UNIVERSIDAD DE BUENOS AIRES
FACULTAD DE CIENCIAS EXACTAS Y NATURALES
DEPARTAMENTO DE MATEMÁTICA

Tesis de Licenciatura

TEORÍA DE CUERPOS DE CLASES

Lucio GUERBEROFF

Director: Ariel Pacetti

Febrero de 2007

A Andrea.

Introducción

El objetivo de este trabajo es presentar la teoría global de cuerpos de clases. A grandes rasgos, esta teoría relaciona la aritmética de un cuerpo de números con sus extensiones de Galois. Más específicamente, la teoría provee una descripción de los grupos de Galois de extensiones (abelianas) en términos del cuerpo de base, además de una clasificación completa de tales extensiones, y una descripción de la manera en que los primos de un cuerpo de números se factorizan en ellas. La historia de la teoría de cuerpos de clases es más que interesante; recomendamos el artículo de H. Hasse en [CaF67] o el libro de S. Lang [Lan94]. Los principales partícipes de su inicio y desarrollo son L. Kronecker, H. Weber, D. Hilbert, T. Takagi, E. Artin, H. Hasse, C. Chevalley, J. Tate y otros.

El análisis aritmético de las ecuaciones algebraicas consiste en resolver las ecuaciones teniendo en cuenta el mínimo cuerpo o anillo al cual pertenecen. Si el cuerpo de base es $\mathbb{Q}$, el cuerpo de los números racionales, este análisis lleva al estudio de sus extensiones finitas, que son llamadas *cuerpos de números*. Uno de los objetivos principales de la teoría de números es "entender" el grupo de Galois absoluto $\mathcal{G}_K = \mathrm{Gal}(K^{al}/K)$ de un cuerpo de números K, por ejemplo $\mathbb{Q}$, donde K^{al} es una clausura algebraica de K. La teoría de cuerpos de clases nos brinda una respuesta bastante satisfactoria con respecto a la abelianización $\mathcal{G}_K^{ab}$.

El corazón de la teoría es la *ley de reciprocidad de Artin*, probada por él mismo en 1927. Si K es un cuerpo de números y L/K es una extensión finita y abeliana, la ley de reciprocidad establece un isomorfismo entre cierto grupo de clases de ideales generalizados y $\mathrm{Gal}(L/K)$. El nombre se debe a que describe la manera en que un primo de K se factoriza en L, y generaliza las leyes de reciprocidad conocidas hasta entonces, como la cuadrática o la cúbica. La manera de demostrar esta ley consiste, esencialmente, en probar que ambos grupos tienen el mismo orden y que la aplicación, llamada *mapa de Artin*, es suryectiva. Para ello, se prueban las dos desigualdades correspondientes, y una de ellas se puede probar usando métodos analíticos, que es como Artin lo hizo.

Asimismo, existe una teoría *local* de cuerpos de clases, en la cual K se reemplaza por un cuerpo local. Históricamente, la teoría local se dedujo de la teoría global; Hasse probó que la teoría global se puede deducir de la local, y propuso desarrollar la teoría local de manera independiente. Esto finalmente fue logrado, y el enfoque moderno de la teoría de cuerpos de clases sigue esta línea: desarrollar la teoría local y deducir de ésta la global. Este punto de vista es el que abordaremos en esta tesis.

En 1936, C. Chevalley introdujo el grupo de *idèles* de K, que se forma a partir de las completaciones de K en las distintas valuaciones. Con ellos se puede formular la teoría de

cuerpos de clases de manera más unificada, incluyendo a las extensiones infinitas y clarificando la relación entre la teoría global y la local. En 1940, Chevalley prueba, de manera puramente algebraica, utilizando cohomología de grupos, la desigualdad que en un principio había sido probada con métodos analíticos. Ésta es la demostración que expondremos aquí.

La teoría de cuerpos de clases sólo tiene en cuenta extensiones abelianas. Para las extensiones no abelianas, en su momento ni siquiera se sabía bien qué debía enunciarse, hasta que hace unos 30 años, R. Langlands inició un vasto programa que incluiría como casos particulares las buscadas leyes de reciprocidad no abelianas. Hoy por hoy, hay muy pocas demostraciones para el caso de cuerpos de números, y las conjeturas abundan. Una manera de estudiar $\mathcal{G}_K$, según la filosofía "Tannakiana", es a través sus representaciones de dimensión finita. Desde este punto de vista, la teoría de cuerpos de clases resuelve el caso de las representaciones de dimensión 1. En general, para entender las representaciones de cualquier dimensión, se le asocian ciertos invariantes (funciones L), y las conjeturas principales establecen relaciones entre éstos y otros invariantes ("automorfos") que tienen propiedades ya estudiadas y establecidas, lo cual permite estudiar dichas representaciones. Esta idea fue originariamente de Artin, y fue fundamental para el tratamiento analítico de la teoría de cuerpos de clases. En éste, la teoría es esencialmente equivalente a que esta correspondencia para dimensión 1 es cierta; las funciones L, en este caso, fueron estudiadas originariamente por Hecke y otros, hasta que Tate, en su tesis de doctorado de 1950, dio un tratamiento innovador utilizando análisis armónico en los grupos de adèles e idèles. En esta tesis no estudiaremos la parte analítica de la teoría. Para estudiar estos enunciados y ver su equivalencia con la teoría aquí expuesta, recomendamos el libro de L. Goldstein ([Gol71]).

Organización El presente trabajo está organizado de la siguiente manera.

En el primer capítulo, presentamos los resultados preliminares básicos sobre los dos puntos de vista que tiene la teoría de números algebraica, vale decir, dominios de Dedekind (punto de vista de ideales) y valuaciones.

En el segundo capítulo, investigamos los distintos tipos de valuaciones que tiene un cuerpo de números y qué sucede con ellas en las extensiones.

En el tercer capítulo, tratamos los adèles e idèles, definiéndolos, probando sus principales propiedades y deduciendo teoremas clásicos de teoría de números a partir de ellas, como la finitud del grupo de clases y el teorema de Dirichlet sobre las unidades.

El cuarto capítulo es el principal. En él enunciamos los teoremas centrales de la teoría global de cuerpos de clases en términos de ideales, y formulamos una reinterpretación de estos teoremas en términos de idèles, debida a Chevalley. Posponemos las demostraciones de estos teoremas hasta el séptimo capítulo. Incluimos también, como corolario de la teoría, una demostración del Teorema de Kronecker-Weber, que afirma que toda extensión abeliana de los racionales es una extensión ciclotómica.

En el quinto capítulo, presentamos un desarrollo de la cohomología de grupos, herramienta necesaria para demostrar los teoremas del cuarto capítulo.

El sexto capítulo es un resumen que contiene los resultados principales de la teoría local de cuerpos de clases. En general, no incluimos las demostraciones por una cuestión de extensión.

En el séptimo capítulo, llevamos a cabo todas las demostraciones de los teoremas del capítulo cuatro. Esencialmente todas se reducen a probar que ciertos grupos de cohomología tienen ciertas propiedades, que se deducen de las propiedades correspondientes de la teoría local. Es importante la reducción que se hace a las extensiones ciclotómicas, algo que ya estaba presente en la demostración original de Artin.

Agradecimientos Varias personas han influido a lo largo de la escritura de esta tesis. Con algunas de ellas he mantenido conversaciones que me han ayudado a comprender una gran variedad de temas, no todos relacionados con los aquí expuestos, y otras han influido más indirectamente brindándome consejos y colaboración en otros aspectos. Olvidándome de muchas, expreso mis agradecimientos a N. Ojeda Bär, R. Miatello, M. Harris, E. Erbaro, T. Krick, N. Sirolli y F. Quallbrunn.

Quisiera agradecer especialmente a A. Pacetti por dirigir esta tesis de licenciatura y por sus innumerables sugerencias y correcciones. Agradezco también en este último aspecto a A. Márquez.

Finalmente, quiero agradecer a mis padres, A. Guerberoff e I. Fisicaro, por el apoyo brindado durante todos estos años.

Lucio Guerberoff
Buenos Aires, Argentina

Contenidos

Capítulo 1

Preliminares

1.1. Dominios de Dedekind

En un curso básico de teoría de números algebraica se prueba que si K es un cuerpo de números entonces $\mathcal{O}_K$ (el anillo de enteros algebraicos) es un dominio íntegro (que no es un cuerpo) que cumple las siguientes tres propiedades:

(1) $\mathcal{O}_K$ es Noetheriano;

(2) $\mathcal{O}_K$ es íntegramente cerrado;

(3) todo ideal primo no nulo de $\mathcal{O}_K$ es maximal.

Un dominio íntegro A (no cuerpo) que cumpla esas tres propiedades se llama un *dominio de Dedekind*. En esta sección, resumiremos la teoría de dominios de Dedekind que necesitaremos. Omitiremos la mayoría de las demostraciones, las cuales se pueden encontrar en [Lan94] o en [Mar77].

Notemos que la propiedad (3) es equivalente a que no haya relación de contención entre ideales primos no nulos distintos.

Todo dominio de ideales principales es un dominio de Dedekind; la recíproca no es cierta, y es fácil encontrar ejemplos de dominios de Dedekind que no son dominios de factorización única, menos aún principales. Sin embargo, los dominios de Dedekind tienen una importante propiedad (de hecho, se puede ver que esta propiedad los caracteriza), que nos dice que todo *ideal* no nulo (y propio) se puede escribir, de manera única, como un producto de ideales primos no nulos a ciertas potencias.

Dados dos ideales $\mathfrak{a}$, $\mathfrak{b}$ de A, decimos que $\mathfrak{a}|\mathfrak{b}$ ($\mathfrak{a}$ *divide* a $\mathfrak{b}$) si existe un ideal $\mathfrak{c}$ tal que

$$\mathfrak{b} = \mathfrak{a}\mathfrak{c}.$$

Sea A un dominio íntegro y K su cuerpo de fracciones. Un *ideal fraccionario* $\mathfrak{a}$ de A es un A-submódulo de K, tal que existe un $d \in K$, $d \neq 0$ con $d\mathfrak{a} \subset A$. Notemos que podemos tomar $d \in A$. Si A es Noetheriano, entonces $d\mathfrak{a}$, y, por lo tanto, $\mathfrak{a}$, es finitamente generado.

Si $\mathfrak{a}$ es un ideal de A entonces es un ideal fraccionario. A estos ideales fraccionarios los llamaremos *ideales enteros*.

La siguiente proposición es de demostración inmediata.

Proposición 1.1.1. *Sea A un dominio Noetheriano. Entonces, dado $\mathfrak{a} \subset K$, son equivalentes:*

(I) $\mathfrak{a}$ *es un ideal fraccionario*;

(II) $\mathfrak{a}$ *es un A-submódulo de K finitamente generado*;

(III) $\mathfrak{a} = x\mathfrak{b}$ *para ciertos $x \in K^\times$ y $\mathfrak{b}$ ideal entero*.

Dado $a \in K$, escribimos (a) para referirnos al ideal fraccionario generado por a, es decir, al A-submódulo de K generado por a; efectivamente es un ideal fraccionario (consiste de todos los elementos de la forma ax con $x \in A$). Notemos que si $a \in A$, esto coincide con el ideal generado por a en A.

Sea I_K el conjunto de ideales fraccionarios no nulos de A (para ser rigurosos, deberíamos notarlo con I_A; haremos el abuso de notación refiriéndonos al dominio correspondiente en los casos necesarios) . Al igual que en los ideales enteros, se pueden multiplicar naturalmente, y el ideal fraccionario A es un elemento unidad. Se tiene una aplicación natural $\mathrm{id} : K^\times \to I_K$, $a \mapsto (a)$.

Teorema 1.1.2. *Sea A un dominio de Dedekind. Entonces todo ideal no nulo y propio de A se factoriza, de manera única, como producto de ideales primos no nulos, e I_K es un grupo libre sobre el conjunto de ideales primos no nulos.*

Para medir cuán lejos está un dominio de Dedekind de ser un dominio principal, lo que naturalmente se hace es "dividir" por los ideales principales. Resulta que el conjunto de los ideales enteros no nulos no es un grupo, y que debemos considerar I_K, el grupo de ideales fraccionarios no nulos. Sea P_K el subgrupo de I_K formado por los ideales fraccionarios *principales* no nulos, es decir, los ideales de la forma (a), con $a \in K^\times$. El grupo I_K/P_K se llama el *grupo de clases de ideales* de A, y se lo denota por $Cl(A)$. Cuando A esté sobreentendido, lo notaremos por $Cl(K)$, y lo llamaremos el grupo de clases de ideales de K. En un primer curso de teoría algebraica de números, se demuestra (¡en general utilizando métodos geométricos!) que $Cl(\mathcal{O}_K)$ es finito. En el caso de cualquier dominio de Dedekind A, esto deja de ser cierto; definimos el *número de clases de ideales* de A (o de K) como el cardinal del grupo de clases, en el caso en que sea finito.

Veremos qué sucede cuando tenemos un dominio de Dedekind A y una extensión de su cuerpo de fracciones K.

Recordemos que, si A es un dominio íntegro contenido en un cuerpo L, el conjunto B formado por los elementos enteros sobre A es un anillo, llamado la *clausura entera* de A en L. Además, si K es el cuerpo de fracciones de A, L es una extensión finita y separable de K y x es entero sobre A entonces $\mathrm{N}_{L/K}(x)$ y $\mathrm{Tr}_{L/K}(x)$ también lo son (al ser productos y sumas de conjugados de x, que son enteros sobre A). Se deduce de manera similar que el polinomio minimal de x sobre K tiene coeficientes enteros sobre A. Además, si x es algebraico sobre K entonces existe un $a \in A$, $a \neq 0$, tal que ax es entero sobre A.

Sea A un dominio de Dedekind. Sea L/K una extensión finita y separable, donde K es el cuerpo de fracciones de A. Entonces la clausura entera de A en L es un A-módulo finitamente generado. Esto permite probar el siguiente resultado.

Teorema 1.1.3. *Sea A un dominio de ideales principales, y L/K una extensión finita y separable de grado n, donde K es el cuerpo de fracciones de A. Entonces la clausura entera de A en L es un A-módulo libre de rango n.*

Dem. Como A-módulo, la clausura entera es sin torsión, y al ser finitamente generado, se sigue que es un A-módulo libre. Es claro que su rango es n. □

Este teorema muestra, por ejemplo, que el anillo de enteros de un cuerpo de números de grado n es un grupo abeliano libre de rango n.

A partir de ahora, $\mathcal{O}_K$ será un dominio de Dedekind y K su cuerpo de fracciones. Sea B un anillo que contiene a $\mathcal{O}_K$. Si $\mathfrak{p}$ es un ideal primo de $\mathcal{O}_K$ y $\mathfrak{P}$ un ideal primo de B, decimos que $\mathfrak{P}$ *está sobre* $\mathfrak{p}$ si $\mathfrak{P} \cap \mathcal{O}_K = \mathfrak{p}$. En ese caso, escribimos $\mathfrak{P}|\mathfrak{p}$, y también decimos que $\mathfrak{P}$ divide a $\mathfrak{p}$. Si B es entero sobre $\mathcal{O}_K$ entonces $\mathfrak{p}B \neq B$, y existe un ideal primo $\mathfrak{P}$ de B sobre $\mathfrak{p}$. Además, $\mathfrak{P}$ es maximal si y sólo si $\mathfrak{p}$ lo es.

Teorema 1.1.4. *Sea L/K una extensión finita y separable, y sea B la clausura entera de $\mathcal{O}_K$ en L. Entonces B es un dominio de Dedekind.*

Dem. Es claro que B es íntegramente cerrado. Si $\mathfrak{P}$ es un ideal primo no nulo de B, está sobre un ideal primo no nulo $\mathfrak{p}$ de $\mathcal{O}_K$, que es entonces maximal. Luego, $\mathfrak{P}$ lo es. Falta ver que B es Noetheriano. Como $\mathcal{O}_K$ es Noetheriano e íntegramente cerrado, B es un $\mathcal{O}_K$-módulo finitamente generado. Luego, todo ideal de B es finitamente generado sobre $\mathcal{O}_K$ (al ser un submódulo de un $\mathcal{O}_K$-módulo finitamente generado con $\mathcal{O}_K$ Noetheriano), y, más aún, sobre B. □

Observación 1.1.5. El teorema es válido sin asumir que L/K sea separable. El caso general se trata separando la extension en $K \subset E \subset L$, donde E/K es separable y L/E es puramente inseparable (es decir, E es la clausura separable de K en L). Para una demostración, ver [Jan96].

Veamos qué pasa ahora cuando consideramos extensiones de Galois de K. En lo sucesivo L/K sera una extensión finita y separable. Con $\mathcal{O}_L$ notaremos a la clausura entera de $\mathcal{O}_K$ en L. Si $\mathfrak{p}$ es un ideal primo de cualquiera de estos dos anillos, una letra minúscula con tal subíndice denotará al *cuerpo residual* correspondiente. Por ejemplo, si $\mathfrak{p}$ es un ideal primo de $\mathcal{O}_K$, notaremos

$$k_{\mathfrak{p}} = \mathcal{O}_K/\mathfrak{p}.$$

En el caso en que L/K sea de Galois, $\mathrm{Gal}(L/K)$ actúa transitivamente sobre los primos de $\mathcal{O}_L$ que están sobre uno dado de $\mathcal{O}_K$; es decir, si $\mathfrak{p}$ es un ideal primo de $\mathcal{O}_K$ y $\mathfrak{P}, \mathfrak{Q}$ son ideales primos sobre $\mathfrak{p}$ en $\mathcal{O}_L$ entonces existe $\sigma \in \mathrm{Gal}(L/K)$ tal que $\sigma\mathfrak{P} = \mathfrak{Q}$. Además, existen sólo finitos ideales primos sobre $\mathfrak{p}$ (aquí no es necesario que la extensión sea de Galois).

Sea $G = \mathrm{Gal}(L/K)$. Dado $\sigma \in G$, es claro que $\sigma\mathcal{O}_L = \mathcal{O}_L$. Sea $\mathfrak{p}$ un ideal primo de $\mathcal{O}_K$ y sea $\mathfrak{P}$ un ideal primo de $\mathcal{O}_L$ sobre $\mathfrak{p}$. Sabemos que $\sigma\mathfrak{P}$ es otro ideal primo de $\mathcal{O}_L$, también sobre $\mathfrak{p}$. Dado $\mathfrak{P}$ un ideal primo de $\mathcal{O}_L$, definimos el *grupo de descomposición de* $\mathfrak{P}$ como

$$D(\mathfrak{P}) = \{\sigma \in G : \sigma(\mathfrak{P}) = \mathfrak{P}\}.$$

Cada $\sigma \in D(\mathfrak{P})$ induce un morfismo $\overline{\sigma} : l_{\mathfrak{P}} \to l_{\mathfrak{P}}$, que deja fijo al subcuerpo $k_{\mathfrak{p}}$. Al ser $D(\mathfrak{P})$ un subgrupo de $\mathrm{Gal}(L/K)$, podemos considerar L^D el cuerpo fijo por este subgrupo, llamado el *cuerpo de descomposición* de $\mathfrak{P}$. Sea $\mathcal{O}_L^D$ la clausura entera de $\mathcal{O}_K$ en L^D, que no es otra cosa que $\mathcal{O}_L \cap L^D$, y sea $\mathfrak{Q} = \mathfrak{P} \cap \mathcal{O}_L^D$, que es un ideal primo de $\mathcal{O}_L^D$. El ideal primo $\mathfrak{P}$ está sobre $\mathfrak{Q}$, y, además, es el único con esta propiedad pues $D(\mathfrak{P}) = \mathrm{Gal}(L/L^D)$ actúa transitivamente sobre los primos que están sobre un mismo primo en L^D.

Proposición 1.1.6. *La extensión L^D/K es la subextensión de L/K más chica tal que $\mathfrak{P}$ es el único ideal primo sobre $\mathfrak{P} \cap L^D$ (que es un ideal primo de $\mathcal{O}_L \cap L^D$).*

Demostración. Sea F como dice la proposición, y sea $H = \mathrm{Gal}(L/F)$. Sea $\mathfrak{q} = \mathfrak{P} \cap F$. Sabemos que todos los primos de $\mathcal{O}_L$ que están sobre $\mathfrak{q}$ son conjugados por elementos de H. Como hay sólo un primo, vemos que H deja $\mathfrak{P}$ fijo, es decir, $H \subset D(\mathfrak{P})$. Así, $F \supset L^D$. □

Con respecto a la extensión $l_{\mathfrak{P}}/k_{\mathfrak{p}}$, se prueba que se trata de una extensión normal. Volvamos por ahora al caso en que L/K no es necesariamente de Galois.

Proposición 1.1.7. *Sea $\mathfrak{P}$ un primo de $\mathcal{O}_L$ sobre $\mathfrak{p}$. La extensión $l_{\mathfrak{P}}/k_{\mathfrak{p}}$ es finita.*

Dem. Es obvio al ser $\mathcal{O}_L$ un $\mathcal{O}_K$-módulo finitamente generado. □

Si L/K es de Galois, llamaremos $G(\mathfrak{P}) = \mathrm{Gal}(l_{\mathfrak{P}}/k_{\mathfrak{p}})$. El núcleo del morfismo $D(\mathfrak{P}) \to G(\mathfrak{P})$ se llama el *grupo de inercia* de $\mathfrak{P}$, denotado por $I(\mathfrak{P})$. Es un subgrupo normal de $D(\mathfrak{P})$ y consiste en los automorfismos de L sobre K que inducen el automorfismo trivial en el cuerpo residual, es decir, los σ tales que $\sigma y \equiv y (\mathrm{mod}\, \mathfrak{P})$ para todo $y \in \mathcal{O}_L$. Su cuerpo fijo, L^I, se llama el *cuerpo de inercia* de $\mathfrak{P}$.

Uno de los problemas generales de la teoría de números algebraica es caracterizar cómo se factorizan los ideales primos de $\mathcal{O}_K$ en extensiones. Sea $\mathfrak{p}$ un ideal primo de $\mathcal{O}_K$, y sea

$$\mathfrak{p}\mathcal{O}_L = \mathfrak{P}_1^{e_1} ... \mathfrak{P}_g^{e_g}$$

la factorización de $\mathfrak{p}$ en $\mathcal{O}_L$, con los $\mathfrak{P}_i$ distintos (de manera que $\mathfrak{P}$ está sobre $\mathfrak{p}$ si y sólo si aparece en este producto). Definimos el *índice de ramificación de $\mathfrak{P}_i$ sobre $\mathfrak{p}$* (o *grado de ramificación*) como $e(\mathfrak{P}_i|\mathfrak{p}) = e_i$. Decimos que $\mathfrak{p}$ *ramifica* en $\mathcal{O}_L$ (o en L) si alguno de los e_i es mayor que 1. En caso contrario decimos que $\mathfrak{p}$ es *no ramificado* en $\mathcal{O}_L$. Si $\mathfrak{P}$ es un primo de $\mathcal{O}_L$, se define $e_{\mathfrak{P}} = e(\mathfrak{P}|\mathfrak{p})$, donde $\mathfrak{p} = \mathfrak{P} \cap \mathcal{O}_K$. También notaremos $e(\mathfrak{P}|\mathfrak{p}) = 0$ si $\mathfrak{P}$ no está sobre $\mathfrak{p}$.

Dado $\mathfrak{P}$ sobre $\mathfrak{p}$, definimos también el *índice* o *grado de inercia* de $\mathfrak{P}$, notado $f_{\mathfrak{P}}$ o $f(\mathfrak{P}|\mathfrak{p})$, como el grado de la extensión $l_{\mathfrak{P}}/k_{\mathfrak{p}}$ (sabemos que es finita por la Proposición 1.1.7).

Se tiene la siguiente fórmula:

$$[L : K] = \sum_{i=1}^{r} e_i f_i.$$

Decimos que $\mathfrak{p}$ se parte completamente si $r = [L : K]$. Por la última fórmula, esto ocurre si y sólo si $f_{\mathfrak{P}} = e_{\mathfrak{P}} = 1$ para todo $\mathfrak{P}|\mathfrak{p}$.

La fórmula se simplifica en el caso de extensiones de Galois: todos los $e_{\mathfrak{P}}$ (para $\mathfrak{P}|\mathfrak{p}$) son iguales a un cierto número e, y los $f_{\mathfrak{P}}$ (para $\mathfrak{P}|\mathfrak{p}$) son iguales a un cierto número f, de manera que $[L:K] = efr$.

Los índices de ramificación y de inercia se comportan bien respecto a torres de extensiones.

Proposición 1.1.8. *Sea $K \subset L \subset M$ una torre de extensiones finitas y separables, y sea $\mathcal{O}_K \subset \mathcal{O}_L \subset \mathcal{O}_M$ la torre correspondiente de clausuras enteras de $\mathcal{O}_K$ en L y en M. Sea $\mathfrak{p}$ un ideal primo de $\mathcal{O}_K$, debajo del ideal primo $\mathfrak{P}$ de $\mathcal{O}_L$, que a su vez está debajo del ideal primo $\mathfrak{Q}$ de $\mathcal{O}_M$. Entonces tenemos que*

$$e(\mathfrak{Q}|\mathfrak{p}) = e(\mathfrak{Q}|\mathfrak{P})e(\mathfrak{P}|\mathfrak{p});$$
$$f(\mathfrak{Q}|\mathfrak{p}) = f(\mathfrak{Q}|\mathfrak{P})f(\mathfrak{P}|\mathfrak{p}).$$

Teorema 1.1.9. *Sea $\mathfrak{p}$ un ideal primo de $\mathcal{O}_K$, debajo del ideal primo $\mathfrak{P}$ de $\mathcal{O}_L$. Sean $\mathfrak{P}^I = \mathfrak{P} \cap L^I$ y $\mathfrak{P}^D = \mathfrak{P} \cap L^D$. Supongamos que la extensión de cuerpos residuales es separable. Entonces tenemos que:*

$$[L:L^I] = e; \quad [L^I:L^D] = f; \quad [L^D:K] = r;$$
$$e(\mathfrak{P}|\mathfrak{P}^I) = e; \quad e(\mathfrak{P}^I|\mathfrak{P}^D) = 1; \quad e(\mathfrak{P}^D|\mathfrak{p}) = 1;$$
$$f(\mathfrak{P}|\mathfrak{P}^I) = 1; \quad f(\mathfrak{P}^I|\mathfrak{P}^D) = f; \quad f(\mathfrak{P}^D|\mathfrak{p}) = 1.$$

El siguiente corolario motiva los nombres de "inercia" y "descomposición".

Corolario 1.1.10. *Supongamos que $D(\mathfrak{P})$ es normal en $\mathrm{Gal}(L/K)$. Entonces $\mathfrak{p}$ se parte en r primos distintos en L^D (es decir, se parte completamente). Si, además, $I(\mathfrak{P})$ es normal en $\mathrm{Gal}(L/K)$, entonces cada uno permanece primo en L^I (es "inerte"). Por último, cada uno es una potencia e-ésima en L.*

Como otro corolario, obtenemos que el orden de $D(\mathfrak{P})$ es ef, el orden de $I(\mathfrak{P})$ es e y el índice de $D(\mathfrak{P})$ en $\mathrm{Gal}(L/K)$ es r. Además, es fácil ver que los grupos de descomposición e inercia de primos distintos arriba de uno mismo, son conjugados en el grupo de Galois. De esta manera, un primo es no ramificado si y sólo si $I(\mathfrak{P}) = 1$ para algún, y, por lo tanto, para todo, ideal primo $\mathfrak{P}$ sobre $\mathfrak{p}$.

Sea $\mathfrak{p}$ un ideal primo de $\mathcal{O}_K$, debajo del ideal primo $\mathfrak{P}$ de $\mathcal{O}_L$. Consideremos el morfismo natural

$$D(\mathfrak{P}) \to \mathrm{Gal}(l_{\mathfrak{P}}/k_{\mathfrak{p}}),$$
$$\sigma \mapsto \overline{\sigma}.$$

Este morfismo es suryectivo e induce un isomorfismo

$$D(\mathfrak{P})/I(\mathfrak{P}) \to \mathrm{Gal}(l_{\mathfrak{P}}/k_{\mathfrak{p}}).$$

En efecto, este último morfismo es inyectivo y ambos grupos tienen orden f.

Supongamos ahora que los cuerpos residuales son finitos (esto pasa siempre en el caso en que K sea un cuerpo de números y $\mathcal{O}_K$ su anillo de enteros). Entonces $l_{\mathfrak{P}}/k_{\mathfrak{p}}$ es una extensión finita de cuerpos finitos, y, por lo tanto, su grupo de Galois tiene un elemento distinguido que lo genera, el *morfismo de Frobenius*, definido por $x \mapsto x^q$, donde q es el orden de $k_{\mathfrak{p}}$. En el caso

en que $\mathfrak{p}$ sea no ramificado en L, obtenemos un único elemento del grupo de Galois de L/K, denotado por $(\mathfrak{P}, L/K)$, que va a parar al morfismo de Frobenius por el isomorfismo anterior. Es un elemento del grupo de Galois de L/K caracterizado por

$$(\mathfrak{P}, L/K)(y) \equiv y^q (\mathrm{mod}\, \mathfrak{P}) \quad \forall y \in \mathcal{O}_L.$$

El morfismo $(\mathfrak{P}, L/K)$ se llama el *símbolo de Artin* de $\mathfrak{P}$. Las siguientes propiedades son inmediatas.

Proposición 1.1.11. *Sea $\mathfrak{p}$ un ideal primo no ramificado, y sea $\mathfrak{P}$ un ideal primo en L sobre $\mathfrak{p}$. Entonces se cumplen las siguientes afirmaciones:*

(I) *si $\sigma \in \mathrm{Gal}(L/K)$,*
$$(\sigma\mathfrak{P}, L/K) = \sigma(\mathfrak{P}, L/K)\sigma^{-1};$$

(II) *el orden de $(\mathfrak{P}, L/K)$ es el índice de inercia $f_{\mathfrak{P}} = f(\mathfrak{P}|\mathfrak{p})$;*

(III) *$\mathfrak{p}$ se parte completamente en L si y sólo si $(\mathfrak{P}, L/K) = 1$.*

La primera propiedad nos dice que los símbolos de Artin de dos primos sobre uno mismo son conjugados en $\mathrm{Gal}(L/K)$. Esto permite asignarle a cada primo no ramificado $\mathfrak{p}$ una clase de conjugación de $\mathrm{Gal}(L/K)$. En el caso particular en que L/K sea abeliana, se trata de un solo elemento, llamado el *símbolo de Artin* de $\mathfrak{p}$, y denotado por

$$(\mathfrak{p}, L/K).$$

Sea S un conjunto finito de ideales primos de $\mathcal{O}_K$. Definimos I_K^S como el subgrupo libre de I_K generado por los ideales primos que no están en S. Consideremos ahora cualquier S tal que contenga a los ideales primos que ramifican. Utilizando la factorización de ideales fraccionarios en ideales primos, podemos definir el *mapa de Artin*:

$$\psi_{L/K} : I_K^S \to \mathrm{Gal}(L/K),$$

$$\prod_{\mathfrak{p} \nmid S} \mathfrak{p}^{a_\mathfrak{p}} \mapsto \prod_{\mathfrak{p} \nmid S} (\mathfrak{p}, L/K)^{a_\mathfrak{p}}.$$

Esta aplicación es el corazón de la teoría de cuerpos de clases, y la mayoría de los resultados que queremos obtener son en realidad propiedades de ella.

Otras propiedades del símbolo de Artin son las siguientes.

Proposición 1.1.12. *Sea $K \subset L \subset M$ una torre de extensiones finitas de Galois, $\mathfrak{Q}$ un ideal primo de M, que está sobre el ideal $\mathfrak{P}$ de L, que a su vez está sobre $\mathfrak{p}$; supongamos que $\mathfrak{p}$ no ramifica en M (y, por lo tanto, tampoco en L). Entonces tenemos que*

(a) $(\mathfrak{Q}, M/L) = (\mathfrak{Q}, M/K)^{f(\mathfrak{P}|\mathfrak{p})}$;

(b) $(\mathfrak{Q}, M/K)\,|_L = (\mathfrak{P}, L/K)$.

Dem. El ítem (a) es trivial, como vemos considerando la torre de extensiones de cuerpos residuales $m_{\mathfrak{Q}} \supset l_{\mathfrak{P}} \supset k_{\mathfrak{p}}$; $f(\mathfrak{P}|\mathfrak{p}) = [l_{\mathfrak{P}} : k_{\mathfrak{p}}]$, y un elemento de Frobenius de la extensión de arriba es elevar a la $f(\mathfrak{P}|\mathfrak{p})$ un elemento de Frobenius de la extensión total. El ítem (b) también es trivial, ya que $(\mathfrak{Q}, M/K)\,|_L$ cumple las propiedades que caracterizan a $(\mathfrak{P}, L/K)$. □

Ejemplo 1.1.13. Sea $m \in \mathbb{N}$ y $\mathbb{Q}(\zeta_m)$ el cuerpo ciclotómico de las raíces m-ésimas de la unidad. Usaremos el siguiente resultado clásico de teoría de números algebraica básica, cuya demostración puede encontrarse en [Mar77] (Capítulo 3, Teorema 26): sea $p \in \mathbb{Z}$ un primo, y escribamos $m = p^k n$ con $p \nmid n$. Entonces el índice de ramificación de p en $\mathbb{Q}(\zeta_m)$ (que no depende del primo arriba pues es una extensión de Galois) es igual a $\varphi(p^k)$, donde φ es la función de Euler, y el índice de inercia f es el menor entero positivo tal que $p^f \equiv 1 (\mathrm{mod}\, n)$ (el orden multiplicativo de p módulo n). En particular, cualquier primo ramificado debe dividir a m. Si $4|m$ entonces los primos ramificados son exactamente los divisores de m, mientras que si $2|m$ y $4 \nmid m$ entonces son todos menos el 2. En cualquier caso se tiene definido el mapa de Artin

$$\psi_m : I_{\mathbb{Q}}(m) \to \mathrm{Gal}(\mathbb{Q}(\zeta_m)/\mathbb{Q}) \simeq (\mathbb{Z}/mZ)^{\times}.$$

Aquí, $I_{\mathbb{Q}}(m)$ se puede identificar con el conjunto de los números racionales a/b, con $a, b > 0$, $(a, b) = (a, m) = (b, m) = 1$. Entonces

$$\psi_m(a/b) = [a][b]^{-1} \in (\mathbb{Z}/mZ)^{\times}.$$

La verificación es trivial, pues basta chequearlo para $\psi(p)$ con p un primo que no divida a m, y este caso sale por definición del símbolo de Artin.

1.2. Valores absolutos

Sea K un cuerpo. Un *valor absoluto* sobre K es una función $|.| : K \to \mathbb{R}$ tal que

(1) $|x| \geq 0 \quad \forall\, x \in K$ y $|x| = 0 \Leftrightarrow x = 0$;

(2) $|xy| = |x||y| \quad \forall\, x, y \in K$;

(3) Existe una constante C tal que $|1 + x| \leq C$ siempre que $|x| \leq 1$.

De esta manera, podemos ver a un valor absoluto como un morfismo de grupos $|.| : K^{\times} \to \mathbb{R}_+$ (donde $\mathbb{R}_+ = \{x \in \mathbb{R} : x > 0\}$) tal que cumple (3), y que lo extendemos a K poniendo $|0| = 0$.

Dado un cuerpo K, siempre existe un valor absoluto sobre él, vale decir, el *valor absoluto trivial*, definido por $|x| = 1$ para $x \neq 0$, $|0| = 0$ ($C = 1$ en (3)). De ahora en más, supondremos que todos los valores absolutos son no triviales.

Como $\mathbb{R}_+$ es sin torsión, todas las raíces de la unidad en K van a parar a 1. En particular, $|1| = |-1| = 1$, y, por lo tanto, $|-x| = |x|$ para todo x en K. Además, trivialmente, tenemos la siguiente proposición.

Proposición 1.2.1. *Sea K un cuerpo finito. Entonces todo valor absoluto sobre K es el valor absoluto trivial.*

Definición 1.2.2. Decimos que dos valores absolutos $|.|_1$ y $|.|_2$ en un cuerpo K son equivalentes si existe un $c \in \mathbb{R}_+$ tal que $|.|_2 = |.|_1^c$.

Notemos que si $|.|_1$ es un valor absoluto, entonces $|.|_2 = |.|_1^c$ también lo es. Claramente, se tiene una relación de equivalencia sobre los valores absolutos (sobre un mismo cuerpo K). Además, es claro que el valor absoluto trivial es equivalente sólo a sí mismo. Una clase de equivalencia de valores absolutos no triviales se llama un *primo* de K, o un *divisor* de K. Generalmente usaremos la letra v para denotar un primo de K, y por $|.|_v$ a un valor absoluto que lo represente.

No es difícil ver que todo valor absoluto es equivalente a uno cuya constante C es igual a 2. Para este tipo de valores absolutos, la siguiente proposición nos da otra caracterización de (3).

Proposición 1.2.3. *Sea $|.| : K \to \mathbb{R}_{\geq 0}$ una función que satisface (1) y (2). Las siguientes condiciones son equivalentes:*

(I) $|1 + x| \leq 2$ *siempre que* $|x| \leq 1$ (*esto es, vale* (3) *con* $C = 2$);

(II) $|x + y| \leq |x| + |y| \quad \forall\, x, y \in K$ (*A esta última propiedad la llamaremos* $(3')$ *o desigualdad triangular*).

Dem. (I)⇒(II): Sean $x, y \in K$. Si alguno es 0, vale trivialmente la desigualdad; luego, supondremos ambos no nulos. Si, por ejemplo, $|x| \leq |y|$, escribimos $x = ay$, con $a \in K$, de manera que $|a| \leq 1$. Luego, $|x + y| = |y(1 + a)| = |y||1 + a| \leq 2|y|$ por hipótesis, y esto último es igual a $2\ \max\{|x|, |y|\}$. Por inducción, probamos que si $x_1, ..., x_{2^r} \in K$ entonces

$$|\sum_{j=1}^{2^r} x_j| \leq 2^r\ \max\{|x_j|\}.$$

De esta manera, si $n \in \mathbb{N}$ y $2^{r-1} < n \leq 2^r$, insertando $2^r - n$ sumandos nulos, obtenemos que

$$|\sum_{j=1}^{n} x_j| \leq 2^r\ \max\{|x_j|\} \leq 2n\ \max\{|x_j|\}.$$

En particular, $|n| \leq 2n|1| = 2n$. Ahora,

$$|x + y|^n = |\sum_j \binom{n}{j} x^j y^{n-j}| \leq 2(n + 1)\ \max\{|\binom{n}{j}||x|^j |y|^{n-j}\} \leq$$

$$\leq 4(n + 1)\ \max\{\binom{n}{j}|x|^j |y|^{n-j}\} \leq 4(n + 1)(|x| + |y|)^n.$$

Tomando raíces n-ésimas y haciendo tender n a infinito, se sigue la desigualdad buscada.

(II)⇒(I): es claro. □

Trabajar con valores absolutos equivalentes es lo mismo, con lo cual, podríamos haber hecho la definición con $(3')$ directamente y suponer ya que todos tienen constante $C = 2$.

Decimos que un valor absoluto $|.|$ es *no arquimedeano* si uno puede tomar $C = 1$ en (3). Esto es lo mismo que decir que

$$|x + y| \leq \text{máx}\{|x|, |y|\}.$$

Esto claramente implica $(3')$, con lo cual, un valor absoluto no arquimedeano cumple (3) tanto con $C = 1$ como con $C = 2$. Decimos que un valor absoluto es *arquimedeano* si no es no arquimedeano (como era de esperarse).

No es difícil ver que la arquimedeanidad está preservada por equivalencias. Por lo tanto, podemos hablar de primos arquimedeanos y no arquimedeanos. En el primer caso, los llamaremos también primos *infinitos*, mientras que en el caso no arquimedeano, primos *finitos*.

Recordemos que, dado un cuerpo K, el *anillo primo* es la imagen de la aplicación canónica $\mathbb{Z} \to K$.

Lema 1.2.4. *Sea $|.|$ un valor absoluto. Entonces $|.|$ es no arquimedeano si y sólo si $|n| \leq 1$ para todo n en el anillo primo de K.*

Dem. Es claro que un valor absoluto no arquimedeano está acotado por 1 en el anillo primo de K. Recíprocamente, sea $|.|$ un valor absoluto que cumple eso. Sabemos que es equivalente a un valor absoluto que cumple la desigualdad triangular, con lo cual, veamos que vale para el caso en que $|.|$ la cumpla. Probaremos ahora que se cumple (3) con $C = 1$. Sea $x \in K$ tal que $|x| \leq 1$. Por la desigualdad triangular,

$$|1 + x|^n = |(1 + x)^n| \leq \sum_j |\binom{n}{j}||x| \leq 1 + 1 + ... + 1 = n + 1.$$

Tomando raíz n-ésima y haciendo tender n a infinito, obtenemos $|1 + x| \leq 1$. Así, $|.|$ es no arquimedeano. □

Corolario 1.2.5. *Si car $K = p \neq 0$ entonces cualquier valor absoluto sobre K es no arquimedeano*

Dem. Esto es claro pues los elementos del anillo primo de K son raíces de la unidad. □

Ejemplo 1.2.6. En $\mathbb{R}$, el valor absoluto usual es un valor absoluto arquimedeano. Lo mismo sucede con $\mathbb{C}$. De hecho, hay un teorema de Gelfand y Tornheim que afirma que un cuerpo K con un valor absoluto arquimedeano es isomorfo a un subcuerpo de $\mathbb{C}$ y su valor absoluto es equivalente al inducido por el valor absoluto usual de $\mathbb{C}$. No necesitaremos este teorema. Para una demostración, ver E. Artin, "Theory of Algebraic Numbers" (Striker, Göttingen), pp. 45 y 67.

Ejemplo 1.2.7. Sea K un cuerpo de números, y $\sigma : K \hookrightarrow \mathbb{C}$ una inmersión. Definimos $|x|_\sigma = |\sigma x|$, donde este último es el valor absoluto usual de $\mathbb{C}$. Entonces $|x|_\sigma$ es un valor absoluto arquimedeano en K. Más adelante, veremos que todo valor absoluto arquimedeano de un cuerpo de números es equivalente a uno de estos.

Ejemplo 1.2.8. Sea K un cuerpo de números de grado n. Sea $\mathfrak{P} \subset \mathcal{O}_K$ un ideal primo. Si $x \in K^\times$, sea $\mathrm{ord}_\mathfrak{P}(x)$ el exponente (entero) al cual aparece $\mathfrak{P}$ en la factorización del ideal fraccionario $(x) = x\mathcal{O}_K$ en ideales primos. Sea $c > 1$ un número real. Definimos el siguiente valor absoluto en K:

$$|x|_\mathfrak{P} = c^{-\mathrm{ord}_\mathfrak{P}(x)}.$$

Usando las propiedades de $\mathrm{ord}_\mathfrak{P}$ es fácil ver que $|.|_\mathfrak{P}$ es un valor absoluto no arquimedeano, llamado $\mathfrak{P}$-ádico (este procedimiento lo podríamos haber hecho con cualquier dominio de Dedekind y su cuerpo de fracciones). A la clase de equivalencia definida por este valor absoluto lo llamaremos $v_\mathfrak{P}$. Veremos luego que todos los valores absolutos no arquimedeanos de un cuerpo de números K son de esta forma. Es fácil probar que ideales primos distintos dan lugar a valores absolutos no equivalentes.

Tomemos, por ejemplo, el caso de $K = \mathbb{Q}$. Sea $p \in \mathbb{Z}$ un número primo. Dado $x \in \mathbb{Q}^\times$, escribimos $x = p^n u/v$, con $p \nmid u$, $p \nmid v$, $n, u, v \in \mathbb{Z}$. Entonces $|x|_p = c^{-n}$. Se suele tomar $c = p$ (en el caso de cuerpos de números, también hay una normalización correspondiente que ya veremos), por razones que serán claras más adelante. A este valor absoluto lo llamamos p-ádico.

Ejemplo 1.2.9. Este ejemplo es parecido al anterior. Sea E un cuerpo y sea $K = E(t)$, donde t es trascendente sobre E. Sea $p = p(t)$ un polinomio irreducible en $E[t]$. Como $E[t]$ es un dominio de factorización única, todo elemento f de $E(t)$ se escribe como $f = p^n u/v$, con $n \in Z$, $u, v \in E[t]$, $p \nmid u$, $p \nmid v$. Dado un número real $c > 1$, tomamos el valor absoluto no arquimedeano

$$|f|_p = c^{-n}$$

(esto es un caso particular del ejemplo anterior, ya que $E[t]$ es un dominio de Dedekind).

Hay un valor absoluto adicional en $E(t)$ (también eligiendo arbitrariamente un número real $c > 1$), definido por

$$|\frac{u}{v}|_\infty = c^{\mathrm{gr}(u)-\mathrm{gr}(v)}.$$

Si $s = t^{-1}$, entonces $K = E(s)$ y vemos que este valor absoluto es del tipo $|.|_p$, con p el polinomio irreducible $p(s) = s$. Luego, es no arquimedeano (es decir, la analogía con $\mathbb{Q}$ no es perfecta).

Las siguientes definiciones suponen que v es un primo no arquimedeano de K (y claramente no dependen de la elección del representante $|.|_v$).

$$\mathcal{O}_v = \{x \in K : |x|_v \leq 1\};$$
$$\mathcal{U}_v = \{x \in K : |x|_v = 1\};$$
$$\mathfrak{p}_v = \{x \in K : |x|_v < 1\}.$$

Es claro que $\mathcal{O}_v$ es un subanillo de K (llamado el *anillo de enteros* de K respecto de v), que K es su cuerpo de fracciones y $\mathfrak{p}_v$ es un ideal de $\mathcal{O}_v$. Es inmediato que $\mathcal{O}_v^\times = \mathcal{U}_v$, y que, por lo tanto, $\mathcal{O}_v$ es un anillo local con ideal maximal $\mathfrak{p}_v$. Cuando el primo en cuestión esté sobreentendido, notaremos también $\mathcal{O}_K, \mathcal{U}_K$ y $\mathfrak{p}_K$ a estos conjuntos.

El cuerpo $k = \mathcal{O}_v/\mathfrak{p}_v$ se llama el *cuerpo residual* de K (o de $\mathcal{O}_v$) respecto del primo v.

Ejemplo 1.2.10. Consideremos un primo $p \in \mathbb{Z}$ y el valor absoluto p-ádico en $\mathbb{Q}$. Entonces el anillo de enteros es $\mathbb{Z}_{(p)}$, la localización de $\mathbb{Z}$ en el ideal primo (p), y $p\mathbb{Z}_{(p)}$ su ideal maximal. En consecuencia el cuerpo residual es $\mathbb{Z}_{(p)}/p\mathbb{Z}_{(p)} = \mathbb{F}_p$.

Más generalmente, si A es un dominio de Dedekind y $\mathfrak{P}$ es un ideal primo de A, considerando el valor absoluto $\mathfrak{P}$-ádico en $K = \mathrm{Frac}(A)$, vemos que el anillo de enteros $A_{\mathfrak{P}}$, y su ideal maximal es $\mathfrak{P}A_{\mathfrak{P}}$. El cuerpo residual es entonces $A_{\mathfrak{P}}/\mathfrak{P}A_{\mathfrak{P}} = A/\mathfrak{P}$.

Teorema 1.2.11 (Ostrowski)**.** *Sea $|.|$ un valor absoluto no trivial en $\mathbb{Q}$. Si es arquimedeano entonces es equivalente al valor absoluto usual $|.|_\infty$. Si es no arquimedeano, es equivalente a un único valor absoluto p-ádico $|.|_p$.*

Demostración. Suponemos en principio que $|.|$ satisface la desigualdad triangular. Sean $m, n \in \mathbb{Z}$, con $n > 1$. Luego, m se puede escribir como

$$a_0 + a_1 n + ... + a_r n^r$$

con los $a_i \in \mathbb{Z}$, $0 \leq a_i < n$, $n^r \leq m$ (es decir, $r \leq \frac{\log m}{\log n}$, para cualquier base $e > 1$). Por la desigualdad triangular, para cada i entre 0 y r tenemos que

$$|a_i| = |1 + 1 + ... + 1| \leq a_i|1| = a_i < n.$$

Llamemos $N = \max\{1, |n|\}$. Luego, también por la desigualdad triangular,

$$|m| \leq \sum_{i=0}^{r} |a_i||n|^i \leq \sum_{i=0}^{r} |a_i| N^r.$$

Juntando las dos desigualdades, obtenemos que

$$|m| \leq (1 + r)nN^r \leq (1 + \frac{\log m}{\log n})nN^{\log m/\log n}.$$

Si en lugar de m utilizamos m^k con $k \in \mathbb{Z}$, vemos que la desigualdad se transforma (tomando raíz k-ésima) en

$$|m| \leq (1 + \frac{k \log m}{\log n})^{1/k} n^{1/k} N^{\log m/\log n}.$$

Hacemos tender ahora $k \to \infty$. Los términos con k tienden a 1, de manera que

$$|m| \leq N^{\log m/\log n}.$$

Consideraremos ahora dos casos posibles:

Caso (I): para todos los enteros $n > 1$, se tiene que $|n| > 1$. En este caso, $N = |n|$, y de la desigualdad obtenida obtenemos que

$$|m|^{1/\log m} \leq |n|^{1/\log n}.$$

Si intercambiamos n y m, y suponemos que $m > 1$, por simetría obtenemos la igualdad, luego, existe un $c > 1$ tal que

$$c = |m|^{1/\log m} = |n|^{1/\log n}$$

para todos los enteros m, n mayores a 1. De aquí que para todo entero $n > 1$, vale que

$$|n| = c^{\log n} = e^{\log c \log n} = n^{\log c}.$$

Llamemos $a = \log c$. Queda entonces $|n| = |n|_\infty^a$ para todo entero $n > 1$, donde $|.|_\infty$ es el valor absoluto usual de $\mathbb{Q}$. Como los valores absolutos son morfismos $\mathbb{Q}^\times \to \mathbb{R}_+$, y estos dos coinciden en un conjunto de generadores de $\mathbb{Q}^\times$ (el conjunto de los primos positivos y -1), se sigue que coinciden en todo $\mathbb{Q}^\times$. Luego, $|.|$ es equivalente a $|.|_\infty$.

Caso (II): existe un $n > 1$ tal que $|n| \leq 1$. En este caso, $N = 1$ y la desigualdad implica que $|m| \leq 1$ para todos los enteros m. Entonces el valor absoluto es no arquimedeano. Sea $\mathfrak{P}$ el ideal primo asociado. Luego, $\mathfrak{P} \cap \mathbb{Z}$ es un ideal primo de $\mathbb{Z}$, distinto de 0 (si este ideal fuese 0, el valor absoluto sería el trivial). Así, $\mathfrak{P} \cap \mathbb{Z} = (p) = p\mathbb{Z}$ para algún primo p. De esta manera, si $m \in \mathbb{Z}$ y no es divisible por p, vemos que m no esta en $\mathfrak{P}$, luego, $|m| = 1$, y, por lo tanto, $|np^r| = |p|^r$ si n es un número racional tal que p no divide ni al numerador ni al denominador. Si a es tal que $|p| = (1/p)^a$ entonces $|x| = |x|_p^a$ para todo $x \in \mathbb{Q}$. Es decir, $|.|$ es equivalente a $|.|_p$. □

1.3. Topología definida por un valor absoluto

Dado un valor absoluto $|.|$ sobre un cuerpo K, existe una topología natural a considerar en K, donde dado un $a \in K$, una base de entornos en a son las "bolas abiertas" $B_\epsilon(a) = \{x \in K : |x - a| < \delta\}$. Si $|.|$ satisface la desigualdad triangular, entonces esta topología es la inducida por la distancia $d(x, y) = |x - y|$. Un ejercicio fácil es que con esta topología K resulta un cuerpo topológico Hausdorff.

La siguiente proposición muestra que podemos hablar de la topología dada por un primo (es decir, que valores absolutos equivalentes dan la misma topología).

Proposición 1.3.1. *Dados dos valores absolutos $|.|_1$ y $|.|_2$, con $|.|_1$ no trivial sobre K, son equivalentes:*

(I) $|.|_1$ *y* $|.|_2$ *inducen la misma topología en* K;

(II) $|x|_1 < 1 \Rightarrow |x|_2 < 1$ *para todo* $x \in K$;

(III) $|.|_1$ *y* $|.|_2$ *son equivalentes*.

Demostración. (I)⇒(II): es claro que el conjunto de los x tales que $|x|_1 < 1$ es exactamente el conjunto de los x tales que x^n tiende a 0 cuando $n \to \infty$. Luego, es clara la implicación.

(II)⇒(III): Al ser $|.|_1$ no trivial, existe un $y \in K$ tal que $|y|_1 > 1$. Sea $a = \log |y|_2 / \log |y|_1$, de manera que $\log |y|_2 = a \log |y|_1$, o $|y|_2 = |y|_1^a$. Sea $x \in K^\times$. Entonces existe un número real b tal que $|x|_1 = |y|_1^b$. Probaremos que $|x|_2 = |y|_2^b$, y esto bastará, ya que entonces $|x|_2 = |y|_1^{ab} = |x|_1^a$.

Sea m/n, $n > 0$, un número racional mayor que b. Entonces $|x|_1 = |y|_1^b < |y|_1^{m/n}$, de manera que $|x^n/y^m|_1 < 1$. Entonces por hipótesis $|x^n/y^m|_2 < 1$, luego, $|x|_2 < |y|_2^{m/n}$. Esto vale para todos los racionales m/n mayores que b, luego, $|x|_2 \leq |y|_2^b$. Por un argumento similar, tomando los racionales menores a b, vemos que $|x|_2 \geq |y|_2^b$, y queda así probada la igualdad.

(III)⇒(I): Es claro. □

Por lo tanto, cuando consideremos valores absolutos sobre un cuerpo, supondremos que cumplen la desigualdad triangular, ya que las propiedades topológicas de K no cambiarán.

Es claro que si v es un primo no arquimedeano, $\mathcal{O}_v$ es un subanillo cerrado de K.

Definición 1.3.2. Un cuerpo K con un valor absoluto $|.|$ se dice completo si lo es como espacio métrico.

Utilizando que todo espacio métrico se puede inyectar en uno completo de manera universal, se prueba el siguiente teorema.

Teorema 1.3.3. *Sea K un cuerpo y $|.|$ un valor absoluto sobre K. Entonces existe un cuerpo $\widehat{K}$, tal que K es (isomorfo a) un subcuerpo de $\widehat{K}$, $\widehat{K}$ posee un valor absoluto que extiende al de K (que también llamaremos $|.|$), respecto del cual $\widehat{K}$ es completo. Además, K es denso en $\widehat{K}$, y $\widehat{K}$ es único con estas propiedades (a menos de isomorfismo).*

Proposición 1.3.4. *$|.|$ es no arquimedeano en $\widehat{K}$ si y sólo si lo es en K. En ese caso, $|\widehat{K}| = |K|$, es decir, los conjuntos de valores son iguales.*

Dem. La primera afirmación es clara por el Lema 1.2.4. Para la segunda, sea $x \in \widehat{K}$, $x \neq 0$. Por densidad, existe un $y \in K$ tal que $|x - y| < |x|$. De aquí se sigue que $|x| = |y|$. □

Sea v un primo de K. Al cuerpo $\widehat{K}$ recién construido lo llamaremos K_v. Si v es no arquimedeano y $|.|_v$ es un valor absoluto que lo representa, seguimos notando con v y $|.|_v$ a las extensiones a K_v. Utilizaremos las siguientes notaciones:

$$\widehat{\mathcal{O}_v} = \{x \in K_v : |x|_v \leq 1\};$$
$$\widehat{\mathcal{U}_v} = \{x \in K_v : |x|_v = 1\};$$
$$\widehat{\mathfrak{p}_v} = \{x \in K_v : |x|_v < 1\};$$
$$\widehat{k} = \widehat{\mathcal{O}_v}/\widehat{\mathfrak{p}_v}.$$

Como antes, a menudo los notaremos como $\widehat{\mathcal{O}_K}$, $\widehat{\mathcal{U}_K}$ y $\widehat{\mathfrak{p}_K}$.

Es fácil ver que $\widehat{\mathcal{O}_v} = \overline{\mathcal{O}_v}$ (clausura en K_v) y que $\widehat{\mathfrak{p}_v} = \overline{\mathfrak{p}_v}$. Más generalmente, $\widehat{\mathfrak{p}_v}^m = \overline{\mathfrak{p}_v^m}$.

Ejemplo 1.3.5. Si $p \in \mathbb{Z}$ es primo, denotamos la completación de $\mathbb{Q}$ con el valor absoluto p-ádico por $\mathbb{Q}_p$. Notamos al anillo de enteros con $\mathbb{Z}_p$, y lo llamamos el anillo de *enteros p-ádicos*.

Más generalmente, si A es un dominio de Dedekind y $\mathfrak{P}$ es un ideal primo de A, llamamos $K_{\mathfrak{P}}$ a la completación ($K = \mathrm{Frac}(A)$).

1.4. Valores absolutos discretos

Un valor absoluto $|.|$ sobre K se dice *discreto* si el conjunto $\{\log|x| : x \in K^\times\}$ es un subgrupo discreto de $\mathbb{R}$ con la suma (como siempre, supondremos que el valor absoluto es no trivial). Notemos que no importa qué base tomemos para el logaritmo, pues multiplicar por un número real un subgrupo discreto de $\mathbb{R}$ nos da otro. Además, si dos valores absolutos son equivalentes, sucede lo mismo, con lo cual, la definición se puede aplicar a primos.

Si $|.|_v$ es un valor absoluto discreto, entonces el subgrupo recién mencionado debe ser libre en un generador, de manera que existe un número real $d > 0$ tal que $\log_e |K^\times|_v = d\mathbb{Z}$, es decir, "$|K^\times|_v = e^{d\mathbb{Z}}$". Si tomamos $c = e^{-d} < 1$, se sigue que los valores de $|x|_v$ para $x \neq 0$ son todos de la forma c^m con $m \in \mathbb{Z}$. Llamaremos *orden* de x a m. Es decir, $\mathrm{ord}(x) = -\log_f |x|$, donde $f = c^{-1} > 1$. Claramente, $\mathrm{ord}(xy) = \mathrm{ord}(x) + \mathrm{ord}(y)$.

Veamos qué sucede si tomamos un valor absoluto equivalente $|.| = |.|_v^a$ $(a > 0)$. Entonces $\log_e |K^\times| = ad\mathbb{Z}$, es decir, "$|K^\times| = e^{ad\mathbb{Z}}$". En este caso, $c' = e^{-ad} < 1$. Sea $x \in K^\times$, entonces $|x|_v = c^m$ y $|x| = (c^a)^m = c'^m$, de manera que el orden sólo depende del primo y no del valor absoluto. Notemos, además, que si v es no arquimedeano, $\mathcal{O}_v$ es el conjunto de los elementos de orden mayor o igual a 0, y $\mathfrak{p}_v$ es el de los de orden mayor a 0.

Dado un primo discreto no arquimedeano v, llamaremos a $\pi \in \mathcal{O}_v$ un *parámetro uniformizador local* (uniformizador, para abreviar) si tiene orden 1. Dado un valor absoluto $|.|_v$, es lo mismo que decir que $|\pi|_v = c$, o que es un elemento de valor absoluto máximo entre los menores a 1. Dos uniformizadores son asociados en $\mathcal{O}_v$.

Proposición 1.4.1. *Sea v un primo no arquimedeano sobre K. Entonces es discreto si y sólo si el ideal $\mathfrak{p}_v$ es principal. En este caso, está generado por cualquier uniformizador π.*

Dem. Supongamos que v es discreto. Sea π un uniformizador, y $c = |\pi|_v$. Claramente, al ser $c < 1$, se tiene que $(\pi) \subset \mathfrak{p}_v$. Sea $x \in \mathfrak{p}_v$. Luego, $|x|_v \leq c$, de manera que $|x/\pi|_v \leq 1$, es decir, $x/\pi \in \mathcal{O}_v$. De esta manera, $x = \pi\frac{x}{\pi} \in (\pi)$.

Supongamos ahora que $\mathfrak{p}_v$ es principal, digamos, $\mathfrak{p}_v = (\pi)$. Luego, para todo $x \in \mathfrak{p}_v$, existe un $a \in \mathcal{O}_v$ tal que $x = a\pi$. Así, $|x|_v = |a|_v|\pi|_v \leq |\pi|_v < 1$. De esta manera, 1 es un punto aislado de $|K^\times|_v$, con lo cual, v es discreto. □

Proposición 1.4.2. *Sea v un primo no arquimedeano discreto sobre K. Todo ideal no nulo de $\mathcal{O}_v$ es de la forma $\mathfrak{p}_v^m$ para algún $m \in \mathbb{N}_0$.*

Dem. Sea π un uniformizador para v, con $|\pi|_v = c$. Sea $\mathfrak{a}$ un ideal no nulo de $\mathcal{O}_v$. Definimos $\mathrm{ord}(\mathfrak{a}) = \text{ínf}\{\mathrm{ord}(x) : x \in \mathfrak{a}, x \neq 0\} \in \mathbb{N}_0$. Sea $a_0 \in \mathfrak{a}$ tal que $\mathrm{ord}(a_0) = \mathrm{ord}(\mathfrak{a})$,y pongamos $m = \mathrm{ord}(a_0)$. Tomando valores absolutos, se obtiene que $|a_0|_v = c^m = |\pi^m|_v$, con lo cual, π^m y a_0 son asociados. Luego, $(\pi^m) \subset \mathfrak{a}$. Probemos ahora que $\mathfrak{a} \subset (\pi^m)$. Si $\mathrm{ord}(x) \geq \mathrm{ord}(\mathfrak{a})$ entonces $x = \pi^{\mathrm{ord}(\mathfrak{a})}y$, con $y \in \mathcal{O}_v$. Además, $\mathfrak{a} \subset \{x \in \mathcal{O}_v : \mathrm{ord}(x) \geq \mathrm{ord}(\mathfrak{a})\}$, de manera que $\mathfrak{a} \subset (\pi^{\mathrm{ord}(\mathfrak{a})}) = (\pi^m)$. □

De acuerdo con estos dos últimos resultados, $\mathcal{O}_v$ es un dominio de ideales principales, local, cuyo único ideal primo no nulo es $\mathfrak{p}_v$.

Proposición 1.4.3. *Sea v un primo discreto no arquimedeano. Entonces π es un uniformizador si y sólo si $\pi \in \mathfrak{p}_v \setminus \mathfrak{p}_v^2$.*

Dem. Sea π un uniformizador; luego, $\mathfrak{p}_v = (\pi)$, con lo cual, es obvio que $\pi \notin \mathfrak{p}_v^2$ ya que $\mathfrak{p}_v \neq \mathfrak{p}_v^2$ ($\mathfrak{p}_v$ es un ideal primo no nulo).

Recíprocamente, supongamos que $\pi \in \mathfrak{p}_v \setminus \mathfrak{p}_v^2$. Al ser $\mathcal{O}_v$ un dominio principal local con único ideal primo no nulo $\mathfrak{p}_v = (p) = p\mathcal{O}_v$ (para un uniformizador p), escribimos $\pi = ap^k$, con $a \in \mathcal{O}_v \setminus \mathfrak{p}_v$, es decir, a una unidad. De esta manera, por hipótesis, $k = 1$. Así, π es asociado a un uniformizador, y, por lo tanto, es un uniformizador. □

Sea v un primo no arquimedeano discreto sobre K. Sea $|.|_v$ un valor absoluto correspondiente, y $c < 1$ como en la discusión anterior. Entonces es claro que

$$\mathcal{O}_v = \{x \in K : |x|_v \leq 1\} = \{x \in K : |x|_v < c^{-1}\} \text{ y}$$
$$\mathfrak{p}_v = \{x \in K : |x|_v < 1\} = \{x \in K : |x|_v \leq c\}$$

De esta manera, $\mathcal{O}_v$ y $\mathfrak{p}_v$ son abiertos y cerrados. Además, todo ideal $\mathfrak{p}_v^m$ se describe como

$$\mathfrak{p}_v^m = \{x \in K : |x|_v \leq c^m\} = \{x \in K : |x|_v < c^{m-1}\},$$

de manera que también es abierto y cerrado en $\mathcal{O}_v$. Los conjuntos $\mathfrak{p}_v^m$ ($m \geq 0$) son un sistema fundamental de entornos del 0: son subgrupos abiertos de K cuya intersección es 0 ($\mathfrak{p}_v^0 = \mathcal{O}_v$). Como también son cerrados, K resulta totalmente disconexo.

Es claro que si v es un primo discreto no arquimedeano, entonces también es discreto el primo correspondiente en K_v (ya que el conjunto de valores es el mismo que el de K).

Supongamos que π es un uniformizador, de manera que $\mathfrak{p}_v = (\pi) = \pi\mathcal{O}_v$ (y $\mathfrak{p}_v^m = (\pi^m)$). Entonces $\widehat{\mathfrak{p}_v} = (\pi) = \pi\widehat{\mathcal{O}_v}$ (esta igualdad es clara ya que v es un primo no arquimedeano discreto de K_v y π es un uniformizador para K_v). También tenemos que $\widehat{\mathfrak{p}_v}^m = (\pi^m) = \pi^m\widehat{\mathcal{O}_v}$. Además, la aplicación natural

$$\mathcal{O}_v/\mathfrak{p}_v \to \widehat{\mathcal{O}_v}/\widehat{\mathfrak{p}_v}$$

es un isomorfismo de grupos. Más generalmente, se tiene el siguiente resultado.

Lema 1.4.4. *Sea v un primo discreto no arquimedeano en K. Dado $m \in \mathbb{N}$, la aplicación natural*

$$\mathcal{O}_v/\mathfrak{p}_v^m \to \widehat{\mathcal{O}_v}/\widehat{\mathfrak{p}_v}^m$$

es un isomorfismo de grupos.

Dem. Veamos que es inyectiva. Sean $x, y \in \mathcal{O}_v$ tales que $x - y \in \widehat{\mathfrak{p}_v}^m$. Entonces $x - y = a\pi^m$, con $a \in \widehat{\mathcal{O}_v}$, es decir, $|a|_v \leq 1$; pero $a = (x-y)/\pi^m \in K$, luego, $a \in \mathcal{O}_v$ y $x = y$ en $\mathcal{O}_v/\mathfrak{p}_v^m$.

Para la suryectividad, sea $y \in \widehat{\mathcal{O}_v}$. Veamos que existe $x \in \mathcal{O}_v$ tal que $x - y \in \widehat{\mathfrak{p}_v}^m$. Sea $\epsilon > 0$ tal que $\epsilon \leq |\pi|_v^m$. Entonces por densidad existe un $x \in \mathcal{O}_v$ tal que $|x - y|_v < \epsilon$. Sabemos que $|x - y|_v = |\pi|_v^k$ para algún k. Para ver la suryectividad, bastará probar que $k \geq m$, y esto es claro por la elección de ϵ. □

Si v es discreto no arquimedeano, como k-módulos ($k = \mathcal{O}_v/\mathfrak{p}_v$), $\mathfrak{p}_v^r/\mathfrak{p}_v^{r+1}$ y k son isomorfos vía multiplicación por π^r ($r \geq 0$).

Por el último lema, se tiene que $\widehat{\mathfrak{p}_v}^r/\widehat{\mathfrak{p}_v}^{r+1}$ es isomorfo a k (componiendo con el isomorfismo de $\widehat{k}$ con k).

Definimos, para cada $i \geq 1$, el subconjunto $U_i = 1 + \mathfrak{p}_v^i$, y llamamos $U_0 = \mathcal{U}_v$. Entonces U_i es un subgrupo de $K^\times$, ya que si $x, y \in \mathfrak{p}_v^i$ entonces

$$(1 + x)(1 + y) = 1 + x + y + xy \in 1 + \mathfrak{p}_v^i \quad (i \geq 1)$$

y

$$(1 - x)^{-1} = 1 + x + x^2 + ...$$

es una serie convergente (ejercicio). El conjunto U_0 es un abierto de $\mathcal{O}_v$ (y, por lo tanto, un abierto de $K^\times$, y también un cerrado), al ser el complemento del cerrado $\mathfrak{p}_v$. Los conjuntos U_i forman un sistema fundamental de entornos del 1 en $K^\times$. Como los $\mathfrak{p}_v^i$ son abiertos y cerrados, también lo son los U_i. De esta manera, $K^\times$ es totalmente disconexo.

Si π es un uniformizador entonces es claro que $K^\times$ es isomorfo (algebraica y topológicamente) al producto $\{\pi\} \times \mathcal{U}_v$, donde $\{\pi\}$ es el grupo cíclico generado por π.

Bajo la aplicación natural

$$\mathcal{O}_v \to k,$$

las unidades $\mathcal{U}_v$ van a parar a elementos no nulos. Luego, se tiene inducido un morfismo

$$\mathcal{U}_v \to k^\times.$$

El núcleo de este morfismo es exactamente U_1, de manera que $\mathcal{U}_v/U_1 \simeq k^\times$.

Más aún, la aplicación

$$\begin{aligned} \mathfrak{p}_v^i &\to U_i, \\ x &\mapsto (1+x) \end{aligned}$$

induce un isomorfismo (para $i \geq 1$)

$$\mathfrak{p}_v^i/\mathfrak{p}_v^{i+1} \to U_i/U_{i+1}.$$

Como corolario, tenemos que para $i \geq 1$, U_i/U_{i+1} es un grupo abeliano isomorfo a k.

Ejemplo 1.4.5. Dado $p \in \mathbb{Z}$ primo, el cuerpo residual de $\mathbb{Q}_p$ es $\mathbb{Z}_p/\mathfrak{m}$, donde $\mathfrak{m}$ es el ideal maximal de $\mathbb{Z}_p$. Por lo visto recién, este cuerpo es isomorfo al cuerpo residual de $\mathbb{Q}$ con respecto al valor absoluto p-ádico, y vimos anteriormente que este cuerpo es $\mathbb{F}_p$.

Proposición 1.4.6. *Sea v un primo no arquimedeano discreto en K, sea S un conjunto de representantes para $\mathcal{O}_v/\mathfrak{p}_v$, y sea π un uniformizador. Entonces la serie*

$$a_{-n}\pi^{-n} + ... + a_0 + a_1\pi + ... + a_r\pi^r + ..., a_i \in S$$

es una serie de Cauchy en K, y toda serie de Cauchy es equivalente a exactamente una de esta forma. De esta manera, todo elemento de K_v tiene un representante único de esta forma, cuyo orden es $-n$.

1.5. Valuaciones

Una *valuación* sobre un cuerpo K es un morfismo de grupos $\mathrm{ord} : K^\times \to \mathbb{R}$ tal que $\mathrm{ord}(x+y) \geq \text{mín}\{\mathrm{ord}(x), \mathrm{ord}(y)\}$. La extenderemos a K vía $\mathrm{ord}(0) = \infty$. Siempre existe una valuación en un cuerpo K, a saber, el morfismo nulo. Supondremos en general que las valuaciones son no nulas. La valuación ord se llamara *discreta* si su imagen cae dentro de $\mathbb{Z}$. Luego, la imagen es de la forma $m\mathbb{Z}$ para algún $m \in \mathbb{N}$. Una valuación discreta se dice *normalizada* si $m = 1$, es decir, si es suryectiva. Dos valuaciones ord_1 y ord_2 se dicen *equivalentes* si existe

un $c \in \mathbb{R}$ tal que $\mathrm{ord}_1 = c.\,\mathrm{ord}_2$ (notar que esto último es una valuación si ord_1 lo es). Además, si una valuación es discreta, cualquier valuación equivalente mediante un múltiplo entero también es discreta. Si ord es una valuación discreta con imagen $m\mathbb{Z}$, entonces $m^{-1}.\,\mathrm{ord}$ es una valuación discreta normalizada equivalente a ord.

Proposición 1.5.1. *Si* ord *es una valuación tal que* $\mathrm{ord}(K^\times)$ *es un subgrupo discreto de* $\mathbb{R}$*, entonces es equivalente a una valuación discreta.*

Dem. Como $\mathrm{ord}(K^\times)$ es un subgrupo discreto, es un retículo. Luego, $\mathrm{ord}(K^\times) = c\mathbb{Z}$ para algún c. Ahora, $c^{-1}.\,\mathrm{ord}$ es una valuación discreta equivalente a ord. □

Ejemplo 1.5.2. Sea K un cuerpo de números y $\mathfrak{P}$ un ideal primo de K. Entonces, con la notación de antes, $\mathrm{ord}_{\mathfrak{P}}$ es una valuación discreta. El valor absoluto $\mathfrak{P}$-ádico definido anteriormente nos dice que $\mathrm{ord}_{\mathfrak{P}}(x) = -\log_c |x|_{\mathfrak{P}}$. Esto nos motiva para la siguiente observación.

Observación 1.5.3. Sea $|.|$ un valor absoluto no arquimedeano sobre K. Sea $e > 1$ un número real. Entonces $\mathrm{ord}(x) = -\log_e |x|$ define una valuación sobre K. Si tomamos otro valor absoluto equivalente, las valuaciones correspondientes son equivalentes. De esta manera, tenemos una aplicación que a cada primo no arquimedeano de K le asigna una clase de valuaciones equivalentes. Esta aplicación es inyectiva, y también suryectiva: dada ord una valuación, definimos $|x| = e^{-\mathrm{ord}(x)}$. Notemos, además, que la constante $e > 1$ no es importante. Es decir, si uno toma otra constante $f > 1$, las aplicaciones correspondientes son exactamente la misma.

Si $|.|$ es discreto, entonces la proposición anterior nos dice que ord es un múltiplo real de una valuación discreta ord_2, digamos, $\mathrm{ord} = a.\,\mathrm{ord}_2$. Luego, $\mathrm{ord}_2(x) = -\log_e |x|^a$ es la valuación asociada de esta manera con un valor absoluto equivalente a $|.|$. Es decir, a los primos no arquimedeanos discretos, la aplicación anterior los lleva a una clase de valuaciones equivalentes entre las cuales se encuentra una valuación discreta. Claramente, es exhaustiva, en el sentido de que toda clase de valuaciones que contenga una discreta (es decir, toda clase de valuaciones cuyas imágenes sean subgrupos discretos de $\mathbb{R}$) proviene de un primo discreto no arquimedeano.

A menudo llamaremos también *primos* (no arquimedeanos) a las clases de valuaciones no nulas equivalentes, y primos *discretos* (no arquimedeanos) a las clases que contengan una valuación discreta. Cuando pueda haber lugar a confusión seremos más específicos.

Sea ord una valuación discreta en K y v un primo discreto no arquimedeano asociado, con valor absoluto $|x|_v = e^{-\mathrm{ord}(x)}$; entonces $|.|_v$ se extiende a K_v. En K_v tomamos $\mathrm{ord}(x) = -\log_e |x|_v$, y vemos que entonces ord se extiende a una valuación discreta en K_v, ya que $|K| = |K_v|$.

Traduciendo los resultados sobre valores absolutos no arquimedeanos discretos a valuaciones discretas, obtenemos que si ord es una valuación discreta normalizada sobre K asociada a un primo v entonces (manteniendo la convención $\mathrm{ord}(0) = \infty$)

$$\begin{aligned}
\mathcal{O}_v &= \{x \in K : \mathrm{ord}(x) \geq 0\};\\
\mathcal{U}_v &= \{x \in K : \mathrm{ord}(x) = 0\};\\
\mathfrak{p}_v &= \{x \in K : \mathrm{ord}(x) > 0\}.
\end{aligned}$$

Además, $\mathfrak{p}_v$ es principal, generado por un uniformizador, es decir, un elemento π tal que $\mathrm{ord}(\pi)$=1 (o más generalmente, si ord no es normalizada, por un π tal que $\mathrm{ord}(\pi) = m$ si $\mathrm{ord}(K^\times) = m\mathbb{Z}$). Otra caracterización ya vista de un tal π es que $\pi \in \mathfrak{p}_v \setminus \mathfrak{p}_v^2$.

1.6. Anillos de valuación discreta

Un *anillo de valuación discreta* A es un dominio de ideales principales que cumple alguna (y por tanto las tres) de las siguientes condiciones equivalentes:

(I) A es local y no es un cuerpo;

(II) A tiene un único ideal primo no nulo;

(III) A tiene exactamente un elemento primo, a menos de asociados.

Dado un anillo de valuación discreta A, cuyo ideal maximal $\mathfrak{m}$ está generado por π, al ser A un dominio de factorización única, todo elemento no nulo x del cuerpo de fracciones K de A se escribe de manera única como $x = \pi^m u$, con u una unidad y $m \in \mathbb{Z}$. Llamamos $\mathrm{ord}(x) = m$. Es inmediato que ord es una valuación discreta normalizada sobre K, y que el anillo de enteros asociado es exactamente A, con ideal maximal $\mathfrak{m}$. Recíprocamente, tenemos el siguiente resultado.

Proposición 1.6.1. *Sea* ord *una valuación discreta sobre un cuerpo K (correspondiente al primo v). Entonces el anillo de enteros correspondiente $\mathcal{O}_v$ es un anillo de valuación discreta con ideal maximal $\mathfrak{p}_v$ generado por un uniformizador. Además, K es su cuerpo de fracciones y la valuación inducida en $\mathcal{O}_v$ por la de K es igual a m veces la valuación definida para un anillo de valuación discreta según su elemento primo.*

Dem. Todo se sigue de los resultados de las Secciones 1.4 y 1.5. Al ser $\mathrm{ord}(K^\times) = m\mathbb{Z}$, uno le asigna el valor absoluto $|x| = e^{-\mathrm{ord}(x)}$ para algún $e > 1$. Como vimos, para este valor absoluto el ideal está generado por un elemento de valuación m. Si $x \in A$, escribimos $x = \pi^k u$, con $k \geq 0$ y u una unidad. Veamos que $\mathrm{ord}(x) = mk$. Basta ver que $\mathrm{ord}(u) = 0$, ya que $\mathrm{ord}(\pi) = m$. Esto es claro pues si $|.|$ es un valor absoluto en K asociado a ord, $|u| = 1$. Luego, la valuación inducida ord es exactamente m veces la definida por π. □

Sabemos también que si π es un uniformizador para el anillo de valuación discreta A entonces todo ideal no nulo de A es de la forma (π^m) para algún $m \in \mathbb{N}_0$.

1.7. Caso en que el cuerpo residual es finito

Analizaremos en esta sección la siguiente situación: K será un cuerpo y v un primo no arquimedeano y discreto sobre él; el cuerpo residual k será finito, con $q = p^f$ elementos. Llamaremos $\mathcal{O}_v$ al anillo de valuación discreta correspondiente y $\mathfrak{p}_v$ a su ideal maximal, generado por π. Por lo visto anteriormente, el cardinal de $\mathfrak{p}_v^i/\mathfrak{p}_v^{i+1}$ ($i \geq 0$) es q, y el de $\mathcal{U}_v/U_1$ es $q-1$. También tenemos el siguiente resultado.

Proposición 1.7.1. *El conjunto $\mathcal{O}_v/\mathfrak{p}_v^i$ $(i \geq 0)$ es finito. De hecho, su cardinal es q^i.*

Dem. Por inducción, el caso $i = 1$ es claro, mientras que por algún teorema de isomorfismo,

$$\mathcal{O}_v/\mathfrak{p}_v^i \simeq \frac{\mathcal{O}_v/\mathfrak{p}_v^{i+1}}{\mathfrak{p}_v^i/\mathfrak{p}_v^{i+1}}.$$

El resultado se sigue de que el último cociente es finito y su denominador también. La fórmula es clara a partir de esto. □

Teorema 1.7.2. *Si K es completo entonces $\mathcal{O}_v$ es compacto (y, por lo tanto, también lo son los conjuntos $\mathfrak{p}_v^m$, $1 + \mathfrak{p}_v^m$ y $\mathcal{U}_v$, al ser cerrados de $\mathcal{O}_v$).*

Dem. Probaremos que $\mathcal{O}_v$ es completo y totalmente acotado (es decir, para cada $\epsilon > 0$ existe un cubrimiento finito de $\mathcal{O}_v$ por conjuntos de diámetro menor o igual que ϵ). Como $\mathcal{O}_v$ es cerrado, es completo, luego, basta probar que es totalmente acotado. Sea π un uniformizador y $|\pi|_v = c < 1$. Afirmamos que el diámetro del conjunto $\mathfrak{p}_v^i$ es c^i. Supongamos esto probado. Entonces como $\mathcal{O}_v/\mathfrak{p}_v^i$ es finito, se sigue que $\mathcal{O}_v$ está cubierto por las finitas coclases de $\mathcal{O}_v/\mathfrak{p}_v^i$, y cada una de estas coclases tiene el mismo diámetro que $\mathfrak{p}_v^i$ (al ser $a \mapsto a+\mathfrak{p}_v^i$ una isometría), de manera que si tomamos i suficientemente grande, tienen diámetros menores que ϵ y el teorema queda probado.

Probemos ahora que el diámetro de $\mathfrak{p}_v^i$ es c^i. Es claro que es menor o igual, ya que v es no arquimedeano. Además, π^i y 0 están en $\mathfrak{p}_v^i$, y distan en exactamente c^i. □

Corolario 1.7.3. *Si K es completo entonces es localmente compacto y totalmente disconexo, y también lo es $K^\times$.*

Dem. Se sigue de que los conjuntos que forman (en ambos casos) un sistema fundamental de entornos de la unidad son compactos. □

También vale el recíproco al corolario.

Teorema 1.7.4. *Sea K un cuerpo con un valor absoluto no arquimedeano $|.|$, localmente compacto. Entonces K es completo, el cuerpo residual es finito y $|.|$ es discreto.*

Dem. Sea c un entorno compacto de 0. Entonces $\pi^n\mathcal{O}_v \subset c$ para n suficientemente grande; como es un cerrado entonces es compacto, y, por lo tanto, $\mathcal{O}_v$ lo es. Como estamos en un espacio métrico, toda sucesión de $\mathcal{O}_v$ tiene una subsucesión convergente, y es fácil deducir de esto que K es completo. Sea $(a_i)_{i\in I}$ un sistema de representantes en $\mathcal{O}_v$ de $\mathcal{O}_v/\mathfrak{p}_v$. Entonces $U_i = \{x \in \mathcal{O}_v : |x - a_i| < 1\}$ es un cubrimiento por abiertos de $\mathcal{O}_v$; como éste es compacto, se sigue que el cuerpo residual es finito. Por último, $\mathfrak{p}_v$ es compacto pues es cerrado en $\mathcal{O}_v$. Sea S_n el conjunto de los $\alpha \in K$ tales que $|\alpha| < 1 - 1/n$. Entonces S_n $(n \in \mathbb{N})$ es un cubrimiento por abiertos de $\mathfrak{p}_v$, y, por lo tanto, $\mathfrak{p}_v = S_n$ para algún n. Dejamos como ejercicio ver que esto implica que $|.|$ es discreto. □

Definición 1.7.5. K es un *cuerpo local* si es localmente compacto respecto a un valor absoluto no trivial.

Los últimos resultados nos dicen que si K es un cuerpo con un primo discreto no arquimedeano v, tal que el cuerpo residual es finito, entonces la completación K_v es un cuerpo local.

Se conoce la estructura de todos los cuerpos locales:

1. Si la característica de K es 0 entonces K es una extensión finita de $\mathbb{Q}_p$ si el primo es no arquimedeano, de grado $n = ef$, donde e es el índice de ramificación $v(p)$ y f el grado de inercia $[k : \mathbb{F}_p]$; si el primo es arquimedeano, K es isomorfo a $\mathbb{R}$ o a $\mathbb{C}$ con sus valores absolutos usuales.

2. Si la característica de K es $p > 0$ entonces K es isomorfo a un cuerpo $k((T))$ de series de potencias formales, donde k es un cuerpo finito y T es un uniformizador.

El primer caso es el que ocurre en las completaciones de cuerpos de números.

Definición 1.7.6. K es un cuerpo global si

(a) es una extensión finita de $\mathbb{Q}$, o

(b) es una extensión finita de $\mathbb{F}_q(t)$ para un cierto q y t trascendente sobre $\mathbb{F}_q$.

Los cuerpos globales tienen la característica de que todas sus completaciones K_v son espacios localmente compactos, y casi todos tienen un subanillo compacto y abierto.

Definición 1.7.7. Sea K un cuerpo y v un primo no arquimedeano discreto de K, tal que el cuerpo residual k es finito con $q = p^f$ elementos. Sea π un uniformizador. Decimos que un valor absoluto $|.|_v$ está *normalizado* si

$$|\pi|_v = q^{-1}.$$

Observación 1.7.8. Siempre hay un valor absoluto normalizado. Si π es un uniformizador y $|.|$ es un valor absoluto cualquiera correspondiente al primo v, sea $c = |\pi|$. Si tomamos $|.|_v = |.|^a$ (donde $a = -\log_c q$), $|.|_v$ está normalizado.

Dicho de otra manera, si ord es una valuación discreta normalizada asociada a v, el valor absoluto $|x|_v = q^{-\mathrm{ord}(x)}$ está normalizado.

Ejemplo 1.7.9. Sea A un dominio de Dedekind y $K = \mathrm{Frac}(A)$. Dado un ideal primo $\mathfrak{P} \subset A$, supongamos que $A/\mathfrak{P}$ es finito, de cardinal q, y definimos como antes

$$|x|_{\mathfrak{P}} = q^{-\mathrm{ord}_{\mathfrak{P}}(x)},$$

donde $\mathrm{ord}_{\mathfrak{P}}$ es la valuación discreta normalizada dada por la factorización en ideales primos. Entonces $|.|_{\mathfrak{P}}$ es un valor absoluto normalizado.

En el caso en que $A = \mathcal{O}_K$ sea el anillo de enteros del cuerpo de números K, tenemos que $q = N\mathfrak{P} = p^f$, donde $N\mathfrak{P}$ denota la norma (usual) del ideal $\mathfrak{P}$, es decir, el índice de $\mathfrak{P}$ en $\mathcal{O}_K$. El primo p es el único tal que $\mathfrak{P} \cap \mathbb{Z} = p\mathbb{Z}$, y f es el grado de la extensión $[\mathcal{O}_K/\mathfrak{P} : \mathbb{F}_p]$ (*grado de inercia* de $\mathfrak{P}$). De ahora en más, si K es un cuerpo de números y v un primo de K, $|.|_v$ denotará el valor absoluto normalizado recién definido.

Capítulo 2

Primos y extensiones

En este capítulo tendremos como objetivo principal caracterizar los primos de un cuerpo de números. Para ello, debemos analizar cómo se comportan los primos en las extensiones.

2.1. Producto tensorial de cuerpos

Sea K un cuerpo y A, B cuerpos que contienen a K. Podemos formar la K-álgebra $A \otimes_K B$. Sea $\{b_1, ..., b_n\}$ una base de B como K-espacio vectorial, y supongamos que A es un cuerpo topológico. Entonces podemos considerar la biyección

$$A \otimes_K B \to A^n,$$
$$\sum_{i=1}^{n} a_i \otimes b_i \mapsto (a_1, ..., a_n),$$

que nos permite darle a $A \otimes_K B$ una topología, llamada *topología del producto tensorial*, que, además, hace que la suma y la multiplicación sean continuas.

Podemos considerar también el morfismo $A \to A \otimes_K B$, $a \mapsto a \otimes 1$, que es inyectivo por ser A un cuerpo.

Lema 2.1.1. *Supongamos que B es una extensión separable de K de grado n. Entonces $A \otimes_K B$ es isomorfo al producto directo de un número finito de cuerpos K_j, cada uno conteniendo una copia isomorfa de A y una copia isomorfa de B. Más aún, K_j es una extensión finita y separable de A.*

Dem. Escribamos $B = K(\theta)$, con $\theta \in K$, y sea f el polinomio minimal de θ sobre K; es un polinomio separable irreducible de grado n. El conjunto $\{1, \theta, ..., \theta^{n-1}\}$ es una base de B como K-espacio vectorial, y, por lo tanto, $A \otimes_K B = A[\overline{\theta}]$ (viendo a A dentro de $A \otimes_K B$), donde $\{1, \overline{\theta}, ..., \overline{\theta}^{n-1}\}$ son linealmente independientes sobre A y $f(\overline{\theta}) = 0$.

Si bien f es irreducible en $K[X]$, no tiene por qué serlo en $A[X]$. Supongamos que la factorización en irreducibles de $A[X]$ es

$$f = \prod_{j=1}^{J} g_j.$$

Al ser f separable, los g_j deben ser distintos. Sea $K_j = A(\theta_j)$, donde θ_j es una raíz de g_j.

Consideramos para cada j el morfismo de anillos

$$\mu_j : A \otimes_K B \to K_j,$$

$$h(\overline{\theta}) \mapsto h(\theta_j) \quad h \in A[X],$$

y tomamos el morfismo

$$\prod_{j=1}^{J} \mu_j : A \otimes_K B \to \prod_{j=1}^{J} K_j.$$

Afirmamos que es un isomorfismo. Sea $h \in A[X]$ tal que $h(\overline{\theta})$ está en el núcleo. Entonces h es divisible por todos los g_j, con lo cual, también es divisible por f y, por lo tanto, $h(\theta) = 0$. Luego, el morfismo es inyectivo. Además, ambos tienen la misma dimensión como A-espacio vectorial, y, por lo tanto, la aplicación es un isomorfismo.

Basta ver que los morfismos de anillos

$$B \to A \otimes_K B \to K_j$$

son monomorfismos. Para ello basta ver que son no nulos, por ser B un cuerpo, y esto es trivial. □

Corolario 2.1.2. *Para $\alpha \in B$, se tiene que (viendo a B metido en K_j)*

$$\mathrm{N}_{B/K}\, \alpha = \prod_{j=1}^{J} \mathrm{N}_{K_j/A}\, \alpha :$$

$$\mathrm{Tr}_{B/K}\, \alpha = \sum_{j=1}^{J} \mathrm{Tr}_{K_j/A}\, \alpha.$$

Dem. Sea $\{b_1, ..., b_n\}$ una base de B como K-espacio vectorial y $\{1 \otimes b_1, ..., 1 \otimes b_n\}$ la correspondiente base de $A \otimes_K B$ como A-espacio vectorial. La norma y la traza de α son el determinante y la traza de la transformación lineal $x \mapsto \alpha x$ ($x \in B$), y es fácil ver usando estas bases que son iguales al determinante y la traza de la transformación lineal $x \mapsto (1 \otimes \alpha)x$ ($x \in A \otimes_K B$). Vía la identificación anterior como suma directa de subespacios, la transformación lineal es multiplicar por $(\alpha, ..., \alpha)$ (viendo aquí a α como $\mu_j(1 \otimes \alpha)$), y los subespacios K_j quedan invariantes bajo esta aplicación. Luego, se siguen las fórmulas. □

2.2. Extensión de valores absolutos

Proposición 2.2.1. *Sea K un cuerpo con un valor absoluto $|.|$, respecto del cual es completo, y sea V un K-espacio vectorial de dimension finita. Entonces todas las normas sobre V son equivalentes. En particular, V es completo.*

Dem. [Lan93]. □

Sean $K \subset L$ cuerpos, con $|.|_K$, $|.|_L$ valores absolutos. Decimos que $|.|_L$ *extiende* a $|.|_K$ si coinciden en K. Si v, w son primos sobre K y L, con valores absolutos $|.|_v$ y $|.|_w$, decimos que w extiende a v (o está sobre v) si $|.|_w$ es equivalente a $|.|_v$ sobre K.

Teorema 2.2.2. *Sea K completo con respecto a un valor absoluto $|.|$ y sea L/K una extensión finita de grado n. Entonces existe exactamente un valor absoluto sobre L que extiende a $|.|$; es más, viene dado por*

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

Dem. Unicidad. Si dos valores absolutos $|.|_1$ y $|.|_2$ extienden a $|.|$ entonces son normas equivalentes por la proposición anterior, y, por lo tanto, definen la misma topología en L. Luego, son valores absolutos equivalentes, con lo cual, $|.|_1 = |.|_2^a$ para algún a. Como coinciden en K, debe ser $a = 1$.

Existencia. Haremos la demostración en el caso en que K sea localmente compacto; es el único caso que necesitaremos (los cuerpos completos que consideraremos en este trabajo serán todos completaciones de cuerpos de números, que son localmente compactos).

Es claro que la fórmula propuesta cumple las dos primeras propiedades de un valor absoluto, y que extiende a $|.|$. La dificultad consiste en probar que existe C tal que $|1 + y|_L \leq C$ para $|y|_L \leq 1$. Sea $\|.\|$ una norma en L, considerado como K-espacio vectorial (siempre existe; por ejemplo, la norma infinito, definida a partir de una base). Luego, la fórmula para $|.|_L$ define una función no nula, continua en el conjunto compacto $\{\|y\| = 1\}$. Sean Δ, δ tales que $\Delta \geq |y|_L \geq \delta > 0$ para $\|y\| = 1$. Luego, obtenemos que

$$\Delta \geq \frac{|y|_L}{\|y\|} \geq \delta > 0$$

para todo $y \neq 0$. Supongamos ahora que $|y|_L \leq 1$. Entonces $\|y\| \leq \delta^{-1}$ y, por lo tanto,

$$|1 + y|_L \leq \Delta\|1 + y\| \leq \Delta(\|1\| + \|y\|) \leq \Delta(\|1\| + \delta^{-1}) = C.$$

□

Observación. Si bien en la demostración probamos directamente que la fórmula sirve, es útil notar que en verdad es consecuencia de la existencia y unicidad. En efecto, sea M la clausura normal de L/K; luego, existe una única extensión de $|.|$ a M, que denotamos por $|.|_M$. Si σ es un automorfismo de M/K entonces

$$|y|_\sigma = |\sigma y|_M$$

también es una extensión de $|.|$ a M, de manera que $|.|_\sigma = |.|_M$. Ahora,

$$\mathrm{N}_{L/K}\, y = \prod_\sigma \sigma y$$

para $y \in L$, donde σ recorre todos los automorfismos de M/K. Luego,

$$|\,\mathrm{N}_{L/K}\, y| = |\,\mathrm{N}_{L/K}\, y|_M = \prod_\sigma |\sigma y|_M = |y|_M^n,$$

donde $n = [L : K]$.

De la Proposición 2.2.1 y el Teorema 2.2.2 obtenemos inmediatamente el siguiente resultado.

Corolario 2.2.3. *Sea K un cuerpo y v un primo respecto del cual K es completo, y sea L/K una extensión finita y separable. Entonces existe un único primo w sobre v, y, además, L es completo.*

Teorema 2.2.4. *Sea K un cuerpo con un valor absoluto $|.|$, y sea L/K una extensión finita y separable de grado n. Entonces existen como mucho n extensiones de $|.|$ a L, digamos $|.|_1, ..., |.|_J$. Sean $\widetilde{K}$ y $L_1, ..., L_J$ las distintas completaciones. Entonces se tiene un isomorfismo algebraico y topológico*

$$\widetilde{K} \otimes_K L \simeq \prod_{j=1}^{J} L_j,$$

donde el miembro de la derecha tiene la topología producto. Además, los L_j son extensiones finitas y separables de $\widetilde{K}$.

Dem. Sabemos que $\widetilde{K} \otimes_K L$ es de esa forma, donde los L_j son extensiones finitas y separables de $\widetilde{K}$. Como $\widetilde{K}$ es completo, por el teorema anterior tenemos que existe una única extensión $|.|_j^*$ de $|.|$ a los L_j, y estos resultan completos respecto de este valor absoluto. Más aún, por la demostración del Lema 2.1.1, se tienen inyecciones

$$\lambda_j : L \to \widetilde{K} \otimes_K L \to L_j.$$

Luego, podemos definir una extensión $|.|_j$ en L de $|.|$ poniendo

$$|y|_j = |\lambda_j y|_j^*.$$

Por otra parte, $\lambda_j(L)$ es denso en L_j respecto de $|.|_j$, porque $L = K \otimes_K L$ es denso en $\widetilde{K} \otimes_K L$ y la aplicación $\widetilde{K} \otimes_K L \to L_j$ es suryectiva y continua. Luego, L_j es exactamente la completación de L respecto de $|.|_j$. Ahora debemos probar que los $|.|_j$ son distintos y que son las únicas extensiones de $|.|$ a L.

Sea $\|.\|$ un valor absoluto (no trivial) en L que extiende a $|.|$. Entonces $\|.\|$ se extiende por continuidad a una función $\widetilde{K} \otimes_K L \to \mathbb{R}$, también denotada $\|.\|$. Por continuidad, se tiene que si $x, y \in \widetilde{K} \otimes_K L$ entonces $\|x + y\| \leq \max(\|x\|, \|y\|)$ y $\|xy\| = \|x\|\|y\|$.

Consideremos $\|.\|$ restringido a un cierto L_j (vía $L_j \to \widetilde{K} \otimes_K L$, $x \mapsto (0, .., x, .., 0)$). Si en algún $x \in L_j$, $\|x\| \neq 0$ entonces $\|x\| = \|y\|\|xy^{-1}\|$ para todo $y \neq 0$ en L_j, de manera que la restricción es idénticamente nula o es un valor absoluto en L_j. En realidad, $\|.\|$ no puede inducir un valor absoluto en dos L_j distintos:

$$(x_1, 0, ..., 0).(0, x_2, ..., 0) = (0, ..., 0),$$

y, por lo tanto, $\|x_1\|\|x_2\| = 0$ si $x_1 \in L_1$, $x_2 \in L_2$. Además, hay algún L_j tal que sobre él no es idénticamente nulo.

Luego, $\|.\|$ induce un valor absoluto en exactamente un L_j y claramente extiende el valor absoluto $|.|$ de $\widetilde{K}$. Luego, $\|.\| = |.|_j$ para exactamente un j.

Sólo resta probar que el isomorfismo enunciado es también topológico. Sea $(x_1, ..., x_n) \in \prod_{j=1}^{J} L_j$. Sea

$$\|(x_1, ..., x_n)\| = \text{máx}(|x_j|_j).$$

Claramente, $\|.\|$ es una norma en el $\widetilde{K}$-espacio vectorial $\prod_{j=1}^{J} L_j$ que induce la topología producto. Por otra parte, cualquier par de normas son equivalentes, al ser $\widetilde{K}$ completo; de esta manera, $\|.\|$ induce la topología del producto tensorial en $\widetilde{K} \otimes_K L$, y esto prueba que la aplicación es un homeomorfismo. □

De las demostraciones anteriores obtenemos el siguiente resultado.

Corolario 2.2.5. *Sea $L = K(\theta)$ (separable) y sea $f \in K[X]$ el polinomio minimal de θ. Supongamos que*

$$f = \prod_{j=1}^{J} g_j$$

es la factorización en irreducibles de f en $\widetilde{K}[X]$. Entonces $L_j = \widetilde{K}(\theta_j)$, donde $g_j(\theta_j) = 0$.

2.3. Valores absolutos normalizados

Sea K un cuerpo con un valor absoluto $|.|$. Principalmente nos interesarán los siguientes casos:

- $|.|$ es discreto no arquimedeano, con cuerpo residual finito.
- La completación de K es $\mathbb{R}$.
- La completación de K es $\mathbb{C}$.

Estos casos se pueden resumir en una sola condición: que la completación sea localmente compacta (en el caso de característica 0). La razón principal por la cual nos centramos en estos casos es que, como veremos, son los únicos valores absolutos posibles que se pueden definir sobre un cuerpo de números.

En el primer caso, tenemos una noción, según la Definición 1.7.7, de que $|.|$ sea un valor absoluto normalizado. En el segundo caso, decimos que $|.|$ es normalizado si es igual al valor absoluto usual de $\mathbb{R}$, mientras que en el último caso si es el *cuadrado* del valor absoluto usual de $\mathbb{C}$.

Queremos ver ahora cuál es la extensión normalizada de un valor absoluto normalizado. Sea K completo respecto a un valor absoluto $|.|$ discreto y no arquimedeano. Sea L/K finita y separable, $\mathcal{O}_K$, $\mathcal{O}_L$ los anillos de valuación discreta correspondientes y $\mathfrak{p}$, $\mathfrak{P}$ sus ideales maximales, donde $\mathfrak{p} = (\pi)$ y $\mathfrak{P} = (\Pi)$. Como $\mathcal{O}_L$ es la clausura entera de $\mathcal{O}_K$ en L, podemos usar los resultados del Capítulo 1 sobre dominios de Dedekind. Entonces se tiene que $\pi = u\Pi^e$ para algún e (el índice de ramificación), con u una unidad. Sea f el índice de inercia de $\mathfrak{P}$ sobre $\mathfrak{p}$, y sean q y Q los grados residuales, de manera que q es el cardinal de $\mathcal{O}_K/\mathfrak{p}$ y Q el de $\mathcal{O}_L/\mathfrak{P}$. Como son anillos de valuación discreta, hay un único primo en cada uno, de manera que $ef = n$. Además, $Q = q^f$.

Teorema 2.3.1. *Sea K completo respecto al valor absoluto normalizado $|.|$ y sea L una extensión finita y separable de K de grado n. Entonces el valor absoluto normalizado $\|.\|$ que es equivalente a la única extensión de $|.|$ a L está dado por*

$$\|y\| = |\,\mathrm{N}_{L/K}\, y| \quad .$$

Dem. En el caso arquimedeano las dos posibilidades son triviales. Supongamos entonces que K es no arquimedeano. Sea $|.|_L$ la única extensión de $|.|$ a L; luego, sabemos que $\|.\| = |.|^c$ para algún c; queremos ver que $c = n$. Probaremos que la fórmula vale para un uniformizador, y eso será suficiente. Con la notación de las últimas observaciones,

$$\|\pi\| = \|\Pi\|^e = Q^{-e} = q^{-ef} = |\pi|^n.$$

□

En el caso no completo, el resultado es el siguiente.

Teorema 2.3.2. *Sea $|.|$ un valor absoluto normalizado en un cuerpo K, y sea L/K finita y separable de grado n. Entonces*

$$\prod_{j=1}^{J} \|y\|_j = |\,\mathrm{N}_{L/K}\, y|,$$

donde $\|.\|_j$ son los valores absolutos normalizados equivalentes a las extensiones de $|.|$ a L.

Dem. Escribamos

$$\widetilde{K} \otimes_K L = \prod_{j=1}^{J} L_j,$$

donde $\widetilde{K}$ es la completación de K, como en el Teorema 2.2.4. Entonces por el Corolario 2.1.2 se tiene que, para $y \in L$,

$$\mathrm{N}_{L/K}\, y = \prod_{j=1}^{J} \mathrm{N}_{L_j/\widetilde{K}}\, y.$$

Como $|.|$ es un valor absoluto normalizado en $\widetilde{K}$, sea $\|.\|_j$ la extensión normalizada en L_j. Por el teorema anterior,

$$\prod_{j=1}^{J} \|y\|_j = \prod_{j=1}^{J} |\,\mathrm{N}_{L_j/\widetilde{K}}\, y|_j = \prod_{j=1}^{J} |\,\mathrm{N}_{L_j/\widetilde{K}}\, y| = |\prod_{j=1}^{J} \mathrm{N}_{L_j/\widetilde{K}}\, y| = |\,\mathrm{N}_{L/K}\, y|.$$

□

2.4. Extensiones locales inducidas

Sea K un cuerpo de números y v definido por un cierto ideal primo $\mathfrak{p}$ de $\mathcal{O}_K$, y sea L/K una extensión finita y separable. Tomemos la factorización

$$\mathfrak{p}\mathcal{O}_L = \mathfrak{P}_1^{e_1}...\mathfrak{P}_r^{e_r},$$

y elijamos w un primo en L definido por algún $\mathfrak{P}_i$ fijo, de manera que w está sobre v.

Tenemos la siguiente situación:

$$\begin{array}{ccc} L & \longrightarrow & L_w \\ \uparrow & & \uparrow \\ K & \longrightarrow & K_v. \end{array}$$

Ya vimos que la extensión L_w/K_v es finita y separable. Además, es inmediato que el primo w de L_w está sobre el primo v de K_v.

Sean $C = \widehat{\mathcal{O}_v}$ y $D = \widehat{\mathcal{O}_w}$. Afirmamos que D es la clausura entera de C en L_w. En efecto, es claro que $\widehat{\mathcal{O}_v} \subset \widehat{\mathcal{O}_w}$, de manera que la clausura entera de C en L_w está contenida en $\widehat{\mathcal{O}_w}$, al ser este último íntegramente cerrado en L_w. Por otra parte, todo elemento de $\widehat{\mathcal{O}_w}$ es entero sobre $\widehat{\mathcal{O}_v}$, y esto prueba lo que queríamos. De la misma manera, $\mathcal{O}_w = (\mathcal{O}_L)_{\mathfrak{P}_i}$ es la clausura entera de $\mathcal{O}_v = (\mathcal{O}_K)_{\mathfrak{P}}$ en L.

Esto, en particular, implica que $\widehat{\mathfrak{p}_w}$ es un ideal primo sobre $\widehat{\mathfrak{p}_v}$, al ser los únicos primos de dichos anillos de valuación discreta.

El índice de ramificación $e = e(\widehat{\mathfrak{P}_w}|\widehat{\mathfrak{p}_v})$ cumple que $\mathrm{ord}_w(x) = e.\,\mathrm{ord}_v(x)$ para todo $x \in K_v$. En particular, para todo $x \in K$. El e que cumple esto para $x \in K$ no es otro que el índice de ramificación $e(\mathfrak{P}_i|\mathfrak{p})$. Con respecto al índice de inercia $f = f(\widehat{\mathfrak{P}_w}|\widehat{\mathfrak{p}_v})$, sucede que $\widehat{\mathcal{O}_w}/\widehat{\mathfrak{P}_w} \simeq \mathcal{O}_w/\mathfrak{P}_w$, y $\widehat{\mathcal{O}_v}/\widehat{\mathfrak{p}_v} \simeq \mathcal{O}_v/\mathfrak{p}_v$. Luego, $f = f(\mathfrak{P}_w|\mathfrak{p}_v) = [\mathcal{O}_w/\mathfrak{P}_w : \mathcal{O}_v/\mathfrak{p}_v] = [\mathcal{O}_L/\mathfrak{P}_i : \mathcal{O}_K/\mathfrak{p}]$ (esta última igualdad se sigue de que $\mathcal{O}_v = (\mathcal{O}_K)_{\mathfrak{p}}$ y su ideal maximal es el generado por $\mathfrak{p}$, y de que el cuerpo residual de la localización en un maximal es el cuerpo residual global). Entonces f es el grado de inercia de $\mathfrak{P}_i$ sobre $\mathfrak{p}$.

Utilizando los resultados del capítulo I, se tiene que

$$[L_w : K_v] = e(\widehat{\mathfrak{P}_w}|\widehat{\mathfrak{p}_v})f(\widehat{\mathfrak{P}_w}|\widehat{\mathfrak{p}_v}).$$

De esta manera, $[L_w : K_v] = e(\mathfrak{P}_i|\mathfrak{p})f(\mathfrak{P}_i|\mathfrak{p})$.

2.5. Los primos de un cuerpo de números

Sea K un cuerpo de números. Dado $\mathfrak{P} \subset \mathcal{O}_K$ un ideal primo no nulo, tenemos definido el valor absoluto $|.|_{\mathfrak{P}}$, y dos ideales primos distintos dan lugar a valores absolutos no equivalentes. Además, para cada inmersión $\sigma : K \hookrightarrow \mathbb{C}$, tenemos el valor absoluto arquimedeano $|x|_\sigma = |\sigma x|$. Consideramos $\sigma_1, ..., \sigma_r$ las inmersiones *reales*, es decir, tales que la imagen está contenida en $\mathbb{R}$. Sean $\sigma_{r+1}, ..., \sigma_{r+s}$ las inmersiones *complejas* (esto es, cuya imagen no está contenida en $\mathbb{R}$), tales que ninguna es el conjugado de otra, de manera que $r + 2s = n = [K : \mathbb{Q}]$. En ambos casos, la completación K_σ de K no es otra cosa que la clausura de $\sigma(K)$ en $\mathbb{C}$. En el caso real,

al ser $\mathbb{Q} \subset \sigma(K) \subset \mathbb{R}$, se tiene que $K_\sigma = \mathbb{R}$. En el caso complejo, $K_\sigma \subset \mathbb{C}$ contiene a $\mathbb{R}$ propiamente, de manera que $K_\sigma = \mathbb{C}$.

Es claro que un valor absoluto arquimedeano no es equivalente a uno no arquimedeano.

Teorema 2.5.1 (Ostrowski)**.** *Los valores absolutos recién definidos son todos no equivalentes entre sí, y cualquier valor absoluto sobre K es equivalente a uno de ellos.*

Dem. El teorema ya lo probamos para $K = \mathbb{Q}$ en el capítulo I. Por las observaciones recién hechas, para la primer parte nos resta ver que si $|.|_{\sigma_i}$ es equivalente a $|.|_{\sigma_j}$ entonces $i = j$ $(i, j = 1, ..., r + s)$. Supongamos que son equivalentes. Entonces $\sigma_j \circ \sigma_i^{-1} : \sigma_i(K) \to \sigma_j(K)$ es una función continua (respecto al valor absoluto usual de $\mathbb{C}$) y se extiende, por lo tanto, a las clausuras, es decir, a las completaciones. Si σ_i es real, entonces $\overline{\sigma_i(K)} = \mathbb{R}$ y $\sigma_j \circ \sigma_i^{-1}$ es la identidad, ya que hay una única inmersión de $\mathbb{R}$ en $\mathbb{C}$. Luego, $\sigma_i = \sigma_j$, y, por lo tanto, $i = j$.

Si σ_i es complejo entonces σ_j también lo es, y la extensión de $\sigma_j \circ \sigma_i^{-1}$ es la identidad o la conjugación compleja. Por la elección que hicimos de los σ_i, debe ser la identidad, y en consecuencia $i = j$.

Finalmente, sea $|.|$ un valor absoluto sobre K. Entonces $|.|$ es equivalente sobre $\mathbb{Q}$ a $|.|_p$ para un único p primo o $p = \infty$. Recordemos que, por los resultados de las secciones anteriores, si $K = \mathbb{Q}(\theta)$ y f es el polinomio minimal de θ sobre $\mathbb{Q}$ entonces hay tantas extensiones de $|.|_p$ (digamos que hay J) como factores irreducibles tenga f en $\mathbb{Q}_p[X]$. Supongamos que $|.|$ es no arquimedeano, de manera que $p \in \mathbb{Z}$, y escribamos $p\mathcal{O}_K = \mathfrak{P}_1^{e_1}...\mathfrak{P}_r^{e_r}$. Entonces $J = r$; en efecto, escribamos

$$\mathbb{Q}_p \otimes_{\mathbb{Q}} K \simeq \prod_{j=1}^{J} K_j,$$

donde K_j son las completaciones. Como $|.|_{\mathfrak{P}_i}$ extienden a $|.|_p$, se tiene que $r \leq J$, y supongamos que las primeras r extensiones son las definidas por los $\mathfrak{P}_i$. Ahora bien, $n = \dim_{\mathbb{Q}}(K) = \dim_{\mathbb{Q}_p}(\mathbb{Q}_p \otimes_{\mathbb{Q}} K) = \sum_{j=1}^{r} e_j f_j$, donde f_j son los índices de inercia. Además, afirmamos que $e_j f_j = \mathrm{gr}(g_j)$ para $j = 1, .., r$; esto es pues el grado de g_j es el grado de la extensión $K_{\mathfrak{P}_j}/\mathbb{Q}_p$, y esto es igual a $e_j f_j$ por los resultados de la sección anterior.

Por otra parte,

$$\dim_{\mathbb{Q}_p}(\mathbb{Q}_p \otimes_{\mathbb{Q}} K) = \sum_{j=1}^{J} \dim_{\mathbb{Q}_p} K_j = \sum_{j=1}^{J} \mathrm{gr}(g_j).$$

Luego, $\sum_{j=1}^{r} \mathrm{gr}(g_j) = \sum_{j=1}^{J} \mathrm{gr}(g_j)$ y, por lo tanto, $r = J$. Entonces se sigue que las únicas extensiones de $|.|_p$ a K son las dadas por los $\mathfrak{P}_i$. En particular, como $|.|$ es equivalente sobre $\mathbb{Q}$ a $|.|_p$, se sigue que $|.|$ es equivalente a $|.|_{\mathfrak{P}_i}$ para algún i.

Supongamos que $|.|$ es arquimedeano. Entonces es equivalente a una extensión de $|.|_\infty$. La cantidad de extensiones J es exactamente el número de factores irreducibles que tiene f sobre $\mathbb{R}[X]$. Cada factor de grado 1 da lugar a una inmersión en $\mathbb{R}$ (la que manda θ en la raíz de tal factor), y al ser las raíces distintas (pues la extensión es separable), deben ser todas las inmersiones distintas. Luego, la cantidad de factores de grado 1 es menor o igual que r. De la misma manera, cada factor de grado 2 nos da dos maneras de meter K en $\mathbb{C}$ (no en $\mathbb{R}$), y una es

la conjugada de la otra. Se sigue que la cantidad de factores de grado 2 es menor o igual que s, y, por lo tanto, $J \leq r + s$. Como ya tengo $r + s$ extensiones, se sigue que todas están inducidas por las inmersiones en $\mathbb{C}$ (y son exactamente $r + s$). □

Si L/K es una extensión finita y separable y v es un primo infinito de K, entonces todo primo w de L sobre v es infinito. Escribimos $e(w|v) = 2$ si v es real y w es complejo, y 1 en cualquier otro caso. Decimos que v es *ramificado* en L si es real en K y alguna de sus extensiones a L es compleja. Escribimos $f(w|v) = 1$ siempre. Es fácil ver entonces que sigue valiendo la fórmula $[L_w : K_v] = e(w|v)f(w|v)$.

Teorema 2.5.2. *Sea L/K una extensión finita de cuerpos de números y v un primo de K. Entonces*

$$[L : K] = \sum_{w|v} [L_w : K_v].$$

El grado de la extensión local es ef, donde e y f son los índices de ramificación y de inercia de los primos en cuestión.

Además, si v es no arquimedeano, correspondiente a un ideal primo $\mathfrak{p}$, los únicos w que están sobre v son los definidos por los ideales primos que dividen a $\mathfrak{p}$; si v es arquimedeano, correspondiente a una inmersión σ, los únicos primos sobre v son los definidos por las extensiones de σ a L.

Dem. La fórmula se sigue del Teorema 2.2.4. La observación para los primos finitos se sigue de la demostración del teorema anterior. Para el caso infinito, sea v un primo de K correspondiente a una inmersión $\sigma : K \to \mathbb{C}$, y w un primo de L sobre K. Entonces sabemos que w está representado por un valor absoluto $|.|_\tau$, con $\tau : L \to \mathbb{C}$. Sea $\varphi = \tau|_K$. Se sigue inmediatamente que $|.|_\varphi$ es equivalente a $|.|_\sigma$, y, por lo tanto, $\varphi = \sigma$ o $\varphi = \overline{\sigma}$. Como tanto τ como $\overline{\tau}$ definen el mismo primo w, se sigue que w se corresponde con una extensión de σ a L. □

2.6. Acción del grupo de Galois y completaciones

Sea L/K una extensión finita de Galois de cuerpos de números, con $G = \mathrm{Gal}(L/K)$. Si $\sigma \in G$ y w es un primo de L, sea σw el primo definido por $|x|_{\sigma w} = |\sigma^{-1}x|_w$. Es fácil ver que en el caso en que w esté definido por un ideal primo $\mathfrak{P} \subset \mathcal{O}_L$, σw es el primo correspondiente al ideal $\sigma\mathfrak{P}$, mientras que si w es arquimedeano, digamos inducido por una inmersión $\theta : L \hookrightarrow \mathbb{C}$, entonces σw es el inducido por $\theta \circ \sigma^{-1}$.

Una sucesión de Cauchy para w, actuada por σ, nos da una sucesión de Cauchy para σw, y viceversa; luego, σ induce por continuidad un isomorfismo $\sigma_w : L_w \to L_{\sigma w}$. Si v es el primo de K debajo de w entonces σ_w es un K_v-isomorfismo.

Definimos ahora el grupo de descomposición de w como

$$D(w) = \{\sigma \in G : \sigma w = w\}.$$

Es claro que si w es no arquimedeano, correspondiente a un ideal primo $\mathfrak{P}$ entonces $D(w)$ coincide con lo que en el capítulo 1 llamamos $D(\mathfrak{P})$. La definición extiende esta noción para primos infinitos.

Notemos que

$$D(\sigma w) = \sigma D(w)\sigma^{-1},$$

con lo cual, el grupo de descomposición de w está determinado a menos de conjugación por el primo v.

Por lo dicho antes, se tiene una inyección $i : D(w) \to \mathrm{Gal}(L_w/K_v)$.

Proposición 2.6.1. *La extensión L_w/K_v es finita y Galois, y la inyección i es un isomorfismo.*

Dem. El caso arquimedeano es trivial, mientras que en el caso finito, ya vimos que la extensión es finita y separable. Entonces la proposición es equivalente a probar que las desigualdades

$$(D(w) : 1) \leq (\mathrm{Gal}(L_w/K_v) : 1) \leq [L_w : K_v]$$

son igualdades. Ya vimos en el capítulo 1 que efectivamente $(D(w) : 1) = e(w|v)f(w|v)$, y esto es el grado de la extensión L_w/K_v. □

Finalmente, en el primer capítulo vimos que dado un ideal primo $\mathfrak{p}$ de K, G actúa transitivamente sobre los ideales primos de L que están sobre $\mathfrak{p}$. El siguiente resultado afirma lo mismo para los infinitos.

Proposición 2.6.2. *Sea L/K de Galois y v un primo infinito de K. Entonces G actúa transitivamente sobre los primos de L sobre v.*

Dem. Sea $\sigma : K \to \mathbb{C}$ una inmersión correspondiente a v. La teoría básica de extensiones de Galois dice que hay exactamente $[L : K]$ extensiones de σ a L, y todas son de la forma $\tau\varphi^{-1}$, donde τ es una extensión fija cualquiera y $\varphi \in \mathrm{Gal}(L/K)$. Si w_1 y w_2 son primos infinitos de L sobre v, correspondientes a extensiones τ_1, τ_2 de σ, entonces existe $\varphi \in \mathrm{Gal}(L/K)$ tal que $\tau_2 = \tau_1\varphi^{-1}$. Entonces $w_1 = \varphi w_2$, pues $|x|_{w_2} = |\tau_2 x| = |\tau_1\varphi^{-1}x| = |\varphi^{-1}x|_{w_1} = |x|_{\varphi w_1}$. □

Capítulo 3

Adèles e Idèles

3.1. Producto directo restringido

Dado un cuerpo de números K (la teoría sigue siendo válida si tomamos más en general un cuerpo global, pero trabajaremos mayormente con cuerpos de números), para hablar de problemas del tipo "local-global", es a veces conveniente considerar todos los cuerpos K_v al mismo tiempo, y pegar de alguna manera toda esta información local para obtener datos globales. Para ello el lenguaje natural es el de adèles e idèles. Lo primero que uno trataría de hacer es formar el producto de todos los K_v. Aquí están todos los elementos que nos interesan, y es un anillo topológico, pero tiene varias desventajas: en principio, no es localmente compacto (y necesitamos compacidad local para hacer análisis), y la mayoría de sus elementos están completamente lejos de estar en la imagen natural de K en el producto. Sabemos que un elemento x de K está en $\mathcal{O}_v$ para casi todos los primos v. Esta última observación nos da una pista de qué es lo que debemos tomar; además, la topología que debemos considerar es a fin de cuentas la única que nos podría servir. Introduciremos ahora el tipo de objeto que buscamos de forma un poco más general.

Sea $\{G_v\}$ una familia de grupos topológicos abelianos localmente compactos, donde v recorre un cierto conjunto de índices. Sea S_0 un conjunto finito de índices, y supongamos que para cada $v \notin S_0$ tenemos un subgrupo $H_v \subset G_v$ abierto y compacto. Formamos el conjunto $\prod_v' G_v = \{(\alpha_v) : \alpha_v \in H_v \text{ para todo } v \text{ excepto para un conjunto finito } S \supset S_0\}$. Esto es claramente un subgrupo del producto directo de los G_v, y se llama el *producto directo restringido* de los grupos G_v respecto de los subgrupos H_v.

Para cada conjunto finito $S \supset S_0$, consideramos los conjuntos

$$\prod_{v \in S} N_v \times \prod_{v \notin S} H_v,$$

donde $N_v \subset G_v$ es un entorno de 1 en G_v. Es fácil ver que esta familia sirve como un sistema fundamental de entornos del 1 y, por lo tanto, $\prod_v' G_v$ es un grupo topológico. Además, en los conjuntos

$$G^S = \prod_{v \in S} G_v \times \prod_{v \notin S} H_v$$

(que son abiertos) la topología producto es la misma que la heredadad del producto directo restringido; de esta manera son localmente compactos, y, por lo tanto, también lo es el producto directo restringido. Finalmente, notemos que si los G_v son anillos topológicos, y los H_v son subanillos abiertos y compactos entonces el producto directo restringido resulta un anillo topológico localmente compacto (con las operaciones naturales).

3.2. Adèles

Consideremos un cuerpo de números K. A partir de ahora, cada vez que pongamos $|.|_v$ nos referiremos a un valor absoluto normalizado.

Como se ve en las demostraciones de que el grupo de clases de K es finito y del teorema de las unidades de Dirichlet, es conveniente ver a K metido en un espacio euclídeo $\mathbb{R}^n$ ($n = [K : \mathbb{Q}]$), viendo este ultimo espacio como el producto de las completaciones de K en todos los primos arquimedeanos. Veremos que es útil considerar todos los primos de K. El lenguaje del producto directo restringido nos será muy útil en este caso. Obtendremos resultados importantes sobre la aritmética intrínseca de K a partir de argumentos topológicos sobre los adèles e idèles (en particular, probaremos una versión más general de los teoremas recién mencionados).

Sean K_v todas las completaciones de K, donde v recorre los primos de K. Son anillos topológicos localmente compactos. Sea S_∞ el conjunto de los primos arquimedeanos, de manera que si $v \notin S_\infty$, tenemos que K_v tiene un subanillo abierto y compacto, vale decir, $\widehat{\mathcal{O}}_v$. A partir de ahora, escribiremos simplemente $\mathcal{O}_v$ para referirnos a este anillo, para no sobrecargar la notación. Llamaremos *anillo de adèles* $\mathbb{A}_K$ de K al producto directo restringido correspondiente, que es un anillo localmente compacto.

Dado $S \supset S_\infty$ finito, llamaremos a $\mathbb{A}_K^S$ el conjunto de *S-adèles*, es decir,

$$\mathbb{A}_K^S = \prod_{v \notin S} \mathcal{O}_v \times \prod_{v \in S} K_v.$$

Existe una inyección natural $K \to \mathbb{A}_K$ dada por $x \mapsto (x, x, ...)$, dado que si $x \in K$ entonces está en K_v para todo v y en $\mathcal{O}_v$ para todos los primos no arquimedeanos excepto para un número finito. Llamaremos a los elementos de esta imagen *adèles principales*. Probaremos primero que K es discreto con la topología inducida de $\mathbb{A}_K$, y luego un teorema fundamental que afirma que $\mathbb{A}_K/K$ es compacto.

Los entornos de 0 en la topología de los adèles son los conjuntos $\prod_{v \in S} N_v(\epsilon) \times \prod_{v \notin S} \mathcal{O}_v$, donde $N_v(\epsilon) = \{x \in K_v : |x|_v < \epsilon\}$, con $\epsilon > 0$ y $S \supset S_\infty$ finito.

El siguiente teorema es una generalización del teorema chino del resto. La denominación "débil" es porque hay un teorema de aproximación "fuerte", que es más complicado de probar y no necesitaremos.

Teorema 3.2.1 (Teorema de aproximación débil)**.** *Sean $v_1, ..., v_r$ primos de K, $x_1, \dots, x_r \in K$ y $\epsilon > 0$. Entonces existe $x \in K$ tal que $|x - x_i|_{v_i} < \epsilon$ $(1 \leq i \leq r)$.*

Dem. Probaremos primero que existen $y_i \in K$ $(i = 1, \dots, n)$ tales que $|y_i|_{v_i} > 1$ y $|y_i|_{v_j} < 1$ $(j \neq i)$. En ese caso, $\lim_{k\to\infty} \frac{y_i^k}{1+y_i^k} = \lim_{k\to\infty} \frac{1}{1+y_i^{-k}} = 1$ con respecto a v_i, y 0 con respecto a

v_j para $j \neq i$. Si tomamos

$$x = \sum_{i=1}^{r} \frac{y_i^k}{1+y_i^k} x_i$$

con k suficientemente grande, x cumple que $|x' - x_i|_{v_i} < \epsilon$ para $i = 1, \ldots, r$.

Por simetría, basta encontrar y_1 tal que $|y_1|_{v_1} > 1$ y $|y_1|_{v_i} < 1$ para $i = 2, \ldots, n$. Lo hacemos por inducción en r.

$r = 2$: como v_1 y v_2 no son equivalentes, existen $\alpha, \beta \in K$ tal que $|\alpha|_{v_1} < 1$, $|\alpha|_{v_2} \geq 1$, $|\beta|_{v_1} \geq 1$ y $|\beta|_{v_2} < 1$. Tomamos entonces $y_1 = \beta\alpha^{-1}$.

$r \geq 3$: por el caso $r-1$, existe $z \in K$ tal que $|z|_{v_1} > 1$, $|z|_{v_i} < 1$ ($i = 2, \ldots, r-1$), y por el caso $r = 2$, existe $w \in K$ tal que $|w|_{v_1} > 1$, $|w|_{v_r} < 1$. Tomamos entonces

$$y_1 = \begin{cases} z & \text{si} \quad |z|_{v_r} < 1; \\ z^k w & \text{si} \quad |z|_{v_r} = 1; \\ \frac{z^k}{1+z^k} w & \text{si} \quad |z|_{v_r} > 1 \end{cases}$$

donde $k \in \mathbb{N}$ es suficientemente grande. □

Observación. El teorema de aproximación sigue valiendo si en lugar de tomar $x_i \in K$ tomamos $x_i \in K_{v_i}$: basta tomar $x_i' \in K$ cerca de x_i y $x \in K$ cerca de los x_i'. El teorema dice entonces que K es denso en $\prod_{i=1}^{r} K_{v_i}$ (incluido de manera diagonal).

Teorema 3.2.2 (Fórmula del producto)**.** *Sea K un cuerpo de números y $x \in K^\times$. Entonces*

$$\prod_v |x|_v = 1,$$

donde v recorre todos los primos de K y $|.|_v$ son los valores absolutos normalizados.

Dem. Notemos que en el producto hay sólo finitos términos distintos de 1, ya que un elemento no nulo de un cuerpo de números es una unidad para casi todos los primos. Luego, el producto está efectivamente bien definido.

Probaremos primero la fórmula para $K = \mathbb{Q}$. En este caso, si $p, q \in \mathbb{N}$ son números primos, $|q|_p = 1$ si $q \neq p$ y $|q|_q = 1/q$. Además, $|q|_\infty = q$, con lo cual, la fórmula vale para primos, y por multiplicatividad vale para todo $x \in \mathbb{Q}^\times$.

Ahora sea K cualquiera y $x \in K^\times$. Para cada p primo de $\mathbb{Q}$ (incluyendo ∞), se tiene por el Teorema 2.3.2 que

$$|\,\mathrm{N}_{K/\mathbb{Q}}\, x|_p = \prod_{v|p} |x|_v,$$

y, por lo tanto,

$$\prod_v |x|_v = \prod_p \prod_{v|p} |x|_v = \prod_p |\,\mathrm{N}_{K/\mathbb{Q}}\, x|_p = 1.$$

□

Proposición 3.2.3. *La inyección $K \hookrightarrow \mathbb{A}_K$ manda K en un subanillo discreto.*

Dem. Probemos que 0 es un punto aislado de $\mathbb{A}_K$. Decir que un elemento (α_v) está cerca de 0 en la topología de los adèles es decir que $|\alpha_v|_v \leq 1$ para todos los v salvo finitos de ellos, para los cuales $|\alpha_v| < \epsilon$ para cierto $\epsilon > 0$. Esto implica que $(\alpha_v) = 0$ por la fórmula del producto. □

Proposición 3.2.4. *Tenemos que $\mathbb{A}_K^{S_\infty} + K = \mathbb{A}_K$.*

Dem. Sea $\alpha = (\alpha_v) \in \mathbb{A}_K$. Sea $T = \{v < \infty : \alpha_v \notin \widehat{\mathcal{O}}_v\}$. Utilizando la Proposición 1.4.6 (y el hecho de que $\mathcal{O}_v/\mathfrak{p}_v \simeq \widehat{\mathcal{O}}_v/\widehat{\mathfrak{p}}_v$), podemos escribir, para cada $v \in T$, $\alpha_v = \psi_v + \beta_v$, donde $\beta_v \in \widehat{\mathcal{O}}_v$ y $\psi_v \in K$ es un elemento tal que $|\psi_v|_w \leq 1$ para todo $w \neq v$ finito. Para $v \notin T$, finito, tomemos $\beta_v = \alpha_v$ y $\psi_v = 0$. Como T es finito, tiene sentido considerar $\psi = \sum_{v<\infty} \psi_v \in K$. Afirmamos que $\alpha - \psi \in \mathbb{A}_K^{S_\infty}$. En efecto, si v es un primo finito,

$$(\alpha - \psi)_v = \alpha_v - \psi_v - \sum_{w \neq v} \psi_w = \beta_v - \sum_{w \neq v} \psi_w \in \widehat{\mathcal{O}}_v.$$

Esto termina la demostración, pues $\alpha = \alpha - \psi + \psi$. □

Teorema 3.2.5. *El conjunto $\mathbb{A}_K/K$ es compacto.*

Dem. Probaremos que existe $D \subset \mathbb{A}_K^{S_\infty}$ compacto tal que

$$D + \mathcal{O}_K = \mathbb{A}_K^{S_\infty}.$$

Entonces por la proposición anterior,

$$D + K = D + \mathcal{O}_K + K = \mathbb{A}_K^{S_\infty} + K = \mathbb{A}_K,$$

y, por lo tanto, $\mathbb{A}_K/K$, al ser la imagen de D bajo la aplicación continua canónica

$$\mathbb{A}_K \to \mathbb{A}_K/K,$$

resultará compacto.

Sea $R_\infty = \prod_{v \in S_\infty} K_v$, un $\mathbb{R}$-espacio vectorial de dimensión $r + 2s = n = [K : \mathbb{Q}]$. Podemos meter K en R_∞ vía la aplicación

$$x \mapsto (x^{(1)}, ..., x^{(r+s)}),$$

donde $x \mapsto x^{(i)}$ son las inmersiones de K en $\mathbb{C}$. Sea $\{\theta_1, ..., \theta_n\}$ una base entera de K; afirmamos que las imágenes de estos elementos forman una base de R_∞ sobre $\mathbb{R}$. En efecto, la imagen de θ_i es el vector

$$(\theta_i^{(1)}, ..., \theta_i^{(r)}, \frac{\theta_i^{(r+1)} + \overline{\theta_i^{(r+1)}}}{2}, \frac{\theta_i^{(r+1)} - \overline{\theta_i^{(r+1)}}}{2i}, ...) \in \mathbb{R}^n.$$

Haciendo operaciones elementales de filas en una matriz, se ve que el determinante de esta colección de n vectores es simplemente $2^s \det(\theta_i^{(j)})_{ij}$. Esto no es otra cosa que 2^s multiplicado

por el discriminante de la base $\{\theta_1, ..., \theta_n\}$, que es distinto de 0. Luego, las imágenes de los θ_i son linealmente independientes y, por lo tanto, forman una base de $\mathbb{R}^n$.

Para simplificar la notación, identifiquemos $\mathcal{O}_K$ con su imagen en $\mathbb{R}_\infty$. Luego, todo elemento $a \in R_\infty$ se escribe de manera única como

$$a = b + c$$

con $c \in \mathcal{O}_K$ y $b = \sum_{i=1}^n t_i\theta_i$, $0 \leq t_i < 1$. Sea R_K el conjunto de elementos de R_∞ de la forma $\sum_{i=1}^n s_i\theta_i$ con $0 \leq s_i \leq 1$. Es claramente un compacto de R_∞. Luego, tomamos el compacto de $\mathbb{A}_K^{S_\infty}$ definido por

$$D = R_K \times \prod_{v<\infty} \mathcal{O}_v.$$

Como $R_K + \mathcal{O}_K = R_\infty$, se ve que $D + \mathcal{O}_K = \mathbb{A}_K^{S_\infty}$. □

3.3. Idèles

Los idèles tienen muchos usos importantes; por un lado, que permiten trabajar fácilmente con extensiones infinitas. Por otra parte, clarifican mucho la relación entre la teoría local de cuerpos de clases y la global. Esto lo veremos con más claridad en los capítulos siguientes.

Los idèles son los elementos del grupo $\mathbb{I}_K = \mathbb{A}_K^\times$. Un adèle (α_v) es inversible si y sólo si cada componente lo es; es decir, $\mathbb{I}_K$ es el producto directo restringido de los $K_v^\times$ (respecto de los conjuntos $\mathcal{U}_v = \mathcal{O}_v^\times$ para los primos finitos). Hay que tener cuidado, ya que las dos topologías que tenemos en $\mathbb{I}_K$, la del producto directo restringido y la inducida como subespacio de $\mathbb{A}_K$, no coinciden. Consideraremos a $\mathbb{I}_K$ con la topología dada por el producto directo restringido. Nuevamente, si $S \supset S_\infty$ es un conjunto finito, llamamos *conjunto de S-idèles* a $\mathbb{I}_K^S$.

Como antes, podemos inyectar $K^\times \to \mathbb{I}_K$, y sigue valiendo que $K^\times$ es discreto. Sin embargo, no es cierto que $\mathbb{I}_K/K^\times$ sea compacto; aún así, es el producto de un grupo compacto con $\mathbb{R}_+$, y es un grupo de suma importancia; lo llamaremos *grupo de clases de idèles de* K, y lo denotaremos por $\mathbf{C}_K$.

Existe una aplicación natural $\mathrm{id} : \mathbb{I}_K \to I_K$ dada por $(\alpha_v) \mapsto \prod_{v<\infty} v^{\mathrm{ord}_v(\alpha_v)}$; la definición es válida ya que para casi todo v, $\mathrm{ord}_v(\alpha_v) = 0$. Su núcleo es exactamente $\mathbb{I}_K^{S_\infty}$.

Definimos el *contenido* o *volumen* $|.| : \mathbb{I}_K \to \mathbb{R}_+$ por $|(\alpha_v)| = \prod_v |\alpha_v|_v$ (es un producto finito), donde $|.|_v$ es un valor absoluto normalizado correspondiente a v. Es un epimorfismo de grupos, cuyo núcleo se denota por $\mathbb{I}_K^1$, llamado grupo de *idèles de contenido 1*. Tenemos, por lo tanto, una sucesión exacta corta de grupos

$$1 \to \mathbb{I}_K^1 \to \mathbb{I}_K \to \mathbb{R}_+ \to 1.$$

Por la fórmula del producto, $K^\times \subset \mathbb{I}_K^1$.

Teorema 3.3.1. *El grupo* $\mathbf{C}_K^1 = \mathbb{I}_K^1/K^\times$ *es compacto.*

Una vez probado este teorema, podremos describir $\mathbf{C}_K$ como el producto de un grupo compacto y $\mathbb{R}_+$. En efecto, podemos tomar la aplicación $j : \mathbb{R}_+ \to \mathbb{I}_K$ dada por

$$j(t) = (t^{1/n}, ..., t^{1/n}, 1, 1, ...),$$

donde las primeras son las coordenadas de los primos infinitos, y los unos corresponden a los primos finitos. Si $t \in \mathbb{R}_+$, tenemos que $|j(t)| = |t^{r_1/n+2r_2/n}| = t$ (recordar que el valor absoluto normalizado de un primo complejo es el cuadrado del valor absoluto usual). Luego, la sucesión exacta corta se parte y tenemos que

$$\mathbb{I}_K \simeq \mathbb{I}_K^1 \times \mathbb{R}_+.$$

Además, como $K^\times \subset \mathbb{I}_K^1$, obtenemos que

$$\mathbf{C}_K \simeq \mathbf{C}_K^1 \times \mathbb{R}_+.$$

Antes de probar el Teorema 3.3.1, necesitaremos repasar algunos hechos básicos sobre medidas de Haar.

Si G es un grupo localmente compacto, G posee una medida no nula μ tal que

(a) Todas las funciones continuas con soporte compacto a valores complejos son μ-integrables;

(b) μ es invariante bajo traslaciones a izquierda, es decir,

$$\int_G f(g)d\mu(g) = \int_G f(xg)d\mu(g) \quad \forall\, x \in G,$$

para toda f μ-integrable.

Esta medida es única salvo un múltiplo por una constante positiva. Tal medida se llama *medida de Haar a izquierda* en G. Si μ denota una medida de Haar a izquierda, para cualquier $A \subset G$ μ-medible, $x \in G$, vale que

$$\mu(A) = \mu(xA).$$

Todo conjunto boreliano de G es μ-medible. Más aún, si $A \subset G$ es un abierto no vacío, $\mu(A) > 0$, mientras que si A es compacto, $\mu(A) < \infty$.

Sea σ un isomorfismo algebraico y topológico de G. Si $A \subset G$ es μ-medible, σA también lo es. Podemos definir una medida μ' en G vía

$$\mu'(A) = \mu(\sigma A) \quad \forall\, A\ \mu\text{-medible}.$$

Es trivial ver que μ' es otra medida de Haar a izquierda de G, que, por lo tanto, difiere de μ en un factor constante positivo. A esta constante la llamamos *módulo del automorfismo* σ, y es denotada por $\mathrm{mod}_G(\sigma)$ (o $\mathrm{mod}(\sigma)$). Luego, el módulo está caracterizado por

$$\mu' = \mathrm{mod}(\sigma)\mu.$$

Es claro que el módulo es independiente de la elección original de la medida de Haar a izquierda. Si G es compacto entonces G es μ-medible y $\sigma G = G$ para todo automorfismo σ. Luego, $\mathrm{mod}(\sigma) = 1$ para todo σ. Si G es discreto entonces $\{e\}$ es μ-medible, y $\sigma(e) = e$ para todo σ; luego, $\mathrm{mod}(\sigma) = 1$.

Sea $H \subset G$ un subgrupo normal y cerrado, y sea σ un automorfismo de G tal que $\sigma(H) = H$. Entonces $\sigma_1 = \sigma|_H$ es un automorfismo de H. Además, σ_2, el morfismo inducido en G/H por σ, es un automorfismo de G/H.

Proposición 3.3.2. *Con las notaciones de arriba,* $\mathrm{mod}_G(\sigma) = \mathrm{mod}_H(\sigma_1)\,\mathrm{mod}_{G/H}(\sigma_2)$.

Dem. Se sigue inmediatamente del teorema de Fubini. □

Proposición 3.3.3. *Sea* v *un primo de* K, $x \in K_v^\times$ *y* σ_x *el automorfismo de* K_v *definido por* $y \mapsto xy$. *Entonces* $\mathrm{mod}_{K_v}(\sigma_x) = |x|_v$.

Dem. Lo probaremos en el caso v finito; cuando v es infinito es un resultado trivial. Sin pérdida de generalidad, podemos suponer que $|x|_v \leq 1$. En efecto, si lo probamos para este caso, y $|x|_v > 1$, como $|x^{-1}|_v \leq 1$, vemos que $(\mathrm{mod}(\sigma_x))^{-1} = \mathrm{mod}(\sigma_x^{-1}) = \mathrm{mod}(\sigma_{x^{-1}}) = |x^{-1}|_v = |x|_v^{-1}$.

Sea entonces $|x|_v \leq 1$. Entonces

$$\mu(x\mathcal{O}_v) = \mathrm{mod}(\sigma_x)\mu(\mathcal{O}_v), \quad (*)$$

donde μ es una medida de Haar de K_v. Ahora, $x\mathcal{O}_v = \mathfrak{p}_v^s$, donde $s = \mathrm{ord}_v(x)$. En el capítulo uno (Proposición 1.7.1), probamos que $\mathcal{O}_v/\mathfrak{p}_v^s$ es finito, de hecho, de cardinal q^s, donde q es el cardinal de $\mathcal{O}_v/\mathfrak{p}_v$, es decir, la norma del ideal primo de $\mathcal{O}_K$ correspondiente a v. Sea

$$\mathcal{O}_v = \cup_{i=1}^r (x_i + \mathfrak{p}_v^s)$$

una descomposición en coclases, donde $r = q^s$. Entonces

$$\mu(\mathcal{O}_v) = \sum_{i=1}^r \mu(x_i + \mathfrak{p}_v^s) = r\mu(\mathfrak{p}_v^s),$$

por la invariancia de la medida de Haar. Luego,

$$\mu(\mathfrak{p}_v^s) = r^{-1}\mu(\mathcal{O}_v) = q^{-\,\mathrm{ord}_v(x)}\mu(\mathcal{O}_v).$$

Esto, junto con que $|x|_v = q^{-\,\mathrm{ord}_v(x)}$ y con la ecuación $(*)$, prueban lo que queríamos. □

Sea $\alpha \in \mathbb{I}_K$. Entonces α define un automorfismo σ_α de $\mathbb{A}_K$ vía $\sigma_\alpha(\beta) = \alpha\beta$.

Proposición 3.3.4. *Para todo* $\alpha \in \mathbb{I}_K$, *vale que* $\mathrm{mod}(\sigma_\alpha) = |\alpha|$.

Dem. Sea $S = S_\infty \cup \{v < \infty : |\alpha_v|_v \neq 1\}$. Consideremos los S-adèles $\mathbb{A}_K^S$; como es un subgrupo abierto de $\mathbb{A}_K$, se tiene que $\mathbb{A}_K/\mathbb{A}_K^S$ es discreto, luego, por la Proposición 3.3.2 y una observación anterior, vemos que

$$\mathrm{mod}_{\mathbb{A}_K}(\sigma_\alpha) = \mathrm{mod}_{\mathbb{A}_K^S}(\sigma_\alpha) =$$

$$= \prod_{v \in S} \mathrm{mod}_{K_v}(\sigma_\alpha|_{K_v}).$$

Tenemos $\sigma_\alpha|_{K_v} = \sigma_{\alpha_v}$. Luego, $\mathrm{mod}_{K_v}(\sigma_\alpha|_{K_v}) = |\alpha_v|_v$ por la Proposición 3.3.3. Entonces

$$\mathrm{mod}_{\mathbb{A}_K}(\sigma_\alpha) = \prod_{v \in S} |\alpha_v|_v = \prod_v |\alpha_v|_v.$$

□

Probaremos a continuación una versión moderna del teorema de Minkowski sobre la existencia de puntos de retículos en regiones convexas del espacio euclídeo.

Teorema 3.3.5 (Minkowski-Chevalley-Weil)**.** *Existe un $\delta > 0$ tal que si $\eta \in \mathbb{I}_K$ y $|\eta| > \delta$ entonces existe $x \in K^\times$ con $|x_v|_v \leq |\eta_v|_v$ para todos los primos v.*

Dem. Para v infinito, sea $F_v = \{x \in K_v : |x|_v \leq 1\}$. Sea $M = \prod_{v \in S_\infty} F_v \times \prod_{v < \infty} \mathcal{O}_v \subset \mathbb{A}_K$. La afirmación del teorema es equivalente a que $|\eta| > \delta$ implica que existe $x \in K^\times$ tal que $x\eta^{-1} \in M$; esto último ocurre si y sólo si $\eta M \cap K \neq \{0\}$. Probaremos que si esta intersección es 0 entonces $|\eta| \leq \delta$ para una cierta constante δ que sólo depende de K. Sea μ' una medida de Haar en el grupo compacto $\mathbb{A}_K/K$ tal que $\mu'(\mathbb{A}_K/K) = 1$. Sea μ'' una medida de Haar en el grupo discreto K tal que cada fconjunto de un elemento tenga medida 1. Por el teorema de Fubini, existe una medida de Haar μ en $\mathbb{A}_K$ tal que

$$\int_{\mathbb{A}_K} f(x)d\mu(x) = \int_{\mathbb{A}_K/K} \left(\int_K f(\alpha + x)d\mu''(x) \right) d\mu'(\alpha) =$$

$$= \int_{\mathbb{A}_K/K} \left(\sum_{x \in K} f(\alpha + x) \right) d\mu'(\alpha).$$

Sea $\pi : \mathbb{A}_K \to \mathbb{A}_K/K$ la proyección canónica. Entonces π es inyectiva en ηM: si $\pi(\eta m) = 0$ entonces $\eta m \in K \cap \eta M = \{0\}$, y, por lo tanto, $m = 0$.

Sea f la función característica de ηM y $\overline{f}$ la función característica de $\pi(\eta M)$. Para $\alpha \in \mathbb{A}_K$, existe como mucho un $x \in K$ tal que $\alpha + x \in \eta M$. Luego,

$$\mu(\eta M) = \int_{\mathbb{A}_K} f(\alpha)d\mu(\alpha) = \int_{\mathbb{A}_K/K} \overline{f}(\alpha)d\mu'(\alpha) \leq$$

$$\leq \mu'(\mathbb{A}_K/K) = 1.$$

Hemos probado que si $\eta M \cap K = \{0\}$ entonces $\mu(\eta M) \leq 1$. Ahora bien, $\mu(\eta M) = |\eta|\mu(M)$, por la Proposición 3.3.4, de manera que $|\eta| \leq 1/\mu(M)$. Luego, si $|\eta| > 1/\mu(M)$ entonces $\eta M \cap K \neq \{0\}$. □

Demostración del Teorema 3.3.1. Sean $\delta > 0$ y M como en el Teorema 3.3.5 y sea $\eta \in \mathbb{I}_K$ tal que $|\eta| > \delta$. Observemos primero que $\eta^2 M.M$ es compacto, pues es la imagen continua de un compacto de $\mathbb{A}_K \times \mathbb{A}_K$. Como $K^\times$ es discreto en $\mathbb{I}_K$, $K^\times \cap \eta^2 M.M$ es discreto y compacto, y, por lo tanto, finito; supongamos que $K^\times \cap \eta^2 M.M = \{y_1, ..., y_g\}$. Sea $\alpha \in \mathbb{I}_K^1$. Entonces $|\alpha\eta| > \delta$. Por el Teorema 3.3.5, $\alpha\eta M \cap K \neq \{0\}$. Sea $x \neq 0$ en esta intersección. Entonces $x\alpha^{-1}\eta M \subset \eta^2 M.M$. Por la fórmula del producto, $|x\alpha^{-1}\eta| > \delta$, y de vuelta por el Teorema 3.3.5, existe $y \in K^\times \cap x\alpha^{-1}\eta M$. Entonces y es alguno de los y_i, digamos $y = y_1$. Se tiene entonces que $\alpha x^{-1} \in y_1^{-1}\eta M$. Sea $C = \cup_{i=1}^g y_i^{-1}\eta M$. Hemos probado que si $\alpha \in \mathbb{I}_K^1$, existe $x \in K$ tal que $\alpha x^{-1} \in C$. Luego, $\mathbf{C}_K^1$ es la imagen continua de C bajo la proyección canónica. Como C es compacto, el teorema queda probado. □

Usaremos ahora el Teorema 3.3.1 para recuperar los teoremas que mencionamos al principio del capítulo.

Sea S un conjunto finito de primos de K que contenga a los primos infinitos. Recordemos que I_K^S es el subgrupo libre de I_K generado por los ideales primos que no están en S. Notamos con P_K al conjunto de ideales fraccionarios no nulos de K, y con $P_K^S = P_K \cap I_K^S$.

Definición 3.3.6. El orden del grupo I_K^S/P_K^S se llama el *S-número de clases de K*, y lo notamos con h_K^S. Si S consiste de los primos infinitos, el S-número de clases es llamado simplemente el número de clases de K, denotado por h_K.

Teorema 3.3.7. *El S-número de clases h_K^S es finito. Más aún, $h_K^S = h_K^T$ para todos $S, T \supset S_\infty$.*

Recordemos que tenemos definido $\mathrm{id} : \mathbb{I}_K \to I_K$. Podemos tomar más en general $\mathrm{id}_S : \mathbb{I}_K \to I_K^S$, definido por

$$\mathrm{id}_S(\alpha) = \prod_{v \notin S} v^{\mathrm{ord}_v(\alpha_v)}.$$

Es claro que id_S es un morfismo de grupos suryectivo, y su núcleo es $\mathbb{I}_K^S$. Cuando $S = S_\infty$, $\mathrm{id}_S = \mathrm{id}$.

Dem. del Teorema 3.3.7. En vista de la observación de arriba,

$$\mathbb{I}_K/\mathbb{I}_K^S \simeq I_K^S.$$

La preimagen de P_K^S bajo este isomorfismo es $(K^\times \mathbb{I}_K^S)/\mathbb{I}_K^S$. Por lo tanto,

$$I_K^S/P_K^S \simeq (\mathbb{I}_K/\mathbb{I}_K^S)/((K^\times \mathbb{I}_K^S)/\mathbb{I}_K^S) \simeq \mathbb{I}_K/(K^\times \mathbb{I}_K^S).$$

Como $\mathbb{I}_K^S$ es un abierto de $\mathbb{I}_K$, $K^\times \mathbb{I}_K^S$ es abierto, y, por lo tanto, $\mathbb{I}_K/(K^\times \mathbb{I}_K^S)$ es discreto. Probaremos a continuación que es compacto, y, por lo tanto, finito.

Es claro que $\mathbb{I}_K = \mathbb{I}_K^1 \mathbb{I}_K^S = \mathbb{I}_K^1 K^\times \mathbb{I}_K^S$, con lo cual, $\mathbb{I}_K/K^\times \mathbb{I}_K^S \simeq \mathbb{I}_K^1/(\mathbb{I}_K^1 \cap K^\times \mathbb{I}_K^S)$ por alguno de los teoremas de isomorfismo. Además, $\mathbb{I}_K^1 \cap K^\times \mathbb{I}_K^S = K^\times(\mathbb{I}_K^1 \cap \mathbb{I}_K^S)$, y se sigue entonces que

$$\mathbb{I}_K/K^\times \mathbb{I}_K^S \simeq \mathbb{I}_K^1/(K^\times(\mathbb{I}_K^1 \cap \mathbb{I}_K^S)).$$

Consideremos la aplicación natural

$$\mathbb{I}_K^1 \to \mathbb{I}_K^1/(K^\times(\mathbb{I}_K^S \cap \mathbb{I}_K^1)).$$

Como $K^\times$ está contenido en el núcleo, $\mathbb{I}_K^1/(K^\times(\mathbb{I}_K^S \cap \mathbb{I}_K^1))$ es la imagen continua de $\mathbb{I}_K^1/K^\times$; por el Teorema 3.3.1, esto es compacto, y, por lo tanto, $\mathbb{I}_K/K^\times \mathbb{I}_K^S$ también lo es.

Hemos probado entonces que h_K^S es finito. Probaremos ahora que es igual a h_K, que es el números de clases de K. En efecto, la aplicación $I_K(S)/P_K(S) \to I_K/P_K$ es inyectiva. Veamos que es suryectiva. Sea $\mathfrak{a}$ un ideal fraccionario, $\mathfrak{a} = \mathfrak{b}\mathfrak{c}^{-1}$, con $\mathfrak{b}, \mathfrak{c}$ ideales enteros. Si $c \in \mathfrak{c}$ es un elemento no nulo entonces $\mathfrak{c}|(c)$ y, por lo tanto, $\mathfrak{a}(c)$ es un ideal entero. Esto prueba en primer lugar que toda clase de ideales en $Cl(K)$ está representada por un ideal entero $\mathfrak{a}$.

Escribamos entonces $\mathfrak{a} = \prod_{\mathfrak{p}\in S} \mathfrak{p}^{n(\mathfrak{p})}\mathfrak{b}$, con $\mathfrak{b} \in I_K(S)$. Para cada $\mathfrak{p} \in S$, sea $\pi_\mathfrak{p} \in \mathfrak{p} \setminus \mathfrak{p}^2$ un uniformizador. Por el Teorema chino del resto, existe $a \in \mathcal{O}_K$ tal que

$$a \equiv \pi_\mathfrak{p}^{n(\mathfrak{p})} (\mathrm{mod}\, \mathfrak{p}^{n(\mathfrak{p})+1})$$

para cada $\mathfrak{p} \in S$. Estas congruencias implican que $\mathrm{ord}_\mathfrak{p}(a) = n(\mathfrak{p})$ para todo $\mathfrak{p} \in S$ y, por lo tanto, $(a) = \prod_{\mathfrak{p}\in S} \mathfrak{p}^{n(\mathfrak{p})}\mathfrak{b}'$, con $\mathfrak{b}' \in I_K(S)$. Finalmente, $a^{-1}\mathfrak{a} \in I_K(S)$ y representa la misma clase que $\mathfrak{a}$ en $Cl(K)$. La aplicación $I_K(S)/P_K(S) \to Cl(K)$ es entonces biyectiva. □

Observación 3.3.8. Según el último teorema, cada clase de ideales en $Cl(K)$ está representada por un ideal en $I_K(S)$. Afirmamos aún más: cada clase se puede representar por un ideal *entero* en $I_K(S)$. En efecto, sea $\mathfrak{a} \in I_K(S)$, $\mathfrak{a} = \mathfrak{b}\mathfrak{c}^{-1}$, con $\mathfrak{b}, \mathfrak{c}$ ideales enteros en $I_K(S)$. Sea $c \in \mathfrak{c}$ distinto de cero, tal que $\mathrm{ord}_\mathfrak{p}(c) = 0$ para todo $\mathfrak{p} \in S$ (existe por el Teorema chino del resto). Se tiene que $c\mathfrak{a}$ es entero, y esto prueba nuestra afirmación.

Ahora estudiaremos la estructura de los grupos de unidades. Sea S un conjunto finito de primos que contenga a los infinitos.

Definición 3.3.9. Una *S-unidad* es un elemento $x \in K$ tal que $\mathrm{ord}_v(x) = 0$ para todo $v \notin S$.

En el caso $S = S_\infty$, las S-unidades son simplemente las unidades de $\mathcal{O}_K$. Sea $\mathcal{U}_K(S)$ el grupo de S-unidades de K. Sea W_K el grupo de todas las unidades de $\mathcal{O}_K$ de orden finito; esto no es otra cosa que el grupo de todas las raíces de la unidad en K, y es claro que $W_K \subset \mathcal{U}_K(S)$ para todo S. Sea $V_K(S) = \mathcal{U}_K(S)/W_K$.

Teorema 3.3.10 (Dirichlet-Minkowski-Hasse-Chevalley)**.** *Supongamos que S tiene s elementos. Entonces:*

(I) *W_K es un grupo finito*;

(II) *$V_K(S)$ es un grupo abeliano libre de rango $s-1$*;

(III) $\mathcal{U}_K(S) \simeq W_K \times V_K(S)$.

Dem. Por las observaciones recién hechas, W_K es exactamente el subgrupo de $\mathcal{U}_K(S)$ de elementos de orden finito. Si (I) y (II) son ciertos entonces $\mathcal{U}_K(S)$ es un grupo abeliano finitamente generado; (III) se sigue entonces del teorema de estructura para estos grupos. Probemos entonces (I) y (II).

Definimos dos subgrupos de $\mathbb{I}_K^1$ de la siguiente manera:

$$G = \mathbb{I}_K^S \cap \mathbb{I}_K^1,$$

$$G_0 = \prod_v \mathcal{U}_v,$$

donde v recorre todos los primos de K (esto tiene sentido incluso para los primos infinitos, definiendo las unidades como los elementos de valor absoluto 1). Entonces

$$G \cap K^\times = \mathcal{U}_K(S),$$

$$G_0 \cap K^\times = W_K.$$

Es claro que G es abierto en $\mathbb{I}_K^1$ y G_0 es compacto. Como $K^\times$ es discreto, $G_0 \cap K^\times$ es compacto y discreto; por lo tanto, es finito, y entonces se sigue (I).

Además, $V_K(S) \simeq (G \cap K^\times)/(G_0 \cap K^\times)$. Observemos que $G \cap K^\times$ es discreto, y, por lo tanto, $(G \cap K^\times)/(G_0 \cap K^\times)$ lo es. Como G es un subgrupo abierto de $\mathbb{I}_K^1$, también es cerrado y, por lo tanto, $GK^\times/K^\times$, la imagen de G bajo la aplicación natural $\mathbb{I}_K^1 \to \mathbb{I}_K^1/K^\times$, es un cerrado; por el Teorema 3.3.1, es un compacto. Entonces también es compacto $GK^\times/G_0K^\times$, al ser la imagen continua de $GK^\times/K^\times$. Luego, como

$$GK^\times/G_0K^\times = GG_0K^\times/G_0K^\times = G/(G \cap G_0K^\times) =$$

$$= G/G_0(G \cap K^\times) = (G/G_0)/(G_0(G \cap K^\times)/G_0),$$

vemos que este último grupo es compacto.

Resumiendo, hemos probado que $G_0(G \cap K^\times)/G_0$ es un grupo discreto, y el cociente de G/G_0 por él es compacto.

Saquemos un primo fijo v de S, digamos un primo infinito, y sea S_1 el conjunto obtenido de S al sacarlo. Construimos la siguiente aplicación:

$$\log : G \to \mathbb{R}^{s-1},$$

$$(x_v) \mapsto (\log |x_v|_v)_{v \in S_1}.$$

Notemos que no importa en verdad qué primo sacamos, ya que si $(x_v) \in \mathbb{I}_K^1$ entonces la suma de los logaritmos de los valores absolutos da 0 y podemos obtener el restante en función de los demás.

La imagen $\log(G)$ de G bajo esta aplicación es $\mathbb{R}$ en cada primo infinito y un grupo cíclico infinito en los primos finitos de S_1. Luego, $\mathbb{R}^{s-1}/\log(G)$ es compacto, y el núcleo de la aplicación no es otra cosa que G_0. De esta manera, G/G_0 puede verse como un subgrupo de $\mathbb{R}^{s-1}$ con cociente compacto. Como probamos más arriba, $G_0(G \cap K^\times)/G_0$ es un subgrupo de G/G_0 con cociente compacto. Luego, $V_K(S) \simeq G_0(G \cap K^\times)/G_0$ se puede ver como un subgrupo discreto de $\mathbb{R}^{s-1}$ con cociente compacto: si $A \supset B \supset C$ es una sucesión de grupos topológicos, B un cerrado de A, C un cerrado de B, A/B compacto, B/C compacto, entonces A/C es compacto. La demostración entonces termina con el siguiente lema. □

Lema 3.3.11. *Sea Γ un subgrupo discreto de $\mathbb{R}^m$ con cociente compacto. Entonces Γ es un grupo abeliano libre de rango m.*

Dem. Sea E el $\mathbb{R}$-espacio vectorial generado por Γ. Tenemos una sucesión exacta de aplicaciones continuas:

$$\mathbb{R}^m/\Gamma \to \mathbb{R}^m/E \to 0,$$

con lo cual, $\mathbb{R}^m/E$ es un compacto. Esto implica que $E = \mathbb{R}^m$. Sea $\{x_1, ..., x_m\} \subset \Gamma$ una base de $\mathbb{R}^m$. Sea Γ_1 el grupo abeliano libre generado por los x_i. Es claro que $\Gamma_1 \subset \Gamma$. Además, Γ/Γ_1 es un cerrado de $\mathbb{R}^m/\Gamma_1$, con lo cual, es compacto. Como Γ_1 es abierto en Γ (pues Γ es discreto), el cociente es discreto. Por lo tanto, Γ/Γ_1 es finito. Como Γ/Γ_1 y Γ_1 son finitamente

generados, también lo es Γ. Por el teorema de estructura, Γ es un grupo abeliano libre de rango r, y debe ser $r \geq m$. Suponiendo que $r > m$, sea $\{e_1, ..., e_r\}$ una $\mathbb{Z}$-base de Γ. Entonces

$$e_1 = \sum_{i=2}^{r} a_i e_i$$

para ciertos $a_i \in \mathbb{R}$ no todos nulos.

Dado $\epsilon > 0$, existe un entero N no nulo tal que $Na_2, ..., Na_n$ distan de un entero en menos de ϵ. Entonces Ne_1 es la suma de una combinación $\mathbb{Z}$-lineal de $e_2, ..., e_r$ y una combinación $\mathbb{R}$-lineal de $e_2, ..., e_n$ con coeficientes de módulo más chico que ϵ. Haciendo ϵ suficientemente chico, como Γ es discreto, la última combinación lineal debería ser 0. Entonces

$$Ne_1 = \sum_{i=2}^{r} M_i e_i,$$

donde los $M_i \in \mathbb{Z}$. Esto contradice la $\mathbb{Z}$-independencia lineal de los e_i. Finalmente queda probado que Γ es libre de rango m.

□

Finalmente incluimos el siguiente resultado que usaremos más adelante.

Lema 3.3.12. (a) *Sea S un conjunto finito de primos de K y sea $\mathbb{I}_{K,S} = \{x \in \mathbb{I}_K : x_v = 1 \ \forall v \in S\}$. Entonces $K^\times \mathbb{I}_{K,S}$ es denso en $\mathbb{I}_K$.*

(b) *Existe $S \supset S_\infty$ tal que $\mathbb{I}_K = K^\times \mathbb{I}_K^S$.*

Dem. (a): Sea $x \in \mathbb{I}_K$. Consideremos un entorno arbitrario $xU(T, \epsilon)$ de x, donde $U(T, \epsilon) = \prod_{v \in T} N_v(\epsilon) \times \prod_{v \notin T} \mathcal{U}_v$, siendo $T \supset S_\infty$ finito y $N_v(\epsilon) = \{a \in K_v^\times : |a - 1|_v < \epsilon\}$. Si agrandamos T agregándole finitos primos (tantos como queramos), achicamos el entorno. Luego, podemos suponer que T contiene a S. Sea $M = \min\{|x_v|_v : v \in T\}$, y sea $0 < \delta < M\epsilon$. Por el teorema de aproximación débil (Teorema 3.2.1), existe $\alpha \in K^\times$ tal que $|x_v - \alpha|_v < \delta$ para todo $v \in T$. Tomemos x' el idèle definido por: $x'_v = 1$ para $v \in T$, $x'_v = x_v/\alpha$ para $v \notin T$. Entonces $x' \in \mathbb{I}_{K,T} \subset \mathbb{I}_{K,S}$. Luego, $\alpha x' \in K^\times \mathbb{I}_{K,S}$. Afirmamos que $\alpha x' \in xU(T, \epsilon)$, esto es, que $\alpha x' x^{-1} \in U(T, \epsilon)$. En efecto, $(\alpha x' x^{-1})_v = 1$ si $v \notin T$ y α/x_v si $v \in T$. Entonces resta ver que $|\alpha/x_v - 1|_v < \epsilon$ para $v \in T$. Esto se sigue de que $|\alpha/x_v - 1|_v = |\alpha - x_v|_v/|x_v|_v < \delta/M < \epsilon$.

(b): Tomemos $S \supset S_\infty$ tal que contenga a un conjunto de primos cuyas clases generen el grupo de clases de ideales $Cl(K)$. Esto significa que todo ideal fraccionario $\mathfrak{a}$ se puede escribir como

$$\mathfrak{a} = \mathfrak{b}(x),$$

con $\mathfrak{b}$ en el subgrupo $\langle S \rangle$ de $\mathbb{I}_K$ generado por los primos de S y $x \in K^\times$. Sea $i : K^\times \to I_K/\langle S \rangle$ la aplicación natural. Entonces tenemos que $(I_K/\langle S \rangle)/i(K^\times) = 0$. Por otra parte, si consideramos el epimorfismo $\mathrm{id} : \mathbb{I}_K \to I_K/\langle S \rangle$ (cuyo núcleo es $\mathbb{I}_K^S$), tenemos que $K^\times \mathbb{I}_K^S = \mathrm{id}^{-1}(i(K^\times))$, y, por lo tanto, $\mathbb{I}_K/K^\times \mathbb{I}_K^S = 0$. □

Capítulo 4

Teoría global de cuerpos de clases

4.1. Notaciones y definiciones

En este capítulo K será un cuerpo de números. Un *módulo* $\mathfrak{m}$ de K es un producto formal (finito) de primos, finitos o infinitos,

$$\mathfrak{m} = \prod_v v^{\mathfrak{m}(v)},$$

donde $\mathfrak{m}(v) \in \mathbb{N}_0$, $\mathfrak{m}(v) = 0$ ó 1 si v es real, y $\mathfrak{m}(v) = 0$ si v es complejo. De esta manera, todo módulo se puede escribir como

$$\mathfrak{m} = \mathfrak{m}_0 \mathfrak{m}_\infty,$$

donde $\mathfrak{m}_0$ es un ideal de $\mathcal{O}_K$ y $\mathfrak{m}_\infty$ es un producto de primos reales distintos. Si todos los exponentes son 0, escribimos $\mathfrak{m} = 1$. Decimos que un primo *divide* a $\mathfrak{m}$ si aparece en $\mathfrak{m}$ con exponente positivo.

Dado $\alpha \in K^\times$ y v un primo real, notamos con α_v la imagen de α en K_v, y decimos que $\alpha_v > 0$ si $\sigma(\alpha) > 0$, donde σ es una inmersión correspondiente a v. Decimos que $\alpha \equiv^* 1 (\mathrm{mod}\, \mathfrak{m})$ si $\mathrm{ord}_v(\alpha - 1) \geq \mathfrak{m}(v)$ para los primos finitos que dividen a $\mathfrak{m}$, y $\alpha_v > 0$ en los primos reales que dividen a $\mathfrak{m}$.

Dado S un conjunto finito de primos (finitos o infinitos) de K, sea I_K^S el subgrupo libre de I_K generado por los ideales primos que no están en S (esto generaliza la definición del capítulo I, donde S sólo consistía de primos finitos).

Definimos $I_K(\mathfrak{m})$ como $I_K^{S(\mathfrak{m})}$, donde $S(\mathfrak{m})$ consiste de todos los primos (finitos e infinitos) que dividen a $\mathfrak{m}$. Es decir, $I_K(\mathfrak{m})$ es el subgrupo libre de I_K generado por los ideales primos que no dividen a $\mathfrak{m}$. Sea $P_K(\mathfrak{m}) = \{(\alpha) : \alpha \in K^\times, \mathrm{ord}_v(\alpha) = 0 \; \forall v \text{ finito}, v|\mathfrak{m}\}$. Definimos también $K_{\mathfrak{m},1} = \{\alpha \in K^\times : \alpha \equiv^* 1 (\mathrm{mod}\, \mathfrak{m})\}$. Si $\mathrm{id} : K^\times \to I_K$ denota la aplicación usual $\alpha \mapsto (\alpha)$ entonces llamamos $P_{K,1}(\mathfrak{m}) = \mathrm{id}(K_{\mathfrak{m},1})$; es claro que $P_{K,1}(\mathfrak{m}) \subset P_K(\mathfrak{m})$. El *grupo de clases radial módulo* $\mathfrak{m}$ se define como $C_\mathfrak{m} = I_K(\mathfrak{m})/P_{K,1}(\mathfrak{m})$, y un *subgrupo de congruencia modulo* $\mathfrak{m}$ es por definición un subgrupo $H \leq I_K(\mathfrak{m})$ tal que $P_{K,1}(\mathfrak{m}) \subset H$. Los subgrupos de congruencia están en correspondencia con los subgrupos de $C_\mathfrak{m}$ vía $H \leftrightarrow \widetilde{H} = p(H)$, donde $p : I_K(\mathfrak{m}) \to C_\mathfrak{m}$ es la proyección canónica.

Ejemplo 4.1.1. Tomemos el módulo $\mathfrak{m} = (m)\infty$ de $\mathbb{Q}$, donde $m \in \mathbb{Z}$ y ∞ representa el único primo infinito de $\mathbb{Q}$. Escribamos $m = p_1^{e_1} \dots p_k^{e_k}$. Entonces $\mathbb{Q}_{\mathfrak{m},1}$ consiste de los números racionales a/b, con $a, b \in \mathbb{Z}$, $(a, m) = (b, m) = 1$, $(a/b) > 0$, tales que $ab^{-1} = 1$ en $(\mathbb{Z}/p_i^{e_i}\mathbb{Z})^\times$ para todo i, esto es, tales que $a \equiv b (\mathrm{mod}\, m)$.

4.2. El mapa de Artin

Sea L/K una extensión finita y abeliana de cuerpos de números y S el conjunto de primos (finitos o infinitos) de K que ramifican en L. Recordemos que tenemos definido el mapa de Artin:

$$\psi_{L/K} : I_K^S \to \mathrm{Gal}(L/K),$$
$$\prod_{\mathfrak{p} \notin S} \mathfrak{p}^{e_\mathfrak{p}} \mapsto \prod_{\mathfrak{p} \notin S} \left(\frac{L/K}{\mathfrak{p}}\right)^{e_\mathfrak{p}}.$$

De esta manera, si $\mathfrak{m}$ es un módulo tal que todos los primos ramificados dividen a $\mathfrak{m}$, tenemos que $I_K(\mathfrak{m}) \subset I_K^S$ y podemos considerar $\psi_{L/K} : I_K(\mathfrak{m}) \to \mathrm{Gal}(L/K)$.

Teorema 4.2.1 (Reciprocidad)**.** *Existe un módulo $\mathfrak{m}$ tal que $S(\mathfrak{m}) = S$, $\psi_{L/K}$ es suryectiva y el núcleo $\ker(\psi_{L/K})$ es un subgrupo de congruencia para $\mathfrak{m}$, es decir, $\psi_{L/K}(P_{K,1}(\mathfrak{m})) = 1$ (más aún, el núcleo es exactamente $\mathrm{N}_{L/K}(I_L^{S'})P_{K,1}(\mathfrak{m})$, donde S' es el conjunto de primos que están sobre primos de S). Así, esto induce un isomorfismo*

$$I_K(\mathfrak{m})/\,\mathrm{N}_{L/K}(I_L^{S'})P_{K,1}(\mathfrak{m}) \to \mathrm{Gal}(L/K).$$

En el siguiente teorema, "única" quiere decir única contenida en una clausura algebraica fija de K.

Teorema 4.2.2 (Existencia)**.** *Dado $\mathfrak{m}$ un módulo de K y H un subgrupo de congruencia módulo $\mathfrak{m}$, existe una única extensión L/K finita abeliana, tal que los primos que ramifican dividen a $\mathfrak{m}$, y tal que $H = \ker(\psi_{L/K} : I_K(\mathfrak{m}) \to \mathrm{Gal}(L/K))$. De esta manera, $\mathrm{Gal}(L/K)$ es isomorfo a $C_\mathfrak{m}/\widetilde{H}$, donde $\widetilde{H}$ es la imagen de H en $C_\mathfrak{m}$.*

La extensión L/K dada por el teorema de existencia se llama *cuerpo de clases* de H. En particular, tomando $H = P_{K,1}(\mathfrak{m})$, tenemos para cada módulo $\mathfrak{m}$ una extensión finita abeliana $K_\mathfrak{m}$, que llamaremos *cuerpo de clases radial módulo* $\mathfrak{m}$. El grupo $\mathrm{Gal}(K_\mathfrak{m}/K)$ es isomorfo a $C_\mathfrak{m}$, vía el mapa de Artin. La extensión $K_\mathfrak{m}$, donde $\mathfrak{m} = 1$, se llama *cuerpo de clases de Hilbert* de K.

4.3. Reinterpretación de Chevalley en términos de idèles

En esta sección interpretaremos las nociones anteriores con idèles. Sea $\mathfrak{m}$ un módulo de K. Definimos

$$\mathbb{I}_\mathfrak{m} = \left(\prod_{v \nmid \mathfrak{m}} K_v^\times \times \prod_{v|\mathfrak{m}, v<\infty} 1 + \widehat{\mathfrak{p}_v}^{\mathfrak{m}(v)} \times \prod_{v|\mathfrak{m}, v \in S_\infty} \mathbb{R}_+ \right) \bigcap \mathbb{I}_K$$

y

$$W_{\mathfrak{m}} = \prod_{v\nmid\mathfrak{m},v<\infty} \mathcal{U}_v \times \prod_{v\nmid\mathfrak{m},v\in S_\infty} K_v^\times \times \prod_{v|\mathfrak{m},v<\infty} 1+\widehat{\mathfrak{p}_v}^{\mathfrak{m}(v)} \times \prod_{v|\mathfrak{m},v\in S_\infty} \mathbb{R}_+ \subset \mathbb{I}_K.$$

Observemos que viendo a $K^\times \subset \mathbb{I}_K$, se tiene que $\mathbb{I}_{\mathfrak{m}} \cap K^\times = K_{\mathfrak{m},1}$.

Proposición 4.3.1. (1) *La aplicación* $\mathrm{id} : \mathbb{I}_{\mathfrak{m}} \to I_K(\mathfrak{m})$ *induce un isomorfismo de grupos*

$$\mathbb{I}_{\mathfrak{m}}/K_{\mathfrak{m},1}W_{\mathfrak{m}} \xrightarrow{\eta_{\mathfrak{m}}} C_{\mathfrak{m}}.$$

(2) *La inlcusión* $\mathbb{I}_{\mathfrak{m}} \hookrightarrow \mathbb{I}_K$ *induce un isomorfismo*

$$\mathbb{I}_{\mathfrak{m}}/K_{\mathfrak{m},1} \xrightarrow{\theta_{\mathfrak{m}}} \mathbf{C}_K\,.$$

Dem. (1) Es inmediato que id manda $K_{\mathfrak{m},1}W_{\mathfrak{m}}$ en $P_{K,1}(\mathfrak{m})$ y el morfismo inducido en los cocientes es biyectivo.

(2) El núcleo de $\mathbb{I}_{\mathfrak{m}} \to \mathbb{I}_K/K^\times$ es $K^\times \cap \mathbb{I}_{\mathfrak{m}}$ (intersección dentro de $\mathbb{I}_K$), y esto es $K_{\mathfrak{m},1}$. Luego, tenemos definida una inyección

$$\mathbb{I}_{\mathfrak{m}}/K_{\mathfrak{m},1} \hookrightarrow \mathbb{I}_K/K^\times.$$

Queremos ver que es suryectiva. Sea $x \in \mathbb{I}_K$, y sea $M = \mín\{|x_v|_v : v|\mathfrak{m}\}$. Sea $\epsilon > 0$ suficientemente chico, de tal manera que si $a \in \mathbb{I}_K$ es tal que $|a_v - 1|_v < \epsilon/M$ para todo $v|\mathfrak{m}$ entonces $a \in \mathbb{I}_{\mathfrak{m}}$. Por el teorema de aproximación, existe $\alpha \in K^\times$ tal que $|x_v - \alpha|_v < \epsilon$ para todo $v|\mathfrak{m}$. Entonces $|(\alpha/x_v) - 1|_v < \epsilon/|x_v|_v \leq \epsilon/M$, con lo cual, $y = \alpha/x$ es un elemento de $\mathbb{I}_{\mathfrak{m}}$; también lo es, por lo tanto, $1/y$ y se sigue la suryectividad.

□

Esto permite ver a todos los grupos radiales $C_{\mathfrak{m}}$ como cocientes del grupo de clases de idèles $\mathbf{C}_K$.

Proposición 4.3.2. *Sea* N *un subgrupo de* $\mathbb{I}_K$. *Entonces* N *es abierto si y sólo si* $W_{\mathfrak{m}} \subset N$ *para algún módulo* $\mathfrak{m}$.

Dem. Como $W_{\mathfrak{m}}$ es un subgrupo que es un entorno de 1, es claro que si $W_{\mathfrak{m}} \subset N$ entonces N es abierto. Recíprocamente, sea N abierto. Entonces como $1 \in N$, N contiene un entorno de 1 de la forma $\prod_{v\in S} N_v \times \prod_{v\notin S} \mathcal{U}_v$, donde $S \supset S_\infty$ es un conjunto finito y N_v es un entorno de 1 en K_v. Si $v \in S$ es un primo finito, entonces $N_v \supset 1 + \widehat{\mathfrak{p}_v}^{\mathfrak{m}(v)}$ para ciertos $\mathfrak{m}(v) \in \mathbb{N}$. Tomemos $\mathfrak{m}$ como el producto de todos los $v \in S$ finitos, elevados a las potencias $\mathfrak{m}(v)$, y todos los v reales. Entonces

$$W_{\mathfrak{m}} = \prod_{v\in S,v<\infty} (1+\widehat{\mathfrak{p}_v}^{\mathfrak{m}(v)}) \times \prod_{v\notin S} \mathcal{U}_v \times \prod_{v \text{ reales}} \mathbb{R}_+ \times \prod_{v \text{ complejos}} K_v^\times = H_1H_2,$$

donde

$$H_1 = \prod_{v\in S, v<\infty} (1+\widehat{\mathfrak{p}_v}^{\mathfrak{m}(v)}) \times \prod_{v\notin S} \mathcal{U}_v \times 1$$

y

$$H_2 = 1 \times \prod_{v \text{ reales}} \mathbb{R}_+ \times \prod_{v \text{ complejos}} K_v^\times.$$

Entonces tenemos que $H_1 \subset N$. La demostración estará terminada si podemos ver que $H_2 \subset N$. Es fácil probar que la topología de H_2 es la misma que la topología producto, con lo cual, H_2 es un subgrupo conexo de $\mathbb{I}_K$ que contiene a 1. Luego, está contenido en la componente conexa D_K de la identidad de $\mathbb{I}_K$. Como N es abierto y cerrado en $\mathbb{I}_K$ (al ser un subgrupo abierto), se tiene que $D_K \cap N$ es un subgrupo abierto y cerrado de D_K, con lo cual, $D_K = D_K \cap N$, es decir, $D_K \subset N$. Finalmente, $H_2 \subset N$. □

Proposición 4.3.3. *Sea N un subgrupo abierto de $\mathbf{C}_K$. Entonces el índice $(\mathbf{C}_K : N)$ es finito.*

Dem. Es claro que basta probar que $(\mathbb{I}_K : N)$ es finito para $K^\times \subset N \subset \mathbb{I}_K$ abierto. Por la proposición anterior, existe un módulo $\mathfrak{m}$ tal que $W_\mathfrak{m} \subset N$. Luego, $K^\times W_\mathfrak{m} \subset N$ y, por lo tanto, se tiene una aplicación suryectiva

$$\mathbb{I}_K/K^\times W_\mathfrak{m} \to \mathbb{I}_K/N.$$

Veremos que el grupo de la izquierda es finito. Es claro que la aplicación natural

$$\mathbb{I}_\mathfrak{m} \to \mathbb{I}_K/K^\times W_\mathfrak{m}$$

induce un isomorfismo entre $\mathbb{I}_\mathfrak{m}/K_{\mathfrak{m},1}W_\mathfrak{m} \simeq \mathbb{I}_K/K^\times W_\mathfrak{m}$. El primero de estos grupos es isomorfo a lo que llamamos $C_\mathfrak{m} = I_K(\mathfrak{m})/P_{K,1}(\mathfrak{m})$; probaremos entonces que es finito. Basta ver que $I_K(\mathfrak{m})/P_K(\mathfrak{m})$ y $P_K(\mathfrak{m})/P_{K,1}(\mathfrak{m})$ lo son. El primero de estos grupos es finito por el Teorema 3.3.7.

Veamos ahora que $P_K(\mathfrak{m})/P_{K,1}(\mathfrak{m})$ también es finito. Sea $K_{\mathfrak{m},0} = \{\alpha \in K^\times : \mathrm{ord}_\mathfrak{p}(\alpha) = 0\ \forall \mathfrak{p}|\mathfrak{m}_0\}$. Se tiene una aplicación suryectiva

$$K_{\mathfrak{m},0}/K_{\mathfrak{m},1} \to P_K(\mathfrak{m})/P_{K,1}(\mathfrak{m}).$$

Probaremos que el grupo de la izquierda se mete inyectivamente en

$$\prod_{v|\mathfrak{m} \text{ real}} \{\pm 1\} \times (\mathcal{O}_K/\mathfrak{m}_0)^\times,$$

y como este grupo es finito, esto terminará la demostración.

Sea $\alpha \in K_{\mathfrak{m},0}$. Escribamos $(\alpha) = \mathfrak{a}\mathfrak{b}^{-1}$, con $\mathfrak{a}, \mathfrak{b}$ ideales enteros de $I_K(\mathfrak{m})$. Entonces $\mathfrak{a}$ y $\mathfrak{b}$ representan la misma clase $\mathcal{C}$ en $Cl(K)$. Como vimos en la observación 3.3.8, podemos tomar $\mathfrak{d}$ un ideal entero de $I_K(\mathfrak{m})$ que represente la clase $\mathcal{C}^{-1}$. Luego, $(\alpha) = \mathfrak{a}\mathfrak{d}(\mathfrak{b}\mathfrak{d})^{-1} = (a)(b)^{-1}$ para ciertos $a, b \in \mathcal{O}_K \cap K_{\mathfrak{m},0}$. Para cada $\mathfrak{p}|\mathfrak{m}_0$, mandamos α a $[a][b]^{-1} \in (\mathcal{O}_K/\mathfrak{p}^{\mathfrak{m}(\mathfrak{p})})^\times$, que tiene sentido pues a y b son coprimos con $\mathfrak{p}$; esta aplicación no depende de la elección de a y b

con esas propiedades. Si v es un primo real que divide a $\mathfrak{m}$, mandamos α a 1 si $\alpha_v > 0$ y a -1 en caso contrario. Obtenemos entonces una aplicación

$$K_{\mathfrak{m},0} \to \prod_{v|\mathfrak{m} \text{ real}} \{\pm 1\} \times \prod_{\mathfrak{p}|\mathfrak{m}_0} (\mathcal{O}_K/\mathfrak{p}^{\mathfrak{m}(\mathfrak{p})})^\times.$$

El núcleo es exactamente $K_{\mathfrak{m},1}$, y esto termina la demostración, pues

$$\prod_{\mathfrak{p}|\mathfrak{m}_0} (\mathcal{O}_K/\mathfrak{p}^{\mathfrak{m}(\mathfrak{p})})^\times \simeq (\mathcal{O}_K/\mathfrak{m}_0)^\times$$

por el Teorema chino del resto. Aunque no lo necesitemos, observemos que en realidad tenemos un isomorfismo (usar el teorema de aproximación). □

Sean S un conjunto finito de primos de K y G un grupo abeliano finito. Decimos que un módulo $\mathfrak{m}$ es *admisible* para un morfismo $\psi : I_K^S \to G$ si $S \subset S(\mathfrak{m})$ y $\psi(P_{K,1}(\mathfrak{m})) = 1$. También decimos que ψ admite un módulo.

Es muy fácil ver que si $S \subset S'$ y $\psi : I_K^S \to G$ admite un módulo entonces su restricción a $I_K^{S'}$ también admite un módulo.

Sea $\mathbb{I}_{K,S}$ el conjunto de idèles cuyas componentes en los primos de S son 1.

Proposición 4.3.4. *Sea $\psi : I_K^S \to G$ y $\mathfrak{m}$ un módulo admisible para ψ (donde S es un conjunto finito de primos de K y G es un grupo abeliano finito). Entonces existe un único morfismo $\phi : \mathbb{I}_K \to G$ tal que*

(I) *ϕ es continuo (al considerar en G la topología discreta);*

(II) *$\phi(K^\times) = 1$;*

(III) *$\phi(x) = \psi(\mathrm{id}(x))$ para todo $x \in \mathbb{I}_{K,S(\mathfrak{m})}$.*

Recíprocamente, si $\phi : \mathbb{I}_K \to G$ es un morfismo continuo tal que $\phi(K^\times) = 1$ entonces proviene de un $\psi : I_K^S \to G$ que admite un módulo (para cierto S).

Dem. Sea $\mathfrak{m}$ un módulo admisible para ψ. Consideremos

$$\mathbf{C}_K \to \mathbb{I}_\mathfrak{m}/K_{\mathfrak{m},1} \to \mathbb{I}_\mathfrak{m}/K_{\mathfrak{m},1}W_\mathfrak{m} \to C_\mathfrak{m}.$$

Las flechas de las puntas son isomorfismos (Proposición 4.3.1) mientras que la del medio es un epimorfismo. Como ψ se factoriza por $C_\mathfrak{m}$, podemos considerarlo como un morfismo $\psi : C_\mathfrak{m} \to G$. Vía la cadena de morfismos, encontramos un morfismo $\phi : \mathbb{I}_K \to G$ tal que $\phi(K^\times) = 1$. Es continuo pues al anularse en $W_\mathfrak{m}$, el núcleo es un abierto, y cumple que $\phi(x) = \psi(\mathrm{id}(x))$ para $x \in \mathbb{I}_\mathfrak{m}$, en particular, para $x \in \mathbb{I}_{K,S(\mathfrak{m})}$.

Para la unicidad, por el Lema 3.3.12, $K^\times \mathbb{I}_{K,S(\mathfrak{m})}$ es un denso de $\mathbb{I}_K$, y se sigue que ϕ está unívocamente determinada por las condiciones (I), (II) y (III).

Sea ahora $\phi : \mathbb{I}_K \to G$ continuo tal que $\phi(K^\times) = 1$. Entonces el núcleo de ϕ es un subgrupo abierto de $\mathbb{I}_K$. Por la Proposición 4.3.2, existe un módulo $\mathfrak{m}$ tal que $\phi(W_\mathfrak{m}) = 1$. Utilizando la cadena de morfismos de recién, tenemos primero un morfismo $\mathbf{C}_K \to G$, que convertimos

mediante el primer isomorfismo en un morfismo $\mathbb{I}_{\mathfrak{m}}/K_{\mathfrak{m},1} \to G$. Como $\phi(W_{\mathfrak{m}}) = 1$, obtenemos un morfismo $\mathbb{I}_{\mathfrak{m}}/K_{\mathfrak{m},1}W_{\mathfrak{m}} \to G$, que vía el isomorfismo con $C_{\mathfrak{m}}$, da lugar a un morfismo de $C_{\mathfrak{m}}$ en G. Componiendo con la proyección natural, conseguimos un morfismo $\psi : I_K(\mathfrak{m}) \to G$ que se factoriza por $C_{\mathfrak{m}}$, y este el ψ que buscábamos (con $S = S(\mathfrak{m})$). □

Definición 4.3.5. Dada L/K finita y abeliana, decimos que *la ley de reciprocidad se cumple para* L/K si existe $\phi_{L/K} : \mathbb{I}_K \to \mathrm{Gal}(L/K)$ continuo, tal que $\phi_{L/K}(K^\times) = 1$ y $\phi_{L/K}(x) = \psi_{L/K}(\mathrm{id}(x))$ si $x \in \mathbb{I}_{K,S}$, donde S consiste de los primos ramificados de L/K. En ese caso, también llamaremos mapa de Artin a $\phi_{L/K}$.

Se sigue entonces que el Teorema 4.2.1 implica la ley de reciprocidad. Por otra parte, en la Sección 4.6.1 probaremos que si valen los Teoremas 4.5.1-4.5.4 (que incluyen la ley de reciprocidad) entonces el Teorema 4.2.1 es cierto. Finalmente, en el último capítulo construiremos el mapa de Artin $\phi_{L/K}$ y probaremos todas las propiedades que debe tener.

4.4. Norma de idèles

Sea L/K una extensión finita de Galois con grupo de Galois $G = \mathrm{Gal}(L/K)$. Dado $x \in \mathbb{I}_L$, queremos definir un idèle $\mathrm{N}_{L/K}\, x \in \mathbb{I}_K$, la *norma de* x. Queremos que sea compatible con la norma usual $\mathrm{N}_{L/K}$ de $L^\times$ en $K^\times$. Para ello, debe suceder que si $x \in L^\times$, viendo a x como idèle principal de L, sea $(\mathrm{N}_{L/K}\, x)_v = \mathrm{N}_{L/K}\, x = \prod_{\sigma \in G} \sigma x$. Sabemos que G permuta transitivamente los primos que están sobre v, y que se escribe como la unión disjunta de las coclases del grupo de descomposición de un primo fijo sobre v, tantas como primos distintos haya sobre él. Por otra parte, el grupo de descomposición de un primo w sobre v es isomorfo al grupo de Galois local $\mathrm{Gal}(L_w/K_v)$.

Definición 4.4.1. Sea $x \in \mathbb{I}_L$. Se define $\mathrm{N}_{L/K}\, x \in \mathbb{I}_K$ como el idèle

$$(\mathrm{N}_{L/K}\, x)_v = \prod_{w|v} \mathrm{N}_{L_w/K_v}\, x_v.$$

Por las observaciones recién hechas, el siguiente diagrama

$$\begin{array}{ccc} L^\times & \longrightarrow & \mathbb{I}_L \\ {\scriptstyle \mathrm{N}_{L/K}}\downarrow & & \downarrow{\scriptstyle \mathrm{N}_{L/K}} \\ K^\times & \longrightarrow & \mathbb{I}_K \end{array}$$

es conmutativo. Por lo tanto, $\mathrm{N}_{L/K}$ induce un morfismo (que llamamos de la misma manera) $\mathrm{N}_{L/K} : \mathbf{C}_L \to \mathbf{C}_K$. Es claro que $\mathrm{N}_{L/K}$ es continua.

Sea L/K una extensión finita de Galois (no necesariamente abeliana), con $G = \mathrm{Gal}(L/K)$. Entonces G actúa en $\mathbb{A}_L$ de la siguiente manera: si $\alpha = (\alpha_w) \in \mathbb{A}_L$, $(\sigma\alpha)_{\sigma w} = \sigma_w \alpha_w$ (donde $\sigma_w : L_w \to L_{\sigma w}$ es el isomorfismo inducido por σ); es claro que la acción deja fija a $\mathbb{I}_L$, de manera que G actúa en $\mathbb{I}_L$. Tenemos también una inclusión $i : \mathbb{I}_K \to \mathbb{I}_L$ dada por $i(x)_w = x_v$ si $w|v$.

Proposición 4.4.2. *Sea L/K finita de Galois. Entonces $i(\mathrm{N}_{L/K}(x)) = \prod_{\sigma\in\mathrm{Gal}(L/K)} \sigma x$ para todo $x \in \mathbb{I}_L$.*

Dem. Sea w un primo de L, sobre el primo v de K. Sean $w_1, \ldots, w_r$ todos los primos de L sobre v. Para cada i, tomemos $\sigma_i \in \mathrm{Gal}(L/K)$ tal que $\sigma_i w_i = w$. Entonces $\mathrm{Gal}(L/K)$ se escribe como la unión disjunta de los conjuntos $\sigma_i D(w_i)$. Entonces

$$\prod_{\sigma\in\mathrm{Gal}(L/K)} (\sigma x)_w = \prod_{\sigma\in\mathrm{Gal}(L/K)} \sigma_{\sigma^{-1}w} x_{\sigma^{-1}w} =$$

$$\prod_{i=1}^{r} \prod_{\tau\in D(w_i)} (\sigma_i\tau)_{(\sigma_i\tau)^{-1}w} x_{(\sigma_i\tau)^{-1}w} = \prod_{i=1}^{r} \prod_{\tau\in D(w_i)} (\sigma_i)_{w_i} \tau_{w_i}(x_{w_i}) =$$

$$= \prod_{i=1}^{r} (\sigma_i)_{w_i} \mathrm{N}_{L_{w_i}/K_v}(x_{w_i}) = \prod_{i=1}^{r} \mathrm{N}_{L_{w_i}/K_v}(x_{w_i}) = (i(\mathrm{N}_{L/K}(x)))_w$$

(observar que $(\sigma_i)_{w_i}(\mathrm{N}_{L_{w_i}/K_v}(x_{w_i})) = \mathrm{N}_{L_{w_i}/K_v}(x_{w_i})$ ya que $\mathrm{N}_{L_{w_i}/K_v}(x_{w_i}) \in K_v$). □

Recordemos que también tenemos definida la norma para ideales. Vale decir, si $\mathfrak{Q}$ es un ideal primo de L, $\mathrm{N}_{L/K}\,\mathfrak{Q} = \mathfrak{P}^f$, donde $\mathfrak{P} = \mathfrak{Q} \cap K$ y f es el grado de inercia de $\mathfrak{Q}$ sobre $\mathfrak{P}$. Es fácil ver que el siguiente diagrama conmuta:

$$\begin{array}{ccc} L^\times & \xrightarrow{id} & I_L \\ {\scriptstyle \mathrm{N}_{L/K}}\downarrow & & \downarrow{\scriptstyle \mathrm{N}_{L/K}} \\ K^\times & \xrightarrow{id} & I_K, \end{array}$$

esto es, $\mathrm{N}_{L/K}((x)) = (\mathrm{N}_{L/K}(x))$. De esta manera tenemos un morfismo inducido $\mathrm{N}_{L/K} : Cl(L) \to Cl(K)$. El siguiente lema relaciona este morfismo con la norma del grupo de clases de idèles.

Lema 4.4.3. *El siguiente diagrama conmuta*

$$\begin{array}{ccc} \mathbb{I}_L & \xrightarrow{id} & I_L \\ {\scriptstyle \mathrm{N}_{L/K}}\downarrow & & \downarrow{\scriptstyle \mathrm{N}_{L/K}} \\ \mathbb{I}_K & \xrightarrow{id} & I_K. \end{array}$$

Dem. Sea $x = (x_w) \in \mathbb{I}_L$. Entonces si $y = \mathrm{N}_{L/K}\, x$ tenemos que $y_v = \prod_{w|v} \mathrm{N}_{L_w/K_v}\, x_w$. Por una parte, $\mathrm{id}(x) = \prod_{w<\infty} w^{\mathrm{ord}_w(x_w)}$, con lo cual, $\mathrm{N}_{L/K}(\mathrm{id}(x)) = \prod_{w<\infty} \mathrm{N}_{L/K}(w)^{\mathrm{ord}_w(x_w)}$. Si w es finito, $\mathrm{N}_{L/K}\, w = v^{f(w|v)}$, donde v es el primo de K debajo de w. Luego, tenemos que

$$\mathrm{N}_{L/K}(\mathrm{id}(x)) = \prod_{w<\infty} v^{f(w|v)\,\mathrm{ord}_w(x_w)}.$$

Ahora debemos calcular $\mathrm{id}(y) = \prod_{v<\infty} v^{\mathrm{ord}_v(y_v)}$. Pero $\mathrm{ord}_v(y_v) = \sum_{w|v} \mathrm{ord}_v(\mathrm{N}_{L_w/K_v} x_w)$, y

$$\mathrm{ord}_v(\mathrm{N}_{L_w/K_v} x_w) = \frac{1}{e(w|v)} \mathrm{ord}_w(\mathrm{N}_{L_w/K_v} x_w),$$

pues $\mathrm{N}_{L_w/K_v} x_w \in K_v$. Así, obtenemos que

$$\mathrm{ord}_v(\mathrm{N}_{L_w/K_v} x_w) = \frac{1}{e(w|v)} \sum_{\sigma \in \mathrm{Gal}(L_w/K_v)} \mathrm{ord}_w(\sigma x_w).$$

Como $\mathrm{ord}_w(\sigma x_w) = \mathrm{ord}_w(x_w)$ y $(\mathrm{Gal}(L_w/K_v) : 1) = [L_w : K_v] = e(w|v)f(w|v)$, se sigue entonces que

$$\mathrm{ord}_v(\mathrm{N}_{L_w/K_v} x_w) = f(w|v)\, \mathrm{ord}_w(x_w).$$

Luego,

$$\mathrm{id}(y) = \prod_{v<\infty} v^{\sum_{w|v} f(w|v)\, \mathrm{ord}_w(x_w)} = \prod_{w<\infty} w^{f(w|v)\, \mathrm{ord}_w(x_w)},$$

y con esto se termina la demostración. □

Como corolario, tenemos que el siguiente diagrama es conmutativo:

$$\begin{array}{ccc} \mathbf{C}_L & \longrightarrow & Cl(L) \\ {\scriptstyle \mathrm{N}_{L/K}}\downarrow & & \downarrow{\scriptstyle \mathrm{N}_{L/K}} \\ \mathbf{C}_K & \longrightarrow & Cl(K). \end{array}$$

Lema 4.4.4. *Sean L/K y L'/K' extensiones finitas y abelianas, con $K \subset K'$, $L \subset L'$ finitas. Sea S un conjunto de primos de K que contenga a los ramificados en L' (y, por lo tanto, también a los ramificados en L) y S' el conjunto de primos de K' sobre los de S (con lo cual, contiene a los ramificados en L'). Entonces el siguiente diagrama es conmutativo:*

$$\begin{array}{ccc} I_{K'}^{S'} & \xrightarrow{\psi_{L'/K'}} & \mathrm{Gal}(L'/K') \\ {\scriptstyle \mathrm{N}_{K'/K}}\downarrow & & \downarrow{\scriptstyle \mathrm{res}} \\ I_K^S & \xrightarrow{\psi_{L/K}} & \mathrm{Gal}(L/K), \end{array}$$

donde res *es la aplicación natural.*

Dem. Sea $\mathfrak{p}'$ un ideal de K' sobre un ideal $\mathfrak{p}$ de K que no está en S. Entonces $\mathrm{N}_{K'/K}(\mathfrak{p}') = \mathfrak{p}^{f(\mathfrak{p}'|\mathfrak{p})}$. Debemos probar entonces que $\psi_{L/K}(\mathfrak{p})^{f(\mathfrak{p}'|\mathfrak{p})} = \mathrm{res}\, \psi_{L'/K'}(\mathfrak{p}')$. Esto se sigue inmediatamente de la Proposición 1.1.12. □

Corolario 4.4.5. *Sea L/K finita y abeliana, y S el conjunto de primos ramificados. Entonces $\psi_{L/K}(\mathrm{N}_{L/K}(I_L^{S'}) = 1$, donde S' es el conjunto de primos de L sobre los de S.*

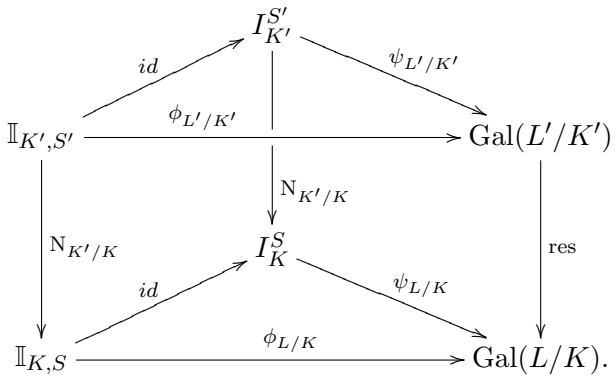
Dem. Tomar $K' = L = L'$ en el lema anterior. □

Proposición 4.4.6. *Sean L/K y L'/K' extensiones finitas y abelianas, con $K \subset K'$, $L \subset L'$ finitas. Supongamos que se cumple la ley de reciprocidad para L/K y L'/K'. Entonces el siguiente diagrama es conmutativo:*

$$\begin{array}{ccc} \mathbb{I}_{K'} & \xrightarrow{\phi_{L'/K'}} & \mathrm{Gal}(L'/K') \\ {\scriptstyle \mathrm{N}_{K'/K}}\downarrow & & \downarrow{\scriptstyle \mathrm{res}} \\ \mathbb{I}_K & \xrightarrow{\phi_{L/K}} & \mathrm{Gal}(L/K), \end{array}$$

donde res *es la aplicación natural.*

Dem. Sea S un conjunto finito de primos de K suficientemente grande. Sea S' el conjunto de primos de K' que están sobre primos de S. Consideremos el siguiente dibujo:



Por el Lema 4.4.3, el paralelogramo de la izquierda conmuta. El de la derecha también, por el Lema 4.4.4. Además, el techo y el piso conmutan por las propiedades del mapa de Artin. Luego, el rectángulo frontal conmuta, con lo cual, $\mathrm{res} \circ \phi_{L'/K'}$ coincide con $\phi_{L/K} \circ \mathrm{N}_{K'/K}$ en el conjunto $\mathbb{I}_{K',S'}$; como también coinciden en $(K')^\times$, son iguales en $(K')^\times \mathbb{I}_{K',S'}$. Por el Lema 3.3.12 , este conjunto es denso en $\mathbb{I}_{K'}$. La proposición queda probada pues las cuatro aplicaciones son continuas. □

Corolario 4.4.7. *Sean L/K finita abeliana y K' un cuerpo intermedio, $K \subset K' \subset L$, tales que L/K y L/K' cumplen la ley de reciprocidad. Entonces $\phi_{L/K}(\mathrm{N}_{K'/K}\, \mathbb{I}_{K'}) \subset \mathrm{Gal}(L/K')$.*

Dem. Tomar $L = L'$ en la proposición anterior. □

Corolario 4.4.8. *Sea L/K finita abeliana tal que cumple la ley de reciprocidad. Entonces $\phi_{L/K}(\mathrm{N}_{L/K}\, \mathbb{I}_L) = 1$.*

Dem. Tomar $K' = L' = L$ en la proposición anterior. □

Como $\phi_{L/K}(K^\times) = 1$, el último corolario dice que $\phi_{L/K}(K^\times \mathrm{N}_{L/K}\, \mathbb{I}_L) = 1$. En la siguiente sección veremos entre otras cosas que el núcleo es exactamente $K^\times \mathrm{N}_{L/K}\, \mathbb{I}_L$.

4.5. Teoremas principales

Reformularemos todos los teoremas hechos al principio de este capítulo en términos de idèles.

Teorema 4.5.1. *Toda extensión abeliana finita L/K cumple la ley de reciprocidad.*

Teorema 4.5.2. *El mapa de Artin $\phi_{L/K}$ es suryectivo y $\ker(\phi_{L/K}) = K^\times \mathrm{N}_{L/K}\, \mathbb{I}_L$. Por lo tanto, $\phi_{L/K}$ induce un isomorfismo*

$$\mathbb{I}_K/K^\times \mathrm{N}_{L/K}\, \mathbb{I}_L \xrightarrow{\phi_{L/K}} \mathrm{Gal}(L/K).$$

Si vemos a $\phi_{L/K}$ como un morfismo $\phi_{L/K} : \mathbf{C}_K \to \mathrm{Gal}(L/K)$ entonces su núcleo es $\mathrm{N}_{L/K}\, \mathbf{C}_L$, e induce un isomorfismo

$$\mathbf{C}_K \,/\, \mathrm{N}_{L/K}\, \mathbf{C}_L \xrightarrow{\phi_{L/K}} \mathrm{Gal}(L/K).$$

Teorema 4.5.3. *Sea $K \subset K' \subset L$ una torre de extensiones abelianas finitas. Entonces el siguiente diagrama es conmutativo:*

$$\begin{array}{ccc} \mathbf{C}_K \,/\, \mathrm{N}_{L/K}\, \mathbf{C}_L & \xrightarrow{\phi_{L/K}} & \mathrm{Gal}(L/K) \\ \downarrow & & \downarrow{\scriptstyle \mathrm{res}} \\ \mathbf{C}_K \,/\, \mathrm{N}_{K'/K}\, \mathbf{C}_{K'} & \xrightarrow{\phi_{K'/K}} & \mathrm{Gal}(K'/K), \end{array}$$

donde la flecha de la derecha es el morfismo natural $(\mathrm{N}_{L/K}\, \mathbf{C}_L \subset \mathrm{N}_{K'/K}\, \mathbf{C}_{K'})$.

Observemos que dada L/K extensión finita y abeliana, el subgrupo $\mathrm{N}_{L/K}\, \mathbf{C}_L \leq \mathbf{C}_K$ es abierto y de índice finito. El siguiente teorema asegura la recíproca.

Teorema 4.5.4 (Existencia)**.** *Para todo $N \subset \mathbf{C}_K$ subgrupo abierto, existe una única extension L/K finita abeliana (dentro de una clausura algebraica fija K^{al}) tal que $N = \mathrm{N}_{L/K}\, \mathbf{C}_L$.*

Los grupos que aparecen en el último teorema se llaman *grupos norma*, y la extensión L/K correspondiente se llama *cuerpo de clases* de N. Notemos que todo subgrupo abierto de $\mathbf{C}_K$ es de índice finito (Proposición 4.3.3); en el caso de un cuerpo global cualquiera K esto no es necesariamente cierto, y en el teorema hay que pedir subgrupos abiertos de índice finito. Si N es un subgrupo abierto de $\mathbb{I}_K$, el cuerpo de clases de N se define como el cuerpo de clases de su imagen en $\mathbf{C}_K$. Notemos que su imagen coincide con la imagen de $K^\times N$.

A veces se suele denominar *ley de reciprocidad* a ambos resultados 4.5.1 y 4.5.2.

Observación 4.5.5. Si suponemos válidos los Teoremas 4.5.1 y 4.5.2, el Teorema 4.5.3 se sigue entonces de la Proposición 4.4.6.

Sea K^{ab} la clausura abeliana de K, la unión de todas las extensiones finitas y abelianas dentro de una clausura algebraica fija K^{al}. Por el Teorema 4.5.3, podemos hacer el paso al límite y obtener un morfismo $\phi_K : \mathbf{C}_K \to \mathrm{Gal}(K^{ab}/K)$ (que es el límite de los grupos de Galois de las extensiones finitas y abelianas L/K). Se puede ver que este morfismo es suryectivo, continuo (al considerar en $\mathrm{Gal}(K^{ab}/K)$ la topología profinita, es decir, la topología limite de los $\mathrm{Gal}(L/K)$ considerados discretos) y cumple que para toda extensión finita y abeliana L/K, define un isomorfismo

$$\mathbf{C}_K / N_{L/K}\, \mathbf{C}_L \to \mathrm{Gal}(L/K).$$

El núcleo de ϕ_K es la componente conexa de la identidad D_K en $\mathbf{C}_K$, y se obtiene un isomorfismo canónico $\mathbf{C}_K / D_K \simeq \mathrm{Gal}(K^{ab}/K)$. Sin embargo, esta componente conexa puede llegar a ser muy complicada.

El siguiente corolario es consecuencia inmediata de los últimos teoremas.

Corolario 4.5.6. *La aplicación $L \longleftrightarrow \mathrm{N}_{L/K}\, \mathbf{C}_L$ (respectivamente $L \longleftrightarrow K^\times \mathrm{N}_{L/K}\, \mathbb{I}_L$) establece una biyección entre extensiones finitas abelianas de K y subgrupos abiertos de $\mathbf{C}_K$ (respectivamente de $\mathbb{I}_K$ tales que contienen a $K^\times$). Si L se corresponde con N y L' con N' entonces $L \subset L'$ si y sólo si $N \supset N'$; LL' se corresponde con $N \cap N'$, y $L \cap L'$ con NN'.*

Dem. Sólo falta probar las últimas tres afirmaciones. Sean N, N' subgrupos abiertos de $\mathbf{C}_K$ y L, L' sus cuerpos de clases. El núcleo del mapa de Artin $\mathbf{C}_K \to \mathrm{Gal}(LL'/K)$ es $N \cap N'$ debido a las propiedades de consistencia con torres de extensiones. Luego, el cuerpo de clases de $N \cap N'$ es LL'.

Supongamos que $L \subset L'$. Por la transitividad de la norma, se sigue que $N \supset N'$. Si $N \supset N'$ entonces $N \cap N' = N'$. Por un lado, $(\mathbf{C}_K : N') = [L' : K]$, y por otro, $(\mathbf{C}_K : N') = (\mathbf{C}_K : N' \cap N) = [LL' : K]$. Como $K \subset L' \subset LL'$, se sigue que $L' = LL'$, con lo cual, $L \subset L'$.

Ahora, consideremos el mapa de Artin $\mathbf{C}_K \to \mathrm{Gal}(L \cap L'/K)$. De vuelta por las propiedades de consistencia, tanto N como N' están contenidos en el núcleo, con lo cual, el producto también. □

Observación 4.5.7. Por la teoría de Galois infinita, se tiene una correspondencia entre subgrupos abiertos de índice finito de $\mathrm{Gal}(K^{ab}/K)$ y extensiones finitas y abelianas L/K, dada por $L/K \mapsto \mathrm{Gal}(K^{ab}/L)$. Además, todo subgrupo abierto de $\mathbf{C}_K$ contiene a D_K (ver la demostración de la Proposición 4.3.2), con lo cual, el mapa de Artin establece una correspondencia biyectiva entre subgrupos abiertos de índice finito de $\mathbf{C}_K$ y de $\mathrm{Gal}(K^{ab}/K)$. Finalmente, la teoría de cuerpos de clases nos hace corresponder tales subgrupos de $\mathbf{C}_K$ con extensiones finitas y abelianas. Es inmediato ver que estas tres correspondencias son compatibles.

Corolario 4.5.8. *Sea L/K el cuerpo de clases de $N \subset \mathbf{C}_K$, y sea $N' \supset N$. Entonces el cuerpo de clases de N' es el cuerpo fijo de $\phi_{L/K}(N') \subset \mathrm{Gal}(L/K)$.*

Dem. Sea L' el cuerpo fijo de $\phi_{L/K}(N')$, que es una extensión finita y abeliana. Por las propiedades de consistencia del mapa de Artin, es fácil ver que N' es el núcleo de $\phi_{L'/K} : \mathbf{C}_K \to \mathrm{Gal}(L'/K)$, con lo cual, L' es el cuerpo de clases de N'. □

Observación 4.5.9. Hasta aquí no hemos hablado de cómo se relaciona la ley de reciprocidad de Artin con las leyes de reciprocidad clásicas. Es interesante hacer los ejercicios del final de [CaF67], en donde se vislumbra esta relación.

4.6. Relación con los grupos de clases de ideales

Suponiendo los Teoremas 4.5.1-4.5.4 probaremos 4.2.1 y 4.2.2.

Lema 4.6.1. *Sea L/K una extensión finita de cuerpos locales no arquimedeanos, tal que $\mathrm{N}_{L/K}(L^\times)$ tiene índice finito en $K^\times$. Entonces $\mathrm{N}_{L/K}(L^\times)$ es abierto en $K^\times$.*

Dem. Sabemos que $\mathcal{U}_L = \mathcal{O}_L^\times$ es compacto, con lo cual, $\mathrm{N}_{L/K}(\mathcal{U}_L)$ es cerrado en $K^\times$. Como $\mathrm{N}_{L/K}(\mathcal{U}_L) \subset \mathcal{U}_K$, y sólo las unidades tienen norma que son unidades, se tiene un morfismo inyectivo $\mathcal{U}_K/\mathrm{N}_{L/K}(\mathcal{U}_L) \hookrightarrow K^\times/\mathrm{N}_{L/K}(L^\times)$. Por lo tanto, $\mathrm{N}_{L/K}(\mathcal{U}_L)$ es un cerrado de $\mathcal{U}_K$ de índice finito, con lo cual, es abierto en $\mathcal{U}_K$ (y por ende en $K^\times$, al serlo $\mathcal{U}_K$). Luego, $\mathrm{N}_{L/K}(L^\times)$ contiene un subgrupo abierto, y, por lo tanto, debe ser abierto. □

Proposición 4.6.2. *Sea L/K finita. Entonces $\mathrm{N}_{L/K}\,\mathbb{I}_L$ es un subgrupo abierto de $\mathbb{I}_K$ (y, por lo tanto, también lo son $K^\times\,\mathrm{N}_{L/K}\,\mathbb{I}_L$ y su imagen $\mathrm{N}_{L/K}(\mathbf{C}_L)$ en $\mathbf{C}_K$).*

Dem. Para cada primo v, sea w un primo de L sobre v. Sea S el conjunto de primos ramificados en L/K. Si $v \notin S$ entonces $\mathcal{U}_v = \mathrm{N}_{L_w/K_v}(\mathcal{U}_w)$; esto se debe a 6.2.8. Si v es ramificado y finito, como $\mathrm{N}_{L_w/K_v}(L_w^\times)$ es abierto en $K_v^\times$ (por 6.1.1 y el lema anterior), existe un $r_v \in \mathbb{N}$ tal que $\mathrm{N}_{L_w/K_v}(L_w^\times) \supset 1 + \widehat{\mathfrak{p}_v}^{r_v}$. Si v es ramificado e infinito entonces es real y $\mathbb{R}_+$ (visto dentro de $K_v^\times$) es exactamente el grupo de normas de la extensión local L_w/K_v, donde w es un primo complejo sobre v. Tomando $V = \prod_{v\in S, v<\infty}(1+\widehat{\mathfrak{p}_v}^{r_v}) \times \prod_{v\in S, v\in S_\infty}\mathbb{R}_+ \times \prod_{v\notin S}\mathcal{U}_v$, al ser $\mathcal{U}_v = K_v^\times$ si v es infinito, se sigue que V es un entorno de 1 y $\mathrm{N}_{L/K}\,\mathbb{I}_K \supset V$. Luego, $\mathrm{N}_{L/K}\,\mathbb{I}_L$ es abierto al tratarse de subgrupos. □

Sea L/K una extensión finita y abeliana. Sabemos que un subgrupo $N \subset \mathbb{I}_K$ es abierto si sólo si $W_\mathfrak{m} \subset N$ para algún módulo $\mathfrak{m}$. En ese caso, diremos que $\mathfrak{m}$ es *admisible* para N. Diremos que $\mathfrak{m}$ es admisible para L/K si lo es para $K^\times\,\mathrm{N}_{L/K}\,\mathbb{I}_L$.

Notemos que si $\mathfrak{n}|\mathfrak{m}$ entonces $W_\mathfrak{m} \subset W_\mathfrak{n}$, y dados $\mathfrak{m}$ y $\mathfrak{n}$, $W_\mathfrak{m}W_\mathfrak{n} = W_{(\mathfrak{m},\mathfrak{n})}$ (siendo $(\mathfrak{m},\mathfrak{n})$ el máximo común divisor de $\mathfrak{m}$ y $\mathfrak{n}$ con la definición obvia). Dado N abierto, existe un módulo $\mathfrak{f}(N)$ minimal entre los admisibles para N, que lo llamaremos el *conductor* de N; es admisible y divide a cualquier otro admisible para N. El conductor de L/K es el conductor de $K^\times\,\mathrm{N}_{L/K}\,\mathbb{I}_L$.

Proposición 4.6.3. *Sea L/K finita y abeliana. Entonces los primos ramificados son exactamente los que dividen a $\mathfrak{f}(L/K)$.*

Demostración. En la demostración de la Proposición 4.6.2, vimos que el grupo de normas contiene a $W_\mathfrak{m}$ para un cierto módulo $\mathfrak{m}$, divisible exactamente por los primos ramificados. Luego, es admisible y, por lo tanto, el conductor lo divide.

Para la recíproca, sea v un primo ramificado. Debemos ver que $v|\mathfrak{f}(L/K)$. Supongamos primero que v es finito. Entonces, al ser ramificado, por 6.2.8, se tiene que si $w|v$ entonces

$\mathcal{U}_v \neq \mathrm{N}_{L_w/K_v}\mathcal{U}_w$. De aquí se sigue que debe dividir al conductor, ya que es fácil ver que si un elemento es de la forma $\prod_{w|v}\mathrm{N}_{L_w/K_v}\,y_w$ entonces es una norma local en cada extensión.

En el caso en que v sea infinito y $w|v$, debe ser v real y w complejo; por lo tanto,

$$\mathrm{N}_{L_w/K_v}\,L_w^\times = \mathbb{R}_+$$

y $v|\mathfrak{f}(L/K)$. □

Corolario 4.6.4. *Sea L/K finita y abeliana y $\mathfrak{m}$ un módulo admisible para L/K. Entonces $\mathfrak{m}$ es divisible por todos los primos ramificados.*

Proposición 4.6.5. *Sea L/K finita y abeliana. Entonces $\mathfrak{m}$ es admisible para L/K si y sólo si $S \subset S(\mathfrak{m})$ y $\psi_{L/K}(P_{K,1}(\mathfrak{m})) = 1$, donde S es el conjunto de primos ramificados.*

Dem. Sea $\mathfrak{m}$ admisible para L/K. Por el corolario anterior, $S \subset S(\mathfrak{m})$; además, $\phi_{L/K}(W_\mathfrak{m}) = 1$. Mirando la demostración de la Proposición 4.3.4, construimos $\psi : I_K(\mathfrak{m}) \to \mathrm{Gal}(L/K)$ tal que $\psi(P_{K,1}(\mathfrak{m})) = 1$. Pero ψ y $\psi_{L/K}$ deben coincidir en $I_K(\mathfrak{m})$, y esto prueba una implicación.

Recíprocamente, sea $\mathfrak{m}$ tal que $S \subset S(\mathfrak{m})$ y $\psi_{L/K}(P_{K,1}(\mathfrak{m})) = 1$. Veremos que $L \subset K_\mathfrak{m}$ (el cuerpo de clases radial), y por la Proposición 4.6.7, $\mathfrak{f}(L/K)|\mathfrak{m}$, con lo cual, $\mathfrak{m}$ será admisible para L/K (ver las demostraciones de la última sección de este capítulo). Sea $\psi = \psi_{L/K} : I_K(\mathfrak{m}) \to \mathrm{Gal}(L/K)$ y $\psi_\mathfrak{m} = \psi_{K_\mathfrak{m}/K} : I_K(\mathfrak{m}) \to \mathrm{Gal}(K_\mathfrak{m}/K)$. La imagen de $\ker(\psi)$ por $\psi_\mathfrak{m}$ nos da un subgrupo de $\mathrm{Gal}(K_\mathfrak{m}/K)$, que debe ser de la forma $\mathrm{Gal}(K_\mathfrak{m}/\widetilde{L})$ para una subextensión $K \subset \widetilde{L} \subset K_\mathfrak{m}$. Afirmamos que $L = \widetilde{L}$.

Tanto en L/K como en $\widetilde{L}/K$ los primos ramificados dividen a $\mathfrak{m}$ (por hipótesis y por estar $\widetilde{L} \subset K_\mathfrak{m}$). Sea $\widetilde{\psi} = \psi_{\widetilde{L}/K} : I_K(\mathfrak{m}) \to \mathrm{Gal}(\widetilde{L}/K)$. Probaremos que $\ker(\psi) = \ker(\widetilde{\psi})$, y por la unicidad del teorema de existencia, $L = \widetilde{L} \subset K_\mathfrak{m}$.

Si r denota la restricción $r : \mathrm{Gal}(K_\mathfrak{m}/K) \to \mathrm{Gal}(\widetilde{L}/K)$, entonces $r \circ \psi_\mathfrak{m} = \widetilde{\psi}$. Supongamos que $\widetilde{\psi}(x) = 1$. Entonces $\psi_\mathfrak{m}(x) \in \ker(r) = \mathrm{Gal}(K_\mathfrak{m}/\widetilde{L}) = \psi_\mathfrak{m}(\ker(\psi))$. Entonces $x = yz$, con $y \in \ker(\psi_\mathfrak{m})$ y $z \in \ker(\psi)$. Como $\ker(\psi_\mathfrak{m}) = P_{K,1}(\mathfrak{m})$ y $\psi(P_{K,1}(\mathfrak{m})) = 1$ por hipótesis, se sigue que $x \in \ker(\psi)$.

Recíprocamente, si $x \in \ker(\psi)$, $\psi_\mathfrak{m}(x) \in \mathrm{Gal}(K_\mathfrak{m}/\widetilde{L})$ y, por lo tanto, $\widetilde{\psi}(x) = r\psi_\mathfrak{m}(x) = 1$. Esto prueba lo que queríamos.

□

Observemos que siempre existe un módulo admisible para L/K, pues el grupo de normas es abierto, pero esto no implica que podamos pasar por alto el resto de los teoremas de la sección anterior, ya que usamos fuertemente la existencia del mapa de Artin $\phi_{L/K}$.

4.6.1. La ley de reciprocidad

A lo largo de esta sección, L/K será una extensión finita y abeliana. El conjunto S consistirá de los primos ramificados (finitos o infinitos) de la extensión, y S' será el conjunto de primos de L que están sobre los de S.

Por el Teorema 4.5.1, L/K cumple la ley de reciprocidad, con lo cual, la Proposición 4.3.4 implica que existe un módulo $\mathfrak{m}$ con $\psi : I_K(\mathfrak{m}) \to \mathrm{Gal}(L/K)$ tal que $\psi(P_{K,1}(\mathfrak{m})) = 1$ y

$\phi_{L/K}(x) = \psi(\mathrm{id}(x))$ si $x \in \mathbb{I}_{K,S(\mathfrak{m})}$. De hecho, si nos fijamos en el $\mathfrak{m}$ que tomamos en la demostración de la Proposición 4.3.4, podemos tomarlo como el conductor (pues $\phi_{L/K}$ se anula en $W_{\mathfrak{m}}$ si $\mathfrak{m}$ es admisible para L/K), de manera que $S(\mathfrak{m}) = S$. Por las propiedades de $\phi_{L/K}$, se sigue que ψ no es otra cosa que el mapa de Artin $\psi_{L/K}$.

Consideremos $\mathrm{id} : \mathbb{I}_{\mathfrak{m}} \to I_K(\mathfrak{m})$. Es claramente un epimorfismo que se factoriza por $K_{\mathfrak{m},1}$, y que, por lo tanto, da lugar a un epimorfismo $p_{\mathfrak{m}} : \mathbb{I}_{\mathfrak{m}}/K_{\mathfrak{m},1} \to I_K(\mathfrak{m})$. Sea $\omega_{\mathfrak{m}} = \theta_{\mathfrak{m}}^{-1}$ (ver Proposición 4.3.1).

Proposición 4.6.6. *La aplicación $p_{\mathfrak{m}} \circ \omega_{\mathfrak{m}}$ induce un isomorfismo*

$$\mathbb{I}_K/K^\times \mathrm{N}_{L/K}\, \mathbb{I}_L \to I_K(\mathfrak{m})/P_{K,1}(\mathfrak{m})\, \mathrm{N}_{L/K}(I_L^{S'}).$$

Dem. Consideremos $\mathrm{id} : \mathbb{I}_{\mathfrak{m}} \to I_K(\mathfrak{m})$, cuyo núcleo es $W_{\mathfrak{m}}$; afirmamos primero que

$$\mathrm{id}^{-1}(P_{K,1}(\mathfrak{m})\, \mathrm{N}_{L/K}(I_L^{S'})) = K_{\mathfrak{m},1} W_{\mathfrak{m}}\, \mathrm{N}_{L/K}(\mathbb{I}_{L,S'}),$$

donde $\mathbb{I}_{L,S'}$ son los idèles de L con coordenada 1 en los primos de S'. En efecto, sea $x \in \mathbb{I}_{\mathfrak{m}}$ tal que $\mathrm{id}(x) = \mathrm{id}(a)\, \mathrm{N}_{L/K}(\mathfrak{b})$, con $a \in K_{\mathfrak{m},1}$ y $\mathfrak{b} \in I_L^{S'}$. Tomamos $y \in \mathbb{I}_L$ definido de la siguiente manera: $y_w = 1$ si w es infinito, $w \in S'$ ó w es finito y coprimo con $\mathfrak{b}$. Si w es finito, $w \notin S'$ y $w|\mathfrak{b}$, sea $t_w \in \mathbb{Z} - \{0\}$ el exponente al cual aparece en $\mathfrak{b}$; tomamos entonces $y_w = \pi_w^{t_w}$, con π_w un uniformizador. De esta manera, $\mathrm{id}(y) = \mathfrak{b}$, y, además, $y \in \mathbb{I}_{L,S'}$. Por la Proposición 4.4.3, $\mathrm{id}(x) = \mathrm{id}(a\, \mathrm{N}_{L/K}(y))$, y se sigue entonces que $x \in K_{\mathfrak{m},1} W_{\mathfrak{m}}\, \mathrm{N}_{L/K}(\mathbb{I}_{L,S'})$. Para probar la otra inclusión, notemos que $W_{\mathfrak{m}}$ va a parar a 1, $K_{\mathfrak{m},1}$ a $P_{K,1}(\mathfrak{m})$ y $\mathrm{N}_{L/K}(\mathbb{I}_{L,S'})$ a $\mathrm{N}_{L/K}(I_L^{S'})$.

Hemos obtenido entonces un isomorfismo

$$\mathbb{I}_{\mathfrak{m}}/K_{\mathfrak{m},1} W_{\mathfrak{m}}\, \mathrm{N}_{L/K}(\mathbb{I}_{L,S'}) \simeq I_K(\mathfrak{m})/P_{K,1}(\mathfrak{m})\, \mathrm{N}_{L/K}(I_L^{S'}).$$

Probaremos ahora que $\omega_{\mathfrak{m}}^{-1}(K_{\mathfrak{m},1} W_{\mathfrak{m}}\, \mathrm{N}_{L/K}(\mathbb{I}_{L,S'})/K_{\mathfrak{m},1}) = K^\times\, \mathrm{N}_{L/K}(\mathbb{I}_L)/K^\times$, y esto terminará la demostración. Para probarlo, basta demostrar que $K_{\mathfrak{m},1} W_{\mathfrak{m}}\, \mathrm{N}_{L/K}(\mathbb{I}_{L,S'}) = \mathbb{I}_{\mathfrak{m}} \cap K^\times\, \mathrm{N}_{L/K}(\mathbb{I}_L)$.

Veamos la primera inclusión. En primer lugar, $K_{\mathfrak{m},1} \subset \mathbb{I}_{\mathfrak{m}} \cap K^\times$ y $\mathrm{N}_{L/K}(\mathbb{I}_{L,S'}) \subset \mathbb{I}_{\mathfrak{m}} \cap \mathrm{N}_{L/K}(\mathbb{I}_L)$. Además, como $\mathfrak{m}$ es admisible, se tiene que $W_{\mathfrak{m}} \subset \mathbb{I}_{\mathfrak{m}} \cap \mathrm{N}_{L/K}(\mathbb{I}_L)$.

Para la otra inclusión, sea $x \in \mathbb{I}_{\mathfrak{m}} \cap K^\times\, \mathrm{N}_{L/K}(\mathbb{I}_L)$. Escribamos $x = \alpha\, \mathrm{N}_{L/K}(y)$, con $\alpha \in K^\times$, $y \in \mathbb{I}_L$.

Sea $\epsilon > 0$ suficientemente chico (a determinar) y tomemos $M = \mín\{|(\mathrm{N}_{L/K}\, y^{-1})_v|_v : v|\mathfrak{m}\}$. Sea ahora $\delta > 0$ tal que las siguientes condiciones

$$|a_w - b_w|_w < \delta \ \forall w|v \ \forall v|\mathfrak{m}$$

(con $a_w, b_w \in L_w^\times$) impliquen que

$$|\prod_{w|v} \mathrm{N}_{L_w/K_v}\, a_w - \prod_{w|v} \mathrm{N}_{L_w/K_v}\, b_w|_v < M\epsilon \ \forall v|\mathfrak{m}$$

(esto lo podemos hacer porque el producto de las normas locales $\prod_{w|v} L_w^\times \to K_v^\times$ es continuo).

Ahora bien, por el teorema de aproximación, existe $\gamma \in L^\times$ tal que $|\gamma - y_w^{-1}|_w < \delta$ para todo $w|v$, para todo $v|\mathfrak{m}$. Entonces se tiene que

$$|\prod_{w|v} \mathrm{N}_{L_w/K_v}\, \gamma - \prod_{w|v} \mathrm{N}_{L_w/K_v}(y_w)^{-1}|_v < M\epsilon$$

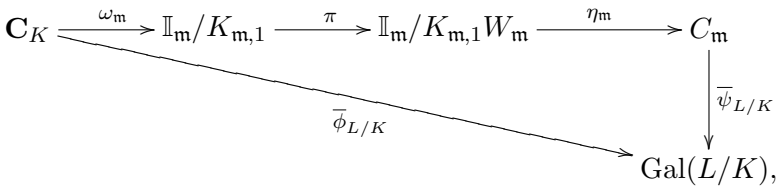
para todo $v|\mathfrak{m}$. Es decir, $|\,\mathrm{N}_{L/K}\,\gamma - (\mathrm{N}_{L/K}\,y^{-1})_v|_v < M\epsilon$. Luego, se sigue que

$$|(\mathrm{N}_{L/K}\,\gamma y)_v - 1|_v < \epsilon$$

para todo $v|\mathfrak{m}$, con lo cual, $\mathrm{N}_{L/K}(\gamma y) \in \mathbb{I}_\mathfrak{m}$ si tomamos ϵ suficientemente chico. Luego, escribiendo $x = \alpha\,\mathrm{N}_{L/K}(\gamma^{-1})\,\mathrm{N}_{L/K}(\gamma y)$, al estar $x \in \mathbb{I}_\mathfrak{m}$, obtenemos que $\alpha\,\mathrm{N}_{L/K}(\gamma^{-1}) \in \mathbb{I}_\mathfrak{m} \cap K^\times = K_{\mathfrak{m},1}$.

Ahora bien, descompongamos $\mathrm{N}_{L/K}(\gamma y) = \mathrm{N}_{L/K}(a)\,\mathrm{N}_{L/K}(b)$, donde $a \in \mathbb{I}_{L,S'}$, y b tiene componente 1 en todos los primos que no están en S' y coordenada γy_w en los $w \in S'$. Para concluir la demostración, debemos ver que $\mathrm{N}_{L/K}(b) \in W_\mathfrak{m}$, y esto es inmediato. □

Queremos ver que $\psi_{L/K}$ es suryectiva y su núcleo es exactamente $P_{K,1}(\mathfrak{m})N_{L/K}I_L^{S'}$. Consideremos $\overline{\psi}_{L/K} : C_\mathfrak{m} \to \mathrm{Gal}(L/K)$ y $\overline{\phi}_{L/K} : \mathbf{C}_K \to \mathrm{Gal}(L/K)$, los morfismos obtenidos de pasar al cociente $\psi_{L/K}$ y $\phi_{L/K}$ respectivamente. Tomemos el siguiente diagrama:



donde π es la proyección al cociente. Afirmamos que es conmutativo. En efecto, el hecho de que $\theta_\mathfrak{m}$ sea un isomorfismo dice que dado $x \in \mathbb{I}_K$, existe $y \in \mathbb{I}_\mathfrak{m}$ tal que $\overline{x} = \overline{y}$ en $\mathbf{C}_K$. La aplicación $\omega_\mathfrak{m}$ entonces manda $\overline{x}$ en $[y] \in \mathbb{I}_\mathfrak{m}/K_{\mathfrak{m},1}$. El morfismo π lo manda en $\{y\} \in \mathbb{I}_\mathfrak{m}/K_{\mathfrak{m},1}W_\mathfrak{m}$. Pero podemos escribir $y = pz$, donde $p_v = y_v$ para $v \in S$, $p_v = 1$ para $v \notin S$, $z_v = 1$ para $v \in S$ y $z_v = y_v$ para $v \notin S$, de manera que $z \in \mathbb{I}_{K,S}$ y $p \in W_\mathfrak{m}$. Como $\{y\} = \{z\} \in \mathbb{I}_\mathfrak{m}/K_{\mathfrak{m},1}W_\mathfrak{m}$, se tiene que $\{y\}$ va a parar a $\langle \mathrm{id}(z)\rangle \in C_\mathfrak{m}$ vía $\eta_\mathfrak{m}$, y el recorrido final de $\overline{x}$ por uno de los caminos del diagrama es $\psi_{L/K}(\mathrm{id}(z))$. Pero como $z \in \mathbb{I}_{K,S}$, tenemos que $\psi_{L/K}(\mathrm{id}(z)) = \phi_{L/K}(z)$. Por otra parte, $\overline{\phi}_{L/K}(\overline{x}) = \overline{\phi}_{L/K}(\overline{y}) = \phi_{L/K}(p)\phi_{L/K}(z) = \phi_{L/K}(z)$ (pues al ser $\mathfrak{m}$ admisible, $\phi_{L/K}(W_\mathfrak{m}) = 1$), lo que queríamos demostrar.

Ahora bien, al ser el diagrama conmutativo y $\overline{\phi}_{L/K}$ suryectivo, se sigue que $\overline{\psi}_{L/K}$ lo es, y, por lo tanto, también lo es $\psi_{L/K}$.

Tomemos ahora $N = \ker(\psi_{L/K} : I_K(\mathfrak{m}) \to \mathrm{Gal}(L/K))$. Sabemos que $P_{K,1}(\mathfrak{m}) \subset N$, y por el Corolario 4.4.5, $\mathrm{N}_{L/K}(I_L^{S'}) \subset N$. Queda probado entonces que $P_{K,1}(\mathfrak{m})\,\mathrm{N}_{L/K}(I_L^{S'}) \subset N$.

Sabemos que

$$(I_K(\mathfrak{m}) : N) = [L : K],$$

mientras que, por otra parte,

$$(I_K(\mathfrak{m}) : P_{K,1}(\mathfrak{m})\,\mathrm{N}_{L/K}(I_L^{S'})) = (\mathbb{I}_K : K^\times\,\mathrm{N}_{L/K}\,\mathbb{I}_L) = [L:K]$$

(esto último es debido a que $\ker(\phi_{L/K}) = K^\times\,\mathrm{N}_{L/K}\,\mathbb{I}_L$). Entonces $N = P_{K,1}(\mathfrak{m})\,\mathrm{N}_{L/K}(I_L^{S'})$, y queda probado el Teorema 4.2.1.

Como resultado particular, resaltamos que el mapa de Artin induce tal isomorfismo para *cualquier* módulo admisible $\mathfrak{m}$. En efecto, lo acabamos de ver para el caso en que $S(\mathfrak{m}) = S$. Para el caso general, basta considerar el isomorfismo de la última proposición, en la cual sólo se usa que $\mathfrak{m}$ es admisible. Además, hemos probado que si el núcleo del mapa de Artin es un subgrupo de congruencia, $\mathfrak{m}$ debe ser admisible, y existe un $\mathfrak{f}$ admisible (el conductor de la extensión) tal que es mínimo con esa propiedad.

4.6.2. El teorema de existencia

Sea $\mathfrak{m}$ un módulo de K y H un subgrupo de congruencia para $\mathfrak{m}$. Vía los isomorfismos $\theta_\mathfrak{m}$ y $\eta_\mathfrak{m}$ de la Proposición 4.3.1, se tiene un epimorfismo $p_\mathfrak{m} : \mathbf{C}_K \to C_\mathfrak{m}$. Considerando $\widetilde{H}$, la imagen de H en $C_\mathfrak{m}$, conseguimos un subgrupo $G \subset \mathbf{C}_K$ definido por $G = p_\mathfrak{m}^{-1}(\widetilde{H})$. Si $q : \mathbb{I}_K \to \mathbf{C}_K$ es la proyección al cociente, se tiene que $W_\mathfrak{m} \subset q^{-1}(G)$, y como q es abierta, resulta que G es abierto en $\mathbf{C}_K$. Por el Teorema 4.5.4, existe una extensión finita y abeliana L/K tal que $G = \mathrm{N}_{L/K}(\mathbf{C}_L)$. Además, por construcción, $\mathfrak{m}$ es admisible para L/K. Luego, los primos ramificados de esta extensión dividen a $\mathfrak{m}$ y $\ker(\psi_{L/K} : I_K^{S(\mathfrak{m})} \to \mathrm{Gal}(L/K)) = P_{K,1}(\mathfrak{m})\,\mathrm{N}_{L/K}(I_L^{S(\mathfrak{m})'})$. Probemos que H es igual a este último grupo, con lo cual, se tendrá que $H = \ker(\psi_{L/K} : I_K^{S(\mathfrak{m})} \to \mathrm{Gal}(L/K))$.

Por definición, $P_{K,1}(\mathfrak{m}) \subset H$; es fácil ver que $\mathrm{N}_{L/K}(I_L^{S(\mathfrak{m})'})$ también. Ahora consideramos índices: $(I_K(\mathfrak{m}) : H) = (C_\mathfrak{m} : \widetilde{H}) = (\mathbf{C}_K : G) = [L:K]$. Finalmente, se sigue que H debe ser el núcleo de $\psi_{L/K} : I_K(\mathfrak{m}) \to \mathrm{Gal}(L/K)$.

Para la unicidad, sea $\widetilde{L}/K$ tal que los primos ramificados dividen a $\mathfrak{m}$ y $H = \ker(\psi_{\widetilde{L}/K} : I_K(\mathfrak{m}) \to \mathrm{Gal}(\widetilde{L}/K)$. Debemos ver que esto implica que $G = \mathrm{N}_{\widetilde{L}/K}\,\mathbf{C}_{\widetilde{L}}$; luego, por la unicidad del Teorema 4.5.4, $L = \widetilde{L}$. La demostración no es más que el tipo de cuentas que estuvimos haciendo hasta ahora y la dejamos como ejercicio.

4.6.3. Cuerpos de clases radiales

Recordemos que, dado $\mathfrak{m}$, habíamos definido $K_\mathfrak{m}$, el cuerpo de clases radial módulo $\mathfrak{m}$, como el cuerpo de clases del subgrupo de congruencia $P_{K,1}(\mathfrak{m})$. Según vimos en 4.6.2, debe ser el cuerpo de clases de $K^\times W_\mathfrak{m}$ (o de $W_\mathfrak{m}$). Se sigue inmediatamente que $\mathfrak{f}(K^\times W_\mathfrak{m})|\mathfrak{m}$, y esto implica que los primos ramificados en $K_\mathfrak{m}$ dividen a $\mathfrak{m}$. El siguiente resultado dice que $K_\mathfrak{m}$ es la máxima extensión finita y abeliana cuyo conductor divide a $\mathfrak{m}$. En particular, $\mathcal{H}_K$, el cuerpo de clases de Hilbert de K ($K_\mathfrak{m}$ con $\mathfrak{m} = 1$) es una extensión finita, abeliana, no ramificada (en ningún primo), maximal con esta propiedad. Además, el mapa de Artin establece un isomorfismo entre $\mathrm{Gal}(\mathcal{H}_K/K)$ y $Cl(K)$ e implica que un ideal primo se parte completamente en $\mathcal{H}_K$ si

y sólo si es principal. Otra propiedad interesante del cuerpo de Hilbert es que *todo* ideal de K es principal en $\mathcal{H}_K$. La demostración de este resultado no es complicada. Artin la redujo a un resultado sobre teoría de grupos. Se puede encontrar en [Mil97]. Este teorema no implica que todo ideal de $\mathcal{H}_K$ sea principal, pues no todo ideal proviene de K. Se puede entonces tomar el cuerpo de Hilbert de $\mathcal{H}_K$, y así sucesivamente, obteniendo una torre de extensiones en la que cada cuerpo es el cuerpo de Hilbert del anterior. Una pregunta interesante es si esta torre es finita, en cuyo caso se tendría una extensión finita de K con número de clases 1. La respuesta es que no siempre es así (ver el artículo de P. Roquette en [CaF67]).

Proposición 4.6.7. *Sea L/K finita y abeliana y $\mathfrak{m}$ un módulo de K. Entonces $L \subset K_{\mathfrak{m}}$ si y sólo si $\mathfrak{f}(L/K)|\mathfrak{m}$.*

Dem. Para una implicación, observemos que en general vale que si $K \subset L \subset M$ entonces $\mathfrak{f}(L/K)|\mathfrak{f}(M/K)$; esto se sigue inmediatamente de la transitividad de la norma. Para la otra implicación, sea $\mathfrak{m}$ un módulo divisible por el conductor, es decir, un módulo admisible. Se tiene entonces que $K^\times W_{\mathfrak{m}} \subset K^\times \mathrm{N}_{L/K}\, \mathbb{I}_L$. Por el Corolario 4.5.6, es obvio que $L \subset K_{\mathfrak{m}}$. □

Corolario 4.6.8. *Toda extensión finita y abeliana de K está contenida en $K_{\mathfrak{m}}$ para algún $\mathfrak{m}$, y el conductor es el mínimo tal $\mathfrak{m}$.*

Analizaremos ahora el caso de $K = \mathbb{Q}$, y veremos un contraejemplo de que el conductor del cuerpo de clases radial no es siempre el módulo.

Proposición 4.6.9. *Sea $m \in \mathbb{Z}$ y $\mathfrak{m} = (m)\infty$. Entonces $\mathbb{Q}_{\mathfrak{m}} = \mathbb{Q}(\zeta_m)$, el cuerpo ciclotómico de las raíces m-ésimas de la unidad.*

Dem. Por el Ejemplo 1.1.13, $\mathbb{Q}(\zeta_m)$ es una extensión finita y abeliana de $\mathbb{Q}$, cuyos primos ramificados dividen a m. Además, el mapa de Artin

$$\psi : I_{\mathbb{Q}}(m) \to \mathrm{Gal}(\mathbb{Q}(\zeta_m)/\mathbb{Q}) \simeq (\mathbb{Z}/m\mathbb{Z})^\times$$

está dado por $\psi(a/b) = [a][b]^{-1}$, donde $(a/b) > 0$ y $(a, b) = (a, m) = (b, m) = 1$. Según el ejemplo 4.1.1, se sigue que el núcleo del mapa de Artin es exactamente $P_{\mathbb{Q},1}(\mathfrak{m})$, y por la unicidad del teorema de existencia, se sigue el resultado. □

Como consecuencia, si tomamos, por ejemplo, $\mathfrak{m} = (2)\infty$, vemos que el cuerpo de clases radial módulo $\mathfrak{m}$ es $\mathbb{Q}(\zeta_2) = \mathbb{Q}$. Luego, el conductor es 1, que es estrictamente más chico que $\mathfrak{m}$.

Corolario 4.6.10 (Teorema de Kronecker-Weber)**.** *Toda extensión finita y abeliana de $\mathbb{Q}$ es ciclotómica (esto es, está contenida en $\mathbb{Q}(\zeta_m)$ para algún m).*

Dem. Todo módulo de $\mathbb{Q}$ es de la forma $\mathfrak{m} = (m)\infty^\epsilon$, con $m \in \mathbb{Z}$ y $\epsilon = 0, 1$. Luego, el conductor de cualquier extensión finita y abeliana L de $\mathbb{Q}$ divide a $(m)\infty$ para algún m. De aquí se sigue que L está contenida en $\mathbb{Q}_{(m)\infty} = \mathbb{Q}(\zeta_m)$. □

Observación 4.6.11. El último teorema se puede probar sin usar teoría de cuerpos de clases. Ver [Mar77] para una guía de la demostración.

Ejercicio 4.6.12. Si m es el mínimo número natural tal que $K \subset \mathbb{Q}(\zeta_m)$, entonces $\mathfrak{f}(K/\mathbb{Q})$ es (m) si $K \subset \mathbb{R}$ y $(m)\infty$ si no.

Capítulo 5

Cohomología de grupos

La cohomología de grupos es una herramienta fundamental tanto en la teoría de cuerpos de clases como en otros contextos. Omitiremos varias demostraciones, principalmente las que son puramente formales; en el caso en que la demostracion ilustre ideas que nos sean útiles para otras cosas, la haremos con mas detalle. Para un tratamiento completo, consultar el libro de Cartan-Eilenberg [CaE56].

5.1. Definiciones

Sean G un grupo, y A un grupo abeliano. Decimos que G actúa (a izquierda) en A si se tiene un morfismo de grupos $G \to \mathrm{Aut}(A)$. Esto es equivalente a decir que se tiene una aplicación

$$G \times A \to A,$$
$$(g, a) \mapsto g.a$$

tal que $(gg').a = g.(g'.a)$ para $g, g' \in G$ y $a \in A$, y tal que $g.(a + a') = g.a + g.a'$ para $g \in G$ y $a, a' \in A$. Esto también es equivalente a darle a A una estructura de $\mathbb{Z}G$-módulo. De ahora en más, nos referiremos a un tal A como un G-módulo. Notemos que dado cualquier grupo abeliano A, podemos considerarlo como un G-módulo vía la acción trivial $g.a = a$ para $g \in G, a \in A$.

Sea A un G-módulo. Notaremos con A^G al subgrupo de A de los invariantes por la acción de G. Es el subgrupo más grande de A sobre el cual G actúa trivialmente, y depende funtorialmente de A. Si B es otro G-módulo, notaremos con $\mathrm{Hom}_G(A, B)$ al grupo de morfismos de G-módulos entre A y B, y con $\mathrm{Hom}_{\mathbb{Z}}(A, B)$ al grupo de morfismos de grupos abelianos. Observemos que a $\mathrm{Hom}_{\mathbb{Z}}(A, B)$ le podemos dar una estructura de G-módulo de la siguiente manera: dado $g \in G$ y $\varphi \in \mathrm{Hom}_{\mathbb{Z}}(A, B)$, $g.\varphi$ es la aplicación $a \mapsto g.\varphi(g^{-1}.a)$, $a \in A$. Es fácil ver que

$$\mathrm{Hom}_G(A, B) = (\mathrm{Hom}_{\mathbb{Z}}(A, B))^G.$$

En particular, si vemos a $\mathbb{Z}$ como G-módulo trivial,

$$\mathrm{Hom}_G(\mathbb{Z}, A) = (\mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z}, A))^G \cong A^G,$$

y esto define un isomorfismo natural entre los funtores $\mathrm{Hom}_G(\mathbb{Z}, -)$ y $(-)^G$.

Diremos que un G-módulo A es *coinducido* si es isomorfo a un G-módulo de la forma

$$\mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z}G, X),$$

donde X es cualquier grupo abeliano (con la acción trivial de G), y que es *relativamente inyectivo* si es un sumando directo de un coinducido.

La categoría de G-módulos consiste entonces de los grupos abelianos en los cuales G actúa, es decir, las representaciones de G (en grupos abelianos); se tienen como es usual las teorías de cohomología y de homología. Dado A un G-módulo, definimos los grupos de cohomología de G con coeficientes en A vía

$$H^q(G, A) = \mathrm{Ext}^q_{\mathbb{Z}G}(\mathbb{Z}, A) \quad \forall\, q \geq 0,$$

donde consideramos a $\mathbb{Z}$ con la acción trivial. Es decir, $H^q(G, -)$ son los funtores derivados a derecha del funtor exacto a izquierda $\mathrm{Hom}_G(\mathbb{Z}, -) \cong (-)^G$. No son sólo una sucesión de funtores; son un "δ-funtor cohomológico": para cada $q \geq 0$ y para cada sucesión exacta corta de G-módulos

$$0 \to A \to B \to C \to 0$$

hay un "morfismo de conexión"

$$\delta : H^q(G, C) \to H^{q+1}(G, A),$$

con el cual se forma la sucesión exacta "larga"

$$... \to H^q(G, B) \to H^q(G, C) \to H^{q+1}(G, A) \to H^{q+1}(G, B) \to ...$$

Además, estos morfismos de conexión dependen funtorialmente en la sucesión exacta corta.

Recordemos la definición de funtor derivado y la forma en que se construyen estos grupos de cohomología: se toma una resolución proyectiva de $\mathbb{Z}$ por G-módulos

$$... \to P_1 \to P_0 \to \mathbb{Z} \to 0$$

y se le aplica $\mathrm{Hom}_G(-, A)$. La cohomología en grado q del complejo obtenido (la imagen cocientada por el núcleo en el lugar q) es entonces $H^q(G, A)$.

Las siguientes propiedades caracterizan al δ-funtor cohomológico $\{H^q(G, -), \delta\}$:

1. $H^0(G, A) = A^G$;
2. $H^q(G, A) = 0$ para $q \geq 1$ si A es un G-módulo inyectivo.

(estas son propiedades generales de los funtores derivados). La segunda propiedad se puede reemplazar por la siguiente.

Proposición 5.1.1. *$H^q(G, A) = 0$ para $q \geq 1$ si A es relativamente inyectivo.*

Dem. Por aditividad, sólo debemos probar esto para el caso en que A sea coinducido, digamos $A = \mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z}G, X)$. Pero si B es un G-módulo, $\mathrm{Hom}_G(B, A) \cong \mathrm{Hom}_{\mathbb{Z}}(B \otimes_{\mathbb{Z}G} \mathbb{Z}G, X) \cong \mathrm{Hom}_{\mathbb{Z}}(B, X)$. Aplicando esto a una resolución proyectiva como antes, se tiene que el q-ésimo grupo de cohomología del complejo obtenido no es otra cosa que $\mathrm{Ext}^q_{\mathbb{Z}}(\mathbb{Z}, X)$, que es 0 para $q \geq 1$ por ser $\mathbb{Z}$ un $\mathbb{Z}$-módulo proyectivo. □

Como podemos tomar cualquier resolución proyectiva de $\mathbb{Z}$, construiremos una en particular, llamada "complejo estándar". Tomamos P_i como el $\mathbb{Z}$-módulo libre con base G^{i+1}, es decir, con base los elementos $(g_0, ..., g_i)$, con $g_0, ..., g_i \in G$. La acción de G es punto a punto: $s.(g_0, ..., g_i) = (sg_0, ..., sg_i)$. El módulo P_i es claramente libre como G-módulo, y *a fortiori* proyectivo. Observemos que $P_0 = \mathbb{Z}G$.

Debemos definir las diferenciales. Para $i \geq 0$, tomamos $d_{i+1} : P_{i+1} \to P_i$ dada por

$$d_{i+1}(g_0, ..., g_{i+1}) = \sum_{j=0}^{i+1} (-1)^j (g_0, ..., g_{j-1}, g_{j+1}, ..., g_{i+1}),$$

y $\epsilon : P_0 \to \mathbb{Z}$ definido por $\epsilon(g) = 1$ para todo $g \in G$. Es decir, $\epsilon(\sum_{g\in G} \lambda_g g) = \sum_{g\in G} \lambda_g$. Es un ejercicio rutinario verificar que efectivamente tenemos una resolución. Aplicando $\mathrm{Hom}_G(-, A)$, obtenemos $\mathrm{Hom}_G(P_i, A)$, que no es otra cosa que el conjunto de funciones $f : G^{i+1} \to A$ tales que $f(sg_0, ..., sg_i) = s.f(g_0, ..., g_i)$ para todos $s, g_0, ..., g_i \in G$ (esto es porque $\mathrm{Hom}_G(P_i, A) = (\mathrm{Hom}_{\mathbb{Z}}(P_i, A))^G$). Pero una tal f está determinada por los valores que toma en elementos de la forma $(1, g_1 g_2, ..., g_1 g_2 ... g_i)$. Es fácil ver que se tiene entonces una biyección entre $\mathrm{Hom}_G(P_i, A)$ y el conjunto de funciones de G^i en A (no necesariamente G-lineales). Bajo esta identificación, la diferencial $\partial_i : \mathrm{Hom}_G(P_{i-1}, A) \to \mathrm{Hom}_G(P_i, A)$ queda (para $i \geq 1$):

$$(\partial_i \varphi)(g_1, ..., g_i) = g_1.\varphi(g_2, ..., g_i) + \sum_{j=1}^{i-1} (-1)^j \varphi(g_1, ..., g_j g_{j+1}, ..., g_i) + (-1)^i \varphi(g_1, ..., g_{i-1}).$$

Análogamente se pueden definir los *grupos de homología* de G como los funtores derivados a izquierda del funtor exacto a derecha $\mathbb{Z} \otimes_G -$ (notamos con $\otimes_G$ al producto tensorial sobre $\mathbb{Z}G$), es decir, si A es un grupo abeliano en el cual G actúa,

$$H_q(G, A) = \mathrm{Tor}_q^{\mathbb{Z}G}(\mathbb{Z}, A).$$

Una observación fácil es que el funtor $\mathbb{Z} \otimes_G -$ es naturalmente isomorfo al funtor $(-)_G$, donde por definición, $A_G = A/I_G A$, siendo I_G el ideal de aumentación de G. Esto es, I_G es el núcleo del morfismo canónico $\epsilon : \mathbb{Z}G \to \mathbb{Z}$. Notemos que I_G está generado por los elementos de la forma $g - 1$ con $g \in G$. La colección de funtores $\{H_q(G, -), \Delta\}$ constituyen un "δ-funtor homológico", con morfismo de conexión Δ, caracterizado por

1. $H_0(G, A) = A_G$;

2. $H_q(G, A) = 0$ para $q \geq 1$ si A es un G-módulo proyectivo.

Como antes, esta última condición se puede reemplazar por la enunciada en la siguiente proposición. Si A y B son dos G-módulos, se le puede dar a $A \otimes_{\mathbb{Z}} B$ una estructura de G-módulo vía $g.(a \otimes b) = g.a \otimes g.b$. No es difícil ver que $(A \otimes_{\mathbb{Z}} B)_G \simeq A \otimes_G B$. Decimos que A es *inducido* si es de la forma $\mathbb{Z}G \otimes_{\mathbb{Z}} X$ para un cierto grupo abeliano X (con la acción trivial de G), y que es *relativamente proyectivo* si es un factor directo de un inducido.

Proposición 5.1.2. *$H_q(G, A) = 0$ para $q \geq 1$ si A es relativamente proyectivo.*

Nos interesará una caracterización del primer grupo de homología de $\mathbb{Z}$ viéndolo como G-módulo trivial para cualquier G. Consideremos la sucesión exacta corta

$$0 \to I_G \to \mathbb{Z}G \to \mathbb{Z} \to 0.$$

Como $\mathbb{Z}G$ es un G-módulo inducido, $H_1(G, \mathbb{Z}G) = 0$. Luego, la sucesión exacta larga de homología da lugar a una sucesión exacta

$$0 \to H_1(G, \mathbb{Z}) \to I_G/I_G^2 \to \mathbb{Z}G/I_G\mathbb{Z}G \to \mathbb{Z} \to 0.$$

La aplicación del medio es la inducida por la inclusión $I_G \hookrightarrow \mathbb{Z}G$ y, por lo tanto, es cero. Esto implica que el morfismo de borde es un isomorfismo

$$H_1(G, \mathbb{Z}) \simeq I_G/I_G^2,$$

y, además, dice que $(\mathbb{Z}G)_G = \mathbb{Z}$, es decir, $\mathbb{Z}$ es el cociente más grande de $\mathbb{Z}G$ en el cual G actúa trivialmente. Aquí, I_G^2 es el subgrupo de $\mathbb{Z}G$ generado por los elementos de la forma $(g-1)(h-1)$ con $g, h \in G$.

Lema 5.1.3. *Sea G' el conmutador de G, y $G^{ab} = G/G'$. Entonces la aplicación $g \mapsto (g-1) + I_G^2$ induce un isomorfismo*

$$G^{ab} \to I_G/I_G^2.$$

Dem. Consideremos la aplicación $g \mapsto (g-1) + I_G^2 : G \to I_G/I_G^2$. Es un morfismo de grupos pues

$$gh - 1 = (g-1)(h-1) + (g-1) + (h-1) \equiv (g-1) + (h-1) (\mathrm{mod}\, I_G^2).$$

Al ser I_G/I_G^2 abeliano, este morfismo se factoriza por G^{ab}.

El grupo I_G es libre, y una base consiste de los elementos de la forma $g-1$ con $g \in G$, $g \neq 1$. Tomemos el morfismo $I_G \to G^{ab}$ dado por mandar $g-1$ a la clase de g. Como

$$(g-1)(h-1) = (gh-1) - (g-1) - (h-1),$$

vemos que $(g-1)(h-1)$ va a parar a 1. Como estos elementos generan I_G^2, el morfismo se factoriza por I_G/I_G^2. Es inmediato ver que las aplicaciones son mutuamente inversas. □

Corolario 5.1.4. *El grupo $H_1(G, \mathbb{Z})$ es canónicamente isomorfo a G^{ab}.*

Volviendo a la cohomología, utilizaremos el complejo estándar para dar una descripción explícita del primer grupo de cohomología $H^1(G,A)$. Por definición, consiste en el grupo de los 1-cociclos cocientado por los 1-cobordes $Z^1(G,A)/B^1(G,A)$. El grupo de 1-cociclos es $Z^1(G,A) = \ker(\partial_2) = \{\varphi : G \to A : \delta_2(\varphi) = 0\}$, es decir, consiste de los *morfismos cruzados*: funciones φ de G en A tales que $\varphi(g_1g_2) = g_1.\varphi(g_2) + \varphi(g_1)$. Por otra parte, un 1-cociclo es un 1-coborde si y sólo si existe un $a \in A^G$ tal que $\varphi(g) = g.a - a$ para todo $g \in G$.

Diremos ahora explícitamente quién es el morfismo de conexión $\delta : H^0(G,C) \to H^1(G,A)$ (para una sucesión exacta corta de G-módulos $0 \to A \to B \to C \to 0$). Sea $c \in H^0(G,C) = C^G$. Lo levantamos a $b \in B$ vía el epimorfismo $B \to C \to 0$, y consideramos $\partial_1(b)$, el 1-coborde de B definido por $\partial_1(b)(g) = g.b - b$. Por el morfismo $B \to C$, $g.b - b$ va a parar a 0 para todo $g \in G$, con lo cual, si vemos a A como un submódulo de B, se tiene que $g.b - b \in A$ para todo $g \in G$. De esta manera, $\partial_1(b)$ se puede ver como un 1-cociclo de A. Se ve entonces que $\delta(c)$ es la clase $\overline{\partial_1(b)}$ de este cociclo en $H^1(G,A)$.

Lema 5.1.5. *Sean M_i $(i \in I)$ G-módulos. Entonces*

$$H^q(G, \prod M_i) \simeq \prod H^q(G, M_i).$$

Dem. Como $H^q(G,A) = \mathrm{Ext}^q_{\mathbb{Z}G}(\mathbb{Z}, A)$, para calcularlo podemos tomar resoluciones inyectivas de A, y calcular la cohomología del complejo obtenido de esta resolución aplicando $(-)^G$. Sea $M_i \to I_i$ una resolución inyectiva de M_i. Como el producto de G-módulos inyectivos es inyectivo, $\prod M_i \to \prod I_i$ es una resolución inyectiva de $\prod M_i$ (aquí debemos usar que el producto de sucesiones exactas de G-módulos da una sucesión exacta). Por lo tanto,

$$H^q(G, \prod M_i) = H^q((\prod I_i)^G) = H^q(\prod (I_i^G)) = \prod H^q(I_i^G) = \prod H^q(G, M_i).$$

En la anteúltima igualdad, usamos el hecho trivial de que la cohomología de un producto de complejos es el producto de las cohomologías. □

Lema 5.1.6. *Sea I un conjunto dirigido, es decir, un conjunto parcialmente ordenado tal que dados dos elementos cualquiera hay uno que es mayor que ambos. Sea M la unión de ciertos G-submódulos M_i, con $M_i \subset M_j$ si $i \leq j$. Entonces*

$$H^q(G, M) = \varinjlim H^q(G, M_i).$$

Dem. Lo dejamos como ejercicio. Se sigue del hecho de que el límite directo de sucesiones exactas es una sucesión exacta, y, por lo tanto, la formación del límite directo conmuta con el pasaje a la cohomología en los complejos. □

5.2. Cambio de grupo

Sean G y G' dos grupos. Sea $f : G' \to G$ un morfismo de grupos y A un G-módulo. Le podemos dar a A una estructura de G'-módulo, vía $g'.a = f(g').a$. Notaremos a este G'-módulo por f^*A. Es claro que $A^G \subset (f^*A)^{G'}$, con lo cual, se tiene definido un morfismo $H^0(G,A) \to H^0(G', f^*A)$. Como $H^0(G,-)$ es un δ-funtor cohomológico universal y $H^0(G', f^*-)$ es un

δ-funtor cohomológico, este morfismo se extiende de manera única a un morfismo de δ-funtores cohomológicos $f_q^* : H^q(G, -) \to H^q(G', f^*-)$.

Podemos hacer algo más general. Sean A un G-módulo y A' un G'-módulo, y sea $\gamma : A \to A'$ un morfismo de grupos abelianos; decimos que γ es *compatible* con f si $\gamma(f(s').a) = s'.\gamma(a)$ para todos $s' \in G'$ y $a \in A$. Esto es lo mismo que decir que γ es un morfismo de G'-módulos $f^*A \to A'$. Induce, por lo tanto, un morfismo de δ-funtores cohomológicos $H^q(G', f^*A) \to H^q(G', A')$, que, componiéndolo con f_q^*, da lugar a un morfismo

$$(f, \gamma)_q^* : H^q(G, A) \to H^q(G', A').$$

Ejemplos:

1. Sea H un subgrupo de G y $f : H \hookrightarrow G$ la inclusión. Se tiene entonces un morfismo para todo $q \geq 0$ llamado *restricción*

   $$\mathrm{Res} : H^q(G, A) \to H^q(H, A),$$

   que en grado 0 coincide con la inclusión $A^G \hookrightarrow A^H$. En términos del complejo estándar, la restricción es efectivamente restringir cociclos de G a cociclos de H.

2. Sea H un subgrupo normal de G y $f = \pi : G \to G/H$ la proyección canónica. Sea $\gamma : A^H \to A$ la inclusión. Entonces γ y f son compatibles y se tiene un morfismo para $q \geq 0$, llamado *inflación*,

   $$\mathrm{Inf} : H^q(G/H, A^H) \to H^q(G, A).$$

Todo lo que hicimos hasta aquí se puede hacer también para homología. En particular, si H es un subgrupo de G, se tiene un morfismo, llamado *correstricción*,

$$\mathrm{Cor} : H_q(H, A) \to H_q(G, A).$$

Veremos ahora un resultado elemental que nos será muy útil. Sean H un subgrupo de G y B un H-módulo. Definimos el G-módulo $B^* = \mathrm{Hom}_H(\mathbb{Z}G, B)$, donde la acción de G está dada por $(s.\varphi)(g) = \varphi(gs)$. Sea $\theta : B^* \to B$ definida por $\theta(\varphi) = \varphi(1)$. Luego, θ y la inclusión $H \hookrightarrow G$ son compatibles, y queda definido un morfismo

$$\theta_q : H^q(G, B^*) \to H^q(H, B)$$

para todo $q \geq 0$.

Lema 5.2.1 (Shapiro)**.** *Los morfismos θ_q son isomorfismos para todo $q \geq 0$.*

Dem. Probaremos que θ_0 es un isomorfismo. Como la familia $\{\theta_q\}$ es un morfismo de δ-funtores cohomológicos, y $H^q(G, (-)^*)$ es universal, se sigue que θ_q es un isomorfismo para todo $q \geq 0$ por propiedades formales de los δ-funtores cohomológicos.

Consideremos entonces $\theta_0 : (B^*)^G \to B^H$. Tenemos que $(B^*)^G = \{\varphi \in \mathrm{Hom}_H(\mathbb{Z}G, B) : \varphi(gs) = \varphi(g) \forall s, g \in G\}$ y $\theta_0(\varphi) = \varphi(1)$ para tal φ. Es un isomorfismo, pues φ está determinada por su valor en 1: $\varphi(s) = \varphi(1s) = \varphi(1)$, y es claro que dado $a \in B^H$, la función φ definida por $\varphi(s) = a$ para $s \in G$ está en $(B^*)^G$. □

Sea A un G-módulo y $t \in G$. Consideramos el morfismo $\varphi_t : G \to G$, $\varphi_t(s) = tst^{-1}$. Notemos con A^t a $\varphi_t^* A$, y consideremos los morfismos inducidos en la cohomología

$$(\varphi_t)_q^* : H^q(G, A) \to H^q(G, A^t).$$

Por otra parte, $\theta : A^t \to A$, $\theta(a) = t^{-1}.a$ da lugar a un isomorfismo de G-módulos, que induce entonces isomorfismos en la cohomología

$$H^q(\theta) : H^q(G, A^t) \to H^q(G, A).$$

Proposición 5.2.2. *El morfismo $(\varphi_t)_q^* \circ H^q(\theta)$ es la identidad para todo $q \geq 0$.*

Dem. Lo probamos en grado 0, y por propiedades de δ-funtores cohomológicos, vale para todo grado. Es muy fácil ver que $(A^t)^G = t.A^G$ y en grado cero las aplicaciones son:

$$t.A^G \xrightarrow{t^{-1}.} A^G \xrightarrow{t.} t.A^G.$$

□

5.3. La sucesión Inflación-Restricción

Teorema 5.3.1. *Sean A un G-módulo y H un subgrupo normal de G. Entonces la sucesión*

$$0 \longrightarrow H^1(G/H, A^H) \xrightarrow{\text{Inf}} H^1(G, A) \xrightarrow{\text{Res}} H^1(H, A)$$

es exacta.

Dem. La demostración consiste en una verificación con los cociclos del complejo estándar. Notemos que si $\overline{f} \in H^q(G/H, A^H)$, con $f : (G/H)^q \to A^H$, y $\pi : G \to G/H$ la proyección canónica, entonces $\text{Inf}(\overline{f}) = \overline{f \circ \pi}$, siendo $f \circ \pi : G^q \to A$ dada por $f \circ \pi(g_1, ..., g_q) = f(\pi(g_1), ..., \pi(g_q))$. Por otra parte, si $\overline{g} \in H^q(G, A)$, con $g : G^q \to A$, entonces $\text{Res}(\overline{g}) = \overline{g|_{H^q}}$. Probemos ahora la exactitud de la sucesión.

- $\text{Res} \circ \text{Inf} = 0$: Sea $\overline{f} \in H^1(G/H, A^H)$. Entonces $\text{Inf}(\overline{f}) = \overline{\varphi}$, donde $\varphi : G \to A$ es el 1-cociclo dado por $\varphi(g) = f(\pi(g))$. Luego, $\text{Res}(\text{Inf}(\overline{f})) = \overline{\varphi|_H}$. Pero $\varphi|_H(h) = \varphi(h) = f(\pi(h)) = f(\pi(1))$ para todo $h \in H$, pues $\pi(h) = \pi(1)$ al ser $1 \in H$. Por otra parte, al ser f un cociclo, $f(\pi(1)) = f(\pi(1)\pi(1)) = \pi(1)f(\pi(1)) + f(\pi(1)) = f(\pi(1)) + f(\pi(1))$; luego, $f(\pi(1)) = 0$.

- Exactitud en $H^1(G/H, A^H)$: Debemos probar que Inf es un monomorfismo. Sea $f : G/H \to A^H$ un 1-cociclo tal que $\text{Inf}(\overline{f}) = 0$. Esto significa que existe $a \in A$ tal que $f(\pi(g)) = ga - a$ para todo $g \in G$. Basta ver que $a \in A^H$, con lo cual, f será un coborde. Sabemos que si $g_1, g_2 \in G$ están en la misma coclase de G/H entonces $f(\pi(g_1)) = f(\pi(g_2))$. Luego, $ga - a = gha - a$ para todo $g \in G$ y $h \in H$. Tomando $g = 1$, obtenemos que $a \in A^H$.

- Exactitud en $H^1(G,A)$: Sea $f: G \to A$ un 1-cociclo tal que $\mathrm{Res}(\overline{f}) = 0$. Esto significa que existe $a \in A$ tal que $f(h) = ha - a$ para todo $h \in H$. Sea s el 1-coborde definido por $s(g) = ga - a$. Entonces $\overline{s} = 0$, con lo cual, $\overline{f} = \overline{f - s}$. Esto nos permite suponer que $f|_H = 0$.

  Al ser f un cociclo, $f(st) = f(s) + s.f(t)$. Si tomamos $t \in H$, obtenemos que f es constante en las coclases de H en G, y si tomamos $s \in H, t \in G$, tenemos que la imagen de f está contenida en A^H. Luego, $\overline{f}$ es la inflación de la clase de un cociclo $G/H \to A^H$.

□

Proposición 5.3.2. *Sean G un grupo y H un subgrupo normal de G. Sea $q \geq 1$ tal que $H^1(H,A) = ... = H^{q-1}(H,A) = 0$. Entonces la sucesión*

$$0 \longrightarrow H^q(G/H, A^H) \xrightarrow{\mathrm{Inf}} H^q(G,A) \xrightarrow{\mathrm{Res}} H^q(H,A)$$

es exacta.

Demostración. Lo hacemos por inducción ("aumento de dimensión"). Para $q = 1$, las hipótesis son vacuas y la afirmación es el teorema anterior. Supongamos que vale para $q-1$, con $q > 1$. Consideramos el G-módulo $A^* = \mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z}G, A)$, con la inyección $A \hookrightarrow A^*$ dada por $a \mapsto (g \mapsto ga)$. Sea $A' = A^*/A$, de manera que tenemos la siguiente sucesión exacta de G-módulos:

$$0 \to A \to A^* \to A' \to 0.$$

Como, en particular, es una sucesión exacta corta de H-módulos, obtenemos la sucesión exacta larga de cohomología:

$$0 \longrightarrow A^H \longrightarrow (A^*)^H \longrightarrow (A')^H \longrightarrow$$

$$H^1(H,A) \longrightarrow H^1(H,A^*) \longrightarrow H^1(H,A') \longrightarrow \cdots$$

$$\cdots \to H^{q-1}(H,A) \to H^{q-1}(H,A^*) \to H^{q-1}(H,A') \longrightarrow$$

$$H^q(H,A) \longrightarrow H^q(H,A^*) \longrightarrow H^q(H,A') \longrightarrow \cdots$$

Al ser $\mathbb{Z}G$ un $\mathbb{Z}H$-módulo libre, tenemos que A^* es $\mathbb{Z}H$-coinducido. Luego, $H^i(H,A^*) = 0$ para todo $i \geq 1$. De la sucesión exacta larga obtenemos entonces que $H^i(H,A') \simeq H^{i+1}(H,A)$ para todo $i \geq 1$. Luego, por hipótesis, $H^i(H,A') = 0$ para $i = 1, ..., q-2$. Consideremos entonces el siguiente diagrama (claramente conmutativo por ser Inf y Res morfismos de δ-funtores cohomológicos):

$$\begin{array}{ccccccc}
0 & \longrightarrow & H^{q-1}(G/H,(A')^H) & \xrightarrow{\mathrm{Inf}} & H^{q-1}(G,A') & \xrightarrow{\mathrm{Res}} & H^{q-1}(H,A') \\
 & & \downarrow{\scriptstyle \delta} & & \downarrow{\scriptstyle \delta} & & \downarrow{\scriptstyle \delta} \\
0 & \longrightarrow & H^q(G/H,A^H) & \xrightarrow{\mathrm{Inf}} & H^q(G,A) & \xrightarrow{\mathrm{Res}} & H^q(H,A).
\end{array}$$

Por lo recién probado y por hipótesis inductiva, sabemos que la fila de arriba es exacta. Probemos que los δ son isomorfismos. Esto demostrará que la fila de abajo también lo es. El tercer δ es un isomorfismo pues es el que aparece en la sucesión exacta larga que tenemos escrita.

Notemos que todavía no usamos que $H^1(H, A) = 0$. Esto nos dice que la sucesión de G/H-módulos

$$0 \to A^H \to (A^*)^H \to (A')^H \to 0$$

es exacta. Aplicando la sucesión exacta larga de cohomología para G/H y observando que $(A^*)^H$ es $\mathbb{Z}[G/H]$-coinducido, tenemos que los morfismos de conexión $\delta : H^i(G/H, (A')^H) \to H^i(G/H, A^H)$ son isomorfismos para $i \geq 1$, con lo cual, el primer δ del diagrama es un isomorfismo.

El segundo $\delta : H^{q-1}(G, A') \to H^q(G, A)$ es un isomorfismo pues $H^i(G, A^*) = 0$ para todo $i \geq 1$ al ser A^* un G-módulo coinducido. □

Recordemos que, si H es un subgrupo de G, tenemos definidos morfismos

$$\mathrm{Res} : H^q(G, A) \to H^q(H, A) \quad q \geq 0,$$
$$\mathrm{Cor} : H_q(H, A) \to H_q(G, A) \quad q \geq 0.$$

Definiremos a continuación la restricción en la homología y la correstricción en la cohomología, en el caso en que $(G : H)$ sea finito.

Para definir $\mathrm{Cor} : H^q(H, A) \to H^q(G, A)$, lo hacemos primero en grado 0. Si $a \in A^H$, sea

$$\mathrm{N}_{G/H}(a) = \sum_s sa,$$

donde la suma se toma sobre un conjunto de representantes de G/H. El resultado no depende de la elección de estos representantes, pues $a \in A^H$, y define un elemento de A^G. Este morfismo se extiende a todo grado por propiedades formales y da lugar a un morfismo de δ-funtores cohomológicos. La definición concreta en grados más altos no nos interesa; para esto, ver [CaE56].

Proposición 5.3.3. *El morfismo* $\mathrm{Cor} \circ \mathrm{Res} : H^q(G, A) \to H^q(G, A)$ *consiste en multiplicar por* $(G : H)$.

Dem. Basta chequearlo en grado 0, y esto es trivial por la definición de la correstricción recién hecha. □

En la homología, definimos $\mathrm{Res} : H_0(G, A) = A_G \to H_0(H, A) = A_H$ de la siguiente manera. Dado $a \in A$, si s, s' están en la misma coclase de G/H entonces $s^{-1}a = s'^{-1}a$ en A_H, y, por lo tanto, podemos definir

$$\mathrm{N}'_{G/H}(a) = \sum_s s^{-1}a,$$

donde la suma se toma sobre un conjunto de representantes de G/H; es fácil ver que no depende de la clase de a en A_G. Como antes, este morfismo se extiende en todo grado y da lugar a un morfismo de δ-funtores homológicos. El siguiente resultado es análogo al caso anterior.

Proposición 5.3.4. *El morfismo* $\mathrm{Cor} \circ \mathrm{Res} : H_q(G, A) \to H_q(G, A)$ *consiste en multiplicar por* $(G : H)$.

5.4. Cohomología de Tate

Proposición 5.4.1. *Sea G un grupo finito. Entonces los G-módulos coinducidos e inducidos son los mismos.*

Dem. Sean X un grupo abeliano y $A = \mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z}G, X)$, $B = \mathbb{Z}G \otimes_{\mathbb{Z}} X$. Es fácil ver que los morfismos de G-módulos $A \to B$, $\varphi \mapsto \sum_{s\in G} s \otimes \varphi(s)$, y $B \to A$, $s \otimes x \mapsto (\sum \mu_g g \mapsto \mu_s x)$ son inversos. □

Sea G un grupo finito, y $\mathrm{N} = \sum_{s\in G} s \in \mathbb{Z}G$. Sea A un G-módulo. Consideramos el endomorfismo $\mathrm{N}_A : A \to A$, "multiplicar por N". Es fácil ver que $I_G A \subset \ker(\mathrm{N}_A)$ y que $\mathrm{Im}(\mathrm{N}_A) \subset A^G$. Luego, N_A induce un morfismo $\mathrm{N}_A^* : H_0(G, A) \to H^0(G, A)$. Definimos

$$\widehat{H}_0(G, A) = \ker(\mathrm{N}_A^*) = \ker(\mathrm{N}_A)/I_G A,$$
$$\widehat{H}^0(G, A) = \mathrm{coker}(\mathrm{N}_A^*) = A^G/\,\mathrm{N}_A(A).$$

Proposición 5.4.2. *Si A es inducido* (*equivalentemente, coinducido*) *entonces $\widehat{H}^0(G, A) = \widehat{H}_0(G, A) = 0$.*

Dem. Digamos que $A = \mathbb{Z}G \otimes_{\mathbb{Z}} X$. Entonces todo elemento de A se escribe de manera única como $\sum_{s\in G} s \otimes x_s$, con $x_s \in X$, y tal elemento queda fijo por la acción de G si y sólo si todos los x_s son iguales a un cierto x. En este caso, el elemento es la norma de $1 \otimes x$ y, por lo tanto, $\widehat{H}^0(G, A) = 0$. La cuenta para $\widehat{H}_0(G, A)$ es muy similar y la omitimos. □

Los *grupos de cohomología de Tate* se definen para $q \in \mathbb{Z}$ por:

$$\begin{aligned}
&\widehat{H}^q(G, A) = H^q(G, A) && \text{si } q \geq 1;\\
&\widehat{H}^0(G, A) = A^G/N_A(A);\\
&\widehat{H}^{-1}(G, A) = \widehat{H}_0(G, A);\\
&\widehat{H}^{-q}(G, A) = H_{q-1}(G, A) && \text{si } q \geq 2.
\end{aligned}$$

El siguiente resultado afirma que se pueden "pegar" las sucesiones exactas largas de homología y cohomología. Su demostración es puramente formal y puede encontrarse en [CaE56].

Teorema 5.4.3. *Sea $0 \to A \to B \to C \to 0$ una sucesión exacta corta de G-módulos. Entonces se tiene una sucesión exacta larga*

$$... \to \widehat{H}^q(G, A) \to \widehat{H}^q(G, B) \to \widehat{H}^q(G, C) \to \widehat{H}^{q+1}(G, A) \to ...$$

Sólo nos interesa el morfismo $\widehat{\delta} : \widehat{H}_0(G, C) \to \widehat{H}^0(G, A)$. Por definición, $\widehat{H}_0(G, C) = \ker(\mathrm{N}_C^*)$. Sea $c \in \ker(\mathrm{N}_C^*) \subset H_0(G, C)$, y sea $b \in H_0(G, B)$ tal que va a parar a c por el morfismo inducido por $B \to C$. Luego, $\mathrm{N}_B^*(b)$ va a parar a 0 en $H^0(G, B)$. Sea $a \in H^0(G, A)$ tal que va a parar a $\mathrm{N}_B^*(b)$. Entonces se define $\widehat{\delta}(c)$ como la clase de a en $\widehat{H}^0(G, A)$.

Los grupos de cohomología de Tate definen un "δ-funtor cohomológico en todas las dimensiones", que se anula en los módulos relativamente proyectivos. De aquí se siguen las siguientes propiedades:

(a) Tomando la sucesión exacta corta $0 \to A \to A^* \to A' \to 0$, al ser A^* coinducido, obtenemos que

$$\widehat{H}^q(G,A) = \widehat{H}^{q-1}(G,A') \quad \forall q \in \mathbb{Z},$$

y esto permite calcular los grupos de cohomología de manera inductiva.

(b) Si consideramos ahora el G-módulo inducido $A_* = \mathbb{Z}G \otimes_{\mathbb{Z}} A$ (mirando aquí A como grupo abeliano), con el epimorfismo de G-módulos $A_* \to A$, $s \otimes x \mapsto s.x$, tenemos que $A = A_*/A'$ es cociente de un inducido, y la sucesión exacta corta $0 \to A' \to A_* \to A \to 0$ nos dice que

$$\widehat{H}^q(G,A) = \widehat{H}^{q+1}(G,A') \quad \forall q \in \mathbb{Z},$$

pudiéndose calcular así los grupos de cohomología inductivamente "para arriba".

Definiremos ahora restricción y correstricción para los grupos de cohomología de Tate. Sea G un grupo finito y H un subgrupo. Para $q \geq 1$, $\mathrm{Res} : \widehat{H}^q(G,A) \to \widehat{H}^q(H,A)$ es el de antes; para $q \geq 2$, $\mathrm{Res} : \widehat{H}^{-q}(G,A) \to \widehat{H}^{-q}(H,A)$ es el de la homología. Consideremos el morfismo $\mathrm{N}'_{G/H} : A_G \to A_H$. Es fácil ver que manda $\widehat{H}_0(G,A)$ en $\widehat{H}_0(H,A)$, induciendo entonces un morfismo en grado -1. En grado 0, la restricción es el morfismo inducido por $A^G \hookrightarrow A^H$. Tenemos así definido $\mathrm{Res} : \widehat{H}^q(G,A) \to \widehat{H}^q(H,A)$ para todo $q \in \mathbb{Z}$. Se puede ver que es un morfismo de δ-funtores cohomológicos mediante un cálculo explícito en los grados del medio. Más aún, es el único morfismo de δ-funtores cohomológicos tal que en grado 0 es el inducido por $A^G \hookrightarrow A^H$.

Para la correstricción, ya tenemos definidos $\mathrm{Cor} : \widehat{H}^q(H,A) \to \widehat{H}^q(G,A)$ para $q \geq 1$, y $\mathrm{Cor} : \widehat{H}^{-q}(H,A) \to \widehat{H}^{-q}(G,A)$ para $q \geq 2$. En grado -1, $\mathrm{Cor} : \widehat{H}_0(H,A) \to \widehat{H}_0(G,A)$ consiste en mandar la clase de un elemento a en $H_0(H,A)$ a la clase del mismo a en $H_0(G,A)$; es fácil ver que esta aplicación está bien definida. En grado 0, consideramos el morfismo $\mathrm{N}_{G/H} : A^H \to A^G$, que induce el morfismo deseado. Se puede ver que $\mathrm{Cor} : \widehat{H}^q(H,A) \to \widehat{H}^q(G,A)$ ($q \in \mathbb{Z}$) es el único morfismo de δ-funtores cohomológicos que en grado -1 coincide con el inducido por $\ker(\mathrm{N}_A^H) \hookrightarrow \ker(\mathrm{N}_A^G)$ (siendo $\mathrm{N}_A^G, \mathrm{N}_A^H$ los morfismos de multiplicación definidos al principio para G y H respectivamente).

Inmediatamente tenemos el siguiente resultado.

Proposición 5.4.4. *El morfismo* $\mathrm{Cor} \circ \mathrm{Res} : \widehat{H}^q(G,A) \to \widehat{H}^q(G,A)$ *consiste en multiplicar por* $(G:H)$ *para todo* $q \in \mathbb{Z}$.

En particular, tomando $H = 1$ (de manera que $\widehat{H}^q(H,A) = 0$ para todo q), podemos probar el siguiente resultado.

Proposición 5.4.5. *Si* $g = (G:1)$ *entonces* $g\widehat{H}^q(G,A) = 0$ *para todo* $q \in \mathbb{Z}$.

Corolario 5.4.6. *Si* A *es un* G*-módulo, finitamente generado como* $\mathbb{Z}$*-módulo, entonces* $\widehat{H}^q(G,A)$ *es un grupo finito para todo* q.

Dem. Por la definición con ciclos y cociclos, es claro que $\widehat{H}^q(G,A)$ es finitamente generado. Al ser de torsión, debe ser un grupo finito. □

Corolario 5.4.7. *Sea S un p-subgrupo de Sylow de G. Entonces para todo $q \in \mathbb{Z}$,* $\mathrm{Res} : \widehat{H}^q(G,A) \to \widehat{H}^q(S,A)$ *es un monomorfismo en la componente p-primaria de $\widehat{H}^q(G,A)$.*

Dem. Escribamos $(G:1) = p^a m$ con $p \nmid m$. Si $x \in \widehat{H}^q(G,A)$ es tal que $\mathrm{Res}(x) = 0$ entonces $\mathrm{Cor} \circ \mathrm{Res}(x) = mx = 0$. Esto implica que $x = 0$. □

Corolario 5.4.8. *Si* $\mathrm{Res}(x) = 0$ *en* $\widehat{H}^q(S,A)$ *para todo subgrupo de Sylow S de G entonces* $x = 0$.

5.5. Productos "cup"

Teorema 5.5.1. *Sea G un grupo finito. Entonces existe una única familia de morfismos*

$$\widehat{H}^p(G,A) \otimes_{\mathbb{Z}} \widehat{H}^q(G,B) \to \widehat{H}^{p+q}(G, A \otimes_{\mathbb{Z}} B)$$

(notados por $(a \otimes b) \mapsto a.b$), definidos para todos los enteros p, q y todos los G-módulos A, B, tal que:

(I) *los morfismos son funtoriales en A y en B;*

(II) *para $p = q = 0$, están inducidos por el producto natural*

$$A^G \otimes_{\mathbb{Z}} B^G \to (A \otimes_{\mathbb{Z}} B)^G;$$

(III) *si $0 \to A \to A' \to A'' \to 0$ es una sucesión exacta de G-módulos, tal que $0 \to A \otimes_{\mathbb{Z}} B \to A' \otimes_{\mathbb{Z}} B \to A'' \otimes_{\mathbb{Z}} B \to 0$ también es exacta, entonces para $a'' \in \widehat{H}^p(G,A'')$ y $b \in \widehat{H}^q(G,B)$ se tiene que*

$$(\delta a'').b = \delta(a''.b) \quad \in \widehat{H}^{p+q+1}(G, A \otimes_{\mathbb{Z}} B);$$

(IV) *si $0 \to B \to B' \to B'' \to 0$ es una sucesión exacta de G-módulos, tal que $0 \to A \otimes_{\mathbb{Z}} B \to A \otimes_{\mathbb{Z}} B' \to A \otimes_{\mathbb{Z}} B'' \to 0$ también es exacta, entonces para $a \in \widehat{H}^p(G,A)$ y $b'' \in \widehat{H}^q(G,B'')$ se tiene que*

$$a.(\delta b'') = (-1)^p \delta(a.b'') \quad \in \widehat{H}^{p+q+1}(G, A \otimes_{\mathbb{Z}} B).$$

Dem. Ver cualquiera de las referencias citadas en este capítulo. □

Las siguientes propiedades se prueban fácilmente de manera formal.

Proposición 5.5.2. (I) $(a.b).c = a.(b.c)$ *(al identificar $(A \otimes_{\mathbb{Z}} B) \otimes_Z C$ con $A \otimes_{\mathbb{Z}} (B \otimes_{\mathbb{Z}} C)$);*

(II) $a.b = (-1)^{\dim(a).\dim(b)} b.a$ *(al identificar $A \otimes_{\mathbb{Z}} B$ con $B \otimes_{\mathbb{Z}} A$);*

(III) $\mathrm{Res}(a.b) = \mathrm{Res}(a).\mathrm{Res}(b)$;

(IV) $\mathrm{Cor}(a.\mathrm{Res}(b)) = \mathrm{Cor}(a).b$.

5.6. Grupos cíclicos y cocientes de Herbrand

Sea G es un grupo cíclico de orden n y s un generador de G. Sean N y D los elementos de $\mathbb{Z}G$ definidos por

$$\mathrm{N} = \sum_{t \in G} t = \sum_{i=0}^{n-1} s^i,$$

$$\mathrm{D} = s - 1.$$

Consideramos el siguiente complejo de cocadenas: $K^i = \mathbb{Z}G$ ($i \in \mathbb{Z}$). La diferencial $d : K^i \to K^{i+1}$ está dada por multiplicación por D (respectivamente por N) si i es par (respectivamente impar). Dado A un G-módulo, sea $K(A) = K \otimes_{\mathbb{Z}G} A$; entonces $K^i(A) = A$ para todo i, y la diferencial $d : K^i(A) \to K^{i+1}(A)$ está dada por multiplicación por D si i es par, y multiplicación por N si i es impar.

Una sucesión exacta corta $0 \to A \to B \to C \to 0$ de G-módulos da lugar a una sucesión exacta corta de complejos

$$0 \to K(A) \to K(B) \to K(C) \to 0,$$

y, por lo tanto, a una sucesión exacta larga de cohomología; en particular, da lugar a un operador de coborde δ.

Proposición 5.6.1. *El funtor cohomológico $\{H^q(K(-)), \delta\}$ es isomorfo al funtor $\{\widehat{H}^q(G, -), \delta\}$.*

Dem. Es claro que $\widehat{H}^0(G, A) = H^0(K(A))$ y que $\widehat{H}^{-1}(G, A) = H^{-1}(K(A))$, y que los operadores de coborde δ que relacionan H^0 con H^{-1} son los mismos. Luego, por la Proposición 5.4.2, $H^q(K(A)) = 0$ ($q = 0, -1$) cuando A es un G-módulo relativamente proyectivo. Como $H^q(K(A))$ sólo depende de la paridad de q, para tal A, $H^q(K(A)) = 0$ para todo $q \in \mathbb{Z}$. Se sigue formalmente que los dos δ-funtores cohomológicos son isomorfos. □

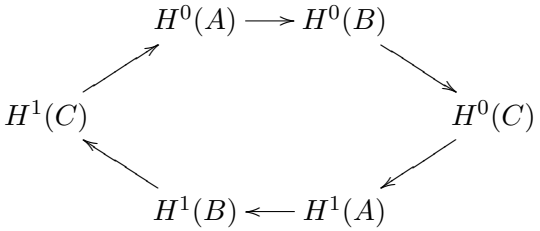
Corolario 5.6.2. *El grupo $\widehat{H}^q(G, A)$ depende sólo de la paridad de q. Más explícitamente,*

$$\widehat{H}^q(G, A) = \ker(\mathrm{D})/\operatorname{Im}(\mathrm{N}) = A^G/\mathrm{N}\,A \quad \text{si } q \equiv 0 (\mathrm{mod}\, 2);$$

$$\widehat{H}^q(G, A) = \ker(\mathrm{N})/\operatorname{Im}(\mathrm{D}) = \ker(\mathrm{N})/I_G A \quad \text{si } q \equiv 1 (\mathrm{mod}\, 2).$$

Observación 5.6.3. Los isomorfismos de arriba *dependen* del generador s de G que estamos tomando. Otra forma de ver esto es la siguiente. Dado s, tomamos un carácter $\chi^s : G \to \mathbb{Q}/\mathbb{Z}$ tal que $\chi^s(s) = 1/n$. La sucesión exacta corta $0 \to \mathbb{Z} \to \mathbb{Q} \to \mathbb{Q}/\mathbb{Z} \to 0$ da lugar a un morfismo de conexión que transforma χ^s en $\delta\chi^s \in H^2(G, \mathbb{Z})$. Entonces el isomorfismo que da la periodicidad $\widehat{H}^q(G, A) \to \widehat{H}^{q+2}(G, A)$ está dado por hacer producto "cup" con $\delta\chi^s$. Una demostración de esto está dada por la fórmula para los productos "cup" dada en [CaE56], p. 252. En particular, en grado 0 es hacer $a \mapsto a.\delta\chi^s$, que claramente depende de s.

A partir de ahora, notaremos con $H^0(A) = \widehat{H}^0(G, A)$ y $H^1(A) = \widehat{H}^1(G, A)$. En virtud de la periodicidad, una sucesión exacta corta de G-módulos $0 \to A \to B \to C \to 0$ da lugar a un hexágono exacto (obtenido luego de pegar la sucesión exacta larga):



Definimos $h_q(A) = (H^q(A) : 1)$ $(q = 0, 1)$ cuando sea finito. Si ambos son finitos, definimos el *cociente de Herbrand* de A como

$$h(A) = h_0(A)/h_1(A).$$

Proposición 5.6.4. *Sea $0 \to A \to B \to C \to 0$ una sucesión exacta corta de G-módulos (G cíclico). Entonces si dos de los tres cocientes de Herbrand $h(A), h(B), h(C)$ están definidos, también lo está el tercero y*

$$h(B) = h(A).h(C).$$

Dem. Miremos el hexágono exacto de arriba. Supongamos, por ejemplo, que los grupos finitos son $H^0(A)$, $H^1(A)$, $H^0(B)$ y $H^1(B)$. Sea M_1 la imagen de $H^0(A)$ en $H^0(B)$, y así sucesivamente alrededor del hexágono según las agujas del reloj. Entonces la sucesión $0 \to M_2 \to H^0(C) \to M_3 \to 0$ es exacta. Además, M_2 y M_3 son grupos finitos: M_2 es la imagen de $H^0(B)$ en $H^0(C)$ y M_3 es un subgrupo de $H^1(A)$. Luego, $H^0(C)$ es finito, y de la misma manera se ve que lo es $H^1(C)$. Si $m_i = (M_i : 1)$, los órdenes de los grupos $H^0(A), ..., H^1(C)$ son respectivamente $m_6m_1, m_1m_2, ..., m_5m_6$, y, por lo tanto, $h(B) = h(A).h(C)$. □

Proposición 5.6.5. *Si A es un G-módulo finito entonces $h(A) = 1$.*

Dem. Consideremos las siguientes sucesiones exactas:

$$0 \longrightarrow A^G \longrightarrow A \xrightarrow{\mathrm{D}} A \longrightarrow A_G \longrightarrow 0,$$

$$0 \longrightarrow H^1(A) \longrightarrow A_G \xrightarrow{\mathrm{N}^*_A} A^G \longrightarrow H^0(A) \longrightarrow 0.$$

De la primera se deduce que A_G y A^G son grupos finitos del mismo orden, y vemos a partir de la segunda que lo mismo sucede con $H^0(A)$ y $H^1(A)$. □

Corolario 5.6.6. *Sean A, B G-módulos y $f : A \to B$ un morfismo de G-módulos con núcleo y conúcleo finitos. Entonces si algunos de los dos cocientes de Herbrand $h(A), h(B)$ está definido, también lo está el otro y son iguales.*

Dem. Supongamos, por ejemplo, que $h(A)$ está definido. Consideremos las sucesiones exactas

$$0 \to \ker(f) \to A \to \mathrm{Im}(f) \to 0,$$

$$0 \to \mathrm{Im}(f) \to B \to \mathrm{coker}(f) \to 0.$$

De las dos proposiciones anteriores, $h(\mathrm{Im}(f))$ está definido y es igual a $h(A)$, y, por lo tanto, $h(B)$ está definido y es igual a $h(A)$. □

Si E es un $\mathbb{R}$-espacio vectorial, decimos que $L \subset E$ es un *retículo maximal* si es un subgrupo de $(E, +)$ generado por una $\mathbb{R}$-base de E. Esto es equivalente a pedir que la aplicación canónica

$$\mathbb{R} \otimes_{\mathbb{Z}} L \to E$$

sea un isomorfismo. La misma definición se puede hacer cambiando $\mathbb{R}$ por $\mathbb{Q}$.

Proposición 5.6.7. *Sea $G \to \mathrm{End}(E)$ una representación de G, donde E es un $\mathbb{R}$-espacio vectorial de dimensión finita (esto es, E es un $\mathbb{R}G$-módulo). Sean $L, L' \subset E$ dos retículos maximales de E invariantes por la acción de G. Entonces si alguno de los dos $h(L), h(L')$ está definido, también lo está el otro y son iguales.*

Dem. Necesitaremos el siguiente resultado técnico.

Lema 5.6.8. *Sea G un grupo finito y k un cuerpo infinito. Sean M, M' dos kG-módulos de dimensión finita sobre k tales que $M \otimes_k \Omega$ y $M' \otimes_k \Omega$ son isomorfos como ΩG-módulos, para un cierto cuerpo $\Omega \supset k$. Entonces M y M' son isomorfos como kG-módulos.*

Dem. La aplicación $\varphi \otimes \omega \mapsto \varphi \otimes (.\omega)$ (donde $(.\omega) : \Omega \to \Omega$ es multiplicación por ω) induce un isomorfismo de Ω-espacios vectoriales

$$\mathrm{Hom}_{kG}(M, M') \otimes_k \Omega \simeq \mathrm{Hom}_{\Omega G}(M \otimes_k \Omega, M' \otimes_k \Omega).$$

Para probar esto, mostraremos primero que la aplicación (definida de igual manera)

$$\mathrm{Hom}_k(M, M') \otimes_k \Omega \to \mathrm{Hom}_{\Omega}(M \otimes_k \Omega, M' \otimes_k \Omega)$$

es un isomorfismo de Ω-espacios vectoriales. Es fácil ver que ambos tienen la misma dimensión; probemos, por lo tanto, que es inyectiva. Sean $f : M \to M'$ k-lineal y $\omega \in \Omega$ tales que $f \otimes (.\omega) : M \otimes_k \Omega \to M' \otimes_k \Omega$ es el morfismo nulo. Entonces $f(m) \otimes (\omega\tau) = 0$ en $M' \otimes_k \Omega$ para todos $m \in M$, $\tau \in \Omega$. Si f no es el morfismo nulo, existe $m \in M$ tal que $f(m) \neq 0$. Como en los espacios vectoriales el producto tensorial de dos elementos es 0 si y sólo si alguno de ellos lo es, se sigue que $\omega\tau = 0$ para todo $\tau \in \Omega$. Por lo tanto, $\omega = 0$, y esto prueba que la aplicación es entonces un isomorfismo. Dejamos como ejercicio probar que los morfismos G-lineales de cada lado se corresponden, es decir, que f es G-lineal si y sólo si $f \otimes (.\omega)$ es G-lineal para todo $\omega \in \Omega$.

Como M y M' son isomorfos como kG-módulos, tienen la misma dimensión sobre k. De esta manera, si elegimos bases de M y M', tiene sentido hablar del *determinante* de un elemento

de $\mathrm{Hom}_{kG}(M, M')$, o de $\mathrm{Hom}_{\Omega G}(M \otimes_k \Omega, M' \otimes_k \Omega)$, y que $\det(f) = \det(f \otimes 1)$ si $f \in \mathrm{Hom}_{kG}(M, M')$.

Por el isomorfismo de recién, se sigue que si φ_i es una k-base para $\mathrm{Hom}_{kG}(M, M')$, también lo son los elementos $\varphi_i \otimes 1$ de $\mathrm{Hom}_{\Omega G}(M \otimes_k \Omega, M' \otimes_k \Omega)$. Como $M \otimes_k \Omega$ y $M' \otimes_k \Omega$ son ΩG-isomorfos, existen $\omega_i \in \Omega$ tales que $\sum_i \omega_i(\varphi_i \otimes 1)$ es inversible. Luego, su determinante es no nulo. De esta manera, el polinomio

$$F(t) = \det(\sum_i t_i(\varphi_i \otimes 1)) \in k[t_1, ..., t_m]$$

no es idénticamente cero, ya que $F((\omega_i)) \neq 0$. Como k es infinito, existen $b_i \in k$ tales que $F((b_i)) \neq 0$. Entonces $\sum_i b_i\varphi_i$ es un kG-isomorfismo entre M y M'. □

Para demostrar la proposición, sean $M = L \otimes_{\mathbb{Z}} \mathbb{Q}$ y $M' = L' \otimes_{\mathbb{Z}} \mathbb{Q}$. Entonces $M \otimes_{\mathbb{Q}} \mathbb{R}$ es isomorfo a $M' \otimes_{\mathbb{Q}} \mathbb{R}$ como $\mathbb{R}G$-módulo. Luego, existe un $\mathbb{Q}G$-isomorfismo $\varphi : L \otimes_{\mathbb{Z}} \mathbb{Q} \to L' \otimes_{\mathbb{Z}} \mathbb{Q}$, y L se aplica inyectivamente por φ en un retículo contenido en $(1/N)L'$ para algún $N \in \mathbb{N}$. Para ver esto último, usamos que $\varphi(L')$ y L son retículos maximales del mismo $\mathbb{Q}$-espacio vectorial; escribimos los elementos de una base de $\varphi(L')$ en términos de una base de L y tomamos N un denominador común de los coeficientes.

Si tomamos entonces $f = N.\varphi$, se sigue que f aplica L inyectivamente en L'; como ambos son grupos abelianos libres del mismo rango (finito), el conúcleo de f es finito. El resultado que queremos probar se sigue entonces del corolario 5.2.

□

5.7. Teorema de Tate

A lo largo de esta sección, todos los grupos de cohomología serán los de Tate y, por lo tanto, escribiremos H^q en lugar de $\widehat{H}^q$ para $q \in \mathbb{Z}$.

Teorema 5.7.1. *Sean G un grupo finito y A un G-módulo. Si $H^1(H, A) = H^2(H, A) = 0$ para todo subgrupo H de G entonces $H^q(G, A) = 0$ para todo $q \in \mathbb{Z}$.*

Dem. Si G es cíclico se sigue de la periodicidad de la cohomología. Supongamos que G es soluble; probaremos el teorema en esta situación por inducción en el orden de G.

Al ser G soluble, contiene un subgrupo propio (a menos que $G = 1$) normal H tal que G/H es cíclico. Como el orden de H es menor que el orden de G, por hipótesis inductiva se tiene que $H^q(H, A) = 0$ para todo $q \in \mathbb{Z}$. Por la Proposición 5.3.2, tenemos una sucesión exacta

$$0 \longrightarrow H^q(G/H, A^H) \xrightarrow{\mathrm{Inf}} H^q(G, A) \xrightarrow{\mathrm{Res}} H^q(H, A)$$

para cada $q \geq 1$. Como $H^1(G, A) = H^2(G, A) = 0$, se tiene que

$$H^1(G/H, A^H) = H^2(G/H, A^H) = 0.$$

Al ser G/H cíclico, obtenemos que $H^q(G/H, A^H) = 0$ para todo $q \geq 1$. Por lo tanto, $H^q(G, A) = 0$ para todo $q \geq 1$. Veamos que $H^0(G, A) = 0$. Sea $a \in A^G$; como $H^0(G/H, A^H)$

$= 0$, existe $b \in A^H$ tal que $\mathrm{N}_{G/H}(b) = a$, y como $H^0(H, A) = 0$, existe $c \in A$ tal que $\mathrm{N}_H(c) = b$. Entonces $\mathrm{N}_G(c) = \mathrm{N}_{G/H}(\mathrm{N}_H(c)) = a$, y, por lo tanto, $H^0(G, A) = 0$.

Sean $A^* = \mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z}G, A)$ y $A' = A/A^*$; tenemos la sucesión exacta corta

$$0 \to A \to A^* \to A' \to 0.$$

Como A^* es $\mathbb{Z}H$-coinducido para todo subgrupo H, tenemos que $H^q(H, A^*) = 0$ para todo $q \in \mathbb{Z}$ y para todo H (Proposiciones 5.4.1 y 5.4.2). Por lo tanto, $H^q(H, A) = H^{q-1}(H, A')$ para todo q. Entonces A' satisface las hipótesis del teorema, y luego, por lo probado recién, $H^q(G, A') = 0$ para todo $q \geq 0$. Además, la sucesión exacta implica que $H^{-1}(G, A) = H^0(G, A') = 0$. Repitiendo el argumento se sigue que $H^q(G, A) = 0$ para todo $q \in \mathbb{Z}$.

Sea ahora G un grupo finito arbitrario. Si G y A satisfacen las hipótesis del teorema, también las satisfacen G_p y A para G_p un p-subgrupo de Sylow de G. Como un p-grupo finito es soluble, se tiene que $H^q(G_p, A) = 0$ para todo $q \in \mathbb{Z}$ y para todo primo p. Por el Corolario 5.4.6, la componente p-primaria de $H^q(G, A)$ es 0 para todo p y todo q, y, por lo tanto, $H^q(G, A) = 0$ para todo $q \in \mathbb{Z}$. □

Teorema 5.7.2 (Tate)**.** *Sean G un grupo finito y A un G-módulo. Supongamos que para todo subgrupo H de G se cumple que*

(a) $H^1(H, A) = 0$ *y*

(b) $H^2(H, A)$ *es cíclico de orden* $(H : 1)$.

Entonces para todo q existe un isomorfismo

$$H^q(G, \mathbb{Z}) \to H^{q+2}(G, A)$$

que depende sólo de la elección de un generador de $H^2(G, A)$.

Dem. Sea γ un generador de $H^2(G, A)$. Como $\mathrm{Cor} \circ \mathrm{Res} : H^q(G, A) \to H^q(H, A)$ es multiplicar por $(G : H)$, $\mathrm{Res}(\gamma)$ genera $H^2(H, A)$ para cualquier subgrupo H.

Sea $\varphi : G \times G \to A$ un cociclo que represente a γ. Sea $A(\varphi)$ la suma directa de A con el grupo abeliano libre con base dada por los símbolos x_σ, uno para cada $\sigma \in G$, $\sigma \neq 1$. Extendemos la acción de G en A a una acción en $A(\varphi)$ de la siguiente manera:

$$\sigma x_\tau = x_{\sigma\tau} - x_\sigma + \varphi(\sigma, \tau).$$

Utilizamos el símbolo x_1 para denotar $\varphi(1, 1)$. Chequeemos que es efectivamente una acción. Por un lado,

$$(\rho\sigma)x_\tau = x_{\rho\sigma\tau} - x_{\rho\sigma} + \varphi(\rho\sigma, \tau),$$

mientras que

$$\rho(\sigma x_\tau) = \rho(x_{\sigma\tau} - x_\sigma + \varphi(\sigma, \tau)) =$$
$$= x_{\rho\sigma\tau} - x_\rho + \varphi(\rho, \sigma\tau) - (x_{\rho\sigma} - x_\rho + \varphi(\rho, \sigma)) + \rho\varphi(\sigma, \tau).$$

Las dos expresiones coinciden pues, al ser φ un cociclo, se cumple que

$$\rho\varphi(\sigma, \tau) + \varphi(\rho, \sigma\tau) = \varphi(\rho\sigma, \tau) + \varphi(\rho, \sigma)$$

(fijarse quién es el morfismo de borde). Notemos que φ es el coborde del 1-cociclo $\sigma \mapsto x_\sigma$, de manera que γ va a parar a 0 bajo la aplicación $H^2(G, A) \to H^2(G, A(\varphi))$.

Probaremos a continuación que las hipótesis del teorema implican que $H^1(H, A(\varphi)) = H^2(H, A(\varphi)) = 0$ para todo subgrupo H. Tomemos la sucesión exacta corta

$$0 \to I_G \to \mathbb{Z}G \to \mathbb{Z} \to 0.$$

Aquí, I_G es el grupo abeliano libre con base los elementos $\sigma - 1$ con $\sigma \in G$, $\sigma \neq 1$. Como $\mathbb{Z}G$ es un H-módulo inducido, $H^q(H, \mathbb{Z}G) = 0$ para todo $q \in \mathbb{Z}$. Por lo tanto,

$$H^1(H, I_G) = H^0(H, \mathbb{Z}) = \mathbb{Z}/(H : 1)\mathbb{Z},$$

$$H^2(H, I_G) = H^1(H, \mathbb{Z}) = 0.$$

En el último paso usamos que $H^1(H, \mathbb{Z}) = \mathrm{Hom}(H, \mathbb{Z})$, y como H es un grupo de torsión, no hay morfismos no nulos.

Sea $\alpha : A(\varphi) \to \mathbb{Z}G$ el morfismo aditivo dado por $\alpha(a) = 0$ si $a \in A$ y $\alpha(x_\sigma) = \sigma - 1$. Entonces

$$0 \longrightarrow A \longrightarrow A(\varphi) \xrightarrow{\alpha} I_G \longrightarrow 0$$

es una sucesión exacta de G-módulos. Como $H^1(H, A) = 0 = H^2(H, I_G)$, la sucesión larga de cohomología da lugar a la sucesión exacta

$$0 \to H^1(H, A(\varphi)) \to H^1(H, I_G) \to H^2(H, A) \to H^2(H, A(\varphi)) \to 0.$$

El último morfismo es el morfismo nulo, pues $H^2(H, A)$ está generado por $\mathrm{Res}(\gamma)$, y el morfismo lo manda a la restricción de la imagen de γ en $H^2(G, A(\varphi))$, que es 0. Luego, $H^2(H, A(\varphi)) = 0$, y, además, $H^1(H, I_G) \to H^2(H, A)$ es suryectiva; como ambos grupos tienen el mismo orden, esta aplicación debe ser un isomorfismo. Por ser inyectiva, se tiene que $H^1(H, A(\varphi)) = 0$. El teorema anterior implica entonces que $H^q(G, A(\varphi)) = 0$ para todo $q \in \mathbb{Z}$. Considerando las dos sucesiones exactas cortas y el hecho de que $H^q(G, \mathbb{Z}G) = 0$ para todo $q \in \mathbb{Z}$, se obtiene un isomorfismo

$$H^q(G, \mathbb{Z}) \to H^{q+2}(G, A).$$

□

Observación 5.7.3. Se puede ver que el isomorfismo construido consiste en hacer producto "cup" contra el generador γ.

5.8. Cohomología de Galois

En esta sección no haremos todas las demostraciones. Se pueden consultar en [Ser79] y en el Capítulo III de [CaF67].

Sea L/K una extensión de Galois de cuerpos (no necesariamente finita). Su grupo de Galois es un grupo topológico profinito, igual al límite inverso de los grupos $\mathrm{Gal}(K'/K)$, donde K' recorre las subextensiones finitas de Galois de L/K.

Sea G un grupo profinito. Dado M un G-módulo, decimos que M es un G-módulo *topológico* si la aplicación $G \times M \to M$ es continua, donde M tiene la topología discreta. En este caso, definimos los grupos de cohomología *continuos* vía

$$H^q(G, M) = \varinjlim H^q(G/H, A^H),$$

donde H recorre los subgrupos abiertos y normales de G. El límite directo se toma respecto de los morfismos de inflación. Las propiedades de $H^q(G, M)$ son similares a las de los grupos de cohomología usual (y no cambiaremos la notación, aclarando en cada caso si es necesario): son un funtor, y se pueden calcular de la misma manera usando el complejo estándar, pero utilizando funciones continuas $G^q \to M$.

Sea ahora L/K una extensión de Galois (finita o infinita), con grupo de Galois G. Escribimos $H^q(L/K)$ en lugar de $H^q(G, L^\times)$. El grupo $H^2(L/K)$ se llama *grupo de Brauer* de L/K, denotado por $\mathrm{Br}(L/K)$.

Se puede ver que si L es isomorfo a L' entonces $H^q(L/K)$ y $H^q(L'/K)$ son isomorfos *canónicamente*. Esto se aplica en el caso particular en que $L = K^s$ es una clausura algebraica separable de K. El grupo $H^2(K^s/K)$ se llama *grupo de Brauer* de K, y lo denotamos por $\mathrm{Br}(K)$. Por definición de la topología de $\mathrm{Gal}(K^s/K)$, es el límite directo de los $H^2(L/K)$, donde L/K recorre las extensiones finitas de Galois contenidas en K^s.

Proposición 5.8.1. *Sea K'/K una extensión de Galois que contiene a la extensión de Galois L/K. Entonces hay una sucesión exacta*

$$0 \to \mathrm{Br}(L/K) \to \mathrm{Br}(K'/K) \to \mathrm{Br}(K'/L).$$

En el caso de extensiones finitas, esta sucesión no es otra cosa que la de la Proposición 5.3.2, con $q = 2$ (inflación-restricción), mientras que el caso infinito se deduce pasando al límite. Llamaremos Res también a la aplicación $\mathrm{Br}(K'/K) \to \mathrm{Br}(K'/L)$. Tomando K' como una clausura separable de K que contenga a L, obtenemos el siguiente resultado.

Corolario 5.8.2. *Sea L/K una extensión de Galois. Entonces hay una sucesión exacta*

$$0 \to \mathrm{Br}(L/K) \to \mathrm{Br}(K) \to \mathrm{Br}(L).$$

A la aplicación $\mathrm{Br}(K) \to \mathrm{Br}(L)$ la llamaremos $\mathrm{Res}_{K/L}$. Decimos que un elemento $\alpha \in \mathrm{Br}(K)$ *se parte* por una extensión finita de Galois L/K si está en el núcleo de $\mathrm{Res}_{K/L}$. Por el último corolario, esto equivale a decir que $\alpha \in \mathrm{Br}(L/K)$, viendo a éste como subgrupo de $\mathrm{Br}(K)$.

El siguiente resultado dice que el límite directo que forma el grupo de Brauer es, de hecho, una unión.

Proposición 5.8.3. *Para todo cuerpo K se tiene que $\mathrm{Br}(K) = \bigcup \mathrm{Br}(L/K)$, donde L/K recorre las extensiones finitas de Galois contenidas en K^s.*

Finalmente, necesitaremos un resultado sobre la acción del grupo de Galois de una extensión en el cuerpo de arriba.

Teorema 5.8.4. *Sea L/K una extensión finita de Galois, con grupo de Galois G. Entonces $H^1(G, L^\times) = 0$.*

Dem. Sea $s \mapsto a_s$ un 1-cociclo no nulo. Si $c \in L$, sea

$$b = \sum_{t \in G} a_t.t(c).$$

Por el teorema de independencia de caracteres ([Lan93], VI, §4), podemos elegir c tal que $b \neq 0$. Por otra parte,

$$s(b) = \sum_t s(a_t).st(c) = \sum_t a_s^{-1} a_{st}.st(c) = a_s^{-1} b,$$

y esto prueba que a_s es un coborde. □

Corolario 5.8.5 (Teorema 90 de Hilbert)**.** *Si G es cíclico, s es un generador y $x \in L^\times$ tiene norma 1 entonces existe $y \in L^\times$ tal que $x = y/s(y)$.*

Capítulo 6

Teoría local de cuerpos de clases

Enumeraremos aquí los resultados sobre la teoría local de cuerpos de clases que necesitaremos. Para una exposición detallada sobre este tema, ver el articulo de J.-P. Serre en [CaF67], o su libro [Ser79]. En cierto sentido, la teoría local es más sencilla, pues en los cuerpos locales hay un sólo primo a considerar.

Demostraremos los Teoremas 4.5.1-4.5.4 a partir de los resultados de este capítulo. Más específicamente, para probar la existencia del mapa de Artin $\phi_{L/K} : \mathbb{I}_K \to \mathrm{Gal}(L/K)$ (a partir de ahora llamado mapa de Artin *global*), utilizaremos que ya existen los llamados mapas de Artin *locales*.

Sea L/K una extensión finita de Galois de cuerpos de números. Entonces las extensiones locales L_w/K_v también son finitas de Galois y son todas isomorfas entre sí (sobre K_v). Denotaremos por L^v a cualquiera de ellas, y por $G^v = \mathrm{Gal}(L^v/K_v)$ al grupo de Galois local. Recordemos que $\mathrm{Gal}(L_w/K_v)$ se identifica con el grupo de descomposición de w, con lo cual, G^v es alguno de estos grupos. En el caso en que la extensión L/K sea abeliana, este grupo es único, es decir, no depende del w elegido sobre v.

Supongamos que se cumple la ley de reciprocidad para L/K abeliana finita. Sea $\phi_{L/K} : \mathbb{I}_K \to G = \mathrm{Gal}(L/K)$ el mapa de Artin global. Para cada primo v de K, tenemos definidos dos morfismos $i_v : K_v^\times \to \mathbb{I}_K$ y $j_v : \mathbb{I}_K \to K_v^\times$; i_v es la inclusión que manda x en el idèle cuya coordenada v es x y las otras coordenadas son 1 y j_v es la proyección en la componente v. Sea $\phi_v = \phi_{L/K} \circ i_v : K_v^\times \to G$.

Proposición. *Sea $\mathcal{M}$ una subextensión de L^v/K_v, $K_v \subset \mathcal{M} \subset L^v$. Entonces*

$$\phi_v(\mathrm{N}_{\mathcal{M}/K_v} \mathcal{M}^\times) \subset \mathrm{Gal}(L^v/\mathcal{M})$$

(viendo a este último como subgrupo de G). En particular, $\phi_v(K_v^\times) \subset G^v$ y

$$\phi_v(\mathrm{N}_{L^v/K_v}(L^v)^\times) = 1.$$

Dem. Sea $M = L \cap \mathcal{M}$, que no es otra cosa que el cuerpo fijo en L/K del subgrupo de $\mathrm{Gal}(L/K)$ que le corresponde a $\mathrm{Gal}(L^v/\mathcal{M})$ vía la identificación del grupo de Galois local con el grupo de descomposición. Entonces $\mathrm{Gal}(L/M)$ se identifica con $\mathrm{Gal}(L^v/\mathcal{M})$. Dejamos

como ejercicio probar que $\mathcal{M} = M_w$ para w un primo de M sobre v. Consideremos el siguiente diagrama conmutativo:

$$\begin{array}{ccc} \mathcal{M} = M_w & \xrightarrow{i_w} & \mathbb{I}_M \\ \Big\downarrow{\scriptstyle \mathrm{N}_{\mathcal{M}/K_v}} & & \Big\downarrow{\scriptstyle \mathrm{N}_{M/K}} \\ K_v & \xrightarrow{i_v} & \mathbb{I}_K. \end{array}$$

Por el Corolario 4.4.7 con $M = K'$, tenemos que $\phi_v(\mathrm{N}_{\mathcal{M}/K_v}\,\mathcal{M}^\times) \subset \phi_{L/K}(\mathrm{N}_{M/K}\,\mathbb{I}_M) \subset \mathrm{Gal}(L/M)$, que se identifica con $\mathrm{Gal}(L^v/\mathcal{M})$. □

Al morfismo ϕ_v lo llamamos *mapa de Artin local*. Sea $x \in \mathbb{I}_K$. Entonces

$$x = \lim_S \prod_{v \in S} i_v(x_v),$$

donde el límite se toma sobre todos los conjuntos finitos de primos S. Como $\phi_{L/K}$ es continuo, tenemos que

$$\phi_{L/K}(x) = \lim_S \prod_{v \in S} \phi_v(x_v).$$

Pero hay sólo finitos v para los cuales $\phi_v(x_v) \neq 1$: si v no ramifica y x_v es una v-unidad entonces es una norma de L^v/K_v (6.2.8) y, por lo tanto, $\phi_v(x_v) = 1$ por la proposición anterior. Por lo tanto, podemos escribir

$$\phi_{L/K}(x) = \prod_v \phi_v(x_v).$$

De esta manera, conocer el mapa de Artin global es equivalente a conocer todos los mapas de Artin locales. Para construir entonces el mapa de Artin global, tomaremos los mapas locales ϕ_v obtenidos en la teoría local de cuerpos de clases y probaremos que $\prod_v \phi_v$ satisface las propiedades que caracterizan a $\phi_{L/K}$ (es decir, es un morfismo continuo $\mathbb{I}_K \to \mathrm{Gal}(L/K)$ que se anula en $K^\times$ y tal que $\phi_{L/K}(x) = \psi_{L/K}(\mathrm{id}(x))$ si $x \in \mathbb{I}_{K,S}$, donde S es el conjunto de primos ramificados).

6.1. Mapa de reciprocidad

Sea L/K una extensión finita de Galois de cuerpos locales no arquimedeanos, con grupo de Galois $G = \mathrm{Gal}(L/K)$ de orden n. Entonces existe un morfismo $\phi_{L/K} : K^\times \to G^{ab}$ (el abelianizado de G), llamado el *mapa de reciprocidad local* o *norm residue symbol* que define un isomorfismo $\phi_{L/K} : K^\times/\mathrm{N}_{L/K}\,L^\times \to G^{ab}$. Estaremos interesados principalmente en el caso L/K abeliana, con lo cual, $G^{ab} = G$. En el caso en que los cuerpos sean arquimedeanos, también existe tal $\phi_{L/K}$; el único caso no trivial es $K = \mathbb{R}$ y $L = \mathbb{C}$, en cuyo caso $\phi_{\mathbb{C}/\mathbb{R}} : \mathbb{R}^\times \to \mathrm{Gal}(\mathbb{C}/\mathbb{R})$ está dado por $x \mapsto 1$ si $x > 0$ y $x \mapsto c$ si $x < 0$ (donde c es la conjugación compleja). Supondremos que los cuerpos siempre son no arquimedeanos, enunciando los resultados que sean válidos para los arquimedeanos cuando sea necesario.

Dado $a \in K^\times$, notamos con $\overline{a}$ su clase en $K^\times / \mathrm{N}_{L/K} L^\times$, y escribimos $(a, L/K) = \phi_{L/K}(\overline{a})$. La razón del nombre *norm residue symbol* es que dice si $a \in K^\times$ es una norma de $L^\times$ o no; es decir, $(a, L/K) = 1$ si y sólo si a es una norma de $L^\times$.

El morfismo $(\alpha, L/K)$ satisface la siguiente propiedad de compatibilidad: si $K \subset L' \subset L$ es una torre de extensiones de Galois con $G = \mathrm{Gal}(L/K)$ y $H = Gal(L/L')$, entonces $(\alpha, L/K)\,|_{L'} = (\alpha, L'/K)$. Esto permite definir $\phi_K : K^\times \to \mathrm{Gal}(K^{ab}/K)$.

La otra condición de compatibilidad que cumple es la siguiente: sea K'/K una extensión finita y separable. Se tiene un morfismo natural $i : \mathrm{Gal}(K'^{ab}/K') \to \mathrm{Gal}(K^{ab}/K)$, y el siguiente diagrama es conmutativo:

$$\begin{array}{ccc} K'^\times & \xrightarrow{\phi_{K'}} & \mathrm{Gal}(K'^{ab}/K') \\ \downarrow{\scriptstyle \mathrm{N}_{K'/K}} & & \downarrow{\scriptstyle i} \\ K^\times & \xrightarrow{\phi_K} & \mathrm{Gal}(K^{ab}/K). \end{array}$$

Como consecuencia, si L/K es una extensión finita y abeliana, el siguiente diagrama conmuta:

$$\begin{array}{ccc} K'^\times & \xrightarrow{\phi_{LK'/K'}} & \mathrm{Gal}(LK'/K') \\ \downarrow{\scriptstyle \mathrm{N}_{K'/K}} & & \downarrow{\scriptstyle i} \\ K^\times & \xrightarrow{\phi_{L/K}} & \mathrm{Gal}(L/K). \end{array}$$

Utilizando el isomorfismo del mapa de reciprocidad (y el hecho de que el resultado es trivial para cuerpos locales arquimedeanos), podemos probar el siguiente resultado.

Proposición 6.1.1. *Sea L/K una extensión finita Galois de cuerpos locales. Entonces $\mathrm{N}_{L/K} L^\times$ tiene índice finito en $K^\times$.*

6.2. Cohomología

En esta sección, un cuerpo local será un cuerpo local no arquimedeano.

Teorema 6.2.1. *Existe un isomorfismo $\mathrm{inv}_K : \mathrm{Br}(K) \to \mathbb{Q}/\mathbb{Z}$.*

Para no tener que distinguir cuando estemos en la teoría global, en el caso en que K sea arquimedeano, hay dos posibilidades: si $K = \mathbb{R}$, $\mathrm{Br}(\mathbb{R})$ es un grupo de orden 2 y se tiene una aplicación $\mathrm{inv}_{\mathbb{R}} : \mathrm{Br}(\mathbb{R}) \to \mathbb{Q}/\mathbb{Z}$, cuya imagen es $\{0, 1/2\}$, y en el caso en que $K = \mathbb{C}$, $\mathrm{Br}(\mathbb{C}) = 0$ e $\mathrm{inv}_{\mathbb{C}}$ es el morfismo nulo.

Proposición 6.2.2. *Sea L/K una extensión finita de grado n. Entonces el siguiente diagrama es conmutativo:*

$$\begin{array}{ccccccc} 0 & \longrightarrow & \mathrm{Br}(L/K) & \longrightarrow & \mathrm{Br}(K) & \xrightarrow{\mathrm{Res}_{K/L}} & \mathrm{Br}(L) \\ & & & & \downarrow{\scriptstyle \mathrm{inv}_K} & & \downarrow{\scriptstyle \mathrm{inv}_L} \\ 0 & \longrightarrow & \frac{1}{n}\mathbb{Z}/\mathbb{Z} & \longrightarrow & \mathbb{Q}/\mathbb{Z} & \xrightarrow{.n} & \mathbb{Q}/\mathbb{Z}, \end{array}$$

donde $\mathrm{Res}_{K/L}$ *es la aplicación del Corolario 5.8.2. Por lo tanto, se tiene un isomorfismo*

$$\mathrm{inv}_{L/K} : \mathrm{Br}(L/K) \to \frac{1}{n}\mathbb{Z}/\mathbb{Z}.$$

El elemento $u_{L/K} \in \mathrm{Br}(L/K)$ que se corresponda con $\frac{1}{n}$ vía $\mathrm{inv}_{L/K}$ se llama la *clase fundamental* de L/K. Es un generador del grupo $\mathrm{Br}(L/K)$.

Corolario 6.2.3. *Sea L/K una extensión finita de grado n. Entonces $\mathrm{Br}(L/K)$ es cíclico de orden n.*

Proposición 6.2.4. *Sea $L' \supset L \supset K$ una torre de extensiones finitas de Galois. Entonces*

$$\mathrm{Res}(u_{L'/K}) = u_{L'/L};$$

$$\mathrm{Inf}(u_{L/K}) = [L' : L]u_{L'/K},$$

donde $\mathrm{Res} : \mathrm{Br}(L'/K) \to \mathrm{Br}(L'/L)$ *e* $\mathrm{Inf} : \mathrm{Br}(L/K) \to \mathrm{Br}(L'/K)$ *son las aplicaciones de la Proposición 5.7.1. Por lo tanto,*

$$\mathrm{inv}_{E/K} \circ \mathrm{Inf} = \mathrm{inv}_{L/K}\,.$$

Proposición 6.2.5. *Sea L/K una extensión de Galois de grado n de cuerpos locales, no ramificada. Sean $G = \mathrm{Gal}(L/K)$ y $\mathcal{U}_L$ el grupo de unidades de L. Entonces G actúa en $\mathcal{U}_L$ y*

$$\widehat{H}^q(G,\mathcal{U}_L) = 0 \quad \forall q.$$

Proposición 6.2.6. *Sea L/K una extensión cíclica de cuerpos locales de orden n. Entonces $h(G,\mathcal{U}_L) = 1$ y $h(G, L^\times) = n$.*

Corolario 6.2.7. *Bajo las hipótesis de la última proposición, $(\mathcal{U}_K : \mathrm{N}_{L/K}\,\mathcal{U}_L) = e$, donde e es el índice de ramificación.*

Dem. Sea σ un generador de G. Notemos que el índice de $\mathrm{N}_{L/K}\,\mathcal{U}_L$ en $\mathcal{U}_K$ es el numerador del cociente de Herbrand. Probemos entonces que el denominador es e.

Necesitaremos el siguiente resultado técnico de teoría de grupos. Sea f un morfismo de un grupo abeliano A en otro grupo; denotaremos con A^f su imagen y con A_f su núcleo. Sea B un subgrupo de A. Entonces

$$(A : B) = (A^f : B^f)(A_f : B_f),$$

en el sentido de que si dos de los índices son finitos, el tercero también lo es y son iguales. En efecto, consideremos la composición de f con la proyección al cociente $A \to A^f \to A^f/B^f$. El núcleo es $B + A_f$, con lo cual, se tiene un isomorfismo $A^f/B^f \simeq A/(B + A_f)$. Por otra parte, $(B + A_f)/B \simeq A_f/(B \cap A_f) = A_f/B_f$. Como $A \supset B + A_f \supset B$, se sigue el resultado.

Consideremos ahora el morfismo $(1-\sigma) : \mathcal{U}_L \to \mathcal{U}_L$, dado por $x \mapsto x/\sigma(x)$. El denominador del cociente de Herbrand es el orden de $\widehat{H}_0(G,\mathcal{U}_L)$, que es el índice de $\mathcal{U}_L^{1-\sigma}$ en el núcleo de $\mathrm{N}_{L/K} : \mathcal{U}_L \to \mathcal{U}_L$. Por el Teorema 90 de Hilbert, este núcleo es $(L^\times)^{1-\sigma}$. Luego, el denominador del cociente de Herbrand es

$$((L^\times)^{1-\sigma} : \mathcal{U}_L^{1-\sigma}) = ((L^\times)^{1-\sigma} : (K^\times\mathcal{U}_L)^{1-\sigma}) = (L^\times : K^\times\mathcal{U}_L)/(L^\times_{1-\sigma} : (K^\times\mathcal{U}_L)_{1-\sigma})).$$

Además, $(L^\times : K^\times\mathcal{U}_L) = e$ pues $L^\times/\mathcal{U}_L \simeq \langle\pi_L\rangle$ con π_L un uniformizador, $K^\times\mathcal{U}_L/\mathcal{U}_L \simeq K^\times/\mathcal{U}_K \simeq \langle\pi_K\rangle$ y $\pi_K = u\pi_L^e$ con una unidad u. Además, $L^\times_{1-\sigma} = K^\times$, con lo cual, $(L^\times_{1-\sigma} : (K^\times\mathcal{U}_L)_{1-\sigma}) = 1$. Luego, el denominador es exactamente e.

□

Corolario 6.2.8. *Sea L/K una extensión abeliana de cuerpos locales. Entonces L/K es no ramificada si y sólo si toda unidad es la norma de una unidad.*

Dem. Una dirección sale tomando $q = 0$ en 6.2.5, pues la aplicación N considerada en la cohomología de Tate no es otra cosa que la norma usual de la extensión. Recíprocamente, si la extensión es ramificada entonces existe una subextensión cíclica $L \supset M \supset K$ con M/K ramificada: por el teorema de estructura para grupos finitos abelianos y teoría de Galois, toda extensión finita y abeliana es composición de cíclicas, y si un primo no ramifica en dos extensiones, tampoco ramifica en el compuesto; para este último resultado, ver el Teorema 31 del Capítulo 4 de [Mar77]. Pero si toda unidad de K es la norma de una unidad de L, entonces toda unidad es la norma de una unidad de M por transitividad, y por el corolario anterior esto no puede suceder. □

Proposición 6.2.9. *Sea K un cuerpo local, $|.|_K$ un valor absoluto normalizado y $n \in \mathbb{N}$ coprimo con la característica de K. Consideremos a $\mathbb{Z}/n\mathbb{Z}$ actuando trivialmente en $K^\times$. Entonces $h(K^\times) = n/|n|_K$ y $h(\mathcal{U}_K) = 1/|n|_K$.*

Observación 6.2.10. El resultado también es válido para el caso $K = \mathbb{R}$ o $K = \mathbb{C}$.

Daremos ahora una caracterización de $(\alpha, L/K)$. Recordemos que, dada L/K de Galois, no ramificada, el grupo de Galois es canónicamente isomorfo al grupo de Galois de la extensión residual, con lo cual, tiene un elemento distinguido $\mathrm{Frob}_{L/K}$ llamado *morfismo de Frobenius*.

Necesitaremos ahondar un poco más en las propiedades de las extensiones no ramificadas de un cuerpo local no arquimedeano K. Sea K^{nr} la unión de todas las extensiones no ramificadas L/K contenidas en una cierta clausura separable de K; se denomina la *extension no ramificada maximal* de K. Toda subextensión finita de K^{nr} es no ramificada sobre K, abeliana, y existe un único elemento $\mathrm{Frob}_K \in \mathrm{Gal}(K^{nr}/K)$ con la siguiente propiedad: si L/K es una subextensión finita de K^{nr}/K entonces $\mathrm{Frob}_K|_L = \mathrm{Frob}_{L/K}$.

Teorema 6.2.11. *Sea $\phi_K : K^\times \to \mathrm{Gal}(K^{ab}/K)$ el mapa de reciprocidad, donde K^{ab} es una clausura abeliana de K que contiene a K^{nr}. Sea π_K un uniformizador. de K. Entonces*

$$\phi_K(\pi_K)|_{K^{nr}} = \mathrm{Frob}_K,$$

y si L/K es una extensión finita de Galois no ramificada y $a \in K^\times$, entonces

$$\phi_{L/K}(a) = \mathrm{Frob}_{L/K}^{\mathrm{ord}_K(a)},$$

donde $\mathrm{ord}_K(a) \in \mathbb{Z}$ es la valuación normalizada de a.

6.3. Extensiones ciclotómicas de $\mathbb{Q}_p$

Sea p un primo de $\mathbb{Q}$. Estamos interesados en describir el mapa de reciprocidad $\phi_{\mathbb{Q}_p(\zeta)/\mathbb{Q}_p} : \mathbb{Q}_p^\times \to \mathrm{Gal}(\mathbb{Q}_p(\zeta)/\mathbb{Q}_p)$, donde ζ es una raíz m-ésima primitiva de la unidad.

Caso $p = \infty$. En este caso, $\mathbb{Q}_p = \mathbb{R}$, y $\mathbb{R}(\zeta) = \mathbb{C}$, a menos que $m = 1, 2$, en cuyo caso el mapa de reciprocidad es el trivial. Si $m > 2$, el mapa de reciprocidad ya lo describimos antes y consiste de mandar los elementos positivos a la identidad y los negativos a la conjugación compleja.

Caso $p < \infty$. Sea $x = up^\nu \in \mathbb{Q}_p^\times$, donde $u \in \mathcal{U}_p = \mathbb{Z}_p^\times$ y $\nu \in \mathbb{Z}$. Entonces $\phi_{\mathbb{Q}_p(\zeta)/\mathbb{Q}_p}(x)$ (que está determinado por su acción en ζ) manda ζ en ζ^{p^ν} si p no divide a m. Esto es inmediato de ver pues $\mathbb{Q}_p(\zeta_m)/\mathbb{Q}_p$ es no ramificada y, por lo tanto, toda unidad es una norma y va a parar a 1; por otra parte, p debe ir a parar al morfismo de Frobenius, que es efectivamente elevar a la p.

Si m es una potencia de p, digamos $m = p^r$, entonces $\phi_{\mathbb{Q}_p(\zeta)/\mathbb{Q}_p}(x)(\zeta) = \zeta^{u^{-1}}$, donde u^{-1} lo consideramos un entero vía los isomorfismos

$$\mathbb{Z}_p/p^r\mathbb{Z}_p \simeq \mathbb{Z}_{(p)}/p^r\mathbb{Z}_{(p)} \simeq \mathbb{Z}/p^r\mathbb{Z}$$

(ver Capítulo 1).

El caso de m cualquiera, $m = p^r n$, con $p \nmid n$, se describe usando los dos casos anteriores.

Capítulo 7

Demostraciones de los teoremas principales

7.1. Cohomología de Idèles

Sea L/K una extensión finita de Galois de cuerpos de números, con grupo de Galois G. Recordemos que, para cada primo w de L, tenemos definida una aplicación inyectiva

$$i_w : L_w^\times \to \mathbb{I}_L.$$

Notemos que la imagen de $L_w^\times$ en $\mathbb{I}_L$ por esta aplicación no queda fija por la acción de G definida en 4.4. Si v es el primo de K debajo de w, el subgrupo más chico con esta propiedad que contiene a $L_w^\times$ es $\prod_{w|v} L_w^\times$. De esta manera, G actúa en $\prod_{w|v} L_w^\times$, y también en $\prod_{w|v} \mathcal{U}_w$.

Proposición 7.1.1. *Sea v un primo de K y w_0 un primo de L sobre v. Entonces*

$$H^q(G, \prod_{w|v} L_w^\times) \simeq H^q(D(w_0), L_{w_0}^\times) \quad \forall q \geq 0.$$

Vale lo mismo reemplazando $L_w^\times$ por $\mathcal{U}_w$.

Dem. Probaremos primero que $\prod_{w|v} L_w^\times \simeq \mathrm{Hom}_{D(w_0)}(\mathbb{Z}G, L_{w_0}^\times)$ como G-módulos. Definimos una aplicación $\alpha \mapsto f_\alpha$, donde $f_\alpha(\sigma) = \sigma_{\sigma^{-1}w_0}(\alpha_{\sigma^{-1}w_0})$. Es inmediato ver que $f_\alpha \in \mathrm{Hom}_{D(w_0)}(\mathbb{Z}G, L_{w_0}^\times)$ y que $\alpha \mapsto f_\alpha$ es un morfismo de G-módulos.

Dada $f \in \mathrm{Hom}_{D(w_0)}(\mathbb{Z}G, L_{w_0}^\times)$, tomamos α_f definido por $(\alpha_f)_w = \sigma_{w_0}(f(\sigma^{-1}))$ si $\sigma w_0 = w$. Es muy fácil ver que no depende del σ elegido y que define una inversa para la aplicación anterior.

Luego, tenemos que $H^q(G, \prod_{w|v} L_w^\times) \simeq H^q(G, \mathrm{Hom}_{D(w_0)}(\mathbb{Z}G, L_{w_0}^\times)) \simeq H^q(D(w_0), L_{w_0}^\times)$ por el lema de Shapiro (5.2.1). □

Por la última proposición, los grupos de cohomología $H^q(D(w), L_w^\times)$ son todos isomorfos entre sí para $w|v$. Más aún: son *canónicamente* isomorfos. En efecto, sean w_0 y w_1 dos primos sobre v. Entonces existe $\sigma \in G$ tal que $w_1 = \sigma w_0$, y se tienen isomorfismos compatibles

$D(w_0) \to D(w_1)$, $\tau \mapsto \sigma\tau\sigma^{-1}$ y $L_{w_1}^\times \to L_{w_0}^\times$, $x \mapsto (\sigma^{-1})_{w_1} x$. Luego, se tiene un isomorfismo $H^q(D(w_1), L_{w_1}^\times) \to H^q(D(w_0), L_{w_0}^\times)$ (ver Capítulo 5, Sección 5.2). En principio este isomorfismo depende de σ. Pero si $w_1 = \sigma' w_0$ entonces $\sigma' = \sigma\tau$ con $\tau \in D(w_0)$. Es fácil ver que los isomorfismos definidos por σ y σ' difieren por el automorfismo de $H^q(D(w_0), L_{w_0}^\times)$ definido por τ como en la Proposición 5.2.2, que debe ser la identidad. Tiene sentido entonces usar la notación $H^q(G^v, (L^v)^\times)$ para cualquier $H^q(D(w), L_w^\times)$ si $w|v$, y lo mismo para $H^q(G^v, \mathcal{U}^v)$.

Proposición 7.1.2. *Sea L/K finita de Galois, con grupo de Galois G. Entonces:*

(I) $\mathbb{I}_K \simeq \mathbb{I}_L^G$;

(II) $H^q(G, \mathbb{I}_L) \simeq \bigoplus_v H^q(G^v, (L^v)^\times)$.

Dem. (I): En principio tenemos una inclusión $\mathbb{I}_K \hookrightarrow \mathbb{I}_L$, definida por $\alpha \mapsto \beta$, donde $\beta_w = \alpha_v$ si $w|v$. Un elemento $\beta = (\beta_w) \in \mathbb{I}_L$ está fijo por G si y sólo si cada subfamilia $(\beta_w)_{w|v}$ queda fija por G. Pero esto último ocurre si y sólo si los β_w con $w|v$ son un mismo número de $K_v^\times$, independiente de w (en virtud de que $D(w_0) \simeq \mathrm{Gal}(L_w/K_v)$). Entonces la imagen de $\mathbb{I}_K$ en $\mathbb{I}_L$ es exactamente $\mathbb{I}_L^G$.

(II): Para cada conjunto finito S de primos de K que contenga a los primos ramificados y a los infinitos, sea

$$\mathbb{I}_L^S = \prod_{v\in S}\Big(\prod_{w|v} L_w^\times\Big) \times \prod_{v\notin S}\Big(\prod_{w|v} \mathcal{U}_w\Big).$$

Sabemos que $\mathbb{I}_L$ es la unión directa de los $\mathbb{I}_L^S$, donde S recorre los conjuntos finitos de primos de K que contienen a los que ramifican y a los infinitos. Como la cohomología de grupos finitos conmuta con productos (Proposición 5.1.5) y con uniones directas (Proposición 5.1.6), debemos mirar la cohomología de cada factor.

Por 6.2.5, $\prod_{v\notin S}(\prod_{w|v} \mathcal{U}_w)$ tiene cohomología trivial si S contiene a los primos ramificados. En consecuencia, por la proposición anterior,

$$H^q(G, \mathbb{I}_L^S) \simeq \prod_{v\in S} H^q(G^v, (L^v)^\times).$$

Finalmente,

$$H^q(G, \mathbb{I}_L) \simeq \varinjlim_S H^q(G, \mathbb{I}_L^S) = \bigoplus_v H^q(G^v, (L^v)^\times).$$

□

Para más adelante, necesitaremos una descripción explícita del segundo isomorfismo en términos de cociclos. Sea $\alpha : G^q \to \mathbb{I}_L$ un q-cociclo. Entonces la componente v-ésima en $\bigoplus_v H^q(G^v, (L^v)^\times)$ está representada por el cociclo $\beta : (G^v)^q \to (L^v)^\times$, definido de la siguiente manera: sea w un primo fijo sobre v, $L^v = L_w$. Entonces $\beta(\sigma_1, \ldots, \sigma_q) = \alpha(\sigma_1, \ldots, \sigma_q)_w$, donde vemos a $\sigma_i \in G^v$ dentro de G. Dejamos la verificación como ejercicio.

Corolario 7.1.3. *Sea L/K finita de Galois, con grupo de Galois G. Entonces $H^1(G, \mathbb{I}_L) = 0$.*

Dem. En virtud de la proposición anterior, esto no es otra cosa que el Teorema 5.8.4. □

7.2. Primera desigualdad

Consideremos la sucesión exacta $0 \to L^\times \to \mathbb{I}_L \to \mathbf{C}_L \to 0$. La acción de G en $\mathbb{I}_L$ induce una acción en $\mathbf{C}_L$.

Proposición 7.2.1. *Sea L/K finita de Galois, con grupo de Galois G. Entonces $\mathbf{C}_K \simeq \mathbf{C}_L^G$.*

Dem. La sucesión exacta corta de recién nos da una sucesión exacta larga de cohomología

$$0 \to H^0(G, L^\times) \to H^0(G, \mathbb{I}_L) \to H^0(G, \mathbf{C}_L) \to H^1(G, L^\times).$$

Dado que $H^1(G, L^\times) = 0$ por el Teorema 5.8.4, obtenemos que la sucesión

$$0 \to K^\times \to \mathbb{I}_K \to \mathbf{C}_L^G \to 0$$

es exacta. □

Notamos con $h(G, A)$ al cociente de Herbrand de un G-módulo A (si está definido).

Teorema 7.2.2. *Sea L/K cíclica de grado n. Sea $G = \mathrm{Gal}(L/K)$. Entonces $h(G, \mathbf{C}_L) = n$.*

Dem. Sea S un conjunto finito de primos de K suficientemente grande, de manera tal que $\mathbb{I}_L = L^\times \mathbb{I}_L^S$, donde

$$\mathbb{I}_L^S = \prod_{v \in S} (\prod_{w|v} L_w^\times) \times \prod_{v \notin S} (\prod_{w|v} \mathcal{U}_w).$$

Más precisamente, si T es un conjunto de primos de L que contiene a los infinitos, tal que $\mathbb{I}_L = L^\times \mathbb{I}_L^T$ (Lema 3.3.12), sea S el conjunto de primos de K debajo de los de T. Agrandando T si fuese necesario, podemos suponer que S contiene también a todos los primos ramificados. Se tiene entonces que

$$\mathbf{C}_L = \mathbb{I}_L / L^\times \simeq \mathbb{I}_L^S / (L^\times \cap \mathbb{I}_L^S) = \mathbb{I}_L^S / U_L(T),$$

donde $U_L(T) = L^\times \cap \mathbb{I}_L^S$ consiste de las "T-unidades", es decir, elementos de $L^\times$ que son unidades en L_w si $w \notin T$. Luego, tenemos que

$$h(G, \mathbf{C}_L) = h(G, \mathbb{I}_L^S) / h(G, U_L(T)),$$

siempre que el lado de la derecha esté definido.

Calcularemos primero $h(G, \mathbb{I}_L^S)$. Como S contiene a los primos ramificados, por la Proposición 6.2.5 vale que $\prod_{v \notin S} (\prod_{w|v} \mathcal{U}_w)$ tiene cohomología trivial. Por lo tanto, como $h(G, -)$ conmuta con productos finitos,

$$h(G, \mathbb{I}_L^S) = \prod_{v \in S} h(G, \prod_{w|v} L_w^\times).$$

Por la Proposición 7.1.1, $h(G, \prod_{w|v} L_w^\times) = h(G^v, (L^v)^\times)$. Además, por el Teorema 5.8.4, $H^1(G^v, (L^v)^\times) = 0$, y por el Corolario 6.2.3, $H^2(G^v, (L^v)^\times)$ es un grupo cíclico de orden $n_v = [L^v : K_v]$. Por lo tanto,

$$h(G, \mathbb{I}_L^S) = \prod_{v \in S} n_v.$$

Ahora determinaremos $h(G, U_L(T))$. Si queremos probar que $h(G, \mathbf{C}_L) = n$, debemos probar que $nh(G, U_L(T)) = \prod_{v \in S} n_v$. La idea será construir un $\mathbb{R}$-espacio vectorial en el cual G actúe, y dos retículos maximales invariantes cuyos cocientes de Herbrand coincidan respectivamente con $nh(G, U_L(T))$ y $\prod_{v \in S} n_v$.

Como espacio de la representación tomamos el conjunto de las funciones de T en $\mathbb{R}$, y lo llamamos V. Es decir, $V \simeq \mathbb{R}^t$, donde $t = \#T$. La acción de G está dada por $(\sigma f)(w) = f(\sigma^{-1} w)$; de esta manera, $(\sigma f)(\sigma w) = f(w)$.

Sea $N = \{f \in V : \mathrm{Im}(f) \subset \mathbb{Z}\}$. Entonces N es un retículo maximal de V, ya que genera V. Podemos pensar a N como isomorfo a $\prod_{v \in S} (\prod_{w|v} \mathbb{Z}_w)$, donde $\mathbb{Z}_w \simeq \mathbb{Z}$ y la acción de G es punto a punto en cada $v \in S$ y por permutación de los $\mathbb{Z}_w$ para todos los w sobre un $v \in S$ fijo. Además, para cada $v \in S$, $\prod_{w|v} \mathbb{Z}_w \simeq \mathrm{Hom}_{G^v}(\mathbb{Z}G, \mathbb{Z})$ (para $G^v = D(w_0)$, con $w_0|v$ fijo) como G-módulos, viendo a $\mathbb{Z}$ con la acción trivial de G^v. Luego,

$$h(G, N) = \prod_{v \in S} h(G, \prod_{w|v} \mathbb{Z}_w) = \prod_{v \in S} h(G^v, \mathbb{Z}) = \prod_{v \in S} (G^v : 1) = \prod_{v \in S} n_v$$

por el lema de Shapiro. Hemos usado que $h(G, \mathbb{Z}) = (G : 1)$ si vemos a $\mathbb{Z}$ como G-módulo trivial.

Para el siguiente retículo, consideremos la aplicación $\lambda : U_L(T) \to V$ dada por $a \mapsto f_a$, donde $f_a(w) = \log |a|_w$. Entonces λ es un morfismo de G-módulos. Sea M^0 la imagen de λ. Nos remitimos a la demostración del teorema de las unidades (Teorema 3.3.10) para decir que M^0 está contenido en $V^0 = \{f \in V : \sum_{w \in T} f(w) = 0\}$, es un retículo maximal de V^0, y el núcleo de λ es finito. Entonces $h(G, U_L(T)) = h(G, M^0)$, ya que $h(G, U_L(T))$ está definido por ser $U_L(T)$ finitamente generado y por el Corolario 5.4.6. Consideremos ahora la función $e : T \to \mathbb{R}$ dada por $e(w) = 1$ para todo w. Entonces e queda fija por G y no está en V^0. Tomamos $M = M^0 + \mathbb{Z}e$. Entonces M es un retículo maximal de V pues $M \otimes_{\mathbb{Z}} \mathbb{R} = V^0 + \mathbb{R}e = V$. Más aún, $h(G, M) = h(G, M^0)h(G, \mathbb{Z}) = h(G, M^0)n = h(G, U_L(T))n$.

Obtenemos entonces que $nh(G, U_L(T)) = \prod_{v \in S} n_v / n$, como queríamos. □

Corolario 7.2.3 (Primera desigualdad)**.** *Si L/K es cíclica de grado n entonces*

$$(\mathbb{I}_K : K^\times \mathrm{N}_{L/K} \mathbb{I}_L) \geq n.$$

Dem. La Proposición 4.4.2 nos dice que la norma usual se corresponde con la norma definida para la cohomología de Tate vía el isomorfismo $\mathbf{C}_K \simeq \mathbf{C}_L^G$, donde G es el grupo de Galois de L/K. Por lo tanto,

$$(\mathbb{I}_K : K^\times \mathrm{N}_{L/K} \mathbb{I}_L) = (\mathbf{C}_K \,/\, \mathrm{N}_{L/K} \mathbf{C}_L) = (\widehat{H}^0(G, \mathbf{C}_L) : 1) \geq h(G, \mathbf{C}_L) = n.$$

□

Corolario 7.2.4. *Sea L/K finita y abeliana, y D un subgrupo de $\mathbb{I}_K$ tal que*

(a) $D \subset \mathrm{N}_{L/K} \mathbb{I}_K$;

(b) $K^\times D$ *es denso en* $\mathbb{I}_K$.

Entonces $L = K$.

Dem. Podemos suponer que L/K es cíclica; si este no fuera el caso, tomamos L' tal que $L \supset L' \supset K$ y L'/K sea cíclica. Tendremos entonces que $D \subset \mathrm{N}_{L/K}\,\mathbb{I}_K \subset \mathrm{N}_{L'/K}\,\mathbb{I}_{L'}$.

Por la Proposición 4.4.8, $K^\times \mathrm{N}_{L/K}\,\mathbb{I}_L$ es un subgrupo abierto de $\mathbb{I}_K$, con lo cual, es cerrado. También es denso, pues contiene al denso D. Entonces $(\mathbb{I}_K : K^\times \mathrm{N}_{L/K}\,\mathbb{I}_K) = 1$. Por el corolario anterior, debe ser $[L : K] = 1$. □

Corolario 7.2.5. *Sea L/K finita y abeliana. Si $L \neq K$ entonces existen infinitos primos de K que no se parten completamente en L.*

Dem. Supongamos que hay sólo finitos. Sea S un conjunto finito que los contenga. Sea $D = \mathbb{I}_{K,S} = \{x \in \mathbb{I}_K : x_v = 1\ \forall v \in S\}$. Si $v \notin S$ y $w|v$ entonces $[L_w : K_v] = e(w|v)f(w|v) = 1$, con lo cual, $L_w = K_v$. Luego, $D \subset \mathrm{N}_{L/K}\,\mathbb{I}_L$. Por el Lema 3.3.12, $K^\times D$ es denso en $\mathbb{I}_K$. Llegamos así a una contradicción. □

Corolario 7.2.6. *Sea L/K finita y abeliana, y S un conjunto de primos de K que contenga a los primos ramificados. Entonces $\mathrm{Gal}(L/K)$ está generado por los elementos $\psi_{L/K}(\mathfrak{p})$ para $\mathfrak{p} \notin S$. Luego, el mapa de Artin es suryectivo.*

Dem. Sea G' el subgrupo de $\mathrm{Gal}(L/K)$ generado por los $\psi_{L/K}(\mathfrak{p})$ con $\mathfrak{p} \notin S$ (siempre $\mathfrak{p}$ finito). Sea L' el cuerpo fijo de G'. Para $\mathfrak{p} \notin S$, se tiene que $\psi_{L'/K}(\mathfrak{p}) = \psi_{L/K}(\mathfrak{p})\,|_{L'}$, que es la identidad. Luego, todos los primos $\mathfrak{p} \notin S$ se parten completamente en L', y, por lo tanto, $L' = K$. Entonces $G' = \mathrm{Gal}(L/K)$. □

7.3. Teoría de Kummer

Para probar la segunda desigualdad, necesitaremos los principales resultados de la teoría de Kummer. Para las demostraciones, nos remitimos a [Lan94] o [Mil97].

A lo largo de toda esta sección, K es un cuerpo que contiene una raíz n-ésima primitiva de la unidad, ζ (en particular, la característica de K es 0 o no divide a n). Si $\alpha \in K$, por $\alpha^{1/n}$ nos referiremos a una raíz n-ésima de α (contenida en una clausura algebraica de K). Si β es una tal raíz, $\theta\beta$ también lo es para cualquier raíz n-ésima de la unidad θ. Como todas están en K, la notación $K(\alpha^{1/n})$ tiene sentido y consiste de adjuntar a K todas las raíces n-ésimas de α. Si $B \subset K$ es un conjunto, por $K(B^{1/n})$ nos referiremos al compuesto de todas las extensiones $K(\beta^{1/n})$ con $\beta \in B$.

Decimos que un grupo abeliano G tiene exponente n si $\sigma^n = 1$ para todo $\sigma \in G$; una extensión abeliana tiene exponente n si su grupo de Galois lo tiene. El resultado principal de la teoría de Kummer establece una biyección entre extensiones finitas y abelianas de K de exponente n y ciertos subgrupos de $K^\times$ que contienen a $K^{\times n}$, más específicamente, subgrupos $K^\times \supset B \supset K^{\times n}$ tales que $(B : K^{\times n})$ es finito.

La biyección hace corresponderle a B la extensión $K_B = K(B^{1/n})$. Si $\beta_1, \ldots, \beta_m$ son representantes de B en el cociente $B/K^{\times n}$ entonces $K_B = K(\beta_1^{1/n}, \ldots, \beta_m^{1/n})$. Más aún, se cumple que $(K_B : K) = (B : K^{\times n})$.

Ahora necesitaremos saber, en el caso en que K sea un cuerpo de números (tal que contiene una raíz ζ como siempre), cómo se factorizan los primos de K en las extensiones K_B; sólo nos alcanzará con saber que ciertos primos son no ramificados.

Proposición 7.3.1. *Sea K un cuerpo de números tal que contiene una raíz n-ésima primitiva de la unidad. Sea $L = K(\beta_1^{1/n}, \ldots, \beta_m^{1/n})$. Sea v un primo finito de K. Si $n\beta_i$ es una unidad en K_v para todo i entonces v es no ramificado en L.*

7.4. Segunda desigualdad

Probaremos ahora que $[\mathbb{I}_K : K^\times \mathrm{N}_{L/K}\, \mathbb{I}_L] \leq n$, a partir de lo cual se deduce la igualdad. Una manera de demostrar esta desigualdad es utilizando métodos analíticos; así es como se había hecho en un principio, y nos remitimos a [Lan94], Capítulo VIII, para este enfoque. La prueba que damos a continuación se debe a Chevalley (1940), quien buscaba un tratamiento puramente algebraico de la teoría de cuerpos de clases.

Probaremos algo más fuerte que la desigualdad.

Teorema 7.4.1. *Sea L/K una extensión de Galois de grado n, con grupo de Galois G. Entonces*

(1) $(\widehat{H}^0(G, \mathbf{C}_L) : 1)$ *y* $(\widehat{H}^2(G, \mathbf{C}_L) : 1)$ *son finitos y dividen a* n;

(2) $\widehat{H}^1(G, \mathbf{C}_L) = 0$.

La demostración de este teorema la haremos en varios pasos.

Paso 1. Afirmamos que basta probar el teorema para el caso en que G es un p-grupo (es decir, un grupo de orden una potencia de p), para p primo. En efecto, como los $\widehat{H}^q(G, \mathbf{C}_L)$ son de torsión para todo q (Proposición 5.4.5), son suma directa de sus componentes primarias. Sea p un primo arbitrario y sea H un p-subgrupo de Sylow de G. Por el Corolario 5.4.7, $\mathrm{Res} : \widehat{H}^q(G, \mathbf{C}_L) \to \widehat{H}^q(H, \mathbf{C}_L)$ es un monomorfismo en la componente p-primaria de $\widehat{H}^q(G, \mathbf{C}_L)$. Como el teorema es válido para L/L^H, se sigue que la componente p-primaria de $H^1(G, \mathbf{C}_L)$ es 0. Además, siendo $\widehat{H}^i(H, \mathbf{C}_L)$ $(i = 0, 2)$ finito, se sigue que $\widehat{H}^i(G, \mathbf{C}_L)$ $(i = 0, 2)$ es finito. Más aún, la mayor potencia de p que divide a su orden es el orden de la componente p-primaria, que es menor o igual que el orden de la componente p-primaria de $\widehat{H}^i(H, \mathbf{C}_L)$; esto es la mayor potencia de p que divide a $(\widehat{H}^i(H, \mathbf{C}_L) : 1)$, que sabemos que es menor o igual que la que divide a G por hipótesis. Haciendo esto para todo p, se sigue que el teorema es válido para el caso general.

Paso 2. Podemos suponer que G es cíclico de orden p primo. En efecto, supongamos que probamos el teorema para este caso. Para el caso general, podemos suponer de entrada que G es un p-grupo. Vamos a probarlo por inducción en el orden de G. Como G es un p-grupo, existe un subgrupo H normal en G de índice p. Por el Teorema 5.3.1 (y usando que $(\mathbf{C}_L)^H = \mathbf{C}_{L^H}$) tenemos una sucesión exacta

$$0 \longrightarrow H^1(G/H, \mathbf{C}_{K'}) \xrightarrow{\mathrm{Inf}} H^1(G, \mathbf{C}_L) \xrightarrow{\mathrm{Res}} H^1(H, \mathbf{C}_L),$$

donde $K' = L^H$. Como K'/K es Galois con grupo de Galois G/H (cíclico de orden p), el teorema vale para K'/K. Luego, $H^1(G/H, \mathbf{C}_{K'}) = 0$; por inducción, $H^1(H, \mathbf{C}_L) = 0$, y, por lo tanto, $H^1(G, \mathbf{C}_L) = 0$.

Como $H^1(H, \mathbf{C}_L) = 0$, tomando $q = 2$ en la Proposición 5.3.2, se ve que la sucesión

$$0 \longrightarrow H^2(G/H, \mathbf{C}_{K'}) \xrightarrow{\text{Inf}} H^2(G, \mathbf{C}_L) \xrightarrow{\text{Res}} H^2(H, \mathbf{C}_L)$$

es exacta. De vuelta por inducción e hipótesis, se sigue que el orden de $H^2(G, \mathbf{C}_L)$ divide a $(G : 1)$.

Finalmente, al ser la norma transitiva, $\mathrm{N}_{K'/K}$ define una aplicación suryectiva

$$\mathbf{C}_{K'} / \mathrm{N}_{L/K'}(\mathbf{C}_L) \to \mathrm{N}_{K'/K}(\mathbf{C}_{K'}) / \mathrm{N}_{L/K}(\mathbf{C}_L).$$

Como

$$(\mathbf{C}_K : \mathrm{N}_{L/K}(\mathbf{C}_L)) = (\mathbf{C}_K : \mathrm{N}_{K'/K}(\mathbf{C}_{K'}))(\mathrm{N}_{K'/K}(\mathbf{C}_{K'}) : \mathrm{N}_{L/K}(\mathbf{C}_L))$$

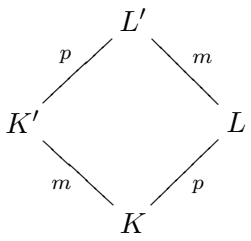
y

$$(\mathrm{N}_{K'/K}(\mathbf{C}_{K'}) : \mathrm{N}_{L/K}(\mathbf{C}_L)) | (\mathbf{C}_{K'} : \mathrm{N}_{L/K'}(\mathbf{C}_L)),$$

nuevamente por hipótesis e inducción se sigue que $(\widehat{H}^0(G, \mathbf{C}_L) : 1)$ divide a $[L : K]$.

Observación. Si G es cíclico de órden n, $\widehat{H}^0(G, \mathbf{C}_L) \simeq H^2(G, \mathbf{C}_L)$ y por el Teorema 7.2.2 $h(G, \mathbf{C}_L) = (\widehat{H}^0(G, \mathbf{C}_L) : 1)/(H^1(G, \mathbf{C}_L) : 1) = n$; luego, basta probar que $(\widehat{H}^0(G, \mathbf{C}_L) : 1) \mid n$ para deducir que $(H^1(G, \mathbf{C}_L) : 1) = 1$.

Paso 3. Podemos suponer que K contiene las raíces p-ésimas de la unidad. En efecto, consideremos $K' = K(\zeta)$, donde ζ es una raíz p-ésima primitiva de la unidad contenida en una clausura algebraica de K que contiene a L. Sea $L' = LK' = L(\zeta)$. Si m es el grado de K'/K, entonces m divide a $p - 1$, con lo cual, es coprimo con $p = [L : K]$. Luego, $K' \cap L = K$, $\mathrm{Gal}(L'/K)$ es isomorfo a $\mathrm{Gal}(L/K) \times \mathrm{Gal}(K'/K)$ y se tiene el siguiente diagrama de extensiones:



Consideremos el siguiente diagrama:

$$\begin{array}{ccc}
\mathbf{C}_L & \xrightarrow{\mathrm{N}_{L/K}} & \mathbf{C}_K \\
\downarrow{\scriptstyle i_L} & & \downarrow{\scriptstyle i_K} \\
\mathbf{C}_{L'} & \xrightarrow{\mathrm{N}_{L'/K'}} & \mathbf{C}_{K'} \\
\downarrow{\scriptstyle \mathrm{N}_{L'/L}} & & \downarrow{\scriptstyle \mathrm{N}_{K'/K}} \\
\mathbf{C}_L & \xrightarrow{\mathrm{N}_{L/K}} & \mathbf{C}_K,
\end{array}$$

donde i_L e i_K son los morfismos inducidos por las inclusiones $\mathbb{I}_L \subset \mathbb{I}_{L'}$ y $\mathbb{I}_K \subset \mathbb{I}_{K'}$. Usando la Proposición 4.4.2 y el hecho de que $\mathrm{Gal}(L'/K') = \mathrm{Gal}(L/K)$, es fácil ver que el cuadrado de arriba conmuta, mientras que la transitividad de la norma implica que el cuadrado de abajo también; por lo tanto, se tiene el siguiente diagrama conmutativo con filas exactas:

$$\begin{array}{ccccccc}
\mathbf{C}_L & \xrightarrow{\mathrm{N}_{L/K}} & \mathbf{C}_K & \longrightarrow & \mathbf{C}_K \,/\, \mathrm{N}_{L/K}\, \mathbf{C}_L & \longrightarrow & 0 \\
\downarrow{\scriptstyle i_L} & & \downarrow{\scriptstyle i_K} & & \downarrow & & \\
\mathbf{C}_{L'} & \xrightarrow{\mathrm{N}_{L'/K'}} & \mathbf{C}_{K'} & \longrightarrow & \mathbf{C}_{K'} \,/\, \mathrm{N}_{L'/K'}\, \mathbf{C}_{L'} & \longrightarrow & 0 \\
\downarrow{\scriptstyle \mathrm{N}_{L'/L}} & & \downarrow{\scriptstyle \mathrm{N}_{K'/K}} & & \downarrow & & \\
\mathbf{C}_L & \xrightarrow{\mathrm{N}_{L/K}} & \mathbf{C}_K & \longrightarrow & \mathbf{C}_K \,/\, \mathrm{N}_{L/K}\, \mathbf{C}_L & \longrightarrow & 0.
\end{array}$$

Las dos composiciones, $\mathrm{N}_{L'/L} \circ i_L$ y $\mathrm{N}_{K'/K} \circ i_K$, están dadas por elevar a la m. Luego, la composición de la tercer columna también es elevar a la m. Ahora bien, elevar a la m es un isomorfismo de $\mathbf{C}_K \,/\, \mathrm{N}_{L/K}\, \mathbf{C}_L$, pues es un grupo de torsión en el que cada elemento no trivial tiene orden p (toda potencia p-ésima es una norma) y $(p, m) = 1$. En particular, obtenemos una aplicación suryectiva $\mathbf{C}_{K'} \,/\, \mathrm{N}_{L'/K'}\, \mathbf{C}_{L'} \to \mathbf{C}_K \,/\, \mathrm{N}_{L/K}\, \mathbf{C}_L$. Luego, $(\mathbf{C}_K : \mathrm{N}_{L/K}\, \mathbf{C}_L)$ divide a $(\mathbf{C}_{K'} \,/\, \mathrm{N}_{L'/K'}\, \mathbf{C}_{L'})$, que por hipótesis divide a p.

Paso 4. Hemos reducido todo a probar que $\widehat{H}^0(G, \mathbf{C}_L)$ es finito y su orden divide a p para una extensión L/K cíclica de grado p primo, con K tal que contiene las raíces p-ésimas de la unidad. Lo probaremos en un caso más general.

Teorema 7.4.2. *Sea L/K una extensión abeliana de exponente p primo, con grupo de Galois $G \simeq (\mathbb{Z}/p\mathbb{Z})^r$, tal que K contiene a las raíces p-ésimas de la unidad. Entonces $(\mathbf{C}_K : \mathrm{N}_{L/K}\, \mathbf{C}_L)$ divide a $[L : K] = p^r$.*

Observación 7.4.3. Como vimos antes, basta probar este teorema para el caso $r = 1$ y el caso general se deduce de éste. Sin embargo, la demostración para el caso de r arbitrario no se dificulta para nada, y aporta algunos resultados útiles para más adelante.

Dem. Por teoría de Kummer (ver la sección anterior), sabemos que $L = K(a_1^{1/p}, \ldots, a_r^{1/p})$ para ciertos $a_1, \ldots, a_r \in K$. Sea S un conjunto finito de primos de K, suficientemente grande tal que:

(I) $S \supset S_\infty$;

(II) S contenga a todos los primos de K sobre p;

(III) $\mathbb{I}_K = K^\times \mathbb{I}_K^S$ (Lema 3.3.12);

(IV) $a_1, \ldots, a_r \in \mathcal{U}_K(S)$, es decir, $\mathrm{ord}_v(a_i) = 0$ para todo $v \notin S$, $i = 1, \ldots, r$.

Sea $M = K(\mathcal{U}_K(S)^{1/p})$. Sabemos por el teorema de las unidades que $\mathcal{U}_K(S)$ es finitamente generado y, por lo tanto, M/K es una extensión finita. Además, por teoría de Kummer y por la condición (II), S contiene a los primos de K ramificados en M. Se tiene que $M \supset L \supset K$ y

$$\mathcal{U}_K(S) = M^{\times p} \cap \mathcal{U}_K(S) \supset L^{\times p} \cap \mathcal{U}_K(S) \supset K^{\times p} \cap \mathcal{U}_K(S) = \mathcal{U}_K(S)^p.$$

Por teoría de Kummer, M/K es de exponente p y, por lo tanto, tiene orden una potencia de p, digamos que $[M : K] = p^s$. Sabemos que $[L : K] = p^r$, y sea t tal que $[M : L] = p^t$, de manera que $s = t + r$.

Por el teorema de las unidades, $\mathcal{U}_K(S)$ es isomorfo a $\mathbb{Z}^{\sharp S - 1} \times W_K$, donde W_K son las raíces de la unidad en K, que obviamente contienen a las raíces p-ésimas de 1. Luego, W_K es un grupo finito, cíclico, cuyo orden es divisible por p. De esta manera, se tiene que

$$\mathcal{U}_K(S)/\mathcal{U}_K(S)^p \simeq (\mathbb{Z}/p\mathbb{Z})^{\sharp S}. \tag{1}$$

Por otra parte, $\mathcal{U}_K(S)/\mathcal{U}_K(S)^p = \mathcal{U}_K(S)/\mathcal{U}_K(S) \cap K^{\times p} \simeq K^{\times p}\mathcal{U}_K(S)/\mathcal{U}_K(S)$, de manera que $K^{\times p}\mathcal{U}_K(S)$ es un subgrupo de $K^\times$ que contiene a $K^{\times p}$ con índice $p^{\sharp S}$; la extensión que la teoría de Kummer le hace corresponder no es otra que M. Se tiene entonces que $s = \sharp S$.

Como $\mathcal{U}_K(S) \cap L^{\times p} \supset \mathcal{U}_K(S) \cap K^{\times p}$, se tiene que $\mathcal{U}_K(S)/\mathcal{U}_K(S) \cap L^{\times p}$ es finito, y, por lo tanto, $\mathcal{U}_K(S)L^{\times p}$ contiene a $L^{\times p}$ con índice finito, y la extensión de Kummer correspondiente es M. Luego,

$$[M : L] = p^t = (\mathcal{U}_K(S) : L^{\times p} \cap \mathcal{U}_K(S)). \tag{2}$$

Finalmente, como $s = t + r$, se tiene que

$$p^r = (L^{\times p} \cap \mathcal{U}_K(S) : \mathcal{U}_K(S)^p). \tag{3}$$

Probaremos entonces que $(\mathbf{C}_K : \mathrm{N}_{L/K}\, \mathbf{C}_L)$ divide a ese índice.

Si w es un primo de L sobre un primo $v \notin S$ de K entonces w no ramifica en M; luego, tenemos definido el mapa de Artin $\psi_{M/L}(w)$. Por el Corolario 7.2.6, los $\psi_{M/L}(w)$ generan $\mathrm{Gal}(M/L)$. Sean $w_1, \ldots, w_t$ tales que $\psi_{M/L}(w)$ sean una base de $\mathrm{Gal}(M/L)$ (como $\mathbb{F}_p$-espacio vectorial); sean $v_1, \ldots, v_t$ los primos de K debajo de ellos. Sabemos que no ramifican en M, con lo cual, tenemos definido $\psi_{M/K}(v_i) \in \mathrm{Gal}(M/K)$. Afirmamos que $\psi_{M/K}(v_i) = \psi_{M/L}(w_i)$ $(i = 1, \ldots, t)$. En efecto, sea w_i' un primo de M sobre w_i. Entonces $M_{w_i'}/K_{v_i}$ es no ramificada

y, por lo tanto, cíclica; además, es de exponente p pues su grupo de Galois es isomorfo a un subgrupo de $\mathrm{Gal}(M/K)$. Luego, es trivial o de orden p. Además, $M_{w_i'} \neq L_{w_i}$: si así lo fuese, el grado de inercia de w_i' sobre w_i sería 1, y $\psi_{M/L}(w_i)$ no es trivial por ser un elemento de una base. Obtenemos entonces que $L_{w_i} = K_{v_i}$; el grado de inercia de w_i sobre v_i es entonces 1 y por la Proposición 1.1.12, $\psi_{M/L}(w_i) = \psi_{M/K}(v_i)$, como queríamos.

Sea $T = \{v_1, \ldots, v_t\}$. Afirmamos que

$$L^{\times p} \cap \mathcal{U}_K(S) = \{a \in \mathcal{U}_K(S) : a \in K_v^{\times p} \ \ \forall v \in T\}. \tag{4}$$

En efecto, si $a \in L^{\times p} \cap \mathcal{U}_K(S)$, a es una potencia p-ésima en L_w para todo w. En particular, lo es para los w_i; como $L_{w_i} = K_{v_i}$, se sigue que a está en el conjunto de la derecha. Recíprocamente, si a está en el miembro derecho entonces $a^{1/p} \in M$. Como $a \in K_v^{\times p}$ para $v \in T$, $a^{1/p} \in K_v$ para $v \in T$ y, por lo tanto, queda fijo por todos los $\psi_{M/K}(v) = \psi_{L/K}(w)$; como estos generan $\mathrm{Gal}(M/L)$, se tiene que $a^{1/p} \in L$ y esto prueba la otra inclusión.

Sea

$$E = \prod_{v \in S} K_v^{\times p} \times \prod_{v \in T} K_v^{\times} \times \prod_{v \notin S \cup T} \mathcal{U}_v. \tag{5}$$

Entonces $E \subset \mathbb{I}_K^{S \cup T}$. Afirmamos que $E \subset \mathrm{N}_{L/K}\, \mathbb{I}_L$. Basta probar que si $a = (a_v) \in E$ entonces a_v es una norma local para todo v, esto es, $a_v \in \mathrm{N}_{L_w/K_v} L_w^{\times}$, donde w es un primo sobre v. Si $v \in S$, sabemos que $K_v^{\times} / \mathrm{N}_{L_w/K_v} L_w^{\times} \simeq \mathrm{Gal}(L_w/K_v)$ (para primos finitos, esto es 6.1, y para primos infinitos es trivial ya que $\mathbb{R}^{\times}/\mathbb{R}_+^{\times} \simeq \mathbb{Z}/2\mathbb{Z}$); toda potencia p-ésima aquí es trivial y, por lo tanto, todo elemento de $K_v^{\times p}$ es una norma. Si $v \in T$, $L_w = K_v$ y el resultado es trivial. Finalmente, si v no ramifica, todas las unidades son normas (6.2.8), y esto prueba lo que queríamos.

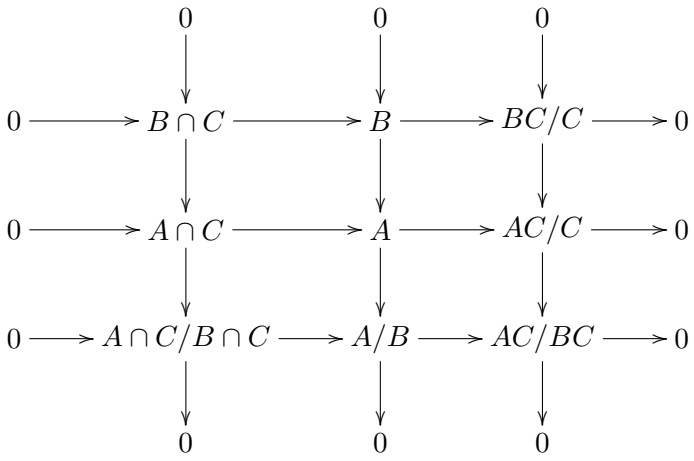
Sabemos que $(\mathbf{C}_K : \mathrm{N}_{L/K}\, \mathbf{C}_L) = (\mathbb{I}_K : K^{\times}\, \mathrm{N}_{L/K}\, \mathbb{I}_L)$, que, por lo recién probado, divide a $(\mathbb{I}_K : K^{\times} E)$. Ahora, elegimos S tal que

$$\mathbb{I}_K = K^{\times} \mathbb{I}_K^S = K^{\times} \mathbb{I}_K^{S \cup T},$$

con lo cual, $(\mathbf{C}_K : \mathrm{N}_{L/K}\, \mathbf{C}_L)$ divide a $(K^{\times} \mathbb{I}_K^{S \cup T} : K^{\times} E)$.

Según un resultado de teoría de grupos, si A, B, C son subgrupos de un grupo abeliano tales que $A \supset B$ entonces $(AC : BC)(A \cap C : B \cap C) = (A : B)$, en el sentido de que si dos de los índices son finitos entonces el tercero también lo es y vale la igualdad (para probar esto,

considerar el diagrama conmutativo



en el cual las dos filas de arriba y todas las columnas son exactas; probar que la tercera fila es exacta es un ejercicio fácil de "perseguir el diagrama", y esto implica lo que queríamos).

Luego, para probar el teorema será suficiente mostrar que

$$\frac{(\mathbb{I}_K^{S\cup T} : E)}{(\mathbb{I}_K^{S\cup T} \cap K^\times : E \cap K^\times)} = p^r. \tag{6}$$

Observemos que $\mathbb{I}_K^{S\cup T} \cap K^\times = \mathcal{U}_K(S \cup T)$.

Primero calcularemos $(\mathbb{I}_K^{S\cup T} : E)$. Por definición de ambos conjuntos, este índice es igual a $\prod_{v\in S}(K_v^\times : K_v^{\times p})$. Consideremos a $K_v^\times$ con la acción trivial del grupo $\mathbb{Z}/p\mathbb{Z}$; por la Proposición 6.2.9, se tiene que el cociente de Herbrand es $h(K_v^\times) = p/|p|_v$, donde $|.|_v$ es un valor absoluto normalizado; por otra parte, como las raíces p-ésimas de la unidad están en $K_v^\times$, el cociente de Herbrand es igual a $(K_v^\times : K_v^{\times p})/p$. De esta manera, se tiene que

$$(K_v^\times : K_v^{\times p}) = p^2/|p|_v.$$

Así,

$$(\mathbb{I}_K^{S\cup T} : E) = p^{2s} \prod_{v\in S} 1/|p|_v = p^{2s} \tag{7}$$

por la fórmula del producto y el hecho de que $|p|_v = 1$ si $v \notin S$.

Notemos que por (7), para probar (6) bastará con ver que

$$(\mathcal{U}_K(S \cup T) : E \cap K^\times) = p^{2s-r} = p^{s+t}. \tag{8}$$

Como en (1), cambiando S por $S \cup T$, vemos que $(\mathcal{U}_K(S \cup T) : \mathcal{U}_K(S \cup T)^p) = p^{s+t}$. Por lo tanto, bastará ver que $E \cap K^\times = \mathcal{U}_K(S \cup T)^p$. Es claro que $\mathcal{U}_K(S \cup T)^p \subset E \cap K^\times$. La otra inclusión la deduciremos del siguiente resultado.

Lema. *Sea K tal que contiene a las raíces p-ésimas de la unidad. Sea S un conjunto finito de primos que satisface las condiciones* (I)*,* (II) *y* (III)*. Sea T un conjunto de primos disjunto de S, tal que la aplicación $\mathcal{U}_K(S) \to \prod_{v\in T} \mathcal{U}_v/\mathcal{U}_v^p$ es suryectiva. Entonces $E \cap K^\times \subset K^{\times p}$.*

Dem. del lema. Sea $b \in E \cap K^\times$ y consideremos $K' = K(b^{1/p})$. Bastará ver que $K' = K$. Sea

$$D = \prod_{v \in S} K_v^\times \times \prod_{v \in T} \mathcal{U}_v^p \times \prod_{v \notin S \cup T} \mathcal{U}_v.$$

Veremos que $D \subset \mathrm{N}_{K'/K}\, \mathbb{I}_{K'}$ y que $K^\times D = \mathbb{I}_K$, y el Corolario 7.2.4 implicará entonces que $K' = K$. Para ver que D está contenido en el grupo de normas, sea v un primo de K. Entonces la completación de K' respecto de un primo sobre v es $K_v(b^{1/p})$. Si $v \in S$, esto es K_v (pues $b \in E \cap K^\times$), con lo cual, todo elemento de K_v es una norma. Si $v \in T$, la teoría local de cuerpos de clases nos dice que el índice $(K_v^\times : \mathrm{N}\, K_v(b^{1/p})^\times)$ es igual al grado $[K_v(b^{1/p}) : K_v]$, que divide a p. Luego, toda potencia p-ésima es una norma. Finalmente, si $v \notin S \cup T$, $K_v(b^{1/p})$ es no ramificada sobre K_v pues pb es una unidad en v; luego, toda unidad es una norma.

Veamos ahora que $\mathbb{I}_K = K^\times D$. Es claro que $\mathbb{I}_K^S/D \simeq \prod_{v \in T} \mathcal{U}_v/\mathcal{U}_v^p$, y, por hipótesis, $\mathcal{U}_K(S) \to \prod_{v \in T} \mathcal{U}_v/\mathcal{U}_v^p$ es suryectiva. Por lo tanto, $\mathbb{I}_K^S = D\mathcal{U}_K(S)$ e $\mathbb{I}_K = K^\times \mathbb{I}_K^S = K^\times D\mathcal{U}_K(S) = K^\times D$, como queríamos probar. □

Debemos deducir la otra inclusión. Sólo necesitamos ver que la aplicación $\mathcal{U}_K(S) \to \prod_{v \in T} \mathcal{U}_v/\mathcal{U}_v^p$ es suryectiva. Sea H su núcleo. Basta ver que $(\mathcal{U}_K(S) : H) = \prod_{v \in T} (\mathcal{U}_v : \mathcal{U}_v^p)$. Por la Proposición 6.2.9, el cociente de Herbrand de $\mathcal{U}_v$ es $1/|p|_v$, y como $\mathcal{U}_v$ contiene a las raíces p-ésimas de 1, vale que $\prod_{v \in T} (\mathcal{U}_v : \mathcal{U}_v^p) = \prod_{v \in T} p/|p|_v$, que es igual a p^t ya que $|p|_v = 1$ si $v \in T$. Por otra parte, $H = L^{\times p} \cap \mathcal{U}_K(S)$, por (4), y entonces $(\mathcal{U}_K(S) : H) = p^t$ por (2). □

Corolario 7.4.4. *Sea L/K finita y abeliana con grupo de Galois G. Supongamos que existe un mapa de Artin $\phi_{L/K}$ como en la Definición* 4.3.5. *Entonces induce un isomorfismo*

$$\mathbf{C}_K \,/\, \mathrm{N}_{L/K}\, \mathbf{C}_L \to G.$$

Dem. El corolario 7.2.6 implica que $\phi_{L/K}$ debe ser suryectivo. Como su núcleo contiene a $K^\times \mathrm{N}_{L/K}\, \mathbb{I}_L$, la segunda desigualdad implica que debe ser un isomorfismo. □

7.5. Grupo de Brauer e invariantes

Sea L/K una extensión finita de Galois de cuerpos de números, de grado n, con grupo de Galois G. En la sección anterior vimos que $H^1(G, \mathbf{C}_L) = 0$; luego, la sucesión exacta corta $0 \to L^\times \to \mathbb{I}_L \to \mathbf{C}_L \to 0$ da lugar a una sucesión exacta $0 \to H^2(G, L^\times) \to H^2(G, \mathbb{I}_L) \to H^2(G, \mathbf{C}_L)$. Pero

$$H^2(G, L^\times) = \mathrm{Br}(L/K)$$

y

$$H^2(G, \mathbb{I}_L) = \bigoplus_v H^2(G^v, (L^v)^\times) = \bigoplus_v \mathrm{Br}(L^v/K_v)$$

(Proposición 7.1.2). Luego, se tiene una aplicación inyectiva $\mathrm{Br}(L/K) \to \bigoplus_v \mathrm{Br}(L^v/K_v)$. Si $\alpha \in \mathrm{Br}(L/K)$, llamamos α_v a su componente v-ésima en esta suma, y definimos $\mathrm{inv}_v(\alpha) = \mathrm{inv}_v(\alpha_v)$, donde $\mathrm{inv}_v : \mathrm{Br}(L^v/K_v) \subset \mathrm{Br}(K_v) \to \mathbb{Q}/\mathbb{Z}$ es el isomorfismo del Teorema 6.2.1. Tiene sentido considerar $\sum_v \mathrm{inv}_v(\alpha)$, pues sólo finitos α_v son no nulos.

Queremos extender esto ahora a cualquier $\alpha \in \mathrm{Br}(K)$. Sabemos que $\alpha \in \mathrm{Br}(L/K)$ para una extensión L/K finita de Galois. Debemos probar que $\mathrm{inv}_v(\alpha)$ no depende de tal extensión. Supongamos que $\alpha \in \mathrm{Br}(M/K)$, y sea $L' = ML$. Para cada v, sea w un primo de L sobre v, y w' un primo de L' sobre w'. Se tiene un diagrama conmutativo:

$$\begin{array}{ccc}
\mathrm{Br}(L/K) & \xrightarrow{\mathrm{Inf}} & \mathrm{Br}(L'/K) \\
\downarrow & & \downarrow \\
\bigoplus_v \mathrm{Br}(L_w/K_v) & & \bigoplus_v \mathrm{Br}(L'_{w'}/K_v) \\
\downarrow{\scriptstyle p_v} & & \downarrow{\scriptstyle p_v} \\
\mathrm{Br}(L_w/K_v) & \xrightarrow{\mathrm{Inf}} & \mathrm{Br}(L'_{w'}/K_v) \\
\downarrow{\scriptstyle \mathrm{inv}_v} & & \downarrow{\scriptstyle \mathrm{inv}_v} \\
\mathbb{Q}/\mathbb{Z} & \xrightarrow{\mathrm{id}} & \mathbb{Q}/\mathbb{Z}.
\end{array}$$

Para ver que el cuadrado de arriba conmuta, hay que utilizar la expresión explícita en términos de cociclos del isomorfismo de la Proposición 7.1.2; el de abajo conmuta por 6.2.4. Luego, $\mathrm{inv}_v(\alpha)$ (tomado con respecto a L/K) es igual a $\mathrm{inv}_v(\mathrm{Inf}(\alpha))$ (tomado con respecto a L'/K). Por simetría, vale lo mismo para M, y se sigue que inv_v da lo mismo con L que con M. Se tiene entonces una aplicación

$$\mathrm{inv}_v : \mathrm{Br}(K) \to \mathbb{Q}/\mathbb{Z}.$$

Podemos hacer algo más: si para cada extensión L/K como recién, cambiamos $\mathrm{Br}(L/K)$ por $H^2(\mathrm{Gal}(L/K), \mathbb{I}_L)$, vale exactamente lo mismo, sólo nos tenemos que olvidar de la aplicación $\mathrm{Br}(K) \to \bigoplus_v \mathrm{Br}(L^v/K_v)$. Luego, si definimos $H^2(G^s, \mathbb{I}_{K^s})$ como el límite directo de los $H^2(\mathrm{Gal}(L/K), \mathbb{I}_L)$, con L/K recorriendo las extensiones finitas de Galois, sigue valiendo que el límite es una unión (probar como ejercicio los resultados sobre grupos de Brauer de la Sección 5.8 para estos grupos) y tenemos definido

$$\mathrm{inv}_v : H^2(G^s, \mathbb{I}_{K^s}) \to \mathbb{Q}/\mathbb{Z},$$

que consiste en "pegar" las aplicaciones $\mathrm{inv}_v : H^2(\mathrm{Gal}(L/K), \mathbb{I}_L) \simeq \bigoplus_v \mathrm{Br}(L^v/K_v) \to \mathbb{Q}/\mathbb{Z}$.

7.6. Ley de reciprocidad

Completaremos aquí la demostración de los Teoremas 4.5.1 y 4.5.2. Sea L/K finita y abeliana, con grupo de Galois G. Por lo visto hasta aquí, sólo necesitamos construir el mapa de Artin $\phi_{L/K}$.

Sea v un primo (finito) de K. Si w y w' son primos de L sobre v, sea $\sigma \in \mathrm{Gal}(L/K)$ tal que $w' = \sigma w$. Sean Ω, Ω' clausuras abelianas de K_v que contengan a L_w y a $L_{w'}$ respectivamente, y sean K_v^{nr} y $K_v^{nr'}$ las extensiones maximales no ramificadas de K_v en Ω y en Ω' respectivamente. El isomorfismo $\sigma_w : L_w \to L_{w'}$ se extiende a un isomorfismo $\widetilde{\sigma} : \Omega \to \Omega'$

y da lugar a un isomorfismo θ entre $\mathrm{Gal}(\Omega/K_v)$ y $\mathrm{Gal}(\Omega'/K_v)$, dado por $\tau \mapsto \widetilde{\sigma}\tau\widetilde{\sigma}^{-1}$. Sean $\phi_v : K_v^\times \to \mathrm{Gal}(\Omega/K_v)$ y $\phi'_v : K_v^\times \to \mathrm{Gal}(\Omega'/K_v)$ los mapas de reciprocidad locales de la Sección 6.1. Utilizando la caracterización dada en el Teorema 6.2.11, es fácil ver que $\theta\phi_v = \phi'_v$. Luego, viendo a $\mathrm{Gal}(L_w/K_v)$ y a $\mathrm{Gal}(L_{w'}/K_v)$ dentro de $\mathrm{Gal}(L/K)$ como el grupo de descomposición G^v, se deduce que $\phi_v : K_v^\times \to G^v$ es independiente del primo que tomemos arriba de v. En el caso de v infinito la afirmación es trivial.

Definimos $\phi_{L/K} : \mathbb{I}_K \to G$ como el producto de todos los mapas de reciprocidad locales:

$$\phi_{L/K}(x) = \prod_v \phi_v(x_v).$$

Esta definición es correcta, ya que para casi todo v, $x_v \in \mathcal{U}_v$ y v es no ramificado, y por el Corolario 6.2.8 se tiene que x_v es una norma y, por lo tanto, $\phi_v(x_v) = 1$.

Sea S el conjunto de primos ramificados de L/K. Si v es un primo infinito no ramificado entonces el mapa de reciprocidad local ϕ_v es trivial; si v es finito no ramificado, sea $\psi_v \in G^v$ el morfismo de Frobenius de L^v/K_v. Por la Proposición 6.2.11, $\phi_v(x_v) = \psi_v^{\mathrm{ord}_v(x_v)}$. En consecuencia,

$$\phi_{L/K}(x) = \prod_{v\notin S, v<\infty} \psi_v^{\mathrm{ord}_v(x_v)} \quad \text{si } x \in \mathbb{I}_{K,S}.$$

Es muy fácil ver que $\psi_v = \psi_{L/K}(v)$, utilizando la caracterización de ambos. Se sigue entonces que $\phi_{L/K}(x) = \psi_{L/K}(\mathrm{id}(x))$ si $x \in \mathbb{I}_{K,S}$.

Por otra parte, es claro que $\phi_{L/K}$ es continuo pues su núcleo contiene a $\mathrm{N}_{L/K}\,\mathbb{I}_L$, que es un abierto de $\mathbb{I}_K$. Luego, $\phi_{L/K}$ cumple dos de las propiedades que se necesitan para que valga la ley de reciprocidad. El punto crucial es probar que se anula en $K^\times$.

Para terminar de probar el Teorema 4.5.1, enunciaremos dos resultados que relacionaremos luego.

Teorema 7.6.1. (a) *Para toda extensión finita y abeliana L/K, la función definida arriba $\phi_{L/K}$ se anula en $K^\times$.*

(b) $\sum_v \mathrm{inv}_v(\alpha) = 0$ *para todo* $\alpha \in \mathrm{Br}(K)$.

Lo que necesitamos demostrar es la parte (a). La idea será la siguiente:

Paso 1. Probar (a) para extensiones L/K finitas ciclotómicas (esto es, $L \subset K(\zeta)$ para ζ una raíz primitiva de la unidad).

Paso 2. Deducir (b) para $\alpha \in \mathrm{Br}(L/K)$, con L/K ciclotómica cíclica.

Paso 3. Deducir (b) para $\alpha \in \mathrm{Br}(K)$ arbitrario.

Paso 4. Deducir (a) para toda L/K abeliana finita.

Necesitaremos algunos lemas técnicos para relacionar (a) con (b). Sea L/K finita de Galois, con grupo de Galois G. Consideremos el isomorfismo $H^q(G, \mathbb{I}_L) \to \bigoplus_v H^q(G^v, (L^v)^\times)$ de la Proposición 7.1.2, y llamémoslo momentáneamente η.

Lema 7.6.2. *El siguiente diagrama es conmutativo:*

$$\begin{array}{ccc} H^q(G,\mathbb{I}_L) & \xrightarrow{\eta} & \bigoplus_v H^q(G^v,(L^v)^\times) \\ \downarrow{\scriptstyle \mathrm{Res}} & & \downarrow{\scriptstyle p_v} \\ H^q(G^v,\mathbb{I}_L) & \xrightarrow{a_v^*} & H^q(G^v,(L^v)^\times), \end{array}$$

donde p_v es la proyección y a_v^* es la inducida por la proyección $a_v : \mathbb{I}_L \to (L^v)^\times$.

Dem. La omitimos. Consiste en una verificación directa con q-cociclos y la expresión explícita de los cuatro morfismos en términos de ella. □

Sea L/K finita y abeliana. Dado $\chi \in \mathrm{Hom}(G,\mathbb{Q}/\mathbb{Z}) = H^1(G,\mathbb{Z})$ un carácter de G, sea $\delta\chi \in H^2(G,\mathbb{Z})$ la imagen por el morfismo de conexión. Para cada primo v, sea χ_v la restricción al grupo de descomposición G^v. Dado $x \in \mathbb{I}_K$, sea $\overline{x}$ su imagen en $\mathbb{I}_K/\,\mathrm{N}_{L/K}\,\mathbb{I}_L = \widehat{H}^0(G,\mathbb{I}_L)$. Entonces se tiene el producto "cup" $\overline{x}.\delta\chi \in H^2(G,\mathbb{I}_L)$.

Lema 7.6.3. *Con las notaciones de recién, se tiene que*

$$\mathrm{inv}_v(\overline{x}.\delta\chi) = \chi_v(\phi_v(x_v)),$$

y, por lo tanto,

$$\sum_v \mathrm{inv}_v(\overline{x}.\delta\chi) = \chi(\phi_{L/K}(x)).$$

Dem. Usando las notaciones del último lema, se tiene que $\mathrm{inv}_v(\overline{x}.\delta\chi) = \mathrm{inv}_v(p_v(\eta(\overline{x}.\delta\chi)))$ por definición de $\mathrm{inv}_v : H^2(G,\mathbb{I}_L) \to \mathbb{Q}/\mathbb{Z}$. Pero el lema implica que esto es igual a

$$\mathrm{inv}_v(a_v^*(\mathrm{Res}(\overline{x}.\delta\chi))).$$

Por la Proposición 5.5.2, esto es

$$\mathrm{inv}_v(a_v^*(\mathrm{Res}(\overline{x}).\,\mathrm{Res}(\delta\chi))).$$

Pero $\mathrm{Res}(\delta\chi)) = \delta\chi_v$, y como $a_v^*(\mathrm{Res}(\overline{x})) = \overline{x_v}$ (clase en $K_v/\,\mathrm{N}_{L^v/K_v}(L^v)^\times$), las propiedades funtoriales del producto "cup" implican que

$$\mathrm{inv}_v(\overline{x}.\delta\chi) = \mathrm{inv}_v(\overline{x_v}.\delta\chi_v) = \chi_v(\phi_v(x_v)).$$

La última igualdad se sigue de la teoría local ([CaF67]). La otra afirmación del lema se sigue inmediatamente por definición de $\phi_{L/K}$. □

Paso 4. Aplicamos el último lema con $x \in K^\times$; sea $\widetilde{x}$ su imagen en $\widehat{H}^0(G,L^\times)$. Entonces $\widetilde{x}.\delta\chi \in H^2(G,L^\times) \subset \mathrm{Br}(K)$ para todo χ carácter de G. Sea $\overline{x}$ la imagen de x en $\widehat{H}^0(G,\mathbb{I}_L)$, de manera que $\overline{x}.\delta\chi \in H^2(G,\mathbb{I}_L)$; por la funtorialidad del producto "cup", $\overline{x}.\delta\chi$ es la imagen

de $\widetilde{x}.\delta\chi$ via la aplicación $H^2(G, L^\times) \to H^2(G, \mathbb{I}_L)$ inducida por $L^\times \hookrightarrow \mathbb{I}_L$. Además, el lema implica que

$$\chi(\phi_{L/K}(x)) = \sum_v \mathrm{inv}_v(\overline{x}.\delta\chi),$$

con lo cual, si (b) vale para cualquier $\alpha \in \mathrm{Br}(K)$, se tiene que $\chi(\phi_{L/K})) = 0$. Como esto vale para todo χ, se sigue que $\phi_{L/K}(x) = 1$ si $x \in K^\times$.

Paso 2. Probaremos en realidad que si vale (a) para una extensión finita cíclica entonces vale (b) para $\alpha \in \mathrm{Br}(L/K)$, con L/K cíclica. Sea s un generador de G y χ^s como en la Observación 5.6.3. Entonces la aplicación $\widehat{H}^0(G, L^\times) \to H^2(G, L^\times)$ que consiste en tomar producto "cup" con χ^s es un isomorfismo; esto implica que todo elemento de $H^2(G, L^\times)$ es de la forma $\widetilde{x}.\delta\chi^s$. Si vale (a) para L/K entonces el lema implica que

$$\sum_v \mathrm{inv}_v(\overline{x}.\delta\chi^s) = \chi^s(\phi_{L/K}(x)) = 0,$$

donde $\overline{x}$ es la imagen en $\widehat{H}^0(G, \mathbb{I}_L)$. Esto implica (b).

Paso 1. Reduciremos todo al caso en que el cuerpo de base sea $\mathbb{Q}$ y la extensión sea $\mathbb{Q}(\zeta_m)/\mathbb{Q}$.

Lema 7.6.4. *Si el Teorema 7.6.1(a) vale para L/K y $K \subset K' \subset L$ entonces vale para K'/K.*

Dem. Se sigue de que $\phi_{K'/K}$ es la composición de $\phi_{L/K}$ con $\mathrm{Gal}(L/K) \to \mathrm{Gal}(K'/K)$, lo cual se debe a que es cierto para los mapas de Artin locales. □

El último lema implica que podemos suponer que $L = K(\zeta)$. Ahora lo reduciremos al caso $K = \mathbb{Q}$. Sea $M = \mathbb{Q}(\zeta)$ y sean $G' = \mathrm{Gal}(L/K)$ y $G = \mathrm{Gal}(M/\mathbb{Q})$. Entonces $L = MK$, y se tiene una inyección natural $G' \hookrightarrow G$. El siguiente diagrama es conmutativo:

$$\begin{array}{ccc} \mathbb{I}_K & \xrightarrow{\phi_{L/K}} & G' \\ {\scriptstyle \mathrm{N}_{K/\mathbb{Q}}}\downarrow & & \downarrow \\ \mathbb{I}_{\mathbb{Q}} & \xrightarrow{\phi_{M/\mathbb{Q}}} & G. \end{array}$$

La conmutatividad se sigue de la definición de la norma y de "pegar" los diagramas conmutativos del caso local. Dejamos los detalles como ejercicio.

Sea entonces $x \in K^\times$. Si vale el Teorema 7.6.1(a) para $M/\mathbb{Q}$, entonces $\mathrm{N}_{K/\mathbb{Q}}(x) \in \mathbb{Q}^\times$ y, por lo tanto, $\phi_{M/\mathbb{Q}}\,\mathrm{N}_{K/\mathbb{Q}}(x) = 1$. Como $G' \to G$ es inyectiva, se sigue que $\phi_{L/K}(x) = 1$.

Veamos que $\phi_{\mathbb{Q}(\zeta_m)/\mathbb{Q}}(x) = 1$ si $x \in \mathbb{Q}^\times$. Basta ver que $\phi_{\mathbb{Q}(\zeta_m)/\mathbb{Q}}(x)\,\big|_{\mathbb{Q}(\zeta_{\ell^r})} = 1$ para todo primo ℓ tal que $\ell^r | m$ y $\ell^{r+1} \nmid m$. Por lo tanto, podemos suponer que $m = \ell^r \neq 2$. Además, por multiplicatividad basta ver que vale en los casos $x = -1$, $x = \ell$ y $x = q$ un primo distinto de ℓ.

Por definición, $\phi_{\mathbb{Q}(\zeta_m)/\mathbb{Q}}(x) = \prod_p \phi_p(x)$, donde

$$\phi_p = \phi_{\mathbb{Q}_p(\zeta_m)/\mathbb{Q}_p} : \mathbb{Q}_p^\times \to \mathrm{Gal}(\mathbb{Q}_p(\zeta_m)/\mathbb{Q}_p).$$

Utilizamos la caracterización dada en la Sección 6.3, y obtenemos que, haciendo la identificación $(\mathbb{Z}/m\mathbb{Z})^\times \simeq \mathrm{Gal}(\mathbb{Q}(\zeta_m)/\mathbb{Q})$ dada por $[n] \longleftrightarrow (\zeta_m \mapsto \zeta_m^n)$,

$$\phi_p(-1) = \begin{cases} [1], & p \neq l, \infty; \\ [-1], & p = l, \infty. \end{cases}$$

$$\phi_p(q) = \begin{cases} [1], & p = \infty, p \neq q, l, \infty; \\ [q], & p = q; \\ [q^{-1}], & p = l. \end{cases}$$

$$\phi_p(l) = [1] \ \ \forall p.$$

En cualquier caso, $\prod_p \phi_p(x) = 1$.

Paso 3. Basta probar que todo $\alpha \in \mathrm{Br}(K)$ se parte por una extensión ciclotómica cíclica. Sea L/K una extensión finita de Galois cualquiera. Entonces $\alpha \in \mathrm{Br}(L/K)$ si y sólo si está en el núcleo de $\mathrm{Res}_{K/L} : \mathrm{Br}(K) \to \mathrm{Br}(L)$. Pero un elemento $\beta \in \mathrm{Br}(L)$ es 0 si y sólo si $\mathrm{inv}_w(\beta) = 0$ para todo primo w de L (ya que $\mathrm{Br}(L)$ se inyecta en la suma directa de los grupos de Brauer locales). Utilizando explícitamente con cociclos el isomorfismo de la Proposición 7.1.2, y reduciendo al caso local (Proposición 6.2.2), es fácil ver que si $w|v$ entonces $\mathrm{inv}_w(\mathrm{Res}_{K/L}(\alpha)) = [L_w : K_v]\,\mathrm{inv}_v(\alpha)$. Luego, $\alpha \in \mathrm{Br}(L/K)$ si y sólo si $[L_w : K_v]\,\mathrm{inv}_v(\alpha) = 0$ para todo primo w de L y todo primo v debajo. Notemos que $\mathrm{inv}_v(\alpha) = 0$ para casi todo v, con lo cual, son finitas condiciones. Luego, existe m tal que $m\,\mathrm{inv}_v(\alpha) = 0$ (en $\mathbb{Q}/\mathbb{Z}$) para todo v. El siguiente lema termina entonces con la demostración del Paso 3.

Lema 7.6.5. *Sea K un cuerpo de números, S un conjunto finito de primos de K y $m \in \mathbb{N}$. Entonces existe una extensión L/K cíclica, ciclotómica, tal que los grados locales son divisibles por m en los primos finitos de S y por 2 en los primos reales de S.*

Dem. Dejamos como ejercicio fácil ver que es suficiente considerar $K = \mathbb{Q}$ (para el caso general, tomar $m[K : \mathbb{Q}]$). Sea q un primo de $\mathbb{Z}$ y r arbitrario (grande). Consideremos la extensión $L(q) = \mathbb{Q}(\zeta)$, donde ζ es una raíz q^r-ésima primitiva de la unidad. El grupo de Galois de $L(q)$ sobre $\mathbb{Q}$ es isomorfo a la suma directa de un grupo cíclico de orden $q-1$ y un grupo cíclico de orden q^{r-1} si q es impar, mientras que $\mathrm{Gal}(L(2)/\mathbb{Q})$ es isomorfo a la suma directa de un grupo cíclico de orden 2 y otro de orden 2^{r-2}. Por lo tanto, existe una subextensión $L'(q)$ cíclica ciclotómica de grado q^{r-1} si q es impar, de grado 2^{r-2} si $q = 2$.

Consideremos $\mathbb{Q}_p(\zeta)$, donde p es un primo finito de $\mathbb{Q}$. Sabemos que el grado local $[\mathbb{Q}_p(\zeta) : \mathbb{Q}_p]$ es igual a $e_p f_p$, donde e_p, f_p son el grado de ramificación y de inercia de p en la extensión $L(q)/\mathbb{Q}$. Utilizaremos los resultados enunciados en el Ejemplo 1.1.13. Si $p = q$, $e_p = \varphi(q^r)$ y $f_p = 1$; si $p \neq q$, $e_p = 1$ y f_p es el orden multiplicativo de p módulo q^r. En cualquier caso, se tiene que $[\mathbb{Q}_p(\zeta) : \mathbb{Q}_p] \to \infty$ cuando $r \to \infty$.

Como $[L(q) : L'(q)] = q-1$ si q es impar y $[L(2) : L'(2)] = 2$, localizando en cada primo $p < \infty$, se tiene que $[L(q)^p : L'(q)^p] \leq q-1$ y $[L(2)^p : L'(2)^p] \leq 2$. Obtenemos entonces que $[L'(q)^p : \mathbb{Q}_p]$ es una potencia de q que tiende a ∞ cuando r tiende a ∞.

Supongamos que los factores primos de m son $q_1, \ldots, q_n$ (impares) y eventualmente 2. Consideramos L el compuesto de las extensiones $L'(q_1), \ldots, L'(q_n)$ y eventualmente $L'(2)$. Es una extensión de $\mathbb{Q}$, cíclica ciclotómica, y los grados locales cumplen lo requerido si tomamos r suficientemente grande (para el eventual primo del infinito, notar que $L'(q)/\mathbb{Q}$ es una extensión totalmente compleja para todo q, esto es, toda inmersión en $\mathbb{C}$ es no real). □

7.7. Clases fundamentales

Sea L/K una extensión finita de Galois de grado n, con grupo de Galois G. Nuestro objetivo será probar que $H^2(G, \mathbf{C}_L)$ es cíclico de orden n.

Consideremos el siguiente diagrama:

$$\begin{array}{ccccccc} & & & & & & H^2(G, \mathbf{C}_L) \\ & & & & & \nearrow & \\ 0 & \longrightarrow & \mathrm{Br}(L/K) & \longrightarrow & H^2(G, \mathbb{I}_L) & & \\ & & & & & \searrow^{\sum} & \\ & & & & & & \mathbb{Q}/\mathbb{Z}. \end{array}$$

La fila de arriba es la sucesión exacta larga de cohomología; la última aplicación no tiene que ser necesariamente suryectiva. Notamos con $H^2(G, \mathbf{C}_L)'$ a su imagen. La aplicación $\sum$ consiste en sumar los invariantes locales.

Como la imagen de inv_v es el grupo cíclico $\frac{1}{n_v}\mathbb{Z}/\mathbb{Z}$ (n_v = grado local), se sigue que la imagen de $\sum$ es el grupo cíclico $\frac{1}{n_0}\mathbb{Z}/\mathbb{Z}$, donde n_0 es el mínimo común múltiplo de los n_v (notemos que hay sólo finitos n_v pues todos dividen a n). Observemos que n divide a n_0, pero no es cierto que siempre sean iguales.

En la sección anterior, probamos que la fila de abajo del diagrama es un complejo, es decir, la composición de las dos aplicaciones es cero. Esto implica que podemos definir un morfismo suryectivo

$$H^2(G, \mathbf{C}_L)' \to \frac{1}{n_0}\mathbb{Z}/\mathbb{Z}.$$

Notando con $H^2(G^s, \mathbf{C}_{K^s})'$ al límite de los $H^2(G, \mathbf{C}_L)'$, obtenemos el diagrama

$$\begin{array}{ccccccc} & & & & & & H^2(G^s, \mathbf{C}_{K^s}) \\ & & & & & \nearrow & \\ 0 & \longrightarrow & \mathrm{Br}(K) & \longrightarrow & H^2(G^s, \mathbb{I}_{K^s}) & & \\ & & & & & \searrow^{\sum} & \\ & & & & & & \mathbb{Q}/\mathbb{Z} \end{array}$$

y podemos definir un morfismo $H^2(G^s, \mathbf{C}_{K^s})' \to \mathbb{Q}/\mathbb{Z}$.

Supongamos que L/K cumple que $n_0 = n$. Entonces:

(a) La aplicación $H^2(G, \mathbf{C}_L)' \to \frac{1}{n}\mathbb{Z}/\mathbb{Z}$ es un isomorfismo (pues es suryectiva y

$$(H^2(G, \mathbf{C}_L)' : 1) \leq (H^2(G, \mathbf{C}_L) : 1) \leq n$$

por el Teorema 7.4.1).

(b) $H^2(G, \mathbf{C}_L)' = H^2(G, \mathbf{C}_L)$ y ambos tienen orden n.

(c) La sucesión

$$0 \longrightarrow \mathrm{Br}(L/K) \longrightarrow H^2(G, \mathbb{I}_L) \xrightarrow{\Sigma} \tfrac{1}{n}\mathbb{Z}/\mathbb{Z} \longrightarrow 0$$

es exacta.

Lema 7.7.1. *Si L/K es cíclica entonces $n = n_0$.*

Dem. Sea $S \supset S_\infty$ un conjunto de primos que contenga a los ramificados. Sabemos que $\psi_{L/K} : I_K^S \to \mathrm{Gal}(L/K)$ es suryectivo, y al ser $\mathrm{Gal}(L/K)$ cíclico existe v primo finito fuera de S tal que $\psi_{L/K}(v)$ genera $\mathrm{Gal}(L/K)$; en particular, tiene orden n. Pero el orden de $\psi_{L/K}(v)$ es $f_v = n_v$ y, por lo tanto, $n_v = n$. En consecuencia $n \leq n_0$ y, por lo tanto, deben ser iguales. □

En particular, si L/K es una extensión ciclotómica cíclica,

$$0 \longrightarrow \mathrm{Br}(L/K) \longrightarrow H^2(G, \mathbb{I}_L) \xrightarrow{\Sigma} \tfrac{1}{[L:K]}\mathbb{Z}/\mathbb{Z} \longrightarrow 0$$

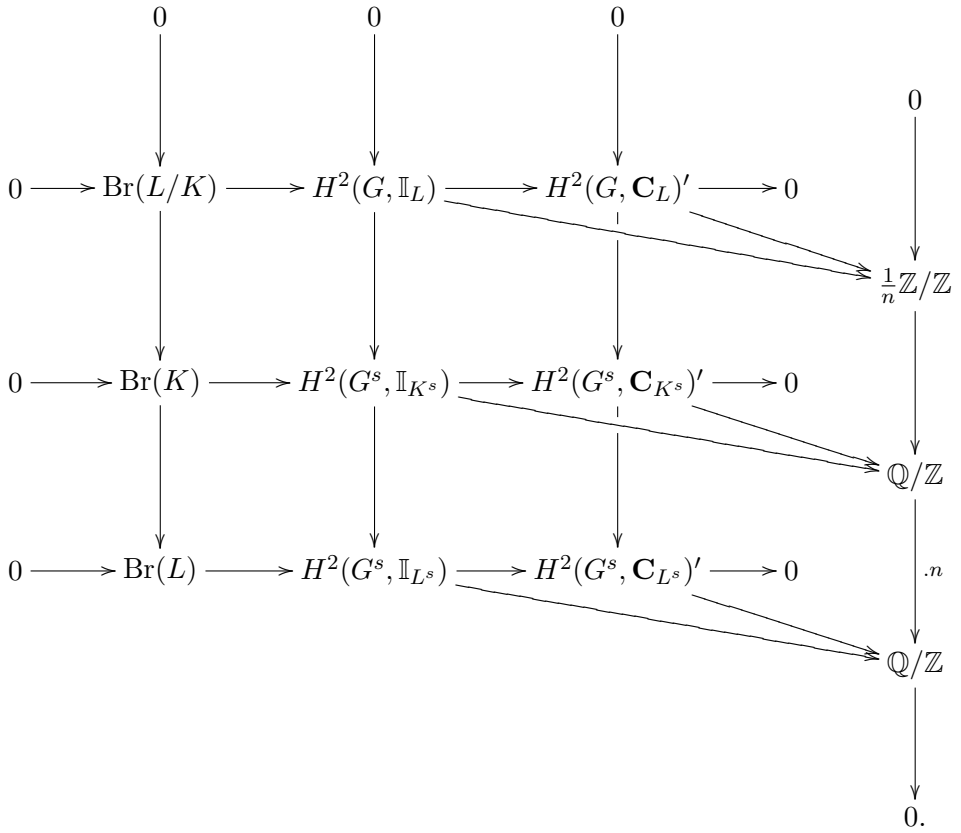
es exacta. Como para cada n existe una extensión ciclotómica cíclica de grado al menos n (usar el Lema 7.6.5 con un primo finito fijo) y $\mathrm{Br}(K)$ (respectivamente $H^2(G^s, \mathbb{I}_{K^s})$) es el límite directo (unión directa) de los $\mathrm{Br}(L/K)$ (respectivamente $H^2(G, \mathbb{I}_L)$), donde L/K recorre tales extensiones (ver el paso 3 de la sección anterior y notar que las observaciones anteriores al Lema 7.6.5 son válidas para $\alpha \in H^2(G^s, \mathbb{I}_{K^s})$), se tiene la siguiente sucesión exacta:

$$0 \longrightarrow \mathrm{Br}(K) \longrightarrow H^2(G^s, \mathbb{I}_{K^s}) \xrightarrow{\Sigma} \mathbb{Q}/\mathbb{Z} \longrightarrow 0.$$

Se la denomina *sucesión exacta fundamental* de la teoría global de cuerpos de clases.

Recordemos (Sección 5.8) que la sucesión $0 \to \mathrm{Br}(L/K) \to \mathrm{Br}(K) \to \mathrm{Br}(L)$ se obtiene pasando al límite las sucesiones $0 \to \mathrm{Br}(L/K) \to \mathrm{Br}(E/K) \to \mathrm{Br}(E/L)$, con E/K finita de Galois que contiene a L. Razonando de la misma manera con los idèles o con el grupo de clases de idèles (usando que $H^1(G, \mathbb{I}_L) = H^1(G, \mathbf{C}_L) = 0$), obtenemos el siguiente gran diagrama

conmutativo tridimensional:



En efecto, lo único que nos resta probar es la conmutatividad del diagrama

$$\begin{array}{ccc} H^2(G^s, \mathbb{I}_{K^s}) & \longrightarrow & \mathbb{Q}/\mathbb{Z} \\ \downarrow & & \downarrow .n \\ H^2(G^s, \mathbb{I}_{L^s}) & \longrightarrow & \mathbb{Q}/\mathbb{Z}, \end{array}$$

y para ello basta ver que si $E \supset L \supset K$ es tal que E/L y E/K son finitas de Galois entonces

$$\begin{array}{ccc} H^2(\mathrm{Gal}(E/K), \mathbb{I}_E) & \xrightarrow{\Sigma} & \mathbb{Q}/\mathbb{Z} \\ \downarrow \mathrm{Res} & & \downarrow .n \\ H^2(\mathrm{Gal}(E/L), \mathbb{I}_E) & \xrightarrow{\Sigma} & \mathbb{Q}/\mathbb{Z} \end{array}$$

lo es, pues el primer diagrama se obtiene de éste por paso al límite. Esto se hace reduciendo al caso local y usando la Proposición 6.2.2.

Afirmamos ahora que la aplicación $H^2(G^s, \mathbf{C}_{K^s})' \to \mathbb{Q}/\mathbb{Z}$ es biyectiva. La suryectividad se sigue inmediatamente de que $H^2(G^s, \mathbb{I}_{K^s}) \to \mathbb{Q}/\mathbb{Z}$ lo es. Por la misma razón, si un elemento va

a parar a cero en $\mathbb{Q}/\mathbb{Z}$, proviene de un elemento de $H^2(G^s, \mathbb{I}_{K^s})$ que va a parar a cero, y, por lo tanto, de un elemento de $\mathrm{Br}(K)$; luego, es cero. De la misma manera se ve que $H^2(G^s, \mathbf{C}_{L^s}) \to \mathbb{Q}/\mathbb{Z}$ también es biyectiva. Tenemos entonces el siguiente diagrama conmutativo de filas exactas:

$$\begin{array}{ccccccccc} 0 & \longrightarrow & \frac{1}{n}\mathbb{Z}/\mathbb{Z} & \longrightarrow & \mathbb{Q}/\mathbb{Z} & \xrightarrow{\cdot n} & \mathbb{Q}/\mathbb{Z} & \longrightarrow & 0 \\ & & \uparrow & & \uparrow & & \downarrow & & \\ 0 & \longrightarrow & H^2(G, \mathbf{C}_L)' & \longrightarrow & H^2(G^s, \mathbb{I}_{K^s}) & \longrightarrow & H^2(G^s, \mathbb{I}_{L^s}). & & \end{array}$$

Usando el hecho de que las flechas verticales del medio y de la derecha son isomorfismos, es muy fácil ver que la de la izquierda es suryectiva. Pero $H^2(G, \mathbf{C}_L)'$ es un subgrupo de $H^2(G, \mathbf{C}_L)$, cuyo orden divide a n por el Teorema 7.4.1. Se sigue entonces que

$$H^2(G, \mathbf{C}_L)' = H^2(G, \mathbf{C}_L) \simeq \frac{1}{n}\mathbb{Z}/\mathbb{Z},$$

y, por lo tanto, $H^2(G, \mathbf{C}_L)$ es cíclico de orden n. Llamamos inv_K al isomorfismo $H^2(G, \mathbf{C}_L) \simeq \frac{1}{n}\mathbb{Z}/\mathbb{Z}$, y al generador $u_{L/K}$ que provenga de $\frac{1}{n}$ por esta aplicación lo llamamos *clase fundamental* de L/K.

Observemos que también hemos probado que en el diagrama tridimensional podemos suprimir las $'$.

Observación 7.7.2. Si L/K es una extensión finita de Galois, estamos en las hipótesis del Teorema de Tate (5.7.2), y se tienen isomorfismos

$$\widehat{H}^q(G, \mathbb{Z}) \to \widehat{H}^{q+2}(G, \mathbf{C}_L).$$

El caso $q = -2$ nos da un isomorfismo

$$G^{ab} \simeq \mathbf{C}_K \,/\, \mathrm{N}_{L/K}\, \mathbf{C}_L,$$

que no es otra cosa que la inversa del mapa de Artin. La razón de esto es que en el caso local se utilizan las mismas herramientas (Teorema de Tate), una vez probado que el H^2 es cíclico, y se *definen* los mapas de Artin locales de esta manera. Abstrayendo todas estas nociones en lo que Artin y Tate llaman *formaciones de clases*, se obtiene un tratamiento totalmente abstracto y cohomológico de la teoría de cuerpos de clases, tanto local como global.

El siguiente teorema elimina cualquier esperanza de que los grupos norma sirvan para clasificar extensiones no abelianas.

Teorema 7.7.3. *Sea E una extensión finita de K (no necesariamente de Galois), y M la máxima subextensión abeliana. Entonces*

$$\mathrm{N}_{E/K}\, \mathbf{C}_E = \mathrm{N}_{M/K}\, \mathbf{C}_M\,.$$

Dem. Sea L una extensión finita de Galois de K que contenga a E, con $G = \mathrm{Gal}(L/K)$ y $H = \mathrm{Gal}(L/E)$. Utilizando los isomorfismos que mencionamos recién, se tiene un diagrama conmutativo

$$\begin{array}{ccc} \widehat{H}^{-2}(H,\mathbb{Z}) & \xrightarrow{\simeq} & \widehat{H}^{0}(H,\mathbf{C}_L) \\ \downarrow{\scriptstyle \mathrm{Cor}} & & \downarrow{\scriptstyle \mathrm{Cor}} \\ \widehat{H}^{-2}(G,\mathbb{Z}) & \xrightarrow{\simeq} & \widehat{H}^{0}(G,\mathbf{C}_L), \end{array}$$

que se identifica con el diagrama

$$\begin{array}{ccc} H^{ab} & \xrightarrow{\simeq} & \mathbf{C}_E \,/\, \mathrm{N}_{L/E}\, \mathbf{C}_L \\ \downarrow & & \downarrow{\scriptstyle \mathrm{N}_{E/K}} \\ G^{ab} & \xrightarrow{\simeq} & \mathbf{C}_K \,/\, \mathrm{N}_{L/K}\, \mathbf{C}_L\,. \end{array}$$

Luego, el conúcleo de $H^{ab} \to G^{ab}$ es isomorfo a $\mathbf{C}_K \,/\, \mathrm{N}_{E/K}\, \mathbf{C}_E$. Pero a su vez, como M es la máxima subextensión abeliana de L contenida en E, es el cuerpo fijo de $G'H$. Por lo tanto, $\mathrm{Gal}(M/K) \simeq \mathrm{Gal}(L/K)/\mathrm{Gal}(L/M) = G/G'H \simeq (G/G')/(G'H)/G' \simeq \mathrm{coker}(H^{ab} \to G^{ab})$. De esta manera, $\mathbf{C}_K \,/\, \mathrm{N}_{E/K}$ es isomorfo a $\mathrm{Gal}(M/K)$, que por la ley de reciprocidad es isomorfo a $\mathbf{C}_K \,/\, \mathrm{N}_{M/K}\, \mathbf{C}_M$. Como $\mathrm{N}_{M/K}\, \mathbf{C}_M \supset \mathrm{N}_{E/K}\, \mathbf{C}_E$, se sigue que ambos grupos son iguales. □

Corolario 7.7.4. *Una extensión finita E/K es abeliana si y sólo si $(\mathbf{C}_K : \mathrm{N}_{E/K}\, \mathbf{C}_E) = [E : K]$.*

7.8. El teorema de existencia

Probaremos aquí el Teorema 4.5.4. Sea $N \subset \mathbf{C}_K$ un subgrupo abierto de índice finito. Diremos que N es un *grupo norma* si existe L/K finita y abeliana tal que $N = \mathrm{N}_{L/K}\, \mathbf{C}_L$.

Si N es un grupo norma y $N' \supset N$ entonces N' es un grupo norma. Esto se sigue mirando la demostración del Corolario 4.5.8.

Proposición 7.8.1. *Sea K un cuerpo de números tal que contiene una raíz p-ésima primitiva de la unidad (p un primo). Sea S un conjunto finito de primos que cumpla las condiciones* (I)*,* (II) *y* (III) *enunciadas en la demostración del Teorema 7.4.2. Sea $M = K(\mathcal{U}_K(S)^{1/p})$. Entonces*

$$K^\times \mathrm{N}_{M/K}\, \mathbb{I}_M = K^\times E, \text{ donde } E = \prod_{v\in S} K_v^{\times p} \times \prod_{v\notin S} \mathcal{U}_v.$$

Dem. Consideremos la demostración del Teorema 7.4.2. Tomemos $L = M$; entonces T es vacío, $t = 0$ y $s = r$. Además, el E que definimos allí es el mismo que definimos recién, y, por lo tanto, $E \subset \mathrm{N}_{M/K}\, \mathbb{I}_M$; además, $(\mathbb{I}_K^S : K^\times E) = p^s = [M : K]$. Por otra parte, por la ley de reciprocidad, $(\mathbb{I}_K : K^\times \mathrm{N}_{M/K}\, \mathbb{I}_M) = p^s$. Se sigue entonces el resultado. □

Lema Clave. *Sea p un primo y K un cuerpo de números tal que contiene una raíz p-ésima primitiva de 1. Entonces todo subgrupo abierto de $\mathbf{C}_K$ de índice p es un grupo norma.*

Dem. Sea N un tal subgrupo; sea H su preimagen en $\mathbb{I}_K$. Entonces H es un subgrupo abierto de $\mathbb{I}_K$; luego, existe un conjunto finito $S \supset S_\infty$ (que podemos agrandar tanto como queramos) tal que $H \supset \prod_{v\in S} 1 \times \prod_{v\notin S} \mathcal{U}_v$. Además, como $(\mathbf{C}_K : N) = p$, $\mathbb{I}_K^p \subset H$, y, por lo tanto, $H \supset \prod_{v\in S} K_v^{\times p} \times \prod_{v\notin S} \mathcal{U}_v = E$. Luego, $N = H/K^\times \supset EK^\times/K^\times$. Por la proposición anterior, N es un grupo norma. □

Lema 7.8.2. *Sea K'/K una extensión finita y $N \subset \mathbf{C}_K$ abierto. Si $N' = \mathrm{N}_{K'/K}^{-1}(N) \subset \mathbf{C}_{K'}$ es un grupo norma para K' entonces N es un grupo norma para K.*

Dem. Sea L/K' finita y abeliana tal que $\mathrm{N}_{L/K'} \mathbf{C}_L = N'$. Sea M la máxima subextensión abeliana de L/K. Por el Teorema 7.7.3,

$$\mathrm{N}_{M/K} \mathbf{C}_M = \mathrm{N}_{L/K} \mathbf{C}_L = \mathrm{N}_{K'/K}(N') \subset N.$$

Luego, N es un grupo norma pues contiene a otro. □

Dem. del Teorema de Existencia. Lo hacemos por inducción en el índice de N. Si es 1 entonces $N = \mathbf{C}_K = \mathrm{N}_{K/K} \mathbf{C}_K$.

Sea p un primo que divide al índice de N. Sea $K' = K(\zeta)$, donde ζ es una raíz p-ésima primitiva de la unidad, y sea $N' = \mathrm{N}_{K'/K}^{-1}(N)$. Por el último lema, basta ver que N' es un grupo norma. El índice de N' en $\mathbf{C}_{K'}$ divide al de N en $\mathbf{C}_K$, y podemos suponer que son iguales, ya que, en otro caso, la hipótesis inductiva nos asegura que N' es un grupo norma. Tenemos entonces que p divide a $(\mathbf{C}_{K'} : N')$, y, por lo tanto, $\mathbf{C}_{K'}/N'$ tiene un subgrupo de orden p. Luego, existe N_1' subgrupo de $\mathbf{C}_{K'}$ tal que $N_1' \supset N'$ y $(\mathbf{C}_{K'} : N_1') = p$. El lema clave anterior nos dice que N_1' es un grupo norma, y, por lo tanto, existe L/K' finita y abeliana tal que $N_1' = \mathrm{N}_{L/K'} \mathbf{C}_L$. Sea $N'' = \mathrm{N}_{L/K'}^{-1}(N')$. Consideremos entonces la aplicación

$$\mathrm{N}_{L/K'} : \mathbf{C}_L/N'' \to \mathbf{C}_{K'}/N',$$

que es un monomorfismo cuya imagen es N_1'/N'. Como este cociente está contenido propiamente en $\mathbf{C}_{K'}/N'$ (ya que $(\mathbf{C}_{K'} : N_1') = p > 1$), se tiene que

$$(\mathbf{C}_L : N'') < (\mathbf{C}_{K'} : N') = (\mathbf{C}_K : N).$$

Por hipótesis inductiva, N'' es un grupo norma, y el último lema implica entonces que N' lo es. □

Debemos probar ahora la unicidad. Sean L, L' dos extensiones finitas y abelianas contenidas en una clausura algebraica fija K^{al}. Sea M el compuesto de L con L', que es una extensión finita

y abeliana de K. Utilizando el Teorema 4.5.3, se tiene el siguiente diagrama conmutativo:

$$\begin{array}{ccc} \mathbf{C}_K \,/\, \mathrm{N}_{M/K}\, \mathbf{C}_M & \xrightarrow{\phi_{M/K}} & \mathrm{Gal}(M/K) \\ \downarrow & & \downarrow{\scriptstyle \mathrm{res}} \\ \mathbf{C}_K \,/\, \mathrm{N}_{L/K}\, \mathbf{C}_L & \xrightarrow{\phi_{L/K}} & \mathrm{Gal}(L/K). \end{array}$$

Como las flechas horizontales son isomorfismos, el núcleo de res, que es $\mathrm{Gal}(M/L)$ es la imagen isomorfa bajo $\phi_{M/K}$ de $\mathrm{N}_{L/K}\, \mathbf{C}_L \,/\, \mathrm{N}_{M/K}\, \mathbf{C}_M$. Luego, L, al ser el cuerpo fijo del núcleo de res, está determinado como subcuerpo de M por el grupo $\mathrm{N}_{L/K}\, \mathbf{C}_L$. Cambiando L por L', se ve que si $\mathrm{N}_{L/K}\, \mathbf{C}_L = \mathrm{N}_{L/K}\, \mathbf{C}_{L'}$ entonces $L = L'$. Observemos que la unicidad salía directamente de los Teoremas 4.5.1-4.5.3.

Bibliografía

[CaE56] Cartan, H. & Eilenberg, S., *Homological Algebra*, Princeton University Press, 1956.

[CaF67] Cassels, J. & Frölich, A., Eds., *Algebraic Number Theory*, Academic Press Inc. (London) Ltd., 1967.

[Cox89] Cox, D., *Primes of the form* $x^2 + ny^2$, John Wiley & Sons, Inc., 1989.

[Gol71] Goldstein, L., *Analytic Number Theory*, Prentice Hall, Inc., 1971.

[Jan96] Janusz, G., *Algebraic Number Fields (Second Edition)*, Graduate Studies in Mathematics **7**, American Mathematical Society, 1996.

[Lan93] Lang, S,. *Algebra (Third Edition)*, Addison-Wesley Publishing Company, Inc., 1997.

[Lan94] Lang, S., *Algebraic Number Theory (Second Edition)*, Graduate Texts in Mathematics **110**, Springer-Verlag New York, Inc., 1994.

[Mar77] Marcus, D., *Number Fields*, Springer-Verlag New York, Inc., 1977.

[Mil97] Milne, J., *Class Field Theory*, 1997. Disponible en www.jmilne.org.

[Ser79] Serre, J.-P., *Local Fields*, Springer-Verlag New York, Inc., 1979.