrm{N}_{E/F}\,\mathfrak{N}_E$.

Tenemos que cada $\mathcal{T}_L \neq \emptyset$ pues ya que $\tilde{\vec{\alpha}} \in \mathfrak{N}_F$, se tiene que para cada $L \supseteq F$, $\tilde{\vec{\alpha}} \in \mathrm{N}_{L/F}\,C_L = \mathrm{N}_{E/F}(\mathrm{N}_{L/E}\,C_L)$. Por otro lado el conjunto $\{\mathcal{T}_L\}_{L\supseteq E}$ tiene la propiedad de la intersección finita puesto que $\bigcap_{i=1}^{s} \mathcal{T}_{L_i} \supseteq \mathcal{T}_L$ para $L \supseteq L_i$, $1 \leq i \leq s$. Se sigue que para probar que $\bigcap_{L\supseteq E} \mathcal{T}_L \neq \emptyset$, es suficiente probar que cada $\mathcal{T}_L$ es compacto.

Se tiene que $\mathrm{N}_{L/E}\,C_L$ es cerrado y $\mathrm{N}_{E/F}^{-1}(\tilde{\vec{\alpha}})$ es compacto, por lo que $\mathcal{T}_L$ es cerrado en $\mathrm{N}_{E/F}^{-1}(\tilde{\vec{\alpha}})$ y por tanto es compacto. El resultado se sigue. □

Lema 6.8.15. *Para todo $K \subseteq F \subseteq K^{\mathrm{ab}}$ tal que $[F : K] < \infty$, se tiene que* $\mathrm{núc}\,\varphi_{F,l}$, *donde $\varphi_{F,l} : C_F \longrightarrow C_F$ está dada por $\varphi_{F,l}(\tilde{\vec{\alpha}}) = \tilde{\vec{\alpha}}^l$, es un conjunto compacto.*

Demostración. Se tiene que $\mathrm{núc}\,\varphi_{F,l} = \{\tilde{\vec{\alpha}} \in C_F \mid \tilde{\vec{\alpha}}^l = 1\}$. Ahora bien, si $\tilde{\vec{\alpha}} \in \mathrm{núc}\,\varphi_{F,l}$, entonces $1 = \|\tilde{\vec{\alpha}}^l\| = \|\tilde{\vec{\alpha}}\|^l$ y $\|\tilde{\vec{\alpha}}\| \in \mathbb{R}^+$, por lo que $\|\tilde{\vec{\alpha}}\| = 1$. Se sigue que $\tilde{\vec{\alpha}} \in C_{F,0}$. Puesto que $\varphi_{F,l}$ es continua, $\mathrm{núc}\,\varphi_{F,l}$ es cerrado en $C_{F,0}$ y como $C_{F,0}$ es compacto, se sigue que $\mathrm{núc}\,\varphi_{F,l}$ es compacto. □

Teorema 6.8.16. *Para cada número primo l, se tiene que $\mathfrak{N}_E \subseteq C_E^l$ para cada extensión abeliana finita E/K con $\zeta_l \in E$.*

Demostración. Sea $\tilde{\vec{\alpha}} \in \mathfrak{N}_E$.

Si $l = p = \mathrm{car}\,K$: Entonces, como $\tilde{\vec{\alpha}} \in \mathfrak{N}_E$, se tiene que $(\tilde{\vec{\alpha}}, M/E) = 1$ donde M es la máxima extensión abeliana de E de exponente p. Del Teorema 6.6.17 se obtiene que $\tilde{\vec{\alpha}} \in C_E^p$ (en este caso, $\zeta_p = 1 \in E$ para todo E).

Sea $l \neq p = \mathrm{car}\,K$: Sea E tal que $\zeta_l \in E$. Sea S un conjunto finito no vacío de primos de E que contiene a todos los divisores de l, $\mathfrak{p}|l$, los primos arquimediano y suficientemente grande tal que $J_E = J_{E,S}E^*$.

Sean $D = \prod_{\mathfrak{p}\in S}(E_{\mathfrak{p}}^*)^l \times \prod_{\mathfrak{p}\notin S} U_{\mathfrak{p}}$ y $E_1 = E\big((E^S)^{1/l}\big)$. De la teoría de Kummer, obtenemos

$$[E_1 : E] = [E^S : (E^S)^l] = l^s, \quad \text{donde} \quad s = |S|.$$

Se tiene

$$[J_E : DE^*] = [J_{E,S}E^* : DE^*] \underset{\substack{\uparrow \\ \text{Corolario 6.8.6}}}{=} \frac{[J_{E,S} : D]}{[J_{E,S} \cap E^* : D \cap E^*]}$$
$$= \frac{[J_{E,S} : D]}{[E^S : (E^S)^l]} = \frac{\prod_{\mathfrak{p}\in S}[E_{\mathfrak{p}}^* : (E_{\mathfrak{p}}^*)^l]}{[E^S : (E^S)^l]}.$$

De la Proposición 5.3.1, se tiene

$$[E_{\mathfrak{p}}^* : (E_{\mathfrak{p}}^*)^l] = \frac{l^2}{|l|_{\mathfrak{p}}}.$$

Para $\mathfrak{p} \notin S$, $|l|_{\mathfrak{p}} = 1$ por lo que

$$\prod_{\mathfrak{p}\in S}[E_{\mathfrak{p}}^* : (E_{\mathfrak{p}}^*)^l] = \prod_{\mathfrak{p}\in S}\frac{l^2}{|l|_{\mathfrak{p}}} = \frac{l^{2s}}{\prod_{\mathfrak{p}}|l|_{\mathfrak{p}}} = l^{2s}.$$

Por tanto

$$[J_E : DE^*] = \frac{l^{2s}}{l^s} = l^s = [E_1 : E].$$

De esta forma obtenemos

$$\begin{aligned}[J_E : DE^*] &= [E_1 : E] = [C_E : \mathrm{N}_{E_1/E}\, C_{E_1}] \\ &= \big[J_E/E^* : (\mathrm{N}_{E_1/E}\, J_{E_1})E^*/E^*\big] = [J_E : (\mathrm{N}_{E_1/E}\, J_{E_1})E^*].\end{aligned}$$

Se sigue que $DE^* = (\mathrm{N}_{E_1/E}\, J_{E_1})E^*$, puesto que, por el Teorema 6.6.7, tenemos $DE^* \subseteq (\mathrm{N}_{E_1/E}\, J_{E_1})E^*$.

Sea $\tilde{\vec{\alpha}} \in \mathfrak{N}_E$. En particular $\tilde{\vec{\alpha}}$ es norma desde E_1, $\vec{\alpha} \in (\mathrm{N}_{E_1/D}\, J_{E_1})E^* = DE^*$. Por tanto, $\tilde{\vec{\alpha}}$ tiene un representante $\vec{\beta} \in D$. Cualesquiera dos representantes de $\tilde{\vec{\alpha}}$ difieren por un elemento $\delta \in D \cap E^* = (E^S)^l$. Ahora $\vec{\beta}$ es una l-potencia para todos los primos de S. Veremos que también es una l-potencia para todo $\mathfrak{p} \notin S$.

Para $S' \supseteq S$, definimos $D' = \prod_{\mathfrak{p}\in S'}(E_{\mathfrak{p}}^*)^l \times \prod_{\mathfrak{p}\in S'} U_{\mathfrak{p}}$ y se tiene $D'E^* = (\mathrm{N}_{E_1'/E}\, J_{E_1'})E^*$, $E_1' = E\big((E^{s'})^{1/l}\big)$.

Se tiene que $\tilde{\vec{\alpha}}$ tiene un representante $\vec{\gamma} \in D'$. Se puede escribir $\vec{\gamma} = \vec{\eta}^{\,l} \cdot \vec{\gamma}'$ donde $\vec{\gamma}'$ es una unidad fuera de S' y 1 en los primos de S', $\vec{\eta}$ es 1 fuera de S'. Sea $x \in E$ tal que $\vec{\eta} = x \cdot \vec{\xi}$ donde $\vec{\xi} \in J_{E,S}$. Entonces $\vec{\eta}^{\,l} = x^l \cdot \vec{\xi}^{\,l}$ y $\vec{\gamma} = x^l \cdot \vec{\xi}^{\,l} \cdot \vec{\gamma}'$. Se sigue $\vec{\gamma}$ es una l-potencia para todos los primos l en S'. Por tanto $\vec{\gamma}$ difiere de $\vec{\beta}$ por una l-potencia y por tanto $\vec{\beta}$ es una l-potencia en S'. Puesto que podemos incluir cualquier primo en S', se sigue que $\tilde{\vec{\alpha}} \in C_E^l$. □

Teorema 6.8.17. *Para cualquier $K \subseteq F \subseteq K^{\mathrm{ab}}$ tal que $[F : K] < \infty$, se tiene que $\mathfrak{N}_F$ es (infinitamente) divisible, es decir, para toda $m \in \mathbb{N}$, $\mathfrak{N}_F^m = \mathfrak{N}_F$.*

Demostración. Es suficiente probar que $\mathfrak{N}_F^l = \mathfrak{N}_F$ para cualquier número primo l.

Se tiene que $\mathfrak{N}_F = \mathrm{N}_{E/F}\, \mathfrak{N}_E$ para cada extensión finita E/F. Tomando E suficientemente grande para l en el sentido de que $\mathfrak{N}_E \subseteq C_E^l$, se tiene

$$\mathfrak{N}_F = \mathrm{N}_{E/F}\, \mathfrak{N}_E \subseteq \mathrm{N}_{E/F}\, C_E^l = \big(\mathrm{N}_{E/F}\, C_E\big)^l. \tag{6.8.9}$$

Sea $\tilde{\vec{\alpha}} \in \mathfrak{N}_F$. El símbolo $\big(\tilde{\vec{\alpha}}\big)^{1/l}$ denota al conjunto de elementos de C_F cuya l-potencia es $\tilde{\vec{\alpha}}$: $\tilde{\vec{\alpha}}^{1/l} := \{\tilde{\vec{\beta}} \in C_F \mid \tilde{\vec{\beta}}^l = \tilde{\vec{\alpha}}\}$.

De (6.8.9), se obtiene que los conjuntos

$$X_E := \big(\mathrm{N}_{E/F}\, C_E\big) \cap \big(\tilde{\vec{\alpha}}\big)^{1/l}$$

son no vacíos. Por tanto estos conjuntos satisfacen la propiedad de intersección finita:

$$\bigcap_{i=1}^{r} X_{E_i} \supseteq X_E \neq \emptyset \quad \text{para } E \text{ tal que } E_i \subseteq E \text{ para toda } 1 \leq i \leq r.$$

Además $\mathrm{N}_{E/F}\, C_E$ es cerrado (Corolario 6.7.38) y $\tilde{\vec{\alpha}}^{1/l}$ es compacto (Lema 6.8.15) por lo que X_E es un conjunto compacto. Se sigue que $\bigcap_E X_E \neq \emptyset$. Si $\tilde{\vec{\beta}} \in \bigcap_E X_E$, entonces $\tilde{\vec{\beta}} \in \mathfrak{N}_F \bigcap \big(\tilde{\vec{\alpha}}\big)^{1/l}$, por tanto $\tilde{\vec{\beta}} \in \mathfrak{N}_F$ y $\tilde{\vec{\beta}}^l = \tilde{\vec{\alpha}}$ lo que prueba el teorema. □

Proposición 6.8.18. *Sea K cualquier campo global y sea $H \subseteq C_K$ cualquier subgrupo divisible. Entonces $H \subseteq \mathfrak{N}_K$.*

Demostración. Sea $h \in H$ y sea L/K una extensión abeliana finita. Se tiene que $(h, L/K) \in \mathrm{Gal}(L/K)$. Sea $|\,\mathrm{Gal}(L/K)| = n$. Sea $h_1 \in H$ con $h_1^n = h$. Se sigue que

$$\rho_K(h)|_L = (h, L/K) = (h_1^n, L/K) = (h_1, L/K)^n = 1,$$

lo que implica que $h \in \mathrm{N}_{L/K}\, C_L$ y $h \in \bigcap_L \mathrm{N}_{L/K}\, C_L = \mathfrak{N}_K$. □

Corolario 6.8.19. *Se tiene que $\mathfrak{N}_K$ es el máximo subgrupo divisible de C_K.* □

Corolario 6.8.20. *Si K es un campo numérico, ρ_K es suprayectiva y no inyectiva.*

Demostración. Se tiene que $C_K \cong C_{K,0} \times \mathbb{R}^+$ y $\mathbb{R}^+$ es divisible, por lo que $\mathbb{R}^+ \subseteq \mathfrak{N}_K = \text{núc}\, \rho_K$. Por tanto ρ_K no es inyectiva.

Por otro lado, $\rho_K(C_K) = \rho_K(C_{K,0}) \subseteq G_K^{\mathrm{ab}}$ y $\rho_K(C_K)$ es denso en G_K^{ab} y $\rho(C_{K,0})$ es compacto, de donde se sigue que $\rho_K(C_K) = G_K^{\mathrm{ab}}$. □

Lema 6.8.21. *Sea A cualquier subgrupo de índice finito en C_K, donde K es un campo global. Entonces, si $H < C_K$ es un subgrupo divisible, se tiene $H \subseteq A$.*

Demostración. Sea $h \in H$. Sea $[C_K : A] = n < \infty$. Existe $h_1 \in H < C_K$ con $h_1^n = h \in A$. □

Con todos estos elementos, damos otra demostración del teorema de existencia para campos numéricos (Teorema 6.8.9).

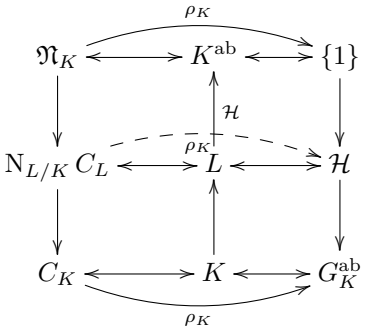
Teorema 6.8.22 (Teorema de existencia en característica 0). *Sea K un campo numérico. Sea H un subgrupo abierto de C_K de índice finito. Entonces H es un grupo de normas.*

Demostración. Se tiene que $\operatorname{núc}\rho_K = \mathfrak{N}_K$ es divisible. Por tanto $\operatorname{núc}\rho_K \subseteq H$. Se tiene que H es cerrado en C_K. Sea $H_0 := H \cap C_{K,0}$. Entonces H_0 es cerrado en $C_{K,0}$, por tanto compacto y $[C_{K,0} : H_0] = [C_K : H]$ pues $\mathbb{R}^+ \subseteq H$ por ser divisible. Sea $C_{K,0} \xrightarrow{\mu} C_K/H$, $\tilde{\vec{\xi}} \longmapsto \tilde{\vec{\xi}}$ mód H, el mapeo natural.

Sea $\tilde{\vec{\xi}} \cdot x \in C_K$, $\tilde{\vec{\xi}} \in C_{K,0}$, $x \in \mathbb{R}^+$. Entonces $\mu(\tilde{\vec{\xi}}) = \tilde{\vec{\xi}}$ mód $H = \tilde{\vec{\xi}}x$ mód H. Por tanto μ es suprayectiva y $\operatorname{núc}\mu = H \cap C_{K,0} = H_0$.

Sea $\mathcal{H} = \rho_K(H_0)$ el cual es un subgrupo cerrado de G_K^{ab} por ser compacto, y como $\mathfrak{N}_K \subseteq H$, se tiene que $H_0 = \rho_K^{-1}(\mathcal{H}) \cap C_{K,0}$. De hecho, se tiene $\rho_K^{-1}(\mathcal{H}) = \rho_K^{-1}(\rho_K(H_0)) \supseteq H_0$, de donde $\rho_K^{-1}(\mathcal{H}) \cap C_{K,0} \supseteq H_0$. Recíprocamente, si $\tilde{\vec{\xi}} \in \rho_K^{-1}(\mathcal{H}) \cap C_{K,0}$, entonces $\rho_K(\tilde{\vec{\xi}}) \in \mathcal{H} = \rho_K(H_0)$. Por tanto existe $\tilde{\vec{\alpha}} \in H_0$ tal que $\tilde{\vec{\xi}} = \tilde{\vec{\alpha}} \cdot \tilde{\vec{\beta}}$ con $\tilde{\vec{\beta}} \in \operatorname{núc}\rho_K \subseteq H$ y $\tilde{\vec{\beta}} = \tilde{\vec{\xi}}\tilde{\vec{\alpha}}^{-1} \in C_{K,0}$. Se sigue que $\tilde{\vec{\xi}} \in H \cap C_{K,0} = H_0$.

Como consecuencia de lo anterior, tenemos que $[G_K^{\mathrm{ab}} : \mathcal{H}] = [C_{K,0} : H_0] = [C_K : H]$. Sea $L := (K^{\mathrm{ab}})^{\mathcal{H}}$. Entonces, si $\tilde{\vec{\alpha}} \in \mathrm{N}_{L/K} C_L$, se tiene $\rho_K(\tilde{\vec{\alpha}})\big|_L = 1$, lo cual implica que $\rho_K(\tilde{\vec{\alpha}}) \in \mathcal{H}$. Se sigue que $\mathrm{N}_{L/K} C_L \subseteq \rho_K^{-1}(\mathcal{H})$.



Se tiene que $[C_K : \mathrm{N}_{L/K} C_L] = [L : K] = [G_K^{\mathrm{ab}} : \mathcal{H}] = [C_K : H]$.

Se sigue que $\mathrm{N}_{L/K} C_L = H$ y esto concluye el teorema de existencia. □

Con respecto al núcleo de ρ_K para un campo numérico K, Tate probó el siguiente resultado.

Teorema 6.8.23. *Si K es un campo numérico y $\rho_K : C_K \longrightarrow G_K^{\mathrm{ab}}$ es el mapeo de reciprocidad,* $\operatorname{núc}\rho_K = \mathfrak{N}_K$ *es la componente conexa de* 1 *y se tiene*

$$\mathfrak{N}_K \cong \left(\frac{\hat{\mathbb{Z}} \times \mathbb{R}}{\mathbb{Z}}\right)^t \oplus \left(\frac{\mathbb{R}}{\mathbb{Z}}\right)^s \oplus \mathbb{R},$$

donde s es el número de lugares complejos de K y t es el rango de las unidades totalmente positivas de K ($\mathbb{R}^+ \overset{\log}{\cong} \mathbb{R}$).

Demostración. Ver [7, Chapter IX, páginas 65–70], [120, Chapter VI, Section 1, Exercises 1–10, páginas 367–368]. □

6.8.4. Teorema de existencia en característica $p > 0$

Ahora estudiemos el caso de campos de funciones. Sean K un campo global de funciones y $\rho_K : C_K \longrightarrow G_K^{\mathrm{ab}}$ el símbolo de la norma residual.

Se tiene que $\mathrm{Gal}(K\mathbb{F}_q^{\mathrm{ab}}/K) \cong \mathrm{Gal}(\mathbb{F}_q^{\mathrm{ab}}/\mathbb{F}_q) \cong \hat{\mathbb{Z}}$ y $\mathrm{Gal}(K\mathbb{F}_q^{\mathrm{ab}}/K) = \overline{\langle \mathrm{Fr}_K \rangle}$ donde Fr_K es el automorfismo de Frobenius, $\mathbb{F}_q^{\mathrm{ab}} \xrightarrow{\mathrm{Fr}_K} \mathbb{F}_q^{\mathrm{ab}}$, $x \longmapsto x^q$.

Sea $\sigma \in G_K^{\mathrm{ab}}$ y $\sigma|_{\mathbb{F}_q^{\mathrm{ab}}} = \mathrm{Fr}_K^{\nu}$. Se define $\nu := \mathrm{ord}(\sigma) \in \hat{\mathbb{Z}}$.

Si $\tilde{\vec{\alpha}} \in C_K$, escribimos $\tilde{\vec{\alpha}} = \tilde{\vec{\alpha}}_1^n \tilde{\vec{\alpha}}_0$ con $\tilde{\vec{\alpha}}_1$ un elemento de C_K de grado 1 fijado de antemano y $\tilde{\vec{\alpha}}_0 \in C_{K,0}$. Se tiene $\mathrm{gr}\, \tilde{\vec{\alpha}} = n$. En término de valores absolutos, tenemos $\|\tilde{\vec{\alpha}}_1\| = q$, $\|\tilde{\vec{\alpha}}_0\| = 1$ y $\mathrm{gr}\, \tilde{\vec{\alpha}}_1 = 1$, $\mathrm{gr}\, \tilde{\vec{\alpha}}_0 = 0$.

Se tiene que $\rho_K(\tilde{\vec{\alpha}}) = (\tilde{\vec{\alpha}}, K) = \prod_{\mathfrak{p}} (\alpha_{\mathfrak{p}}, L_{\mathfrak{p}}/K_{\mathfrak{p}})$.

Teorema 6.8.24. *Para $\tilde{\vec{\alpha}} \in C_K$, $\rho_K(\tilde{\vec{\alpha}}) = (\tilde{\vec{\alpha}}, K)$, se tiene*

$$\mathrm{ord}\left((\tilde{\vec{\alpha}}, K)\right) = \mathrm{gr}\left(\tilde{\vec{\alpha}}\right) \in \mathbb{Z}.$$

En particular, si $\tilde{\vec{\alpha}} \in \mathrm{núc}\, \rho_K$, necesariamente $\tilde{\vec{\alpha}} \in C_{K,0}$, esto es, $\mathrm{núc}\, \rho_K \subseteq C_{K,0}$.

Demostración. Recordemos que $\mathrm{gr}\, \tilde{\vec{\alpha}} = \mathrm{gr}\, \vec{\alpha} = \sum_{\mathfrak{p}} \mathrm{gr}_{\mathfrak{p}}\, \alpha_{\mathfrak{p}}$, donde $\mathrm{gr}_{\mathfrak{p}} = \mathrm{gr}\, \mathfrak{p} \cdot v_{\mathfrak{p}}(\alpha_{\mathfrak{p}})$.

Ahora bien, $|\alpha_{\mathfrak{p}}|_{\mathfrak{p}} = q_{\mathfrak{p}}^{-v_{\mathfrak{p}}(\alpha_{\mathfrak{p}})}$ donde $q_{\mathfrak{p}} = |K(\mathfrak{p})|$ es la cardinalidad del campo residual y $[K(\mathfrak{p}) : \mathbb{F}_q] = \mathrm{gr}\, \mathfrak{p}$. Por tanto $q_{\mathfrak{p}} = |K(\mathfrak{p})| = q^{\mathrm{gr}\, \mathfrak{p}}$. Esto es,

$$|\alpha_{\mathfrak{p}}|_{\mathfrak{p}} = q_{\mathfrak{p}}^{-v_{\mathfrak{p}}(\alpha_{\mathfrak{p}})} = q^{-\mathrm{gr}\, \mathfrak{p} \cdot v_{\mathfrak{p}}(\alpha_{\mathfrak{p}})} = q^{-\mathrm{gr}_{\mathfrak{p}}\, \alpha_{\mathfrak{p}}}.$$

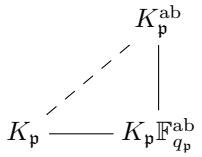
De esta forma, tenemos:

$$\|\tilde{\vec{\alpha}}\| = \|\vec{\alpha}\| = \prod_{\mathfrak{p}} |\alpha_{\mathfrak{p}}|_{\mathfrak{p}} = q^{-\sum_{\mathfrak{p}} \mathrm{gr}_{\mathfrak{p}}\, \alpha_{\mathfrak{p}}} = q^{-\mathrm{gr}\, \vec{\alpha}} = q^{-\mathrm{gr}\, \tilde{\vec{\alpha}}},$$

y en particular

$$\|\tilde{\vec{\alpha}}\| = 1 \iff \mathrm{gr}\, \tilde{\vec{\alpha}} = 0.$$

Sean $K_{\mathfrak{p}}$ es cualquier completación y $\sigma \in G_{K_{\mathfrak{p}}}^{\mathrm{ab}} = \mathrm{Gal}(K_{\mathfrak{p}}^{\mathrm{ab}}/K_{\mathfrak{p}})$, $K_{\mathfrak{p}}(\mathfrak{p}) = \mathbb{F}_{q_{\mathfrak{p}}} = \mathbb{F}_{q^{\mathrm{gr}\, \mathfrak{p}}}$.



Sea $\sigma|_{K_{\mathfrak{p}}\mathbb{F}_{q_{\mathfrak{p}}}^{\mathrm{ab}}} \in \mathrm{Gal}(K_{\mathfrak{p}}\mathbb{F}_{q_{\mathfrak{p}}}^{\mathrm{ab}}/K_{\mathfrak{p}}) \cong \mathrm{Gal}(\mathbb{F}_{q_{\mathfrak{p}}}^{\mathrm{ab}}/\mathbb{F}_{q_{\mathfrak{p}}})$.

Se tiene que si $\mathrm{Fr}_{\mathfrak{p}}$ es el Frobenius respectivo a $\mathbb{F}_{q_{\mathfrak{p}}}^{\mathrm{ab}}/\mathbb{F}_{q_{\mathfrak{p}}}$, entonces se tiene que $\overline{\langle \mathrm{Fr}_{\mathfrak{p}} \rangle} = \mathrm{Gal}(\mathbb{F}_{q_{\mathfrak{p}}}^{\mathrm{ab}}/\mathbb{F}_{q_{\mathfrak{p}}})$. Esto es, $\mathrm{Fr}_{\mathfrak{p}} : \mathbb{F}_{q_{\mathfrak{p}}}^{\mathrm{ab}} \longrightarrow \mathbb{F}_{q_{\mathfrak{p}}}^{\mathrm{ab}}$ está dada por $\mathrm{Fr}_{\mathfrak{p}}(x) = x^{q_{\mathfrak{p}}} = x^{q^{\mathrm{gr}\,\mathfrak{p}}} = \mathrm{Fr}_K^{\mathrm{gr}\,\mathfrak{p}}$ puesto que $\mathbb{F}_{q_{\mathfrak{p}}}^{\mathrm{ab}} = \mathbb{F}_q^{\mathrm{ab}}$ y $\overline{\langle \mathrm{Fr}_{\mathfrak{p}} \rangle} = \mathrm{Gal}(\mathbb{F}_{q_{\mathfrak{p}}}^{\mathrm{ab}}/\mathbb{F}_{q_{\mathfrak{p}}}) \subseteq \mathrm{Gal}(\mathbb{F}_{q_{\mathfrak{p}}}^{\mathrm{ab}}/\mathbb{F}_q) = \overline{\langle \mathrm{Fr}_K \rangle}$.

Si $\sigma|_{K_{\mathfrak{p}}\mathbb{F}_{q_{\mathfrak{p}}}^{\mathrm{ab}}} = \mathrm{Fr}_{\mathfrak{p}}^n$, se define $\mathrm{ord}_{\mathfrak{p}}(\sigma) = n$. Por tanto, $\mathrm{ord}_{\mathfrak{p}}(\sigma) = n$ implica $\mathrm{ord}_K(\sigma) = n \cdot \mathrm{gr}\,\mathfrak{p}$ y así, $\mathrm{ord}_K(\sigma) = \mathrm{gr}\,\mathfrak{p} \cdot \mathrm{ord}_{\mathfrak{p}}(\sigma)$ y, en particular,

$$\mathrm{ord}_K(\alpha_{\mathfrak{p}}, K_{\mathfrak{p}}) = \mathrm{gr}\,\mathfrak{p} \cdot \mathrm{ord}_{\mathfrak{p}}(\alpha_{\mathfrak{p}}, K_{\mathfrak{p}}).$$

Ahora veamos que $\mathrm{ord}_{\mathfrak{p}}(\alpha_{\mathfrak{p}}, K_{\mathfrak{p}}) = v_{\mathfrak{p}}(\alpha_{\mathfrak{p}})$. Se tiene $(\alpha_{\mathfrak{p}}, K_{\mathfrak{p}})|_{K_{\mathfrak{p}}\mathbb{F}_{q_{\mathfrak{p}}}^{\mathrm{ab}}} = (\alpha_{\mathfrak{p}}, K_{\mathfrak{p}}\mathbb{F}_{q_{\mathfrak{p}}}^{\mathrm{ab}}/K_{\mathfrak{p}}) = \mathrm{Fr}_{\mathfrak{p}}^{v_{\mathfrak{p}}(\alpha_{\mathfrak{p}})}$ puesto que la extensión $K_{\mathfrak{p}}\mathbb{F}_{q_{\mathfrak{p}}}^{\mathrm{ab}}/K_{\mathfrak{p}}$ es no ramificada.

Se sigue que $\mathrm{ord}_{\mathfrak{p}}(\alpha_{\mathfrak{p}}, K_{\mathfrak{p}}) = v_{\mathfrak{p}}(\alpha_{\mathfrak{p}}) \in \mathbb{Z}$.

Ahora bien, puesto que $(\tilde{\vec{\alpha}}, K) = \prod_{\mathfrak{p} \in \mathbb{Z}_K} (\alpha_{\mathfrak{p}}, K_{\mathfrak{p}})$, se obtiene

$$\begin{aligned} \mathrm{ord}_K\left(\tilde{\vec{\alpha}}, K\right) &= \sum_{\mathfrak{p} \in \mathbb{P}_K} \mathrm{ord}_{\mathfrak{p}}(\alpha_{\mathfrak{p}}, K_{\mathfrak{p}}) = \sum_{\mathfrak{p} \in \mathbb{P}_K} \mathrm{gr}\,\mathfrak{p} \cdot v_{\mathfrak{p}}(\alpha_{\mathfrak{p}}) \\ &= \sum_{\mathfrak{p} \in \mathbb{P}_{\mathfrak{p}}} \mathrm{gr}_{\mathfrak{p}}\,\alpha_{\mathfrak{p}} = \mathrm{gr}(\tilde{\vec{\alpha}}) \in \mathbb{Z}. \end{aligned}$$

En particular, si $\tilde{\vec{\alpha}} \in \mathrm{núc}\,\rho_K$, se tiene $\left(\tilde{\vec{\alpha}}, K\right)|_{K\mathbb{F}_{q_{\mathfrak{p}}}^{\mathrm{ab}}} = \mathrm{Id} = \mathrm{Fr}_K^0$ y $\mathrm{ord}_K(\tilde{\vec{\alpha}}, K) = \mathrm{gr}\left(\tilde{\vec{\alpha}}\right) = 0$ y $\tilde{\vec{\alpha}} \in C_{K,0}$. □

Observación 6.8.25. Si A es un grupo localmente compacto, entonces si A_0 es la componente conexa de la identidad, A_0 es un subgrupo abierto y cerrado de A y A/A_0 es totalmente disconexo.

Proposición 6.8.26. *Se tiene que $A_0 = \bigcap_H H$, donde H recorre todos los subgrupos normales abiertos de A.*

Demostración. Se tiene que para $x \in A$, $x^{-1}A_0x$ es conexo y contiene a la identidad, por lo que $x^{-1}A_0x = A_0$ y A_0 es un subgrupo normal. Ahora, si H es cualquier subgrupo abierto de A, escribimos $A = H \cup H_1$ con $H_1 = \bigcup_{\substack{x \in G \\ x \notin H}} xH$, por lo que H_1 es abierto. Esta es una disconexión pues $1 \in H$. Por tanto $A_0 \subseteq H$ y $A_0 \subseteq \bigcap_H H$.

Recíprocamente, $H := A_0$ es normal y abierto, por lo que $\bigcap_H H \subseteq A_0$. □

Sea H un subgrupo normal cerrado tal que A/H es totalmente disconexo. Sea $\pi : A \longrightarrow A/H$ la proyección natural, la cual es continua. Los abiertos de A/H son los conjuntos U/H con U abierto en A y $H \subseteq U$. Puesto que A/H es totalmente disconexo, $A_0 \subseteq \text{núc}\,\pi = H$ y por tanto la proyección natural $A/A_0 \longrightarrow\!\!\!\!\rightarrow A/H$ es suprayectiva. En otras palabra, A/A_0 es el grupo cociente máximo totalmente disconexo.

Regresando a C_K y $C_{K,0}$ donde K es un campo global de funciones, recordemos que tanto C_K como $C_{K,0}$ son totalmente disconexos (Corolario 6.2.11). Por tanto $\{1\} = \bigcap_{\substack{H \lhd C_K \\ H \text{ abierto}}} H = \bigcap_{\substack{H \lhd C_{K,0} \\ H \text{ abierto de } C_{K,0}}} H$.

Ahora, si H es cualquier subgrupo, ya sea de C_K o de $C_{K,0}$, de índice finito, digamos $[C_K : H] = n < \infty$ o $[C_{K,0} : H] = n < \infty$, se tiene $\text{núc}\,\rho_K \subseteq H$. Así,

$$\text{núc}\,\rho_K \subseteq \bigcap_{[C_{K,0}:H]<\infty} H \subseteq \bigcap_{\substack{H \lhd C_{K,0} \\ H \text{ abierto}}} = D = \{1\},$$

donde D es la componente conexa de la identidad y $D = \{1\}$. Por tanto $\text{núc}\,\rho_K = \{1\}$, esto es, ρ_K es inyectiva.

Teorema 6.8.27. *Si K es un campo global de funciones y si $\rho_K : C_K \longrightarrow G_K^{\text{ab}}$ es el símbolo de la norma residual, entonces ρ_K es inyectiva y no suprayectiva.*

Demostración. Se tiene que $\text{gr}\left(\{\rho_K(\tilde{\tilde{\alpha}}) | \tilde{\tilde{\alpha}} \in C_K\}\right) = \mathbb{Z} \neq \hat{\mathbb{Z}}$, por lo que ρ_K no es suprayectiva. □

Sea $K/\mathbb{F}_q$ un campo global de funciones congruente sobre $\mathbb{F}_q$. Se tiene $\overline{\mathbb{F}_q} = \mathbb{F}_q^{\text{sep}} = \mathbb{F}_q^{\text{ab}} = \bigcup_{n=1}^{\infty} \mathbb{F}_{q^n}$ una cerradura algebraica de $\mathbb{F}_q$. Se tiene que $K\mathbb{F}_q^{\text{ab}}$ es la máxima extensión de constantes de K y además $K\mathbb{F}_q^{\text{ab}} \subseteq K^{\text{ab}}$. Además

$$\text{Gal}(K\mathbb{F}_q^{\text{ab}}/K) \cong \text{Gal}(\mathbb{F}_q^{\text{ab}}/\mathbb{F}_q) = \text{Gal}\Big(\bigcup_{n=1}^{\infty} \mathbb{F}_{q^n}/\mathbb{F}_q\Big) = \text{Gal}\left(\varinjlim_n \mathbb{F}_{q^n}/\mathbb{F}_q\right)$$
$$\cong \varprojlim_n \text{Gal}\left(\mathbb{F}_{q^n}/\mathbb{F}_q\right) \cong \varprojlim_n \left(\mathbb{Z}/n\mathbb{Z}\right) \cong \hat{\mathbb{Z}},$$

la completación $\mathbb{Z}$.

Además, $C_K \cong C_{K,0} \times \mathbb{Z} \xrightarrow{\rho_K} \text{Gal}(K^{\text{ab}}/K) \xrightarrow{\text{rest}} \text{Gal}(K\mathbb{F}_{q^n}/K)$, $\sigma \longmapsto \sigma|_{K\mathbb{F}_{q^n}}$ y se tiene $\text{núc}\left(\text{rest} \circ \rho_K\right) = C_{K,0} \times n\mathbb{Z}$ (Teorema 6.8.3).

Tenemos el isomorfismo inducido,

$$\theta : \frac{C_K}{C_{K,0} \times n\mathbb{Z}} \xrightarrow{\cong} \text{Gal}(K\mathbb{F}_{q^n}/K) \cong \text{Gal}(\mathbb{F}_{q^n}/\mathbb{F}_q) \cong \frac{\mathbb{Z}}{n\mathbb{Z}}.$$

Se sigue que

$$\tilde{\rho}_K : \frac{C_K}{C_{K,0}} \longrightarrow \mathrm{Gal}(K\mathbb{F}_q^{\mathrm{ab}}/K) \cong \hat{\mathbb{Z}}.$$

En particular obtenemos nuevamente que ρ_K no es suprayectiva y que $C_{K,0} = \mathrm{núc}\,\rho_K|_{\mathbb{Z}}$. Más precisamente, si $\tilde{\vec{\alpha}} \in C_{K,0}$, se tiene $\rho_K\big(\tilde{\vec{\alpha}}\big)|_{K\mathbb{F}_q^{\mathrm{ab}}} = \big(\tilde{\vec{\alpha}}, K\big)|_{K\mathbb{F}_q^{\mathrm{ab}}} = 1$, por lo que $\big(\tilde{\vec{\alpha}}, K\big) \in \mathrm{Gal}(K^{\mathrm{ab}}/K\mathbb{F}_q^{\mathrm{ab}})$.

Ahora bien, $\rho_K(C_K)$ es denso en $G_K^{\mathrm{ab}} = \mathrm{Gal}(K^{\mathrm{ab}}/K)$ y $C_{K,0}$ es compacto por lo que $\rho_K(C_{K,0})$ es denso y compacto en $\mathrm{Gal}(K^{\mathrm{ab}}/K\mathbb{F}_q^{\mathrm{ab}})$, por tanto es suprayectiva y como ρ_K es inyectiva obtenemos que

$$\rho_K|_{C_{K,0}} : C_{K,0} \longrightarrow \mathrm{Gal}(K^{\mathrm{ab}}/K\mathbb{F}_q^{\mathrm{ab}})$$

es un isomorfismo algebraico y topológico.

Sea $\pi : J_K \longrightarrow C_K = J_K/K^*$ el epimorfismo natural. Se tiene el siguiente diagrama conmutativo con filas exactas

$$\begin{array}{ccccccccc}
1 & \longrightarrow & J_{K,0} & \hookrightarrow & J_K & \overset{\mathrm{gr}}{\twoheadrightarrow} & \mathbb{Z} & \longrightarrow & 0 \\
 & & \downarrow{\scriptstyle \pi} & \circlearrowright & \downarrow{\scriptstyle \pi} & \circlearrowright & \downarrow{\scriptstyle \mathrm{Id}} & & \\
1 & \longrightarrow & C_{K,0} & \hookrightarrow & C_K & \overset{\mathrm{gr}}{\twoheadrightarrow} & \mathbb{Z} & \longrightarrow & 0
\end{array}$$

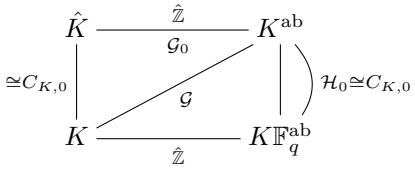
Sea $\vec{\alpha}_1 \in J_K$ es de grado 1, entonces para $\vec{\alpha} \in J_K$ arbitrario, el mapeo $\vec{\alpha} \longrightarrow \big(\vec{\alpha}_1^{-\,\mathrm{gr}\,\vec{\alpha}} \cdot \vec{\alpha}, \vec{\alpha}_1^{\mathrm{gr}\,\vec{\alpha}}\big)$ induce isomorfismos

$$J_K \cong J_{K,0} \times \langle \vec{\alpha}_1 \rangle \quad \text{y} \quad C_K \cong C_{K,0} \times \langle \tilde{\vec{\alpha}}_1 \rangle.$$

Como consecuencia del Teorema 6.8.24, se obtiene que ρ_K nos da un isomorfismo topológico:

Teorema 6.8.28. *Sean $\mathcal{G} = \mathrm{Gal}(K^{\mathrm{ab}}/K) = G_K^{\mathrm{ab}}$, $\mathcal{H}_0 = \mathrm{Gal}(K^{\mathrm{ab}}/K\mathbb{F}_q^{\mathrm{ab}})$ y $\mathcal{G}_0 = \mathrm{Gal}(K\mathbb{F}_q^{\mathrm{ab}}/K) \cong \hat{\mathbb{Z}}$. Entonces $\mathcal{G}/\mathcal{H}_0 \cong \mathcal{G}_0$ y ρ_K es un isomorfismo algebraico y topológico de $C_{K,0}$ sobre $\mathcal{H}_0$, es decir, $C_{K,0} \overset{\rho_K}{\cong} \mathrm{Gal}(K^{\mathrm{ab}}/K\mathbb{F}_q^{\mathrm{ab}})$ y $\mathcal{G}$ es el producto directo de $\mathcal{H}_0$ y $\mathcal{G}_0$,*

$$\mathcal{G} \cong \mathcal{H}_0 \times \mathcal{G}_0, \quad \mathrm{Gal}(K^{\mathrm{ab}}/K) \cong \mathrm{Gal}(K^{\mathrm{ab}}/K\mathbb{F}_q^{\mathrm{ab}}) \times \mathrm{Gal}(K\mathbb{F}_q^{\mathrm{ab}}/K).$$



El campo de constantes de $\hat{K} := \big(K^{\mathrm{ab}}\big)^{\mathcal{G}_0}$ es $\mathbb{F}_q$.

Demostración. Sea $\mathbb{F}_{q^n}$ el campo de constantes del campo $\hat{K}$. Se tiene que $K = \hat{K} \cap K\mathbb{F}_q^{\mathrm{ab}} \supseteq K\mathbb{F}_{q^n} \cap K\mathbb{F}_q^{\mathrm{ab}} \supseteq \mathbb{F}_{q^n}$, por lo que $\mathbb{F}_{q^n} \subseteq K$ de donde se sigue que $n = 1$ y que $\mathbb{F}_q$ es el campo de constantes de $\hat{K}$.

Se tiene que $\mathcal{H}_0 \cong C_{K,0}$ tanto algebraica como topológicamente. Ahora bien, puesto que $\mathcal{G}_0 \cong \hat{\mathbb{Z}}$, la sucesión

$$1 \longrightarrow \mathcal{H}_0 \longrightarrow \mathcal{G} \xrightarrow{\pi} \mathcal{G}_0 \longrightarrow 1$$

se escinde pues $\hat{\mathbb{Z}} = \overline{\langle \mathrm{Fr}_K \rangle}$ es la cerradura de $\mathbb{Z}$ en $\mathcal{G}_0$. Más precisamente, si $x \in \mathcal{G}$ es tal que $\pi(x) = \mathrm{Fr}_K$, entonces $\varphi(\mathrm{Fr}_K) = x$ es el mapeo de escisión, extendiéndolo de manera continua a todo $\hat{\mathbb{Z}}$. □

Detallando más el Teorema 6.8.28, el siguiente resultado nos da la información relevante acerca de las extensiones de constantes.

Teorema 6.8.29. *Existen dos diagramas conmutativos de sucesiones exactas. En cada diagrama, la flecha vertical de la izquierda es un isomorfismo de grupos topológicos.*

$$\begin{array}{ccccccccc}
1 & \longrightarrow & C_{K,0} & \xrightarrow{i} & C_K & \xrightarrow{\mathrm{gr}} & \mathbb{Z} & \longrightarrow & 0 \\
 & & \cong \downarrow & & \downarrow & & \downarrow & & \\
 & & \rho'_K = \rho_K|_{C_{K,0}} & & \rho_K & & \rho_{\mathbb{F}_q} & & \\
1 & \longrightarrow & \mathrm{Gal}(K^{\mathrm{ab}}/K\mathbb{F}_q^{\mathrm{ab}}) & \xrightarrow[i]{} & \mathrm{Gal}(K^{\mathrm{ab}}/K) & \xrightarrow[\mathrm{rest}]{} & \mathrm{Gal}(K\mathbb{F}_q^{\mathrm{ab}}/K) & \longrightarrow & 1 \\
 & & & & & & \| & & \\
 & & & & & & \mathrm{Gal}(\mathbb{F}_q^{\mathrm{ab}}/\mathbb{F}_q) \cong \hat{\mathbb{Z}} & &
\end{array}$$

$$\begin{array}{ccccccccc}
1 & \longrightarrow & I_{K,0} & \xrightarrow{i} & I_K & \xrightarrow{\mathrm{gr}} & \mathbb{Z} & \longrightarrow & 0 \\
 & & \cong \downarrow & & \downarrow & & \downarrow \rho_{\mathbb{F}_q} & & \\
1 & \longrightarrow & \mathrm{Gal}(K^{\mathrm{nr}}/K\mathbb{F}_q^{\mathrm{ab}}) & \xrightarrow[i]{} & \mathrm{Gal}(K^{\mathrm{nr}}/K) & \xrightarrow[\mathrm{rest}]{} & \mathrm{Gal}(K\mathbb{F}_q^{\mathrm{ab}}/K) & \longrightarrow & 1
\end{array}$$

Aquí se tiene $\rho_{\mathbb{F}_q} \colon \mathbb{Z} \longrightarrow \mathrm{Gal}(K^{\mathrm{ab}}/K)$ *definida por* $\rho_{\mathbb{F}_q}(n) = \mathrm{Fr}_K^n$, *donde* Fr_K *denota al automorfismo de Frobenius.*

Demostración. En el primer diagrama, $(\rho_{\mathbb{F}_q} \circ \mathrm{gr})(\tilde{\vec{x}}) = \rho_{\mathbb{F}_q}(\mathrm{gr}\,\tilde{\vec{x}}) = \mathrm{Fr}_K^{\mathrm{gr}\,\tilde{\vec{x}}}$. Por el otro lado, $\mathrm{rest}\,\rho_K(\tilde{\vec{x}}) = \rho_{K\mathbb{F}_q^{\mathrm{ab}}}(\vec{x}) = \mathrm{Fr}_K^{\mathrm{gr}\,\tilde{\vec{x}}}$.

El lado izquierdo del diagrama es conmutativo, es decir $i \circ \rho'_K = \rho_K \circ i$ y $\mathrm{núc}(i \circ \rho'_K) = \mathrm{núc}\,\rho'_K = \mathrm{núc}(\rho_K \circ i) = 0$ pues se tiene que ρ_K es inyectiva en el caso de campos de funciones. Por lo tanto ρ'_K es una inyección y tenemos que $\mathrm{im}\,\rho'_K = \mathrm{núc}\,\mathrm{rest} = \mathrm{Gal}(K^{\mathrm{ab}}/K\mathbb{F}_q^{\mathrm{ab}})$.

Ahora bien, por el Lema de la Serpiente (Teorema 4.1.8), se tiene la sucesión exacta

$$1 \to \text{núc}\,\rho'_K \to \text{núc}\,\rho_K \to \text{núc}\,\rho_{\mathbb{F}_q} \to$$
$$\to \text{conúcleo}\,\rho'_K \to \text{conúcleo}\,\rho_K \to \text{conúcleo}\,\rho_{\mathbb{F}_q} \to 1.$$

Usando que ρ_K es inyectiva en el caso de campos de funciones, que $\text{conúcleo}\,\rho_K = \hat{\mathbb{Z}}/\mathbb{Z}$, que $\rho_{\mathbb{F}_q}$ es inyectiva y que $\text{conúcleo}\,\rho_{\mathbb{F}_q} = \hat{\mathbb{Z}}/\mathbb{Z}$, se sigue

$$1 \to \text{núc}\,\rho'_K \to 1 \to 1 \to \text{conúcleo}\,\rho'_K \to \hat{\mathbb{Z}}/\mathbb{Z} \to \hat{\mathbb{Z}}/\mathbb{Z} \to 0$$

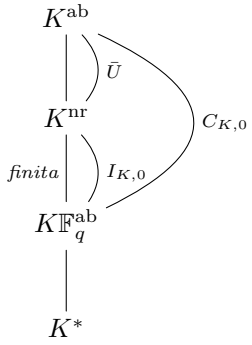
es exacta por lo $\text{núc}\,\rho'_K = 1$ y $\text{conúcleo}\,\rho'_K = 1$ de donde se sigue que ρ'_K es un isomorfismo.

El segundo diagrama, proviene del primero al dividir la primera sucesión entre $\bar{U} = UK^*/K^*$, con $U = \prod_{\mathfrak{p}\in\mathbb{P}_K} U_{\mathfrak{p}}$: $C_{K,0}/\bar{U} = I_{K,0}$, $C_K/\bar{U} = I_K$ y usando que $\rho_K(\bar{U}) = \text{Gal}(K^{\text{ab}}/K^{\text{nr}})$ pues $C_K/\bar{U} \cong \text{Gal}(K^{\text{nr}}/K)$ según el TCCG. □

Notemos que, en particular, se tiene que $\bar{U}$ corresponde a la máxima extensión no ramificada abeliana de K.

Corolario 6.8.30. *Se tiene*

$$C_{K,0} \cong \text{Gal}(K^{\text{ab}}/K\mathbb{F}_q^{\text{ab}}), \quad I_{K,0} \cong \text{Gal}(K^{\text{nr}}/K\mathbb{F}_q^{\text{ab}}).$$



En particular $K^{\text{nr}}/K\mathbb{F}_q^{\text{ab}}$ *es una extensión finita.* □

En adición tenemos $C_K = \langle\tilde{\vec{\alpha}}_1\rangle \times C_{K,0}$, con $\vec{\alpha} \in J_K$ tal que $|\tilde{\vec{\alpha}}_1| = q^{-1}$ o $\text{gr}\,\tilde{\vec{\alpha}}_1 = 1$ y C_K es isomorfo a $\mathbb{Z} \times C_{K,0}$ pero no de manera canónica, esto es, $C_{K,0}$ es único no así la copia de $\mathbb{Z}$ que podemos seleccionar dentro de C_K para obtener el producto directo. Notemos que tenemos una copia de $\mathbb{Z}$ en C_K para cada $\tilde{\vec{\alpha}}_1 \in C_K$ con $\text{gr}\,\tilde{\vec{\alpha}}_1 = 1$.

Definición 6.8.31. Se define otra topología en C_K: las vecindades de 1 son los subgrupos abiertos de índice finito en la topología usual de C_K. Esta nueva topología se llama la *topología de clase*

La topología de clase es estrictamente menos fina que la topología usual, como veremos en el Teorema 6.8.32.

Teorema 6.8.32. *La topología de clase coincide con la original en $C_{K,0}$, induce la* topología de ideales *sobre $\mathbb{Z}$ y la topología producto sobre $\mathbb{Z}\times C_{K,0}$. La topología de ideales de $\mathbb{Z}$ consiste de la topología generada por las vecindades de 0 por los ideales $\{n\mathbb{Z}\}_{n\neq 0}$. Es decir, V es una vecindad de 0 si contiene a algún ideal $n\mathbb{Z}$ con $n\neq 0$. La completación de $\mathbb{Z}$ con respecto a esta topología es el anillo de Prüfer:*

$$\hat{\mathbb{Z}} = \varprojlim_{n} \mathbb{Z}/n\mathbb{Z}.$$

Demostración. Sea B un subgrupo abierto de índice finito en C_K. Sea $\tilde{\vec{\alpha}}\in B$ con $\operatorname{gr}\tilde{\vec{\alpha}} = \min\{n\in\mathbb{N} \mid \text{existe } \tilde{\vec{\beta}}\in B \text{ con } \operatorname{gr}\tilde{\vec{\beta}} = n\}$. Sea $B_0 = B\cap C_{K,0}$ y $B = \bigcup_{n\in\mathbb{Z}} \tilde{\vec{\alpha}}^n B_0$. Ahora bien, B_0 es un conjunto abierto de C_K pues $C_{K,0}$ es abierto en C_K (Proposición 6.2.13).

Veremos que B_0 es de índice finito en $C_{K,0}$. Sea $\mathfrak{m} = \prod_{\mathfrak{p}} \mathfrak{p}^{\gamma_{\mathfrak{p}}}$ con $\gamma_{\mathfrak{p}}\geq 0$ para toda $\mathfrak{p}$ y $\gamma_{\mathfrak{p}} = 0$ para casi toda $\mathfrak{p}$. $\mathfrak{m}$ recibe el nombre de *modulus*. Un sistema fundamental de vecindades de 1 en J_K está dado por los grupos

$$J_K^{\mathfrak{m}} = \prod_{\mathfrak{p}\nmid\mathfrak{m}} U_{\mathfrak{p}} \times \prod_{\mathfrak{p}\mid\mathfrak{m}} U_{\mathfrak{p}}^{(\gamma_{\mathfrak{p}})},$$

donde $U_{\mathfrak{p}}^{(\gamma_{\mathfrak{p}})}$ son los grupos consistentes de los elementos $\alpha_{\mathfrak{p}}\in K_{\mathfrak{p}}^*$ tales que $\alpha_{\mathfrak{p}}\equiv 1 \bmod \mathfrak{p}^{\gamma_{\mathfrak{p}}}$ para $\mathfrak{p}|\mathfrak{m}$. Se tiene que $U_{\mathfrak{p}}^{(\gamma_{\mathfrak{p}})}\subseteq U_{\mathfrak{p}}$ y que si $\vec{\alpha}\in J_K^{\mathfrak{m}}$, entonces $\operatorname{gr}\vec{\alpha} = 0$. Sea $C_L^{\mathfrak{m}} := J_K^{\mathfrak{m}}K^*/K^*$, los cuales forman un sistema fundamental de vecindades de $1\in C_K$ y $C_K^{\mathfrak{m}}\subseteq C_{K,0}$. Se tiene

$$[C_{K,0} : C_K^{\mathfrak{m}}] = [C_{K,0} : U_K K^*/K^*][U_K K^*/K^* : C_K^{\mathfrak{m}}],$$

donde $U_K = \prod_{\mathfrak{p}} U_{\mathfrak{p}}$. Ahora bien, $C_{K,0}/\big(U_K K^*/K^*\big) \cong I_{K,0}$, el cual es un grupo finito.

Por otro lado, $\big[U_{\mathfrak{p}} : U_{\mathfrak{p}}^{(\gamma_{\mathfrak{p}})}\big] < \infty$, por lo que

$$[U_K K^*/K^* : C_K^{\mathfrak{m}}] \leq \prod_{\mathfrak{p}\mid\mathfrak{m}} \big[U_{\mathfrak{p}} : U_{\mathfrak{p}}^{(\gamma_{\mathfrak{p}})}\big] < \infty.$$

El subgrupo abierto B_0 debe contener a algún subgrupo abierto $C_K^{\mathfrak{m}}$ por lo que $[C_{K,0} : B_0] < \infty$. Por otro lado, $B\cap\mathbb{Z}$ es un subgrupo de índice finito en $\mathbb{Z}$ por lo que $B\cap\mathbb{Z} = n\mathbb{Z}$ para algún $n\in\mathbb{N}$. Por tanto, la topología inducida en $\mathbb{Z}$ es la topología de ideales. □

Definición 6.8.33. Se define $\hat{C}_K := C_{K,0}\times\big(\tilde{\vec{\alpha}}_1\big)^{\hat{\mathbb{Z}}} \cong C_{K,0}\times\hat{\mathbb{Z}}$, es decir, $\hat{C}_K \cong C_{K,0}\times\big\{\tilde{\vec{\alpha}}_1^{\mu}\big\}_{\mu\in\hat{\mathbb{Z}}}$.

Observación 6.8.34. Se tiene que

$$\hat{C}_K \cong \varprojlim_{B} C_K/B,$$

donde B recorre los subgrupos abiertos de índice finito de C_K.

Es decir, $\hat{C}_K$ es la completación en la topología de Krull de C_K.

Observación 6.8.35. Puesto que tanto $C_{K,0}$ como $\hat{\mathbb{Z}}$ son compactos, se sigue que $\hat{C}_K$ es compacto.

Se tiene que $\rho_K : C_K \longrightarrow \mathrm{Gal}(K^{\mathrm{ab}}/K)$ es uniformemente continua en la nueva topología, de hecho, si U es un abierto de $G := \mathrm{Gal}(K^{\mathrm{ab}}/K)$, existe un subgrupo abierto H de G con $H \subseteq U$ pues los subgrupos abiertos definen la topología de Krull. Entonces H es de índice finito. Sea $L := (K^{\mathrm{ab}})^H$ el campo fijo bajo H y se tienen $\mathrm{Gal}(L/K) \cong G/H$. De la ley de reciprocidad, tenemos

$$\rho_K|_L = \psi_{L/K} : C_K/\,\mathrm{N}_{L/K}(C_L) \xrightarrow{\cong} G/H.$$

Ahora bien, $\mathrm{N}_{L/K}\, C_L$ es abierto en C_K y si $\tilde{\vec{\alpha}}\tilde{\vec{\beta}}^{-1} \in \mathrm{N}_{L/K}\, C_L$, entonces $\rho_K\big(\tilde{\vec{\alpha}}\tilde{\vec{\beta}}^{-1}\big) = \rho_K(\tilde{\vec{\alpha}})\rho_K(\tilde{\vec{\beta}})^{-1} \in H$, de donde obtenemos que ρ_K es uniformemente continua.

Por tanto, ρ_K se extiende de manera única a la completación, en la nueva topología, $\hat{C}_K$ de C_K y $\hat{C}_K \cong C_{K,0} \times \hat{\mathbb{Z}}$ el cual es compacto. Por tanto $\rho_K\big(\hat{C}_K\big)$ es denso y compacto, de donde se sigue que $\rho_K\big(\hat{C}_K\big) \cong G$. Puesto que ρ_K es inyectiva, se tiene $\rho_K : \hat{C}_K \longrightarrow G$ es un isomorfismo tanto algebraico como topológico.

Con todos estos elementos, se demuestra el Teorema de Existencia para campos de funciones. De hecho se hace más, se da una correspondencia biyectiva entre subgrupos cerrados de $\hat{C}_K$ y los subgrupos cerrados de $\mathcal{G} = \mathrm{Gal}(K^{\mathrm{ab}}/K)$.

Teorema 6.8.36 (Teorema de Existencia para campo de funciones). *Sea K un campo global de funciones. Sea H un subgrupo abierto de índice finito en C_K. Entonces existe una extensión abeliana finita L de K tal que $H = \mathcal{N}_L = \mathrm{N}_{L/K}\, C_L$ Más aún, L es el campo fijo de $\rho_K(H)$: $L = (K^{\mathrm{ab}})^{\rho_K(H)}$ donde $\rho_K = (\_, K) \colon C_K \longrightarrow \mathrm{Gal}(K^{\mathrm{ab}}/K)$ es el símbolo de la norma residual u homomorfismo de Artin.*

Demostración. Sea H un subgrupo abierto de índice finito de C_K. Sea $H_0 = H \cap C_{K,0}$. Puesto que

$$\frac{H}{H_0} \cong \frac{H}{(H \cap C_{K,0})} \cong \frac{HC_{K,0}}{C_{K,0}} \subseteq \frac{C_K}{C_{K,0}} \cong \mathbb{Z},$$

se tiene que $H = \cup_{n\in\mathbb{Z}} h^n H_0$ para algún $h \in H$. Por otro lado, debido a que tenemos el isomorfismo $C_K = C_{K,0} \times \mathbb{Z} = C_{K,0} \times \langle \tilde{\vec{\alpha}}_1 \rangle$ con $|\tilde{\vec{\alpha}}_1| = q^{-1}$, podemos tomar $h = \tilde{\vec{\alpha}}_1^{\,d}$ para alguna d. Se tiene que $\hat{\mathbb{Z}}/d\hat{\mathbb{Z}} \cong \mathbb{Z}/d\mathbb{Z}$ de manera natural ($\mathbb{Z} \hookrightarrow \hat{\mathbb{Z}} \xrightarrow[\varphi]{\text{mód } d} \hat{\mathbb{Z}}/d\hat{\mathbb{Z}}$, $\mathrm{núc}\,\varphi = d\mathbb{Z}$ y se prueba que φ es un epimorfismo).

Sea $\hat{H} := H_0 \times d\hat{\mathbb{Z}}$, esto es, $\hat{H}$ es la completación de H en la nueva topología. Entonces $\hat{C}_K = C_{K,0} \times \hat{\mathbb{Z}}$, por lo que

$$\frac{\hat{C}_K}{\hat{H}} = \frac{C_{K,0} \times \hat{\mathbb{Z}}}{H_0 \times d\hat{\mathbb{Z}}} \cong \frac{C_{K,0}}{H_0} \times \frac{\mathbb{Z}}{d\mathbb{Z}} \cong \frac{C_{K,0} \times \mathbb{Z}}{H_0 \times d\mathbb{Z}} \cong \frac{C_K}{H}$$

lo cual implica $[C_K : H] = d[C_{K,0} : H_0] = [\hat{C}_K : \hat{H}]$.

Sea $\mathcal{H} = \rho_K(\hat{H}) \subseteq \mathrm{Gal}(K^{\mathrm{ab}}/K) = \mathcal{G}$. Se tiene que $\mathcal{H}$ es cerrado en $\mathcal{G}$ y pues que ρ_K es un isomorfismo

$$[\mathcal{G} : \mathcal{H}] = [\rho_K(\hat{C}_K) : \rho_K(\hat{H})] \underset{\substack{\uparrow \\ \rho_K \text{ es un} \\ \text{isomorfismo}}}{=} [\hat{C}_K : \hat{H}] = [C_K : H],$$

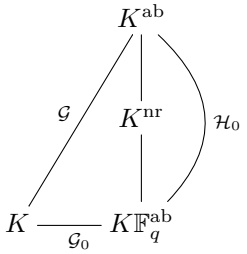
es decir, $[C_K : H] = [\mathcal{G} : \mathcal{H}]$.

Sea L el campo fijo de K^{ab} por $\mathcal{H} = \rho_K(\hat{H})$, es decir, $L := (K^{\mathrm{ab}})^{\mathcal{H}}$. Entonces $[L : K] = [\mathcal{G} : \mathcal{H}] = [C_K : H]$.

Además, $\mathrm{Gal}(L/K) \cong \frac{\mathrm{Gal}(K^{\mathrm{ab}}/K)}{\mathrm{Gal}(K^{\mathrm{ab}}/L)} \cong \frac{\mathcal{G}}{\mathcal{H}} \cong \frac{C_K}{\mathrm{N}_{L/K}\, C_L}$ y $\rho_K(C_K) \subseteq \mathcal{G}$, por lo que $\rho_K(\mathrm{N}_{L/K}\, C_L) \subseteq \mathcal{H}$ lo cual implica que $\mathrm{N}_{L/K}\, C_L \subseteq H$. Finalmente, puesto que $[C_K : \mathrm{N}_{L/K}\, C_L] = [L : K] = [C_K : H]$, se sigue que $\mathcal{N}_L = \mathrm{N}_{L/K}\, C_L = H$. □

6.8.5. Extensiones geométricas y de constantes de campos de funciones

Analicemos con más detalle parte de la discusión anterior. Sea K^{nr} la máxima extensión no ramificada de K contenida en K^{ab}, donde K es un campo global de funciones. Se tiene que $K\mathbb{F}_q^{\mathrm{ab}} \subseteq K^{\mathrm{nr}}$. Consideremos el siguiente diagrama



donde $\mathcal{H}_0 = \mathrm{Gal}(K^{\mathrm{ab}}/K\mathbb{F}_q^{\mathrm{ab}}) \cong C_{K,0}$,
$\mathcal{G}_0 \cong \mathcal{G}/\mathcal{H}_0 \cong \mathrm{Fr}_K^{\hat{\mathbb{Z}}}$, $\mathcal{G} = \mathrm{Gal}(K^{\mathrm{ab}}/K)$.

Sea $\sigma \in \mathcal{G}$ con $\sigma|_{K\mathbb{F}_q^{\mathrm{ab}}} = \mathrm{Fr}_K^{\mathrm{ord}\,\sigma}$. En general tenemos $\sigma|_{K\mathbb{F}_q^{\mathrm{ab}}} \in \mathcal{G}_0 \cong \overline{\langle \mathrm{Fr}_K \rangle} = \mathrm{Fr}_K^{\hat{\mathbb{Z}}}$.

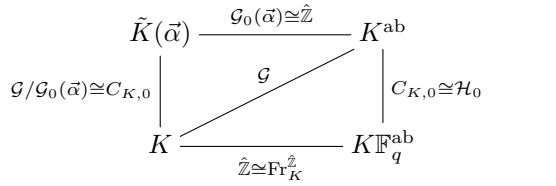
Sea $\rho_K \colon C_K \longrightarrow \mathcal{G}$ el mapeo de reciprocidad. Se tiene $\mathrm{ord}\, \rho_K\big(\tilde{\vec{\alpha}}\big) = \mathrm{gr}\, \tilde{\vec{\alpha}}$. En particular se tiene que $\mathrm{ord}\, \rho_K\big(\tilde{\vec{\alpha}}\big) \in \mathbb{Z}$ y no en $\hat{\mathbb{Z}}$. Además $\mathcal{H}_0 \cong C_{K,0}$ bajo el mapeo ρ_K, $\mathcal{G} \cong \mathcal{H}_0 \times \mathcal{G}_0$, $\mathcal{G}_0 = \mathrm{Gal}(K\mathbb{F}_q^{\mathrm{ab}}/K)$ y la sucesión exacta

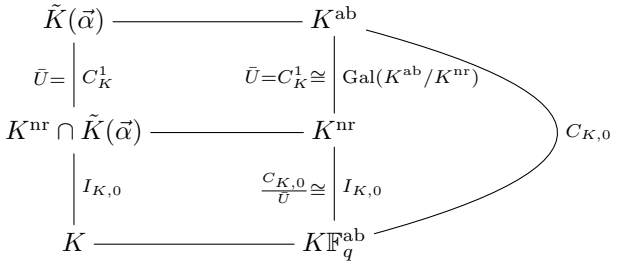
$$1 \longrightarrow \mathcal{H}_0 \longrightarrow \mathcal{G} \longrightarrow \mathcal{G}_0 \longrightarrow 1$$

se escinde con $\mathrm{Fr}_K^{\hat{\mathbb{Z}}} \cong \mathcal{G}_0 \longrightarrow \mathcal{G}$, $\mathrm{Fr}_K \mapsto \sigma$ con $\operatorname{ord}\sigma = 1$, esto es, $\sigma|_{K\mathbb{F}_q^{\mathrm{ab}}} = \mathrm{Fr}_K$ y cada uno de estos se puede obtener mediante $\vec{\alpha} \in J_K$ con $\operatorname{gr}\vec{\alpha} = 1$, $\rho_K(\tilde{\vec{\alpha}}) = \sigma$.

Para cada $\vec{\alpha} \in J_K$ tal que $\operatorname{gr}\vec{\alpha} = 1$ definimos un campo $\tilde{K}(\vec{\alpha})$ con $\tilde{K}(\vec{\alpha}) := (K^{\mathrm{ab}})^{\mathcal{G}_0(\vec{\alpha})}$ donde $\mathcal{G}_0(\vec{\alpha}) \subseteq \mathcal{G}$ es la escisión $\psi\colon \mathcal{G}_0 \longrightarrow \mathcal{G}_0(\vec{\alpha}) \subseteq \mathcal{G}$, $\mathrm{Fr}_K \longmapsto \rho_K(\vec{\alpha})$.

Se tiene que $\tilde{K}(\vec{\alpha}) \cap K\mathbb{F}_q^{\mathrm{ab}} = K$ y por tanto el campo de constantes de $\tilde{K}(\vec{\alpha})$ es $\mathbb{F}_q$. Con el isomorfismo $\hat{C}_K = C_{K,0} \times \tilde{\vec{\alpha}}^{\hat{\mathbb{Z}}}$ con $\operatorname{gr}\vec{\alpha} = 1$, $\rho_K\colon \hat{C}_K \longrightarrow \mathcal{G} = \mathrm{Gal}(K^{\mathrm{ab}}/K)$, $\rho_K(C_{K,0}) = \mathcal{H}_0$, $\rho_K(\tilde{\vec{\alpha}}) \in \mathcal{G}$, tenemos los diagramas





donde $\bar{U} = \frac{UK^*}{K^*}$ y donde el grupo de normas de $K^{\mathrm{nr}} \cap \tilde{K}(\vec{\alpha})$ es $\bar{U} \times \mathbb{Z}$ y

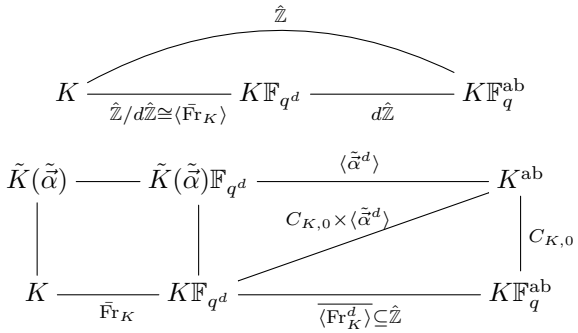
$$\frac{C_K}{\bar{U} \times \mathbb{Z}} \cong \frac{C_{K,0} \times \mathbb{Z}}{\bar{U} \times \mathbb{Z}} \cong \frac{C_{K,0}}{\bar{U}} \cong I_{K,0}.$$

Todas las extensiones de K contenidas en $\tilde{K}(\vec{\alpha})$ tienen campo de constantes $\mathbb{F}_q$ y la máxima extensión de K no ramificada dentro de $\tilde{K}(\vec{\alpha})$ es $K^{\mathrm{nr}} \cap \tilde{K}(\vec{\alpha})$ y

$$\mathrm{Gal}(K^{\mathrm{nr}} \cap \tilde{K}(\vec{\alpha})/K) \cong \mathrm{Gal}(K^{\mathrm{nr}}/K\mathbb{F}_q^{\mathrm{ab}}) \cong I_{K,0}.$$

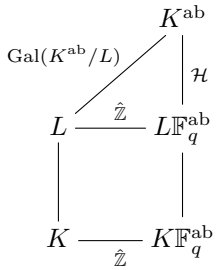
Notemos que $\mathcal{G}_0(\vec{\alpha}) \cong \vec{\alpha}^{\hat{\mathbb{Z}}} \cong \hat{\mathbb{Z}}$, por lo que $K^{\mathrm{nr}} \cap \tilde{K}(\vec{\alpha}) = \tilde{K}(\vec{\alpha})^{\mathrm{nr}}$ corresponde a $C_K^1 \times \mathcal{G}_0(\vec{\alpha}) \cong C_K^1 \times \vec{\alpha}^{\hat{\mathbb{Z}}}$, donde $C_K^1 = \mathrm{Gal}(K^{\mathrm{ab}}/K^{\mathrm{nr}})$. Es decir, $\tilde{K}(\vec{\alpha})^{\mathrm{nr}} = (K^{\mathrm{ab}})^{C_K^1 \times \mathcal{G}_0(\vec{\alpha})}$.

Ahora bien, $\tilde{K}(\vec{\alpha})\mathbb{F}_q^{\mathrm{ab}} = K^{\mathrm{ab}}$, $\mathrm{Gal}(K^{\mathrm{ab}}/\tilde{K}(\vec{\alpha})) \cong \hat{\mathbb{Z}}$ y $K^{\mathrm{ab}}/\tilde{K}(\vec{\alpha})$ es una extensión de constantes. Si $K\mathbb{F}_{q^d}$ es la extensión de constantes de grado d sobre K, entonces $\mathrm{Gal}(K\mathbb{F}_{q^d}/K) = \langle \bar{\mathrm{Fr}}_K \rangle$ donde $\bar{\mathrm{Fr}}_K := \mathrm{Fr}_K$ mód $d\hat{\mathbb{Z}}$, es decir

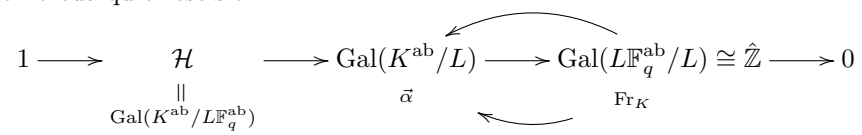


esto es, la extensión de constantes de grado d de K corresponde al grupo $C_{K,0} \times \langle \tilde{\vec{\alpha}}^d \rangle \subseteq C_K$ (lo cual ya se había obtenido en el Teorema 6.8.3) y la extensión de constantes de grado d de $\tilde{K}(\vec{\alpha})$ corresponde al grupo $\langle \tilde{\vec{\alpha}}^d \rangle$. Es decir $C_{K,0} \times \langle \tilde{\vec{\alpha}}^d \rangle$ es el grupo de normas de $K\mathbb{F}_{q^d}$. Aquí estamos identificando, bajo el mapeo de reciprocidad ρ_K, $\tilde{\vec{\alpha}}$ con Fr_K y $C_{K,0}$ con $\mathcal{H}_0$.

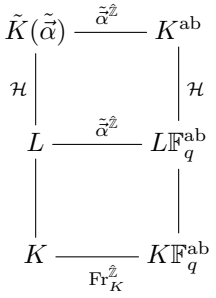
Sea ahora L/K una extensión abeliana finita y geométrica, es decir, el campo de constantes de L es $\mathbb{F}_q$. Entonces $L \cap K\mathbb{F}_q^{\mathrm{ab}} = K$.



Sea $\mathcal{H} = \mathrm{Gal}(K^{\mathrm{ab}}/L\mathbb{F}_q^{\mathrm{ab}})$ y $\mathrm{Gal}(K^{\mathrm{ab}}/L) \cong \mathcal{H} \times \hat{\mathbb{Z}}$ como antes y $\hat{\mathbb{Z}}$ se obtiene como cualquier escisión:



y $\mathrm{gr}\,\vec{\alpha} = 1$. Por tanto $\hat{\mathbb{Z}} \cong \langle \vec{\alpha}^{\hat{\mathbb{Z}}} \rangle$ y $(K^{\mathrm{ab}})^{\hat{\mathbb{Z}}} = \tilde{K}(\vec{\alpha})$ de antes. Es decir, $L \subseteq \tilde{K}(\vec{\alpha})$ para algún $\vec{\alpha}$.



Es decir, toda extensión abeliana finita geométrica está contenida en alguna de las extensiones $\tilde{K}(\vec{\alpha})$.

6.8.6. Sobre los campos de constantes

Teorema 6.8.37. *Sea $B < C_K$ un subgrupo abierto de índice finito. Sea $d := \min\{n \in \mathbb{N} \mid$ existe $\tilde{\vec{b}} \in B$ con $\operatorname{gr}\tilde{\vec{b}} = n\}$. Entonces si E es el campo asociado a B, es decir $B = \mathrm{N}_{E/K} C_E$, el campo de constantes de E es $\mathbb{F}_{q^d}$.*

Demostración. Primero notemos que para cualquier campo F, el campo de constantes de F es $\mathbb{F}_{q^r}$ donde $F \cap K\mathbb{F}_q^{\mathrm{ab}} = K\mathbb{F}_{q^r}$.

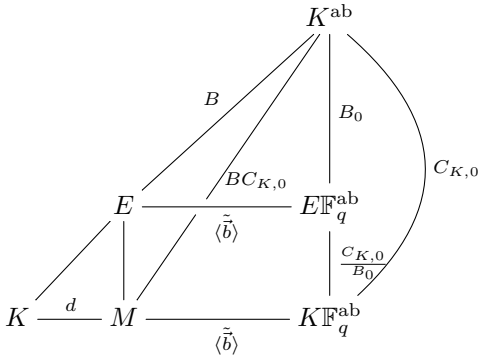
Consideremos $\tilde{\vec{b}} \in B$ con $\operatorname{gr}\tilde{\vec{b}} = d$. Sea $B_0 := B \cap C_{K,0}$. Se tiene

$$\frac{B}{B_0} = \frac{B}{B \cap C_{K,0}} \cong \frac{BC_{K,0}}{C_{K,0}} \subseteq \frac{C_K}{C_{K,0}} \cong \mathbb{Z}.$$

Veamos que $[B : B_0] = \infty$. Esto es claro de lo anterior, pues de otra forma, al tener $B/B_0 \subseteq \mathbb{Z}$, necesariamente $B = B_0 \subseteq C_{K,0}$ pero entonces $[C_K : B] \geq [C_K : C_{K,0}] = \infty$. En resumen $B/B_0 \cong \mathbb{Z}$. Este isomorfismo viene dado por la sucesión exacta de grupos

$$1 \longrightarrow B_0 \longrightarrow B \underset{\varphi}{\overset{\mathrm{gr}}{\rightleftarrows}} d\mathbb{Z} \longrightarrow 0,$$

donde φ es el mapeo de escisión dado por $\varphi(d) = \tilde{\vec{b}}$ y $B \cong \langle\tilde{\vec{b}}\rangle \times B_0$.



Sea M el campo correspondiente a $BC_{K,0}$. Se tiene

$$BC_{K,0} = \langle\tilde{\vec{b}}\rangle B_0 C_{K,0} = \langle\tilde{\vec{b}}\rangle C_{K,0} \cong \langle\tilde{\vec{b}}\rangle \times C_{K,0}.$$

Se sigue que $M = E \cap K\mathbb{F}_q^{\mathrm{ab}}$. Puesto que $M \subseteq K\mathbb{F}_q^{\mathrm{ab}}$, M/K es una extensión de constantes de grado

$$[M : K] = [C_K : BC_{K,0}] = [\mathbb{Z} \times C_{K,0} : d\mathbb{Z} \times C_{K,0}] = [\mathbb{Z} : d\mathbb{Z}] = d.$$

Por tanto el campo de constantes de E es $\mathbb{F}_{q^d}$. □

6.9. Leyes de descomposición de primos en campos globales

Consideremos K un campo global arbitrario.

Teorema 6.9.1. *Sea L/K una extensión abeliana finita de campos globales de grado n y sea $\mathfrak{p}$ un primo de K no ramificado en L. Sea $\pi \in K_{\mathfrak{p}}$ un elemento primo, $v_{\mathfrak{p}}(\pi) = 1$. Sea*

$$\lceil\pi\rceil_{\mathfrak{p}} = (\ldots, 1, 1, \pi, 1, 1, \ldots) \in J_K.$$

Sea f el mínimo entero positivo tal que $\lceil\tilde{\pi}\rceil_{\mathfrak{p}}^f \in \mathrm{N}_{L/K} C_L$. Entonces el primo $\mathfrak{p}$ se factoriza en la extensión L en $h = n/f$ primos distintos $\mathfrak{P}_1, \ldots, \mathfrak{P}_h$ de grado relativo f, es decir

$$\mathrm{con}_{K/L}\, \mathfrak{p} = \mathfrak{P}_1 \cdots \mathfrak{P}_h, \quad [\mathcal{O}_{\mathfrak{P}_i}/\mathfrak{P}_i : \mathcal{O}_{\mathfrak{p}}/\mathfrak{p}] = f.$$

Esto es, si conocemos $\mathrm{N}_{L/K} C_L$ podemos determinar la descomposición de $\mathfrak{p}$ en L.

Demostración. Puesto que $\mathfrak{p}$ es no ramificado, $\mathfrak{p}$ se escribe como $\mathfrak{p} = \mathfrak{P}_1 \cdots \mathfrak{P}_h$ con cada $\mathfrak{P}_i$, $1 \le i \le h$ de grado f'. Se tiene que $C_K/\mathrm{N}_{L/K} C_L \cong \mathrm{Gal}(L/K)$. Se tiene $f = o\big(\overline{\lceil\tilde{\pi}\rceil}_{\mathfrak{p}}\big)$ en $C_K/\mathrm{N}_{L/K} C_L$ el cual es el orden de

$$\psi_{L/K}\big(\overline{\lceil\tilde{\pi}\rceil}_{\mathfrak{p}}\big) = \prod_{\mathfrak{q}\in\mathbb{P}_K} \big(\big(\overline{\lceil\tilde{\pi}\rceil}_{\mathfrak{p}}\big)_{\mathfrak{q}}, L_{\mathfrak{q}}/K_{\mathfrak{q}}\big) = \big(\pi, L_{\mathfrak{p}}/K_{\mathfrak{p}}\big) = \mathrm{Fr}_{\mathfrak{p}}$$

el automorfismo de Frobenius en $L_{\mathfrak{P}}/K_{\mathfrak{p}}$, la cual es una extensión no ramificada. Ahora bien $\langle\mathrm{Fr}_{\mathfrak{p}}\rangle = \mathrm{Gal}(L_{\mathfrak{p}}/K_{\mathfrak{p}}) \subseteq \mathrm{Gal}(L/K)$. Por tanto $f = o(\mathrm{Fr}_{\mathfrak{p}}) = [L_{\mathfrak{p}} : K_{\mathfrak{p}}] = f'$. Se sigue que $f = f' = n/h$. □

Corolario 6.9.2. *Sea $\mathfrak{p}$ finito y no ramificado en L. Si $\pi_{\mathfrak{p}}$ es un elemento primo de $K_{\mathfrak{p}}$, entonces $\theta(\pi_{\mathfrak{p}}) \in C_K/H$ se mapea al automorfismo de Frobenius $\left(\dfrac{L/K}{\mathfrak{p}}\right) \in \mathrm{Gal}(L/K)$ bajo el isomorfismo $C_K/H \overset{\rho_K}{\cong} \mathrm{Gal}(L/K)$.*

Demostración. Es inmediato de los Teoremas 6.9.1 y 5.2.2. □

Teorema 6.9.3. *Sea L/K una extensión abeliana finita de campos globales. Sea $\mathfrak{p}$ un lugar de K. Sea*

$$\theta = \psi_{L/K} \circ \lceil\ \rfloor_{\mathfrak{p}} \colon K_{\mathfrak{p}}^* \xrightarrow{\lceil\ \rfloor_{\mathfrak{p}}} J_K \xrightarrow{\psi_{L/K}} \mathrm{Gal}(L/K).$$

Entonces

(1) *Para $n \geq 0$, $\theta(U_{\mathfrak{p}}^{(n)})$ es el grupo de ramificación superior $G^n(L/K)$ donde $G = \mathrm{Gal}(L/K)$:*

$$\theta(U_{\mathfrak{p}}^{(n)}) = G^n(L/K), \quad n \geq 0.$$

En particular, si $n = 0$,

$$\theta(U_{\mathfrak{p}}^{(0)}) = \theta(U_{\mathfrak{p}}) = G^0(L/K) = G_0(L/K) = I(\mathfrak{P}|\mathfrak{p})$$

es el grupo de inercia.
(2) *$\theta(K_{\mathfrak{p}}^*)$ es el grupo de descomposición $D = D(\mathfrak{P}|\mathfrak{p})$.*

Demostración. Por el Teorema 6.7.33, se tiene que $\psi \circ \lceil\ \rfloor_{\mathfrak{p}} = \theta = (\_, L_{\mathfrak{p}}/K_{\mathfrak{p}})$. Por tanto, por el Teorema 5.8.75, se tiene

$$\theta(U_{\mathfrak{p}}^{(n)}) = (U_{\mathfrak{p}}^{(n)}, L_{\mathfrak{p}}/K_{\mathfrak{p}}) = G^n(L/K).$$

Esto es (1).

Para probar (2), tenemos, del Teorema TCCL, que

$$(\_, L_{\mathfrak{p}}/K_{\mathfrak{p}}) \colon K_{\mathfrak{p}}^* \longrightarrow \mathrm{Gal}(L_{\mathfrak{p}}/K_{\mathfrak{p}}) \cong D(\mathfrak{P}|\mathfrak{p})$$

es suprayectivo. Por tanto

$$\theta(K_{\mathfrak{p}}^*) = (K_{\mathfrak{p}}^*, L_{\mathfrak{p}}/K_{\mathfrak{p}}) = D(\mathfrak{P}|\mathfrak{p}).$$ □

Corolario 6.9.4. *Sea K un campo global, L una extensión abeliana finita de K y H el subgrupo abierto de índice finito de C_K que corresponde a L, es decir, $H = \mathcal{N}_L = \mathrm{N}_{L/K} C_L$, $C_K/H \cong \mathrm{Gal}(L/K)$.*

Para un lugar $\mathfrak{p}$ de K, consideremos la composición

$$\mu \colon K_{\mathfrak{p}}^* \xrightarrow{\lceil\ \rfloor_{\mathfrak{p}}} C_K \xrightarrow{\pi} C_K/H.$$

(1) *$\mathfrak{p}$ se descompone totalmente en $L \iff \mu(K_{\mathfrak{p}}^*) = 1 \iff K_{\mathfrak{p}}^* \subseteq H$.*
(2) *Si $\mathfrak{p}$ es finito, $\mathfrak{p}$ es no ramificado $\iff \mu(U_{\mathfrak{p}}) = 1 \iff U_{\mathfrak{p}} \subseteq H$.*

Equivalentemente, si $(\_, L/K)$ denota al símbolo de Artin, entonces

(1) *$\mathfrak{p}$ se descompone totalmente $\iff (K_{\mathfrak{p}}^*, L/K) = 1$.*
(2) *Si $\mathfrak{p}$ es finito, $\mathfrak{p}$ es no ramificado $\iff (U_{\mathfrak{p}}, L/K) = 1$.*

Demostración. (1) Se tiene que $\mathfrak{p}$ se descompone totalmente en $L \iff D(\mathfrak{P}|\mathfrak{p}) = \{1\} \iff \mu(K_{\mathfrak{p}}^*) = \{1\}$.
(2) Si $\mathfrak{p}$ es finito, $\mathfrak{p}$ es no ramificado $\iff I(\mathfrak{P}|\mathfrak{p}) = \{1\} \iff \mu(U_{\mathfrak{p}}) = \{1\}$. □

El siguiente teorema es la versión global del Teorema 5.7.13.

Teorema 6.9.5. *Sea E/F una extensión abeliana finita de campos globales y sea E el campo de clase de $\Lambda \subseteq C_F$, esto es, $\mathrm{N}_{E/F} C_E = \Lambda$. Sea L/F una extensión finita y separable. Entonces LE/L es una extensión finita y el grupo de normas correspondiente es $\mathrm{N}_{L/F}^{-1}(\Lambda)$.*

$$\begin{array}{ccc} L & \xrightarrow{\mathrm{N}_{L/F}^{-1}(\Lambda)} & LE \\ | & & | \\ F & \xrightarrow[\Lambda]{} & E \end{array}$$

Demostración. Sea $\psi_{EL/L}\colon C_L \longrightarrow \mathrm{Gal}(LE/L)$ el mapeo de Artin. El grupo de normas correspondiente a LE/L es $\operatorname{núc}\psi_{LE/L}$, esto es, $C_L/\operatorname{núc}\psi_{LE/L} \cong \mathrm{Gal}(LE/L)$. Por el Teorema 6.7.21 tenemos el diagrama conmutativo

$$\begin{array}{ccc} C_L & \xrightarrow{\psi_{LE/L}} & \mathrm{Gal}(LE/L) \\ {\scriptstyle \mathrm{N}_{L/F}}\downarrow & & \downarrow{\scriptstyle \mathrm{rest}} \\ C_F & \xrightarrow[\psi_{E/F}]{} & \mathrm{Gal}(E/F) \end{array}$$

Además el $\mathrm{rest}\colon \mathrm{Gal}(LE/L) \longrightarrow \mathrm{Gal}(E/F)$ es inyectivo y $\mathrm{rest}\circ\psi_{LE/L} = \psi_{E/F}\circ \mathrm{N}_{L/F}$. Por tanto

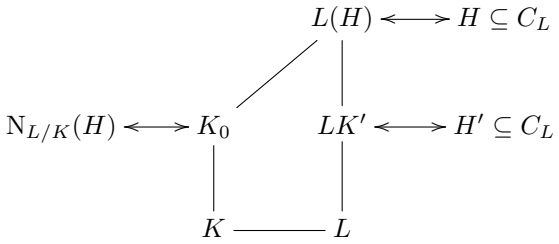
$$\begin{aligned} \tilde{\vec{x}} \in \operatorname{núc}\psi_{LE/L} &\iff \psi_{LE/L}(\tilde{\vec{x}}) = 1 \iff \\ \mathrm{rest}\circ\psi_{LE/L}(\tilde{\vec{x}}) = 1 = \psi_{E/F}\circ \mathrm{N}_{L/F}(\tilde{\vec{x}}) &\iff \\ \mathrm{N}_{L/F}(\tilde{\vec{x}}) \in \operatorname{núc}\psi_{E/F} = \Lambda &\iff \tilde{\vec{x}} \in \mathrm{N}_{L/F}^{-1}(\Lambda). \end{aligned}$$ □

El siguiente resultado es importante para la teoría de campos de géneros.

Teorema 6.9.6. *Sea L/K una extensión finita y separable de campos globales. Sea H un subgrupo abierto de índice finito en C_L y sea $L(H)$ su campo de clase. Sea K_0 la máxima extensión abeliana de K contenida en $L(H)$. Entonces el grupo de normas de K_0 es $\mathrm{N}_{L/K}(H)$, es decir, $\mathrm{N}_{K_0/K} C_{K_0} = \mathrm{N}_{L/K} H$.*

Demostración. La norma $\mathrm{N}_{L/K}\colon C_L \longrightarrow C_K$ es un mapeo abierto (Teorema 6.3.2) por lo que $\mathrm{N}_{L/K}(H)$ es abierto en C_K. Por otro lado, del hecho de

que H es de índice finito en C_L, se sigue que $\mathrm{N}_{L/K}(H)$ es de índice finito en $\mathrm{N}_{L/K}\, C_L$.



Ahora bien, L/K es una extensión finita por lo que $\mathrm{N}_{L/K}\, C_L$ es de índice finito en C_K. Por tanto $\mathrm{N}_{L/K}(H)$ es de índice finito en C_K y se sigue que $\mathrm{N}_{L/K}(H)$ es tanto cerrado como abierto en C_K.

Sea K' el campo asociado a $\mathrm{N}_{L/K}(H)$ y sea Λ el grupo de normas asociado a K_0. Por el Teorema 6.9.5 se tiene que LK'/L corresponde al grupo de normas $\mathrm{N}_{L/K}^{-1}(\mathrm{N}_{L/K}(H)) \supseteq H$ lo cual implica que $LK' \subseteq L(H)$, de donde obtenemos que $K' \subseteq K_0$. Por tanto $\Lambda \subseteq \mathrm{N}_{L/K}(H)$. Puesto que $LK_0 \subseteq L(H)$, del Teorema 6.9.5, obtenemos que $\mathrm{N}_{L/K}^{-1}(\Lambda) \supseteq H$. Se sigue que $\mathrm{N}_{L/K}(H) \subseteq \Lambda$. Por tanto $\Lambda = \mathrm{N}_{L/K}(H)$ probando el resultado. □

Lo que probamos a continuación refuerza nuevamente que la teoría que estamos desarrollando únicamente es válida para extensiones abelianas. Este es la razón del porqué la primera desigualdad únicamente es válida para extensiones abelianas. La demostración, tanto para el caso local como para el global, es consecuencia del teorema de existencia.

Teorema 6.9.7 (Limitación de normas). *Sea L/K una extensión finita y separable, ya sea de campos locales o de campos globales. Sea L'/K la máxima subextensión abeliana de L/K. Enconces*

$$\mathrm{N}_{L/K}\, A_L = \mathrm{N}_{L'/K}\, A_{L'} \quad \textit{donde} \quad A_L = \begin{cases} L^* & \textit{si } L \textit{ es local,} \\ C_L & \textit{si } L \textit{ es global.} \end{cases}$$

Demostración. Sea $H := \mathrm{N}_{L/K}\, A_L$. Entonces H es un subgrupo abierto y de índice finito de A_K. Por el teorema de existencia, existe una extensión abeliana finita F de K tal que $\mathrm{N}_{F/K}\, A_F = H$. Puesto que

$$H = \mathrm{N}_{F/K}\, A_F \subseteq \mathrm{N}_{L'/K}\, A_{L'},$$

se sigue que $L' \subseteq F$. Puesto que L' es la máxima subsextensión abeliana de L/K y F/K es abeliana, $F \subseteq L'$ y por tanto $F = L'$. □

7

Grupos de congruencias

Con el objetivo de hacer más transparente el Teorema de Existencia, vamos a estudiar los llamados *grupos de congruencias* para un campo global K, particularmente los campos numéricos. Para el caso de campos de funciones, debemos posponer un poco la discusión pues necesitaremos una condición extra que automáticamente se cumple para campos numéricos.

Definición 7.0.1. Un *módulus* $\mathfrak{m}$ es un producto formal $\mathfrak{m} = \prod_{\mathfrak{p}\in\mathbb{P}_K} \mathfrak{p}^{n_\mathfrak{p}}$ donde $n_\mathfrak{p} \geq 0$ para todo $\mathfrak{p} \in \mathbb{P}_K$, $n_\mathfrak{p} = 0$ para casi todo $\mathfrak{p}$, $n_\mathfrak{p} = 0$ si $\mathfrak{p}$ es complejo y $n_\mathfrak{p} = 0$ o 1 si $\mathfrak{p}$ es real.

Extendemos la definición de unidades a todos los lugares.

Definición 7.0.2. Dado un campo global K y $\mathfrak{p}$ un lugar arbitrario de K se define el *grupo de las $n_\mathfrak{p}$ unidades de K*, donde $n_\mathfrak{p} \geq 0$ por

$$U_\mathfrak{p}^{(n_\mathfrak{p})} = \begin{cases} 1 + \mathfrak{p}^{n_\mathfrak{p}} & \text{si } \mathfrak{p} \nmid \infty \text{ y } n_\mathfrak{p} \geq 1, \\ U_\mathfrak{p}^{(0)} = U_\mathfrak{p} & \text{si } \mathfrak{p} \nmid \infty \text{ y } n_\mathfrak{p} = 0, \\ \mathbb{R}^+ \subseteq K_\mathfrak{p}^* & \text{si } \mathfrak{p} \text{ es real y } n_\mathfrak{p} = 1, \\ \mathbb{R}^* = K_\mathfrak{p}^* & \text{si } \mathfrak{p} \text{ es real y } n_\mathfrak{p} = 0, \\ \mathbb{C}^* = K_\mathfrak{p}^* & \text{si } \mathfrak{p} \text{ es complejo.} \end{cases} \tag{7.0.1}$$

De esta forma tenemos que si $\mathfrak{p}$ es real, entonces $U_\mathfrak{p}^{(1)} = \mathbb{R}^+$ y $[K_\mathfrak{p}^* : U_\mathfrak{p}] = [\mathbb{R}^* : \mathbb{R}^+] = 2$.

Definición 7.0.3. Para un lugar $\mathfrak{p}$ y un elemento $\alpha_\mathfrak{p}$ se define

$$\alpha_\mathfrak{p} \equiv 1 \text{ mód } \mathfrak{p}^{n_\mathfrak{p}} \iff \alpha_\mathfrak{p} \in U_\mathfrak{p}^{(n_\mathfrak{p})}.$$

En particular si $\mathfrak{p}$ es complejo o es real y $n_\mathfrak{p} = 0$ la congruencia no impone ninguna restricción sobre $\alpha_\mathfrak{p}$. Si $\mathfrak{p}$ es real y $n_\mathfrak{p} = 1$, $\alpha_\mathfrak{p} \equiv 1 \text{ mód } \mathfrak{p}^{n_\mathfrak{p}} \iff \alpha_\mathfrak{p} \in U_\mathfrak{p}^{(n_\mathfrak{p})} = \mathbb{R}^+ \iff \alpha_\mathfrak{p} > 0$.

Definición 7.0.4. Sea $\mathfrak{m} = \prod_{\mathfrak{p}\in\mathbb{P}_K} \mathfrak{p}^{n_\mathfrak{p}}$ un módulus en un campo global. Para un idèle $\vec{\alpha} = (\alpha_\mathfrak{p})_{\mathfrak{p}\in\mathbb{P}_K} \in J_K$ definimos

$$\vec{\alpha} \equiv 1 \text{ mód } \mathfrak{m} \iff \alpha_\mathfrak{p} \equiv 1 \text{ mód } \mathfrak{p}^{n_\mathfrak{p}} \ \forall\ \mathfrak{p} \in \mathbb{P}_K \iff \alpha_\mathfrak{p} \in U_\mathfrak{p}^{(n_\mathfrak{p})} \ \forall\ \mathfrak{p} \in \mathbb{P}_K.$$

Se define el *grupo de los idèles congruentes a* 1 *módulo* $\mathfrak{m}$ por

$$J_K^\mathfrak{m} := \{\vec{\alpha} \in J_K \mid \vec{\alpha} \equiv 1 \text{ mód } \mathfrak{m}\} = \prod_{\mathfrak{p}\in\mathbb{P}_K} U_\mathfrak{p}^{(n_\mathfrak{p})}.$$

Definición 7.0.5. Para un campo global K, los elementos *totalmente positivos* $\alpha \in K$ son los elementos tales que $\mathfrak{m}$ involucra a todos los lugares reales y todos estos lugares tienen exponente 1, esto es, $\alpha \equiv 1 \text{ mód } U_\mathfrak{p}^{(1)}$ para todo $\mathfrak{p}$ real.

Equivalentemente $\alpha \in K$ es totalmente positivo si $\sigma\alpha > 0$ para todo σ lugar real (es decir para todo encaje $\sigma\colon K \to \mathbb{C}$ tal que $\sigma(K) \subseteq \mathbb{R}$).

De esta forma si $\mathfrak{m}$ es un módulus tal que para todo lugar real $\mathfrak{p}$, el exponente en $\mathfrak{m}$ de $\mathfrak{p}$ es 1, entonces los elementos que satisfacen $\alpha \equiv 1 \text{ mód } \mathfrak{m}$ son elementos totalmente positivos.

Observación 7.0.6. El elemento $1+\sqrt{2}$ es positivo pero no totalmente positivo pues $\varphi\colon \mathbb{Q}(\sqrt{2}) \to \mathbb{R}$, $\sqrt{2} \mapsto -\sqrt{2}$, satisface que $\varphi(1+\sqrt{2}) = 1-\sqrt{2} < 0$.

También notemos que el ser totalmente positivo depende del campo ambiente. Por ejemplo, -1 es totalmente positivo en $\mathbb{Q}(i)$ pero no en $\mathbb{Q}$.

Definición 7.0.7. El grupo $C_K^\mathfrak{m} := J_K^\mathfrak{m} K^*/K^* \subseteq C_K$ se llama el *subgrupo de congruencias módulo* $\mathfrak{m}$ *de* C_K. El cociente $C_K/C_K^\mathfrak{m}$ se llama el *grupo de clases de rayos módulo* $\mathfrak{m}$.

Ejemplo 7.0.8. Si $\mathfrak{m} = 1$, esto es, $n_\mathfrak{p} = 0$ para toda $\mathfrak{p}$. Tenemos

$$J_K^\mathfrak{m} = J_K^1 = \prod_{\mathfrak{p}\mid\infty} K_\mathfrak{p}^* \times \prod_{\mathfrak{p}\nmid\infty} U_\mathfrak{p} = \prod_{\mathfrak{p}\in\mathbb{P}_K} U_\mathfrak{p}^{(0)} = U_K,$$
$$J_K/J_K^1 K^* \cong C_K/C_K^1 \cong C_K/U_K K^* \cong I_K \cong D_K/P_K.$$

(ver después de la Definición 6.2.9).

Con esta nueva terminología, se tiene que

$$J_K/J_K^1 = \bigoplus_{\mathfrak{p}\in\mathbb{P}_K} K_\mathfrak{p}^*/U_\mathfrak{p}^{(0)} \cong \bigoplus_{\substack{\mathfrak{p}\in\mathbb{P}_K \\ \mathfrak{p} \text{ finito}}} \mathbb{Z} \cong D_K.$$

Por lo tanto

$$C_K/C_K^1 = \text{conúcleo}(K^* \to J_K/J_K^1) \cong D_K/(K^*) = D_K/P_K = I_K.$$

También obtenemos que $C_K^1 \subseteq C_{K,0}$ y que $C_{K,0}/C_K^1 \cong I_{K,0}$ en el caso de campos de funciones.

Volvemos a enunciar lo anterior con esta nueva terminología para referencia futura.

Teorema 7.0.9. *Sea K un campo global. Entonces*

$$C_K/C_K^1 \cong I_K \quad K \text{ cualquier campo global,}$$
$$C_{K,0}/C_K^1 \cong I_{K,0} \quad K \text{ un campo de funciones.} \qquad \square$$

7.1. Campos numéricos

Observación 7.1.1. Cuando K es un campo numérico, se probará que $[C_K : C_K^{\mathfrak{m}}] < \infty$, pero si K es un campo de funciones, entonces $[C_K : C_K^{\mathfrak{m}}] = \infty$. De hecho, en este caso, $C_K/C_K^1 \cong I_K$ y $[C_K : C_K^1] = |I_K| = \infty$. Este problema lo solucionaremos más adelante. En cualquier caso, esto es, K un campo global arbitrario, $C_K^{\mathfrak{m}}$ es un subgrupo abierto de C_K.

Debido a lo anterior, en esta subsección únicamente consideraremos K un campo numérico.

Teorema 7.1.2. *Sea K un campo numérico. Los grupos de normas de C_K, es decir los grupos $\mathrm{N}_{L/K} C_L$ donde L/K es una extensión abeliana finita, son precisamente los subgrupos de C_K que contienen a algún subgrupo de congruencias $C_K^{\mathfrak{m}}$.*

Demostración. Se tiene que, por definición, $J_K^{\mathfrak{m}} = \prod_{\mathfrak{p}\in\mathbb{P}_K} U_{\mathfrak{p}}^{(n_{\mathfrak{p}})}$, donde $\mathfrak{m} = \prod_{\mathfrak{p}\in\mathbb{P}_K} \mathfrak{p}^{n_{\mathfrak{p}}}$, es un subgrupo abierto de J_K. Puesto que C_K tiene la topología cociente, $C_K^{\mathfrak{m}}$ es un subgrupo abierto de C_K el cual tiene índice

$$\begin{aligned}[C_K : C_K^{\mathfrak{m}}] &= [C_K : C_K^1][C_K^1 : C_K^{\mathfrak{m}}] = |I_K|[C_K^1 : C_K^{\mathfrak{m}}] = h_K[J_K^1 K^* : J_K^{\mathfrak{m}} K^*] \\ &\leq h_K[J_K^1 : J_K^{\mathfrak{m}}] = h_K \prod_{\mathfrak{p}\in\mathbb{P}_K} [U_{\mathfrak{p}} : U_{\mathfrak{p}}^{(n_{\mathfrak{p}})}] < \infty\end{aligned}$$

pues $n_{\mathfrak{p}} = 0$ para casi toda $\mathfrak{p} \in \mathbb{P}_K$.

De esta forma obtenemos que $C_K^{\mathfrak{m}}$ es un subgrupo abierto (y por tanto cerrado) de índice finito en C_K, por lo que $C_K^{\mathfrak{m}}$ es un grupo de normas (Teorema TCCG). Sea ahora cualquier H subgrupo de C_K con $H \supseteq C_K^{\mathfrak{m}}$ para algún módulus $\mathfrak{m}$. Puesto que $[C_K : C_K^{\mathfrak{m}}] < \infty$, se tiene $[H : C_K^{\mathfrak{m}}] < \infty$. Por tanto $H = \bigcup_{\text{finita}} xC_K^{\mathfrak{m}}$ de donde se sigue que H es un subgrupo abierto de C_K y por tanto es un grupo de normas.

Recíprocamente, sea H un grupo de normas de C_K, es decir, H es un subgrupo abierto y cerrado de índice finito en C_K. Sean $J_K \overset{\theta}{\twoheadrightarrow} C_K$ la proyección natural y $\mathcal{H} := \theta^{-1}(H)$. Entonces $\mathcal{H}$ es un subgrupo abierto de J_K, por lo que $\mathcal{H}$ contiene a un subconjunto de la forma

$$W = \prod_{\mathfrak{p}\in S} W_{\mathfrak{p}} \times \prod_{\mathfrak{p}\notin S} U_{\mathfrak{p}},$$

donde S es un conjunto finito y cada $W_{\mathfrak{p}}$ es una vecindad abierta de $1 \in K_{\mathfrak{p}}^*$.

Si $\mathfrak{p} \in S$ es finito, podemos tomar $W_{\mathfrak{p}} = U_{\mathfrak{p}}^{(n_{\mathfrak{p}})}$ para algún $n_{\mathfrak{p}} \geq 0$ debido a que los subgrupos $\left\{U_{\mathfrak{p}}^{(n_{\mathfrak{p}})}\right\}_{n_{\mathfrak{p}} \in \mathbb{N} \cup \{0\}}$ forman una base de vecindades de 1 en $K_{\mathfrak{p}}^*$. Si $\mathfrak{p} \in S$ es infinito, $W_{\mathfrak{p}}$ genera ya sea a $\mathbb{R}^+$ o a todo $K_{\mathfrak{p}}^* \in \{\mathbb{R}^*, \mathbb{C}^*\}$. De esta forma, el subgrupo generado por W es de la forma $J_K^{\mathfrak{m}}$ para el módulus $\mathfrak{m} = \prod_{\mathfrak{p} \in \mathbb{P}_K} \mathfrak{p}^{n_{\mathfrak{p}}}$. Se sigue que $\mathcal{H} = \theta^{-1}(H)$ contiene a $J_K^{\mathfrak{m}}$ y por ende H contiene a $C_K^{\mathfrak{m}}$. □

Observación 7.1.3. El Teorema 7.1.2 no es aplicable a campos de funciones pues para todo módulus $\mathfrak{m}$, $C_K^{\mathfrak{m}} \subseteq C_K^1$ de donde obtenemos

$$[C_K : C_K^{\mathfrak{m}}] \geq [C_K : C_K^1] = |I_K| = \infty.$$

Lo que si se tiene es que $C_{K,0} \cong \mathrm{Gal}(K^{\mathrm{ab}}/K\mathbb{F}_q^{\mathrm{ab}})$ y $C_K^{\mathfrak{m}} \subseteq C_{K,0}$ para cualquier módulus $\mathfrak{m}$. Más aún, si $H \subseteq C_{K,0}$ es un subgrupo abierto y de índice finito en $C_{K,0}$, entonces $H \supseteq C_K^{\mathfrak{m}}$ para algún $\mathfrak{m}$ y H es cerrado en $C_{K,0}$. Por teoría de Galois (Teorema 2.3.2), si $(K^{\mathrm{ab}})^H = L$ y $(K^{\mathrm{ab}})^{C_K^{\mathfrak{m}}} = K^{\mathfrak{m}}$ entonces $L \subseteq K^{\mathfrak{m}}$ exactamente como en el caso numérico y podríamos hacer una discusión totalmente análoga que lo discutido en esta sección para campos numéricos a esta situación de campos de funciones. La diferencia es que para campos de funciones L y $K^{\mathfrak{m}}$ no corresponden con grupos de normas. Para un remedio a esta situación, ver Sección 7.2.

Volvemos a nuestra situación en que K es un campo numérico.

Definición 7.1.4. El campo de clase $K^{\mathfrak{m}}/K$ correspondiente al grupo de congruencias $C_K^{\mathfrak{m}}$, es decir, $\mathrm{N}_{K^{\mathfrak{m}}/K} C_{K^{\mathfrak{m}}} = C_K^{\mathfrak{m}}$, se llama el *campo de clases de rayos módulo* $\mathfrak{m}$.

Se tiene que, para campos numéricos, $\boxed{\mathrm{Gal}(K^{\mathfrak{m}}/K) \cong C_K/C_K^{\mathfrak{m}}}$.

Observación 7.1.5. El Teorema 7.1.2 prueba que toda extensión abeliana finita L/K de campos numéricos está contenida en algún campo de clases de rayos $K^{\mathfrak{m}}$. Esto es, si L/K es una extensión abeliana finita, existe $K^{\mathfrak{m}}$ tal que $L \subseteq K^{\mathfrak{m}}$. Esto se sigue del Corolario 6.7.29 pues si L corresponde a H, y $K^{\mathfrak{m}}$ corresponde a $C_K^{\mathfrak{m}}$ entonces $H \supseteq C_K^{\mathfrak{m}} \iff L \subseteq K^{\mathfrak{m}}$.

También tenemos que si $\mathfrak{m}|\mathfrak{n}$ entonces $C_L^{\mathfrak{n}} \subseteq C_K^{\mathfrak{m}}$ y por consiguiente $K^{\mathfrak{m}} \subseteq K^{\mathfrak{n}}$.

Definición 7.1.6. Sean K un campo numérico y L/K una extensión abeliana finita, y sea $\mathcal{N}_L = \mathrm{N}_{L/K} C_L \subseteq C_K$. Se define el *conductor* $\mathfrak{f} = \mathfrak{f}_{L/K} = \mathfrak{f}(L/K)$ de L/K (o de $\mathcal{N}_L$) como el máximo común divisor de todos los moduli $\mathfrak{m}$ tales que $L \subseteq K^{\mathfrak{m}}$, esto es, $C_K^{\mathfrak{m}} \subseteq \mathcal{N}_L$.

En otras palabras, $K^{\mathfrak{f}}/K$ es el mínimo campo de clases de rayos que contiene a L/K y si $L \subseteq K^{\mathfrak{m}}$, entonces $\mathfrak{f}|\mathfrak{m}$.

Se tiene que dado un campo numérico K y $\mathfrak{m}$ un módulus, se tiene

Teorema 7.1.7.

(1) *Existe una única extensión $K^{\mathfrak{m}}$ de K que tiene la siguiente propiedad: si $\mathfrak{p}$ es un ideal primo no cero de $\mathcal{O}_K$ que no divide a $\mathfrak{m}$ entonces $\mathfrak{p}$ es no ramificado y se tiene*

$$\mathfrak{p} \text{ es totalmente descompuesto en } K^{\mathfrak{m}} \iff$$
$$\text{existe un elemento totalmente positivo } \alpha \in \mathcal{O}_K \text{ tal que}$$
$$\mathfrak{p} = (\alpha), \quad \alpha \equiv 1 \text{ mód } \mathfrak{m}.$$

(ver la Observación 7.1.5*).*
(2) *$K^{\mathfrak{m}}/K$ es una extensión abeliana finita de K y toda extensión abeliana finita de K está contenida en algún $K^{\mathfrak{m}}$.*
(3) *Si $\mathfrak{n} \subseteq \mathfrak{m}$ entonces $K^{\mathfrak{m}} \subseteq K^{\mathfrak{n}}$.*
(4) *Si L/K es una extensión abeliana finita entonces existe un ideal no cero $\mathfrak{f}$ de $\mathcal{O}_K$ máximo tal que $L \subseteq K^{\mathfrak{m}}$. Además para todo ideal primo $\mathfrak{p}$ no cero de $\mathcal{O}_K$, $\mathfrak{p}$ es ramificado en $L \iff \mathfrak{p}|\mathfrak{f}$.*

El ideal $\mathfrak{f}$ dado en (4) *es el* conductor *(ver Definición* 7.1.6*).*
Los campos $K^{\mathfrak{m}}$ son los campos de clases de rayos *(Definición* 7.1.4*).* □

Ejemplos 7.1.8. (1) Sea $K = \mathbb{Q}$, $\mathfrak{m} = (n)$. Para cada primo p de $\mathbb{Z}$, se tiene que p es totalmente positivo pero $-p$ no lo es. Sea $\mathfrak{p}$ generado por $\pm p$. Así que decir "existe un entero totalmente positivo α tal que $\mathfrak{p} = (\alpha)$ con $\alpha \equiv 1$ mód n" no es equivalente a únicamente decir "$\mathfrak{p} = (p)$ con un número primo positivo tal que $p \equiv 1$ mód n". Esto es, $\mathbb{Q}(\zeta_n)$ tiene la propiedad $K^{\mathfrak{m}}$, más precisamente, $\mathbb{Q}(\zeta_n) = \mathbb{Q}^{(n)}$. Por la unicidad podemos concluir que $\mathbb{Q}(\zeta_n) = \mathbb{Q}^{(n)}$. Se tiene $\mathfrak{f} = \mathfrak{m} = (n)$.
(2) Para $K = \mathbb{Q}(\zeta_3)$, $\mathfrak{f} = (6)$, $K^{\mathfrak{f}} = \mathbb{Q}(\zeta_3, \sqrt[3]{2}) = K(\sqrt[3]{2})$ (ver [84, table 5.7, página 10]).
(3) $K = \mathbb{Q}(\sqrt{-5})$, $K^{\mathcal{O}_K} = \mathbb{Q}(\sqrt{-5}, \sqrt{-1}) = K(\sqrt{-1})$ (campo de clase de Hilbert, ver Definición 7.1.18).
(4) $K = \mathbb{Q}(\sqrt{-6})$, $K^{\mathcal{O}_K} = \mathbb{Q}(\sqrt{-6}, \zeta_3) = K(\zeta_3) = K(\sqrt{-3})$ (campo de clase de Hilbert).
Es fácil ver que $\mathbb{Q}(\sqrt{-5}, \sqrt{-1})/\mathbb{Q}(\sqrt{-5})$ y que $\mathbb{Q}(\sqrt{-6}, \zeta_3)/\mathbb{Q}(\sqrt{-6})$ son extensiones no ramificadas. Ver [136, Subsección 6.4.1].

A continuación presentamos la relación entre $K^{\mathfrak{m}}$ y $K^{\mathfrak{n}}$ para dos móduli $\mathfrak{m}$, $\mathfrak{n}$ de un campo numérico.

Se tiene que $K^{\mathfrak{m}}$ es el campo de clase de $C_K^{\mathfrak{m}}$ y $K^{\mathfrak{n}}$ es el campo de clase de $C_K^{\mathfrak{n}}$:

$$K^{\mathfrak{m}} \longleftrightarrow C_K^{\mathfrak{m}}, \quad K^{\mathfrak{n}} \longleftrightarrow C_K^{\mathfrak{n}}.$$

Por el Teorema 6.7.32, se tiene

$$K^{\mathfrak{m}} \subseteq K^{\mathfrak{n}} \iff C_K^{\mathfrak{n}} \subseteq C_K^{\mathfrak{m}} \iff C_K^{\mathfrak{f}_{K^{\mathfrak{n}}}} \subseteq C_K^{\mathfrak{f}_{K^{\mathfrak{m}}}} \iff \mathfrak{f}_{K^{\mathfrak{m}}} | \mathfrak{f}_{K^{\mathfrak{n}}}.$$

Escribimos $C_K^{\mathfrak{m}} = \mathcal{N}_{K^{\mathfrak{m}}}$ y $C_K^{\mathfrak{n}} = \mathcal{N}_{K^{\mathfrak{n}}}$. Entonces $\mathcal{N}_{K^{\mathfrak{m}} \cap K^{\mathfrak{n}}} = \mathcal{N}_{K^{\mathfrak{m}}} \mathcal{N}_{K^{\mathfrak{n}}} = C_K^{\mathfrak{m}} C_K^{\mathfrak{n}}$.

Sean $\mathfrak{c} = \mathrm{mcd}(\mathfrak{m}, \mathfrak{n})$ y $\mathfrak{d} = \mathrm{mcm}(\mathfrak{m}, \mathfrak{n})$. Entonces $\mathfrak{c} | \mathfrak{m}$ y $\mathfrak{c} | \mathfrak{n}$ por lo que $K^{\mathfrak{c}} \subseteq K^{\mathfrak{m}} \cap K^{\mathfrak{n}}$. Similarmente $K^{\mathfrak{m}} K^{\mathfrak{n}} \subseteq K^{\mathfrak{d}}$.

Ahora, veamos que $C_K^{\mathfrak{c}} \subseteq C_K^{\mathfrak{m}} C_K^{\mathfrak{n}}$. Sean $\mathfrak{m} = \prod_{\mathfrak{p}} \mathfrak{p}^{m_{\mathfrak{p}}}$ y $\mathfrak{n} = \prod_{\mathfrak{p}} \mathfrak{p}^{n_{\mathfrak{p}}}$. Entonces $\mathfrak{c} = \prod_{\mathfrak{p}} \mathfrak{p}^{\mathrm{mín}\{m_{\mathfrak{p}}, n_{\mathfrak{p}}\}} = \prod_{\mathfrak{p}} \mathfrak{p}^{c_{\mathfrak{p}}}$ y $\mathfrak{d} = \prod_{\mathfrak{p}} \mathfrak{p}^{\mathrm{máx}\{m_{\mathfrak{p}}, n_{\mathfrak{p}}\}} = \prod_{\mathfrak{p}} \mathfrak{p}^{d_{\mathfrak{p}}}$.

Sea $\vec{\alpha} \equiv 1$ mód $\mathfrak{c}$. Entonces $\alpha_{\mathfrak{p}} \in U_{\mathfrak{p}}^{(c_{\mathfrak{p}})}$. Definimos idèles $\vec{\beta}$ y $\vec{\gamma}$ dados por

$$\beta_{\mathfrak{p}} = \begin{cases} 1 & \text{si } n_{\mathfrak{p}} < m_{\mathfrak{p}} \\ \alpha_{\mathfrak{p}} & \text{si } n_{\mathfrak{p}} \geq m_{\mathfrak{p}} \end{cases}, \qquad \gamma_{\mathfrak{p}} = \begin{cases} \alpha_{\mathfrak{p}} & \text{si } n_{\mathfrak{p}} < m_{\mathfrak{p}} \\ 1 & \text{si } n_{\mathfrak{p}} \geq m_{\mathfrak{p}} \end{cases}.$$

Se sigue que $\vec{\beta} \equiv 1$ mód $\mathfrak{n}$ y que $\vec{\gamma} \equiv 1$ mód $\mathfrak{m}$. Por tanto $\vec{\alpha} = \vec{\beta}\vec{\gamma} \in C_K^{\mathfrak{n}} C_K^{\mathfrak{m}}$ lo cual implica $C_K^{\mathfrak{c}} \subseteq C_K^{\mathfrak{n}} C_K^{\mathfrak{m}}$.

Ahora, tenemos $C_K^{\mathfrak{m}} \subseteq C_K^{\mathfrak{c}}$ y $C_K^{\mathfrak{n}} \subseteq C_K^{\mathfrak{c}}$ por lo que $C_K^{\mathfrak{m}} C_K^{\mathfrak{n}} \subseteq C_K^{\mathfrak{c}}$. Se siguen las igualdades

$$C_K^{\mathfrak{c}} = C_K^{\mathfrak{n}} C_K^{\mathfrak{m}} = C_K^{\mathrm{mcd}(\mathfrak{n},\mathfrak{m})} \quad \text{y} \quad K^{\mathfrak{c}} = K^{\mathrm{mcd}(\mathfrak{n},\mathfrak{m})} = K^{\mathfrak{n}} \cap K^{\mathfrak{m}}.$$

Por otro lado $\mathfrak{n} | \mathfrak{d}$ y $\mathfrak{m} | \mathfrak{d}$. Por tanto $C_K^{\mathfrak{d}} \subseteq C_K^{\mathfrak{n}} \cap C_K^{\mathfrak{m}}$. Recíprocamente, consideremos $\vec{\alpha} \in C_K^{\mathfrak{n}} \cap C_K^{\mathfrak{m}}$. Entonces $\alpha_{\mathfrak{p}} \in U_{\mathfrak{p}}^{(n_{\mathfrak{p}})} \cap U_{\mathfrak{p}}^{(m_{\mathfrak{p}})} = U_{\mathfrak{p}}^{(\mathrm{máx}\{n_{\mathfrak{p}}, m_{\mathfrak{p}}\})} = U_{\mathfrak{p}}^{(d_{\mathfrak{p}})}$. Se sigue que $\vec{\alpha} \in C_K^{\mathfrak{d}}$ y que $C_K^{\mathfrak{n}} \cap C_K^{\mathfrak{m}} \subseteq C_K^{\mathfrak{d}}$. Hemos obtenido las igualdades

$$C_K^{\mathfrak{n}} \cap C_K^{\mathfrak{m}} = C_K^{\mathfrak{d}} \quad \text{y} \quad K^{\mathfrak{d}} = K^{\mathfrak{n}} K^{\mathfrak{m}}.$$

Resumimos nuestra discusión anterior en la siguiente proposición.

Proposición 7.1.9. *Si* $\mathfrak{n}$ *y* $\mathfrak{m}$ *son dos moduli,* $\mathfrak{c} = \mathrm{mcd}(\mathfrak{n}, \mathfrak{m})$ *y* $\mathfrak{d} = \mathrm{mcm}(\mathfrak{n}, \mathfrak{m})$*, entonces*

$$K^{\mathfrak{c}} = K^{\mathfrak{n}} \cap K^{\mathfrak{m}} \quad y \quad K^{\mathfrak{d}} = K^{\mathfrak{n}} K^{\mathfrak{m}}. \qquad \square$$

Observación 7.1.10. En general no se cumple que $\mathfrak{m}$ sea el conductor $\mathfrak{f}$ de $K^{\mathfrak{m}}/K$ aunque por supuesto $\mathfrak{f} | \mathfrak{m}$. Esto se debe a que se puede tener $C_K^{\mathfrak{f}} = C_K^{\mathfrak{m}}$ con $\mathfrak{f} | \mathfrak{m}$ y $\mathfrak{f} \neq \mathfrak{m}$. Más adelante (Consecuencia 7.1.13) veremos un ejemplo de este fenómeno. El lector puede pensar que lo esencial radica en que para n impar tenemos $\mathbb{Q}(\zeta_{2n}) = \mathbb{Q}(\zeta_n)$ y el conductor de $\mathbb{Q}(\zeta_{2n})$ es $\mathfrak{f} = n \cdot \infty$ y no $2 \cdot n \cdot \infty$.

Ejemplo 7.1.11. Ver [119, Theorem 7.7, página 100] y [117, Theorems 7.10 y 7.11, página 165]. Consideremos $K = \mathbb{Q}$. Los lugares de $\mathbb{Q}$ son ∞ y $\mathfrak{p} = (p)$ con p un número primo.

Se tiene $J_{\mathbb{Q}} = \{\vec{x} \in (\mathbb{R}^* \times \prod_{p \text{ primo}} \mathbb{Q}_p^*) \mid x_p \in \mathbb{Z}_p^* = U_{\mathbb{Q}_p} \text{ para casi toda } p\}$.

Sea $\mathfrak{m}$ un módulus, $\mathfrak{m} = \mathfrak{m}_0 \cdot \infty^{\varepsilon}$, donde $\mathfrak{m}_0 = \prod_{i=1}^{r} \mathfrak{p}_i^{\alpha_i}$, $\alpha_i \geq 0$, $1 \leq i \leq r$ y $\varepsilon \in \{0, 1\}$ con cada $\mathfrak{p}_i$ un primo finito. Por abuso del lenguaje, si $\mathfrak{p}_i = (p_i)$ con p_i un primo racional positivo, pondremos $\mathfrak{m}_0 = m = \prod_{i=1}^{r} p_i^{\alpha_i}$.

Se tiene

$$J_{\mathbb{Q}}^{\mathfrak{m}_0} = J_{\mathbb{Q}}^{m} = \mathbb{R}^* \times \prod_{p \text{ finito}} U_p^{(n_p)} = \mathbb{R}^* \times \prod_{i=1}^{r} U_{p_i}^{(\alpha_i)} \times \prod_{p \notin \{p_1,\dots,p_r\}} \mathbb{Z}_p^*$$
$$= \mathbb{R}^* \times \prod_{i=1}^{r} (1 + p_i^{\alpha_i}\mathbb{Z}_{p_i}) \times \prod_{p \notin \{p_1,\dots,p_r\}} \mathbb{Z}_p^*$$

y

$$J_{\mathbb{Q}}^{\mathfrak{m}_0\infty} = \mathbb{R}^+ \times \prod_{i=1}^{r} (1 + p_i^{\alpha_i}\mathbb{Z}_{p_i}) \times \prod_{p \notin \{p_1,\dots,p_r\}} \mathbb{Z}_p^*.$$

Sea $(m_0) = \mathfrak{m}_0$, es decir, m_0 es el generador de $\mathfrak{m}_0$ en $\mathbb{Q}^+$. Por supuesto, $m_0 = \prod_{i=1}^{r} p_i^{\alpha_i} \in \mathbb{N}$.

Ahora veamos que $U_p^{(n_p)}$ consiste de normas provenientes de $\mathbb{Q}_p(\zeta_m)/\mathbb{Q}_p$ $(=(\mathbb{Q}(\zeta_m))_{\mathfrak{P}}/\mathbb{Q}_{\mathfrak{p}}$, donde $\mathfrak{P}$ es un primo de $\mathbb{Q}(\zeta_{m_0})$ sobre $\mathfrak{p} = \langle p \rangle)$. Lo anterior se obtiene de la siguiente forma. Escribiendo $m = np^r$ con $\operatorname{mcd}(n,p) = 1$ se tiene $\mathbb{Q}_p(\zeta_m) = \mathbb{Q}_p(\zeta_n)\mathbb{Q}_p(\zeta_{p^r})$ y $\mathbb{Q}_p(\zeta_n)/\mathbb{Q}_p$ es no ramificada pues $p \nmid n$. Por el Teorema 5.1.11, se tiene $\mathrm{N}_{\mathbb{Q}_p(\zeta_n)/\mathbb{Q}_p} U_{\mathfrak{P}} = U_p$ donde $\mathfrak{P}$ es el primo de $\mathbb{Q}_p(\zeta_n)$, lo cual se sigue de que $H^0(G, U_{\mathfrak{P}}) = \{1\}$.

Por otro lado $\mathbb{Q}_p(\zeta_{p^r})/\mathbb{Q}_p$ es una extensión totalmente remificada y se tiene que $\mathrm{N}_{\mathbb{Q}_p(\zeta_{p^r})/\mathbb{Q}_p}\left(\mathbb{Q}_p(\zeta_{p^r})^*\right) = (p) \times U_p^{(r)}$ (Teorema 5.8.58). Del Teorema 5.7.14, si ponemos $L_1 = \mathbb{Q}_p(\zeta_n)$ y $L_2 = \mathbb{Q}_p(\zeta_{p^r})$, entonces $L = \mathbb{Q}_p(\zeta_m) = L_1L_2$ y se sigue, con $r = n_p$, que $U_p^{(n_p)} \subseteq \mathcal{N}_L = \mathcal{N}_{L_1L_2} = \mathcal{N}_{L_1} \cap \mathcal{N}_{L_2} = \mathrm{N}_{\mathbb{Q}_p(\zeta_m)/\mathbb{Q}_p}\left(\mathbb{Q}_p(\zeta_m)\right)^*$.

Ahora se tiene que un idèle $\vec{\alpha} \in J_K$ es la norma de un idèle $\vec{\beta} \in J_L$ si y solamente si cada componente $\alpha_{\mathfrak{p}} \in K_{\mathfrak{p}}^*$ es la norma de un elemento $\beta_{\mathfrak{P}} \in L_{\mathfrak{P}}^*$ para $\mathfrak{P}|\mathfrak{p}$ (ver Teorema 6.3.9). Por tanto se sigue $C_{\mathbb{Q}}^{\mathfrak{m}_0\infty} \subseteq \mathrm{N}_{\mathbb{Q}(\zeta_m)/\mathbb{Q}}(C_{\mathbb{Q}(\zeta_m)})$.

Consideremos $\mathfrak{m} = \mathfrak{m}_0\infty$. Se tiene que

$$[C_{\mathbb{Q}} : C_{\mathbb{Q}}^{\mathfrak{m}}] = [C_{\mathbb{Q}} : C_{\mathbb{Q}}^{1}][C_{\mathbb{Q}}^{1} : C_{\mathbb{Q}}^{\mathfrak{m}}] = h_{\mathbb{Q}}[J_{\mathbb{Q}}^{1}\mathbb{Q}^* : J_{\mathbb{Q}}^{\mathfrak{m}}\mathbb{Q}^*]$$
$$= 1 \cdot \frac{[J_{\mathbb{Q}}^{1} : J_{\mathbb{Q}}^{\mathfrak{m}}]}{[(J_{\mathbb{Q}}^{1} \cap \mathbb{Q}^*) : (J_{\mathbb{Q}}^{\mathfrak{m}} \cap \mathbb{Q}^*)]},$$

donde hemos utilizado el Corolario 6.8.6.

Ahora bien se tiene que $J_{\mathbb{Q}}^{1} = \mathbb{R}^* \times \prod_p U_p$ y que $J_{\mathbb{Q}}^{\mathfrak{m}} = \mathbb{R}^+ \times \prod_p U_p^{(n_p)}$, por lo que $J_{\mathbb{Q}}^{1} \cap \mathbb{Q}^* = \{1, -1\}$ y $J_{\mathbb{Q}}^{\mathfrak{m}} \cap \mathbb{Q}^* = \{1\}$. Por tanto obtenemos

$$[C_{\mathbb{Q}} : C_{\mathbb{Q}}^{\mathfrak{m}}] = \frac{1}{2}\prod_p [U_p : U_p^{(n_p)}][\mathbb{R}^* : \mathbb{R}^+] = \prod_p [U_p : U_p^{(n_p)}] = \prod_{p|m} p^{n_p - 1}(p-1)$$
$$= \varphi(m) = [\mathbb{Q}(\zeta_m) : \mathbb{Q}] = [C_{\mathbb{Q}} : \mathrm{N}_{\mathbb{Q}(\zeta_m)/\mathbb{Q}}(C_{\mathbb{Q}(\zeta_m)})]$$

y ya que tenemos $C_{\mathbb{Q}}^{\mathfrak{m}} \subseteq \mathrm{N}_{\mathbb{Q}(\zeta_m)/\mathbb{Q}}(C_{\mathbb{Q}(\zeta_m)})$ entonces $C_{\mathbb{Q}}^{\mathfrak{m}} = \mathrm{N}_{\mathbb{Q}(\zeta_m)/\mathbb{Q}}(C_{\mathbb{Q}(\zeta_m)})$.

En particular obtenemos que $\mathbb{Q}^{\mathfrak{m}} = \mathbb{Q}(\zeta_m)$.

Si consideramos ahora $\mathfrak{m} = \mathfrak{m}_0$, entonces se tiene que $C_{\mathbb{Q}}^{\mathfrak{m}_0} \subseteq C_{\mathbb{Q}}^{\mathfrak{m}}$, por lo que $\mathbb{Q}^{\mathfrak{m}_0} \subseteq \mathbb{Q}^{\mathfrak{m}}$. Por otro lado $[J_{\mathbb{Q}}^{\mathfrak{m}} : J_{\mathbb{Q}}^{\mathfrak{m}_0}] = 2$ de donde $[\mathbb{Q}^{\mathfrak{m}} : \mathbb{Q}^{\mathfrak{m}_0}] = 2$. Finalmente puesto que las normas de $\mathbb{Q}^{\mathfrak{m}_0}$ no están contenidas en $\mathbb{R}^+$, el campo $\mathbb{Q}^{\mathfrak{m}_0}$ necesariamente es real. Se sigue que $\mathbb{Q}^{\mathfrak{m}_0} = \mathbb{Q}(\zeta_m)^+ = \mathbb{Q}(\zeta_m + \zeta_m^{-1})$.

Corolario 7.1.12 (Teorema de Kronecker–Weber). *Toda extensión abeliana finita $L/\mathbb{Q}$ está contenida en algún campo ciclotómico.*

Más aún, si $L/\mathbb{Q}$ es una extensión abeliana finita con $L \subseteq \mathbb{R}$, entonces existe $m \in \mathbb{N}$ tal que $L \subseteq \mathbb{Q}(\zeta_m)^+$.

Se tiene que si $\mathfrak{m} = \mathfrak{m}_0\infty = m\infty$ es un módulus arbitrario de $\mathbb{Q}$, entonces $\mathbb{Q}^{\mathfrak{m}} = \mathbb{Q}(\zeta_m)$ y $\mathbb{Q}^{\mathfrak{m}_0} = \mathbb{Q}(\zeta_m)^+$.

Demostración. Los campos de clases de rayos de $\mathbb{Q}$ son los campos $\mathbb{Q}(\zeta_m)$ y $\mathbb{Q}(\zeta_m)^+ \subseteq \mathbb{Q}(\zeta_m)$ y toda extensión abeliana finita está contenida en algún campo de clases de rayos. Además $\mathfrak{m}_0|\mathfrak{m}_0\infty = \mathfrak{m}$ por lo que $K^{\mathfrak{m}_0} \subseteq K^{\mathfrak{m}} = \mathbb{Q}^{\mathfrak{m}} = \mathbb{Q}(\zeta_m)$. □

Consecuencia 7.1.13. El conductor de $K^{\mathfrak{m}}$ puede ser $\mathfrak{f} \neq \mathfrak{m}$, $\mathfrak{f}|\mathfrak{m}$. Por ejemplo, si $m \in \mathbb{N}$ es impar y $\mathfrak{m} = 2m\infty$ se tiene $\mathbb{Q}^{\mathfrak{m}} = \mathbb{Q}(\zeta_{2m}) = \mathbb{Q}(\zeta_m) = \mathbb{Q}^{\mathfrak{f}}$ donde $\mathfrak{f} = m\infty \neq \mathfrak{m}$.

Observación 7.1.14. Los campos de clases de rayos deben ser considerados como los análogos a los campos ciclotómicos pues $\mathbb{Q}^{\mathfrak{m}} = \mathbb{Q}(\zeta_m)$ donde $\mathfrak{m} = m \cdot \infty$ y si $\mathfrak{m}_0 = m$, entonces $\mathbb{Q}^{\mathfrak{m}_0} = \mathbb{Q}(\zeta_m)^+ = \mathbb{Q}(\zeta_m + \zeta_m^{-1})$.

Observación 7.1.15. Si consideramos a $\mathbb{C}/\mathbb{R}$ como una extensión de campos locales, entonces $\mathrm{N}_{\mathbb{C}/\mathbb{R}}\,\mathbb{C}^* = (\mathbb{R}^*)^2 = \mathbb{R}^+ = U_{\mathbb{R}}^{(1)}$. Por tanto el conductor en este caso es $\mathfrak{f} = \mathfrak{p}$ donde $\mathfrak{p}$ es el primo real.

Teorema 7.1.16. *Si $\mathfrak{f}$ es el conductor de una extensión abeliana finita L/K de campos numéricos y si si $\mathfrak{f}_{\mathfrak{p}}$ es conductor local de $L_{\mathfrak{p}}/K_{\mathfrak{p}}$ para $\mathfrak{p} \in \mathbb{P}_K$, entonces*

$$\mathfrak{f} = \mathfrak{f}_{L/K} = \prod_{\mathfrak{p} \in \mathbb{P}_K} \mathfrak{f}_{\mathfrak{p}}.$$

Demostración. Sean $\mathcal{N} = \mathrm{N}_{L/K}\, C_L$ y $\mathfrak{n} := \prod_{\mathfrak{p} \in \mathbb{P}_K} \mathfrak{f}_{\mathfrak{p}} = \prod_{\mathfrak{p} \in \mathbb{P}_K} \mathfrak{p}^{n_{\mathfrak{p}}}$. Por definición se tiene que para un módulus $\mathfrak{m} = \prod_{\mathfrak{p} \in \mathbb{P}_K} \mathfrak{p}^{m_{\mathfrak{p}}}$ tal que $C_K^{\mathfrak{m}} \subseteq \mathcal{N} = \mathrm{N}_{L/K}\, C_L$, entonces $C_K^{\mathfrak{m}} \subseteq C_K^{\mathfrak{f}} \subseteq \mathcal{N} \iff \mathfrak{f}|\mathfrak{m}$ y $C_K^{\mathfrak{f}} \subseteq \mathcal{N}$. Que $C_K^{\mathfrak{n}} \subseteq \mathcal{N}$ se prueba con el argumento al final de la demostración. Por tanto debemos probar que

$$C_K^{\mathfrak{m}} \subseteq \mathcal{N} \iff \mathfrak{n}|\mathfrak{m} \iff n_{\mathfrak{p}} \leq m_{\mathfrak{p}} \text{ para toda } \mathfrak{p} \iff f_{\mathfrak{p}}|\mathfrak{p}^{m_{\mathfrak{p}}}.$$

Se tiene:

$$\begin{aligned} C_K^{\mathfrak{m}} \subseteq \mathcal{N} &\iff \big(\vec{\alpha} \equiv 1 \bmod \mathfrak{m} \Longrightarrow \tilde{\vec{\alpha}} \in \mathcal{N}\big) \text{ para } \vec{\alpha} \in J_K \\ &\iff \big(\vec{\alpha} \equiv 1 \bmod \mathfrak{m} \Longrightarrow \lceil \alpha_{\mathfrak{p}} \rceil_{\mathfrak{p}} = (\ldots, 1, 1, \alpha_{\mathfrak{p}}, 1, 1, \ldots) \\ &\qquad\qquad \in \mathcal{N} \cap K_{\mathfrak{p}}^* = \mathrm{N}_{\mathfrak{p}}\, L_{\mathfrak{p}}^* \text{ para toda } \mathfrak{p}\big) \quad \text{(Teorema 6.3.9)} \\ &\iff \big(\alpha_{\mathfrak{p}} \in U_{\mathfrak{p}}^{(m_{\mathfrak{p}})} \Longrightarrow \alpha_{\mathfrak{p}} \in \mathrm{N}_{\mathfrak{p}}\, L_{\mathfrak{p}}^* \text{ para toda } \mathfrak{p}\big) \\ &\iff U_{\mathfrak{p}}^{(m_{\mathfrak{p}})} \subseteq \mathrm{N}_{\mathfrak{p}}\, L_{\mathfrak{p}}^* \text{ para toda } \mathfrak{p} \iff \mathfrak{f}_{\mathfrak{p}} | \mathfrak{p}^{m_{\mathfrak{p}}} \text{ para toda } \mathfrak{p}. \end{aligned}$$

Esto mismo prueba que $C_K^{\mathfrak{n}} \subseteq \mathcal{N}$ y por tanto $\mathfrak{n} = \mathfrak{f}$. □

Corolario 7.1.17. *Sea L/K una extensión abeliana finita de campos numéricos. Un primo $\mathfrak{p}$ de K es ramificado en $L \iff \mathfrak{p} | \mathfrak{f}$ donde $\mathfrak{f}$ es el conductor de L/K.*

Demostración. $\mathfrak{p}$ es ramificado en $L \iff \mathfrak{p}$ es ramificado en $L_{\mathfrak{P}}/K_{\mathfrak{p}} \iff \mathfrak{p} | \mathfrak{f}_{\mathfrak{p}}$ (Teorema 5.7.11). □

Definición 7.1.18. Sea K un campo numérico. El *campo de clase de Hilbert* K_H es la máxima extensión abeliana no ramificada de K.

Corolario 7.1.19. *El campo de clase de Hilbert K_H es el campo de clases de rayos módulo 1, es decir, $K_H = K^1$ (1 el módulus trivial) y*

$$\mathrm{Gal}(K_H/K) = \mathrm{Gal}(K^1/K) \cong C_K/C_K^1 \cong I_K. \qquad \square$$

En otras palabras, el campo de clase de Hilbert K_H de K corresponde a $J_K^{(1)} = \prod_{\mathfrak{p}} U_{\mathfrak{p}}$ o $C_K^{(1)} = J_K^{(1)} K^*/K^* = (\prod_{\mathfrak{p}} U_{\mathfrak{p}}) K^*/K^*$.

Definición 7.1.20. El *campo de clase de Hilbert extendido* K_{H^+} de un campo numérico K es la máxima extensión abeliana de K no ramificada en los primos finitos.

El campo K_{H^+} es el campo de clases de rayos módulo 1_+ donde 1_+ es el módulus $1_+ := \prod_{\mathfrak{p} \text{ real}} \mathfrak{p}$ (esto permite la ramificación de los primos reales). Los subgrupo de idèles correspondientes a los grupos de congruencias módulo 1_+ y módulo 1, y los grupos de congruencias mismos son:

$$J_K^{1_+} = \prod_{\mathfrak{p} \text{ real}} \mathbb{R}^+ \times \prod_{\mathfrak{p} \text{ complejo}} \mathbb{C}^* \times \prod_{\mathfrak{p} \nmid \infty} U_{\mathfrak{p}}, \quad C_K^{1_+} = J_K^{1_+} K^*/K^*,$$

$$J_K^{1} = \prod_{\mathfrak{p} \text{ real}} \mathbb{R}^* \times \prod_{\mathfrak{p} \text{ complejo}} \mathbb{C}^* \times \prod_{\mathfrak{p} \nmid \infty} U_{\mathfrak{p}}, \quad C_K^{1} = J_K^{1} K^*/K^*,$$

respectivamente. Se sigue que

$$\frac{J_K}{J_K^{1_+}} \cong \bigoplus_{\mathfrak{p}\ real} \frac{\mathbb{R}^*}{\mathbb{R}^+} \bigoplus \bigoplus_{\mathfrak{p} \nmid \infty} \frac{K_{\mathfrak{p}}^*}{U_{\mathfrak{p}}} \cong \Big(\bigoplus_{\mathfrak{p} \text{ real}} C_2 \Big) \bigoplus \Big(\bigoplus_{\mathfrak{p} \nmid \infty} \mathbb{Z} \Big) \cong C_2^r \oplus D_K \quad \text{y}$$

$$C_K/C_K^{1_+} = \text{conúcleo}\left(K^* \longrightarrow J_K/J_1^{1_+}\right) = J_K/J_K^{1_+} K^*$$

donde r es el número de lugares reales en K y C_n denota el grupo cíclico de n elementos.

Ejemplo 7.1.21. Por el teorema del discriminante de Minkowski, esto es, en toda extensión propia de $\mathbb{Q}$ hay primos finitos ramificados, entonces

$$\mathbb{Q}_H = \mathbb{Q}_{H^+} = \mathbb{Q}$$

y $r = 1$ en este caso. Notemos que $J^1_{\mathbb{Q}}/J^{1_+}_{\mathbb{Q}} \cong C_2$ pero $C^1_{\mathbb{Q}}/C^{1_+}_{\mathbb{Q}} = 1$.

Para K un campo numérico, se tiene

$$\frac{J_K}{J^1_K} \cong \bigoplus_{\mathfrak{p}\mid\infty} \frac{K^*_{\mathfrak{p}}}{U_{\mathfrak{p}}} \cong D_K \quad \text{y} \quad \frac{J^1_K}{J^{1_+}_K} \cong C_2^r.$$

Además

$$\mathrm{Gal}(K_{H^+}/K_H) \cong \frac{\mathrm{Gal}(K^{\mathrm{ab}}/K_H)}{\mathrm{Gal}(K^{\mathrm{ab}}/K_{H^+})} \cong \frac{C^1_K}{C^{1_+}_K} = \frac{J^1_K K^*/K^*}{J^{1_+}_K K^*} \cong \frac{J^1_K K^*}{J^{1_+}_K K^*}$$

y

$$\frac{J^1_K}{J^{1_+}_K} \cong C_2^r \twoheadrightarrow \frac{J^1_K K^*}{J^{1_+}_K K^*} \cong \mathrm{Gal}(K_{H^+}/K_H),$$

de donde $\mathrm{Gal}(K_{H^+}/K_H) \cong C_2^s$ con $s \leq r =$ número de lugares reales de K.

7.2. Campos de clases de rayos en campos de funciones

Ahora consideramos K un campo global de funciones. La máxima extensión abeliana no ramificada K^{nr} de K es el campo de clase correspondiente al grupo $U_K = \prod_{\mathfrak{p}\in\mathbb{P}_K} U_{\mathfrak{p}}$, el cual es abierto y cerrado en J_K puesto que $U_{\mathfrak{p}}$ es abierto y cerrado en $K^*_{\mathfrak{p}}$ para toda $\mathfrak{p}$, por lo que, por un lado es abierto por definición de la topología de J_K y por otro lado es compacto pues $U_{\mathfrak{p}}$ es compacto (ver Proposiciones 3.2.1 y 3.2.2) y U_K tiene la topología producto. Más precisamente K^{nr} es el campo correspondiente de $C^1_K = K^*U_K/K^* = C^1_K \subseteq C_{K,0} \subseteq C_K$ y $[C_K : C^1_K] = \infty = |\mathrm{Gal}(K^{\mathrm{nr}}/K)|$ (ver Observación 7.1.3). K^{nr} no es un campo de clase en el sentido de normas. Además $K\mathbb{F}_q^{\mathrm{ab}} \subseteq K^{\mathrm{nr}}$.

Se tiene $U_K \cap K^* = \{x \in K^* \mid v_{\mathfrak{p}}(x) = 0 \text{ para toda } \mathfrak{p} \in \mathbb{P}_K\} = \mathbb{F}_q^*$. Además $U_K \subseteq J_{K,0}$ y $J_{K,0}/U_K \cong D_{K,0}$, el grupo de divisores de grado 0. Por el isomorfismo $\rho_K : \hat{C}_K \longrightarrow G_K^{\mathrm{ab}}$, se sigue que $C_{K,0} \cong \mathrm{Gal}(K^{\mathrm{ab}}/K\mathbb{F}_q^{\mathrm{ab}})$. Se tiene

$$\frac{C_{K,0}}{C^1_K} \cong \frac{C_{K,0}}{\left(U_K K^*/K^*\right)} \cong \mathrm{Gal}(K^{\mathrm{nr}}/K\mathbb{F}_q^{\mathrm{ab}}) \quad \text{y}$$

$$\Lambda : J_{K,0} \longrightarrow D_{K,0}, \quad \Lambda(\vec{\alpha}) = \mathfrak{a}_{\vec{\alpha}} = \prod_{\mathfrak{p}\in\mathbb{P}_K} \mathfrak{p}^{v_{\mathfrak{p}}(\alpha_{\mathfrak{p}})}, \quad \text{núc}\,\Lambda = U_K K^* \quad \text{y}$$

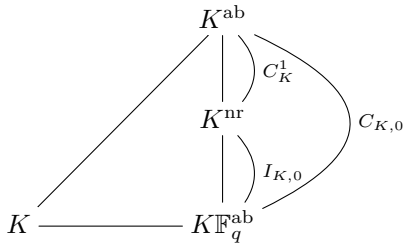
$$J_{K,0} \overset{\Lambda}{\twoheadrightarrow} D_{K,0} \overset{\pi}{\twoheadrightarrow} D_{K,0}/P_K \cong I_{K,0}, \quad \text{núc}(\pi \circ \Lambda) = U_K K^*.$$

Esto es,

$$I_{K,0} \cong \frac{J_{K,0}}{U_K K^*} \cong \frac{J_{K,0}/K^*}{U_K K^*/K^*} \cong \frac{C_{K,0}}{C_K^1} \cong \mathrm{Gal}(K^{\mathrm{nr}}/K\mathbb{F}_q^{\mathrm{ab}})$$
$$(J_K^1 = \prod_{\mathfrak{p}} U_{\mathfrak{p}}^{(0)} = \prod_{\mathfrak{p}} U_{\mathfrak{p}} = U_K, \quad C_K^1 = \frac{J_K^1 K^*}{K^*} = \frac{U_K K^*}{K^*}).$$

Teorema 7.2.1. *Bajo el mapeo de reciprocidad, se tiene el isomorfismo*

$$I_{K,0} \cong \mathrm{Gal}(K^{\mathrm{nr}}/K\mathbb{F}_q^{\mathrm{ab}}) \cong \frac{C_{K,0}}{C_K^1}. \qquad \square$$



Ahora consideremos los grupos de clases de rayos. Sea $\mathfrak{m} = \prod_{\mathfrak{p}\in\mathbb{P}_K} \mathfrak{p}^{n_{\mathfrak{p}}} = \prod_{i=1}^r \mathfrak{p}_i^{\alpha_i}$ un módulus. Sea

$$J_K^{\mathfrak{m}} = \prod_{\mathfrak{p}\in\mathbb{P}_K} U_{\mathfrak{p}}^{(n_{\mathfrak{p}})} = \prod_{\mathfrak{p}\nmid\mathfrak{m}} U_{\mathfrak{p}} \times \prod_{i=1}^r U_{\mathfrak{p}_i}^{(\alpha_i)}.$$

Sea $C_K^{\mathfrak{m}} = J_K^{\mathfrak{m}} K^*/K^*$. Se tiene $C_K^{\mathfrak{m}} \subseteq C_{K,0}$ pues si $\vec{x} \in J_K^{\mathfrak{m}}$, $v_{\mathfrak{p}}(x_{\mathfrak{p}}) = 0$ para toda $\mathfrak{p} \in \mathbb{P}_K$. Además

$$\begin{aligned}
[C_{K,0} : C_K^{\mathfrak{m}}] &= [C_{K,0} : C_K^1][C_K^1 : C_K^{\mathfrak{m}}], \\
[C_{K,0} : C_K^1] &= |\,\mathrm{Gal}(K^{\mathrm{nr}}/K\mathbb{F}_q^{\mathrm{ab}})| = |I_{K,0}| = h_K < \infty \quad \text{y} \\
[C_K^1 : C_K^{\mathfrak{m}}] &= [K^* J_K^1/K^* : K^* J_K^{\mathfrak{m}}/K^*] \le [J_K^1 : J_K^{\mathfrak{m}}] \\
&:= \Psi(\mathfrak{m}) := \prod_{i=1}^r [U_{\mathfrak{p}_i} : U_{\mathfrak{p}_i}^{(\alpha_i)}] \\
&= \prod_{i=1}^r q^{(\alpha_i - 1)\,\mathrm{gr}\,\mathfrak{p}_i} \left(q^{\mathrm{gr}\,\mathfrak{p}_i} - 1\right) < \infty.
\end{aligned}$$

Por lo tanto,

Proposición 7.2.2. *Tenemos* $[C_{K,0} : C_K^{\mathfrak{m}}] \le h_K \Psi(\mathfrak{m}) < \infty$, *donde* $\Psi(\mathfrak{m}) = \prod_{\mathfrak{p}\in\mathrm{sop}(\mathfrak{m})} (q^{\mathrm{gr}\,\mathfrak{p}} - 1) q^{(n_{\mathfrak{p}}-1)\,\mathrm{gr}\,\mathfrak{p}}$, $\mathrm{sop}(\mathfrak{m})$ *denota al soporte de* $\mathfrak{m}$, *es decir* $\mathrm{sop}(\mathfrak{m}) = \{\mathfrak{p} \in \mathbb{P}_K \mid \mathfrak{p}\big|\mathfrak{m}\}$.

Demostración. Para $\mathfrak{m}$ un módulus arbitrario tenemos

$$\begin{aligned}\Psi(\mathfrak{m}) &= \prod_{\mathfrak{p}\in\mathbb{P}_K}[U_\mathfrak{p}:U_\mathfrak{p}^{(n_\mathfrak{p})}] = [U_\mathfrak{p}:U_\mathfrak{p}^{(n_\mathfrak{p})}] = \prod_{i=0}^{n_\mathfrak{p}-1}[U_\mathfrak{p}^{(i)}:U_\mathfrak{p}^{(i+1)}]\\ &= [U_\mathfrak{p}:U_\mathfrak{p}^{(1)}]\prod_{i=1}^{n_\mathfrak{p}-1}[U_\mathfrak{p}^{(i)}:U_\mathfrak{p}^{(i+1)}] = |\mathbb{F}_{q^{\operatorname{gr}\mathfrak{p}}}^*|\prod_{i=1}^{n_\mathfrak{p}-1}|\mathbb{F}_{q^{\operatorname{gr}\mathfrak{p}}}|\\ &= (q^{\operatorname{gr}\mathfrak{p}}-1)q^{(n_\mathfrak{p}-1)\operatorname{gr}\mathfrak{p}}.\end{aligned}$$

□

7.2.1. Otro tipo de clases de rayos en campos de funciones

Sea B un subgrupo abierto de C_K de índice finito. Sea $\tilde{\vec{b}} \in B$ tal que $\operatorname{gr}(\tilde{\vec{b}}) := \min\{\operatorname{gr}(\tilde{\vec{\alpha}}) \mid \tilde{\vec{\alpha}} \in B, \operatorname{gr}(\tilde{\vec{\alpha}}) > 0\}$.

Sea $B_0 := B \cap C_{K,0}$. Entonces $B = \cup_{n=1}^{\infty}\tilde{\vec{b}}^n B_0$ pues

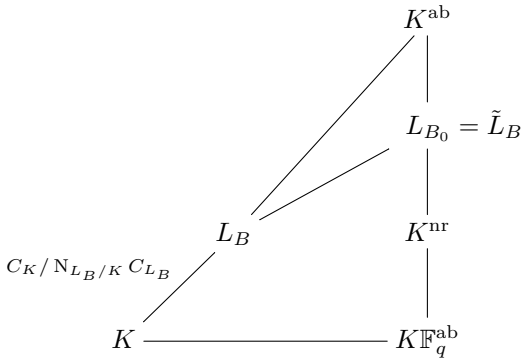
$$B/B_0 = B/(B\cap C_{K,0}) \cong BC_{K,0}/C_{K,0} \subseteq C_K/C_{K,0} \cong \mathbb{Z},$$

y tenemos que B_0 es abierto en $C_{K,0}$ pues B es abierto y puesto que $C_{K,0}$ también es abierto, se tiene que B_0 es abierto.

Ahora bien, se tiene que los conjuntos $C_K^\mathfrak{m}$ forman un sistema fundamental de vecindades de $1 \in C_K$ debido a que los $J_K^\mathfrak{m}$ forman un sistema fundamental de vecindades de $1 \in J_K$. Como B_0 es abierto, entonces B_0 debe contener a algún $C_K^\mathfrak{m} \subseteq B_0$ y

$$h_K\Psi(\mathfrak{m}) = [C_{K,0}:C_K^\mathfrak{m}] = [C_{K,0}:B_0][B_0:C_K^\mathfrak{m}] < \infty,$$

se sigue que $[C_{K,0}:B_0] < \infty$. Sea L_B el campo de clase de B, $C_K/B = C_K/\operatorname{N}_{L_B/K}C_{L_B} \cong \operatorname{Gal}(L_B/K)$ con $B = \operatorname{N}_{L_B/K}C_{L_B}$.



De esta forma, B_0 corresponde al campo $L_{B_0} = \tilde{L}_B := L_B\mathbb{F}_q^{\mathrm{ab}}$ (no podemos decir que $C_K/\operatorname{N}_{\tilde{L}_B/K}C_{\tilde{L}_B} \cong \operatorname{Gal}(\tilde{L}_B/K)$ pues $\tilde{L}_B/K$ es infinita y no tenemos definida la norma).

Las clases de rayos que hemos definido, tienen el inconveniente de no ser de índice finito en C_K. Definimos otros grupos de clases de rayos de tal manera que serán abiertos y de índice finito en C_K. Se puede hacer el estudio para K un campo global arbitrario. Solo haremos el desarrollo para campos de funciones en donde $S \neq \emptyset$. Para el caso numérico, se puede tomar $S = \emptyset$.

Sea K un campo de funciones y sea S un conjunto de lugares de K, el cual, eventualmente, pediremos que sea finito y no vacío.

Definición 7.2.3. Un *S–módulus* es un módulus $\mathfrak{m} = \prod_{\mathfrak{p}\in\mathbb{P}_K} \mathfrak{p}^{n_\mathfrak{p}}$ tal que si $n_\mathfrak{p} > 0$ entonces $\mathfrak{p} \notin S$, es decir, el soporte de $\mathfrak{m}$ es disjunto de S, esto es, si $\mathfrak{m} = \prod_{i=1}^{r} \mathfrak{p}_i^{\alpha_i}$, entonces $S \cap \{\mathfrak{p}_1, \ldots, \mathfrak{p}_r\} = \emptyset$.

Definición 7.2.4. Sea $\mathfrak{m} = \prod_{\mathfrak{p}\in\mathbb{P}_K} \mathfrak{p}^{n_\mathfrak{p}}$ un S–módulus. Se definen los *subgrupos de S–congruencias módulo* $\mathfrak{m}$ por

$$\begin{aligned} J_{K,S}^{\mathfrak{m}} &:= \Big(\prod_{\mathfrak{p}\in S} K_\mathfrak{p}^* \times \prod_{\mathfrak{p}\in\mathbb{P}_K\setminus S} U_\mathfrak{p}^{(n_\mathfrak{p})} \Big) \bigcap J_K \\ &= \Big(\prod_{\mathfrak{p}\in S} K_\mathfrak{p}^* \times \prod_{i=1}^{r} U_{\mathfrak{p}_i}^{(\alpha_i)} \times \prod_{\substack{\mathfrak{p}\notin S\cup \\ \{\mathfrak{p}_1,\ldots,\mathfrak{p}_r\}}} U_\mathfrak{p} \Big) \bigcap J_K \quad \text{y} \\ C_{K,S}^{\mathfrak{m}} &:= \frac{J_{K,S}^{\mathfrak{m}} K^*}{K^*} \end{aligned}$$

de J_K y de C_K respectivamente, y donde $\mathfrak{m} = \prod_{\mathfrak{p}\in\mathbb{P}_K} \mathfrak{p}^{n_\mathfrak{p}}$.

Observación 7.2.5. La intersección con J_K únicamente tiene significado cuando $|S| = \infty$. Cuando S es un conjunto finito, tenemos que $\big(\prod_{\mathfrak{p}\in S} K_\mathfrak{p}^* \times \prod_{\mathfrak{p}\in\mathbb{P}_K\setminus S} U_\mathfrak{p}^{(n_\mathfrak{p})} \big) \subseteq J_K$.

Proposición 7.2.6. *Sea $S \subseteq \mathbb{P}_K$ y $\mathfrak{m} = \prod_{\mathfrak{p}\in\mathbb{P}_K} \mathfrak{p}^{n_\mathfrak{p}}$ un S–módulus.*

(a) *Si $T \subseteq S$ y $\mathfrak{m}|\mathfrak{n}$ donde $\mathfrak{n}$ es un T–módulus, entonces*

$$J_{K,T}^{\mathfrak{n}} \subseteq J_{K,S}^{\mathfrak{m}} \quad y \quad C_{K,T}^{\mathfrak{n}} \subseteq C_{K,S}^{\mathfrak{m}}.$$

(b) *Si $T \subseteq \mathbb{P}_K$ y $\mathfrak{n}$ es un T–módulus,*

$$J_{K,S}^{\mathfrak{m}} J_{K,T}^{\mathfrak{n}} = J_{K,S\cup T}^{\mathrm{mcd}(\mathfrak{m},\mathfrak{n})}.$$

(c) *Los subgrupos de congruencias $J_{K,\emptyset}^{\mathfrak{m}} = J_K^{\mathfrak{m}}$ y $C_{K,\emptyset}^{\mathfrak{m}} = C_K^{\mathfrak{m}}$ con $\mathfrak{m}$ recorriendo todos los módulus, forman una base de vecindades abiertas de 1 en J_K y C_K respectivamente.*

(d) *$J_{K,S}^{\mathfrak{m}}$ y $C_{K,S}^{\mathfrak{m}}$ son abiertos.*

(e) *$J_{K,S}^{1}/J_{K,S}^{\mathfrak{m}} \cong \prod_{\mathfrak{p}} \big(U_\mathfrak{p}/U_\mathfrak{p}^{(m_\mathfrak{p})}\big)$ y $[J_{K,S}^{1} : J_{K,S}^{\mathfrak{m}}] = \Psi(\mathfrak{m})$.*

(f) *$[C_K : C_{K,\emptyset}^{\mathfrak{m}}] = [C_K : C_K^{\mathfrak{m}}] = \infty$ para toda $\mathfrak{m}$.*

(g) *$K^* J_{K,\mathbb{P}_K\setminus \mathrm{sop}(\mathfrak{m})}^{\mathfrak{m}} = J_K$ para toda $\mathfrak{m}$.*

(h) $J^{\mathfrak{m}}_{K,S}$ *es topológicamente generado por* $\lceil K^*_{\mathfrak{p}}\rceil_{\mathfrak{p}}$, $\mathfrak{p}\in S$ *y* $\lceil U^{(n_{\mathfrak{p}})}_{\mathfrak{p}}\rceil_{\mathfrak{p}}$, $\mathfrak{p}\in\mathbb{P}_K\setminus S$, *donde* $\lceil\ \rceil_{\mathfrak{p}}\colon K^*_{\mathfrak{p}}\longrightarrow J_K$ *está definido por* $\lceil x\rceil_{\mathfrak{p}} = (\ldots,1,1,\underset{\underset{\mathfrak{p}}{\uparrow}}{x},1,1,\ldots)$.

Demostración. [10, 11].
(f) Sea $\mathfrak{p}\in\mathbb{P}_K\setminus\operatorname{sop}(\mathfrak{m})$, $K^*_{\mathfrak{p}}\xrightarrow[\lceil\ \rceil_{\mathfrak{p}}]{} J_K/K^*J^{\mathfrak{m}}_{K,\emptyset}$ tiene núcleo $U_{\mathfrak{p}}$ y $K^*_{\mathfrak{p}}/U_{\mathfrak{p}}\cong\mathbb{Z}$.
(g) Se sigue del Teorema de Aproximación de Artin. □

Ahora bien, puesto que $[C_K : C^{\mathfrak{m}}_{K,\emptyset}] = [C_K : C^{\mathfrak{m}}_K] = \infty$, se pedirá en lo futuro que $S\neq\emptyset$. En este caso veremos que $[C_K : C^{\mathfrak{m}}_{K,S}] < \infty$, el cual es un dominio Dedekind.

Sea S un conjunto no vacío de lugares, $S\neq\emptyset$ y sea $\mathcal{O}_S = \cap_{\mathfrak{p}\notin S}\mathcal{O}_{\mathfrak{p}} = \{x\in K \mid v_{\mathfrak{p}}(x)\geq 0\ \forall\ \mathfrak{p}\notin S\}$.

Definición 7.2.7. Sea $\mathfrak{m}$ cualquier S–módulus con $S\neq\emptyset$. Definimos el *S–grupo de clases módulo* $\mathfrak{m}$, $Cl^{\mathfrak{m}}_K(\mathcal{O}_S)$ como el cociente de los ideales fraccionarios de $\mathcal{O}_S$ primos relativos a $\mathfrak{m}$ módulo los ideales principales $z\mathcal{O}_S$ con $z\in K^*\cap J^{\mathfrak{m}}_{K,\mathbb{P}_K\setminus\operatorname{sop}(\mathfrak{m})}$ (si $\mathfrak{m}=1$, $J^{\mathfrak{m}}_{K,\mathbb{P}_K\setminus\operatorname{sop}(\mathfrak{m})} = J^1_{K,\mathbb{P}_K\setminus\emptyset} = J_K$).

En particular $Cl^1_K(\mathcal{O}_S) = Cl_K(\mathcal{O}_S)$ es el grupo de S–clases usuales, es decir, el grupo de clases del dominio Dedekind $\mathcal{O}_S$. En este caso sabemos que $h_S = |Cl(\mathcal{O}_S)| < \infty$. De hecho se tiene la sucesión exacta

$$0\longrightarrow\frac{D_{K,0}(S)}{P_K(S)}\longrightarrow\frac{D_{K,0}}{P_K}\cong I_{K,0}\longrightarrow Cl(\mathcal{O}_S)\xrightarrow{\text{gr}}\mathbb{Z}/d\mathbb{Z}\longrightarrow 0,$$

donde $D_K(S)$ son los divisores con soporte en S, $D_{K,0}(S) = D_K(S)\cap D_{K,0}$ y $d = \operatorname{gr}(D^S_K) = \operatorname{mcd}\{\operatorname{gr}\mathfrak{p}\mid\mathfrak{p}\in S\}$ y $P_K(S) = P_K\cap D_K(S)$.

Teorema 7.2.8. *Sea* $S\subseteq\mathbb{P}_K$, $S\neq\emptyset$ *y sea* $\mathfrak{m}$ *un S–módulus. Entonces*

(a) $Cl^{\mathfrak{m}}_K(\mathcal{O}_S)\cong C_K/C^{\mathfrak{m}}_{K,S}$.
(b) *La sucesión*

$$\mathcal{O}^*_S\longrightarrow\frac{J^1_{K,S}}{J^{\mathfrak{m}}_{K,S}}\longrightarrow\frac{J_K}{K^*J^{\mathfrak{m}}_{K,S}}\longrightarrow\frac{J_K}{K^*J^1_{K,S}}\longrightarrow 1$$

es exacta,
(c) $[C_K : C^{\mathfrak{m}}_{K,S}]$ *es finito.*

Demostración. (a) La función $\theta\colon J^{\mathfrak{m}}_{K,\mathfrak{p}\in\mathbb{P}_K\setminus\operatorname{sop}(\mathfrak{m})}\longrightarrow Cl^{\mathfrak{m}}_K(\mathcal{O}_S)$ dado por

$$\theta(\vec{\alpha}) = \prod_{\mathfrak{p}\in\mathbb{P}_K\setminus S}(\mathfrak{p}\cap\mathcal{O}_S)^{v_{\mathfrak{p}}(\alpha_{\mathfrak{p}})}\ \text{mód}\ P^{\mathfrak{m}}_{K,S}$$

es suprayectiva y $\operatorname{núc}\theta = J^{\mathfrak{m}}_{K,S}\big(K^*\cap J^{\mathfrak{m}}_{K,\mathbb{P}_K\setminus\operatorname{sop}(\mathfrak{m})}\big) = K^*J^{\mathfrak{m}}_{K,S}\cap J^{\mathfrak{m}}_{K,\mathbb{P}_K\setminus\operatorname{sop}(\mathfrak{m})}$.

Por tanto

$$Cl_K^{\mathfrak{m}}(\mathcal{O}_S) = \frac{J_{K,\mathbb{P}_K\setminus \mathrm{sop}(\mathfrak{m})}^{\mathfrak{m}}}{K^* J_{K,S}^{\mathfrak{m}} \cap J_{K,\mathbb{P}_K\setminus \mathrm{sop}(\mathfrak{m})}^{\mathfrak{m}}} = \frac{K^* J_{K,\mathbb{P}_K\setminus \mathrm{sop}(\mathfrak{m})}^{\mathfrak{m}}}{K^* J_{K,S}^{\mathfrak{m}}}$$
$$= \frac{J_K}{K^* J_{K,S}^{\mathfrak{m}}} \cong \frac{C_K}{C_{K,S}^{\mathfrak{m}}}.$$

(b) Se deja al cuidado del lector.
(c) Se sigue de (b) pues tanto $J_{K,S}^1/J_{K,S}^{\mathfrak{m}}$ como $J_K/K^* J_{K,S}^1 \cong Cl(\mathcal{O}_S)$ son grupos finitos. □

Repetimos la demostración de lo fundamental del Teorema 7.2.8 con una notación más simple. Sea S un conjunto finito, $\mathcal{O}_S = \bigcap_{\mathfrak{p}\notin S} \mathcal{O}_{\mathfrak{p}} = \{x \in K \mid v_{\mathfrak{p}}(x) \geq 0 \text{ para toda } \mathfrak{p} \notin S\}$ el cual es un dominio Dedekind y definimos $I_{K,S} = \frac{D_K^S}{P_K^S}$ donde $D_K^S = \frac{D_K}{\langle S\rangle}$ es el grupo de divisores de K con soporte en el complemento de S. Se tiene $D_K = \langle \mathfrak{p} \mid \mathfrak{p} \in \mathbb{P}_K \setminus S\rangle$, y P_K^S son los divisores principales de $\mathcal{O}_S$.

Por el teorema de F.K. Schmidt, $h_S = |I_{K,S}| < \infty$ ([136, Corolario 10.2.14]). Sean

$$\Lambda : J_K \longrightarrow\!\!\!\!\rightarrow D_K^S, \quad \Lambda(\vec{\alpha}) = \prod_{\mathfrak{p}\notin S} \mathfrak{p}^{v_{\mathfrak{p}}(\alpha_{\mathfrak{p}})} \quad \text{y} \quad \pi : D_K^S \longrightarrow I_{K,S}$$

la proyección natural. Sea

$$\psi = \Lambda \circ \pi : J_K \longrightarrow\!\!\!\!\rightarrow I_{K,S}, \quad \psi(\vec{\alpha}) = \prod_{\mathfrak{p}\notin S} \mathfrak{p}^{v_{\mathfrak{p}}(\alpha_{\mathfrak{p}})} \text{ mód } P_K^S.$$

Sea $\vec{\alpha} \in \text{núc}\,\psi$. Entonces $(\pi \circ \Lambda)(\vec{\alpha}) = 1$, por lo que $\Lambda(\vec{\alpha}) \in P_K^S$. Por tanto existe $x \in K^*$ con $\prod_{\mathfrak{p}\notin S} \mathfrak{p}^{v_{\mathfrak{p}}(\alpha_{\mathfrak{p}})} = \prod_{\mathfrak{p}\notin S} \mathfrak{p}^{v_{\mathfrak{p}}(x)}$, donde se sigue que $v_{\mathfrak{p}}(\alpha_{\mathfrak{p}} x^{-1}) = 0$ para toda $\mathfrak{p} \notin S$. De esta forma obtenemos $\vec{\alpha}x^{-1} \in J_{K,S}$. Por tanto $\vec{\alpha} \in J_{K,S}K^*$. El recíproco también se cumple. Se sigue que $\text{núc}\,\psi = J_{K,S}K^*$.

Por tanto

$$I_{K,S} \cong \frac{J_K}{J_{K,S}K^*} \cong \frac{J_K/K^*}{J_{K,S}K^*/K^*} \cong \frac{C_K}{C_{K,S}} \quad \text{y por tanto} \quad I_{K,S} \cong \frac{C_K}{C_{K,S}}.$$

Ahora $C_{K,S} = C_{K,S}^1$, por lo que $[C_K : C_{K,S}^1] < \infty$. Además

$$[C_K : C_{K,S}^{\mathfrak{m}}] = [C_K : C_{K,S}^1][C_{K,S}^1 : C_{K,S}^{\mathfrak{m}}] = |I_{K,S}|[C_{K,S}^1 : C_{K,S}^{\mathfrak{m}}].$$

Además

$$[J_{K,S}^1 : J_{K,S}^{\mathfrak{m}}] = \prod_{\mathfrak{p}\notin S} [U_{\mathfrak{p}} : U_{\mathfrak{p}}^{(m_{\mathfrak{p}})}] = \prod_{i=1}^{r} [U_{\mathfrak{p}_i} : U_{\mathfrak{p}_i}^{(\alpha_i)}] < \infty \quad \text{y}$$
$$[C_{K,S}^1 : C_{K,S}^{\mathfrak{m}}] \leq [J_{K,S}^1 K^*/K^* : J_{K,S}^{\mathfrak{m}} K^*/K^*] \leq [J_{K,S}^1 : J_{K,S}^{\mathfrak{m}}] < \infty.$$

Se sigue que $[C_K : C_{K,S}^{\mathfrak{m}}] < \infty$.
Esto es, nuevamente hemos obtenido

Teorema 7.2.9. *Sean K un campo de funciones, S un conjunto finito no vacío de primos de K y $\mathfrak{m} = \prod_{i=1}^{r} \mathfrak{p}_i^{\alpha_i}$ un módul tal que $S \cap \{\mathfrak{p}_1, \ldots, \mathfrak{p}_r\} = \emptyset$. Sea $C_{K,S}^{\mathfrak{m}} = J_{K,S}^{\mathfrak{m}} K^*/K^*$, donde*

$$J_{K,S}^{\mathfrak{m}} = \prod_{\mathfrak{p} \in S} K_{\mathfrak{p}}^* \times \prod_{\substack{\mathfrak{p} \notin S \cup \\ \{\mathfrak{p}_1, \ldots, \mathfrak{p}_r\}}} U_{\mathfrak{p}} \times \prod_{i=1}^{r} U_{\mathfrak{p}_i}^{(\alpha_i)}.$$

Entonces $[C_K : C_{K,S}^{\mathfrak{m}}] < \infty$. □

Definición 7.2.10. Por el teorema de existencia, se define $K_S^{\mathfrak{m}}$ como *campo de clase asociado al grupo de congruencia $C_{K,S}^{\mathfrak{m}}$* y se llama el *campo de clases de S–rayos módulo $\mathfrak{m}$*. Se tiene

$$\mathrm{Gal}(K_S^{\mathfrak{m}}/K) \cong J_K/K^* J_{K,S}^{\mathfrak{m}} \cong C_K/C_{K,S}^{\mathfrak{m}} \cong Cl_K^{\mathfrak{m}}(\mathcal{O}_S).$$

Teorema 7.2.11. *En $K_S^{\mathfrak{m}}$, $\mathfrak{p}_1, \ldots, \mathfrak{p}_r$ son los primos ramificados y si $\mathfrak{p} \in S$, entonces $\mathfrak{p}$ se descompone totalmente en $K_S^{\mathfrak{m}}/K$.*

Demostración. Se sigue de que $J_{K,S}^{\mathfrak{m}} = \prod_{\mathfrak{p} \in S} K_{\mathfrak{p}}^* \times \prod_{\substack{\mathfrak{p} \notin S \cup \\ \{\mathfrak{p}_1, \ldots, \mathfrak{p}_r\}}} U_{\mathfrak{p}} \times \prod_{i=1}^{r} U_{\mathfrak{p}_i}^{(\alpha_i)}$.
□

Observación 7.2.12. K_S^1 es el campo de clase de Hilbert de $\mathcal{O}_S$ en el sentido de Rosen, con la pequeña generalización que aquí, de momento, S puede ser infinito. Es decir, K_S^1/K es la máxima extensión abeliana no ramificada de K tal que todos los primos de S se descomponen totalmente. Este es el tercer análogo al campo de clase de Hilbert en campos de funciones.

Cuando $S = \{\mathfrak{p}_\infty\}$ consiste de un solo primo, $K_S^{\mathfrak{m}}$ se puede construir en término de módulos de Drinfeld de rango 1 (ver Hayes [61] y [136, Capítulo 15]).

Proposición 7.2.13. *Si S y T son dos subconjuntos no vacíos de $\mathbb{P}_K$, $\mathfrak{m}$ es un S–módulos y $\mathfrak{n}$ es un T–módulus, entonces*

(a) *Si $S \supseteq T$ y $\mathfrak{m}|\mathfrak{n}$, entonces $K_S^{\mathfrak{m}} \subseteq K_T^{\mathfrak{n}}$.*
(b) $K_S^{\mathfrak{m}} \cap K_T^{\mathfrak{n}} = K_{S \cup T}^{\mathrm{mcd}(\mathfrak{m},\mathfrak{n})}$.
(c) *Si $T \subseteq S$ y $\mathfrak{m}|\mathfrak{n}$ y $\mathfrak{n}$ también es un S–módulus, entonces*

$$[K_S^{\mathfrak{n}} : K_S^{\mathfrak{m}}] \leq [K_T^{\mathfrak{n}} : K_T^{\mathfrak{m}}].$$

Demostración. (a) Se tiene que $C_{K,T}^{\mathfrak{n}} \subseteq C_{K,S}^{\mathfrak{m}}$ por lo que $K_S^{\mathfrak{m}} \subseteq K_T^{\mathfrak{n}}$.
(b) $C_{K,S}^{\mathfrak{m}} C_{K,T}^{\mathfrak{n}} = C_{K,S\cup T}^{\mathrm{mcd}(\mathfrak{m},\mathfrak{n})}$ por lo tanto $K_S^{\mathfrak{m}} \cap K_T^{\mathfrak{n}} = K_{S\cup T}^{\mathrm{mcd}(\mathfrak{m},\mathfrak{n})}$.
(c) Los mapeos de Artin $(\_, K_S^{\mathfrak{m}}/K)$ y $(\_, K_T^{\mathfrak{n}}/K)$ inducen isomorfismos $K^*J_{K,S}^{\mathfrak{m}}/K^*J_{K,S}^{\mathfrak{n}} \cong \mathrm{Gal}(K_S^{\mathfrak{n}}/K_S^{\mathfrak{m}})$ y $K^*J_{K,T}^{\mathfrak{m}}/K^*J_{K,T}^{\mathfrak{n}} \cong \mathrm{Gal}(K_T^{\mathfrak{n}}/K_T^{\mathfrak{m}})$ y el mapeo

$$K^*J_{K,T}^{\mathfrak{m}}/K^*J_{K,T}^{\mathfrak{n}} \longrightarrow K^*J_{K,S}^{\mathfrak{m}}/K^*J_{K,S}^{\mathfrak{n}}$$

es suprayectivo. □

Debido al Teorema 7.1.16, tenemos la siguiente definición.

Definición 7.2.14. Sea L/K una extensión abeliana finita de campos de funciones globales. Entonces definimos el *conductor* de la extensión L/K como

$$\mathfrak{f} = \mathfrak{f}_{L/K} = \mathfrak{f}(L/K) = \prod_{\mathfrak{p}\in\mathbb{P}_K} \mathfrak{f}_{\mathfrak{p}},$$

donde $\mathfrak{f}_{\mathfrak{p}}$ denota al conductor de la extensión de campos locales $L_{\mathfrak{p}}/K_{\mathfrak{p}}$.

Teorema 7.2.15 (Teorema del Conductor). *Sea L/K una extensión abeliana finita de campos de funciones y sea S un subconjunto no vacío de*

$$\mathrm{Spl}(L/K) = \{\mathfrak{p} \in \mathbb{P}_K \mid \mathfrak{p} \text{ se descompone totalmente en } L/K\}.$$

Entonces el conductor $\mathfrak{f} = \mathfrak{f}(L/K)$ es el S–módulus mínimo $\mathfrak{m}$ tal que $L \subseteq K_S^{\mathfrak{m}}$.

Demostración. Sea $\mathfrak{m} = \prod_{\mathfrak{p}\in\mathbb{P}_K} \mathfrak{p}^{n_{\mathfrak{p}}}$ un S–módulus. Por definición de conductor local $\mathfrak{f}_{\mathfrak{p}}(L/K)|\mathfrak{p}^{n_{\mathfrak{p}}} \iff G^{n_{\mathfrak{p}}}(L/K) = 1 \iff U_{\mathfrak{p}}^{(n_{\mathfrak{p}})} \subseteq \mathrm{N}_{L_{\mathfrak{p}}/K_{\mathfrak{p}}} L_{\mathfrak{p}}^* \iff \lceil U_{\mathfrak{p}}^{(n_{\mathfrak{p}})} \rceil_{\mathfrak{p}} \subseteq (\mathrm{N}_{L/K} J_L)K^*$.

Además $\mathfrak{p} \in S$ implica que $\mathfrak{p}$ se descompone totalmente o, equivalentemente, $\lceil K_{\mathfrak{p}}^* \rceil_{\mathfrak{p}} \subseteq (\mathrm{N}_{L/K} J_L)K^*$. Puesto que $(\mathrm{N}_{L/K} J_L)K^*$ es un subgrupo abierto de índice finito en J_K y por lo tanto cerrado, y puesto que $J_{K,S}^{\mathfrak{m}}$ es topológicamente generado por sus subgrupos $\{\lceil K_{\mathfrak{p}}^* \rceil_{\mathfrak{p}} \mid \mathfrak{p} \in S\}$ y $\{\lceil U_{\mathfrak{p}}^{(n_{\mathfrak{p}})} \rceil_{\mathfrak{p}} \mid \mathfrak{p} \notin S\}$, se sigue que $\mathfrak{f}(L/K)|\mathfrak{m} \iff J_{K,S}^{\mathfrak{m}} \subseteq (\mathrm{N}_{L/K} J_L)K^* \iff C_{K,S}^{\mathfrak{m}} \subseteq \mathrm{N}_{L/K} C_L \iff L \subseteq K_S^{\mathfrak{m}}$. □

Teorema 7.2.16. *Sean S un conjunto finito no vacío de lugares de K y $\mathfrak{m}$ un S–módulus. Entonces $K_S^{\mathfrak{m}}$ es la máxima extensión abeliana L/K tal que todos los primos de S son totalmente descompuestos y $\mathfrak{f}(L/K)|\mathfrak{m}$.*

Además, si $d = \mathrm{gr}\, S := \mathrm{mcd}\{\mathrm{gr}\,\mathfrak{p} \mid \mathfrak{p} \in S\}$, $\mathbb{F}_{q^d}$ es el campo de constantes de $K_S^{\mathfrak{m}}$.

Demostración. Sea L/K una extensión abeliana. Si todos los primo de S se descomponen en L/K y $\mathfrak{f}(L/K)|\mathfrak{m}$, entonces, como consecuencia del Teorema 7.2.15, $L \subseteq K_S^{\mathfrak{m}}$.

Recíprocamente, si $L \subseteq K_S^{\mathfrak{m}}$, entonces $\mathfrak{f}(L/K)|\mathfrak{m}$ y por definición de $J_{K,S}^{\mathfrak{m}}$, todos los primos de S se descomponen totalmente en $K_S^{\mathfrak{m}}$. Ahora, si $\mathfrak{p} \in S$ se descompone la extensión de constantes de grado r, entonces $r \mid \operatorname{gr}\mathfrak{p}$. Por lo tanto todos los primos de S se descomponen totalmente en $K\mathbb{F}_{q^r} \iff r|\operatorname{mcd}\{\operatorname{gr}\mathfrak{p} \mid \mathfrak{p} \in S\}$. Se sigue que $\mathbb{F}_{q^d}$ es el campo de constantes de $K_S^{\mathfrak{m}}$. □

Corolario 7.2.17. *(Ver* [136, Teorema 14..3.1]*). Sea K un campo global de funciones con campo de constantes $\mathbb{F}_q$ y sea $S \subseteq \mathbb{P}_K$ no vacío. Sea $d = \operatorname{gr} S = \operatorname{mcd}\{\operatorname{gr}\mathfrak{p} \mid \mathfrak{p} \in S\}$. Entonces el campo de constantes del campo de clase de Hilbert K_S^1 es $\mathbb{F}_{q^d}$.*

En particular, si $K = \mathbb{F}_q(T)$, entonces $K_S^1 = \mathbb{F}_{q^d}(T) = K\mathbb{F}_{q^d}$.

Demostración. La última parte se sigue de que $I_{\mathbb{F}_q(T),0} = \{1\}$, lo cual implica que $\mathbb{F}_q(T)^{\mathrm{nr}} = \mathbb{F}_q(T)\mathbb{F}_q^{\mathrm{ab}}$ y puesto que $\mathbb{F}_q(T)_S^1/\mathbb{F}_q(T)$ es no ramificado, se sigue que $\mathbb{F}_q(T)_S^1 \subseteq \mathbb{F}_q(T)\mathbb{F}_q^{\mathrm{ab}}$, es decir $\mathbb{F}_q(T)_S^1/\mathbb{F}_q(T)$ es una extensión de constantes. □

Observación 7.2.18. El campo K_S^1 es lo que comúnmente se llama el *campo de clase de Hilbert* con respecto a S.

7.2.2. Análogos al campo de clase de Hilbert para campos de funciones

Como hemos mencionado anteriormente, si K^{nr} es la máxima extensión abeliana no ramificada de K, se tiene que $K\mathbb{F}_q^{\mathrm{ab}} \subseteq K^{\mathrm{nr}}$. Sea $\mathcal{T} = \operatorname{Gal}(K^{\mathrm{ab}}/K^{\mathrm{nr}})$, $K^{\mathrm{nr}} = (K^{\mathrm{ab}})^{\mathcal{T}} \supseteq (K^{\mathrm{ab}})^{\mathcal{H}_0} = K\mathbb{F}_q^{\mathrm{ab}}$, es decir, $\mathcal{H}_0 \supseteq \mathcal{T}$, donde $\mathcal{H}_0 = \operatorname{Gal}(K^{\mathrm{ab}}/K\mathbb{F}_q^{\mathrm{ab}})$. Se tienen los diagramas conmutativos (ver Teorema 6.8.29):

$$\begin{array}{ccccccccc}
1 & \longrightarrow & C_{K,0} & \hookrightarrow & C_K & \xrightarrow{\operatorname{gr}} & \mathbb{Z} & \longrightarrow & 0 \\
 & & \cong\downarrow\rho_K & & \downarrow\rho_K & & \downarrow\rho_{\mathbb{F}_q} & & \\
1 & \longrightarrow & \operatorname{Gal}(K^{\mathrm{ab}}/K\mathbb{F}_q^{\mathrm{ab}}) & \longrightarrow & \operatorname{Gal}(K^{\mathrm{ab}}/K) & \xrightarrow[\text{rest}]{} & \operatorname{Gal}(K\mathbb{F}_q^{\mathrm{ab}}/K) & \longrightarrow & 1 \\
 & & \wr\downarrow & & \wr\downarrow & & \wr\downarrow & & \\
 & & \mathcal{H}_0 & & \mathcal{G}=G_K^{\mathrm{ab}} & & \operatorname{Gal}(\mathbb{F}_q^{\mathrm{ab}}/\mathbb{F}_q) & &
\end{array}$$

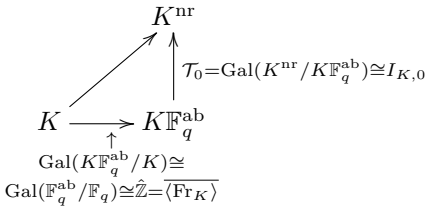
$$\begin{array}{ccccccccc}
1 & \longrightarrow & I_{K,0} & \hookrightarrow & I_K & \xrightarrow{\operatorname{gr}} & \mathbb{Z} & \longrightarrow & 0 \\
 & & \cong\downarrow & & \downarrow\mu & & \downarrow\rho_{\mathbb{F}_q} & & \\
1 & \longrightarrow & \operatorname{Gal}(K^{\mathrm{nr}}/K\mathbb{F}_q^{\mathrm{ab}}) & \hookrightarrow & \operatorname{Gal}(K^{\mathrm{nr}}/K) & \xrightarrow[\text{rest}]{} & \operatorname{Gal}(K\mathbb{F}_q^{\mathrm{ab}}/K) & \longrightarrow & 1 \\
 & & & & \wr\downarrow & & \wr\downarrow & & \\
 & & & & \mathcal{G}/\mathcal{T} & & \operatorname{Gal}(\mathbb{F}_q^{\mathrm{ab}}/\mathbb{F}_q) & &
\end{array}$$

pues $\frac{C_{K,0}}{K^*U_K/K^*} \cong I_{K,0} \cong \frac{\mathrm{Gal}(K^{\mathrm{ab}}/K\mathbb{F}_q^{\mathrm{ab}})}{\mathrm{Gal}(K^{\mathrm{ab}}/K^{\mathrm{nr}})}$ y $\frac{C_K}{U_K K^*/K^*} \cong I_K \cong \frac{\mathrm{Gal}(K^{\mathrm{ab}}/K)}{\mathrm{Gal}(K^{\mathrm{ab}}/K^{\mathrm{nr}})} \cong \mathrm{Gal}(K^{\mathrm{nr}}/K)$.

Ahora, si $\mu(\alpha) = 1$, $(\mathrm{rest}\,\mu)(\alpha) = \rho_{\mathbb{F}_q^{\mathrm{ab}}}(\mathrm{gr}\,\alpha) = 1$ por lo que $\mathrm{gr}\,\alpha = 0$ y por tanto $\alpha \in I_{K,0}$. Se sigue que μ es inyectiva.

En particular $K^{\mathrm{nr}}/K\mathbb{F}_q^{\mathrm{ab}}$ es una extensión finita y $\mathrm{Gal}(K^{\mathrm{nr}}/K\mathbb{F}_q^{\mathrm{ab}}) \cong I_{K,0}$.

Se tiene



Se sigue que la sucesión

$$1 \longrightarrow \mathcal{T}_0 \xrightarrow{\mu} \mathcal{R} = \mathrm{Gal}(K^{\mathrm{nr}}/K) \xrightarrow[\mathrm{rest}]{\varphi} \hat{\mathbb{Z}} \longrightarrow 0$$

es exacta.

7.2.3. Primer análogo al campo de clase de Hilbert

Se tiene que

$$1 \longrightarrow \mathrm{Gal}(K^{\mathrm{nr}}/K\mathbb{F}_q^{\mathrm{ab}}) \longrightarrow \mathrm{Gal}(K^{\mathrm{nr}}/K) \longrightarrow \mathrm{Gal}(K\mathbb{F}_q^{\mathrm{ab}}/K) \longrightarrow 1$$

es exacta, que $\mathrm{Gal}(K^{\mathrm{nr}}/K\mathbb{F}_q^{\mathrm{ab}}) \cong I_{K,0}$ es un grupo finito y además $I_K \xrightarrow{\mu} \mathrm{Gal}(K^{\mathrm{nr}}/K)$ es un inyección. Ahora bien, μ no es un isomorfismo pues I_K es discreto y no finito y $\mathrm{Gal}(K^{\mathrm{nr}}/K)$ es profinito, compacto. De hecho $I_K \cong I_{K,0} \times \mathbb{Z}$. Se tiene $\hat{I}_K \cong I_{K,0} \times \hat{\mathbb{Z}} \cong \mathrm{Gal}(K^{\mathrm{nr}}/K)$.

Podemos considerar a K^{nr} como el primer análogo al campo de clase de Hilbert.

7.2.4. Segundo análogo al campo de clase de Hilbert

Consideremos extensiones abelianas no ramificadas de K que tienen como campo de constantes al mismo campo $\mathbb{F}_q$.

Sean $U_K = \prod_{\mathfrak{p} \in \mathbb{P}_K} U_{\mathfrak{p}}$ y $J^1_{K,\emptyset}$ ($\mathfrak{m} = 1$, $S = \emptyset$), el grupo de rayos módulus 1 con respecto $S = \emptyset$ y sea

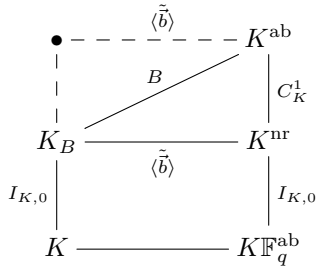
$$C^1_{K,\emptyset} = C^1_K = U_K K^*/K^* \subseteq C_{K,0}.$$

Se tiene que K^{nr} corresponde a U_K o a $U_K K^*/K^*$ (ver después del Teorema 6.8.29), esto es $C^1_K \cong \mathrm{Gal}(K^{\mathrm{ab}}/K^{\mathrm{nr}})$. Además $\hat{C}_K = G_K^{\mathrm{ab}} = \mathrm{Gal}(K^{\mathrm{ab}}/K)$.

Sea $\tilde{\vec{b}} \in C_K$ tal que $\mathrm{gr}(\tilde{\vec{b}}) = 1$. Entonces el subgrupo $B := C^1_K \times \langle \tilde{\vec{b}} \rangle$ es abierto en C_K y puesto que $C_K \cong C_{K,0} \times \langle \tilde{\vec{b}} \rangle$, entonces

$$\frac{C_K}{B} \cong \frac{C_{K,0} \times \langle \tilde{\vec{b}} \rangle}{C_K^1 \times \langle \tilde{\vec{b}} \rangle} \cong \frac{C_{K,0}}{C_K^1} = \frac{C_{K,0}}{C_K^1} \cong I_{K,0}$$

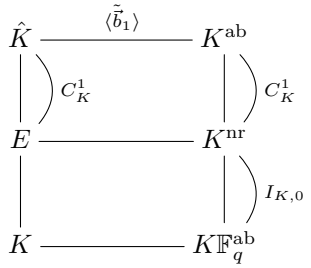
y se sigue que $[C_K : B] = [C_{K,0} : C_K^1] = h_K = |I_{K,0}|$ es el número de clase de K.



El campo de clase K_B de B es el segundo análogo al campo de clase de Hilbert. Puesto que B contiene una copia de $\mathbb{Z}$ ($\longleftrightarrow \langle \mathrm{Fr}_K \rangle = \langle \tilde{\vec{b}} \rangle$) y tales copias de $\mathbb{Z}$ están indexadas por $C_{K,0}$ puesto que $C_K \cong C_{K,0} \times \mathbb{Z}$ y $C_K^1 \longleftrightarrow \prod_{\mathfrak{p} \in \mathbb{P}_K} U_{\mathfrak{p}}$ es la extensión no ramificada K^{nr} de K, se sigue que este campo K_B, denotado por $K_H^{(1)}$, es una extensión abeliana finita no ramificada de K que tiene como campo de constantes a $\mathbb{F}_q$ (ver Teorema 6.8.37).

Veamos que $K_H^{(1)}$ es maximal en el sentido de ser no ramificada con campo de constantes $\mathbb{F}_q$. Sea $K_H^{(1)} \subseteq \hat{K}$ (algún $\hat{K} = \tilde{K}(\vec{\alpha})$, ver principio de esta subsección) y se tiene que $H = \mathrm{N}_{K_H^{(1)}/K} C_{K_H^{(1)}} \subseteq C_K$. Ahora bien, las extensiones no ramificadas deben satisfacer que sus grupos de normas están contenidas en U para que su conductor local sea 1 para todo lugar $\mathfrak{p} \in \mathbb{P}_K$ y entonces su conductor global sea 1.

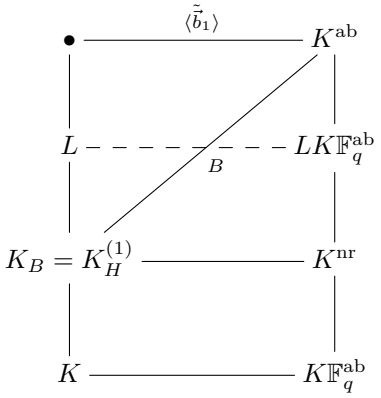
Por otro lado se tiene el diagrama



Por la correspondencia de Galois, K^{nr} corresponde a $E \subseteq \hat{K}$ con $E = \hat{K} \cap K^{\mathrm{nr}}$ y $[E : K] = [K^{\mathrm{nr}} : K\mathbb{F}_q^{\mathrm{ab}}] = h = |I_{K,0}|$.

Ahora bien, E tiene como campo de constantes $\mathbb{F}_q$ lo mismo que $K_H^{(1)}$ pues $K_H^{(1)}$ corresponde a B, esto es, $K_H^{(1)} \longleftrightarrow B = C_K^1 \times \langle \tilde{\vec{b}} \rangle$ con $C_K^1 \cong \mathrm{Gal}(K^{\mathrm{ab}}/K^{\mathrm{nr}})$ y como $\hat{K}$ es fijado por $\tilde{\vec{b}}_1$ y por tanto por $\langle \tilde{\vec{b}}_1 \rangle^{\hat{\mathbb{Z}}}$, se tiene que

$\hat{K} = \left(K^{\mathrm{ab}}\right)^{\langle \tilde{\vec{b}}_1 \rangle^{\hat{\mathbb{Z}}}}$, de donde, $K_H^{(1)} = E$ y por lo tanto $K_H^{(1)}$ es maximal con respecto a ser no ramificada sobre K y tener a $\mathbb{F}_q$ como campo de constantes. De hecho deberíamos haber escrito $K_H^{(\tilde{\vec{b}}_1)} \longleftrightarrow \hat{K}_{\tilde{\vec{b}}_1}$ pues tanto $K_H^{(1)}$ como $\hat{K}$ están determinados por $\tilde{\vec{b}}_1$.



Más precisamente, se tiene $K_H^{(1)} \cap K\mathbb{F}_q^{\mathrm{ab}} = K$ y $K_H^{(1)} K\mathbb{F}_q^{\mathrm{ab}} = K_H^{(1)}\mathbb{F}_q^{\mathrm{ab}} = K^{\mathrm{nr}}$.
Veamos que $K_H^{(1)}$ es maximal con respecto a estas propiedades.

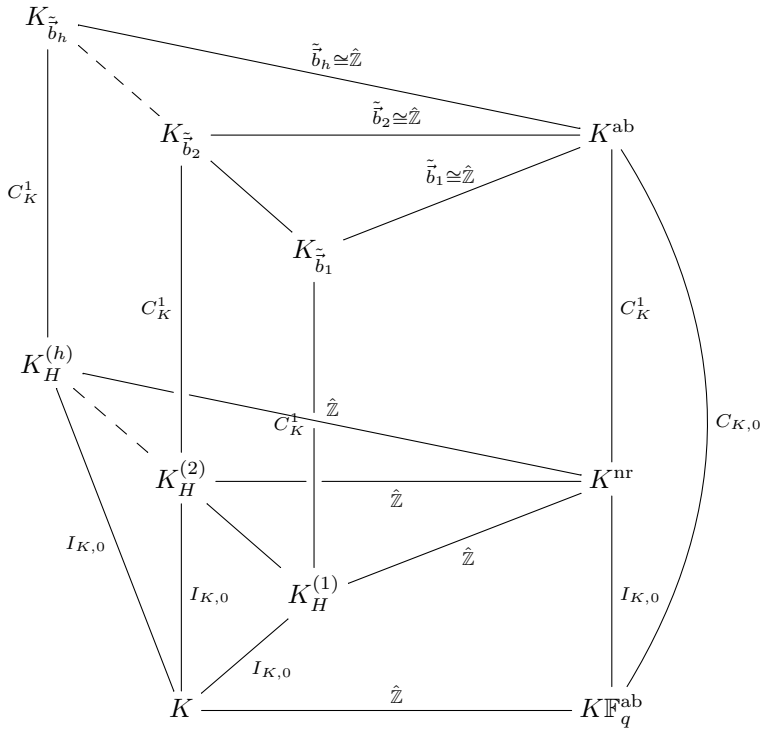
Sea L/K una extensión abeliana, donde el campo de constantes de L es $\mathbb{F}_q$ y tal que $K_H^{(1)} \subseteq L$. Entonces $L \cap K\mathbb{F}_q^{\mathrm{ab}} = K$ y $LK\mathbb{F}_q^{\mathrm{ab}} \supseteq K_H^{(1)} K\mathbb{F}_q^{\mathrm{ab}} = K^{\mathrm{nr}}$. Como L/K es no ramificada, $LK\mathbb{F}_q^{\mathrm{ab}} = K^{\mathrm{nr}}$ y por tanto $LK\mathbb{F}_q^{\mathrm{ab}} = K_H^{(1)} K\mathbb{F}_q^{\mathrm{ab}}$ y de la teoría de Galois se sigue que $L = K_H^{(1)}$.

Pongamos $K_H^{(1)} = K_H^{(\tilde{\vec{b}}_1)}$. Veamos que hay <u>exactamente</u> $h = h_K = |I_{K,0}|$ de estos campos: extensiones abelianas no ramificados de K con campo de constantes $\mathbb{F}_q$ maximales, y todos ellos tienen a su grupo de Galois isomorfo a

$$C_K/B \cong C_{K,0}/C_K^1 \cong I_{K,0}.$$

Por el Observación 2.3.3, tenemos que si L/K es una extensión de Galois, finita o infinita, con grupo de Galois G, se tiene que si $H < G$ y si $\bar{H}$ es la cerradura de H, se tiene $L^H = L^{\bar{H}}$.

Sean $\tilde{\vec{u}}_1, \ldots, \tilde{\vec{u}}_h$, h representantes de $C_{K,0}/C_K^1 \cong I_{K,0}$ y sean $\tilde{\vec{b}}_i := \tilde{\vec{b}}\tilde{\vec{u}}_i$, $1 \leq i \leq h$. Los grupos $B_i := C_K^1 \times \langle \tilde{\vec{b}}_i \rangle$ son todos distintos y $[C_K : B_i] = h$. Los grupos B_i dan lugar a h campos que son maximales en el sentido de ser extensiones abelianas no ramificadas de K y tener como campo de constantes $\mathbb{F}_q$ (son maximales puesto que si $K_H^{(i)}$ es el campo asociado a B_i, entonces $K_H^{(i)}\mathbb{F}_q^{\mathrm{ab}} = K^{\mathrm{nr}}$).

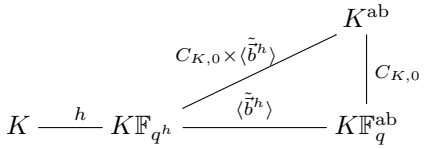


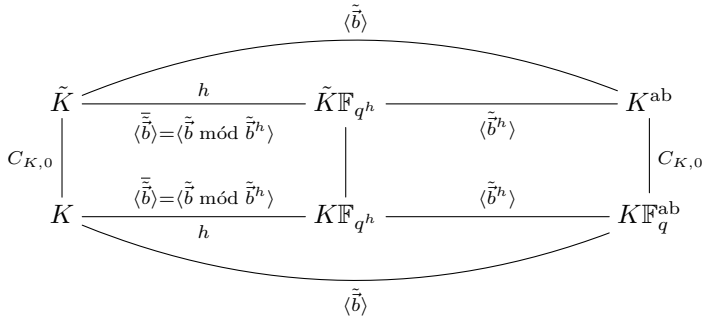
Sea $\tilde{\vec{a}} \in C_K$ con $\operatorname{gr} \tilde{\vec{a}} = 1$. Por tanto $\operatorname{gr}(\tilde{\vec{a}}\tilde{\vec{b}}^{-1}) = 0$ por lo que $\tilde{\vec{a}}$ pertenece a alguna clase $\tilde{\vec{b}}\tilde{\vec{u}}_i$ mód C_K^1. Así, el grupo $A = C_K^1 \times \langle \tilde{\vec{a}} \rangle$ da lugar a un campo de clase de Hilbert como los anteriores y se tiene

$$\frac{C_K}{A} = \frac{C_{K,0} \times \langle \tilde{\vec{b}} \rangle}{C_K^1 \times \langle \tilde{\vec{a}} \rangle} = \frac{C_{K,0} \times \langle \tilde{\vec{b}} \rangle}{C_K^1 \times \langle \tilde{\vec{b}}\tilde{\vec{u}}_i \rangle} = \frac{C_K}{B_i}.$$

Por tanto $A = B_i$.

Los h campos asociados a $B_1, \ldots, B_h$ son todos los campos con campo de constantes $\mathbb{F}_q$, que son extensiones abelianas no ramificadas maximales de K. Sean $K_H^{(1)}, \ldots, K_H^{(h)}$ estos h campos. El campo de clase correspondiente a $C_{K,0} \times \langle \tilde{\vec{b}}^h \rangle$ es la extensión de constantes de grado h de K (ver el principio de esta subsección). Esto es, $L := K\mathbb{F}_{q^h}$ es el campo correspondiente a $C_{K,0} \times \langle \tilde{\vec{b}}^h \rangle$.





Afirmamos que

$$LK_H^{(i)} = LK_H^{(j)} = LK_H^{(1)} \cdots K_H^{(h)} \quad \text{para todos} \quad 1 \le i, j \le h.$$

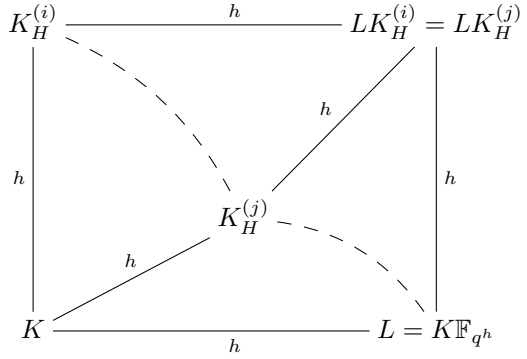
En efecto, puesto que $\tilde{\vec{b}}^h = (\tilde{\vec{b}}_i \tilde{\vec{u}}_i^{-1})^h = \tilde{\vec{b}}_i^h \tilde{\vec{u}}_i^{-h} \equiv \tilde{\vec{b}}_i^h$ mód C_K^1, entonces $\big(C_{K,0} \times \langle\tilde{\vec{b}}^h\rangle\big) \cap \big(C_K^1 \times \langle\tilde{\vec{b}}_i\rangle\big) = C_K^1 \times \langle\tilde{\vec{b}}_i^h\rangle$ y $\tilde{\vec{b}}_i^h, \tilde{\vec{b}}_j^h$ están en la misma clase mód C_K^1.

Se sigue que $\big(C_{K,0} \times \langle\tilde{\vec{b}}^h\rangle\big) \cap \big(C_K^1 \times \langle\tilde{\vec{b}}_i\rangle\big) = \big(C_{K,0} \times \langle\tilde{\vec{b}}^h\rangle\big) \cap \big(C_K^1 \times \langle\tilde{\vec{b}}_j\rangle\big)$ para todo $1 \le i, j \le h$.

Se tiene que $LK_H^{(i)} = LK_H^{(j)}$ y por tanto

$$\underline{LK_H^{(1)}}\, K_H^{(2)} \cdots K_H^{(h)} = \underline{LK_H^{(2)}}\, K_H^{(2)} K_H^{(3)} \cdots K_H^{(h)} = \underline{LK_H^{(2)}}\, K_H^{(3)} \cdots K_H^{(h)}$$
$$= \underline{LK_H^{(3)}}\, K_H^{(3)} \cdots K_H^{(h)} = LK_H^{(3)} \cdots K_H^{(h)} = \cdots = LK_H^{(h)}.$$

Ahora bien, puesto que $L \cap K_H^{(i)} = K$ para toda i por ser L/K extensión de constantes y $K_H^{(i)}/K$ geométrica, se tiene



$[LK_H^{(1)} \cdots K_H^{(h)} : K] = h^2$. Se tiene

$$\mathrm{Gal}(LK_H^{(1)} \cdots K_H^{(h)}/K) \cong \mathrm{Gal}(L/K) \times \mathrm{Gal}(K_H^{(1)}/K) \cong C_h \times I_{K,0}.$$

Este es el segundo análogo al campo de clase de Hilbert.

Teorema 7.2.19. *Sea $h = h_K = |I_{K,0}|$ el número de clase de K. Entonces hay exactamente h campos $K_H^{(i)}$, $1 \leq i \leq h$ con campo de constantes $\mathbb{F}_q$ y tales que $K_H^{(i)}/K$ son extensiones abelianas no ramificadas de K maximales con respecto a estas propiedades. Se tiene que*

$$\mathrm{Gal}(K_H^{(i)}/K) \cong I_{K,0}, \quad 1 \leq i \leq h.$$

Finalmente, si L es la extensión de constantes de K de grado h, se tiene

$$\begin{aligned}\mathrm{Gal}(LK_H^{(i)}/K) = \mathrm{Gal}(LK_H^{(j)}/K) &= \mathrm{Gal}(LK_H^{(1)} \cdots K_H^{(h)}/K) \\ &\cong \mathrm{Gal}(L/K) \times \mathrm{Gal}(K_H^{(i)}/K) \cong C_h \oplus I_{K,0},\end{aligned}$$

para todas $1 \leq i, j \leq h$. □

Ejemplo 7.2.20. La única extensión abeliana geométrica no ramificada de $\mathbb{F}_q(T)$ es $\mathbb{F}_q(T)$ misma.

7.2.5. Tercer análogo al campo de clase de Hilbert

Para un análisis previo a lo que discutimos aquí, ver [136, Capítulo 14], en donde se estudian los campos de géneros de campos de funciones. Ahí se estudia el caso particular de que el conjunto de primos eran los primos sobre el divisor de polos de T. En la siguiente subsección, discutiremos con más detalle este tercer análogo al campo de clase de Hilbert.

En el caso de un campo numérico K, K_H es la máxima extensión abeliana de K no ramificada y K_H es el campo de clase del grupo $J_{K,S}K^*/K^*$, donde S es el conjunto de primos infinitos. En general se define

$$J_{K,S} := \prod_{\mathfrak{p} \notin S} U_{\mathfrak{p}} \times \prod_{\mathfrak{p} \in S} K_{\mathfrak{p}}^*.$$

Es decir, al ser K_H/K no ramificada en S, los primos infinitos se descomponen totalmente en K_H/K. Esto se puede copiar en el caso de campos de funciones tomando como S cualquier conjunto no vacío finito de lugares de K y definiendo como K_H a la máxima extensión abeliana no ramificada de K, tal que todos los lugares de S se descomponen totalmente en K_H/K. Resulta ser que $K_H = K_S^1$ el campo de clases de rayos del módulus 1 con respecto a S. Esto es, K_H corresponde a $J_{K,S}^1 K^*/K^* = C_{K,S}^1$.

Veremos que K_H/K es una extensión finita y que $\mathrm{Gal}(K_H/K) \cong Cl(\mathcal{O}_S)$, el grupo de clases del anillo Dedekind

$$\mathcal{O}_S = \{x \in K \mid v_{\mathfrak{p}}(x) \geq 0 \text{ para toda } \mathfrak{p} \notin S\} = \bigcap_{\mathfrak{p} \notin S} \mathcal{O}_{\mathfrak{p}},$$

donde para todo $S \neq \emptyset$, $Cl(\mathcal{O}_S) = \frac{D_{K,S}}{P_{K,S}} = \frac{\text{divisores primos relativos a } S}{\{(\alpha)_S | \alpha \in K^*\}}$ y donde para $\alpha \in K^*$, se define $(\alpha)_S = \prod_{\mathfrak{p} \notin S} \mathfrak{p}^{v_{\mathfrak{p}}(\alpha)}$ (Teorema 7.2.8).

Más precisamente, el grupo de ideales fraccionarios de $\mathcal{O}_S$ es $D_{K,S} = \frac{D_K}{D_S} = \frac{D_K}{\langle \mathfrak{p} | \mathfrak{p} \in S \rangle} = \langle \mathfrak{p} \in \mathbb{P}_K \mid \mathfrak{p} \notin S \rangle$ y se tiene el epimorfismo

$$\Lambda : J_K \longrightarrow D_K/D_S = \langle \mathfrak{p} \in \mathbb{P}_K \mid \mathfrak{p} \notin S \rangle, \qquad \Lambda(\vec{\alpha}) = \prod_{\mathfrak{p} \notin S} \mathfrak{p}^{v_{\mathfrak{p}}(\alpha_{\mathfrak{p}})}$$

con núcleo $J_{K,S}$, $Cl(\mathcal{O}_S) = \frac{D_K/D_S}{P_S}$ y el epimorfismo inducido

$$\tilde{\Lambda} : J_K \longrightarrow Cl(\mathcal{O}_S)$$

satisface que núc $\tilde{\Lambda} = J_{K,S}K^*$. Por tanto

$$\frac{J_K}{J_{K,S}K^*} \cong \frac{J_K/K^*}{J_{K,S}/K^*} \cong \frac{C_K}{C_{K,S}} = \frac{C_K}{C^1_{K,S}} \cong \mathrm{Gal}(K^1_S/K) \cong Cl(\mathcal{O}_S).$$

En resumen, si S es un conjunto finito no vacío de lugares y sea

$$J_{K,S} := \prod_{\mathfrak{p} \notin S} U_{\mathfrak{p}} \times \prod_{\mathfrak{p} \in S} K^*_{\mathfrak{p}},$$

entonces la máxima extensión abeliana de K no ramificada tal que los primos de S se descomponen totalmente corresponde a $J_{K,S}$ o, equivalentemente, a $J_{K,S}K^*/K^* := C_{K,S}$.

Este será el tercer análogo al campo de clase de Hilbert K_H de K, el cual es igual a K^1_S y es la máxima extensión abeliana no ramificada de K tal que todos los primos de S se descomponen totalmente en K^1_S/K y se tiene

$$\mathrm{Gal}(K^1_S/K) \cong C_K/C^1_{K,S} \cong Cl(\mathcal{O}_S).$$

En la siguiente subsección retomamos este análogo y es el que consideraremos como el campo de clase de Hilbert para campos de funciones.

7.3. Campo de clase de Hilbert en campos de funciones globales

Como mencionamos antes, el estudio de esta subsección puede ser consultado en [131] y en [4].

Sea K un campo global de funciones con campo de constantes $\mathbb{F}_q$. Sea S un conjunto finito no vacío de lugares de K.

Definición 7.3.1. El *campo de clase de Hilbert relativo a* S, $K_{H,S}$, se define como la máxima extensión abeliana de K no ramificada y tal que los primos en S se descomponen totalmente en $K_{H,S}$.

De [136, Teorema 14.3.1] tenemos que el campo de constantes de $K_{H,S}$ es $\mathbb{F}_{q^d}$ donde $d = \mathrm{mcd}(\mathrm{gr}\,\mathfrak{p} \mid \mathfrak{p} \in S)$, que $K_{H,S}/K$ es una extensión abeliana finita y que

$$\mathrm{Gal}(K_{H,S}/K) \cong Cl_S$$

con $Cl_S = Cl(\mathcal{O}_S)$ donde $\mathcal{O}_S = \{x \in K \mid v_{\mathfrak{q}}(x) \geq 0 \text{ para todo } \mathfrak{q} \notin S\}$.

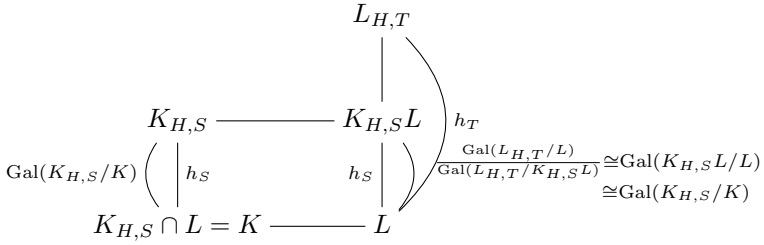
El isomorfismo $\mathrm{Gal}(K_{H,S}/K) \cong Cl_S$ está dado por el mapeo de reciprocidad de Artin: $(\_\_, K_{H,S}/K) = \left(\frac{K_{H,S}/K}{}\right) : Cl_S \longrightarrow \mathrm{Gal}(K_{H,S}/K)$.

Para cualquier campo K y cualquier conjunto S finito no vacío de lugares de K, denotemos por h_S al número de clases de ideales $|Cl_S|$. Sea L/K una extensión finita y separable. Sea $T := \{\mathfrak{P} \in \mathbb{P}_L \mid \mathfrak{P}|_K \in S\}$ y sea $\mathcal{O}_T$ la cerradura entera de $\mathcal{O}_S$ en L.

Proposición 7.3.2. *Se tiene $K_{H,S}L \subseteq L_{H,T}$.*

Demostración. Se sigue del hecho de que $L = KL \subseteq K_{H,S}L$ y de que $K_{H,S}/K$ es abeliana, no ramificada y los primos de S se descomponen totalmente. □

Observación 7.3.3. Si $K_{H,S} \cap L = K$, entonces $h_S | h_T$. En efecto, se tiene $\mathrm{Gal}(K_{H,S}L/L) \cong \mathrm{Gal}(K_{H,S}/K)$ por lo que $h_S = |\mathrm{Gal}(K_{H,S}/K)| = |\mathrm{Gal}(K_{H,S}L/L)||h_T$.



Proposición 7.3.4. *Si algún primo $\mathfrak{p} \in \mathbb{P}_K$ es totalmente ramificado en $\mathcal{O}_T$ o si algún primo $\mathfrak{p} \in S$ es totalmente inerte en L, entonces la norma $\mathrm{N} := \mathrm{N}_{L_{H,T}/K_{H,S}} : Cl_T \longrightarrow Cl_S$ es suprayectiva. En particular se tiene que $h_S | h_T$.*

Demostración. Se tiene que, en cualquiera de los dos casos mencionados, $K_{H,S} \cap L = K$, por lo que el mapeo de restricción $\mathrm{rest} : \mathrm{Gal}(L_{H,T}/L) \longrightarrow \mathrm{Gal}(K_{H,S}/K)$ es suprayectivo y $h_S | h_T$.

De [136, Teorema 16.7.4], se tiene el siguiente diagrama conmutativo

$$\begin{array}{ccc} Cl_T & \xrightarrow[\cong]{(\ ,L_{H,T}/L)} & \mathrm{Gal}(L_{H,T}/L) \\ \Big\downarrow{\scriptstyle \mathrm{N}} & & \Big\downarrow{\scriptstyle \mathrm{rest}\,|_{K_{H,S}}} \\ Cl_S & \xrightarrow[\cong]{(\ ,K_{H,S}/K)} & \mathrm{Gal}(K_{H,S}/K) \end{array}$$

Puesto que $\mathrm{rest}\,|_{K_{H,S}}$, $(\ , L_{H,T}/L)$ y $(\ , K_{H,S}/K)$ son suprayectivas, se sigue que $\mathrm{N} : Cl_T \longrightarrow Cl_S$ es suprayectiva. □

Aquí recordamos la relación que existe entre el número de clases de divisores h_K de un campo de funciones global K y el número de clases de ideales, dada por la fórmual de Schmidt ([136, Corolario 10.2.15]):

$$h_K d = \gamma h_S,$$

donde $\gamma = \left|\frac{D_K(S)_0}{P_K(S)}\right|$ y $d = \operatorname{mcd}(\operatorname{gr}\mathfrak{p} \mid \mathfrak{p} \in S)$.

Observación 7.3.5. Si la extensión L/K es una extensión finita de Galois, entonces $L_{H,T}/K$ también es Galois. La demostración es la misma que la de en la Observación 7.5.4.

A continuación definimos el *campo de clase de Hilbert extendido* de un campo de funciones global.

En el caso de campos numéricos, el campo de clase de Hilbert extendido corresponde al grupo de idèles J_K^{1+}, esto es, a elementos totalmente positivos. Debemos desarrollar un concepto de "totalmente positivo" en un campo de funciones global. Este concepto que usamos aquí fue propuesto por Anglès y Jaulent en [4].

Sean $K = \mathbb{F}_q(T)$, $\mathfrak{p}_\infty$ el primo infinito, es decir, el polo de $(T)_K$, y $K_\infty \cong \mathbb{F}_q\big(\big(\frac{1}{T}\big)\big)$ la completación de K en $\mathfrak{p}_\infty$. Sea $x \in K_\infty^*$. Entonces x se escribe de manera única como

$$x = \Big(\frac{1}{T}\Big)^{n_x} \lambda_x \varepsilon_x, \quad n_x \in \mathbb{Z}, \quad \lambda_x \in \mathbb{F}_q^* \quad \text{y} \quad \varepsilon_x \in U_{K_\infty}^{(1)}.$$

Ponemos $\pi_\infty = 1/T$.

Definición 7.3.6. Se define la *función signo de* K_∞^* como $\phi_\infty \colon K_\infty^* \longrightarrow \mathbb{F}_q^*$ la cual está dada por $\phi_\infty(x) = \lambda_x$ para $x \in K_\infty^*$. El valor $\phi_\infty(x)$ se llama el *signo de* x. También ponemos $\operatorname{sgn}(x) = \phi_\infty(x)$.

Se tiene que ϕ_∞ es un epimorfismo y $\operatorname{núc}\phi_\infty = \langle \pi_\infty \rangle \times U_{K_\infty^*}^{(1)}$.

Observación 7.3.7. Sea $M \in R_T = \mathbb{F}_q[T]$, $M \neq 0$, digamos que M es de grado d y está dado por $M(T) = a_d T^d + a_{d-1}T^{d-1} \cdots + a_1 T + a_0 = a_d T^d\big(1 + \frac{a_{d-1}}{a_d}\big(\frac{1}{T}\big) + \cdots + \frac{a_1}{a_d}\big(\frac{1}{T}\big)^{d-1} + \frac{a_0}{a_d}\big(\frac{1}{T}\big)^d\big) = a_d\big(\frac{1}{T}\big)^{-d}\mu$ con $\mu \in U_{K_\infty^*}^{(1)}$. Se sigue que el signo de M es el coeficiente líder de M: $\operatorname{sgn}(M) = a_d$.

Definición 7.3.8. Sea L una extensión finita y separable de K_∞. Se define el *signo de* L^* por el morfismo $\phi_L = \phi_\infty \circ \mathrm{N}_{L/K_\infty} \colon L^* \longrightarrow \mathbb{F}_q^*$.

Proposición 7.3.9. *Sea una torre de campos* $K_\infty \subseteq E \subseteq L$. *Entonces se tiene*

(1) $\phi_L = \phi_E \circ \mathrm{N}_{L/E}$,
(2) $\mathrm{N}_{L/E}(\operatorname{núc}\phi_L) \subseteq \operatorname{núc}\phi_E$.

Demostración. (1): Se tiene $\phi_L = \phi_\infty \circ \mathrm{N}_{L/K_\infty} = \phi_\infty \circ (\mathrm{N}_{E/K_\infty} \circ \mathrm{N}_{L/E}) = (\phi_E \circ \mathrm{N}_{L/E})$. Por tanto $\phi_L = \phi_E \circ \mathrm{N}_{L/E}$.

(2): Si $x \in \mathrm{núc}\,\phi_L$, entonces $1 = \phi_L(x) = \phi_E(\mathrm{N}_{L/E}(x))$. Por lo tanto $\mathrm{N}_{L/E}(x) \in \mathrm{núc}\,\phi_E$. □

Observación 7.3.10. La completación de $\mathbb{Q}$ en ∞, el lugar arquimediano de $\mathbb{Q}$, es $\mathbb{Q}_\infty = \mathbb{R}$ y la función signo $\phi_\infty \colon \mathbb{R}^* = \mathbb{Q}_\infty^* \longrightarrow \{\pm 1\}$ es $\phi_\infty(x) = 1$ si $x > 0$, $\phi_\infty(x) = -1$ si $x < 0$ y $\mathrm{núc}\,\phi_\infty = \mathbb{R}^+$.

Ahora si $L_v = \mathbb{C}$, entonces para toda $z \in L_v^*$, $\mathrm{N}_{L_v/\mathbb{Q}_\infty} z = \mathrm{N}_{\mathbb{C}/\mathbb{R}}\, z = z\overline{z} = |z|^2 > 0$ y por tanto $\phi_{L_v}(z) = 1$ para toda $z \in L_v$.

También notemos que la definición de signo concuerda con la Definición 7.0.5.

Teorema 7.3.11. *Sean E/K_∞ una extensión finita y separable y $E^{\mathrm{mod}}/K_\infty$ la máxima subextensión abeliana moderadamente ramificada máxima tal que $K_\infty \subseteq E^{\mathrm{mod}} \subseteq E$. Sean f el grado de inercia y e el índice de ramificación de $E^{\mathrm{mod}}/K_\infty$. Entonces $\mathbb{F}_E = \mathbb{F}_{q^f}$ es el campo residual de E^{mod} y*

(1) *existe $\xi \in \mathbb{F}_E^*$ tal que $E^{\mathrm{mod}} = \mathbb{F}_E\Big(\Big(\sqrt[e]{\frac{-\xi}{T}}\Big)\Big)$ y además*

$$\phi_E(E^*) = \langle (\mathbb{F}_q^*)^e, \mathrm{N}_{\mathbb{F}_E/\mathbb{F}_q}(\xi) \rangle,$$

(2) *si además tenemos que $\frac{1}{T} \in \mathrm{N}_{E^{\mathrm{mod}}/K_\infty}((E^{\mathrm{mod}})^*)$, entonces $E^{\mathrm{mod}} = \mathbb{F}_q\Big(\Big(\sqrt[e]{\frac{-1}{T}}\Big)\Big)$ y $\phi_E(E^*) = (\mathbb{F}_q^*)^e$.*

Demostración. Sea $K_\infty \subseteq E^{\mathrm{ab}} \subseteq E$ la máxima extensión abeliana de K_∞ contenida en E. Entonces por el Teorema 6.9.7 obtenemos que $\mathrm{N}_{E/K_\infty}(E^*) = \mathrm{N}_{E^{\mathrm{ab}}/K_\infty}((E^{\mathrm{ab}})^*)$. Puesto que $\phi_E = \phi_\infty \circ \mathrm{N}_{E/K_\infty}$ se sigue que $\phi_E(E^*) = \phi_{E^{\mathrm{ab}}}((E^{\mathrm{ab}})^*)$.

Sea $E^{\mathrm{nr}} = \mathbb{F}_E\Big(\Big(\frac{1}{T}\Big)\Big)$ la máxima extensión no ramificada de K_∞ contenida en E. Se tiene $v_{E^{\mathrm{nr}}}\big(\frac{1}{T}\big) = e(E^{\mathrm{nr}}|K_\infty) v_{K_\infty}\big(\frac{1}{T}\big) = 1 \cdot 1 = 1$, $[\mathbb{F}_E : \mathbb{F}_q] = f = [E^{\mathrm{nr}} : K_\infty]$ y $E^{\mathrm{mod}}/E^{\mathrm{nr}}$ es totalmente ramificada, digamos de grado e, con $\mathrm{mcd}(p, e) = 1$, esto es $p \nmid e$. Sea ρ un elemento uniformizador de E^{mod}. Entonces $v_{E^{\mathrm{mod}}}\big(\frac{1}{T}\big) = e(E^{\mathrm{mod}}|E^{\mathrm{nr}}) v_{E^{\mathrm{nr}}}\big(\frac{1}{T}\big) = e \cdot 1 = e$.

Se tiene $v_{E^{\mathrm{mod}}}\big(\rho^e \big(\frac{1}{T}\big)^{-1}\big) = 0$, esto es, $\rho^e \big(\frac{1}{T}\big)^{-1} \in U_{E^{\mathrm{mod}}} = \mathbb{F}_E^* U_{E^{\mathrm{mod}}}^{(1)}$. Podemos escribir $\rho^e \big(\frac{1}{T}\big)^{-1} = \xi u$ con $\xi \in \mathbb{F}_E^*$ y $u \in U_{E^{\mathrm{mod}}}^{(1)}$. Por tanto $\rho^e = \xi u\big(\frac{1}{T}\big)$. Puesto que $p \nmid e$ se tiene que $(U_{E^{\mathrm{mod}}}^{(1)})^e = U_{E^{\mathrm{mod}}}^{(1)}$ y por tanto existe $v \in U_{E^{\mathrm{mod}}}^{(1)}$ con $v^e = u$. De esta forma tenemos $\rho^e = \xi v^e \big(\frac{1}{T}\big)$ y $v_{E^{\mathrm{mod}}}(v) = 0$. Se sigue que $\big(\frac{\rho}{v}\big)^e = \xi\big(\frac{1}{T}\big)$ y $v_{E^{\mathrm{mod}}}\big(\frac{\rho}{v}\big) = 1$. De esta forma, podemos suponer, tomando $\frac{\rho}{v}$ en lugar de ρ, que $\rho^e = \xi\big(\frac{1}{T}\big)$.

Por lo tanto tenemos $\mathrm{N}_{E^{\mathrm{mod}}/K_\infty}(\rho) = \mathrm{N}_{E^{\mathrm{nr}}/K_\infty} \circ \mathrm{N}_{E^{\mathrm{mod}}/E^{\mathrm{nr}}}(\rho)$. Se tiene

$$\begin{aligned}\operatorname{Irr}(\rho, X, E^{\mathrm{nr}}) = X^e - \xi\Big(\frac{1}{T}\Big) &= \prod_{\sigma\in\operatorname{Gal}(E^{\mathrm{mod}}/E^{\mathrm{nr}})} (x-\sigma(\rho)) \\ &= X^e - \alpha_{e-1} + \cdots + (-1)^e \operatorname{N}_{E^{\mathrm{mod}}/E^{\mathrm{nr}}}(\rho).\end{aligned}$$

Se sigue que $-\xi\big(\frac{1}{T}\big) = (-1)^e \operatorname{N}_{E^{\mathrm{mod}}/E^{\mathrm{nr}}}(\rho)$ y por tanto $\operatorname{N}_{E^{\mathrm{mod}}/E^{\mathrm{nr}}}(\rho) = (-1)^{e-1}\xi\big(\frac{1}{T}\big)$ lo cual implica que

$$\begin{aligned}\operatorname{N}_{E^{\mathrm{mod}}/K_\infty}(\rho) &= \operatorname{N}_{E^{\mathrm{nr}}/K_\infty}\Big((-1)^{e-1}\xi\Big(\frac{1}{T}\Big)\Big) \\ &= (-1)^{(e-1)f}\big(\operatorname{N}_{E^{\mathrm{nr}}/K_\infty}(\xi)\big)\Big(\frac{1}{T}\Big)^f.\end{aligned}$$

Se sigue $\phi_{E^{\mathrm{mod}}}(\rho) = \phi_\infty \circ \operatorname{N}_{E^{\mathrm{mod}}/K_\infty}(\rho) = \phi_\infty\big((-1)^{(e-1)f}\big(\operatorname{N}_{\mathbb{F}_E/\mathbb{F}_q}(\xi)\big)\frac{1}{T^f}\big) = (-1)^{(e-1)f}\operatorname{N}_{\mathbb{F}_E/\mathbb{F}_q}(\xi)$.

Además, puesto que $E^{\mathrm{mod}}/E^{\mathrm{nr}}$ es totalmente ramificada de grado e y la norma en campos finitos es suprayectiva, se tiene

$$\begin{aligned}\phi_{E^{\mathrm{mod}}}(\mathbb{F}_E^*) &= \phi_{E^{\mathrm{nr}}}(\operatorname{N}_{E^{\mathrm{mod}}E^{\mathrm{nr}}}(\mathbb{F}_E^*)) = \phi_{E^{\mathrm{nr}}}((\mathbb{F}_E^*)^e) = \phi_\infty((\operatorname{N}_{E^{\mathrm{nr}}/K_\infty}(\mathbb{F}_E^*))^e) \\ &= \phi_\infty((\operatorname{N}_{E^{\mathrm{nr}}/K_\infty}(\mathbb{F}_{E^{\mathrm{nr}}}^*))^e) = \phi_\infty((\mathbb{F}_q^*)^e) = (\mathbb{F}_q^*)^e.\end{aligned}$$

Ahora bien $(E^{\mathrm{mod}})^* = \langle\rho\rangle \times \mathbb{F}_E^* \times U_{E^{\mathrm{mod}}}^{(1)}$ y

$$\phi_{E^{\mathrm{mod}}}(U_{E^{\mathrm{mod}}}^{(1)}) = \phi_\infty(\operatorname{N}_{E^{\mathrm{mod}}/K_\infty}(U_{E^{\mathrm{mod}}}^{(1)})) = \{1\}$$

pues $\operatorname{N}_{E^{\mathrm{mod}}/K_\infty}(U_{E^{\mathrm{mod}}}^{(1)}) \subseteq U_\infty^{(1)}$.

Se sigue que

$$\begin{aligned}\phi_\infty((E^{\mathrm{mod}})^*) &= \langle\phi_\infty(\rho), \phi_\infty(\mathbb{F}_E^*)\rangle = \langle(-1)^{(e-1)f}\operatorname{N}_{\mathbb{F}_E/\mathbb{F}_q}(\xi), (\mathbb{F}_q^*)^e\rangle \\ &= \langle(-1)^{ef}(-1)^f\operatorname{N}_{\mathbb{F}_E/\mathbb{F}_q}(\xi), (\mathbb{F}_q^*)^e\rangle \\ &= \langle(-1)^{ef}\operatorname{N}_{\mathbb{F}_E/\mathbb{F}_q}(-\xi), (\mathbb{F}_q^*)^e\rangle.\end{aligned}$$

Se tiene $(-1)^{ef} = \pm 1$. Si $(-1)^{ef} = -1$, entonces en caso de que $p = 2$, $-1 = 1$ y en caso de que $p > 2$, ef es impar por lo que tanto e como f son impares. Por tanto $(-1)^e = -1 \in (\mathbb{F}_q^*)^*$. En resumen, tenemos, en cualquier caso,

$$\phi_\infty((E^{\mathrm{mod}})^*) = \langle\operatorname{N}_{\mathbb{F}_E/\mathbb{F}_q}(-\xi), (\mathbb{F}_q^*)^e\rangle.$$

Ahora bien, puesto que $E^{\mathrm{ab}}/E^{\mathrm{mod}}$ es de grado una potencia de p y $\phi_\infty(E^*) \subseteq \mathbb{F}_q^*$ con $\operatorname{mcd}(p, q-1) = 1$, se sigue que

$$\phi_\infty(E^*) = \phi_\infty((E^{\mathrm{ab}})^*) = \phi_\infty((E^{\mathrm{mod}})^*) = \langle(\mathbb{F}_q^*)^e, \operatorname{N}_{\mathbb{F}_E/\mathbb{F}_q}(-\xi)\rangle.$$

Por otro lado $E^{\mathrm{mod}}/K_\infty$ es de grado ef y $E^{\mathrm{nr}} = \mathbb{F}_E\Big(\Big(\frac{1}{T}\Big)\Big) = \mathbb{F}_{q^f}\Big(\Big(\frac{1}{T}\Big)\Big)$ y $E^{\mathrm{mod}} = E^{\mathrm{nr}}(\rho)$ pues $e = \operatorname{gr}\operatorname{Irr}(\rho, X, E^{\mathrm{mod}})$ y $\rho^e = \xi\frac{1}{T}$ por lo que $\rho = \sqrt[e]{\xi\frac{1}{T}} = \sqrt[e]{\frac{\xi}{T}}$. Por tanto

$$E^{\mathrm{mod}} = E^{\mathrm{nr}}\Big(\sqrt[e]{\frac{\xi}{T}}\Big) = \mathbb{F}_E\Big(\Big(\frac{1}{T}\Big)\Big)\Big(\sqrt[e]{\frac{\xi}{T}}\Big) = \mathbb{F}_E\Big(\Big(\sqrt[e]{\frac{\xi}{T}}\Big)\Big).$$

Esto termina la demostración de (1).

Para (2), tenemos que si $\frac{1}{T} \in \mathrm{N}_{E^{\mathrm{mod}}/K_\infty}((E^{\mathrm{mod}})^*)$, entonces existe $\mu \in E^{\mathrm{mod}}$ con $\mathrm{N}_{E^{\mathrm{mod}}/K_\infty}(\mu) = \frac{1}{T}$ de donde $-\xi\Big(\frac{1}{T}\Big) = -\xi\,\mathrm{N}_{E^{\mathrm{mod}}/K_\infty}(\mu) = (-1)^e\,\mathrm{N}_{E^{\mathrm{mod}}/E^{\mathrm{nr}}}(\rho)$ y por tanto $-\xi(-1)^e \in \mathrm{N}_{E^{\mathrm{mod}}/K_\infty}((E^{\mathrm{mod}})^*)$.

Además, como $\frac{1}{T}$ es norma, se tiene que $f = 1$. De hecho se tiene que $\frac{1}{T}$ es uniformizador de E^{nr} y $1 = v_{K_\infty}\Big(\frac{1}{T}\Big) = v_{K_\infty}(\mathrm{N}_{E^{\mathrm{mod}}/K_\infty}(\mu)) = f = f(E^{\mathrm{mod}}|K_\infty)v_{E^{\mathrm{mod}}}(\mu) = 1$, esto es, $f = f(E^{\mathrm{mod}}|K_\infty) = 1$ y $v_{E^{\mathrm{mod}}}(\mu) = 1$. Por otro lado $(-1)^e = \mathrm{N}_{E^{\mathrm{mod}}/K_\infty}(-1) = (-1)^{[E^{\mathrm{mod}}:K_\infty]}$. Se sigue que $-\xi \in \mathrm{N}_{E^{\mathrm{mod}}/K_\infty}((E^{\mathrm{mod}})^*)$.

Sea $-\xi = \mathrm{N}_{E^{\mathrm{mod}}/K_\infty}(\delta)$. Como ρ es un elemento uniformizador de E^{mod}, tenemos

$$(E^{\mathrm{mod}})^* = \langle\rho\rangle \times \mathbb{F}^*_{E^{\mathrm{mod}}} \times U^{(1)}_{E^{\mathrm{mod}}} = \langle\rho\rangle \times \mathbb{F}^*_q \times U^{(1)}_{E^{\mathrm{mod}}}.$$

Ahora bien $v_{K_\infty}(\mathrm{N}_{E^{\mathrm{mod}}/K_\infty}(\rho^s)) = es$ el cual es 0 si y solamente si $s = 0$ lo cual equivale a que $\rho^s = 1$. Además $\mathrm{N}_{E^{\mathrm{mod}}/K_\infty}(U^{(1)}_{E^{\mathrm{mod}}}) \subseteq U^{(1)}_{K_\infty}$. Por tanto $-\xi = \mathrm{N}_{E^{\mathrm{mod}}/K_\infty}(\delta)$ con $\delta \in \mathbb{F}^*_q$ por lo que $-\xi = \delta^e \in (\mathbb{F}^*_q)^e$. Se sigue que

$$\begin{aligned} E^{\mathrm{mod}} &= K_\infty\Big(\sqrt[e]{\frac{\xi}{T}}\Big) = K_\infty\Big(\sqrt[e]{\frac{-(-\xi)}{T}}\Big) = K_\infty\Big(\sqrt[e]{\frac{-\delta^e}{T}}\Big) \\ &= K_\infty\Big(\delta\sqrt[e]{-\frac{1}{T}}\Big) = K_\infty\Big(\sqrt[e]{-\frac{1}{T}}\Big) \end{aligned}$$

lo cual demuestra (2). □

Para el siguiente corolario ver [136, Proposiciones 9.3.19 y 9.3.20].

Corolario 7.3.12. *La extensión abeliana de K_∞ asociada a* $\mathrm{núc}\,\phi_\infty$ *es el campo $K^\phi_\infty := K_\infty\big[\sqrt[q-1]{-1/T}\big] = \mathbb{F}_q\big(\big(\sqrt[q-1]{-1/T}\big)\big)$ la cual es la máxima extensión abeliana moderadamente ramificada de K_∞ tal que $1/T$ es una norma. En particular, si $\mathscr{K}$ es una extensión separable de K_∞, la extensión abeliana de $\mathscr{K}$ asociada a* $\mathrm{núc}\,\phi_{\mathscr{K}}$ *por la teoría local de campos de clase, es la composición $\mathscr{K}^\phi := \mathscr{K}K^\phi_\infty = \mathscr{K}\big[\sqrt[q-1]{-1/T}\big] = \mathscr{K}\big[\sqrt[q-1]{-\pi_\infty}\big]$.*

Demostración. Sea E/K_∞ la extensión asociada a $\mathrm{núc}\,\phi_\infty$ dada por la teoría local de campos de clase, la cual, por construcción, verifica la identidad nórmica: $\mathrm{N}_{E/K_\infty}(E^*) = \mathrm{núc}\,\phi_\infty = U^{(1)}_{K_\infty}\Big(\frac{1}{T}\Big)^{\mathbb{Z}}$ (ver Proposición 5.6.7 y Teoremas 5.8.64 y 5.8.75). De hecho, como $\frac{1}{T}$ es norma, $f = 1$ y $\mathbb{F}^*_q$ corrsponde a la ramificación moderada y $U^{(1)}_{K_\infty}$ a la ramificación salvaje, de donde

$\mathbb{F}_q^* U_{K_\infty}^{(1)} = U_{K_\infty}$ corresponde a la ramificación. Por tanto a primera afirmación se sigue inmediatamente del Teorema 7.3.11 pues $E^{\mathrm{mod}} = \mathbb{F}_q\Big(\Big(\sqrt[e]{-\frac{1}{T}}\Big)\Big)$ y la e máxima es $e = q-1$, esto es, la máxima extensión corresponde a $K_\infty\Big(\sqrt[q-1]{-\frac{1}{T}}\Big) = \mathbb{F}_q\Big(\Big(\sqrt[q-1]{-\frac{1}{T}}\Big)\Big)$.

Ahora (ver Teoremas 5.7.13 y 6.9.5), tenemos que $\phi_{\mathscr{K}} = \phi_\infty \circ \mathrm{N}_{\mathscr{K}/K_\infty}$ lo cual implica $\mathrm{núc}\,\phi_{\mathscr{K}} = \mathrm{N}^{-1}_{\mathscr{K}/K_\infty}(\mathrm{núc}\,\phi_\infty)$. Por tanto, si $H_{\mathscr{K}}$ es el grupo de normas de $\mathscr{K}/K_\infty$, esto es, $\mathrm{N}_{\mathscr{K}/K_\infty}\mathscr{K}^* = H_K$. De esta forma tenemos que $\mathrm{núc}\,\phi_{\mathscr{K}} = H_K \cap H_{\mathrm{núc}\,\phi_\infty} = H_{\mathscr{K}} \cap H_{K_\infty^\phi} = H_{\mathscr{K}K_\infty^\phi}$. Por tanto $\mathrm{núc}\,\phi_{\mathscr{K}} = H_{\mathscr{K}^\phi} = H_{\mathscr{K}K_\infty^\phi}$ y en consecuencia, $\mathscr{K}^\phi = \mathscr{K}K_\infty^\phi = \mathscr{K}\big[\sqrt[q-1]{-1/T}\big]$ (ver Teorema 5.7.14). □

Consideremos L/K una extensión finita y separable. Sea $\mathcal{P}_\infty := \{\mathfrak{p} \in \mathbb{P}_L \mid \mathfrak{p}|\mathfrak{p}_\infty\}$. Sea L_v la completación de L en $v \in \mathcal{P}_\infty$. Se tiene que $\phi_{L_v}(x)$ está bien definido para $x \in L^*$.

Definición 7.3.13. El elemento $x \in L^*$ se llama *totalmente positivo* si $\phi_{L_v}(x) = 1$ para toda $v \in \mathcal{P}_\infty$.

Se define $L^+ = \{x \in L \mid x \text{ es totalmente positivo}\}$.

Definición 7.3.14. El *grupo de signos* de un campo global L se define por $\mathrm{Sig}_L := L^*/L^+$.

Si R es un subgrupo de L^*, la imagen de R bajo Sig_L se denota por $\mathrm{sig}_L(R)$. En particular, $\mathrm{Sig}_L = \mathrm{sig}_L(L^*)$.

Proposición 7.3.15. *Se tiene* $\mathrm{Sig}_L = \mathrm{sig}_L(L^*) \cong \prod_{v\in\mathcal{P}_\infty} \phi_{L_v}(L_v^*)$.

Demostración. Consideremos el mapeo $\theta\colon L^* \longrightarrow \prod_{v\in\mathcal{P}_\infty} \phi_{L_v}(L_v^*)$ definido por $\theta(x) = \big(\phi_{L_{v_1}}(x), \ldots, \phi_{L_{v_s}}(x)\big)$. Entonces θ es un homomorfismo de grupos y $x \in \mathrm{núc}\,\theta \iff \theta(x) = \big(\phi_{L_{v_1}}(x), \ldots, \phi_{L_{v_s}}(x)\big) = (1, \ldots, 1) \iff \phi_{L_v}(x) = 1$ para toda $v \in \mathcal{P}_\infty \iff x \in L^*$ y $\tilde{\theta}\colon L^*/L^+ \longrightarrow \prod_{v\in\mathcal{P}_\infty} \phi_{L_v}(L_v^*)$ es un monomorfismo.

Veamos la suprayectividad de $\tilde{\theta}$. Sea $(\alpha_1, \ldots, \alpha_s) \in \prod_{v\in\mathcal{P}_\infty} \phi_{L_v}(L_v^*)$. Sean $y_i \in L_v^*$ tal que $\phi_{L_v}(y_i) = \alpha_i$. Digamos que $y_i = \sum_{j=m}^{\infty} \beta_j \pi^j$, $m \in \mathbb{Z}$, $\beta_m \neq 0$. Entonces $y_i = \beta_m \pi^m \xi$ con $\xi \in U_{L_v}^{(1)}$ y $\phi_{L_{v_i}} = \phi_\infty(\mathrm{N}_{L_{v_i}/K_\infty}(y_i)) = \phi_\infty(\mathrm{N}_{L_{v_i}/K_\infty}(\beta_m))$.

Sea $x \in L^*$ con $v_{L_{v_i}}(x - y_i) > m$. Ahora bien, $v_{L_{v_i}}(y_i) = m$ por lo que $v_{L_{v_i}}(x) = m$ y $\phi_{L_{v_i}}(y_i) = \phi_{L_{v_i}}(x)$. De esta forma, usando el Teorema de Aproximación de Artin, tomamos $x \in L^*$ tal que $v_{L_{v_i}}(x - y_i) > m_i$ donde $v_{L_{v_i}}(y) = m_i$ y $\big(\phi_{L_{v_1}}(y_1), \ldots, \phi_{L_{v_s}}(y_s)\big) = \big(\phi_{L_{v_1}}(x), \ldots, \phi_{L_{v_s}}(x)\big) = \theta(x)$. Por tanto θ es suprayectiva y $\tilde{\theta}$ es un isomorfismo. □

Observación 7.3.16. Sea L un campo numérico. Entonces $L_v \in \{\mathbb{R}, \mathbb{C}\}$ para $v|\infty$. Entonces $\mathrm{N}_{L_v/\mathbb{R}} L_v^* \in \{\mathbb{R}^+, \mathbb{R}^*\}$ y $\phi_{L_v} L_v^* \subseteq \{\pm 1\}$. Entonces $L^*/L^+ \cong C_2^t$ donde t es e número de lugares reales de L tales que $\mathrm{N}_{L_v/\mathbb{R}} \mathbb{R}^* = \mathbb{R}^*$ pues en este caso $\phi_{L_v}(\mathbb{R}^*) = \{\pm 1\}$.

Definición 7.3.17. Sea $\mathcal{O}_L = \{x \in L \mid v_{\mathfrak{p}}(x) \geq 0 \text{ para todo } \mathfrak{p} \notin \mathcal{P}_\infty\}$. En otras palabras, $\mathcal{O}_L = \mathcal{O}_S$ donde $S = \mathcal{P}_\infty$. Sean $P_L^+ = \{x\mathcal{O}_L \mid x \in L^+\}$ el grupo de ideales principales de $\mathcal{O}_L$ que son generados por un elemento totalmente positivo y definimos el *grupo de clases de ideales extendidos*

$$Cl_L^{\mathrm{ext}} = Cl_L^+ = I_L/P_L^+ = C_S^{\mathrm{ext}} = C_S^+,$$

donde I_L es el grupo de ideales fraccionarios de $\mathcal{O}_L$. Recordemos que $Cl_L = I_L/P_L$ donde $P_L = \{(x) = x\mathcal{O}_L \mid x \in L^*\}$.

Se tiene $|Cl_L| < \infty$ ([136, Corolario 10.2.14]).

Definición 7.3.18. Definimos los siguientes subgrupos del grupo de idèles J_L de L

$$U_L = \prod_{v \in \mathcal{P}_\infty} L_v^* \times \prod_{v \notin \mathcal{P}_\infty} U_{L_v},$$
$$U_L^+ = \prod_{v \in \mathcal{P}_\infty} \mathrm{núc}\, \phi_{L_v} \times \prod_{v \notin \mathcal{P}_\infty} U_{L_v}.$$

Se tiene que U_L y U_L^+ son subgrupos abiertos del grupo de idèles de L, J_L (ver la Observación 6.2.16 y usar el Proposición 3.2.1). Los grupos U_L y U_L^+ son los correspondientes a J_L^1 y J_L^{1+} respectivamente en el caso de campos numéricos.

Proposición 7.3.19. *Los grupos de clases de ideales en el sentido ordinario y en el sentido extendido (o restringido) están dados por los isomorfismos canónicos*

(1) $Cl_L \cong J_L/U_L L^*$,
(2) $Cl_L^+ = Cl_L^{\mathrm{ext}} \cong J_L/U_L^+ L^*$.

Demostración. Es consecuencia del isomorfimso $I_L \cong J_L/U_L$. □

Corolario 7.3.20. *Las clases en el sentido ordinario y en el sentido extendido están ligadas por la sucesión exacta*

$$1 \longrightarrow \mathrm{sig}_L(E_L) \longrightarrow \mathrm{Sig}_L \longrightarrow Cl_L^{\mathrm{ext}} \longrightarrow Cl_L \longrightarrow 1,$$

donde E_L son las unidades de $\mathcal{O}_L$.

Demostración. Sea $\theta\colon Cl_L^{\text{ext}} \longrightarrow Cl_L$ dada por $\vec{\alpha} \bmod U_L^+ L^* \xrightarrow{\theta} \vec{\alpha} \bmod U_L L^*$. Entonces θ es un epimorfismo con núcleo $\operatorname{núc}\theta = U_L L^*/U_L^+ L^*$. Por tanto se tiene la siguiente sucesión exacta

$$1 \longrightarrow U_L L^*/U_L^+ L^* \longrightarrow Cl_L^{\text{ext}} \longrightarrow Cl_L \longrightarrow 1.$$

Sea $\psi\colon U_L/U_L^+ \longrightarrow U_L L^*/U_L^+ L^*$ dada por $\psi(\vec{\alpha} \bmod U_L^+) = \vec{\alpha} \bmod U_L^+ L^*$. Entonces es un epimorfismo bien definido. Ahora, se tiene

$$\frac{U_L}{U_L^+} \cong \prod_{v\in\mathcal{P}_\infty} \frac{L_v^*}{\operatorname{núc}\phi_{L_v}} \cong \prod_{v\in\mathcal{P}_\infty} \phi_{L_v}(L_v^*) \cong \operatorname{Sig}_L .$$

Por tanto se tiene la sucesión exacta

$$1 \longrightarrow \operatorname{núc}\psi = \frac{U_L^+ L^* \cap U_L}{U_L^+} \longrightarrow \frac{U_L}{U_L^+} \cong \operatorname{Sig}_L \longrightarrow \frac{U_L L^*}{U_L^+ L^*} \longrightarrow 1.$$

Se sigue que la sucesión

$$1 \longrightarrow \frac{U_L^+ L^* \cap U_L}{U_L^+} \longrightarrow \operatorname{Sig}_L \longrightarrow Cl_L^{\text{ext}} \longrightarrow Cl_S \longrightarrow 1$$

es exacta.

Ahora sea $\mu\colon L^* \cap U_L \hookrightarrow U_L^+ L^* \cap U_L \longrightarrow \frac{U_L^+ L^* \cap U_L}{U_L^+}$ dada por $\mu(\xi) = \xi \bmod U_L^+$. Verificamos que μ es epimorfismo. Sea $\xi \in U_L^+ L^* \cap U_L$, $\xi = ab \in U_L$ y $a \in U_L^+$, $b \in L^*$. Esto es, $\xi \equiv b \bmod U_L^+$ y $\xi \in U_L$, $b \in L^*$. Por tanto $\mu(b) = \bar{\xi}$ y $b \in L^*$. Entonces se tiene $b = \xi a^{-1} \in U_L U_L^+ = U_L$. Por tanto $b \in U_L \cap L^*$. De esta forma μ es suprayectiva.

Por otro lado, $\operatorname{núc}\mu = (L^* \cap U_L) \cap U_L^+ = L^* \cap U_L^+$ por lo que $\frac{U_L^+ L^* \cap U_L}{U_L^+} \cong \frac{L^* \cap U_L}{L^* \cap U_L^+}$.

Puesto que $U_L = \prod_{v\in\mathcal{P}_\infty} L_v^* \times \prod_{v\notin\mathcal{P}_\infty} U_{L_v}$, $L^* \cap U_L = E_L$ y $L^* \cap U_L^+ = L^* \cap U_L^+ \cap U_L = E_L \cap U_L^+ =: E_L^+$. Por tanto

$$\frac{U_L^+ L^* \cap U_L}{U_L^+} \cong \frac{E_L}{E_L^+} \cong \frac{E_L L^*}{L^*} \cong \operatorname{sig}(E_L),$$

como consecuencia de la Proposición 7.3.15. □

Sea L_H la extensión abeliana de L correspondiente al subgrupo de idèles $L^* U_L$. Entonces L_H es la máxima extensión abeliana de L no ramificada y donde los elementos de $\mathcal{P}_\infty$ se descomponen totalmente. En otras palabras, L_H es el correspondiente al tercer análogo al campo de clase de Hilbert con $L_H = L_{H,S}$ y donde $S = \mathcal{P}_\infty$. Además

$$\operatorname{Gal}(L_H/L) \cong Cl(\mathcal{O}_L) = Cl_L \cong J_L/U_L L^*.$$

Estamos en condiciones de definir el análogo al campo de clase de Hilbert extendido en el caso de campos de funciones globales.

Definición 7.3.21. Sea $L_{H^+} = L_H^{\text{ext}}$ la extensión abeliana de L correspondiente al subgrupo de idèles $L^* U_L^+$ donde $U_L^+ = \prod_{v\in\mathcal{P}_\infty} \text{núc}\,\phi_{L_v} \times \prod_{v\notin\mathcal{P}_\infty} U_{L_v}$.

El campo L_{H^+} recibe el nombre de *el campo de clase de Hilbert extendido* correspondiente a $\mathcal{O}_L$.

Se tiene que L_{H^+}/L es una extensión no ramificada en ningún primo finito, $L_H \subseteq L_{H^+}$ y

$$\text{Gal}(L_{H^+}/L) \cong J_L/L^* U_L^+ \cong I_L/P_L^+ \cong Cl_L^+ \cong Cl_L^{\text{ext}}.$$

Por otro lado, se tiene

$$\frac{U_L}{U_L^+} \cong \prod_{v\in\mathcal{P}_\infty} \frac{L_v^*}{\text{núc}\,\phi_{L_v}} \cong \prod_{v\in\mathcal{P}_\infty} \phi(L_v^*) \cong \frac{L^*}{L^+}.$$

Observación 7.3.22. Como consecuencia del Corolario 7.3.20 se tiene que $[L_{H^+} : L_H]|| \text{Sig}_L\,| = \prod_{v\in S} |\phi_{L_v}(L_v^*)||(q-1)^{|S|}$.

Por tanto, L_{H^+}/L es no ramificada en los primos finitos y moderadamente ramificada en los primos infinitos.

Además

$$\text{Gal}(L_{H^+}/L_H) \cong \frac{\text{Gal}(L_{H^+}/L)}{\text{Gal}(L_H/L)} \cong \frac{U_L L^*}{U_L^+ L^*} \cong \frac{\text{Sig}_L}{\left(\frac{U_L \cap U_L^+ L^*}{U_L^+}\right)}.$$

Todo esto es aplicable a campos numéricos sustituyendo $q-1$ por 2.

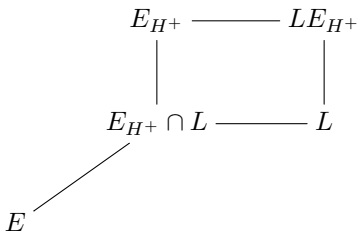
Ejemplos 7.3.23.

(1) Para $L = K = \mathbb{F}_q(T)$, $\text{sig}(L) = \text{sig}(\mathbb{F}_q^*) = \mathbb{F}_q^*$. Esto es, $\text{Sig}_L = \mathbb{F}_q^* = E_L L^+/L^+$, $\text{sig}(E_L) = \mathbb{F}_q^*$. Por tanto, $L_H = L_{H^+} = L$.

(2) Sea $M \in R_T = \mathbb{F}_q[T]$ un polinomio mónico de grado mayor o igual a 1. Sea $L = K(\Lambda_M)$.
Tenemos que para toda $v \in \mathcal{P}_\infty$, $L_v = K_\infty\big(\sqrt[q-1]{-1/T}\big)$, $\phi_{L_v} = \phi_\infty \circ \text{N}_{L_v/K_\infty}$. Por el Teorema 5.8.62, $\text{N}_{L_v/K_\infty} L_v^* = (\pi_\infty) \times U_\infty^{(1)}$ por lo que $\text{núc}\,\phi_{L_v} = L_v^*$ y $\text{Sig}_K = \{1\}$. Se sigue que $L_H = L_{H^+}$.

Observación 7.3.24. Sea L/E una extensión finita y separable de campos globales. Entonces $E_{H^+} \subseteq L_{H^+}$. Si L/E es una extensión de Galois, entonces L_{H^+}/E también es de Galois.

De hecho se tiene



Ahora bien $E_{H^+}/E_{H^+} \cap L$ es una extensión abeliana no ramificada en los primos finitos lo cual implica que LE_{H^+}/L también lo es.

Consideremos la norma $\mathrm{N}_{L/E}\colon C_L = J_L/L^* \longrightarrow C_E = J_E/E^*$ de grupos de idèles y puesto que $N_{L_w/E_v}(\mathrm{núc}\,\phi_{L_w}) \subseteq \mathrm{núc}\,\phi_{E_v}$, $\mathrm{N}_{L/E}(U_L^+) \subseteq U_E^+$ y $\mathrm{N}_{L/E}(L^*) \subseteq E^*$, se sigue que $\mathrm{N}_{L/E}(U_L^+L^*) \subseteq U_E^+E^*$. Ahora bien $U_E^+E^*$ corresponde a E_{H^+}. Por el Teorema 6.9.5 obtenemos que $E_{H^+} \subseteq E_{H^+}L \subseteq L_{H^+}$.

Ahora si L/E es una extensión de Galois, consideremos $\sigma\colon L_{H^+} \longrightarrow \bar{L}_{H^+}$ un monomorfismo tal que $\sigma|_E = \mathrm{Id}_E$. Puesto que L/E es Galois, $\sigma|_L\colon L \longrightarrow \bar{L}$ con $\sigma|_E = \mathrm{Id}_E$, obtenemos que $\sigma(L) = L$. Por otro lado como $\sigma(\mathrm{núc}\,\phi_{L_w}) = \mathrm{núc}\,\phi_{L_{\sigma(w)}}$ se tiene que $\sigma(U_L^+) = U_L^+$ y $\sigma(L^*) = L^*$ lo cual implica que $\sigma(U_L^+L^*) = U_L^+L^*$. Por tanto $\sigma(L_{H^+}) = L_{H^+}$, esto es, $\sigma \in \mathrm{Aut}_E(L_{H^+})$ por lo que L_{H^+}/E es Galois.

Observación 7.3.25. De hecho, para $\star \in \{\mathfrak{ge}, \mathfrak{gex}, H, H^+\}$ y para una extensión finita y separable L/E de campos globales, se tiene que $E_\star \subseteq L_\star$.

Para finalizar esta subsección, veamos cuales son los campos de constantes de L_H para un campo de funciones global L con campo de constantes $\mathbb{F}_q$. Hacemos notar que se calcula el campo de constantes de L_H en [136, Proposición 14.8.3]. Ver también [136, Teorema 14.3.1] y el Corolario 7.2.17 más adelante. Aquí daremos una demostración diferente.

Sea pues L/K una extensión finita y separable donde $K = \mathbb{F}_q(T)$. Recordemos que si tenemos una extensión abeliana finita E/F tal que el campo de constantes de F es $\mathbb{F}_q$ y tal que E corresponde al grupo Λ de idèles de J_F, esto es, $\mathrm{Gal}(E/F) \cong J_F/\Lambda F^*$, entonces si $d = \mín\{n \in \mathbb{N} \mid \text{existe } \vec{\alpha} \in \Lambda \text{ con } \mathrm{gr}\,\vec{\alpha} = n\}$, se tiene que el campo de constantes de E es $\mathbb{F}_{q^d}$ (Teorema 6.8.37).

En [136, Teorema 14.3.1] se da el campo de constantes del campo de clases de Hilbert. A continuación volvemos a obtener este resultado por otros métodos.

Sea $\mathrm{con}_{K/L}\,\mathfrak{p}_\infty = \mathfrak{p}_1^{e_1}\cdots\mathfrak{p}_r^{e_r}$ y sean $t_i := \mathrm{gr}\,\mathfrak{p}_i$, $1 \le i \le r$, $t_0 = \mathrm{mcd}(t_1, \ldots, t_r)$.

Teorema 7.3.26. *Con las notaciones anteriores, el campo de constantes de L_H es $\mathbb{F}_{q^{t_0}}$.*

Demostración. Sean $a_1, \ldots, a_r \in \mathbb{Z}$ tales que $t_0 = \sum_{i=1}^r a_i t_i$. Sea $\vec{\alpha} \in J_L$ el idèle dado por componentes como $\alpha_{\mathfrak{p}_i} = \pi_{\mathfrak{p}_i}^{a_i}$, $1 \le i \le r$ y $\alpha_{\mathfrak{p}} = 1$ para $\mathfrak{p} \nmid \mathfrak{p}_\infty$. Entonces $\vec{\alpha} \in U_L$ y

$$\mathrm{gr}\,\vec{\alpha} = \sum_{i=1}^r a_i\,\mathrm{gr}\,\alpha_{\mathfrak{p}_i} = \sum_{i=1}^r a_i\,\mathrm{gr}\,\mathfrak{p}_i v_{\mathfrak{p}_i}(\pi_{\mathfrak{p}_i}) = \sum_{i=1}^r a_i t_i = t_0.$$

Ahora sea $\vec{\beta} \in U_L$. Entonces las componentes de $\vec{\beta}$ son de la forma $\beta_{\mathfrak{p}_i} = \xi_i \pi_{\mathfrak{p}_i}^{b_i}$, $1 \le i \le r$ con $\xi_i \in U_{\mathfrak{p}_i}$ y $b_i \in \mathbb{Z}$ y $\beta_{\mathfrak{p}} \in U_{\mathfrak{p}}$ para $\mathfrak{p} \nmid \mathfrak{p}_\infty$. Entonces $\mathrm{gr}\,\vec{\beta} =$

$\sum_{i=1}^r b_i t_i$ y puesto que $t_0|t_i$, $1 \leq i \leq r$, $t_0|\operatorname{gr}\vec{\beta}$. Se sigue que $t_0 = \min\{n \in \mathbb{N} \mid \text{existe } \vec{\alpha} \in U_L \text{ tal que } \operatorname{gr}\vec{\alpha} = n\}$. Por el Teorema 6.8.37 obtenemos que el campo de constantes de L_H es $\mathbb{F}_{q^{t_0}}$. □

Teorema 7.3.27. *Sea K/k una extensión finita y separable con $k = \mathbb{F}_q(T)$. Sea $\mathcal{O}_K$ la cerradura entera de $\mathbb{F}_q[T]$ en K. Entonces un ideal fraccionario $\mathfrak{p}$ de $\mathcal{O}_K$ se descompone totalmente en*

(1) *K_H/K si y solamente si $\mathfrak{p}$ es principal;*
(2) *K_{H^+}/K si y solamente si $\mathfrak{p}$ es principal generado por un elemento totalmente positivo de K, es decir un elemento de $K^+ = \{x \in K \mid \phi_{K_\mathfrak{p}}(x) = 1 \text{ para toda } \mathfrak{p}|\mathfrak{p}_\infty\}$.*

Demostración. Del Corolario 6.9.4 se tiene que $\mathfrak{p}$ se descompone totalmente en K_H/K (resp. en K_{H^+}/K) si y solamente si $\theta\lceil K_\mathfrak{p}^*\rceil_\mathfrak{p} := \{(\ldots,1,x,1,\ldots) \mid x \in K_\mathfrak{p}^*\} \subseteq K^*U_K$ (resp. $\subseteq K^*U_K^+$) si y solamente si para toda $x \in K_\mathfrak{p}^*$ existen $\beta_x \in K^*$ y $\vec{\alpha}_x \in U_K$ (resp. $\vec{\alpha}_x \in U_K^+$) tal que $\theta\lceil x\rceil_\mathfrak{p} = \beta_x\vec{\alpha}_x$. Por tanto $\vec{\alpha}_x = (\ldots,\beta_x^{-1},\ldots,\beta_x^{-1},\underset{\underset{\mathfrak{p}}{\uparrow}}{\beta_x^{-1}x},\beta_x^{-1},\ldots,\beta_x^{-1},\ldots)$. Esto es equivalente a $v_\mathfrak{q}(\beta_x) = 0$ para toda $\mathfrak{q} \neq \mathfrak{p}$ y $\mathfrak{q} \nmid \mathfrak{p}_\infty$ y $\left(\beta_x^{-1}\right)_{\mathfrak{q}|\mathfrak{p}_\infty} \in \prod_{\mathfrak{q}|\mathfrak{p}_\infty} K_\mathfrak{q}^*$ (resp. $\left(\beta_x^{-1}\right)_{\mathfrak{q}|\mathfrak{p}_\infty} \in \prod_{\mathfrak{q}|\mathfrak{p}_\infty} \operatorname{núc}\phi_{K_\mathfrak{q}}$).

Sea $x \in K_\mathfrak{p}^*$. El ideal principal en $\mathcal{O}_K$ generado por β_x satisface $\langle\beta_x\rangle = \mathfrak{p}^{n_x} = \beta_x\mathcal{O}_K$. En particular para $x \in K_\mathfrak{p}^*$ con $v_\mathfrak{p}(\beta_x) = 1$ tenemos $\langle\beta_x\rangle = \mathfrak{p}$, $\beta_x \in K^*$. Por tanto $\mathfrak{p}$ es un ideal principal $\mathfrak{p} = \langle\beta_x\rangle$ (resp. $\mathfrak{p}$ es un ideal principal $\mathfrak{p} = \langle\beta_x\rangle$ y $\beta_x \in \operatorname{núc}\phi_{K_\mathfrak{q}}$ para toda $\mathfrak{q}|\mathfrak{p}_\infty$). □

7.4. Teoría global de campos de clase vía ideales o divisores

En la formulación vía idèles de la ley de reciprocidad, las extensiones abelianas finitas corresponden unívocamente con los grupos de normas $\mathrm{N}_{L/K} C_L$. En la formulación vía ideales (campos numéricos), hay una correspondencia (no biyectiva) similar, pero más complicada. Aquí también las extensiones abelianas finitas corresponden a ciertos grupos de normas (más de uno) en el grupo de ideales fraccionarios D_K de K. El símbolo de la norma residual $(\_, L/K)\colon C_K \to \operatorname{Gal}(L/K)$ es reemplazado por el símbolo de Artin, pero este último no está definido en los primos ramificados.

Para un módulus $\mathfrak{m} = \prod_{\mathfrak{p}\in\mathbb{P}_K} \mathfrak{p}^{n_\mathfrak{p}}$, $D_K^\mathfrak{m}$ denotará al grupo de ideales fraccionarios (divisores) primos relativos a la parte finita de $\mathfrak{m}$, $P_K^\mathfrak{m}$ es el grupo de ideales (divisores) principales $(a) \in P_K$ con $a \equiv 1 \bmod \mathfrak{m}$. Esto último significa que si $\mathfrak{p}|\mathfrak{m}$ es finito, entonces $a \equiv 1 \bmod \mathfrak{m}$ significa $a \equiv 1 \bmod \mathfrak{p}^{n_\mathfrak{p}}$ en el sentido usual. Si $\mathfrak{p}$ es real y $n_\mathfrak{p} = 1$, $a \equiv 1 \bmod \mathfrak{m}$ significa $a > 0$ en el lugar $\mathfrak{p}$. Si $n_\mathfrak{p} = 0$ o $\mathfrak{p}$ es complejo $a \equiv 1 \bmod \mathfrak{m}$ no establece ninguna restricción para a.

Definición 7.4.1. El grupo $P_K^{\mathfrak{m}}$ se llama el *rayo módulo* $\mathfrak{m}$ y todo grupo $H_K^{\mathfrak{m}}$ tal que $P_K^{\mathfrak{m}} \subseteq H_K^{\mathfrak{m}} \subseteq D_K^{\mathfrak{m}}$ se llama el *grupo ideal (divisor) módulo* $\mathfrak{m}$ y $D_K^{\mathfrak{m}}/P_K^{\mathfrak{m}}$ se llama el *grupo de rayos módulo* $\mathfrak{m}$.

Si $\mathfrak{m} = 1$, $D_K^{\mathfrak{m}} = D_K$ y $P_K^{\mathfrak{m}} = P_K$, es decir, $D_K^1/P_K^1 = D_K/P_K = I_K$ es el grupo de rayos módulus 1.

Por ejemplo, si denotamos ∞ un lugar real de K (caso numérico) y $\mathfrak{m} = \infty$, se tiene $D_K^{\mathfrak{m}} = D_K^{\infty} = D_K = D_K^1$ y $P_K^{\infty} = \{(a) \in P_K \mid a > 0 \text{ en } \infty\} \subseteq P_K \subseteq D_K$ y $\frac{D_K/P_K^{\infty}}{P_K/P_K^{\infty}} \cong D_K/P_K$, es decir,

$$1 \to \frac{P_K}{P_K^{\infty}} \to \frac{D_K}{P_K^{\infty}} \to \frac{D_K}{P_K} \to 1$$

es exacta. Se puede pensar que D_K/P_K corresponde al campo de clase de Hilbert y que D_K/P_K^{∞} corresponde al campo de clase de Hilbert extendido, de hecho, con más precisión, el campo de clase de Hilbert extendido, corresponde al módulus $\mathfrak{m} := \prod_{\mathfrak{p} \text{ real}} \mathfrak{p}$ y $P_K^{\mathfrak{m}} = \{(a) \in P_K \mid a > 0 \text{ para todo } \mathfrak{p} \text{ real}\}$.

Definición 7.4.2. Sea K un campo numérico. Si L/K es una extensión abeliana finita y $\mathfrak{m}$ es un módulus, $\mathfrak{m}$ se llama *módulus de definición* o *módulus admisible* para L/K si L está contenido en el campo de clases de rayos módulus $\mathfrak{m}$, es decir si $C_K^{\mathfrak{m}} \subseteq \mathrm{N}_{L/K} C_L$ o, equivalentemente, $L \subseteq K^{\mathfrak{m}}$.

Si $\mathfrak{m}|\mathfrak{m}'$ y si $\mathfrak{m}$ es un módulus de definición para L, también lo es $\mathfrak{m}'$ pues $C_K^{\mathfrak{m}'} \subseteq C_K^{\mathfrak{m}}$.

El *conductor* $\mathfrak{f} = \mathfrak{f}_{L/K} = \mathfrak{f}(L/K)$ es el máximo común divisor de los moduli de definición de L/K (Definición 7.4.2).

Definición 7.4.3. Sea K un campo numérico. Si L/K es una extensión abeliana finita y $\mathfrak{m}$ es un módulus de definición de L/K, entonces $H_K^{\mathfrak{m}} := (\mathrm{N}_{L/K} D_K^{\mathfrak{m}}) P_K^{\mathfrak{m}}$ se llama el *grupo ideal definido módulus* $\mathfrak{m}$ asociado a L/K.

Sea $\left(\frac{L/K}{\mathfrak{p}}\right)$ el símbolo de Artin, esto es $\left(\frac{L/K}{\mathfrak{p}}\right) = \mathrm{Fr}_{\mathfrak{p}} \in \mathrm{Gal}(L/K)$ el automorfismo de Frobenius para $\mathfrak{p} \in \mathbb{P}_K$ finito y no ramificado en L.

Teorema 7.4.4. *Sea K un campo global. Sea $\Lambda\colon J_K \to D_K$ dado por*

$$\Lambda(\vec{\alpha}) = \mathfrak{a}_{\vec{\alpha}} = \prod_{\substack{\mathfrak{p} \in \mathbb{P}_K \\ \mathfrak{p} \nmid \infty}} \mathfrak{p}^{v_{\mathfrak{p}}(\alpha_{\mathfrak{p}})}.$$

Entonces si $\mathfrak{m} = \prod_{\mathfrak{p} \in \mathbb{P}_K} \mathfrak{p}^{n_{\mathfrak{p}}}$ es cualquier módulus, Λ induce un isomorfismo

$$\Lambda_{\mathfrak{m}}\colon C_K/C_K^{\mathfrak{m}} \longrightarrow D_K^{\mathfrak{m}}/P_K^{\mathfrak{m}}.$$

Demostración. Se tiene $C_K/C_K^{\mathfrak{m}} \cong J_K/J_K^{\mathfrak{m}}K^*$, donde $J_K^{\mathfrak{m}} = \{\vec{\alpha} \in J_K \mid \vec{\alpha} \equiv 1 \text{ mód } \mathfrak{m}\}$. Sean $S = \{\mathfrak{p} \in \mathbb{P}_K \mid \mathfrak{p}|\mathfrak{m}\}$ y $J_K^{\langle \mathfrak{m}\rangle} = J_K^S = \{\vec{\alpha} \in J_K \mid \alpha_{\mathfrak{p}} = 1 \text{ para todo } \mathfrak{p}|\mathfrak{m}\}$. Notemos que si $S = \{\mathfrak{p} \mid \mathfrak{p}\big|\mathfrak{m}\}$, entonces $J_K^{\langle \mathfrak{m}\rangle} = J_K^S$.

Primero probemos que $J_K = J_K^{\langle \mathfrak{m}\rangle} J_K^{\mathfrak{m}} K^*$. Sea $\vec{\alpha} \in J_K$. Por el Teorema de Aproximación de Artin, existe $a \in K^*$ tal que $\alpha_{\mathfrak{p}} a \equiv 1 \text{ mód } \mathfrak{p}^{n_{\mathfrak{p}}}$ para $\mathfrak{p}|\mathfrak{m}$. Escribimos $\alpha_{\mathfrak{p}} a = \beta_{\mathfrak{p}}\gamma_{\mathfrak{p}}$ con

$$\begin{aligned} &\beta_{\mathfrak{p}} = 1 \quad \text{para} \quad \mathfrak{p}|\mathfrak{m} \quad \text{y} \quad \beta_{\mathfrak{p}} = \alpha_{\mathfrak{p}} a \quad \text{para} \quad \mathfrak{p} \nmid \mathfrak{m}, \\ &\gamma_{\mathfrak{p}} = \alpha_{\mathfrak{p}} a \quad \text{para} \quad \mathfrak{p}|\mathfrak{m} \quad \text{y} \quad \gamma_{\mathfrak{p}} = 1 \quad \text{para} \quad \mathfrak{p} \nmid \mathfrak{m}. \end{aligned}$$

Entonces $\vec{\beta} = (\beta_{\mathfrak{p}})_{\mathfrak{p}} \in J_K^{\langle \mathfrak{m}\rangle}$ y $\vec{\gamma} = (\gamma_{\mathfrak{p}})_{\mathfrak{p}} \in J_K^{\mathfrak{m}}$. Además, se tiene, $\vec{\alpha} = \vec{\beta}\vec{\gamma}a^{-1} \in J_K^{\langle \mathfrak{m}\rangle} J_K^{\mathfrak{m}} K^*$.

Ahora bien $\frac{C_K}{C_K^{\mathfrak{m}}} \cong \frac{J_K}{J_K^{\mathfrak{m}}K^*} = \frac{J_K^{\langle \mathfrak{m}\rangle} J_K^{\mathfrak{m}} K^*}{J_K^{\mathfrak{m}}K^*} \cong \frac{J_K^{\langle \mathfrak{m}\rangle}}{J_K^{\mathfrak{m}}K^* \cap J_K^{\langle \mathfrak{m}\rangle}}$. De esta forma se tiene que $\Lambda\colon J_K \to D_K$ induce un epimorfismo

$$J_K^{\langle \mathfrak{m}\rangle} \xrightarrow{\mu} D_K^{\mathfrak{m}}/P_K^{\mathfrak{m}}, \qquad \vec{\alpha} \xmapsto{\mu} \mu(\vec{\alpha}) = \Lambda(\vec{\alpha}) \text{ mód } P_K^{\mathfrak{m}} = \mathfrak{a}_{\vec{\alpha}} \text{ mód } P_K^{\mathfrak{m}}$$

y $\operatorname{núc}\mu = J_K^{\mathfrak{m}}K^* \cap J_K^{\langle \mathfrak{m}\rangle}$ puesto que de la expresión $\Lambda(\vec{\alpha}) = \prod_{\mathfrak{p}\nmid\infty} \mathfrak{p}^{v_{\mathfrak{p}}(\alpha_{\mathfrak{p}})} = (a) = \prod_{\mathfrak{p}\nmid\infty} \mathfrak{p}^{v_{\mathfrak{p}}(a)} \in P_K^{\mathfrak{m}}$ se sigue que $\alpha_{\mathfrak{p}} a^{-1} \equiv 1 \text{ mód } \mathfrak{p}^{n_{\mathfrak{p}}}$ para toda $\mathfrak{p}$ y por lo tanto tenemos el isomorfismo buscado. □

Sea ahora K un campo numérico. Sea $\mathfrak{m}$ un módulus de K tal que L está contenido en el campo de clases módulus $\mathfrak{m}$, $L \subseteq K^{\mathfrak{m}}$ esto es, $C_K^{\mathfrak{m}} \subseteq \mathcal{N}_L = \mathrm{N}_{L/K} C_L$.

Se tiene que si $\mathfrak{p} \nmid \mathfrak{m}$ entonces $\mathfrak{p}$ es no ramificado y por tanto se obtiene un homomorfismo

$$\left(\frac{L/K}{\phantom{\mathfrak{a}}}\right)\colon D_K^{\mathfrak{m}} \longrightarrow \mathrm{Gal}(L/K)$$

dado por $\left(\frac{L/K}{\mathfrak{a}}\right) = \prod\limits_{\substack{\mathfrak{p}\nmid\mathfrak{m}\\ \mathfrak{p}\nmid\infty}} \left(\frac{L/K}{\mathfrak{p}}\right)^{a_{\mathfrak{p}}}$ donde $\mathfrak{a} = \prod_{\mathfrak{p}} \mathfrak{p}^{a_{\mathfrak{p}}}$ y $\left(\frac{L/K}{\mathfrak{p}}\right)$ es el símbolo de Artin en $\mathfrak{p}$.

Se tiene que si $\mathfrak{p}$ es un ideal primo y $\pi_{\mathfrak{p}}$ es un elemento primo de $K_{\mathfrak{p}}$, entonces $\left(\frac{L/K}{\mathfrak{p}}\right) = \left(\lceil \pi_{\mathfrak{p}} \rceil_{\mathfrak{p}}, L/K\right) = \psi_{L/K}\left(\lceil \pi_{\mathfrak{p}} \rceil_{\mathfrak{p}}\right)$ puesto que ambos son el automorfismo de Frobenius correspondiente a $\mathfrak{p}$.

Teorema 7.4.5 (Reciprocidad vía ideales). *Sea L/K una extensión abeliana finita de campos numéricos y se $\mathfrak{m}$ un módulus de de definición de L/K, esto es, $L \subseteq K^{\mathfrak{m}}$. Entonces el símbolo de Artin induce un epimorfismo*

$$\left(\frac{L/K}{\phantom{\mathfrak{a}}}\right)\colon D_K^{\mathfrak{m}}/P_K^{\mathfrak{m}} \longrightarrow \mathrm{Gal}(L/K)$$

el cual tiene núcleo $H_K^{\mathfrak{m}}/P_K^{\mathfrak{m}}$ *donde* $H_K^{\mathfrak{m}} = (\mathrm{N}_{L/K}\, D_L^{\mathfrak{m}})P_K^{\mathfrak{m}}$ *donde* $D_L^{\mathfrak{m}}$ *son los ideales fraccionarios de* D_L *primos relativos a* $\mathfrak{m}$. *Por tanto* $D_K^{\mathfrak{m}}/H_K^{\mathfrak{m}} \cong \mathrm{Gal}(L/K)$.

Más aún, se tiene un diagrama conmutativo cuyas filas son exactas

$$\begin{array}{ccccccccc} 1 & \longrightarrow & \mathrm{N}_{L/K}\, C_L & \longrightarrow & C_K & \xrightarrow{(\ ,L/K)} & \mathrm{Gal}(L/K) & \longrightarrow & 1 \\ & & \downarrow{\scriptstyle \Lambda_{\mathfrak{m}}} & & \downarrow{\scriptstyle \Lambda_{\mathfrak{m}}} & & \downarrow{\scriptstyle \mathrm{Id}} & & \\ 1 & \longrightarrow & H_K^{\mathfrak{m}}/P_K^{\mathfrak{m}} & \longrightarrow & D_K^{\mathfrak{m}}/P_K^{\mathfrak{m}} & \xrightarrow{\left(\frac{L/K}{}\right)} & \mathrm{Gal}(L/K) & \longrightarrow & 1 \end{array}$$

donde $\Lambda_{\mathfrak{m}}$ *es el mapeo inducido por* Λ *en el Teorema* 7.4.4.

Demostración. El isomorfismo $\Lambda_{\mathfrak{m}} \colon C_K/C_K^{\mathfrak{m}} \longrightarrow D_K^{\mathfrak{m}}/P_K^{\mathfrak{m}}$ da lugar a un diagrama conmutativo

$$\begin{array}{ccc} C_K/C_K^{\mathfrak{m}} & \xrightarrow{(\_,L/K)} & \mathrm{Gal}(L/K) \\ {\scriptstyle \Lambda_{\mathfrak{m}}}\downarrow{\scriptstyle \cong} & & \downarrow{\scriptstyle \mathrm{Id}} \\ D_K^{\mathfrak{m}}/P_K^{\mathfrak{m}} & \xrightarrow[f]{} & \mathrm{Gal}(L/K) \end{array}$$

donde f es el homomorfismo que hace conmutativo el diagrama, es decir $f = (\_, L/K) \circ \Lambda_m^{-1}$.

Veremos que f está dado por el símbolo de Artin.

Como se vio anteriormente, cada clase $C_K/C_K^{\mathfrak{m}}$ está representado por un idèle en $J_K^{\langle \mathfrak{m} \rangle} = \{\vec{\alpha} \in J_K \mid \alpha_{\mathfrak{p}} = 1 \text{ para } \mathfrak{p}|\mathfrak{m}\}$. En particular el grupo $C_K/C_K^{\mathfrak{m}}$ está generado por las clases de los idèles $\lceil \pi_{\mathfrak{p}} \rceil_{\mathfrak{p}}$ donde $\mathfrak{p}$ es un primo finito que no divide a $\mathfrak{m}$ y $\pi_{\mathfrak{p}}$ es un elemento primo de $K_{\mathfrak{p}}$.

Sea $c \in C_K/C_K^{\mathfrak{m}}$ la clase de $\lceil \pi_{\mathfrak{p}} \rceil_{\mathfrak{p}}$. Entonces $\Lambda_{\mathfrak{m}}(c) = \mathfrak{p} \bmod P_K^{\mathfrak{m}}$ y $f(\Lambda_{\mathfrak{m}}(c)) = (c, L/K) = \left(\lceil \pi_{\mathfrak{p}} \rceil_{\mathfrak{p}}, L/K\right) = \left(\dfrac{L/K}{\mathfrak{p}}\right)$. Por lo tanto f es inducido por el símbolo de Artin y $\left(\dfrac{L/K}{}\right) \colon D_K^{\mathfrak{m}} \to \mathrm{Gal}(L/K)$ es un epimorfismo.

Queda por probar que la imagen de $\mathrm{N}_{L/K}\, C_L$ bajo $\Lambda_{\mathfrak{m}} \colon C_K \to D_K^{\mathfrak{m}}/P_K^{\mathfrak{m}}$ es el grupo $H_K^{\mathfrak{m}}/P_K^{\mathfrak{m}}$ pues esta imagen corresponde a $\mathrm{núc}\, f = \mathrm{núc} \left(\dfrac{L/K}{}\right)$. Más precisamente,

$$\begin{array}{ccccccccc} 1 & \longrightarrow & \mathrm{N}_{L/K}\, C_L & \xrightarrow{i} & C_K & \xrightarrow{(\_,L/K)} & \mathrm{Gal}(L/K) & \longrightarrow & 1 \\ & & {\scriptstyle \Lambda_{\mathfrak{m}}}\downarrow & & \downarrow{\scriptstyle \Lambda_{\mathfrak{m}}} & & \downarrow{\scriptstyle \mathrm{Id}} & & \\ 1 & \longrightarrow & B & \xrightarrow{\psi} & D_K^{\mathfrak{m}}/P_K^{\mathfrak{m}} & \xrightarrow{\varphi} & \mathrm{Gal}(L/K) & \longrightarrow & 1 \end{array}$$

por lo que $\mathrm{núc}\, \varphi = B = \mathrm{im}\, \psi = \mathrm{im}\, \Lambda_{\mathfrak{m}}$.

Definimos $J_L^{\langle\mathfrak{m}\rangle} = \{\vec{\alpha} \in J_L \mid \alpha_{\mathfrak{P}} = 1 \text{ para } \mathfrak{P}|\mathfrak{m}\}$ y se tiene que $J_L = J_L^{\langle\mathfrak{m}\rangle} J_L^{\mathfrak{m}} L^*$. Por lo tanto, ya que $\mathrm{N}_{L/K} J_L^{\mathfrak{m}} \subseteq J_K^{\mathfrak{m}}$ y que $\mathrm{N}_{L/K} L^* \subseteq K^*$, se tiene

$$\frac{\mathrm{N}_{L/K} C_L}{C_K^{\mathfrak{m}}} = \frac{\mathrm{N}_{L/K}(J_L)K^*}{J_K^{\mathfrak{m}} K^*} = \frac{(\mathrm{N}_{L/K}(J_L^{\langle\mathfrak{m}\rangle}))J_K^{\mathfrak{m}} K^*}{J_K^{\mathfrak{m}} K^*}.$$

El isomorfismo

$$\Lambda_{\mathfrak{m}} \colon \frac{C_K}{C_K^{\mathfrak{m}}} \cong \frac{J_K^{\langle\mathfrak{m}\rangle} J_K^{\mathfrak{m}} K^*}{J_K^{\mathfrak{m}} K^*} \xrightarrow{\cong} \frac{D_K^{\mathfrak{m}}}{P_K^{\mathfrak{m}}}$$

asigna a la clase $\vec{\alpha} \in J_K^{\langle\mathfrak{m}\rangle}$ la clase del ideal $\Lambda(\vec{\alpha}) = \mathfrak{a}_{\vec{\alpha}} = \prod_{\mathfrak{p}\nmid\infty} \mathfrak{p}^{v_{\mathfrak{p}}(\alpha_{\mathfrak{p}})} \in D_K^{\mathfrak{m}}$.

Los elementos de $\frac{\mathrm{N}_{L/K} C_L}{C_K^{\mathfrak{m}}}$ son las clases representadas por la norma de idèles $\mathrm{N}_{L/K} J_L^{\langle\mathfrak{m}\rangle}$ en $J_K^{\langle\mathfrak{m}\rangle}$. Por tanto son mapeados precisamente sobre las clases de normas de ideales $\mathrm{N}_{L/K} D_L^{\mathfrak{m}}$ en $D_K^{\mathfrak{m}}$ por lo que

$$\Lambda_{\mathfrak{m}}\Big(\frac{\mathrm{N}_{L/K} C_L}{C_K^{\mathfrak{m}}}\Big) = \frac{(\mathrm{N}_{L/K} D_L^{\mathfrak{m}})P_K^{\mathfrak{m}}}{P_K^{\mathfrak{m}}} = \frac{H_K^{\mathfrak{m}}}{P_K^{\mathfrak{m}}}. \qquad \square$$

Corolario 7.4.6. *El símbolo de Artin* $\left(\frac{L/K}{\mathfrak{a}}\right)$, $\mathfrak{a} \in D_K^{\mathfrak{m}}$ *depende únicamente de la clase* $\mathfrak{a}$ mód $P_K^{\mathfrak{m}}$ *y da lugar a un isomorfismo en campos numéricos*

$$\left(\frac{L/K}{\ }\right) \colon \frac{D_K^{\mathfrak{m}}}{H_K^{\mathfrak{m}}} \xrightarrow{\cong} \mathrm{Gal}(L/K). \qquad \square$$

Observación 7.4.7. El Teorema 7.4.5 pone en evidencia que, a diferencia con el grupo de clases de idèles, en donde para cada extensión abeliana finita L/K correspondía un único subgrupo de C_K, a saber, $\mathrm{N}_{L/K} C_L$, cuando usamos ideales, para cada módulus $\mathfrak{m}$ tal que $L \subseteq K^{\mathfrak{m}}$, nos corresponde un grupo $H_K^{\mathfrak{m}}$ y por tanto no tenemos unicidad.

Definición 7.4.8. El grupo $H_K^{\mathfrak{m}} = \mathrm{N}_{L/K}(D_K^{\mathfrak{m}}) \cdot P_K^{\mathfrak{m}}$ se llama el *grupo de ideales declarado módulo* $\mathfrak{m}$ correspondiente a L/K.

Como consecuencia del Teorema de existencia del TCCG ($L \longleftrightarrow \mathcal{N}_L = \mathrm{N}_{L/K} C_L$), se sigue que el mapeo $L \longmapsto H_K^{\mathfrak{m}}$ da lugar a una correspondencia biyectiva entre los campos de clases de rayos módulo $\mathfrak{m}$ y los subgrupos de $D_K^{\mathfrak{m}}$ que contienen a $P_K^{\mathfrak{m}}$: $P_K^{\mathfrak{m}} \subseteq H_K^{\mathfrak{m}} \subseteq D_K^{\mathfrak{m}}$ en campos numéricos.

El siguiente teorema establece que la descomposición de un primo $\mathfrak{p}$ no ramificado en L, se puede leer directamente del grupo de ideales $H_K^{\mathfrak{m}}$ que determinan a L.

Teorema 7.4.9 (Ley de descomposición de primos). *Sea L/K una extensión abeliana de grado n de campos numéricos y sea $\mathfrak{p} \in \mathbb{P}_K$ un ideal primo no ramificado en L. Sea $\mathfrak{m}$ un módulus de definición de L, esto es, $L \subseteq K^{\mathfrak{m}}$, el*

cual no es divisible por $\mathfrak{p}$ *(por ejemplo, se puede tomar como* $\mathfrak{m}$ *al conductor) y sea* $H_K^{\mathfrak{m}}$ *el grupo de ideales correspondiente a* L.

Si f *es el orden de* $\mathfrak{p}$ mód $H_K^{\mathfrak{m}}$ *en* $D_K^{\mathfrak{m}}/H_K^{\mathfrak{m}}$, *esto es,* f *es el mínimo número natural tal que* $\mathfrak{p}^f \in H_K^{\mathfrak{m}}$, *entonces* $\mathfrak{p}$ *se descompone en un producto*

$$\mathfrak{p} = \mathfrak{P}_1 \cdots \mathfrak{P}_h$$

de $h = n/f$ *primos distintos* $\mathfrak{P}_1, \ldots, \mathfrak{P}_h$ *de grado* f *sobre* $\mathfrak{p}$, *donde se tiene* $f = [\mathcal{O}_L/\mathfrak{P}_i : \mathcal{O}_K/\mathfrak{p}]$.

Demostración. Sea $\mathfrak{p} = \mathfrak{P}_1 \cdots \mathfrak{P}_h$ la descomposición de $\mathfrak{p}$ en L. Puesto que $\mathfrak{p}$ es no ramificada, los $\mathfrak{P}_i$ son distintos y de grado igual a f', donde f' es el orden del automorfismo de Frobenius $\mathrm{Fr}_{\mathfrak{p}} = \left(\dfrac{L/K}{\mathfrak{p}}\right)$. Puesto que $D_K^{\mathfrak{m}}/H_K^{\mathfrak{m}} \cong \mathrm{Gal}(L/K)$, f' es el orden de $\mathfrak{p}$ mód $H_K^{\mathfrak{m}}$ en $D_K^{\mathfrak{m}}/H_K^{\mathfrak{m}}$. □

Corolario 7.4.10. *Si* $\mathfrak{p}$ *es no ramificado en* L/K, *entonces* $\mathfrak{p}$ *se descompone totalmente en* $L/K \iff \mathfrak{p} \in H_K^{\mathfrak{m}}$ *(es decir,* $\iff f = 1$*).* □

Corolario 7.4.11. *Sea* L/K *es una extensión abeliana finita de campos numéricos. Entonces hay una infinidad de lugares de* K *totalmente descompuestos en* L. □

Proposición 7.4.12. *Sea* K *un campo numérico. Sea* K_H *el campo de clase de Hilbert. Entonces* $K_H = K^1$ *es el campo de clases de rayos módulo* 1. *Entonces* $\mathfrak{p}$ *se descompone totalmente en* $K_H/K \iff \mathfrak{p}$ *es principal.*

Demostración. En este caso tenemos $C_K/C_K^1 \cong I_K = D_K^1/P_K^1 \underset{\mathfrak{m}=1}{\overset{\cong}{\uparrow}} D_K^{\mathfrak{m}}/H_K^{\mathfrak{m}}$, por lo que $H^1 = P_K$, es decir $D_K = D_K^1$ y $P_K = P_K^1$. Por tanto $\mathfrak{p}$ se descompone totalmente $\iff \mathfrak{p} \in P_K \iff \mathfrak{p}$ es principal. □

Finalmente tenemos el siguiente resultado, conjeturado por Hilbert y cuya demostración es complicada. Se reduce a probar que el mapeo de transferencia $\mathrm{Ver}\colon G/G' \longrightarrow G'/G''$ es el mapeo trivial.

Teorema 7.4.13 (Teorema del ideal principal). *Todo ideal* $\mathfrak{a}$ *de* K *se hace principal en el campo de clase de Hilbert.*

Demostración. [79]. □

Definición 7.4.14 (Definición 7.1.20). Sea K un campo numérico. El *campo de clase de Hilbert extendido* K_{H^+} es la máxima extensión abeliana de K no ramificada en ningún primo finito.

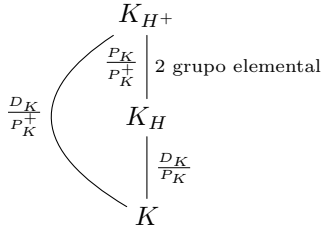
Se tiene que K_{H^+} es el campo de clase de rayos de $\mathfrak{m} = \prod_{\substack{\mathfrak{p} \text{ es real} \\ \mathfrak{p} \in \mathbb{P}_K}} \mathfrak{p}$. En particular $\mathfrak{m}_f = 1$, $\mathfrak{m}_\infty = \infty = \prod_{\mathfrak{p} \text{ real}} \mathfrak{p}$.

Ahora, $D_K^{\mathfrak{m}} = D_K^1 = D_K$ y $P_K^{\mathfrak{m}} = \{(\alpha) \in P_K \mid \alpha \text{ es totalmente positivo}\} = P_K^\infty = P_K^+$. Así $P_K^+ \subseteq P_K \subseteq D_K$ y

$$\mathrm{Gal}(K_{H^+}/K) \cong D_K/P_K^+ \twoheadrightarrow \mathrm{Gal}(K_H/K) \cong D_K/P_K = I_K.$$

y la siguiente sucesión es exacta

$$1 \to \frac{P_K}{P_K^+} \to \frac{D_K}{P_K^+} \to \frac{D_K}{P_K} \to 1$$



Notemos que si r es el número de lugares reales en K, entonces P_K/P_K^+ es un subgrupo del 2–grupo elemental C_2^r y, por supuesto, la contención puede ser propia.

Proposición 7.4.15. *Para K un campo numérico, sea K_{H^+} el campo de clase de Hilbert extendido. Entonces $\mathfrak{p} \in \mathbb{P}_K$, $\mathfrak{p}$ finito, se descompone totalmente en K_{H^+} si y solamente si $\mathfrak{p}$ es principal generado por un elemento totalmente positivo.*

Demostración. El campo K_{H^+} corresponde a $C_K^{1^+}$, donde $1^+ = \prod_{\mathfrak{p} \text{ real}} \mathfrak{p}$ y se tiene $C_K/C_K^{1^+} \cong D_K/P_K^+$. Esto implica que $H^{1^+} = P_K^{1^+} = P_K^+$. Por tanto $\mathfrak{p}$ se descompone totalmente $\iff \mathfrak{p} \in P_K^+ \iff \mathfrak{p}$ es principal generado por un elemento totalmente positivo. □

Observación 7.4.16. Notemos que K_{H^+}/K es una extensión finita a pesar de que permitimos a los primos infinitos ramificarse. Esto no se cumple para los primos finitos. Por ejemplo, se tiene que

$$\bigcup_{n=1}^{\infty} \mathbb{Q}(\zeta_{p^n})^+ = \mathbb{Q}(\zeta_{p^\infty})^+$$

es una extensión abeliana infinita de $\mathbb{Q}$ en la cual solamente el primo p se ramifica.

7.5. Sobre la extensión K_{H^+}/K_H

En esta subsección profundizamos más sobre la extensión K_{H^+}/K_H.

Observación 7.5.1. Existen campos numéricos K tales que $[K_{H^+} : K_H] = 2^s$ con $s > 1$. Dos trabajos en donde se discuten problemas de densidad relacionados con este fenómeno son [34, 66].

Ejemplos 7.5.2. Con respecto a la Observación 7.5.1, usamos el programa Sage para hacer los cálculos de los ejemplos proporcionados en [34, 66].

(1) Sea $K = \mathbb{Q}(\alpha)$, donde $\mathrm{Irr}(x, \alpha, \mathbb{Q}) = x^5 - 2x^4 - 32x^3 + 41x^2 + 220x - 289$. El discriminante de K es $\delta_K = 405,673,292,473$. El grupo de clases extendido de K es $I_K^+ \cong C_4 \times C_4 \times C_2 \times C_2$ y por tanto $\mathrm{Gal}(K_{H^+}/K) \cong C_4 \times C_4 \times C_2 \times C_2$. El grupo de clase de K es $I_K \cong C_2 \times C_2$ y en particular $\mathrm{Gal}(K_H/K) \cong C_2 \times C_2$. Se sigue que

$$\mathrm{Gal}(K_{H^+}/K_H) \cong C_2 \times C_2 \times C_2 \times C_2 = C_2^4.$$

(2) Sea $K = \mathbb{Q}(\beta)$ donde $\mathrm{Irr}(x, \beta, \mathbb{Q}) = x^5 - x^4 - 21x^3 - 7x^2 + 68x + 60$. El discriminante de K es $\delta_K = 52,315,684$. El grupo de clase extendido de K es $I_K^+ \cong C_4 \times C_2 \times C_2$ y el grupo de clase de K es $I_K \cong C_2$. Entonces

$$\mathrm{Gal}(K_{H^+}/K) \cong C_4 \times C_2 \times C_2; \quad \mathrm{Gal}(K_H/K) \cong C_2;$$
$$\mathrm{Gal}(K_{H^+}/K_H) \cong C_2 \times C_2 \times C_2 = C_2^3.$$

(3) Sea $K = \mathbb{Q}(\gamma)$ donde $\mathrm{Irr}(x, \gamma, \mathbb{Q}) = x^5 - 2x^4 - 6x^3 + 8x^2 + 8x + 1$. Entonces

$$\delta_K = 638,597; \quad \mathrm{Gal}(K_{H^+}/K) \cong C_2 \times C_2; \quad \mathrm{Gal}(K_H/K) \cong \{1\};$$
$$\mathrm{Gal}(K_{H^+}/K_H) \cong C_2 \times C_2 = C_2^2.$$

Los siguientes dos ejemplos, satisfacen, en ambos casos, que K es una extensión cúbica abeliana de $\mathbb{Q}$ (por supuesto con grupo de Galois, $\mathrm{Gal}(K/\mathbb{Q}) \cong C_3$).

(4) Sea $f(x) = x^3 - 237x + 316 \in \mathbb{Z}[x]$. Entonces, si K es el campo de descomposición de $f(x)$ sobre $\mathbb{Q}$, entonces $K/\mathbb{Q}$ es abeliana y $\mathrm{Gal}(K/\mathbb{Q}) \cong C_3$. Se tiene

$$\mathrm{Gal}(K_H/K) \cong C_2 \oplus C_6$$

y

$$\mathrm{Gal}(K_{H^+}/K) \cong C_4 \oplus C_{12}.$$

En particular,

$$\mathrm{Gal}(K_{H^+}/K_H) \cong C_2 \oplus C_2.$$

(5) Sea $g(x) = x^3 - x^2 - 234x + 729 \in \mathbb{Z}[x]$. Entonces, si K es el campo de descomposición de $g(x)$ sobre $\mathbb{Q}$, entonces $K/\mathbb{Q}$ es abeliana y $\mathrm{Gal}(K/\mathbb{Q}) \cong C_3$. Se tiene

$$\mathrm{Gal}(K_H/K) \cong C_2 \oplus C_6$$

y

$$\mathrm{Gal}(K_{H^+}/K) \cong C_4 \oplus C_{12}.$$

En particular,

$$\mathrm{Gal}(K_{H^+}/K_H) \cong C_2 \oplus C_2.$$

Sea K un campo numérico y sea J la conjugación compleja. Si $K/\mathbb{Q}$ es una extensión de Galois, se tiene que $J \in \mathrm{Gal}(K/\mathbb{Q})$ puesto que $J|_{\mathbb{Q}} = \mathrm{Id}$. Se tiene que $o(J|_K) = 1$ ó 2. Más aún, se tiene se tiene $J|_K = \mathrm{Id} \iff K \subseteq \mathbb{R}$.

Si $o(J|_K) = 2$, $\{1, J\}$ no necesariamente es normal en $G = \mathrm{Gal}(K/\mathbb{Q})$. Por ejemplo, si $K = \mathbb{Q}\big(\sqrt[3]{2}, \zeta_3\big)$, entonces $K/\mathbb{Q}$ es una extensión de Galois, $\mathrm{Gal}(K/\mathbb{Q}) = \langle \sigma, \tau \rangle \cong S_3$ donde se tiene que $\sigma\big(\sqrt[3]{2}\big) = \sqrt[3]{2}$ y $\sigma(\zeta_3) = \bar{\zeta}_3 = \zeta_3^2$; $\tau\big(\sqrt[3]{2}\big) = \zeta_3\sqrt[3]{2}$ y $\tau(\zeta_3) = \zeta_3$. Entonces $K^{\langle\sigma\rangle} = K \cap \mathbb{R} = \mathbb{Q}\big(\sqrt[3]{2}\big)$ y donde tenemos $\sigma = J|_K$. Además tenemos $K^{\langle\tau\rangle} = \mathbb{Q}(\zeta_3)$ y por tanto $\langle\tau\rangle \triangleleft G$, $\langle\sigma\rangle \not\triangleleft G$, $o(\tau) = 3$ y $o(\sigma) = 2$.

$$\begin{array}{ccc} \mathbb{Q}(\sqrt[3]{2}) & \xrightarrow{\ \sigma\ } & \mathbb{Q}(\sqrt[3]{2}, \zeta_3) \\ \Big| & & \Big| \tau \\ \mathbb{Q} & \longrightarrow & \mathbb{Q}(\zeta_3) \end{array}$$

En general, dado K, consideremos $L := KJ(K)$. Entonces J actúa en L pues $J(L) = J(K)J^2(K) = J(K)K = L$. Si $K \subseteq \mathbb{R}$ entonces $L = K$. Más generalmente, $L = K \iff J$ actúa en K, es decir si $J(K) = K$.

De esta forma, si $K/\mathbb{Q}$ es Galois, $J \in \mathrm{Gal}(K/\mathbb{Q})$ y $[K : K^J] = 1$ ó 2, $\mathrm{Gal}(K/K^J) = \langle J|_K \rangle$ y $K^J = K \cap \mathbb{R}$ pero K^J no necesariamente es normal sobre $\mathbb{Q}$.

En el caso en que $K/\mathbb{Q}$ no sea Galois, tenemos que $K^J = K \cap \mathbb{R}$ y $[K : K^J]$ es en general arbitrario. Por ejemplo, si $K = \mathbb{Q}\big(\zeta_n \sqrt[n]{2}\big)$, $n \in \mathbb{N}$ arbitrario, entonces $K^J = K \cap \mathbb{R} = \mathbb{Q}$ y $[K : K^J] = [K : \mathbb{Q}] = n$.

Como lo establecimos anteriormente, el campo de clase de Hilbert K_H de un campo numérico, corresponde al grupo de idèles

$$J_K^1 = \prod_{\mathfrak{p}} U_{\mathfrak{p}}, \quad C_K^1 = J_K^1 K^*/K^* \quad \text{y} \quad \mathrm{Gal}(K_H/K) \cong C_K/C_K^1 \cong J_K/J_K^1 K^*$$

y el campo de clase de Hilbert extendido K_{H^+} corresponde al grupo de idèles

$$J_K^{1+} = \prod_{\mathfrak{p} \text{ real}} U_{\mathfrak{p}}^{(1)} \times \prod_{\mathfrak{p} \text{ no real}} U_{\mathfrak{p}}, \quad C_K^{1+} = J_K^{1+} K^*/K^* \quad \text{y}$$

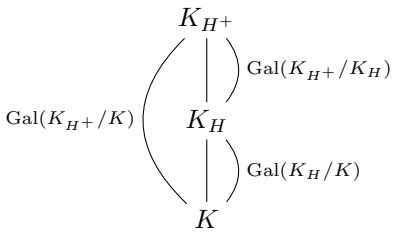
$$\mathrm{Gal}(K_{H^+}/K) \cong C_K/C_K^{1+} \cong J_K/J_K^{1+} K^*.$$

Se sigue que

$$\mathrm{Gal}(K_{H^+}/K_H) \cong (J_K^1 K^*)/(J_K^{1+} K^*).$$

Se tiene la siguiente sucesión exacta

$$\begin{array}{ccccccccc} 1 & \longrightarrow & \mathrm{Gal}(K_{H^+}/K_H) & \longrightarrow & \mathrm{Gal}(K_{H^+}/K) & \longrightarrow & \mathrm{Gal}(K_H/K) & \longrightarrow & 1. \\ & & \| \wr & & \| \wr & & \| \wr & & \\ & & (J_K^1 K^*)/(J_K^{1+} K^*) & & J_K/J_K^{1+} K^* & & J_K/J_K^1 K^* & & \end{array}$$



En resumen, tenemos

$$J_K^1 = \prod_{\mathfrak{p}} U_{\mathfrak{p}} = \prod_{\mathfrak{p} \text{ real}} \mathbb{R}^* \times \prod_{\mathfrak{p} \text{ complejo}} \mathbb{C}^* \times \prod_{\mathfrak{p} \nmid \infty} U_{\mathfrak{p}},$$

$$J_K^{1+} = \prod_{\mathfrak{p} \text{ real}} U_{\mathfrak{p}}^{(1)} \times \prod_{\mathfrak{p} \text{ no real}} U_{\mathfrak{p}} = \prod_{\mathfrak{p} \text{ real}} \mathbb{R}^+ \times \prod_{\mathfrak{p} \text{ complejo}} \mathbb{C}^* \times \prod_{\mathfrak{p} \nmid \infty} U_{\mathfrak{p}},$$

$$\frac{J_K^1}{J_K^{1+}} \cong \prod_{\mathfrak{p} \text{ real}} \frac{\mathbb{R}^*}{\mathbb{R}^+} \cong C_2^r,$$

donde r es el número de lugares reales de K.

Sea $\psi\colon J_K^1/J_K^{1+} \longrightarrow (J_K^1 K^*)/(J_K^{1+} K^*) \cong \mathrm{Gal}(K_{H^+}/K_H)$, el mapeo natural definido por x mód $J_K^{1+} \xrightarrow{\psi} x$ mód $J_K^{1+} K^*$. Entonces ψ es un epimorfismo y $\mathrm{núc}\,\psi = (J_K^1 \cap J_K^{1+} K^*)/J_K^{1+}$. Por tanto tenemos la siguiente sucesión exacta

$$1 \longrightarrow (J_K^1 \cap J_K^{1+} K^*)/J_K^{1+} \longrightarrow (J_K^1)/(J_K^{1+}) \cong C_2^r \longrightarrow \mathrm{Gal}(K_{H^+}/K_H) \longrightarrow 1.$$

Se sigue que $\mathrm{Gal}(K_{H^+}/K_H)$ es un 2–grupo elemental abeliano de rango menor o igual al número de lugares reales r de K.

Ejemplo 7.5.3. Primero notemos que $\mathbb{Q}_{H^+} = \mathbb{Q}_H = \mathbb{Q}$ debido al Teorema de Minkowski el cual establece que en cualquier extensión propia $K/\mathbb{Q}$ hay un primo finito ramificándose (ver Ejemplo 7.1.21).

Ahorca consideremos cualquier campo ciclotómico $K_n = \mathbb{Q}(\zeta_n)$, $n \in \mathbb{N}$ y sea $K_n^+ = \mathbb{Q}(\zeta_n)^+$ el subcampo real. Sean h_n y h_n^+ los números de clase de K_n y K_n^+ respectivamente. Entonces $h_n^+ | h_n$ (ver [136, Teorema 16.7.33]).

Si $h_n = 1$ entonces $h_n^+ = 1$. En este caso se tiene que el campo de clase de Hilbert de K_n es K_n y el de K_n^+ es K_n^+. Consideremos cualquier n tal que

$h_n = 1$ y que n tenga dos factores primos distintos (en ese caso K_n/K_n^+ es no ramificada en todos los primos finitos ([136, Teorema 5.3.2])).

Ahora bien, si $(K_n)_{H^+}$ y $(K_n^+)_{H^+}$ son los campos de clase de Hilbert extendidos de K_n y K_n^+ respectivamente, entonces, puesto que $(K_n^+)_{H^+}/K_n^+$ es abeliana y no ramificada en los primos finitos, se tiene que $(K_n^+)_{H^+} \subseteq (K_n)_{H^+} = (K_n)_H = K_n$ pues $h_n = 1$ y todos los lugares de K_n son complejos. Se sigue que $(K_n^+)_{H^+} = K_n$. En este caso, $r = \varphi(n)/2$ y $P_{K_n^+}/P_{K_n^+}^+ \cong C_2$ que es un subgrupo propio C_2^r para $r > 1$.

Hay 30 campos K_n con $h_n = 1$ ([136, Ejemplo 5.2.10]). Por ejemplo podemos tomar $n = 45$ y en este caso $r = 12$.

Observación 7.5.4. Sea $K/\mathbb{Q}$ una extensión de Galois. Se tiene que tanto K_H como K_{H^+} son extensiones de Galois sobre $\mathbb{Q}$. En efecto, consideremos σ un monomorfismo de K_H en una de sus cerraduras algebraicas, $\sigma\colon K_H \longrightarrow \bar{K}_H$. Se tiene que $\sigma|_K\colon K \longrightarrow \bar{K}$ y puesto que $K/\mathbb{Q}$ es una extensión normal, se tiene que $\sigma(K) = K$. Ahora bien, $\sigma(K_H)/\sigma(K) = K$ es una extensión no ramificada en ningún primo y es una extensión abeliana, se sigue que $K_H\sigma(K_H)/K$ es una extensión abeliana no ramificada, lo cual implica que $\sigma(K_H)K_H \subseteq K_H$, es decir, $\sigma(K_H) = K_H$ y $K_H/\mathbb{Q}$ es una extensión normal.

Un argumento totalmente análogo se aplica a $K_{H^+}/\mathbb{Q}$.

Observación 7.5.5. En un campo real $K/\mathbb{Q}$, $\mathfrak{p}_\infty = \infty$ puede ser ramificado en el caso de que K no sea totalmente real.

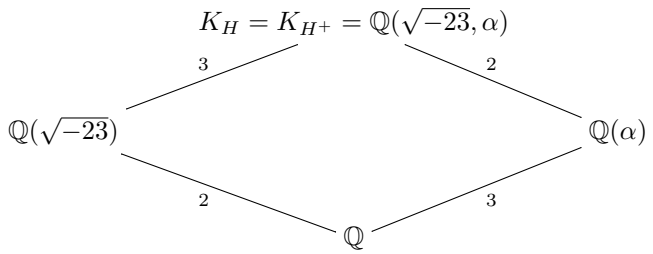
Ejemplo 7.5.6. Sea $K = \mathbb{Q}(\sqrt[3]{2}) \subseteq \mathbb{R}$. Se tiene que K tiene 2 encajes complejos:

$$\sigma_1\colon \sqrt[3]{2} \longrightarrow \sqrt[3]{2}; \quad \sigma_2\colon \sqrt[3]{2} \longrightarrow \zeta_3\sqrt[3]{2}; \quad \sigma_3\colon \sqrt[3]{2} \longrightarrow \zeta_3^2\sqrt[3]{2}.$$

Los encajes σ_2 y σ_3 son complejos y σ_1 es real y $\mathfrak{p}_\infty = \mathcal{P}_{\infty,1}\mathcal{P}_{\infty,2}^2$ donde $\mathcal{P}_{\infty,2}$ corresponde a la pareja de encajes $\{\sigma_2, \sigma_3\}$, $\bar{\sigma}_2 = \sigma_3$.

Observación 7.5.7. Aún en el caso de que la extensión $K/\mathbb{Q}$ sea de Galois, no necesariamente se tiene que $K_H = K_{H^+}^J$.

Ejemplo 7.5.8 (Ver [136, Ejemplo 5.2.10]). Sea $K = \mathbb{Q}(\sqrt{-23})$. Se tiene que $h_K = 3$ y los campos de clase de Hilbert y de Hilbert extendido coinciden pues $K \nsubseteq \mathbb{R}$. Se tiene $K_H = K_{H^+} = \mathbb{Q}(\sqrt{-23}, \alpha)$ donde $\alpha = \sqrt[3]{(25 + 3\sqrt{69})/2} + \sqrt[3]{(25 - 3\sqrt{69})/2}$. Sea $L = \mathbb{Q}(\alpha) \subseteq \mathbb{R}$. Se sigue que $L = K_{H^+}^J \neq K_H$.



8

Campos de géneros vía campos de clase

8.1. Campos de géneros

Los campos de géneros son tratados en [136, Subsección 6.4.1 y Capítulo 14].

Sea K un campo global y sea $\mathscr{K}/K$ una extensión finita y separable. Sea $\mathscr{K}_H$ el campo de clase de Hilbert de $\mathscr{K}$ (en alguna de sus versiones en el caso de campos de funciones).

El *campo de géneros* $\mathscr{K}_{\mathfrak{ge}}$ de $\mathscr{K}/K$ es la máxima extensión $\mathscr{K} \subseteq \mathscr{K}_{\mathfrak{ge}} \subseteq \mathscr{K}_H$ tal que $\mathscr{K}_{\mathfrak{ge}}$ es la composición $\mathscr{K}K_1$ con K_1/K abeliana. Se tiene que $\mathscr{K}_{\mathfrak{ge}}$ depende de la definición de $\mathscr{K}_H$ y de K. Se tiene que K_1 es la máxima extensión abeliana de K contenida en $\mathscr{K}_H$.

Equivalentemente, $\mathscr{K}_{\mathfrak{ge}} = \mathscr{K}K_1$ donde K_1 es la máxima extensión abeliana de K tal que $\mathscr{K}K_1/K$ es no ramificada y satisface las condiciones que se hayan considerado para $\mathscr{K}_H$ (por ejemplo, que los primos de un subconjunto no vacío $S \subseteq \mathbb{P}_K$, se descompongan totalmente en $\mathscr{K}K_1/K$).

En particular, si $\mathscr{K}/\mathbb{Q} = K$ es una extensión abeliana finita, entonces $K_1 = \mathscr{K}_{\mathfrak{ge}}$ y $\mathscr{K}_{\mathfrak{ge}}$ es la máxima extensión abeliana de $\mathbb{Q}$ tal que $\mathscr{K}_{\mathfrak{ge}}/\mathscr{K}$ es no ramificada.

Si $K = \mathbb{F}_q(T)$, $\mathscr{K}/K$ es una extensión abeliana finita y $\mathscr{K}_H$ se define como la máxima extensión abeliana no ramificada de $\mathscr{K}$ y tal que los primos de $S_\infty(\mathscr{K})$ se descomponen totalmente, donde $S_\infty(\mathscr{K}) := \{\mathfrak{p} \in \mathbb{P}_{\mathscr{K}} \mid \mathfrak{p} \cap \mathbb{F}_q(T) = \mathfrak{p}_\infty, \mathfrak{p}_\infty \text{ el polo de T}\}$, entonces $\mathscr{K}_{\mathfrak{ge}}$ es la máxima extensión abeliana de $K = \mathbb{F}_q(T)$ tal que $\mathscr{K}_{\mathfrak{ge}}/\mathscr{K}$ es no ramificada y $S_\infty(\mathscr{K})$ se descompone totalmente en $\mathscr{K}_{\mathfrak{ge}}$.

Teorema 8.1.1. *Sean $\mathscr{K}$ un campo global y $L/\mathscr{K}$ una extensión abeliana finita. Sea L_H el campo de clase con grupo de normas $\mathcal{N}\mathscr{K}^*/\mathscr{K}^*$, donde,*

$$\mathcal{N} = \prod_{\mathfrak{p}\ real} L_{\mathfrak{p}}^* \times \prod_{\mathfrak{p}\nmid\infty} U_{\mathfrak{p}} = L^1 \quad \textit{si } \mathscr{K} \textit{ es numérico y}$$

$$\mathcal{N} = J_{L,S}^1 = \prod_{\mathfrak{p}\in S} L_{\mathfrak{p}}^* \times \prod_{\mathfrak{p}\notin S} U_{\mathfrak{p}} = L_S^1 \quad \textit{si } \mathscr{K} \textit{ es es de funciones.}$$

Entonces $L_{\mathfrak{ge}}$ es la extensión abeliana de $\mathscr{K}$ con grupo de normas igual a $\mathrm{N}_{L/\mathscr{K}}\left(\mathcal{N}\mathscr{K}^*/\mathscr{K}^*\right)$.

Demostración. Puesto que $L/\mathscr{K}$ es abeliana, $L_{\mathfrak{ge}}$ es la máxima extensión abeliana de $\mathscr{K}$ contenida en L_H. El resultado es el contenido del Teorema 6.9.6. □

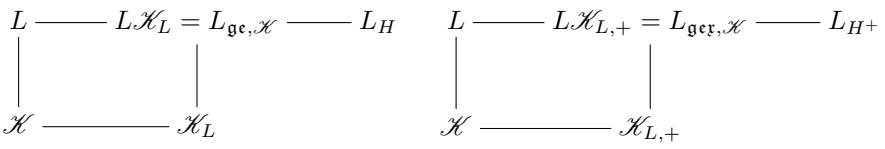
Más adelante, daremos una generalización del Teorema 8.1.1.

Durante este sección usaremos las siguientes definiciones y notaciones. Usaremos K para denotar el campo de funciones racionales $K = \mathbb{F}_q(T)$ o el campo de los números racionales $\mathbb{Q}$. El énfasis será en campos de funciones. El campo de clase de Hilbert L_H de una extensión L/K finita y separable, será la máxima extensión abeliana de L no ramificada y tal que los primos infinitos se descomponen totalmente. Entendemos por los primos infinitos los primos arquimedianos en el caso numérico y los lugares sobre $\mathfrak{p}_\infty$, el polo de T, en el caso de campos de funciones. En el caso numérico la última condición se satisface automáticamente al pedir que la extensión sea no ramificada.

Usaremos las notaciones de la Subsección 7.3.

Definición 8.1.2. Sea $L/\mathscr{K}$ una extensión finita y separable de campos globales. Se define el *campo de géneros $L_{\mathfrak{ge},\mathscr{K}}$ de L con respecto a $\mathscr{K}$* como la máxima extensión de L contenida en L_H tal que es de la forma $L\mathscr{K}_1$ donde $\mathscr{K}_1/\mathscr{K}$ es una extensión abeliana. Al máximo campo $\mathscr{K}_1$ que satisface $L_{\mathfrak{ge},\mathscr{K}} = L\mathscr{K}_1$ lo denotaremos por $\mathscr{K}_L$. En otras palabras, $\mathscr{K}_L$ es la máxima extensión abeliana de $\mathscr{K}$ tal que $L_{\mathfrak{ge},\mathscr{K}} = L\mathscr{K}_L$.

Definición 8.1.3. Sea $L/\mathscr{K}$ una extensión finita y separable de campos globales. El *campo de géneros extendido $L_{\mathfrak{gef},\mathscr{K}}$ de L con respecto a $\mathscr{K}$* se define como la máxima extensión de L contenida en L_{H^+} (ver Definición 7.3.21) que es de la forma $L\mathscr{K}_{1,+}$ donde $\mathscr{K}_{1,+}/\mathscr{K}$ es una extensión abeliana. Al máximo campo $\mathscr{K}_{1,+}$ que satisface $L_{\mathfrak{gef},\mathscr{K}} = L\mathscr{K}_{1,+}$ lo denotamos por $\mathscr{K}_{L,+}$. De esta forma, $\mathscr{K}_{L,+}$ es la máxima extensión abeliana de $\mathscr{K}$ tal que $L_{\mathfrak{gef},\mathscr{K}} = L\mathscr{K}_{L,+}$.



Observación 8.1.4. Cuando $L/\mathscr{K}$ es una extensión abeliana, $L_{\mathfrak{ge},\mathscr{K}}$ es la máxima extensión abeliana de $\mathscr{K}$ contenida en L_H y $L_{\mathfrak{ge}\mathfrak{x},\mathscr{K}}$ es la máxima extensión abeliana de $\mathscr{K}$ contenida en L_{H^+}.

Observación 8.1.5. Se tiene que $\mathscr{K}_L = (\mathscr{K}_L)_{\mathfrak{ge}}$ y $\mathscr{K}_{L,+} = (\mathscr{K}_{L,+})_{\mathfrak{ge}\mathfrak{x}}$.

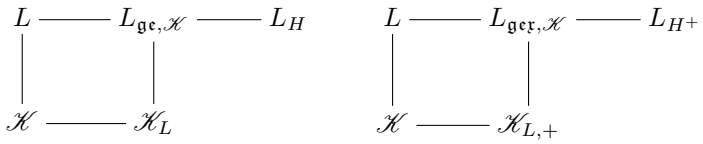
Observación 8.1.6. Cuando $\mathscr{K} = K = \mathbb{Q}$ o $\mathscr{K} = K = \mathbb{F}_q(T)$ y L/K es una extensión finita y separable, usaremos la notación $L_{\mathfrak{ge}} = L_{\mathfrak{ge},K}$ y $L_{\mathfrak{ge}\mathfrak{x}} = L_{\mathfrak{ge}\mathfrak{x},K}$.

El campo $L_{\mathfrak{ge}}$ se estudia extensivamente en [136, Capítulo 14] para el caso de campos de funciones y es introducido en [136, Subsección 6.4.1] en el caso de campos numéricos.

Teorema 8.1.7. *Sea $L/\mathscr{K}$ una extensión finita y separable de campos globales.*

(1) *El subgrupo de clases de idèles de $\mathscr{K}$ que corresponde a la extensión $\mathscr{K}_L$ de $\mathscr{K}$ es la imagen $\mathrm{N}_{L/\mathscr{K}}(U_L L^*/L^*)$ del subgrupo de clases de idèles $U_L L^*/L^*$ asociado a L_H.*
(2) *El subgrupo de clases de idèles de L que corresponde a la extensión abeliana $L_{\mathfrak{ge},\mathscr{K}}$ de L es el subgrupo $\mathrm{N}^{-1}_{L/\mathscr{K}}(\mathrm{N}_{L/\mathscr{K}}(U_L L^*/L^*)) \supseteq U_L L^*/L^*$ del subgrupo $U_L L^*/L^*$ asociado a L_H.*
(3) *El subgrupo de clases de idèles de $\mathscr{K}$ que corresponde a la extensión $\mathscr{K}_{L,+}$ de $\mathscr{K}$ es la imagen $\mathrm{N}_{L/\mathscr{K}}(U_L^+ L^*/L^*)$ del subgrupo de clases de idèles $U_L^+ L^*/L^*$ asociado a L_{H^+}.*
(4) *El subgrupo de clases de idèles de L que corresponde a la extensión abeliana $L_{\mathfrak{ge}\mathfrak{x},\mathscr{K}}$ de L es el subgrupo $\mathrm{N}^{-1}_{L/\mathscr{K}}(\mathrm{N}_{L/\mathscr{K}}(U_L^+ L^*/L^*)) \supseteq U_L^+ L^*/L^*$ del subgrupo $U_L^+ L^*/L^*$ asociado a L_{H^+}.*

Demostración. (1) y (3).



Se tiene que $U_L L^*/L^*$ es el subgrupo de clases de idèles que corresponde a L_H/L y $U_L^+ L^*/L^*$ a L_{H^+}/L. Entonces $\mathscr{K}_L$ es la máxima extensión de $\mathscr{K}$ contenida en L_H y $\mathscr{K}_{L,+}$ la respectiva en L_{H^+}. Por la Teorema 6.9.6 se sigue que el grupo de normas de $\mathscr{K}_L$ es $\mathrm{N}_{L/\mathscr{K}}(U_L L^*/L^*)$ y el de $\mathscr{K}_{L,+}$ es $\mathrm{N}_{L/\mathscr{K}}(U_L^+ L^*/L^*)$. Este es el contenido de (1) y (3) a nivel de subgrupos de idèles.

(2) y (4). Se tiene

$$\begin{array}{ccc} L & \text{---} & L\mathscr{K}_L = L_{\mathfrak{ge},\mathscr{K}} \\ | & & | \\ \mathscr{K} & \text{---} & \mathscr{K}_L \end{array} \qquad \begin{array}{ccc} L & \text{---} & L\mathscr{K}_{L,+} = L_{\mathfrak{ge}\mathfrak{x},\mathscr{K}} \\ | & & | \\ \mathscr{K} & \text{---} & \mathscr{K}_{L,+} \end{array}$$

Por el Teorema 6.7.21 se tiene que los diagramas

$$\begin{array}{ccc} C_L & \xrightarrow{\psi_{L_{\mathfrak{ge}}/L}} & \mathrm{Gal}(L_{\mathfrak{ge}}/L) \\ \downarrow{\scriptstyle \mathrm{N}_{L/\mathscr{K}}} & & \downarrow{\scriptstyle \mathrm{rest}} \\ C_K & \xrightarrow[\psi_{\mathscr{K}_L/\mathscr{K}}]{} & \mathrm{Gal}(\mathscr{K}_L/\mathscr{K}) \end{array} \qquad \begin{array}{ccc} C_L & \xrightarrow{\psi_{L_{\mathfrak{ge}\mathfrak{x}}/L}} & \mathrm{Gal}(L_{\mathfrak{ge}\mathfrak{x}}/L) \\ \downarrow{\scriptstyle \mathrm{N}_{L/\mathscr{K}}} & & \downarrow{\scriptstyle \mathrm{rest}} \\ C_K & \xrightarrow[\psi_{\mathscr{K}_{L,+}/\mathscr{K}}]{} & \mathrm{Gal}(\mathscr{K}_{L,+}/\mathscr{K}) \end{array}$$

son conmutativos. Entonces

$$\mathrm{rest}\,|_{\mathscr{K}_L} \circ \psi_{L_{\mathfrak{ge}}/L} = \psi_{\mathscr{K}_L/\mathscr{K}} \circ \mathrm{N}_{L/\mathscr{K}} \ \text{ y } \ \mathrm{rest}\,|_{\mathscr{K}_{L,+}} \circ \psi_{L_{\mathfrak{ge}\mathfrak{x}}/L} = \psi_{\mathscr{K}_{L,+}/\mathscr{K}} \circ \mathrm{N}_{L/\mathscr{K}}\,.$$

Como $\mathrm{Gal}(L_{\mathfrak{ge}}/L) \cong \mathrm{Gal}(\mathscr{K}_L/\mathscr{K}_L \cap L) \subseteq \mathrm{Gal}(\mathscr{K}_L/\mathscr{K})$ y $\mathrm{Gal}(L_{\mathfrak{ge}\mathfrak{x}}/L) \cong \mathrm{Gal}(\mathscr{K}_{L,+}/\mathscr{K}_{L,+} \cap L) \subseteq \mathrm{Gal}(\mathscr{K}_{L,+}/\mathscr{K})$, se tiene que $\mathrm{rest}\,|_{\mathscr{K}_L}$ y $\mathrm{rest}\,|_{\mathscr{K}_{L,+}}$ son mapeos inyectivos. Se sigue que

$$\begin{gathered} \vec{\alpha} \in \mathrm{núc}\,\psi_{L_{\mathfrak{ge}}/L} \iff \psi_{L_{\mathfrak{ge}}/L}(\vec{\alpha}) = \vec{1} \iff \\ \mathrm{rest}\,|_{\mathscr{K}_L} \circ \psi_{L_{\mathfrak{ge}}/L}(\vec{\alpha}) = \vec{1} = \psi_{\mathscr{K}_L/\mathscr{K}} \circ \mathrm{N}_{L/\mathscr{K}}(\vec{\alpha}) \iff \\ \mathrm{N}_{L/\mathscr{K}}(\vec{\alpha}) \in \mathrm{núc}\,\psi_{\mathscr{K}_L/\mathscr{K}} \iff \vec{\alpha} \in \mathrm{N}_{L/\mathscr{K}}^{-1}(\mathrm{núc}\,\psi_{\mathscr{K}_L/\mathscr{K}}) \end{gathered}$$

esto es,

$$\mathrm{núc}\,\psi_{L_{\mathfrak{ge}}/L} = \mathrm{N}_{L/\mathscr{K}}^{-1}(\mathrm{núc}\,\psi_{\mathscr{K}_L/\mathscr{K}}).$$

Similarmente $\mathrm{núc}\,\psi_{L_{\mathfrak{ge}\mathfrak{x}}/L} = \mathrm{N}_{L/\mathscr{K}}^{-1}(\mathrm{núc}\,\psi_{\mathscr{K}_{L,+}/\mathscr{K}})$.

De esta forma obtenemos que el subgrupo de clases de idèles correspondiente a $L_{\mathfrak{ge}}/L$ es $\mathrm{núc}\,\psi_{L_{\mathfrak{ge}}/L} = \mathrm{N}_{L/\mathscr{K}}^{-1}(\mathrm{núc}\,\psi_{\mathscr{K}_L/\mathscr{K}}) = \mathrm{N}_{L/\mathscr{K}}^{-1}(\mathrm{N}_{L/\mathscr{K}}(U_L L^*/L^*))$. Similarmente para $L_{\mathfrak{ge}\mathfrak{x}}/L$. □

Se tiene la generalización de [136, Corolario 14..3.4]..

Corolario 8.1.8. *Sea $L/\mathscr{K}$ una extensión cíclica de campos globales con $\mathrm{Gal}(L/\mathscr{K}) = G = \langle\sigma\rangle$. Sean $Cl_L \cong \mathrm{Gal}(L_H/L)$, $Cl_L^+ \cong \mathrm{Gal}(L_{H^+}/L)$. Sean los cocientes $\mathcal{G}_{L/\mathscr{K}} := \mathrm{Gal}(L_{\mathfrak{ge}}/L)$ y $\mathcal{G}_{L/\mathscr{K}}^+ := \mathrm{Gal}(L_{\mathfrak{ge}\mathfrak{x}}/L)$ los grupos de géneros y de géneros extendidos respectivamente. Entonces*

$$\mathcal{G}_{L/\mathscr{K}} \cong Cl_L/Cl_L^{\langle\sigma-1\rangle} \quad y \quad \mathcal{G}_{L/\mathscr{K}}^+ \cong Cl_L^+/(Cl_L^+)^{\langle\sigma-1\rangle}.$$

Demostración. Sea $\vec{\alpha} \in J_L$ tal que $\mathrm{N}_{L/\mathscr{K}}\,\vec{\alpha} \in \mathrm{N}_{L/\mathscr{K}}\,U_L\mathscr{K}^*$. Pongamos $\mathrm{N}_{L/\mathscr{K}}(\vec{\alpha}) = \mathrm{N}_{L/\mathscr{K}}(\vec{u}) \cdot x$ con $\vec{u} \in U_L$ y $x \in \mathscr{K}^*$. Se sigue que $x = \mathrm{N}_{L/\mathscr{K}}(\vec{\alpha}/\vec{u}) \in \mathscr{K}^* \cap \mathrm{N}_{L/\mathscr{K}}(J_L)$. Puesto que $L/\mathscr{K}$ es una extensión cíclica, por el principio local–global de Hasse, se sigue que x es una norma de L^*: $x = \mathrm{N}_{L/\mathscr{K}}(y)$. Entonces $\vec{x} = \mathrm{N}_{L/\mathscr{K}}(\vec{y}) = \mathrm{N}_{L/\mathscr{K}}(\vec{\alpha}/\vec{u})$, esto es, $\mathrm{N}_{L/\mathscr{K}}(\vec{\alpha}/\vec{y}\vec{u}) = \vec{1}$. Por el Teorema 90 de Hilbert aplicado a idèles (Teorema 6.3.5), existe $\vec{\beta} \in J_L$ tal que $\vec{\beta}^{(\sigma-1)} = \vec{\alpha}/\vec{y}\vec{u}$, es decir, $\vec{\alpha} = \vec{\beta}^{(\sigma-1)}\vec{y}\vec{u} \in J_L^{\langle\sigma-1\rangle}L^*U_L$. Se sigue que

$$\begin{aligned}\mathcal{G}_{L/\mathscr{K}} &\cong \frac{J_L/L^*}{\mathrm{N}_{L/\mathscr{K}}^{-1}(\mathrm{N}_{L/\mathscr{K}}((U_LL^*)/L^*))} \cong \frac{J_L}{J_L^{\langle\sigma-1\rangle}L^*U_L}\\ &\cong \frac{J_L/(U_LL^*)}{(J_L^{\langle\sigma-1\rangle}U_LL^*)/(U_LL^*)} \cong \frac{J_L/U_LL^*}{(J_L/U_LL^*)^{\langle\sigma-1\rangle}} =\cong \frac{Cl_L}{Cl_L^{\langle\sigma-1\rangle}}.\end{aligned}$$

Similarmente se tiene $\mathcal{G}^+_{L/\mathscr{K}} \cong Cl_L^+/(Cl_L^+)^{\langle\sigma-1\rangle}$. □

Si $E \subseteq K(\Lambda_M)$ para algún $M \in R_T$ en el caso de campos de funciones, o $E/\mathbb{Q}$ una extensión abeliana en el caso numérico, se tiene que $E_{\mathfrak{ge}}$ corresponde a L^+E donde, si X es el grupo de caracteres de Dirichlet asociado al campo E, L es el campo asociado a $Y = \prod_{P\in R_T^+} X_P$ y $L^+ = L\cap K(\Lambda_M)^+$ y similarmente en el caso de campos numéricos ([136, Capítulo 14]).

La pregunta natural es, ¿cual es campo $E_{\mathfrak{ge}_\mathfrak{x}}$?. Veremos que $E_{\mathfrak{ge}_\mathfrak{x}} = L$, es decir, $E_{\mathfrak{ge}_\mathfrak{x}}$ es el campo asociado a Y.

Para resolver este problema, primero determinaremos cual es el subgrupo de idèles de J_K que corresponde al campo de funciones ciclotómico $K(\Lambda_M)$ con $M \in R_T$. Sea $\mathcal{X}_M$ el subgrupo de idèles que corresponde a $K(\Lambda_M)$. Sea $R'_T = R_T \setminus \{P_1, \ldots, P_r\}$, $\pi = 1/T = \pi_\infty$ y $U_\infty = U_{\mathfrak{p}_\infty}$.

Definimos

$$\mathcal{X}_M = \prod_{i=1}^{r} U_{P_i}^{(\alpha_i)} \times \prod_{P\in R'_T} U_P \times [(\pi) \times U_\infty^{(1)}] \tag{8.1.1}$$

donde $M = P_1^{\alpha_1}\cdots P_r^{\alpha_r} \in R_T$.

Observación 8.1.9. Se tiene que $\mathcal{X}_NK^*/K^* \cong \mathcal{X}_N$.

En efecto, si $x \in \mathcal{X}_N \cap K^*$, entonces $x \in U_P$ para toda $P \in R_T$ por lo que $v_P(x) = 0$ para toda $P \in R_T$. Puesto que $\mathrm{gr}(x)_K = 0$, se sigue que $v_\infty(x) = 0$ lo cual implica que $x \in \mathbb{F}_q^*$. Puesto que $x \in (\pi) \times U_\infty^{(1)} = \mathrm{núc}\,\phi_\infty$, $x = 1$. Por tanto, $\frac{\mathcal{X}_NK^*}{K^*} \cong \frac{\mathcal{X}_N}{\mathbb{X}_N\cap K^*} \cong \mathcal{X}_N$.

D. Hayes probó (ver [160, Section 12.8.4, Theorem 12.8.5]) que si $U_T = \{\vec{\alpha} \in J_K \mid \alpha_{\mathfrak{p}_\infty} = 1 \text{ y } \alpha_P \in U_P \text{ para toda } P \in R_T^+\}$, entonces $U_T \cong G_T = \mathrm{Gal}(K_T/K)$ donde $K_T := \bigcup_{M\in R_T} K(\Lambda_M)$.

Proposición 8.1.10. *Sea $U' := \prod_{P\in R_T} U_P \times [(\pi)\times U_\infty^{(1)}]$. Entonces existe un epimorfismo $\psi_M\colon U' \longrightarrow \mathrm{Gal}(K(\Lambda_M)/K) := G_M$ con $\mathrm{núc}\,\psi_M = \mathcal{X}_M$ y por tanto, $U'/\mathcal{X}_M \cong G_M$.*

Demostración. Sea $\vec{\xi} \in U'$. Entonces $\xi_{P_i} \in U_{P_i} = \{\sum_{j=0}^{\infty} a_j P_i^j \mid a_j \in R_T/(P_i), a_0 \neq 0\}$, $1 \leq i \leq r$. Puesto que $K \subseteq K_{P_i}$ es denso, existe $Q_i \in R_T$ con $Q_i \equiv \xi_{P_i}$ mód $P_i^{\alpha_i}$. Por el Teorema Chino del Residuo existe $C \in R_T$ tal que $C \equiv Q_i$ mód $P_i^{\alpha_i}$, $1 \leq i \leq r$ y por tanto $C \equiv \xi_{P_i}$ mód $P_i^{\alpha_i}$, $1 \leq i \leq r$.

Ahora bien, si $C_1 \in R_T$ satisface $C_1 \equiv \xi_{P_i}$ mód $P_i^{\alpha_i}$, $1 \leq i \leq r$, entonces $P_i^{\alpha_i} | C - C_1$ para $1 \leq i \leq r$. Se sigue que $M | C - C_1$ y por tanto $C \in R_T$ es único módulo M. Por otro lado, $v_{P_i}(\xi_{P_i}) = 0$, entonces $P_i \nmid \xi_{P_i}$ de donde se tiene $\mathrm{mcd}(C, M) = 1$. De esta forma tenemos que C mód M define un elemento de G_M.

Dado $\sigma \in G_M$, existe $C \in R_T$ tal que $\sigma\lambda_M = \lambda_M^C$ donde λ_M es un generador de Λ_M. Sea $\vec{\xi} \in U'$ con $\xi_{P_i} = C$, $1 \leq i \leq r$ y $\xi_P = 1 = \xi_\infty$ para toda $P \in R_T'$. Por tanto $\vec{\xi} \mapsto C$ mód M y ψ_M es suprayectiva. Finalmente, $\mathrm{núc}\, \psi_M = \{\vec{\xi} \in U' \mid \xi_{P_i} \equiv 1 \text{ mód } P_i^{\alpha_i}, 1 \leq i \leq r\} = \mathcal{X}_M$ de donde se sigue el resultado. □

Probaremos que $U'/\mathcal{X}_M \cong J_K/\mathcal{X}_M K^*$. Tenemos la composición

$$U' \hookrightarrow J_K \twoheadrightarrow J_K/\mathcal{X}_M K^*, \qquad \mu$$

con $\mathrm{im}\, \mu = U'\mathcal{X}_M K^*/\mathcal{X}_M K^*$ y $\mathrm{núc}\, \mu = U' \cap \mathcal{X}_M K^*$.

Ahora bien, $\mathcal{X}_M \subseteq U'$ por lo que $\mathcal{X}_M \subseteq U' \cap \mathcal{X}_M K^*$. Recíprocamente, si $\vec{\xi} \in U' \cap \mathcal{X}_M K^*$, entonces las componentes de $\vec{\xi}$ están dadas por

$$\xi_P = a \cdot \beta_P, \quad P \in R_T, \quad \vec{\beta} \in \mathcal{X}_M, \quad a \in K^*,$$
$$\xi_\infty = a \cdot \beta_\infty, \quad \beta_\infty \in (\pi) \times U_\infty^{(1)}.$$

Puesto que $\xi_P, \beta_P \in U_P$ se tiene $v_P(\xi_P) = v_P(\beta_P) = 0$ para toda $P \in R_T$. Se sigue que $v_P(a) = 0$ para toda $P \in R_T$. Además, como $\mathrm{gr}\, a = 0$ entonces $v_\infty(a) = 0$ y por tanto $a \in \mathbb{F}_q^*$.

Ahora $\xi_\infty, \beta_\infty \in (\pi) \times U_\infty^{(1)} = \mathrm{núc}\, \phi_\infty$ por lo que $1 = \phi_\infty(\xi_\infty) = \phi_\infty(a)\phi_\infty(\beta_\infty) = \phi_\infty(a)$ de donde $a = 1$. Se sigue que $\vec{\xi} \in \mathcal{X}_M$. Por tanto $\mathrm{núc}\, \mu = \mathcal{X}_M$ y obtenemos una inyección $U'/\mathcal{X}_M \overset{\theta}{\hookrightarrow} J_K/\mathcal{X}_M K^*$.

Falta verificar la suprayectividad de θ, debemos probar $J_K = U'\mathcal{X}_M K^* = U'K^*$. Se tiene que U' corresponde a la máxima extensión no ramificada en ningún primo finito. Sea L/K esta extensión. Como $U_\infty^{(1)}$ corresponde al primer grupo de ramificación y por tanto corresponde a la ramificación salvaje de $\mathfrak{p}_\infty$, se sigue que en L/K hay a lo más un primo ramificado, este es moderadamente ramificado y es de grado 1 ($\mathfrak{p}_\infty$). Por [136, Proposición 10.4.1], L/K es una extensión de constantes.

Finalmente, puesto que $d = \mín\{n \in \mathbb{N} \mid \mathrm{gr}\, \vec{\alpha} = n, \vec{\alpha} \in U'\}$, entonces el campo de constantes de L es $\mathbb{F}_q$ y por tanto $L = K$. Se sigue que $C_K \cong U'$, esto es, $J_K/K^* \cong U'$ de donde obtenemos $J_K = K^*U'$.

Hemos probado

Proposición 8.1.11. *Sea $M = P_1^{\alpha_1} \cdots P_r^{\alpha_r} \in R_T$. Entonces el subgrupo de idèles de J_K que corresponde al campo de funciones ciclotómico $K(\Lambda_M)$ es el subgrupo $\mathcal{X}_N K^*$, donde*

$$\mathcal{X}_M = \prod_{i=1}^{r} U_{P_i}^{(\alpha_i)} \times \prod_{P \in R_T'} U_P \times [(\pi) \times U_\infty^{(1)}]$$

y por tanto el subgrupo de clases de idèles de C_K que corresponde a $K(\Lambda_M)$ es $\mathcal{X}_M K^*/K^* \cong \mathcal{X}_M$. □

Corolario 8.1.12. *El subgrupo de idèles correspondiente al campo $K(\Lambda_M)^+$ es $\mathcal{X}_M^+ K^*$ donde*

$$\mathcal{X}_M^+ = \prod_{i=1}^{r} U_{P_i}^{(\alpha_i)} \times \prod_{P \in R_T'} U_P \times K_\infty^*.$$

Demostración. Si L_1 el campo asociado a $\mathcal{X}_M^+$, el campo de constantes de L_1 es $\mathbb{F}_q$ por el argumento anterior y se tiene

$$\frac{\mathcal{X}_M^+}{\mathcal{X}_M} \cong \frac{K_\infty^*}{(\pi) \times U_\infty^{(1)}} \cong \mathbb{F}_q^*,$$

lo que implica que $[L : L_1] \leq q-1$. Además $\mathfrak{p}_\infty$ se descompone totalmente en L_1 y tiene índice de ramificación $q-1$ en L. Se sigue que $[L : L_1] = q-1$ y $L_1 = K(\Lambda_M)^+$. □

Proposición 8.1.13. *Sea $E \subseteq K(\Lambda_M)$. Si $\mathfrak{p}$ es un primo infinito en E, entonces $1/T$ es una norm de $E_\mathfrak{p}$, esto es, existe $x \in E_\mathfrak{p}$ tal que $\mathrm{N}_{E_\mathfrak{p}/k_\infty} x = 1/T$.*

Demostración. Puesto que $E \subseteq K(\Lambda_M)$ se tiene que $E \subseteq K_\infty(\sqrt[q-1]{-1/T})$ ([136, Proposición 9.3.20]). Por tanto $E_\mathfrak{p} = k_\infty(\sqrt[e]{-1/T})$ con $e | q-1$. Se sigue el resultado (Teorema 7.3.11).

Regresamos a nuestra discusión sobre $E_{\mathfrak{gcf}}$ para $E \subseteq K(\Lambda_M)$. Sea $\Lambda \subseteq J_E$ el subgrupo de idèles de E que corresponde a E_{H^+}, esto es, $\mathrm{N}_{E_{H^+}/E} C_{E_{H^+}} = E^* \Lambda / E^*$. Entonces, por definición, podemos tomar $\Lambda = U_E^+$. Por el Teorema 8.1.7, el subgrupo de clases de idèles de C_K que corresponde $K_{E,+} = E_{\mathfrak{gcf}}/K$ (esto es, como E/K es abeliana, $K_{E,+}$ corresponde a $E_{\mathfrak{gcf}}$) es precisamente $\mathrm{N}_{E/K}(U_E^+)K^*/K^* \cong \mathrm{N}_{E/K} U_E^+$ (pues $\mathrm{N}_{E/K}(U_E^+) \subseteq \prod_{P \in R_T} \times \big((\pi) \times U_\infty^{(1)}\big)$ y $K^* \cap \big(\prod_{P \in R_T} \times \big((\pi) \times U_\infty^{(1)}\big)\big) = \{1\}$).

Se tiene $U_E^+ = \prod_{\mathfrak{p}|\infty} \text{núc}\, \phi_{E_\mathfrak{p}} \times \prod_{\mathfrak{p} \nmid \infty} U_\mathfrak{p}$, donde denotamos $\infty = \mathfrak{p}_\infty$.

Se tiene que si $\mathfrak{p}$ no es ramificado, por lo que $\mathfrak{p} \nmid \infty$ y $\mathfrak{p} \nmid P_i$, $1 \leq i \leq r$, donde $M = P_1^{\alpha_1} \cdots P_r^{\alpha_r}$, entonces se tiene $\mathrm{N}_{E_\mathfrak{p}/K_P}(U_\mathfrak{p}) = U_P$, donde $\mathfrak{p} \cap K = P \in R_T^+$ (Teorema 3.4.9). Si $\mathfrak{p} | P_i$ para algún $1 \leq i \leq r$, se tiene $[U_{P_i} : \mathrm{N}_{E_\mathfrak{p}/K_{P_i}} U_\mathfrak{p}] = e_{E_\mathfrak{p}/K_{P_i}}(\mathfrak{p}|P_i) = \Phi(P_i^{\alpha_i}) = q^{(\alpha_i - 1)d_i}(q-1)$ donde $d_i = \mathrm{gr}\, P_i$.

Ahora bien, puesto que $E \subseteq K(\Lambda_M)$ obtenemos que $E_{\mathfrak{g}\mathfrak{k}} \subseteq K(\Lambda_M)$ y el grupo de J_E correspondiente a $E_{\mathfrak{g}\mathfrak{k}}$ es E^*U_E y por tanto el grupo de C_K que corresponde a $E_{\mathfrak{g}\mathfrak{k}}$ es $\mathrm{N}_{E/K}(U_E)K^*/K^*$. Se tiene

$$\mathrm{N}_{E/K}\, U_E = \prod_{\mathfrak{p}|\mathfrak{p}_\infty} \mathrm{N}_{E_\mathfrak{p}/K_\infty}\, E_\mathfrak{p}^* \times \prod_{P\in R_T}\prod_{\mathfrak{p}|P} \mathrm{N}_{E_\mathfrak{p}/K_P}\, U_\mathfrak{p}.$$

También se tiene

$$N_{E/K}U_E^+ = \prod_{\mathfrak{p}|\mathfrak{p}_\infty} \mathrm{N}_{E_\mathfrak{p}/K_\infty}(\mathrm{núc}\,\phi_{E_\mathfrak{p}}) \times \prod_{P\in R_T}\prod_{\mathfrak{p}|P} \mathrm{N}_{E_\mathfrak{p}/K_P}\, U_\mathfrak{p}.$$

Si ponemos $R_T' := R_T \setminus \{P_1,\dots,P_r\}$, entonces

$$\Big(\prod_{P\in R_T'} U_P \times \prod_{i=1}^{r} U_{P_i}^{(\alpha_i)}\Big)K^* \subseteq \Big(\prod_{P\in R_T}\prod_{\mathfrak{p}|P} \mathrm{N}_{E_\mathfrak{p}/K_P}\, U_\mathfrak{p}\Big)K^*. \tag{8.1.2}$$

Sea $\mathfrak{p}$ un primo infinito en E. Como $E_\mathfrak{p}/K_\infty$ es totalmente ramificado, se tiene $\mathrm{N}_{E_\mathfrak{p}/K_\infty} E_\mathfrak{p}^* \supseteq (\pi_\infty) \times U_P^{(n_0)}$ para algún $n_0 \in \mathbb{N}\cup\{0\}$ (Teorema 5.8.62). Notemos que, como está contenido en un campo de funciones ciclotómico, $E_\mathfrak{p} \subseteq K_\infty(\sqrt[q-1]{-1/T})$ y por tanto $1/T$ es una norma de $E_\mathfrak{p}$ (Corolario 7.3.12).

Se tiene $E_\mathfrak{p}^* = (\pi_{E_\mathfrak{p}}) \times \mathbb{F}_q^* \times U_\mathfrak{p}^{(1)}$ y $\phi_\mathfrak{p} := \phi_{E_\mathfrak{p}} = \phi_\infty \circ \mathrm{N}_{E_\mathfrak{p}/K_\infty}$. Si $x \in \mathrm{núc}\,\phi_{E_\mathfrak{p}}$ entonces $\phi_\infty(\mathrm{N}_{E_\mathfrak{p}/K_\infty}(x)) = \phi_\mathfrak{p}(x) = 1$ por lo que $\mathrm{N}_{E_\mathfrak{p}/K_\infty}(x) \in \mathrm{núc}\,\phi_\infty$ lo que a su vez implica que $x \in \mathrm{N}^{-1}_{E_\mathfrak{p}/K_\infty}(\mathrm{núc}\,\phi_\infty)$. Recíprocamente, si $x \in \mathrm{N}^{-1}_{E_\mathfrak{p}/K_\infty}(\mathrm{núc}\,\phi_\infty)$ entonces $\mathrm{N}_{E_\mathfrak{p}/K_\infty}(x) \in \mathrm{núc}\,\phi_\infty$. Se sigue que $\phi_\infty(\mathrm{N}_{E_\mathfrak{p}/K_\infty} x) = 1 = \phi_\mathfrak{p}(x)$ de donde se obtiene que $x \in \mathrm{núc}\,\phi_\mathfrak{p}$. En resumen, tenemos $\mathrm{núc}\,\phi_\mathfrak{p} = \mathrm{N}^{-1}_{E_\mathfrak{p}/K_\infty}(\mathrm{núc}\,\phi_\infty) = \mathrm{N}^{-1}_{E_\mathfrak{p}/K_\infty}\big((\pi_\infty)\times U_\infty^{(1)}\big)$.

Puesto que $k \subseteq E \subseteq K(\Lambda_M)$, se sigue que $K_\infty \subseteq E_\mathfrak{p} \subseteq K(\Lambda_N)_\mathfrak{P} = K_\infty(\sqrt[q-1]{-1/T})$ donde $\mathfrak{P}$ es un primo en $K(\Lambda_M)$ tal que $\mathfrak{P}|\infty$ y $\mathfrak{p} = \mathfrak{P}\cap E$. El campo asociado a $\mathrm{núc}\,\phi_\infty$ es $K_\infty(\sqrt[q-1]{-1/T})$ y el campo asociado a $\mathrm{núc}\,\phi_\mathfrak{p} = \mathrm{N}^{-1}_{E_\mathfrak{p}/K_\infty}(\mathrm{núc}\,\phi_\infty)$ es $E_\mathfrak{p}(\sqrt[q-1]{-1/T}) = k_\infty(\sqrt[q-1]{-1/T})$ (Corolario 7.3.12). Se sigue que $\mathrm{N}_{E_\mathfrak{p}/K_\infty}(\mathrm{núc}\,\phi_\mathfrak{p}) = \mathrm{núc}\,\phi_\infty$. Por tanto

$$\begin{aligned}\mathrm{N}_{E/k}\, U_E^+ &= \prod_{P\in R_T}\prod_{\mathfrak{p}|P} \mathrm{N}_{E_\mathfrak{p}/k_\infty}\, U_\mathfrak{p} \times \prod_{\mathfrak{p}|\infty} \mathrm{N}_{E_\mathfrak{p}/k_\infty}(\mathrm{núc}\,\phi_\mathfrak{p}) \\ &= \prod_{P\in R_T}\prod_{\mathfrak{p}|P} \mathrm{N}_{E_\mathfrak{p}/k_\infty}\, U_\mathfrak{p} \times (\mathrm{núc}\,\phi_\infty).\end{aligned}$$

De (8.1.2) obtenemos que

$$\begin{aligned}\Big(\prod_{P\in R_T'} U_P \times \prod_{i=1}^{r} U_{P_i}^{(\alpha_i)} \times (\langle\pi_\infty\rangle \times U_\infty^{(1)})\Big)K^* \\ \subseteq \Big(\prod_{P\in R_T}\prod_{\mathfrak{p}|P} \mathrm{N}_{E_\mathfrak{p}/k_P}\, U_\mathfrak{p} \times \prod_{\mathfrak{p}|\infty} \mathrm{N}_{E_\mathfrak{p}/k_\infty}(\mathrm{núc}\,\phi_\mathfrak{p})\Big)K^*.\end{aligned}$$

Por tanto $\mathcal{X}_M K^* \subseteq \mathrm{N}_{E/K}(U_E^+)K^*$ de donde se sigue que $E_{\mathfrak{gcf}} \subseteq K(\Lambda_M)$.

Ahora bien, $E_{\mathfrak{gcf}}/E$ es no ramificada en los primos finitos y como L es el campo asociado a $Y = \prod_{P\in R_T} X_P$, L es la máxima extensión abeliana de E contenida en $K(\Lambda_M)$ no ramificada en los primos finitos, de donde se sigue que $E_{\mathfrak{gcf}} \subseteq L$.

Para probar que $L \subseteq E_{\mathfrak{gcf}}$, basta probar que $L \subseteq E_{H^+}$ pues L/E es abeliana y $E_{\mathfrak{gcf}} \subseteq E_{H^+}$ es la máxima extensión abeliana de E contenida en E_{H^+}.

Ahora bien, para probar que $L \subseteq E_{H^+}$, hay que probar que $\mathrm{N}_{L/E}\, C_L \supseteq \mathrm{N}_{E_{H^+}/E}\, C_{E_{H^+}} = U_E^+ E^*/E^*$, donde $U_E^+ = \prod_{\mathfrak{p}|\infty} \text{núc}\, \phi_{\mathfrak{p}} \times \prod_{\mathfrak{p}\nmid\infty} U_{\mathfrak{p}}$.

Sea $\mathrm{N}_{L/E}\, C_L = \Lambda E^*/E^*$ donde $\Lambda = \mathrm{N}_{L/E}\, J_L$. Basta probar que $U_E^+ \subseteq \Lambda$. Puesto que L/E es no ramificada en todos los primos finitos, si $\mathfrak{p}$ es un primo finito de E y $\mathfrak{P}$ es un primo de L sobre $\mathfrak{p}$, $\mathrm{N}_{L_{\mathfrak{P}}/E_{\mathfrak{p}}}\, U_{\mathfrak{P}} = U_{\mathfrak{p}}$ donde denotamos $U_{\mathfrak{P}} = U_{L_{\mathfrak{P}}}$ y $U_{\mathfrak{p}} = U_{E_{\mathfrak{p}}}$ (Teorema 3.4.9). En particular $\mathrm{N}_{L_{\mathfrak{P}}/E_{\mathfrak{p}}}\, L_{\mathfrak{P}}^* \supseteq U_{\mathfrak{p}}$ y $\mathrm{N}_{L/E}\, J_L \supseteq \prod_{\mathfrak{p}\nmid\infty} U_{\mathfrak{p}}$.

Por otro lado, $L/E_{\mathfrak{ge}}$ es totalmente ramificada en los primos infinitos y los primos infinitos de E son totalmente descompuestos en $E_{\mathfrak{ge}}$, por lo que $(E_{\mathfrak{ge}})_{\mathfrak{p}} = E_{\mathfrak{p}}$ para $\mathfrak{p}|\infty$ y elemento uniformizador de $\mathfrak{p}$ en E lo es para $\mathfrak{p}$ en $E_{\mathfrak{ge}}$.

Por el Teorema 5.8.62, $\pi_{E,\infty} := \pi_{E_{\mathfrak{p}}}$ es norma de $L_{\mathfrak{P}}$ con $\mathfrak{P}|\mathfrak{p}$. Si $(\_, L_{\mathfrak{P}}/E_{\mathfrak{p}})$ representa el mapeo local de Artin, entonces $(U_{E_{\mathfrak{p}}}^{(1)}, L_{\mathfrak{P}}/E_{\mathfrak{p}}) = G^1(L_{\mathfrak{P}}/E_{\mathfrak{p}})$, el primer grupo de ramificación de $L_{\mathfrak{P}}/E_{\mathfrak{p}}$. Puesto que los primos infinitos son moderadamente ramificados en $L_{\mathfrak{P}}/E_{\mathfrak{p}}$, se sigue que $G^1(L_{\mathfrak{P}}/E_{\mathfrak{p}}) = \{1\}$ y $U_{E_{\mathfrak{p}}}^{(1)} \subseteq \mathrm{N}_{L_{\mathfrak{P}}/E_{\mathfrak{p}}}\, L_{\mathfrak{P}}^*$.

El campo de constantes de E y de K es $\mathbb{F}_q$ y todo primo infinito tiene grado 1 en E, por lo que si $\mathfrak{p}$ es un primo infinito de E, $E_{\mathfrak{p}}^* = (\pi_{E,\infty}) \times \mathbb{F}_q^* \times U_{E_{\mathfrak{p}}}^{(1)}$. Notemos que $[E_{\mathfrak{p}} : K_\infty] = ef = e = [K_\infty^* : \mathrm{N}_{E_{\mathfrak{p}}/K_\infty}\, E_{\mathfrak{p}}^*]$ donde e denota al índice de ramificación de $E_{\mathfrak{p}}/K_\infty$. Además como $E_{\mathfrak{p}}/K_\infty$ es total y moderadamente ramificada, $(\pi_\infty) \times U_{E_{\mathfrak{p}}}^{(1)} \subseteq \mathrm{N}_{E_{\mathfrak{p}}/K_\infty}(E_{\mathfrak{p}}^*)$ y $\mathrm{N}_{E_{\mathfrak{p}}/K_\infty}\, \mathbb{F}_q^* = (\mathbb{F}_q^*)^e$. Se sigue que $(\pi_\infty)\times(\mathbb{F}_q^*)^e \times U_\infty^{(1)} \subseteq \mathrm{N}_{E_{\mathfrak{p}}/K_\infty}\, E_{\mathfrak{p}}^*$. De $[K_\infty^* : \mathrm{N}_{E_{\mathfrak{p}}/K_\infty}\, E_{\mathfrak{p}}^*] = e$ obtenemos la igualdad

$$\mathrm{N}_{E_{\mathfrak{p}}/K_\infty}\, E_{\mathfrak{p}}^* = (\pi_\infty) \times (\mathbb{F}_q^*)^e \times U_\infty^{(1)}.$$

Por tanto $\phi_{\mathfrak{p}}(E_{\mathfrak{p}}^*) = \phi_\infty(\mathrm{N}_{E_{\mathfrak{p}}/K_\infty}\, E_{\mathfrak{p}}^*) = \phi_\infty\big((\pi_\infty) \times (\mathbb{F}_q^*)^e \times U_\infty^{(1)}\big) = (\mathbb{F}_q^*)^e$. Se sigue que $\text{núc}\, \phi_{\mathfrak{p}} = (\pi_{E,\infty}) \times R \times U_{E_{\mathfrak{p}}}^{(1)}$ donde $R = \{\lambda \in \mathbb{F}_q^* \mid \lambda^e = 1\} = (\mathbb{F}_q^*)^{(q-1)/e}$. Aquí e es el índice de ramificación de $\mathfrak{p}_\infty$ en E/K.

Notemos que si $\mathfrak{P}$ es un primo infinito de L, $\mathrm{N}_{L_{\mathfrak{P}}/E_{\mathfrak{p}}}\, \mathbb{F}_q^* = (\mathbb{F}_q^*)^{e'}$ donde $e' := e_\infty(L/E_{\mathfrak{ge}}) = e_\infty(L/E)$. Entonces $e'e = e_\infty(L/K)$ y en particular $e'e|q-1$ y $e'\big|\frac{q-1}{e}$. Sea $\mathbb{F}_q^* = \langle\beta\rangle$ con $o(\beta) = q-1$. Sea $\lambda \in R$, $\lambda^e = 1$. Se tiene $\lambda = \beta^s$ para algún s. Por tanto $\lambda^e = \beta^{es} = 1$ y $q-1|es$. Puesto que $e'e|q-1$ se sigue que $e'e|se$ y $e'|s$. De esta forma se obtiene que $\lambda = \beta^s = (\beta^{s/e'})^{e'} \in (\mathbb{F}_q^*)^{e'} \subseteq \mathrm{N}_{L_{\mathfrak{P}}/E_{\mathfrak{p}}}\, L_{\mathfrak{P}}^*$.

Se sigue que $\text{núc}\,\phi_{\mathfrak{p}} \subseteq \mathrm{N}_{L_{\mathfrak{P}}/E_{\mathfrak{p}}} L_{\mathfrak{P}}^*$ y que $U_E^+ = \prod_{\mathfrak{p}|\infty} \text{núc}\,\phi_{\mathfrak{p}} \times \prod_{\mathfrak{p}\nmid\infty} U_{\mathfrak{p}} \subseteq \mathrm{N}_{L/K} J_L$ de donde se obtiene $L \subseteq E_{H^+}$ y por tanto $L = E_{\mathfrak{ge}_{\mathfrak{X}}}$.

Hemos probado

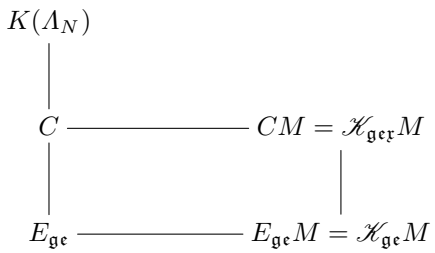
Teorema 8.1.14. *Sea $E \subseteq K(\Lambda_M)$. Entonces el campo de géneros extendido $E_{\mathfrak{ge}_{\mathfrak{X}}}$ de E relativo a K es el campo asociado al grupo de caracteres de Dirichlet $Y = \prod_{P\in R_T} X_P$, donde X es el grupo de caracteres de Dirichlet asociado al campo E.* □

8.2. Extensiones abelianas finitas

Usamos las notaciones de [136, Capítulo 14]. Consideremos $\mathscr{K}/K = \mathbb{F}_q(T)$ una extensión abeliana finita. Sean $n \in \mathbb{N} \cup \{0\}$, $m \in \mathbb{N}$ y $N \in R_T$ tales que $\mathscr{K} \subseteq {}_nK(\Lambda_N)_m$. Sea $E := \mathscr{K}M \cap K(\Lambda_N)$, donde $M = L_nK_m$. Tenemos que $E\mathscr{K}/\mathscr{K}$ es una extensión de constantes, en particular una extensión no ramificada (ver [136, Teorema 14.5.1]). Sea H el grupo de descomposición de los pirmos infinitos de $\mathscr{K}$ en $E\mathscr{K}/\mathscr{K}$. Se tiene que H es canónicamente isomorfo con el grupo de descomposición de los primos infinitos de $E_{\mathfrak{ge}}\mathscr{K}/\mathscr{K}$. Tenemos que $|H|$ es igual al grado de inercia de los primos infinitos de $\mathscr{K}$ en cualquiera de $E\mathscr{K}/\mathscr{K}$ o de $E_{\mathfrak{ge}}\mathscr{K}/\mathscr{K}$. También se tiene que $\mathscr{K}_{\mathfrak{ge}} = E_{\mathfrak{ge}}^H\mathscr{K}$.

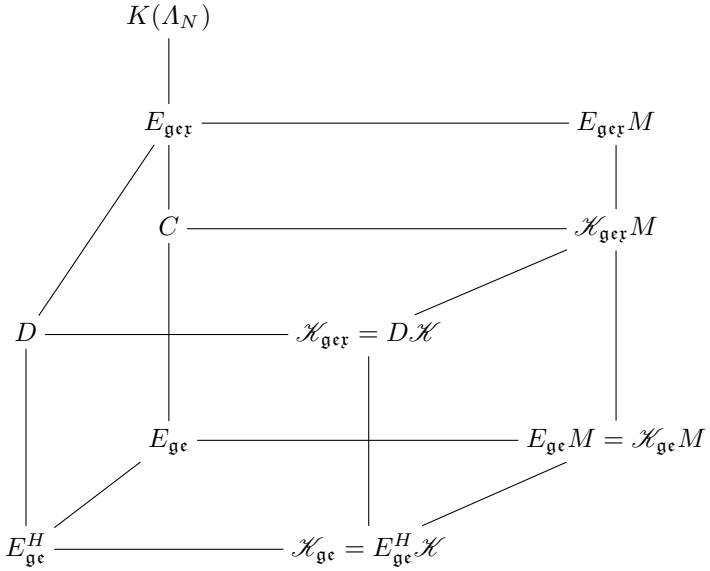
Teorema 8.2.1. *Con las notaciones anteriores, tenemos que $\mathscr{K}_{\mathfrak{ge}_{\mathfrak{X}}} = D\mathscr{K}$ con $(E_{\mathfrak{ge}}^H)_{\mathfrak{ge}_{\mathfrak{X}}} \subseteq D \subseteq E_{\mathfrak{ge}_{\mathfrak{X}}}$. En particular, cuando $H = \{1\}$, tenemos $\mathscr{K}_{\mathfrak{ge}_{\mathfrak{X}}} = E_{\mathfrak{ge}_{\mathfrak{X}}}\mathscr{K}$.*

Demostración. Sabemos que $E_{\mathfrak{ge}}M = \mathscr{K}_{\mathfrak{ge}}M$ (ver la demostración de [136, Teorema 14.5.1]). Sea $C := \mathscr{K}_{\mathfrak{ge}_{\mathfrak{X}}}M \cap K(\Lambda_N) \supseteq \mathscr{K}_{\mathfrak{ge}}M \cap K(\Lambda_N) = E_{\mathfrak{ge}}M \cap K(\Lambda_N) \supseteq E_{\mathfrak{ge}} \cap K(\Lambda_N) = E_{\mathfrak{ge}}$.



Notemos que $\mathscr{K}_{\mathfrak{ge}_{\mathfrak{X}}}M/\mathscr{K}_{\mathfrak{ge}}M$ es no ramificada en los primos finitos pues esto mismo se cumple en $\mathscr{K}_{\mathfrak{ge}_{\mathfrak{X}}}/\mathscr{K}_{\mathfrak{ge}}$. También se tiene que $E_{\mathfrak{ge}}M/E_{\mathfrak{ge}}$ es no ramificada en los primos finitos. En particular $C/E_{\mathfrak{ge}}$ es no ramificada en los primos finitos y $C \subseteq K(\Lambda_N)$. Puesto que $E_{\mathfrak{ge}_{\mathfrak{X}}}/K$ es la máxima extensión abeliana con $E_{\mathfrak{ge}_{\mathfrak{X}}}/E$ no ramificada en los primos finitos y contenida en un campo de funciones ciclotómico, se sigue que $C \subseteq E_{\mathfrak{ge}_{\mathfrak{X}}}$.

Por lo tanto $E_{\mathfrak{ge}} \subseteq C \subseteq E_{\mathfrak{ge}\mathfrak{x}}$ y $\begin{array}{ccccc} E_{\mathfrak{ge}}M & & CM & & E_{\mathfrak{ge}\mathfrak{x}}M \\ \| & \subseteq & \| & \subseteq & \| \\ \mathscr{K}_{\mathfrak{ge}}M & & \mathscr{K}_{\mathfrak{ge}\mathfrak{x}}M & & E_{\mathfrak{ge}\mathfrak{x}}M \end{array}$. En particular $\mathscr{K}_{\mathfrak{ge}\mathfrak{x}}M \subseteq E_{\mathfrak{ge}\mathfrak{x}}M$.



Sea $D := \mathscr{K}_{\mathfrak{ge}\mathfrak{x}} \cap K(\Lambda_N) = E^H_{\mathfrak{ge}}\mathscr{K} \cap K(\Lambda_N) \supseteq E^H_{\mathfrak{ge}} \cap K(\Lambda_N) = E^H_{\mathfrak{ge}}$. Por tanto $E^H_{\mathfrak{ge}} \subseteq D$ y $\mathscr{K}_{\mathfrak{ge}\mathfrak{x}} = D\mathscr{K}$.

Se tiene que la extensión EM/E es no ramificada en los primos finitos. Por lo tanto $DEM = D\mathscr{K}M/EM = \mathscr{K}M$ es no ramificada en los primos finitos puesto que $\mathscr{K}_{\mathfrak{ge}\mathfrak{x}}/\mathscr{K}$ satisface esto mismo. Se sigue que DE/E es no ramificada en los primos finitos por lo que $D \subseteq E_{\mathfrak{ge}\mathfrak{x}}$. De esta forma, obtenemos que $\mathscr{K}_{\mathfrak{ge}\mathfrak{x}} = D\mathscr{K} \subseteq E_{\mathfrak{ge}\mathfrak{x}}\mathscr{K}$.

En el caso particular de que $H = \{1\}$ se tiene que $E \subseteq \mathscr{K}_{\mathfrak{ge}} \subseteq \mathscr{K}_{\mathfrak{ge}\mathfrak{x}}$ de tal forma que $E_{\mathfrak{ge}\mathfrak{x}} \subseteq \mathscr{K}_{\mathfrak{ge}\mathfrak{x}}$ y $\mathscr{K}_{\mathfrak{ge}\mathfrak{x}} = E_{\mathfrak{ge}\mathfrak{x}}\mathscr{K}$.

En el caso general, $E^H_{\mathfrak{ge}} \subseteq D \subseteq E_{\mathfrak{ge}\mathfrak{x}}$ y $E_{\mathfrak{ge}\mathfrak{x}}/E^H_{\mathfrak{ge}}$ es totalmente ramificada en los primos infinitos. Puesto que $E^H_{\mathfrak{ge}} \subseteq \mathscr{K}_{\mathfrak{ge}}$, se sigue que $(E^H_{\mathfrak{ge}})_{\mathfrak{ge}\mathfrak{x}} \subseteq \mathscr{K}_{\mathfrak{ge}\mathfrak{x}}$. Por tanto $(E^H_{\mathfrak{ge}})_{\mathfrak{ge}\mathfrak{x}} \subseteq D$. □

Ejemplo 8.2.2. Sean $\mathscr{K} := K(\sqrt[l]{\gamma D})$ donde l es un número primo tal que $l|q-1$, $D \in R_T$, D mónico con $l \nmid \operatorname{gr} D$, y $\gamma \not\equiv (-1)^{\operatorname{gr} D}$ mód $(\mathbb{F}_q^*)^l$. Entonces $E = M\mathscr{K} \cap K(\Lambda_D) = K(\sqrt[l]{D^*})$ donde $M = K_l$ y $D^* = (-1)^{\operatorname{gr} D}D$. Entonces $H \cong C_l$, $E_{\mathfrak{ge}\mathfrak{x}} = E_{\mathfrak{ge}} = E$, $E^H_{\mathfrak{ge}} = E^H = K$, $\mathscr{K}_{\mathfrak{ge}} = \mathscr{K}$.

Sea $n := \operatorname{gr} D$, $D = T^n + a_{n-1}T^{n-1} + \cdots + a_1T + a_0$, $n = lm - r$ con $0 < r < l$. El primo infinito $\mathfrak{p}_\infty$ se ramifica in $\mathscr{K}/K$, por lo que solamente hay un

único primo infinito $\mathfrak{P}_\infty$ en $\mathscr{K}$. Por tanto, tenemos que $U_{\mathscr{K}} = \mathscr{K}_\infty^* \times \prod_{\mathfrak{p}\nmid\infty} U_\mathfrak{p}$ y $U_{\mathscr{K}}^+ = \operatorname{núc}\phi_{\mathscr{K}_\infty} \times \prod_{\mathfrak{p}\nmid\infty} U_\mathfrak{p}$, donde $\mathscr{K}_\infty = \mathscr{K}_{\mathfrak{P}_\infty}$. Ahora

$$\mathscr{K}_\infty = K_\infty(\sqrt[l]{\gamma D}) = K_\infty(\sqrt[l]{\gamma T^n u}) = K_\infty\big(\sqrt[l]{\gamma T^{-r}(T^m)^l u}\big),$$

donde $u = 1 + a_{n-1}(1/T) + \cdots + a_1(1/T)^{n-1} + a_0(1/T)^n \in U_{\mathscr{K}_\infty}^{(1)}$. Puesto que $p \neq l$, existe $v \in U_{\mathscr{K}_\infty}^{(1)}$ tal que $u = v^l$. Se sigue que $\mathscr{K}_\infty = K_\infty(\sqrt[l]{\gamma T^{-r}}) = K_\infty(\sqrt[l]{\delta/T})$ para algún $\delta \in \mathbb{F}_q^*$, $\delta \not\equiv (-1)$ mód $(\mathbb{F}_q^*)^l$.

Un elemento primo en $\mathscr{K}_\infty$ es $\pi^\star := \pi_{\mathscr{K}_\infty} = \sqrt[l]{\delta/T}$, $(\pi^\star)^l = \delta/T = \delta\pi_\infty$. De aquí que para un elemento arbitrario $x \in \mathscr{K}_\infty^*$, digamos $x = (\pi^\star)^m \xi w$, $m \in \mathbb{Z}$, $\xi \in \mathbb{F}_q^*$, $w \in U_{\mathscr{K}_\infty}^{(1)}$, tenemos que $N_{\mathscr{K}_\infty/K_\infty}(x) = ((-1)^{l-1}\delta\pi_\infty)^m \xi^l w'$, con $w' \in U_\infty^{(1)}$, de tal forma que $\phi_{\mathscr{K}_\infty}(x) = ((-1)^{l-1}\delta)^m \xi^l$. Se sigue que si $x \in \operatorname{núc}\phi_{\mathscr{K}_\infty}$, entonces $l|m$. También se tiene que $\delta^{-1}(\pi^\star)^l \in \operatorname{núc}\phi_{\mathscr{K}_\infty}$.

Por tanto $\min\{m \in \mathbb{N} \mid \text{existe } \vec{\alpha} \in U_K^+ \text{ con } \operatorname{gr}\vec{\alpha} = m\} = l$. Se sigue que el campo de constantes de $H_{\mathscr{K}}^+$ y de $\mathscr{K}_{\mathfrak{ge}\mathfrak{x}}$ es $\mathbb{F}_{q^l}$.

Puesto que el campo de constantes de $\mathscr{K}_{\mathfrak{ge}}$ es $\mathbb{F}_q$, se obtiene que $\mathscr{K}_{\mathfrak{ge}\mathfrak{x}} = \mathscr{K}_{\mathfrak{ge},l} = E_{\mathfrak{ge}\mathfrak{x}}K$.

Ejemplo 8.2.3. Sean l un número primo tal que $l^2|q-1$ y $\mathscr{K} = K(\sqrt[l^2]{\gamma D})$ donde $\gamma \in \mathbb{F}_q^*$, $D = P_1^{\alpha_1}\cdots P_r^{\alpha_r} \in R_T$, $P_1, \ldots, P_r \in R_T^+$, $1 \le \alpha_i \le l^2 - 1$, $1 \le i \le r$, $r \ge 1$. Suponemos que $\operatorname{gr} D = ld$ con $l \nmid d$, que $l \nmid \operatorname{gr} P_1$, que $\operatorname{mcd}(\alpha_i, l) = 1$, $1 \le i \le s$, $s \ge 1$ y que $l|\alpha_j$, $s+1 \le j \le r$. Entonces $e_{P_i}(\mathscr{K}/K) = l^2$ para $1 \le i \le s$, $e_{P_j}(\mathscr{K}/K) = l$ para $s+1 \le j \le r$, y $e_\infty(\mathscr{K}/K) = l$. Puesto que $e_{P_1}(\mathscr{K}/K) = l^2$, el campo de constantes de $\mathscr{K}$ es $\mathbb{F}_q$. Suponemos que $(-1)^{\operatorname{gr} D}\gamma \notin (\mathbb{F}_q^*)^l$. Por lo tanto $\mathbb{F}_q(\sqrt[l^2]{\varepsilon}) = \mathbb{F}_{q^{l^2}}$ donde $\varepsilon = (-1)^{\operatorname{gr} D}\gamma$.

Sean $M = \mathbb{F}_{q^{l^2}}(T) = K_{l^2}$ y $E = \mathscr{K}M \cap K(\Lambda_D)$. Entonces $E = K(\sqrt[l^2]{(-1)^{\operatorname{gr} D} D}) = K(\sqrt[l^2]{D^*}) \subseteq K(\Lambda_D)$. Se tiene

$$E\mathscr{K} = E(\sqrt[l^2]{\varepsilon}) = \mathscr{K}(\sqrt[l^2]{\varepsilon}) = E_{l^2} = \mathscr{K}_{l^2}.$$

De esta forma obtenemos que $f_\infty(\mathscr{K}/K) = [\mathbb{F}_q(\sqrt[l]{\varepsilon}) : \mathbb{F}_q] = l$ y por tanto $f_\infty(E\mathscr{K}/\mathscr{K}) = \frac{f_\infty(E\mathscr{K}/K)}{f_\infty(\mathscr{K}/K)} = \frac{l^2}{l} = l$. Se sigue que $H \cong C_l$ y por tanto $|H| = l$.

También se tiene que $E_{\mathfrak{ge}\mathfrak{x}} = K\big(\sqrt[l^2]{P_1^*}, \ldots, \sqrt[l^2]{P_s^*}, \sqrt[l]{P_{s+1}^*}, \ldots \sqrt[l]{P_r^*}\big)$. Puesto que $l \nmid \operatorname{gr} P_1$, se sigue que $e_\infty\big(K(\sqrt[l^2]{P_1^*})/K\big) = l^2$ y por tanto $e_\infty(E_{\mathfrak{ge}\mathfrak{x}}/K) = l^2$. Puesto que $\operatorname{gr} D = ld$ con $l \nmid d$, tenemos que $e_\infty(E_{\mathfrak{ge}}/K) = l$. Ahora

$$\operatorname{gr} D = ld = \sum_{i=1}^r \alpha_i \operatorname{gr} P_i = \alpha_i \operatorname{gr} P_1 + \sum_{i=2}^s \alpha_i \operatorname{gr} P_i + \sum_{j=s+1}^r \alpha_j \operatorname{gr} P_j,$$

y puesto que $l|\sum_{j=s+1}^r \alpha_j \operatorname{gr} P_j$ y $\operatorname{mcd}(\alpha_i, l) = 1$ para $1 \le i \le s$, se sigue que existe $2 \le i \le s$ con $l \nmid \operatorname{gr} P_i$. Digamos que $l \nmid \operatorname{gr} P_2$.

Sean $a, b \in \mathbb{Z}$ tales que $a \operatorname{gr} P_1 + bl^2 = 1$ (en particular, $\operatorname{mcd}(a, l) = 1$). Por tanto, para $i \geq 2$ tenemos que $\operatorname{gr} P_i - (a \operatorname{gr} P_i) \operatorname{gr} P_1 = b(\operatorname{gr} P_i)l^2$. Sea $Q_i = P_i P_1^{z_i}$ con $z_i := -a \operatorname{gr} P_i$ para $2 \leq i \leq r$. Sea

$$L := K\big(\sqrt[l]{P_1^*},\ \sqrt[l^2]{Q_2}, \ldots,\ \sqrt[l^2]{Q_s}, \sqrt[l]{Q_{s+1}}, \ldots, \sqrt[l]{Q_r}\big).$$

Entonces $e_\infty(L/K) = l$, $e_{P_i}(L/K) = l^2$ para $2 \leq i \leq s$ y $e_{P_j}(L/K) = l$ para $s+1 \leq j \leq r$. Para el primo P_1 tenemos que, puesto que $l \nmid \operatorname{gr} P_2$, que $\sqrt[l^2]{Q_2} = \sqrt[l^2]{P_2 P_1^{-a \operatorname{gr} P_2}}$ y que $\operatorname{mcd}(l, -a \operatorname{gr} P_2) = 1$, entonces $e_{P_1}(K(\sqrt[l^2]{Q_2})/K) = l^2$. De esta forma obtenemos que $e_{P_1}(L/K) = l^2$. Por tanto $E \subseteq L$ y $[E_{\mathfrak{ge}\mathfrak{f}} : L] = l$. Se sigue que

$$\begin{gathered} L = E_{\mathfrak{ge}} = K\big(\sqrt[l]{P_1^*},\ \sqrt[l^2]{Q_2}, \ldots,\ \sqrt[l^2]{Q_s}, \sqrt[l]{Q_{s+1}}, \ldots, \sqrt[l]{Q_r}\big), \\ E_{\mathfrak{ge}\mathfrak{f}} = E_{\mathfrak{ge}\mathfrak{f}} = K\big(\sqrt[l^2]{P_1^*}, \ldots,\ \sqrt[l^2]{P_s^*}, \sqrt[l]{P_{s+1}^*}, \ldots \sqrt[l]{P_r^*}\big), \\ [E_{\mathfrak{ge}\mathfrak{f}} : E_{\mathfrak{ge}}] = l = e_\infty(E_{\mathfrak{ge}\mathfrak{f}}/E_{\mathfrak{ge}}). \end{gathered}$$

Ahora, $E\mathscr{K} = \mathscr{K}_{l^2}$, de tal forma que $H \cong D_\infty(E\mathscr{K}/\mathscr{K}) \cong \operatorname{Gal}(\mathscr{K}_{l^2}/\mathscr{K}_l)$, donde D_∞ denota el grupo de descomposición de los primos infinitos.

$$\begin{array}{c} E\mathscr{K} = \mathscr{K}_{l^2} \\ \Big| \ f_\infty(E\mathscr{K}/\mathscr{K}_l) = l \\ \mathscr{K}_l \\ \Big| \ f_\infty(\mathscr{K}_l/\mathscr{K}) = 1 \\ \mathscr{K} \end{array}$$

Tenemos

$$\begin{gathered} E^H = K(\sqrt[l]{D^*}) = K(\sqrt[l]{D}) \quad \text{y} \\ E^H_{\mathfrak{ge}} = K\big(\sqrt[l^2]{Q_2}, \ldots,\ \sqrt[l^2]{Q_s}, \sqrt[l]{Q_{s+1}}, \ldots, \sqrt[l]{Q_r}\big). \end{gathered}$$

También se obtiene que $(E^H_{\mathfrak{ge}})_{\mathfrak{ge}\mathfrak{f}} = E_{\mathfrak{ge}\mathfrak{f}}$ debido a que $[(E^H_{\mathfrak{ge}})_{\mathfrak{ge}\mathfrak{f}} : K] = \prod_{j=1}^r e_{P_j}(E^H_{\mathfrak{ge}}/K) = [E_{\mathfrak{ge}\mathfrak{f}} : K]$ y $E^H_{\mathfrak{ge}} \subseteq E_{\mathfrak{ge}\mathfrak{f}}$. Se sigue que

$$\begin{aligned} \mathscr{K}_{\mathfrak{ge}\mathfrak{f}} = E_{\mathfrak{ge}\mathfrak{f}}\mathscr{K} &= K\big(\sqrt[l^2]{P_1^*}, \ldots,\ \sqrt[l^2]{P_s^*}, \sqrt[l]{P_{s+1}^*}, \ldots \sqrt[l]{P_r^*}\ \sqrt[l^2]{\gamma D}\big) \\ &= E_{\mathfrak{ge}\mathfrak{f}}(\sqrt[l^2]{\varepsilon}). \end{aligned}$$

Observación 8.2.4. (1) Cuando $H = \{1\}$ se tiene $\mathscr{K}_{\mathfrak{ge}\mathfrak{f}} = \mathscr{K}^{\mathrm{ext}} := E_{\mathfrak{ge}\mathfrak{f}}\mathscr{K}$.

(2) En general tenemos $f_\infty(\mathscr{K}_{\mathfrak{ge}\mathfrak{f}}|\mathscr{K}_{\mathfrak{ge}}) > 1$.

(3) El campo de constantes $\mathscr{K}_{H^+}$ puede ser diferente al de $\mathscr{K}_H$ (Ejemplos 8.2.2 y 8.2.3). En el Ejemplo 8.2.3 se tiene que $\mathbb{F}_{q^l}$ es el campo de constantes de $\mathscr{K}_H$ y $\mathbb{F}_{q^{l^2}}$ es el campo de constantes $\mathscr{K}_{H^+}$.

(4) En general la extensión $\mathscr{K}_{\mathfrak{ge}_\mathfrak{x}}/\mathscr{K}_{\mathfrak{ge}}$ puede contener subextensiones no ramificadas. En el Ejemplo 8.2.3 se tiene que $\mathscr{K}_{\mathfrak{ge}_\mathfrak{x}} = \mathscr{K}_{\mathfrak{ge}}(\sqrt[l^2]{P_1})$ y $\mathscr{K}_{\mathfrak{ge}} \subsetneqq (\mathscr{K}_{\mathfrak{ge}})_{l^2} = \mathscr{K}_{\mathfrak{ge}}(\sqrt[l]{P_1}) \subsetneqq \mathscr{K}_{\mathfrak{ge}_\mathfrak{x}}$. Tenemos que $e_\infty(\mathscr{K}_{\mathfrak{ge}_\mathfrak{x}}|\mathscr{K}_{\mathfrak{ge}}) = f_\infty(\mathscr{K}_{\mathfrak{ge}_\mathfrak{x}}|\mathscr{K}_{\mathfrak{ge}}) = l$.

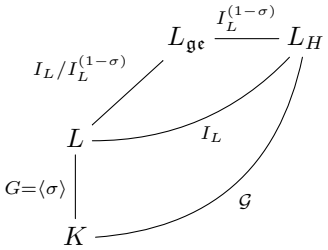
Para ver una descripción de $\mathscr{K}_{\mathfrak{ge}_\mathfrak{x}}$ para una extensión finita y separable $\mathscr{K}/K$, en la mayoría de los casos, ver [124].

Terminamos enunciando dos teoremas clásicos de campos de géneros numéricos desde el punto de vista de campos de clase globales.

Desde el punto de vista de campos de clase, los campos de géneros tienen las siguientes propiedades. En la construcción de Furtwängler del campo de clase de Hilbert, el siguiente teorema es muy importante. Ver [136, Teorema 14.3.3].

Teorema 8.2.5 (Furtwängler, 1907). *Sea L/K una extensión cíclica no ramificada de campos numéricos y sea σ un generador de $G = \mathrm{Gal}(L/K)$. Sea $\mathrm{N}\colon I_L \longrightarrow I_K$ la norma (relativa) de clases de ideales, esto es, $\mathrm{N}\,\mathfrak{a} = \mathfrak{b} \in I_K$ donde $\mathfrak{a} \in I_L$ y $\mathrm{con}_{K/L}\,\mathfrak{b} = \prod_{\theta\in G}\mathfrak{a}^\theta$ (la norma de $\mathfrak{a}$). Entonces* $\mathrm{núc}\,\mathrm{N} = I_L^{(1-\sigma)}$.

Demostración. Se tiene que $I_L \cong \mathrm{Gal}(L_H/L)$ y como L/K es abeliana, el campo de géneros $L_{\mathfrak{ge}}$ de L sobre K, es la máxima extensión abeliana K contenida en L_H.



Sea $\mathcal{G} = \mathrm{Gal}(L_H/K)$ (L_H/K es Galois por la maximalidad de L_H). Entonces, como $L_{\mathfrak{ge}}$ es la máxima extensión abeliana de K contenida en L_H, $\mathrm{Gal}(L_H/L_{\mathfrak{ge}}) = \mathcal{G}'$ el subgrupo conmutador de $\mathcal{G}$. Veamos que $\mathcal{G}' = I_L^{(1-\sigma)}$.

Se tiene que la sucesión $1 \longrightarrow I_L \longrightarrow \mathcal{G} \longrightarrow G \longrightarrow 1$ es exactta por lo que $\mathcal{G} = GI_L = \{\tau\bar{\mathfrak{a}} \mid \tau \in G, \bar{\mathfrak{a}} \in I_L\}$ y G actúa en I_L por conjugación

Para $\bar{\mathfrak{a}} \in I_L \cong \mathrm{Gal}(L_H/L)$ y para $\tau \in G$, se tiene

$$\bar{\mathfrak{a}}^{1-\tau} = (1-\tau)\bar{\mathfrak{a}} = \bar{\mathfrak{a}} \circ \underbrace{(\tau^{-1} \circ \bar{\mathfrak{a}})}_{\substack{\text{acción}\\ \text{conjugación}}} = \bar{\mathfrak{a}} \circ \tau^{-1} \circ \bar{\mathfrak{a}} \circ \tau \in \mathcal{G}',$$

esto es, $I_L^{(1-\sigma)} \subseteq \mathcal{G}'$.

Ahora, $\mathcal{G}/I_L \cong G = \langle\sigma\rangle$ es abeliano, por lo que $\mathcal{G}' \subseteq I_L$.

Sean $x, y \in \mathcal{G}$, digamos $x = \tau\bar{\mathfrak{a}}$, $y = \gamma\bar{\mathfrak{b}}$, entonces

$$x^{-1} = \bar{\mathfrak{a}}^{-1}\tau^{-1} = \tau^{-1}\tau\bar{\mathfrak{a}}^{-1}\tau^{-1} = \tau^{-1}\bar{\mathfrak{a}}^{-\tau^{-1}} \quad \text{y} \quad y^{-1} = \gamma^{-1}\bar{\mathfrak{b}}^{-\gamma^{-1}}.$$

Por tanto

$$xyx^{-1}y^{-1} = (\tau\gamma\bar{\mathfrak{a}}^{\gamma}\bar{\mathfrak{b}})(\tau^{-1}\gamma^{-1}\bar{\mathfrak{a}}^{-\tau^{-1}\gamma^{-1}}\bar{\mathfrak{b}}^{-\gamma^{-1}}).$$

Notemos que si $\bar{\mathfrak{c}} \in I_L$ y $\delta \in G$, $\bar{\mathfrak{c}}\delta = \delta\delta^{-1}\bar{\mathfrak{c}}\delta = \delta\bar{\mathfrak{c}}^{\delta}$. Se sigue que

$$\begin{aligned} xyx^{-1}y^{-1} &= \tau\gamma\tau^{-1}\gamma^{-1}\bar{\mathfrak{a}}^{\gamma\tau^{-1}\gamma^{-1}}\bar{\mathfrak{b}}^{\tau^{-1}\gamma^{-1}}\bar{\mathfrak{a}}^{-\tau^{-1}\gamma^{-1}}\bar{\mathfrak{b}}^{-\gamma^{-1}} \\ &= \bar{\mathfrak{a}}^{\tau^{-1}(1-\gamma^{-1})}\bar{\mathfrak{b}}^{\gamma^{-1}(\tau^{-1}-1)} \in I_G I_L = I_L^{\sigma-1}. \end{aligned}$$

Por lo tanto $\mathcal{G}' \subseteq I_L^{\sigma-1}$ y $\mathcal{G}' = I_L^{\sigma-1}$.

Por otro lado, $L_{\mathfrak{gc}}$ corresponde a $\mathrm{N}_{L/K} I_L$ lo que implica que $\mathrm{Gal}(L_{\mathfrak{gc}}/K) \cong I_K/\mathrm{N}_{L/K} I_L \cong \mathcal{G}/\mathcal{G}' \cong \mathcal{G}/I_L^{(1-\sigma)}$.

En nuestro caso tenemos que, como L/K es no ramificada y abeliana, entonces $L \subseteq K_H \subseteq L_H$ y K_H/K es maximal, abeliana no ramificada, y por tanto $K_H = L_{\mathfrak{gc}}$ y se tiene el diagrama

$$\begin{array}{ccc} \text{núc}\,\mathrm{N} & \xrightarrow{\cong} & \text{núc rest} \cong \mathrm{Gal}(L_H/L_{\mathfrak{gc}}) \\ \downarrow & & \downarrow \\ I_L & \xrightarrow{\cong} & \mathrm{Gal}(L_H/L) \\ {\scriptstyle \mathrm{N}}\downarrow & & \downarrow{\scriptstyle \text{rest}} \\ I_K & \xrightarrow{\cong} & \mathrm{Gal}(K_H/K) \cong \mathrm{Gal}(L_{\mathfrak{gc}}/K) \end{array}$$

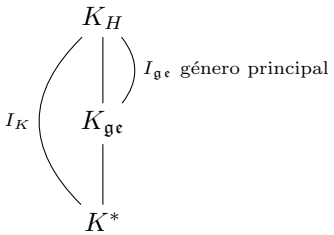
Se sigue que $\text{núc}\,\mathrm{N} \cong \mathrm{Gal}(L_H/L_{\mathfrak{gc}}) \cong \mathcal{G}' \cong I_L^{(1-\sigma)}$. □

Observación 8.2.6. De la demostración del Teorema 8.2.5, se sigue que el resultado sigue siendo válido para $G = \mathrm{Gal}(L/K)$ un grupo abelinao y no únicamente cíclico (ver [136, Teoremas 14.3.2 y 14.3.3 y Corolario 14.3.4]), cambiando $I_L^{(1-\sigma)}$ por $I_G I_L$ donde $I_G = \langle \tau - 1 \mid \tau \in G \rangle$.

En [56], Hasse prueba que si la norma satisface que $\mathrm{N}_{L/K} \colon I_L \longrightarrow I_K^{\mathfrak{f}}$, en donde L/K es una extensión cíclica de grado primo l, y $I_K^{\mathfrak{f}}$ es un grupo de clases de ideales de rayos módulo el conductor $\mathfrak{f}$, se tiene la sucesión exacta

$$1 \longrightarrow I_{\mathfrak{gc}} \longrightarrow I_L \xrightarrow{\mathrm{N}} \frac{H_{L/K}^{\mathfrak{f}}}{P_K^{\mathfrak{f}}} \longrightarrow 1 \qquad (P_K^{\mathfrak{f}} \subseteq H_{L/K}^{\mathfrak{f}} \subseteq I_K^{\mathfrak{f}}),$$

donde $I_{\mathfrak{gc}}$ es el *género principal*:



Más precisamente, $I_K \cong \mathrm{Gal}(K_H/K)$ e $I_{\mathfrak{g}\mathfrak{e}} \cong \mathrm{Gal}(K_H/K_{\mathfrak{g}\mathfrak{e}})$. En particular $I_{\mathfrak{g}\mathfrak{e}} = I_L^{(1-\sigma)}$.

Hasse también probó el *Teorema del género principal* general:

Proposición 8.2.7 (Hasse, 1927). *Sea L/K una extensión cíclica de grado primo de campos numéricos con generador σ y sea $\mathfrak{m}$ un módulus en K. Entonces existe un módulus $\mathfrak{n}$ de L tal que*

(I) $\mathfrak{n}|\mathfrak{m}\mathcal{O}_L$.
(II) $\mathfrak{n}^\sigma = \mathfrak{n}$.
(III) *Para $\beta \in L$ primo relativo a $\mathfrak{n}$, se tiene*

$$\mathrm{N}_{L/K}\,\beta \equiv 1 \text{ mód } \mathfrak{m} \iff \beta = \alpha^{1-\sigma} \text{ mód } \mathfrak{n}$$

para algún $\alpha \in L$. □

Con este resultado, Hasse define el *género principal* H_1 mód $\mathfrak{m}$ en L como el grupo de clase de rayos módulo $\mathfrak{n}$ cuyas normas relativas caen en el grupo de clases de rayos módulo $\mathfrak{m}$ en K.

Teorema 8.2.8 (Hasse). *Sean L/K, $\mathfrak{m}$, $\mathfrak{n}$ como antes. Entonces el género principal $\bar{H}_1$ coincide con el grupo de potencias $1-\sigma$ de las clases de rayos módulo $\mathfrak{n}$ en L.* □

Teorema 8.2.9 (Teorema clásico del género principal). *Sea L/K un extensión cíclica de campos numéricos y sea σ un generador de $\mathrm{Gal}(L/K)$. Entonces $[\mathfrak{a}] \in I_{\mathfrak{g}\mathfrak{e}} \iff \mathrm{N}_{L/K}\,\mathfrak{a} = (\alpha)$ con $\alpha \in K^*$ un residuo nórmico en todos los primos ramificados de L/K, esto es,*

$$\left(\frac{\alpha, L/K}{\mathfrak{p}}\right) = 1 \text{ para todo } \mathfrak{p} \text{ ramificado en } L/K,$$

equivalentemente, $\left(\dfrac{\mathrm{N}_{L/K}\,\mathfrak{a}, L/K}{\mathfrak{p}}\right) = 1 \ \forall\ \mathfrak{p}|\mathfrak{f}(L/K)$. □

Notaciones y convenciones

- $A = \{x \in K \mid v_{\mathfrak{p}}(x) \geq 0, \mathfrak{p} \neq \mathfrak{p}_\infty\}$
- $\mathbb{A}_K$ es el anillo de adèles o reparticiones de K, 210.
- $\mathfrak{a}_{\vec{\alpha}} = \prod_{\mathfrak{p} \in \mathbb{P}_K} \mathfrak{p}^{v_{\mathfrak{p}}(\alpha_{\mathfrak{p}})} \in D_K$ para $\vec{\alpha} \in J_K$, 212
- $\left(\frac{L/K}{\mathfrak{p}}\right) = (L/K, \mathfrak{p}) = (\_, L/K, \mathfrak{p}) = (\_, L/K) = \psi_{L/K}(\mathfrak{p})$ denota el símbolo de Artin, 9
- $\mathrm{Br}(E)$ denota al grupo de Brauer del campo E, 110
- $\mathbb{C}_\infty = \mathbb{C}_p$ completación de la cerradura algebraica de $\mathscr{K}_\infty$
- $\operatorname{car} K$ denota a la característica de K
- $\operatorname{car}(\rho)$ denota la característica de un módulo de Drinfeld
- $c_i(\rho, a)$ denotan a los coeficientes de ρ_a
- $Cl_A = C_A$ grupo de clases de ideales de un dominio Dedekind
- $Cl_S = C_S$ grupo de S–clases ideales
- $\operatorname{coc} D$ el campo de cocientes de un dominio entero D
- $C_K = J_K/K^*$ grupo de clases de idèles del campo global K, 211
- $C_{K,0} = J_{K,0}/K^*$ grupo de clases de idèles de grado 0, 212
- $C_K^{\mathfrak{m}} = J_K^{\mathfrak{m}} K^*/K^* \subseteq C_K$ para un módulus $\mathfrak{m}$, 314
- $C_{K,S}^{\mathfrak{m}} = K^* J_{K,S}^{\mathfrak{m}}/K^*$ para un S–módulus $\mathfrak{m}$, 325
- $Cl_K^{\mathfrak{m}}(\mathcal{O}_S)$ es el cociente de los ideales fraccionarios (divisores) primos relativos a $\mathfrak{m}$ módulo los ideales principales $z\mathcal{O}_S$ con $z \in K^* \cap J_{K,\mathbb{P}_K \setminus \operatorname{sop}(\mathfrak{m})}^{\mathfrak{m}}$ para un un módulus arbitrario $\mathfrak{m}$, $\emptyset \neq S \subseteq \mathbb{P}_K$, 326
- $Cl_L^+ = Cl_L^{\mathrm{ext}}$ grupo de clases extendidos de un campo global, 344
- D_A ideales fraccionarios de un dominio Dedekind A
- D_K grupo de ideales fraccionarios (si K es un campo numérico) o grupo de divisores (si K es un campo global de funciones), 207
- $D_{K,0}$ grupo de divisores de grado 0, K un campo global de funciones, 207
- $D_K^{\mathfrak{m}}$ es el grupo de ideales fraccionales (divisores) primos relativos a la parte finita de un módulus $\mathfrak{m}$, 348
- D_K^S es el grupo de divisores con soporte en el complemento de S, donde S es un conjunto de divisores primos, 278
- $D_{K,0}^S = D_K^S \cap D_{K,0}$, 326

- $D_K(S)$ es el grupo de divisores con soporte en S, donde S es un conjunto de divisores primos
- $D_{K,0}(S)$ grupo de divisores de grado 0 con soporte en S
- $\mathfrak{Dif}_K$ el espacio de diferenciales del campo de funciones K
- $e_{L/K} = e_{L/K}(\mathfrak{P}|\mathfrak{p}) = e(L|K) = e(\mathfrak{P}|\mathfrak{p})$ denota al índice de ramificación de $\mathfrak{P}|\mathfrak{p}$ en la extensión L/K
- $\bar{E}$ cerradura algebraica de un campo E
- $e_{L/K} = e_{L/K}(\mathfrak{P}|\mathfrak{p}) = e(L|K) = e(\mathfrak{P}|\mathfrak{p})$ denota el índice de ramificación de $\mathfrak{P}|\mathfrak{p}$ en la extensión L/K
- $\mathfrak{f}_\mathfrak{p} = \mathfrak{f}_{L/K} = \mathfrak{p}^{c_\mathfrak{p}} = \mathfrak{p}_K^{c_\mathfrak{p}}$, es el conductor local, 155
- $\mathcal{F}_\pi = \{f \in \mathcal{O}_K[[T]] \mid f \equiv \pi T \text{ mód gr } 2, f \equiv T^q \text{ mód } \pi\}$, $\mathcal{O}_K$ el anillo de enteros de un anillo local, 166
- $\left[\dfrac{L/K}{\mathfrak{P}}\right]$ denota al automorfismo de Frobenius, 7
- $F\langle\tau\rangle$ polinomios torcidos
- $\mathrm{Gal}(L/K) = G_{L/K}$ denota el grupo de Galois de la extensión L/K
- $\mathrm{gr}_\mathfrak{p}\,\alpha_\mathfrak{p} = [K(\mathfrak{p}) : \mathbb{F}_q]v_\mathfrak{p}(\alpha_\mathfrak{p}) = [\mathcal{O}_\mathfrak{p}/\mathfrak{p}\colon \mathbb{F}_q] = v_\mathfrak{p}(\alpha_\mathfrak{p}) = f_\mathfrak{p} v_\mathfrak{p}(\alpha_\mathfrak{p}) = \mathrm{gr}\,\mathfrak{p} v_\mathfrak{p}(\alpha_\mathfrak{p})$ para $\vec{\alpha} \in J_K$, 212
- $\mathrm{gr}\,\vec{(\alpha)} = \sum_{\mathfrak{p}\in\mathbb{P}_K} \mathrm{gr}_\mathfrak{p}\,\alpha_\mathfrak{p} = \mathrm{gr}\,\mathfrak{A}_{\vec{\alpha}}$ para $\vec{(\alpha)} \in J_K$, 212
- $H^2(\ |K) = H^2(K^{\mathrm{sep}}|K) = H^2(\mathrm{Gal}(K^{\mathrm{sep}}/K), \mathscr{K})$, K un campo local, 108
- $H^q(L/K) = H^q(\mathrm{Gal}(L/K), \mathscr{K})$, K un campo local, 108
- $H^\mathfrak{m} = (\mathrm{N}_{L/K}\, D_L^\mathfrak{m})P_K^\mathfrak{m}$ para un módulus $\mathfrak{m}$, 18
- $h_A = |\operatorname{Pic}(A)|$ es el número de clase de ideales de A
- h_K es el número de clase de un campo global K
- $I_K = D_K/P_K$ grupo de clases de ideales (divisores) del campo global K, 207
- $I_{K,0}$ grupo de clases de divisores de grado 0 del campo global K de funciones, 207
- $I_K^\mathfrak{m} = D_K^\mathfrak{m}/P_K^\mathfrak{m}$
- J denota la conjugación compleja
- J_K es el grupo de idèles del campo global K, 20, 210
- $J_{K,0} = \{\vec{\alpha} \in J_K \mid \mathrm{gr}\,\vec{\alpha} = \sum_\mathfrak{p} \mathrm{gr}_\mathfrak{p}\,\alpha_\mathfrak{p} = 0\} = \{\vec{\alpha} \in J_K \mid \prod_\mathfrak{p} |\alpha_\mathfrak{p}|_\mathfrak{p} = 1\} \supseteq K^*$ grupo de idèles de grado 0, 212
- $J_K^\mathfrak{m} = \{\alpha \in J_K \mid \alpha \equiv 1 \text{ mód } \mathfrak{m}\} = \prod_{\mathfrak{p}\in\mathbb{P}_K} U_\mathfrak{p}^{(n_\mathfrak{p})}$ donde $\mathfrak{m}$ es un módulus
- $J_K^S = \{\alpha \in J_K \mid \alpha_\mathfrak{p} = 1 \text{ para toda } \mathfrak{p} \in S\}$ donde S es un conjunto de lugares de K
- $J_{K,S} = \prod_{\mathfrak{p}\notin S} U_\mathfrak{p} \times \prod_{\mathfrak{p}\in S} K_\mathfrak{p}^*$ $(J_{K,S} \neq J_K^S)$, donde S es un conjunto finito de lugares
- $J_{K,S}^\mathfrak{m} = \left(\prod_{\mathfrak{p}\in S} K_\mathfrak{p}^* \times \prod_{\mathfrak{p}\notin S} U_\mathfrak{p}^{(n_\mathfrak{p})}\right) \cap J_K$ para $\mathfrak{m}$ un S–módulus
- $\Lambda_{f,n} = \{\lambda \in \Omega \mid v(\lambda) > 0, f^n(\lambda) = 0\}$, 166
- K, $\mathscr{K}$ un campo global de funciones sobre $\mathbb{F}_q$
- K_H campo de clase de Hilbert de un campo global K
- K_{H^+} campo de clase de Hilbert de un campo global K

- K^+ conjunto de elementos totalmente positivos en un campo global K, 343
- $K(\mathfrak{p}) = \tilde{K} = \mathcal{O}_\mathfrak{p}/\mathfrak{p} = \mathbb{F}_q$ el campo residual de K un campo local, 25
- $K_\mathfrak{p}$ es la completación de un campo global K en $\mathfrak{p} \in \mathbb{P}_K$
- $\mathscr{K}_\infty = K_{\mathfrak{p}_\infty}$
- $K_\infty = \mathbb{F}_q(T)_{\mathfrak{p}_\infty}$
- $K^* = (\pi) \times \mathbb{F}_q^* \times U_\mathfrak{p}^{(1)}$, K campo local, 27
- $\bar{K}$ una cerradura algebraica de un campo K
- K^{ab} la máxima extensión abeliana del campo K, 126
- K^{nr} es la máxima extensión no ramificada de K contenida en K^{ab}
- $K^\mathfrak{m}$ campo de clase de $C_K^\mathfrak{m}$, 316
- $K_S^\mathfrak{m}$ es el campo de clase de $C_{K,S}^\mathfrak{m}$
- $K^* \hookrightarrow J_K$ de manera diagonal: $x \mapsto (\ldots, x, x, x \ldots)$, K campo global
- $K = \mathbb{F}_q(T)$
- $\bar{K}$ una cerradura algebraica de K
- $[L : K]_s$ denota el grado de separabilidad de la extensión L/K
- $L^+ = \{x \in L =| \ x$ es totalmente positivo$\}$, 343
- $L_\mathfrak{ge}$ campo de géneros de L
- $L_\mathfrak{gef}$ campo de géneros extendido de L
- $L_{\mathfrak{ge},\mathscr{K}}$ campo de géneros de L con respecto a $\mathscr{K}$
- $L_{\mathfrak{gef},\mathscr{K}}$ campo de géneros extendido de L con respecto a $\mathscr{K}$
- $L_\mathfrak{p}$ denota uno de los campos $\{L_\mathfrak{P}\}_{\mathfrak{P}|\mathfrak{p}}$, para $\mathfrak{p} \in \mathbb{P}_K$, cualquiera pero sólo uno. Es decir, $L_\mathfrak{p}/K_\mathfrak{p}$ denota $L_\mathfrak{P}/K_\mathfrak{p}$ con $L_\mathfrak{P}$ seleccionado arbitrariamente
- Un módulus es $\mathfrak{m} = \prod_{\mathfrak{p} \in \mathbb{P}_K} \mathfrak{p}^{n_\mathfrak{p}}$ donde $n_\mathfrak{p} \geq 0$ para todo $\mathfrak{p} \in \mathbb{P}_K$, $n_\mathfrak{p} = 0$ para casi todo $\mathfrak{p}$, $n_\mathfrak{p} = 0$ si $\mathfrak{p}$ es complejo y $\mathfrak{p} \in \{0, 1\}$ si $\mathfrak{p}$ es real
- $\mu_{L/K} \in H^2(L/K)$ la clase fundamental, $\mathrm{inv}_{L/K}(\mu_{L/K}) = \frac{1}{[L:K]} + \mathbb{Z} \in \left(\frac{1}{[L:K]}\mathbb{Z}\right)/\mathbb{Z}$, 109
- $\mathrm{N}_{L/K} = \mathrm{N}$ denota la norma de L a K, 4
- $\mathrm{N}(\mathfrak{p})$ denota la norma absoluta, 7
- $\mathcal{O}_S = \cap_{\mathfrak{p} \notin S} \mathcal{O}_\mathfrak{p} = \{x \in K^* \mid v_\mathfrak{p}(x) \geq 0$ para toda $\mathfrak{p} \notin S\}$ para $\emptyset \neq S \subseteq \mathbb{P}_K$
- $\mathcal{O}_\mathfrak{p} = \mathcal{O}_K = \{x \in K \mid v_\mathfrak{p}(x) \geq 0\} = \{x \in K \mid |x|_\mathfrak{p} \leq 1\} = \bar{B}(0, 1)$, K un campo local, 25
- P_A ideales principales de un dominio Dedekind A
- P_K grupo de ideales fraccionarios (divisores) principales de un campo global K
- $P_K^\mathfrak{m} = \{(a) \in P_K \mid a \equiv 1 \text{ mód } \mathfrak{m}\}$ para un módulus $\mathfrak{m}$
- $P_{K,\mathfrak{m}}^+ = \{\left(\alpha/\beta\right) \mid \alpha, \beta \in \mathcal{O}_K$ con $\mathrm{mcd}(\alpha\beta, \mathfrak{m}) = 1, \alpha \equiv \beta \text{ mód } \mathfrak{m}$ y α/β es totalmente positivo$\}$, 17
- $P_{K,S}^\mathfrak{m} = K^* \cap J_{K,\mathbb{P}_K \setminus \mathrm{sop}(\mathfrak{m})}^\mathfrak{m}$
- $\mathrm{Pic}(A) = \frac{D_A}{P_A}$ el grupo de Picard de un dominio Dedekind
- $\mathbb{P}_K = \{\mathfrak{p} \mid \mathfrak{p}$ es un lugar de $K\}$ es el conjunto de lugares de K, K un campo global

- $\mathfrak{p} = \{x \in K \mid v_{\mathfrak{p}}(x) > 0\} = \{x \in K \mid |x|_{\mathfrak{p}} < 1\} = B(0,1)$, K es un campo local, 25
- $\mathfrak{p}_\infty$ un lugar fijo de un campo de funciones global K de grado d_∞
- $\pi_\infty = 1/T$ elemento uniformizador del primo infinito $\mathfrak{p}_\infty$ en $K = \mathbb{F}_q(T)$, 339
- $\pi_{\mathfrak{p}} = \pi$ un elemento primo de K, $v_{\mathfrak{p}} = 1$, $\pi \in \mathfrak{p} \setminus \mathfrak{p}^2$, 28
- $\psi_{L/K,\mathfrak{m}} \colon I_K^{\mathfrak{m}} \to \mathrm{Gal}(L/K)$ es el mapeo de Artin, 20
- $\psi_{L/K} \colon K^*/N_{L/K}L^* \xrightarrow[\psi_{L/K}]{\simeq} \mathrm{Gal}(L/K)$, $\psi_{L/K}(a) = (a, L/K)$ mapeo local de Artin o símbolo de la norma residual o símbolo residual nórmico, L/K una extensión abeliana finita de campos locales, 149
- $\Psi(\mathfrak{m}) = \prod_{\mathfrak{p}\in\mathbb{P}_K}[U_{\mathfrak{p}} \colon U_{\mathfrak{p}}^{(n_{\mathfrak{p}})}] = \prod_{\mathfrak{p}\in\mathbb{P}_K}(q^{\mathrm{gr}\,\mathfrak{p}}-1)(q^{(n_{\mathfrak{p}}-1)\,\mathrm{gr}\,\mathfrak{p}})$, para un módulus $\mathfrak{m}$, 324
- $\Psi(\mathfrak{A}) = \left|A/\mathfrak{A}\right|$ donde $\mathfrak{A}$ es un ideal no cero de A
- $\mathbb{Q}_p$ denota al campo de los números p–ádicos
- $\rho \colon A \longrightarrow F\langle\tau\rangle$ un A–módulo de Drinfeld sobre F
- $\rho_K \colon F \to \mathrm{Gal}(\mathrm{ab}\,K/K)$ es el mapeo de reciprocidad o el mapeo local de Artin y $\psi_{L/K} \colon F \to \mathrm{Gal}(L/K)$ es $\psi_{L/K} = \mathrm{rest} \circ \rho_K$, $\mathrm{rest} \colon \mathrm{Gal}(\mathrm{ab}\,K/K) \to \mathrm{Gal}(L/K)$, $\sigma \mapsto \sigma|_L$ para un campo K local o global, $F = J_K$ si K es global y $F = K^*$, si K es local
- $\mathrm{Sig}_L := L^*/L^+$, grupo de signos de un campo global L, 343
- El soporte de $\mathfrak{m}$ es $\{\mathfrak{p} \in \mathbb{P}_K \mid n_{\mathfrak{p}} > 0\}$, donde $\mathfrak{m}$ es un módulus. Si S es un conjunto de divisores primos, el soporte de S es S mismo
- $\mathrm{Spl}(L/K) = \{\mathfrak{p} \in \mathbb{P}_K \mid \mathfrak{p} \text{ se descompone totalmente en } L\}$, 16
- T denota la máxima extensión no ramificada de un campo local K, $T = K^{\mathrm{nr}}$, 180
- TCCG = teorema principal de la teoría de campos de clase globales, 276
- TCCL = Teorema de la Teoría de Campos de Clase Locales, 127
- $\mathrm{Tr}_{L/K} = \mathrm{Tr}$ denota la traza de L a K, 4
- τ el automorfismo de Frobenius sobre $\mathbb{F}_q$: $\tau u = u^q$
- Un S–módulus $\mathfrak{m}$ es tal que $S \cap \mathrm{sop}(\mathfrak{m}) = \emptyset$, donde $S \subseteq \mathbb{P}_K$
- $U_{\mathfrak{p}} = U_K = U_{\mathfrak{p}}^{(0)} = U_K^{(0)} = \{x \in K \mid v_{\mathfrak{p}}(x) = 0\} = \mathcal{O}_{\mathfrak{p}}^*$ el grupo de unidades de $\mathcal{O}_{\mathfrak{p}}$, K campo local, 27
- $U_{\mathfrak{p}}^{(n)} = U_K^{(n)} = 1 + \mathfrak{p}^n = \{x \in K \mid v_{\mathfrak{p}}(x-1) \geq n\} = \{x \in K \mid |x-1|_{\mathfrak{p}} \leq q^{-n}\}$, K campo local, 27
- Para $n \in \mathbb{N}$, W_n denota el grupo de las n–raíces de 1
- $v_\infty = v_{\mathfrak{p}_\infty}$
- v_K denota a la valuación de un campo local K
- $|x|_{\mathfrak{p}} = q^{-v_{\mathfrak{p}}(x)}$, $x_{\mathfrak{p}}$ en un campo local con campo residual de $\mathbb{F}_q$ elementos 25
- $\lceil x_{\mathfrak{p}} \rceil = (\ldots, 1, 1, x_{\mathfrak{p}}, 1, 1, \ldots) \in J_K$, para $x_{\mathfrak{p}} \in K_{\mathfrak{p}}$, K campo global
  $\uparrow$
  $\mathfrak{p}$
- $\mathbb{Z}_p$ es el anillo de los enteros p–ádicos
- $\square$ = terminación de una demostración

☛ $\emptyset$ denota al conjunto vacío

Referencias

1. Albert, A. A., *Cyclic fields of degree p^n over F of characteristic p*, Bulletin A.M.S. **40**, 625–631, (1934).
2. Albu, Toma, *Cogalois theory*, Pure and Applied Mathematics a Dekker Series of Monographs and Textbooks, Inc, New York, 2003.
3. Anglès, Bruno, *On the class group problem for function fields*, Journal of Number Theory **70**, 146–159, (1998).
4. Anglès, Bruno; Jaulent, Jean-François, *Genus Theory of global fields (Théorie des Genres des Corps Globaux)*, Manuscr. Math. **101**, No. 4, 513–532, (2000).
5. Artin, Emil, *Algebraic numbers and algebraic functions*, Providence, RI: AMS Chelsea Publishing, 2006.
6. Artin, Emil; Schreier, Otto, *Eine Kennzeichnung der reell abgeschlossenen Körper*, Hamburg Abhandlungen **5**, 225–231, (1926–1927).
7. Artin, Emil; Tate, John *Class field theory*, de las notas originales de Harvard University Press en 1961, Providence, RI: AMS Chelsea Publishing 2009.
8. Atiyah, Michael Francis; Macdonald, Ian G., *Introduction to commutative algebra*, Addison-Wesley Publishing Co., Reading, Mass.-London-Don Mills, Ont., 1969.
9. Aubry, Yves, *Class number in totally imaginary extensions of totally real function fields*, Finite fields and applications (Glasgow, 1995), 23–29, London Math. Soc. Lecture Note Ser., **233**, Cambridge Univ. Press, Cambridge, 1996
10. Auer, Roland, *Ray class fields of global function fields with many rational places*, Tesis Doctoral, Oldenburg: Carl von Ossietzky Universität Oldenburg, Fachbereich Mathematik, 1999.
11. Auer, Roland , *Ray class fields of global function fields with many rational places*, Acta Arith. **95**, No.2, 97–122 (2000).
12. Bae, Sunghan; Koo, Ja Kyung, *Genus theory for function fields*, J. Austral. Math. Soc. Ser. A **60**, no. 3, 301–310, (1996).
13. Barrera–Mora, Fernando; Rzedowski–Calderón; Villa–Salvador, Gabriel, *On cogalois extensions*, J. Pure Appl. Algebra **76**, 1–11, (1991).
14. Barrera–Mora Fernando; Yslas-Velez, William, *Some results on radical extensions*, J. Algebra **162**, 295–301, (1993).
15. Barreto–Castañeda, Jonny Fernando; Jarquín–Zárate, Fausto; Rzedowski–Calderón, Martha; Villa–Salvador, Gabriel, *Abelian p–extensions and additive polynomials*, International Journal of Mathematics **28**, no. 14, 1–32, (2017).

16. Barreto–Castañeda, Jonny Fernando; Montelongo–Vázquez, Carlos; Reyes–Morales, Carlos Daniel; Rzedowski–Calderón, Martha; Villa–Salvador, Gabriel, *Genus fields of abelian extensions of congruence rational function fields II*, Rocky Mountains Journal of Mathematics **48**, no. 7, 2099–2133, (2018).
17. Bautista–Ancona, Víctor; Rzedowski–Calderón, Martha; Villa–Salvador, Gabriel, *Genus Fields of Cyclic l–extensions of rational function fields*, International Journal of Number Theory **9**, no. 5, 1249–1262, (2013).
18. Brauer, Richard Dagobert; Hasse, Helmut; Noether, Emmy, *Beweis eines Hauptsatzes in der Theorie der Algebren*, J. Reine Angew. Math. **167**, 399–404 (1932).
19. Carlitz, Leonard, *On the representation of a polynomial in a Galois field as the sum of an even number of squares*, Trans. Amer. Math. Soc. **35**, 397–410, (1933).
20. Carlitz, Leonard, *On certain functions connected with polynomials in a Galois field*, Duke Math. J. **1**, 137–168, (1935).
21. Carlitz, Leonard, *A class of polynomials*, Trans. Amer. Math. Soc. **43**, 167–182, (1938).
22. Cassels, John William Scott; Frölich, Albrecht, editors, *Algebraic number theory*, Proceedings of an instructional conference organized by the London Mathematical Society (a NATO Advanced Study Institute) with the support of the International Mathematical Union (held at the University of Sussex, Brighton, September 1–17, 1965), Academic Press, London, 1967.
23. Chapman, Robin J., *Carlitz modules and normal integral bases*, J. Lond. Math. Soc., II. Ser. **44**, No. 2, 250–260, (1991).
24. Chevalley, Claude, *Introduction to the theory of algebraic functions of one variable*, Mathematical Surveys No. **6**, New York, American Mathematical Society XI, 1951.
25. Chevalley, Claude, *Class Field Theory*, Universitat Nagoya, 1954.
26. Chi, Wen–Chen; Li, Anly *Kummer theory of division points over Drinfeld modules of rank one*, J. Pure Appl. Algebra **156**, no. 2–3, 171–185, (2001).
27. Claborn, Luther, *Every abelian group is a class group*, Pacific J. Math. **18**, 219–222, (1966).
28. Clark, David A., *A quadratic field which is Euclidean but not norm-Euclidean*, Manuscr. Math. **83**, No. 3–4, 327–330, (1994).
29. Clement, Rosario, *The genus field of an algebraic function field*, J. Number Theory **40**, no. 3, 359–375, (1992).
30. Conrad, Keith, *History of class field theory*, `http://www.math.uconn.edu/~kconrad/blurbs/gradnumthy/cfthistory.pdf`
31. Deuring, Max, *Lectures on the theory of algebraic functions of one variable*, Lecture Notes in Mathematics **314**, Berlin–Heidelberg–New York, Springer–Verlag, 1973.
32. Drinfel'd, Vladimir G., *Elliptic modules*, Math. USSR, Sb. **23**, 561-592 (1974); translation from Mat. Sb., n. Ser. **94(136)**, 594-627 (1974).
33. Drinfel'd, Vladimir G., *Elliptic modules. II*, Math. USSR, Sb. **31**, 159-170 (1977).
34. Dummit, David S.; Voight, John; Foote, Richard, *The* 2*–Selmer group of a number field and heuristics for narrow class groups and signature ranks of units*, Proc. London Math. Soc. (3) **00**, 1–45, (2018).
35. Fine B.; Rosenberg G., *Number Theory. An introduction via the distribution of primes*, Birkhäuser, 2007.

36. Fröhlich, Albrecht, *The genus field and genus group in finite number fields*, Mathematika **6**, 40–46, (1959).
37. Fröhlich, Albrecht, *The genus field and genus group in finite number fields, II*, Mathematika **6**, 142–146, (1959).
38. Fröhlich, Albrecht, *Central extensions, Galois groups and ideal class groups of number fields*, Contemporary Mathematics, **24**, American Mathematical Society, Providence, RI, 1983.
39. Furuta, Yoshiomi, *The genus field and genus number in algebraic number fields*, Nagoya Math. J. **29**, 281–285, (1967).
40. Galovich, Steven; Rosen, Michael, *The class number of cyclotomic function fields*, J. Number Theory **13**, 363–375, (1981).
41. Galovich, Steven; Rosen, Michael, *Units and class groups in cyclotomic function fields*, J. Number Theory **14**, 156–184, (1982).
42. Gauss, Carl Friedrich, *Disquisitiones arithmeticae*, 1801.
43. Garcia, Arnaldo; Stichtenoth, Henning, *Elementary abelian p–extensions of algebraic function fields*, manuscripta math. **72**, 67–79 (1991).
44. Gekeler, Ernst–Ulrich, *Drinfeld modular curves*, Lecture Notes in Mathematics, **1231**, Springer-Verlag, (1986).
45. Gold, Robert, *Genera in Abelian extensions*, Proc. Am. Math. Soc. **47**, 25–28 (1975).
46. Goss, David, *Basic Structures of Function Fields Arithmetic*, Springer-Verlag, Berlin, (1996).
47. Gras, Georges, *Class field theory. From theory to practice*, Springer Monographs in Mathematics. Berlin: Springer, 2003.
48. Greither, Cornelius; Harrison David Kent, *A Galois correspondence for radical extensions of fields*, J. Pure Appl. Algebra **43**, 257–270, (1986).
49. Hall, Marshal Jr., *Teoría de los grupos*, Editorial F. Trillas, México, 1969.
50. Harari, David, *Galois Cohomology and Class Field Theory*, Springer-Verlag, Switzerland, 2020.
51. Hasse, Helmut, *Theorie der relativ–zyklischen algebraischen Funktionenkörper, insbesondere bei endlichen Konstantenkörper*, J. Reine Angew. Math. **172**, 37–54, (1934).
52. Hasse, Helmut, *Vorlesungen über Zahlentheorie*, Die Grundlehren der mathematischen Wissenschaften, Band **59**, Berlin–Göttingen–Heidelberg, Springer–Verlag, 1950.
53. Hasse, Helmut, *Zur Geschlechtertheorie in quadratischen Zahlkörpern*, J. Math. Soc. Japan **3**, 45–51, (1951).
54. Hasse, Helmut, *Über den Klassenkörper zum quadratischen Zahlkörper mit Discriminant* -47, Acta Arithmetica **IX**, 419–434, (1964).
55. Hasse, Helmut, *Bericht über neuere Untersuchungen und Probleme aus der Theorie der algebraischen Zahlkörper. Teil I: Klassenkörpertheorie. Teil Ia: Beweis zu Teil I. Teil II: Reziprozitätsgesetz*, Würzburg–Wien: Physica–Verlag **135**, (1965).
56. Hasse, Helmut, *Vorlesungen über Klassenkörpertheorie*, Thesaurus Mathematicae, Band **6**, Physica–Verlag, Würzburg, 1967.
57. Hasse, Helmut, *History of Class Field Theory*, in Algebraic Number Theory, J. W. S. Cassels and A. Fröhlich (ed.), Academic Press, New York, 266–279, (1967).
58. Hasse, Helmut, *Eine Folgerung aus H.–W. Leopoldts Theorie der Geschlechter abelscher Zahlkörper*, Math. Nachr. **42**, 261–262, (1969).

59. Hasse, Helmut, *A supplement to Leopoldt's theory of genera in abelian number fields*, J. Number Theory **1**, 4–7, (1969).
60. Hayes, David R., *Explicit class field theory for rational function fields*, Trans. Amer. Math. Soc. **189**, 77–91, (1974).
61. Hayes, David R., *Explicit class field theory in global function fields*, Studies in algebra and number theory, Adv. in Math. Suppl. Stud., **6**, Academic Press, New York-London, 173–217, (1979).
62. Hayes, David R., *Stickelberger elements in function fields*, Compositio Math. **55**, 204–239, (1985).
63. Hayes, David R., *A brief introduction to Drinfel'd modules*, The arithmetic of function fields (Columbus, OH, 1991), Ohio State Univ. Math. Res. Inst. Publ., **2**, de Gruyter, Berlin, 1–32, (1992).
64. Hilbert, David, *Ein neuer Beweis des Kronecker'schen Fundamentalsatzes über Abel'sche Zahlkörper*, Nachr. Ges. Wiss. zu Gottingen **1**, 29-39 (1896/97).
65. Hilbert, David, *The theory of algebraic number fields (Theorie der algebraischen Zahlkörper, Zahlbericht)*, Springer–Verlag, 1998.
66. Hill, Jason, *On finding totally real quintic number fields of minimal signature group rank*, MS Thesis, University of Vermont, Burlington, VT, 2006.
67. Hilton, Peter; Wu, Yel Chiang, *Curso de álgebra moderna*, Editorial Reverté, Barcelona, 1982.
68. Hsu, Chih-Nung, *On Artin conjecture for the Carlitz module*, Compositio Mathematica **106**, 247–266, (1997).
69. Hu, Su; Li, Yan, *The genus fields of Artin–Schreier extensions*, Finite Fields Appl. **16**, no. 4, 255–264, (2010).
70. Ishida, Makoto, *The genus fields of algebraic number fields*, Lecture Notes in Mathematics, Vol. **555**, Springer-Verlag, Berlin-New York, 1976.
71. Ishkhanov, V.V.; Lur´e, B.B.; Faddeev, Dmitriĭ Konstantinovic, *The embedding problem in Galois theory. Transl. from the Russian by N. B. Lebedinskaya*, Translations of Mathematical Monographs **165**, Providence, RI: American Mathematical Society (AMS) xi, 1997.
72. Iwasawa, Kenkichi, *On Γ–extensions of algebraic number fields*, Bull. Amer. Math. Soc. **65**, 183–226, (1959).
73. Iwasawa, Kenkichi, *On the μ–invariants of cyclotomic fields*, Acta Arith. **21**, 99–101, (1972).
74. Iwasawa, Kenkichi, *On Z_l-extensions of algebraic number fields*, Ann. of Math. (2) **98**, 246–326, (1973).
75. Iwasawa, Kenkichi, *Riemann–Hurwitz formula and p-adic Galois representations for number fields*, Tôhoku Math. J. (2) **33**, no. 2, 263–288, (1981).
76. Iwasawa, Kenkichi, *Algebraic functions*, Translated from the 1973 Japanese edition by Goro Kato. Translations of Mathematical Monographs, **118**, American Mathematical Society, Providence, RI, 1993.
77. Iwasawa, Kenkichi, *Local class field theory*, Oxford Mathematical Monographs. New York: Oxford University Press; Oxford: Clarendon Press, 1986.
78. Iwasawa, Kenkichi, *Collected papers. Vol. I, II*, Edited and with a preface by Ichiro Satake, Genjiro Fujisaki, Kazuya Kato, Masato Kurihara and Shoichi Nakajima. With an appreciation of Iwasawa's work in algebraic number theory by John Coates, Springer–Verlag, Tokyo, 2001.
79. Iyanaga, Shokichi, *Zum Beweis des Hauptidealsatze*, Hamb. Abh. **10**, 349–357, (1934).

80. Iyanaga, Shokichi, *The theory of numbers*, North-Holland Mathematical Library. Vol. 8. Amsterdam - Oxford: North- Holland Publishing Company; New York: American Elsevier Publishing Company, 1975.
81. Janusz, Gerald J., *Algebraic number fields*, Academic Press, New York, San Francisco, London, 1973.
82. Janusz, Gerald J., *Algebraic number fields. 2nd ed.*, Providence, RI: American Mathematical Society (AMS), 1996.
83. Johnsen, Karsten, *Lineare Abhängigkeiten von Einheitswurzeln*, Elemente der Mathematik **40**, 57–59, (1985).
84. Kato, Kazuya; Kurokawa, Nobushige; Saito, Takeshi, *Number theory 2. Introduction to class field theory*, Translations of Mathematical Monographs 240; Iwanami Series in Modern Mathematics. Providence, RI: American Mathematical Society (AMS), 2011.
85. Kim, Sungjin, *Nomal Basis Theorem*, `http://www.math.ucla.edu/ i707107 /NBT.pdf`.
86. Kosters, Michiel, *Projective modules over Dedekind Domains*, `http://www.math.leidenuniv.nl/∼edix/tag_2009/michiel_3.pdf`, (2010).
87. Kronecker, Leopold, *Über die algebraisch auflöbaren Gleichungen (I. Abhandlung).*, Ber. K. Akad. Wiss. Berlin, 365–374 (Werke **4**, 1–11), (1853).
88. Lam–Estrada Pablo; Villa–Salvador, Gabriel, *Some remarks on the theory of cyclotomic function fields*, Rocky Mountain Journal of Mathematics **31**, no. 2, 483–502, (2001).
89. Landau, Edmund Georg Hermann, *Handbuch der Lehre von der Verteilung der Primzahlen*, Leipzig u. Berlin: B. G. Teubner. X (1909). Reimpresión AMS Chelsea Publishing, 2000.
90. Lang, Serge, *Algebraic number theory*, Graduate Texts in Mathematics **110**, Springer–Verlag, New York, Berlin, Heidelberg, London, Paris, Tokyo, 1986.
91. Lang, Serge, *Cyclotomic fields I and II, Combined second edition, With an appendix by Karl Rubin*, Graduate Texts in Mathematics, **121**, Springer-Verlag, New York, 1990.
92. Lang, Serge, *Algebra 3rd ed.*, Addison–Wesley Co, Reading, Mass, 1993.
93. Lang, Serge, *Algebraic Number Theory*, 2nd ed., Springer–Verlag, New York, 1994.
94. Lang, Serge; Tate, John, *On Chevalley's proof of Luroths' theomer*, Proceedings of the AMS **3**, no. 4, 621–624, (1952).
95. Lachaud, Gilles; Martin–Deschamps Mireille, *Nombre de points des jacobiennes sur un cops fini*, Acta Arith. **LVI**, 329–340, (1990).
96. Lemmermeyer, Franz, *The Euclidean algorithm in algebraic number fields*, Expo. Math. **13**, No. 5, 385–416 (1995).
97. Lemmermeyer, Franz, *The development of the principal genus theorem*, The shaping of arithmetic after C. F. Gauss's Disquisitiones arithmeticae, 529–561, Springer, Berlin, (2007).
98. Lenstra, Hendrik W. Jr., *Euclid?s algorithm in cyclotomic fields*, J. Lond. Math. Soc., II. Ser. **10**, 457–465 (1975).
99. Lenstra, Hendrik W. Jr., *Euclidean number fields. I. II. III*, Math. Intell. **2**, 6–15, 73–83, 99–103, (1979).
100. Leopoldt, Heinrich–Wolfgang, *Zur Geschlechtertheorie in abelschen Zahlkörpern*, Math. Nachr. **9**, 351–362, (1953).
101. Leopoldt, Heinrich-Wolfgang, *Zur Arithmetik in abelschen Zahlkörpern*, J. Reine Angew. Math. **209**, 54–71, (1962).

102. Lubin, Jonathan, Tate, John, *Formal Complex Multiplication in Local Fields*, Ann. Math. **81**, 380–387, (1965).
103. Madan, Manohar L., *Class Number and Ramification in Fields of Algebraic Functions*, Arch. Math. **XIX**, 121–124, (1968).
104. Madan, Manohar L., *Class number relations in fields of algebraic*, J. Reine Angew. Math. **238**, 89–92 (1969).
105. Madan, Manohar L., *On Class Numbers in Fields of Algebraic Functions*, Arch. Math. **XXI**, 167–171, (1970).
106. Madan, Manohar L.; Queen, Clifford S., *Algebraic function fields of class number one*, Acta Arith. **XX**, 423–432, (1972).
107. Maldonado–Ramírez, Myriam; Rzedowski–Calderón, Martha; Villa–Salvador, Gabriel, *Genus fields of abelian extensions of congruence rational function fields*, Finite Fiels Appl. **20**, 40–54 (2013).
108. Maldonado–Ramírez, Myriam; Rzedowski–Calderón, Martha; Villa–Salvador, G., *Corrigendum to Genus fields of abelian extensions of rational congruence function fields [Finite Fields Appl. 20 (2013) 40–54]*, Finite Fields Appl. **33**, 283–285 (2015).
109. Maldonado–Ramírez, Myriam; Rzedowski–Calderón, Martha; Villa–Salvador, G., *Genus fields of congruence function fields*, Finite Fields Appl. **44**, 56–75, (2017).
110. May, J. Peter, *Notes on Dedekind rings*, `http://www.math.uchicago.edu/~may/MISC/Dedekind.pdf`.
111. McKenzie, R. G., *The ring of cyclotomic integers of modulus thirteen is norm-euclidean*, Ph. D. thesis, Michigan State University, 1988.
112. Milne, James Stuart, *Class Filed Theory*, Version 4.02, March 23, 2013, `https://www.jmilne.org/math/CourseNotes/CFT.pdf`
113. Motzkin, Theodore Samuel, *The Euclidean algorithm*, Bull. Am. Math. Soc. **55**, 1142–1146, (1949).
114. Murty, M. Ram; Esmonde, Jody, *Problems in algebraic number theory*, Second Edition, Graduate Texts in Mathematics **190**, Springer–Verlag, 2005.
115. Narkiewics, Wladyslaw, *Elementary and Analytic Theory of Algebraic Numbers*, Second Edition, Springer–Verlag, Berlin, Heidelberg, New York, London, Paris, Tokyo, Hong Kong, 1990.
116. Narkiewicz, Wladyslaw, *Elementary and analytic theory of algebraic numbers. Third edition*, Springer Monographs in Mathematics. Springer–Verlag, Berlin, 2004.
117. Neukirch, Jürgen, *Class field theory. The Bonn lectures.* Traducción de "Klassenkörpertheorie", Bonn. Math. Schr. **26**, 1967, Berlin: Springer, 2013.
118. Nurkirch, Jürgen, *Neubegründung der Klassen körpertheorie*, Math. Z. **186**, 557–574 (1984).
119. Neukirch, Jürgen, *Class field theory*, Grundlehren der Mathematischen Wissenschaften, **280**, Springer–Verlag, Berlin, Heidelberg, New York, Tokyo, 1986.
120. Neukirch, Jürgen, *Algebraic number theory*, Grundlehren der Mathematischen Wissenschaften. **322**, Springer–Verlag, Berlin, Heidelberg, New York, Barcelona, Hong Kong, London, Milan, Paris, Singapore, Tokyo 1999.
121. Neumann, Olaf, *Two proofs of the Kronecker–Weber theorem "according to Kronecker, and Weber"*, J. Reine Angew. Math. **323**, 105–126 (1981).
122. Peng, Guohua, *The genus fields of Kummer function fields*, J. Number Theory **98** , no. 2, 221–227, (2003).

123. Poonen, Bjorn, *A brief summary of the statements of class field theory*, `http://www-math.mit.edu/%7Epoonen/papers/cft.pdf`, (2012).
124. Ramírez–Ramírez, Elizabeth; Rzedowski–Calderón, Martha; Villa–Salvador, Gabriel, *Genus Fields of Global Fields*, Palestine Journal of Mathematics, **9**, no. 2, 999–1019.
125. Reyes–Morales, Carlos Daniel; Villa–Salvador, Gabriel, *Genus Fields of Kummer ℓ^n–Cyclic Extensions*, `https://arxiv.org/abs/2006.11870`.
126. Ribes, Luis; Zalesskii Pavel, *Profinite groups*, Springer–Verlag, Ergebnisse der Mathematik und ihrer Ganzgebiete Folge 3, **40**, 2000.
127. Roquette, Peter, *Class field theory in characteristic p, its origin and development*, Miyake, Katsuya (ed.), Class field theory – its centenary and prospect. Proceedings of the 7th MSJ International Research Institute of the Mathematical Society of Japan, Tokyo, Japan, June 3–12, 1998. Tokyo: Mathematical Society of Japan. Adv. Stud. Pure Math. **30**, 549–631, (2001).
128. Roquette, Peter, *The Brauer–Hasse–Noether theorem in historical perspective*. Schriften der Mathematisch–Naturwissenschaftlichen Klasse der Heidelberger Akademie der Wissenschaften **15**. Berlin, Springer, (2005).
129. Roquette, Peter, *Contributions to the history of number theory in the 20th century*. Heritage of European Mathematics. Zürich: European Mathematical Society, 2013.
130. Rosen, Michael, *S–units and S–class groups in algebraic function fields*, J. Algebra **26**, 98–108, (1973).
131. Rosen, Michael, *The Hilbert class field in function fields*, Exposition. Math. **5**, no. 4, 365–378, (1987).
132. Rosen, Michael, *Number theory in function fields*, Graduate Texts in Mathematics, **210**, Springer-Verlag, New York, 2002.
133. Rzedowski–Calderón, Martha; Villa–Salvador, Gabriel, *Conductor–discriminant formula for global function fields*, International Journal of Algebra, **5**, no. 32, 1557–1565, (2011).
134. Rzedowski–Calderón, Martha; Villa–Salvador, Gabriel, *Genus fields of Kummer Extensions of Rational Function Fields*, in preparation.
135. Rzedowski–Calderón, Martha; Villa–Salvador, Gabriel Daniel, *Extended Genus Fields of Global Function Fields*, en preparación.
136. Rzedowski–Calderón, Martha; Villa–Salvador, Gabriel Daniel, *Campos Ciclotómicos, tercera versión*, `https://arxiv.org/pdf/1407.3238.pdf`, 14 de diciembre de 2022.
137. Salas Torres, Julio Cesar; Rzedowski–Calderón, Martha, *Caracteres de Dirichlet en campos de funciones*, Soc. Mat. Mexicana, Aportaciones Mat. Comun., **36**, 127–144, (2006).
138. Salas Torres, Julio Cesar; Rzedowski–Calderón, Martha; Villa Salvador, Gabriel, *Tamely ramified extensions and cyclotomic fields in characteristic p*, Palestine Journal of Mathematics **2** (1), 1–5, (2013).
139. Salas Torres, Julio Cesar; Rzedowski–Calderón, Martha; Villa Salvador, Gabriel, *Artin–Schreier and Cyclotomic Extensions*, JP Journal of Algebra, Number Theory and Applications **30**, No. 2, 173–190, (2013).
140. Salas Torres, Julio Cesar; Rzedowski–Calderón, Martha; Villa Salvador, Gabriel, *A combinatorial proof of the Kronecker–Weber Theorem in positive characteristic*, Finite Fields Appl. **26**, 144–161, (2014).

141. Sánchez–Mirafuentes, Marco; Villa–Salvador, Gabriel, *Kummer Type Extensions in Function Fields*, International Journal of Algebra **7**, no. 4, 157–166, (2013).
142. Sánchez–Mirafuentes, Marco; Villa–Salvador, Gabriel, *Radical Extensions for the Carlitz Module*, J. Algebra **398**. 284–302, (2014).
143. Sánchez Mirafuentes, Marco; Salas–Torres, Julio Cesar; Villa–Salvador, Gabriel, *Cogalois Theory and Drinfeld Modules*, Journal of Algebra and Its Applications **19**, no. 1, 2050001 (18 pages), (2020).
144. Schmid, Hermann Ludwig, *Zyklische algebraische Funktionenkörper vom Grade p^n über endlichem Konstantenkörper der Characteristik p*, J. Reine Angew. Math. **175**, 108–123, (1936).
145. Schmid, Hermann Ludwig, *Zur Arithmetik der zyklischen p-Körper*, J. Reine Angew. Math. **176**, 161–167 (1937).
146. Schultheis, Fred, *Carlitz–Kummer function fields*, J. Number Theory **36**, 133–144, (1990).
147. Sémirat, Stéphan, *Class number one problem for imaginary function fields: the cyclic prime power case*, J. Number Theory **84**, 166–183, (2000).
148. Sémirat, Stéphan, *Cyclotomic function fields with ideal class number one*, J. Algebra **236**, 376–395, (2001).
149. Serre, Jean–Pierre, *Cohomologie Galoisienne*, Lecture Notes in Mathematics **5.** Springer, Berlin–Heidelberg–New York, 1964.
150. Serre, Jean–Pierre, *Local class field theory*, Algebraic Number Theory (Proc. Instructional Conf., Brighton, 1965) pp. 128–161 Thompson, Washington, D.C., (1967).
151. Serre, Jean–Pierre *Local fields*, Graduate Texts in Mathematics **67**, New York–Hedelberg–Berlin, Springer–Verlag, 1979.
152. Serre, Jean–Pierre, *Algebraic Groups and Class Fields*, Springer–Verlag, 1988.
153. Stark, Harold M., *On the gap in a theorem of Heegner*, J. Number Theory **1**, 16–27, (1969).
154. Stichtenoth, Henning, *Algebraic function fields and codes. Second edition*, Springer–Verlag, Graduate Texts in Mathematics **254**, Berlin–Heidelberg–New York, 2009.
155. Takagi, Teiji, *Über eine Theorie des relativ Abelschen Zahlkörpers*, Journ. Coll. of Science Tôkyo **41**, 1–33, (1920).
156. Takagi, Teiji, *Über das Reziprozitätsgesetz in einem beliebigen algebraischen Zahlkörper*, Journ. Coll. of Science Tôkyo **44**, 1–50, (1922).
157. Tate, John Torrence, *Global class field theory*, Algebraic Number Theory (Proc. Instructional Conf., Brighton, 1965) pp. 162–203 Thompson, Washington, D.C., (1967).
158. Thakur, Dinesh S., *Function Field Arithmetic*, World Scientific, (2004).
159. Villa–Salvador, Gabriel, *Introducción a la teoría de las funciones algebraicas*, Fondo de Cultura Económica, México, 2003.
160. Villa–Salvador, Gabriel, *Topics in the theory of algebraic function fields*, Mathematics: Theory & Applications, Birkhäuser Boston, Inc., Boston, MA, 2006.
161. Villa–Salvador, Gabriel, *An elementary proof of the conductor–discriminant formula*, International Journal of Number Theory, Vol. **6**, No. 5, 1191–1197, (2010).

162. Villa–Salvador, Gabriel, *Analog of the Kronecker–Weber theorem in positive characteristic*, in Algebraic Curves and Finite Fields. Cryptography and Other Applications, Radon Series on Computational and Applied Mathematics **16**, Harald Niederreiter, Alina Ostafe, Daniel Panario, Arne Winterhof (Eds.), 213–237, De Gruyter 2014.
163. Washington, Lawrence C, *Class numbers and $\mathbb{Z}_p$–extensions*, Math. Ann. **214**, 177–193, (1975).
164. Washington, Lawrence C, *The non p–parts of the class numbers in a cyclotomic $\mathbb{Z}_p$–extensions*, Inventiones Math. **49**, 87–97, (1978).
165. Washington, Lawrence C, *Introduction to cyclotomic fields, Second edition*, Graduate Texts in Mathematics, **83**, Springer-Verlag, New York, 1997.
166. Weber, Heinrich Martin, *Theorie der Abelschen Zahlkörper*, Acta Math. **8**, 193–263, (1886).
167. Weil, André, *Basic number theory*, Classics in Mathematics. Berlin: Springer–Verlag, 1995.
168. Weiss, Edwin, *A Deflation Map*, Journal of Mathematics and Mechanics **8**, No. 2, 309–329, (1959).
169. Weiss, Edwin, *Cohomology of Groups*, Academic Press, New York and London, 1969.
170. Witt, Ernst, *Konstruktion von galoisschen Körpern der Charakteristik p zu vorgegebener Gruppe der Ordnung p^f*, J. Reine Angew. Math. **174**, 237–245, (1936).
171. Witt, Ernst, *Zyklische Körper und Algebren der Charakteristik p vom Grad p^n. Struktur diskret bewerter perfekter Körper mit vollkommenem Restklassenkörper der Characteristik p*, J. Reine Angew. Math. **176**, 126–140, (1936).
172. Wittmann, Christian, *l–class groups of cyclic function fields of degree l*, Finite Fields Appl. **13**, 327–347, (2007).
173. Wu, Qingquan; Scheidler, Renate, *The ramification groups and different of a compositum of Artin–Schreier extensions*, International Journal of Number Theory **6**, no. 7, 1541–1564, (2010).
174. Yamamura, Ken. *he determination of the imaginary abelian number fields with class number one*, Math. Comput. **62**, No. 206, 899–921, (1994).
175. Zhang, Xianke, *A simple construction of genus fields of abelian number fields*, Proc. Amer. Math. Soc. **94**, no. 3, 393–395, (1985).
176. Zaldívar–Cruz, Felipe, *Campos locales*, Universidad Autónoma Metropolitana, Unidad Iztapalapa, 2001.
177. Zaldívar–Cruz, Felipe, *Cohomología de Galois de campos locales*, Aportaciones Matemáticas, Texto Nivel Avanzado **17**, Sociedad Matemática Mexicana, 2001.
178. Zywina, David, *Explicit class field theory for global function fields*, J. Number Theory **133**, No. 3, 1062–1078, (2013).

Índice alfabético