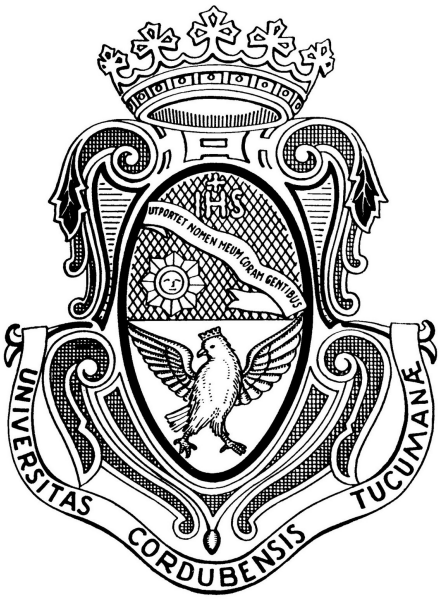
Trabajo Especial

Correspondencia de Langlands en dimensión 1



Facultad de Matemática, Astronomía, Física y Computación
Universidad Nacional de Córdoba

Lucas Villagra Torcomian

Director: Ariel M. Pacetti

A Nora.

Agradecimientos

En primer lugar quiero agradecer a Estefanía, por ser mi sustento emocional en mis últimos años de la carrera. Por su inquebrantable paciencia para escucharme durante horas de mis problemas facultativos, en gran parte por el presente trabajo. Por su tremenda empatía, su interés y por motivarme e incluso asesorarme.

Quiero agradecer también a Agustina, mi eterna compañera de clases y una de las primeras amistades que me trajo la facultad. La encargada de maximizar mi rendimiento académico y de hacer de mis días facultativos algo más agradable.

Agradezco a Leandro C. y a Roberto M., por brindarme su tiempo para escucharme y aconsejarme cuando me fue necesario. Al grupo de teoría de números de la FaMAF, por incluirme, haciendo crecer rápidamente mi sentido de pertenencia.

Un reconocimiento especial es hacia Ariel, por dirigir este escrito, por sus incontables correcciones, su dedicación y sus consejos académicos y personales.

A mi estimada familia quiero agradecerle por ofrecerme desde pequeño todas las posibilidades para desarrollarme personal y académicamente. Por incentivarme y apoyarme en la elección de la carrera. A mi madre, en especial, por estimularme con las olimpíadas de matemática. En este último aspecto le debo mucho también a Nora, por trasmitirme su amor y vocación.

Por último, mi mayor gratitud es para la universidad pública. Por darme la posibilidad de crecer en lo personal mientras me formaba como profesional.

Lucas Villagra Torcomian
Córdoba, Argentina.

Resumen

El objetivo de este trabajo es presentar la correspondencia de Langlands para el caso más simple: dimensión 1.

En la primera parte repasamos la teoría de Galois para extensiones infinitas, necesaria para luego estudiar las representaciones de Galois, uno de los lados de dicha correspondencia. En segunda instancia se abordan las distintas completaciones de un cuerpo de números y sus adèles e idèles, requeridos para tratar con los caracteres de Hecke, el segundo objeto a tener en cuenta en la correspondencia de Langlands.

Luego, se expone la teoría de cuerpos de clases, herramienta fundamental para la conexión de ambos mundos. Por último se trata la correspondencia, relacionando las representaciones de Galois con los caracteres de Hecke para el caso unidimensional y finalizamos el presente trabajo mencionando los ingredientes que aparecen al tratar de generalizar estos resultados a dimensiones mayores (siendo la correspondencia aún una conjetura en varios casos).

Abstract

The main goal of this work is to present Langlands correspondence for the simplest case: dimension 1.

In the first part we review the Galois theory for infinite extensions, necessary to study the Galois representations, one of the sides of this correspondence.

A second part approaches the study of the different completions of a number field and its adèles and idèles, requirements to deal with the Hecke characters, the second object of the Langlands correspondence.

Then, the class field theory is presented, a fundamental tool for the connection of both worlds. Finally the correspondence is treated, relating the Galois representations with the Hecke characters for the one-dimensional case and we conclude this work by mentioning the ingredients that appear when we trying to generalize these results to larger dimensions (the correspondence still being a conjecture in several cases).

Índice general

Introducción

Este trabajo tiene como principal objetivo exponer la correspondencia de Langlands en dimensión 1. El programa surgió como una serie de conjeturas alrededor de 1967 y fue presentado por Robert Langlands, aunque el caso unidimensional tiene sus bases fundamentalmente en la ley de reciprocidad de Artin y en los trabajos de Hecke, encargado de realizar toda la teoría automorfa.

La ley de reciprocidad de Artin (1927) debe su nombre a la ley de reciprocidad cuadrática de Gauss y relaciona extensiones abelianas no ramificadas de un cuerpo de números K con la factorización de números en K. Esta teoría cubre uno de los mundos sobre los que versan las conjeturas de Langlands, con lo cual su estudio nos llevará gran parte este trabajo. Para poder explayarnos en estos tópicos, primero daremos un repaso de la teoría de Galois, que estudia extensiones finitas L de un cuerpo K. La misma fue desarrollada por Galois, y consiste en asociarle un grupo finito (llamado el grupo de Galois de la extensión, y denotado $\mathrm{Gal}(L/K)$) a dicha extensión. La teoría de cuerpos de clases estudia qué extensiones L cumplen que el grupo $\mathrm{Gal}(L/K)$ es conmutativo, y cómo obtenerlas. La misma, permite demostrar la ley de reciprocidad de Gauss (Gauss mismo dio una demostración de su ley de reciprocidad usando extensiones de cuerpos) y la generaliza. Esta teoría se desarrolló gracias al aporte de grandes matemáticos como Kummer, Kronecker, Hensel, Weber, Hilbert, Takagi, Artin, Hasse, Chevalley y Tate.

En lo que se conoce como teoría local de cuerpos de clases, se trabaja reemplazando K por un cuerpo local. Históricamente primero se demostró la llamada teoría global de cuerpos de clases (que correspondía a extensiones finitas de $\mathbb{Q}$) utilizando métodos completamente analíticos, a partir de los cuales se pudieron estudiar cuerpos locales. Hasse fue el primero en dar una demostración de cómo la teoría de cuerpos de clases local implicaba también la teoría global, y propuso encontrar una demostración alternativa directa para el caso local. Ésta, fue dada por el propio Hasse y luego simplificada utilizando cohomología de grupos (utilizando distintas herramientas desarrolladas por Hochschild, Nakayama, Weil, Artin y Tate).

En la década de 1930, Chevalley introduce la noción de idèles, que consiste no en estudiar un cuerpo de números K, sino todas sus posibles completaciones juntas. Años más tarde, éstos permitieron dar una reinterpretación más conceptual del mapa de Artin y de su núcleo. A la vez, los idèles permiten estudiar caracteres de Hecke (estudiados y desarrollados por Hecke años antes de la incorporación de los idèles en la teoría de cuerpos de clases [Hec37]) desde un enfoque más general. Dicho enfoque fue el explotado por Tate en su tesis doctoral de 1950 (y fue clave en generalizar la teoría de cuerpos de clases a casos no conmutativos). Los caracteres de Hecke generalizan a los caracteres de Dirichlet y tienen la propiedad importante de que sus funciones L poseen una continuación analítica y satisfacen una cierta ecuación funcional (como lo hace la función zeta de Riemann). Son justamente estos caracteres los que están (por la correspondencia de Langlands) en correspondencia con las representaciones de Galois

continuas de dimensión 1.

Si bien la teoría de cuerpos de clases explica la relación entre representaciones de Galois abelianas y los caracteres de Hecke, no se sabía muy bien qué objeto tendría que ir del lado analítico al estudiar extensiones finitas que no sean abelianas. Aquí es donde Langlands dio una interpretación profunda de la teoría de clases (que presentamos en este trabajo), y explicó qué objetos deben ir de cada lado de la correspondencia. Para el caso "local" (cuerpos que son completaciones de $\mathbb{Q}$), su propuesta resultó muy fructífera (Langlands demostró los primeros casos de dicha correspondencia), y al día de hoy está casi completamente entendida. No obstante, el caso global es mucho mas complicado, y el objeto que debería reemplazar a los caracteres de Hecke no está demostrado que exista (aunque sí varias de las propiedades que debe satisfacer). Al final del presente trabajo explicaremos brevemente las implicancias de las conjeturas de Langlands, y los resultados demostrados en los últimos años.

Contenidos:

En el primer capítulo se exponen los conceptos básicos para el trabajo. Contiene una sección introductoria a la teoría algebraica de números y una sobre la teoría de Galois para extensiones finitas e infinitas.

En el segundo capítulo se introduce el concepto de representación de Galois y se estudian en más detalle las representaciones de Artin.

El tercer capítulo trata de los lugares y las completaciones de un cuerpo de números y sus extensiones. Los contenidos que se dan son los necesarios para poder entender el resto de los capítulos.

Se definen en el cuarto capítulo los adèles y los idèles y se prueban sus principales propiedades.

El capítulo 5 tiene como objetivo familiarizarse con los caracteres de Hecke. Para ello se estudian primeramente los caracteres de Dirichlet y los de Hecke clásicos.

El sexto capítulo se trata de la teoría de cuerpos de clases. Se definen las nociones básicas y se enuncian los teoremas principales.

Se expone en el último capítulo la correspondencia de Langlands en dimensión 1 y se menciona brevemente cómo se generaliza la correspondencia para dimensiones más altas.

Capítulo 1
Preliminares

1.1. Teoría algebraica de números

En esta sección se darán las nociones y los resultados básicos de la teoría algebraica de números. Para más detalles se puede ver [Mar77], [Lan94] o [Mil17].

Definición 1.1.1. Un **cuerpo de números** es un cuerpo K tal que $K/\mathbb{Q}$ es finita.

Observación 1.1.2. Dado que toda extensión finita es algebraica, tenemos que si K es un cuerpo de números, entonces $K/\mathbb{Q}$ es algebraica.

De ahora en adelante, K va a denotar un cuerpo de números.

Definición 1.1.3. Dado un cuerpo de números K, un elemento $\alpha \in K$ se dice que es un **entero algebraico** de K si existe $p(x) \in \mathbb{Z}[x]$ mónico tal que $p(\alpha) = 0$.

Claramente, un entero algebraico de K es un elemento algebraico en K. Denotamos al conjunto de todos los enteros algebraicos de K por $\mathcal{O}_K$ o por $\mathcal{O}$ si se sobreentiende cuál es el cuerpo en el que estamos trabajando. Es decir,

$$\mathcal{O}_K := \{\alpha \in K : \alpha \text{ es entero algebraico de } K\}.$$

La siguiente proposición nos da otra forma equivalente de definir lo que es un entero algebraico.

Proposición 1.1.4. Sea $\alpha \in \mathbb{C}$. Son equivalentes:

(1) α es entero algebraico.

(2) $m_\alpha(x) \in \mathbb{Z}[x]$, donde $m_\alpha(x)$ es el polinomio minimal de α.

(3) $\mathbb{Z}[\alpha]$ es un $\mathbb{Z}$-módulo finitamente generado.

(4) Existe un $\mathbb{Z}$-submódulo M de $\mathbb{C}$ finitamente generado tal que $\alpha M \subseteq M$.

Demostración: Ver [Mar77, Teorema 2]. □

Corolario 1.1.5. $\mathcal{O}_K$ es un subanillo de K.

Demostración: Sean $\alpha, \beta \in \mathbb{C}$. Por la proposición anterior, $\mathbb{Z}[\alpha]$ y $\mathbb{Z}[\beta]$ son finitamente generados. En consecuencia, $\mathbb{Z}[\alpha, \beta]$ es finitamente generado.

Como $\alpha + \beta, \alpha\beta \in \mathbb{Z}[\alpha, \beta]$, entonces usando nuevamente la Proposición 1.1.4 obtenemos que $\alpha + \beta, \alpha\beta \in \mathcal{O}_K$. Luego, $\mathcal{O}_K$ es un subanillo de K. □

Ejemplo 1.1.6. Notemos que $\mathcal{O}_{\mathbb{Q}} = \mathbb{Z}$. Ésto es así porque si $\alpha \in \mathbb{Z}$ entonces es raíz de $x - \alpha \in \mathbb{Z}[x]$. Recíprocamente, si $\alpha \in \mathcal{O}_{\mathbb{Q}}$ entonces $\alpha \in \mathbb{Q}$ y por la Proposición 1.1.4, $x - \alpha = m_\alpha(x) \in \mathbb{Z}[x]$ y esto nos dice que $\alpha \in \mathbb{Z}$.

En general, para un cuerpo K vale que $K = \mathrm{Frac}(\mathcal{O}_K)$, donde si R es un dominio íntegro, $\mathrm{Frac}(R)$ denota su cuerpo de fracciones. Es decir,

$$\mathrm{Frac}(R) := \left\{ \frac{a}{b} : a, b \in R,\ b \neq 0 \right\} / \sim, \quad \text{donde} \quad \frac{a}{b} \sim \frac{c}{d} \quad \text{si} \quad ad = bc$$

Definición 1.1.7. Un anillo R se dice **Noetheriano** si cumple algunas de las siguientes propiedades equivalentes:

(1) Si existe una cadena ascendente de ideales $I_1 \subseteq I_2 \subseteq I_3 \subseteq ...$ de R, entonces se estaciona, es decir que existe $N \in \mathbb{N}$ tal que $I_n = I_N\ \forall n \geq N$.

(2) Todo ideal es finitamente generado.

Definición 1.1.8. Decimos que un dominio íntegro R es **íntegramente cerrado** si cumple la siguiente propiedad:

$$\text{Si } \alpha \in \mathrm{Frac}(R) \text{ es raíz de un polinomio en } R[x] \text{ entonces } \alpha \in R.$$

Definición 1.1.9. Un **dominio de Dedekind** R es un dominio íntegro que satisface:

(1) R es Noetheriano.

(2) Todo ideal primo no nulo es maximal.

(3) R es íntegramente cerrado.

Teorema 1.1.10. Si K es un cuerpo de números, entonces $\mathcal{O}_K$ es un dominio de Dedekind.

Demostración: Ver [Mar77, Ejercicio 4 del capítulo 2]. □

Queremos estudiar los anillos $\mathcal{O}_K$. Ya enunciado el Teorema 1.1.10, pasaremos momentáneamente a describir algunas propiedades que tienen los dominios de Dedekind. Es decir que de aquí en adelante R va a ser un dominio de Dedekind.

Teorema 1.1.11. Sea $\mathfrak{a}$ un ideal propio de R. Entonces existen $\mathfrak{p}_i$ ideales primos de R y $e_i \in \mathbb{N}$ tales que

$$\mathfrak{a} = \prod_{i=1}^{r} \mathfrak{p}_i^{e_i}$$

Más aún, esta factorización es única salvo orden.

Demostración: Ver [Mar77, Teorema 16]. □

Es sabido que todo anillo DIP (dominio de ideales principales) es DFU (dominio de factorización única). También sabemos que la recíproca no vale en general. La siguiente proposición nos dice que estas nociones son equivalentes en los dominios de Dedekind.

Proposición 1.1.12. Si R es DFU entonces es DIP.

Demostración: Ver [Mar77, Teorema 18]. □

Definición 1.1.13. Dados dos ideales no nulos $\mathfrak{a}, \mathfrak{b}$ de R decimos que $\mathfrak{a}$ y $\mathfrak{b}$ son **coprimos** si no tienen un ideal primo en común dentro de su factorización en ideales primos. Lo denotaremos como $(\mathfrak{a}, \mathfrak{b}) = 1$.

De ahora en adelante, vamos a concentrarnos en el caso $R = \mathcal{O}_K$. A un ideal primo de $\mathcal{O}_K$ lo llamaremos ideal primo de K o simplemente **primo** (de K).

Definición 1.1.14. Un **ideal fraccionario** de K es un $\mathcal{O}_K$-módulo $\mathfrak{a}$ de K tal que existe $b \in \mathbb{Z} \setminus \{0\}$ de manera que cumple que $b\mathfrak{a} \subseteq \mathcal{O}_K$.

Observación 1.1.15. Los ideales enteros de K son ideales fraccionarios de K.

Definición 1.1.16. Un ideal fraccionario $\mathfrak{a}$ se dice que es principal si existe $\alpha \in K$ tal que $\alpha\,\mathcal{O}_K = \mathfrak{a}$.

Proposición 1.1.17. Dado $\mathfrak{a}$ ideal fraccionario no nulo de K, entonces

$$\mathfrak{a} = \prod_{\mathfrak{p}} \mathfrak{p}^{e_\mathfrak{p}},$$

donde la productoria recorre todos los primos $\mathfrak{p}$, $e_\mathfrak{p} \in \mathbb{Z}$ y $e_\mathfrak{p} = 0$ para casi todo $\mathfrak{p}$, i.e., $e_\mathfrak{p} = 0$ salvo para una cantidad finita de $\mathfrak{p}$. Más aún, esta factorización es única salvo orden.

Demostración: Ver [Mar77, Ejercicio 31 del capítulo 3]. □

Entonces se dice que un primo $\mathfrak{p}$ de K **aparece** en $\mathfrak{a}$ si $e_\mathfrak{p} \neq 0$. Si $\mathfrak{b}$ es otro ideal fraccionario de K, decimos que $\mathfrak{a}$ y $\mathfrak{b}$ son **coprimos** si no existe un primo $\mathfrak{p}$ de K que aparezca en $\mathfrak{a}$ y en $\mathfrak{b}$. Esta condición se denota como $(\mathfrak{a}, \mathfrak{b}) = 1$. Notemos que esta noción generaliza la de dos ideales enteros coprimos. Por simplicidad, de ahora en más llamaremos simplemente **ideal** a un ideal fraccionario y si queremos hacer referencia a un ideal de $\mathcal{O}_K$ diremos **ideal entero**.

Proposición 1.1.18. Si $\mathfrak{a}$ y $\mathfrak{b}$ son ideales (fraccionarios) de K entonces $\mathfrak{ab}$ es un ideal de K. Además, si $\mathfrak{a}$ es no nulo entonces el conjunto $\mathfrak{a}^{-1} := \{\alpha \in K : \alpha\mathfrak{a} \subseteq \mathcal{O}_K\}$ es también un ideal fraccionario de K y cumple que $\mathfrak{a}\mathfrak{a}^{-1} = \mathcal{O}_K$.

Demostración: Ver [Mar77, Ejercicio 31 del capítulo 2]. □

Proposición 1.1.19. Si $\mathfrak{a}$ es un ideal entero no nulo de K entonces $\mathcal{O}_K/\mathfrak{a}$ es finito.

Demostración: Ver [Mar77, Página 56]. □

Si $\mathfrak{a}$ es un ideal entero no nulo de K se lama **norma** de $\mathfrak{a}$ al número entero $N(\mathfrak{a}) := |\mathcal{O}_K/\mathfrak{a}|$. Por la Proposición 1.1.19 tenemos que la norma de cualquier ideal no nulo de K es un número finito. Es sabido también que la norma es multiplicativa, es decir que si $\mathfrak{a}, \mathfrak{b}$ son ideales enteros no nulos de K, entonces $N(\mathfrak{ab}) = N(\mathfrak{a})N(\mathfrak{b})$ (ver [Mar77, Teorema 22]).

Vamos a denotar por I_K al conjunto de todos los ideales fraccionarios no nulos de K. Luego, por la Proposición 1.1.18, I_K es un grupo y claramente es abeliano. También, vamos a denotar como P_K al conjunto de los ideales fraccionarios principales no nulos. Es claro entonces que P_K resulta un subgrupo (normal) de I_K. Esto nos da lugar a la siguiente definición.

Definición 1.1.20. Definimos el **grupo de clases de ideales** de $\mathcal{O}_K$ como el cociente I_K/P_K y lo denotaremos por $Cl(K)$.

Se puede ver que si K es un cuerpo de números, entonces $Cl(K)$ es grupo abeliano con una cantidad finita de elementos (ver [Mil17, Teorema 4.4]). Es por eso que tenemos la siguiente definición.

Definición 1.1.21. Definimos el **número de clases** como el número $h_K := |Cl(K)|$.

1.1.1. Factorización en extensiones

Supongamos que K es un cuerpo de números y L/K es una extensión finita. Dado un ideal primo $\mathfrak{p}$ de $\mathcal{O}_K$, se tiene que $\mathfrak{p}\,\mathcal{O}_L$ es un ideal de $\mathcal{O}_L$. Por el Teorema 1.1.11, tenemos que existen primos $\mathfrak{P}_i$ de $\mathcal{O}_L$ tales que

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

A los enteros e_i los llamamos **índice de ramificación** de $\mathfrak{p}$ en $\mathfrak{P}_i$. En este caso decimos que los primos $\mathfrak{P}_i$ están sobre $\mathfrak{p}$ (y que $\mathfrak{p}$ está debajo de $\mathfrak{P}_i$). Usamos la notación $\mathfrak{P}\,|\mathfrak{p}$ para decir que $\mathfrak{P}$ está **sobre** $\mathfrak{p}$ o **divide** a $\mathfrak{p}$ (es decir si aparece en la descomposición en primos de $\mathfrak{p}$) y solemos denotar al índice de ramificación como $e(\mathfrak{P}\,|\mathfrak{p})$. En caso de que $\mathfrak{P}$ no esté sobre $\mathfrak{p}$ diremos que $e(\mathfrak{P}\,|\,\mathfrak{p}) = 0$.

Lema 1.1.22. Un primo $\mathfrak{P}$ de L está sobre un primo $\mathfrak{p}$ de K si y sólo si $\mathfrak{p} = \mathfrak{P} \cap K$.

Demostración: Supongamos primero que $\mathfrak{P}\,|\,\mathfrak{p}$. Entonces $\mathfrak{p} \subseteq \mathfrak{P}$ y por lo tanto $\mathfrak{p} \subseteq \mathfrak{P} \cap \mathcal{O}_K$. Luego, como $\mathfrak{P} \cap K \neq \mathcal{O}_K$ y $\mathfrak{p}$ es maximal resulta que $\mathfrak{p} = \mathfrak{P} \cap K$. Recíprocamente, como $\mathfrak{p} \subseteq \mathfrak{P}$ entonces $\mathfrak{P}\,|\,\mathfrak{p}$. □

Además, notemos que si $\mathfrak{P}$ está sobre $\mathfrak{p}$, entonces resulta $\mathcal{O}_K/\mathfrak{p} \subseteq \mathcal{O}_L/\mathfrak{P}$. Esto es porque a partir de la inclusión canónica $\mathcal{O}_K \hookrightarrow \mathcal{O}_L$ podemos tomar cociente y obtener $\mathcal{O}_K \to \mathcal{O}_L/\mathfrak{P}$. Por último, tomando cociente por el núcleo $\mathfrak{P} \cap \mathcal{O}_K = \mathfrak{p}$ (esta última igualdad vale debido a que $\mathfrak{P} \cap \mathcal{O}_K = \mathfrak{P} \cap K$) se sigue que

$$\mathcal{O}_K/\mathfrak{p} \hookrightarrow \mathcal{O}_L/\mathfrak{P}\,.$$

Si $\mathfrak{P}$ está sobre $\mathfrak{p}$, definimos el **grado de inercia** de $\mathfrak{p}$ en $\mathfrak{P}$ como el número

$$f(\mathfrak{P}\,|\,\mathfrak{p}) := [\mathcal{O}_L/\mathfrak{P} : \mathcal{O}_K/\mathfrak{p}].$$

El siguiente teorema se encarga de relacionar el índice de ramificación y el grado de inercia de un primo dado.

Teorema 1.1.23. Sea L/K extensión, $\mathfrak{p}$ primo de K. Entonces vale que

$$[L:K] = \sum_{\mathfrak{P}\,|\,\mathfrak{p}} e(\mathfrak{P}\,|\,\mathfrak{p}) f(\mathfrak{P}\,|\,\mathfrak{p})$$

Demostración: Primero notemos que la suma del miembro derecho es finita ya que existen finitos $\mathfrak{P}$ que están sobre un $\mathfrak{p}$ fijo. Para probar la igualdad veamos que ambos miembros son iguales a $[\mathcal{O}_L \,/\, \mathfrak{p}\,\mathcal{O}_L : \mathcal{O}_K \,/\, \mathfrak{p}]$. Supongamos que $\mathfrak{p} = \mathfrak{P}_1^{e_1} ... \mathfrak{P}_g^{e_g}$. Por el Teorema chino del resto para ideales,

$$\mathcal{O}_L \,/\, \mathfrak{p}\,\mathcal{O}_L = \mathcal{O}_L \,/ \prod_{i=1}^{r} {\mathfrak{P}_i}^{e_i} \cong \prod_{i=1}^{r} \mathcal{O}_L \,/\, \mathfrak{P}_i^{e_i}\,.$$

Entonces para ver que $\sum_{i=1}^{r} e_i f_i = [\mathcal{O}_L \,/\, \mathfrak{p}\,\mathcal{O}_L : \mathcal{O}_K \,/\, \mathfrak{p}]$ basta ver que el grado de la extensión $(\mathcal{O}_L \,/\, \mathfrak{P}_i^{e_i})/(\mathcal{O}_K \,/\, \mathfrak{p})$ es igual a $e_i f_i$. Para cada r_k, $\mathfrak{P}_i^{r_k} \,/\, \mathfrak{P}_i^{r_k+1}$ es un $(\mathcal{O}_L \,/\, \mathfrak{P}_i)$- módulo y como no hay ningún ideal entre $\mathfrak{P}_i^{r_k}$ y $\mathfrak{P}_i^{r_k+1}$ entonces tiene dimensión 1 como $(\mathcal{O}_L \,/\, \mathfrak{P}_i)$- espacio vectorial, y por lo tanto dimensión f_i como $(\mathcal{O}_K \,/\, \mathfrak{p})$-espacio vectorial. Luego, cada cociente de la cadena

$$\mathcal{O}_L \supset \mathfrak{P}_i \supset \mathfrak{P}_i^2 \supset ... \supset \mathfrak{P}_i^{e_i}$$

tiene dimensión $\mathfrak{f}_i$ sobre $\mathcal{O}_K \,/\, \mathfrak{p}$ y por lo tanto $\mathcal{O}_L \,/\, \mathfrak{P}_i^{e_i}$ tiene dimensión $e_i f_i$. Para ver que $[L:K] = [\mathcal{O}_L \,/\, \mathfrak{p}\,\mathcal{O}_L : \mathcal{O}_K \,/\, \mathfrak{p}]$ ver [Mil17, Teorema 3.34]. □

Definición 1.1.24. Sea L/K una extensión y $\mathfrak{p}$ primo de K. Decimos que $\mathfrak{p}$ **ramifica** si existe un primo $\mathfrak{P}$ de L tal que $e(\mathfrak{P}\,|\,\mathfrak{p}) > 1$. Caso contrario, decimos que $\mathfrak{p}$ **no ramifica**. Decimos que la extensión L/K es **no ramificada** si $\mathfrak{p}$ no ramifica para todo primo $\mathfrak{p}$ de K.

Veamos que en el caso en que L/K es finita y Galois se simplifica la fórmula del Teorema 1.1.23.

Teorema 1.1.25. Sea L/K Galois, $\mathfrak{p}$ primo de K. Entonces:

(1) $\mathrm{Gal}(L/K)$ actúa transitivamente en los primos de L que están sobre $\mathfrak{p}$. Esto es, que si $\mathfrak{P}$ y $\mathfrak{P}'$ son primos de L que están sobre $\mathfrak{p}$ entonces existe $\sigma \in \mathrm{Gal}(L/K)$ tal que $\sigma(\mathfrak{P}) = \mathfrak{P}'$.

(2) Los primos de L que están sobre $\mathfrak{p}$ tienen el mismo índice de ramificación y el mismo grado de inercia.

Demostración: Si $\sigma \in \mathrm{Gal}(L/K)$ entonces $\sigma(\mathcal{O}_L) = \mathcal{O}_L$ y luego si $\mathfrak{P}$ es un primo de L entonces $\sigma(\mathfrak{P})$ también lo es. Más aún, si $\mathfrak{p}\,\mathcal{O}_L = \mathfrak{P}_1^{e_1} ... \mathfrak{P}_g^{e_g}$ tenemos que

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

Es decir que si $\mathfrak{P}\,|\,\mathfrak{p}$ entonces $\sigma(\mathfrak{P})|\,\mathfrak{p}$. Supongamos ahora que $\mathfrak{P}$ y $\mathfrak{P}'$ son dos primos sobre $\mathfrak{p}$ y que no existe $\sigma \in \mathrm{Gal}(L/K)$ tal que $\sigma(\mathfrak{P}) = \mathfrak{P}'$. Por el Teorema Chino de Resto, existe $\beta \in \mathfrak{P}'$ tal que $\beta \notin \sigma(\mathfrak{P})$ para todo $\sigma \in \mathrm{Gal}(L/K)$. Luego, $b := N_{L/K}(\beta) \in \mathcal{O}_K$ y como $\beta \in \mathfrak{P}'$ entonces $b \in \mathfrak{P}'$ y por ende $b \in \mathfrak{P}' \cap \mathcal{O}_K = \mathfrak{p}$. Por otro lado, como $\beta \notin \sigma^{-1}(\mathfrak{P})$ para todo $\sigma \in \mathrm{Gal}(L/K)$ entonces $\sigma(\beta) \notin \mathfrak{P}$. Absurdo, pues $\mathfrak{P}$ es primo y

$$\prod_{\sigma \in \mathrm{Gal}(L/K)} \sigma(\beta) = N_{L/K}(\beta) = b \in \mathfrak{P} \cap \mathcal{O}_K = \mathfrak{p} \subset \mathfrak{P}\,.$$

Queda así demostrada la afirmación. □

Como consecuencia del inciso (2) del teorema anterior tenemos que si el índice de ramificación de los primos de L sobre $\mathfrak{p}$ es e y el grado de inercia es f entonces

$$[L : K] = efg,$$

donde g es la cantidad de primos de L que están sobre $\mathfrak{p}$. Si $e = f = 1$ decimos que $\mathfrak{p}$ se **parte completamente** (en L). En este último caso $\mathfrak{p}$ es no ramificado y $\mathfrak{p}\,\mathcal{O}_L$ es el producto de $[L : K]$ primos distintos.

Definición 1.1.26. Sea L/K Galois con grupo de Galois $G = \mathrm{Gal}(L/K)$ y $\mathfrak{P}$ un primo de L. Definimos el **grupo de descomposición** y al **grupo de inercia** respectivamente como

$$D_{\mathfrak{P}} = \{\sigma \in G : \sigma(\mathfrak{P}) = \mathfrak{P}\}$$
$$I_{\mathfrak{P}} = \{\sigma \in G : \sigma(\alpha) \equiv \alpha \pmod{\mathfrak{P}}\ \forall \alpha \in \mathcal{O}_L\}$$

Observación 1.1.27. Notemos que $I_{\mathfrak{P}} \subseteq D_{\mathfrak{P}}$, porque si $\sigma \in I_{\mathfrak{P}}$ entonces dado $\alpha \in \mathfrak{P} \subseteq \mathcal{O}_L$, vale que $\sigma(\alpha) \in \mathfrak{P}$, pues $\alpha \in \mathfrak{P}$ y $\sigma \in I_{\mathfrak{P}}$. Luego, $\sigma(\mathfrak{P}) \subseteq \mathfrak{P}$, pero esto claramente implica que $\sigma(\mathfrak{P}) = \mathfrak{P}$. Luego, $D_{\mathfrak{P}}$ es un subgrupo de G e $I_{\mathfrak{P}}$ es un subgrupo de $D_{\mathfrak{P}}$.

Definición 1.1.28. Si $\mathfrak{p}$ es un primo de K, llamamos **cuerpo residual** al cociente $\mathcal{O}_K \,/\, \mathfrak{p}$ y lo denotaremos por $k_{\mathfrak{p}}$.

Si tomamos $\sigma \in D_{\mathfrak{P}}$ entonces automáticamente tenemos definida su clase $\overline{\sigma}$ en $l_{\mathfrak{P}} = \mathcal{O}_L \,/\, \mathfrak{P}$ que actúa trivialmente en los elementos de $k_{\mathfrak{p}}$, donde $\mathfrak{p} = \mathfrak{P} \cap \mathcal{O}_K$. Esto nos define un morfismo

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

Proposición 1.1.29. Vale que:

(1) El morfismo $D_{\mathfrak{P}} \to \mathrm{Gal}(l_{\mathfrak{P}}/k_{\mathfrak{p}}),\ \sigma \mapsto \overline{\sigma}$ es suryectivo y tiene como núcleo al grupo de inercia. En particular, $I_{\mathfrak{P}}$ es un subgrupo normal de $D_{\mathfrak{P}}$.

(2) $|I_{\mathfrak{P}}| = e(\mathfrak{P} \,|\, \mathfrak{p})$ y $|D_{\mathfrak{P}}| = e(\mathfrak{P} \,|\, \mathfrak{p}) f(\mathfrak{P} \,|\, \mathfrak{p})$.

Demostración:

(1) σ está en el núcleo $\iff \sigma(\alpha) + \mathfrak{P} = \alpha + \mathfrak{P} \quad \forall \alpha \in \mathcal{O}_L \iff \sigma(\alpha) \equiv \alpha \pmod{\mathfrak{P}} \quad \forall \alpha \in \mathcal{O}_L$ $\iff \sigma \in I_{\mathfrak{P}}$. Para ver que es suryectiva ver [Mar77, Teorema 28].

(2) Para ver que $|D_{\mathfrak{P}}| = e(\mathfrak{P} \,|\, \mathfrak{p}) f(\mathfrak{P} \,|\, \mathfrak{p})$ probemos que $[\mathrm{Gal}(L/K) : D_{\mathfrak{P}}] = g$, con la notación en la que veníamos trabajando. Cada clase a izquierda $\sigma D_{\mathfrak{P}}$ (con $\sigma \in \mathrm{Gal}(L/K)$) manda $\mathfrak{P}$ en $\sigma(\mathfrak{P})$ y es claro que $\sigma D_{\mathfrak{P}} = \tau D_{\mathfrak{P}}$ si y sólo si $\sigma(\mathfrak{P}) = \tau(\mathfrak{P})$. Esto nos dice que existe una correspondencia biunívoca entre las clases a izquierda $\sigma D_{\mathfrak{P}}$ y los primos $\sigma(\mathfrak{P})$, que por el Teorema 1.1.25 son todos los primos que están sobre $\mathfrak{p}$. Por lo tanto, hay g de ellos. Por último, por inciso (1) tenemos que $|D_{\mathfrak{P}}/I_{\mathfrak{P}}| = |\,\mathrm{Gal}(l_{\mathfrak{P}}/k_{\mathfrak{p}})| = [l_{\mathfrak{P}} : k_{\mathfrak{p}}] = f$, lo cual implica que $|I_{\mathfrak{P}}| = e(\mathfrak{P} \,|\, \mathfrak{p})$. □

1.1.2. Norma en extensiones finitas separables

Sea L/K una extensión finita separable de grado n. Podemos definir una función **norma** $N_{L/K} : L^\times \to K^\times$ como

$$N_{L/K}(\alpha) = \prod_{\sigma \in \mathrm{Hom}_K(L,\bar{L})} \sigma(\alpha),$$

donde $\overline{L}$ es una clausura algebraica fija de L.

Notemos que si L/K es Galois con grupo de Galois $G = \mathrm{Gal}(L/K)$, entonces la norma se puede expresar como $N_{L/K}(\alpha) = \prod_{\alpha \in G} \sigma(\alpha)$.

Proposición 1.1.30. La función norma cumple las siguientes propiedades:

(1) $N_{L/K}(\alpha\beta) = N_{L/K}(\alpha)N_{L/K}(\beta) \quad \forall \alpha, \beta \in L^\times$.

(2) $|N_{K/\mathbb{Q}}(\alpha)| = N((\alpha)) \quad \forall \alpha \in K^\times$, viendo a (α) como ideal.

Demostración:

(1) Resulta directo, pues σ es multiplicativa para todo $\sigma \in \mathrm{Aut}_K(L)$.

(2) Ver [Mar77, Teorema 22]. □

Así como tenemos definida una función norma de $L^\times$ a $K^\times$, podemos definir una función de los ideales de I_L a los de I_K. Más aún, podemos hacerlo de tal forma que ésta extienda a la anterior, considerando a L dentro de I_L vía la función $id : L^\times \to I_L, \quad x \mapsto (x)$.

Definición 1.1.31. Definimos la función **norma** $N_{L/K} : I_L \to I_K$ de la siguiente manera:
Si $I \in I_L$, entonces $N_{L/K}(I)$ es el ideal fraccionario generado por $\{N_{L/K}(x) : x \in I\}$.

Lema 1.1.32. Sea $\mathfrak{P} \in I_L$ un primo de L y $\mathfrak{p} = \mathfrak{P} \cap K$. Entonces $N_{L/K}(\mathfrak{P}) = \mathfrak{p}^{f(\mathfrak{P}\,|\,\mathfrak{p})}$.

Demostración: Ver [Jan96, Proposición 8.2]. □

Lema 1.1.33. El siguiente diagrama es conmutativo:

$$\begin{array}{ccc} L^\times & \xrightarrow{id} & I_L \\ {\scriptstyle N_{L/K}}\downarrow & & \downarrow{\scriptstyle N_{L/K}} \\ K^\times & \xrightarrow[id]{} & I_K \end{array}$$

Demostración: Dado $x \in L^\times$, usando la definición (2) tenemos que $N_{L/K}((x))$ es el ideal generado por $N_{L/K}(x)$, que es por definición $(N_{L/K}(x))$. Luego, $N_{L/K}((x)) = (N_{L/K}(x))$. □

El Lema 1.1.33 automáticamente nos define un morfismo $N_{L/K} : Cl(L) \to Cl(K)$, que no tiene por que ser inyectivo o suryectivo.

1.2. Teoría de Galois

Comenzaremos dando una descripción de la teoría de Galois enunciando solamente el principal teorema de Galois para extensiones finitas para poder centrarnos luego en extesiones de Galois infinitas; y finalmente, en nuestro principal objeto de estudio de esta sección, que serán las extensiones abelianas. Para más detalles se puede consultar [Cox12] o [Mil18].

1.2.1. Extensiones finitas

Para el caso de extensiones finitas, tenemos el siguiente teorema de Galois que nos dará una correspondencia entre subgrupos del grupo de Galois y subextensiones.

Teorema 1.2.1. Sea K es un cuerpo y L/K una extensión finita y de Galois con grupo de Galois $G := \mathrm{Gal}(L/K) = \mathrm{Aut}_K(L)$. Entonces existe una correspondencia

$$\begin{array}{ccc} \{\text{subgrupos de } G\} & \longleftrightarrow & \{\text{subextensiones de } L/K\} \\ H & \longrightarrow & L^H \\ \mathrm{Gal}(L/F) & \longleftarrow & F \end{array}$$

donde $L^H := \{\alpha \in L : \sigma(\alpha) = \alpha \ \forall \sigma \in H\}$. Además, se cumple que:

(1) La correspondencia revierte contenciones. Es decir que $H_1 \subseteq H_2 \iff L^{H_1} \supseteq L^{H_2}$.

(2) Los índices son iguales a los grados. Es decir que si $H_2 \subseteq H_1$ entonces

$$[H_1 : H_2] = [L^{H_2} : L^{H_1}].$$

(3) Si $\sigma \in G,\ H < G$, entonces $L^{\sigma H \sigma^{-1}} = \sigma(L^H)$.

(4) $H \lhd G \iff L^H/K$ es normal (y por lo tanto Galois). En tal caso, $\mathrm{Gal}(L^H/K) \cong G/H$.

Demostración: Ver [Mil18, Teorema 3.16]. □

1.2.2. Extensiones infinitas

Cuando tenemos una extensión L/K algebraica pero no finita, entra en juego la topología.

Definición 1.2.2. Un **grupo topológico** es un grupo $(G, \cdot)$ donde G es un espacio topológico y $\cdot : G \times G \to G$ e $i : G \to G,\ g \mapsto g^{-1}$ son funciones continuas (donde $G \times G$ tiene la topología producto).

En general, vamos a denotar un grupo topológico simplemente como G. Notemos que si G es un grupo topológico entonces para cada $g \in G$ tenemos definida la traslación

$$t_g : G \to G,\ h \mapsto gh$$

que resulta claramente biyectiva y más aún, un homeomorfismo.

Luego, la base de entornos de cualquier punto (en particular el 1) determina los abiertos en todos los puntos del grupo. Como consecuencia de este hecho, tenemos el siguiente lema.

Lema 1.2.3. Si G es un grupo topológico y H es un subgrupo de G abierto, entonces H es cerrado.

Demostración: Como H es abierto, entonces gH es abierto para cada $g \in H$. Como

$$G = H \bigsqcup \left(\bigsqcup_{\substack{g \in G/H \\ g \neq 1}} gH \right),$$

donde $\bigsqcup$ indica unión disjunta, entonces $H = (\bigsqcup gH)^c$ es cerrado, pues unión de abiertos es abierto y complemento de un abierto es cerrado. □

Si tenemos L/K una extensión de Galois no finita, queremos dotar a $\mathrm{Gal}(L/K)$ con una topología para que resulte un grupo topológico.

Si S es un subconjunto finito de L, denotamos

$$G(S) := \{\sigma \in G : \sigma(s) = s \ \ \forall s \in S\},$$

que resulta un subgrupo de G.

Lema 1.2.4. $G(S) = \mathrm{Gal}(L/K(S))$

Demostración: Cabe aclarar que tiene sentido hablar del grupo de Galois de $L/K(S)$ ya que si L/K es Galois, entonces $L/K(S)$ también lo es. Veamos ahora ambas contenciones.

Si $\sigma \in G(S)$ entonces fija los elementos de K y de S y luego fija los elementos de $K(S)$. La otra contención es trivial. □

Observación 1.2.5. Como $K(S)/K$ es algebraica y finita (pues S es finito) entonces el índice $[G : G(S)]$ resulta finito.

Proposición 1.2.6. Existe en $G = \mathrm{Gal}(L/K)$ una única topología que lo hace un grupo topológico para el cual los conjuntos $G(S)$ con $|S| < \infty$ forman una base de abiertos de $Id = 1_G$.

Demostración: Para ver que los conjuntos $G(S)$ definen una topología que hacen a $(G, \cdot)$ un grupo topológico, basta ver lo siguiente:

(1) Dados U_1, U_2 entornos de 1 existe U_3 entorno de 1 tal que $U_3 \subseteq U_1 \cap U_2$.

(2) Dado U entorno de 1 existe U' entorno de 1 tal que $U'U' \subseteq U$.

(3) Para todo U entorno de 1 y para todo $g \in G$ existe U' entorno de 1 tal que $U' \subseteq gUg^{-1}$

(4) Para todo U entorno de 1 existe U' entorno de 1 tal que $U' \subseteq U^{-1}$.

Estas cuatro condiciones se satisfacen trivialmente, pues:

(1) Vale porque $G(S_1) \cap G(S_2) = G(S_1 \cup S_2)$. Esto nos dice que los conjuntos $G(S)$ forman una base de entornos.

(2) Vale porque $G(S)$ es un subgrupo, entonces $G(S)G(S) = G(S)$.

(3) Como U es entorno de 1 entonces existe $G(S)$ contenido en U. Dado $\sigma \in G$ definimos $U' := G(\sigma(S))$. Luego, $U' = G(\sigma(S)) = \sigma G(S)\sigma^{-1} \subseteq \sigma U \sigma^{-1}$.

(4) Nuevamente, vale porque $G(S)$ es un subgrupo, entonces $G(S)^{-1} = G(S)$.

Notemos que (3) nos dice que el producto es continuo. En efecto, si U es entorno de 1 y $g_1, g_2 \in G$ son tales que $g_1 g_2 \in U$, entonces existe $\widetilde{U}$ tal que $g_1 g_2 \widetilde{U} \subseteq U$ y además existen entornos de g_1 y g_2 que van a parar a U por el producto, pues por (2), existe U' entorno del 1 tal que $U'U' \subseteq U$. Entonces, por (3) existe un entorno V tal que $g_2^{-1} V g_2 \subseteq U'$ y luego

$$(g_1 V)(g_2 U') = g_1 g_2 (g_2^{-1} V g_2) U' \subseteq g_1 g_2 U' U' \subseteq \widetilde{U} \subseteq U.$$

A su vez, (4) nos asegura que $i : G \to G,\ g \mapsto g^{-1}$ es continua. □

Definición 1.2.7. A la topología dada por la proposición anterior se la llama **topología de Krull**.

Observación 1.2.8. Si L/K es finita, esta topología es la discreta, es decir, que todo subcojunto de G es abierto. En efecto, si L/K es finita entonces $L = K[\alpha_1, ..., \alpha_n]$. Tomando entonces $S = \{\alpha_1, ...\alpha_n\}$ se tiene que $G(S) = \{Id\}$, lo cual nos dice que $\{Id\}$ es abierto y por lo tanto todos los puntos lo son.

Proposición 1.2.9. Si L/K es algebraica y de Galois, entonces $\mathrm{Gal}(L/K)$ es compacto, Hausdorff y totalmente disconexo.

Demostración: Ver [Mil18, Proposición 7.8]. □

Teorema 1.2.10. Si L/K es Galois, entonces se cumplen:

(1) Si $K \subseteq F \subseteq L$ entonces L/F es Galois y $\mathrm{Gal}(L/F) < \mathrm{Gal}(L/K)$ es cerrado.

(2) Si H es subgrupo de $\mathrm{Gal}(L/K)$, entonces $\mathrm{Gal}(L/L^H) = \overline{H}$.

Demostración:

(1) Si $S \subseteq F$ es finito, entonces $G(S)$ es subgrupo abierto de $\mathrm{Gal}(L/K)$ y luego es cerrado por el Lema 1.2.3. Además,

$$\mathrm{Gal}(L/F) = \bigcap_{\substack{S \subseteq F \\ \text{finito}}} G(S).$$

Por lo tanto, $\mathrm{Gal}(L/F)$ es un subgrupo de $\mathrm{Gal}(L/K)$ y es cerrado, pues es intersección de cerrados.

(2) Por (1) sabemos que $\mathrm{Gal}(L/L^H)$ es cerrado y además, claramente contiene a H. Luego,

$$\overline{H} \subseteq \mathrm{Gal}(L/L^H).$$

Por otro lado, como $\mathrm{Gal}(L/L^H) \backslash \overline{H}$ es abierto, entonces si existiera $\sigma \in \mathrm{Gal}(L/L^H) \backslash \overline{H}$, existiría un conjunto finito S tal que

$$\sigma G(S) = \sigma\, \mathrm{Gal}(L/K(S)) \subseteq \mathrm{Gal}(L/L^H) \backslash \overline{H}.$$

Sea $E := K(S)$ y $\phi : \mathrm{Gal}(L/K) \to \mathrm{Gal}(E/K)$ el mapa que restringe, claramente suryectivo. Luego, $\phi(\sigma) = \sigma_{|_E} \notin \phi(H)$. En efecto, supongamos que existe $\tau \in H$ tal que $\tau_{|_E} = \sigma_{|_E}$, entonces $\tau(s) = \sigma(s) \quad \forall s \in E = K(S) \supseteq S$. Resulta así que $\tau \in \sigma G(S) \subseteq \mathrm{Gal}(L/L^H) \backslash \overline{H}$, lo cual es una contradicción, pues $\tau \in H$. Por lo tanto, como $\phi(\sigma) \notin \phi(H)$, σ mueve algún elemento de $E^{\phi(H)} \subseteq L^H$, lo cual es absurdo. □

Ahora sí estamos en condiciones de enunciar el teorema que explica la correspondencia de Galois para extensiones infinitas.

Teorema 1.2.11. Sea L/K una extensión de Galois y $G := \mathrm{Gal}(L/K)$. Entonces existe una correspondencia

$$\begin{array}{ccc} \{\text{subgrupos cerrados de } G\} & \longleftrightarrow & \{\text{subextensiones de } L/K\} \\ H & \longrightarrow & L^H \\ \mathrm{Gal}(L/F) & \longleftarrow & F \end{array}$$

que satisface:

(1) La correspondencia revierte contenciones. Es decir que $H_1 \subseteq H_2 \iff L^{H_1} \supseteq L^{H_2}$.

(2) $H < G$ es abierto si y sólo si L^H/K es finita, en cuyo caso, $[L^H : K] = [G : H]$.

(3) Si $\sigma \in G,\ H < G$, entonces $L^{\sigma H \sigma^{-1}} = \sigma(L^H)$.

(4) $H \lhd G \iff L^H/K$ es normal (y por lo tanto Galois). En tal caso, $\mathrm{Gal}(L^H/K) \cong G/H$.

Demostración: Se sigue de los resultados anteriores. Sólo resta ver (2). Para eso, veamos que $H < G$ cerrado es abierto si y sólo si $[G : H] < \infty$. Como

$$G = H \bigsqcup \left(\bigsqcup_{\substack{g \in G/H \\ g \neq 1}} gH \right)$$

entonces si H es abierto tenemos un cubrimiento abierto de G, que es compacto. Pero como el cubrimiento es disjunto entonces tiene que ser finito y esto implica que hay una cantidad finita de coclases, es decir, que $[G : H] < \infty$.

Recíprocamente, como H es cerrado y tenemos un cubrimiento finito, entonces

$$\bigsqcup_{\substack{g \in G/H \\ g \neq 1}} gH$$

es cerrado (pues es unión finita de cerrados) y luego, H es abierto. □

Capítulo 2

Representaciones de Galois

Dado un cuerpo K, las representaciones de Galois son muy estudiadas para poder entender el grupo $G_K := \mathrm{Gal}(\overline{K}/K)$.

Es sabido que conocer todas las representaciones de un grupo finito determina a éste unívocamente. Veamos entonces que G_K se puede ver como límite (inverso) de una sucesión de grupos finitos.

Definición 2.0.1. Sea $(I, \leq)$ un conjunto parcialmente ordenado dirigido. Sea $\{G_i\}_{i\in I}$ una familia de grupos finitos y $\psi_{ij} : G_j \to G_i$ para todo $i \leq j$ una familia de homomorfismos con las siguientes propiedades:

(1) ψ_{ii} es la identidad en G_i.

(2) $\psi_{ik} = \psi_{ij} \circ \psi_{jk}$ para todo $i \leq j \leq k$.

Definimos como **límite inverso** o **límite proyectivo** de la familia $(\{G_i\}, \{\psi_{ij}\})$ al grupo

$$\varprojlim G_i := \left\{ (g_i)_{i\in I} \in \prod_{i\in I} G_i : \psi_{ij}(g_j) = g_i \text{ para todo } i \leq j \right\}.$$

Es fácil ver que $G := \varprojlim G_i$ es un grupo con la multiplicación coordenada a coordenada. Más aún, podemos dotar a G con la topología menos fina de manera que las proyecciones canónicas $\pi_j : G \to G_j$ resulten continuas. Dicha topología será la topología **profinita**. Con la topología profinita, G resulta un grupo topológico. La siguiente proposición nos dice que los grupos de Galois de extensiones infinitas no son más que límites inversos de grupos de Galois de extensiones finitas.

Proposición 2.0.2. Si L/K es Galois entonces el mapa natural

$$\phi : \mathrm{Gal}(L/K) \to \varprojlim_{\substack{F\subseteq L,\\ F/K \text{ finita}\\ \text{y Galois}}} \mathrm{Gal}(F/K), \quad \sigma \to (\sigma_F)_F$$

es un isomorfismo de grupos topológicos.

Demostración: Por simplicidad, sean

$$G := \mathrm{Gal}(L/K) \quad \text{y} \quad E := \varprojlim_{\substack{F\subseteq L,\\ F/K \text{ finita}\\ \text{y Galois}}} \mathrm{Gal}(F/K).$$

Como G es compacto (por la Proposición 1.2.9) y E es Hausdorff (por ser todo límite inverso Hausdorff), basta ver que ϕ es biyectiva y continua (pues además es trivial que es morfismo de grupos).

Si $\phi(\sigma) = 1_E$, dado $\alpha \in L$, tomando $F = K(\alpha)$, tenemos que F es finita. Tomando la menor extensión de F que resulte Galois sigue siendo finita y σ restringida allí es trivial. Como ésta contiene a α entonces $\sigma(\alpha) = \alpha$, con lo cual ϕ es inyectiva. Para ver que ϕ es suryectiva, sea $\tau = (\tau_F)_F \in E$. Sea σ definida de la siguiente manera: dado $\alpha \in L$, tomamos una extensión finita F_1 de Galois que contenga a $K(\alpha)$ y definimos $\sigma(\alpha) := \tau_{F_1}(\alpha)$. Notemos que σ está bien definida, ya que si F_2 es otra extensión finita de Galois que contiene a $K(\alpha)$ entonces $\tau_{F_1}(\alpha) = \tau_{F_2}(\alpha)$, pues $\tau \in E$. Basta ver que $\sigma \in G$, pues en este caso es claro que $\phi(\sigma) = \tau$. Por un lado, es claro que $\sigma_{|_K} = Id_K$ y por otro lado, dado $\alpha, \beta \in L$, $K(\alpha, \beta)$ es finita y τ es un morfismo, luego, σ lo es.

Por último ϕ es continua porque compuesta con cada proyección es continua, por [Mil18, Proposición 7.7]. □

Si V es un k-espacio vectorial de dimensión n, donde k es un cuerpo topológico, tenemos un isomorfismo no canónico $\mathrm{Aut}_k(V) \cong \mathrm{GL}_n(k)$ dado por elegir una base (pues todo elemento de $\mathrm{Aut}_k(V)$ manda una base en otra).

Además, como $\mathrm{GL}_n(k)$ está contenido en $M_n(k)$ (el conjunto de matrices $n \times n$ con coeficientes en k) y $M_n(k) \cong k^{n^2}$, entonces dotando a $\mathrm{GL}_n(k)$ con la topología inducida de $M_n(k)$ resulta $\mathrm{Aut}_k(V)$ un espacio topológico.

Definición 2.0.3. Una **representación de Galois** es un morfismo continuo

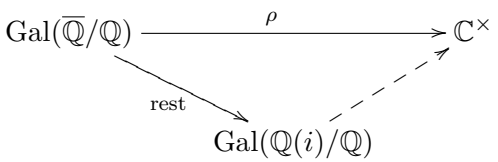
$$\rho : G_K \to \mathrm{Aut}_k(V).$$

Por lo tanto, podemos pensar que una representación es un morfismo continuo de G_K en $\mathrm{GL}_n(k)$.

Ejemplo 2.0.4. Si $n = 1$ y $k = \mathbb{C}$, entonces las representaciones de Galois son caracteres continuos de G_K (es decir, morfismos de grupos de G_K a $\mathbb{C}^\times$). Sea $K = \mathbb{Q}$. Si $\sigma \in G_\mathbb{Q}$ entonces $\sigma(i) = \pm i$. Definamos

$$\rho(\sigma) := \frac{\sigma(i)}{i} \in \{\pm 1\}.$$

Por definición, ρ es trivial en $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}(i))$. Luego, ρ factoriza por $\mathrm{Gal}(\mathbb{Q}(i)/\mathbb{Q})$, es decir que tenemos el siguiente diagrama:



Notemos que como $\mathrm{Gal}(\mathbb{Q}(i)/\mathbb{Q}) \cong \mathbb{Z}/2\mathbb{Z}$ entonces ρ es la representación no trivial de ese grupo y por lo tanto es un caracter. Además, la continuidad de ρ se deduce de que la imagen es discreta y por lo tanto basta ver que el núcleo es abierto, pero $\ker(\rho) = \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}(i)) = G(\{i\})$, que resulta ser un abierto básico.

Definición 2.0.5. Si $\rho_1,\ \rho_2$ son dos representaciones de Galois de G_K en $\mathrm{Aut}_k(V)$ decimos que son **equivalentes** si existe una transformación lineal $\psi \in \mathrm{Aut}_k(V)$ tal que

$$\rho_1(\sigma)(v) = \psi^{-1}(\rho_2(\sigma)(\psi(v)))\ \ \forall \sigma \in G_K,\ \ \forall v \in V.$$

Notemos que cuando identificamos $\mathrm{Aut}_k(V)$ con $\mathrm{GL}_n(V)$ estábamos fijando una base B de V y entonces podíamos pensar a una representación ρ de G_K en $\mathrm{Aut}_k(V)$ como una representación de Galois

$$\rho_B : G_K \to \mathrm{GL}_n(V).$$

Elegir otra base B' de V determina otra representación $\rho_{B'}$ que es equivalente a ρ_B.

Las siguientes definiciones serán útiles en la siguiente sección pero son enunciadas a continuación por mayor generalidad.

Definición 2.0.6. Una representación de Galois es de **dimensión** n si la dimensión de V como k-espacio vectorial es n y es **abeliana** si $\mathrm{Im}(\rho)$ es un grupo abeliano.

Definición 2.0.7. Dada una representación de Galois $\rho : G_K \to \mathrm{Aut}_k(V)$ se dice que un subespacio $U \subseteq V$ es **ρ-invariante** si

$$\rho(\sigma)U \subseteq U \quad \forall \sigma \in G_K.$$

Definición 2.0.8. Una representación de Galois $\rho : G_K \to \mathrm{Aut}_k(V)$ se dice **irreducible** si no existe un subespacio propio no nulo de V que sea ρ-invariante.

Observación 2.0.9. Si $\rho : G_K \to \mathrm{Aut}_k(V)$ es una representación de Galois y U es ρ-invariante entonces tenemos definida una representación de Galois $\rho : G_K \to \mathrm{Aut}_k(U)$.

Definición 2.0.10. Una representación de Galois $\rho : G_K \to \mathrm{Aut}_k(V)$ se dice **semi-simple** si V se puede descomponer como

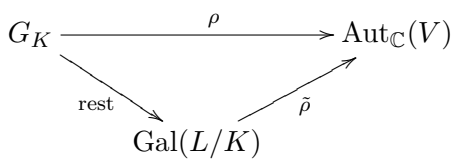
$$V = \bigoplus_i V_i,$$

donde cada V_i es ρ-invariante y las representaciones $\rho : G_K \to \mathrm{Aut}_k(V_i)$ son irreducibles.

2.1. Representaciones de Artin

Con la notación en la que venimos trabajando, una representación de Galois se dice que es un **representación de Artin** si $k = \mathbb{C}$.

Teorema 2.1.1. Si $\rho : G_K \to \mathrm{Aut}_{\mathbb{C}}(V)$ es una representación de Artin entonces ρ factoriza por una extensión finita. Es decir, existe L/K finita y $\tilde{\rho} : \mathrm{Gal}(L/K) \to \mathrm{Aut}_{\mathbb{C}}(V)$ inyectiva tal que el siguiente diagrama conmuta:



Demostración: Sea $H = \ker(\rho)$. Como ρ es un morfismo entonces H un subgrupo de G_K. Notemos que si H es abierto, entonces por el Lema 1.2.3, H es un subgrupo cerrado y entonces es de la forma $\mathrm{Gal}(\overline{K}/L)$, donde L/K es finita. Luego, ρ factoriza por $\mathrm{Gal}(\overline{K}/K)/H$, que resulta isomorfo a $\mathrm{Gal}(L/K)$, y es claro que $\widetilde{\rho}$ es inyectiva, pues U es el núcleo de ρ. Luego, basta ver que H es abierto.

Para eso, supongamos primero que $n = 1$, con lo cual tenemos $\rho : G_K \to \mathbb{C}^\times$. Sea U un entorno abierto del 1 en $\mathbb{C}^\times$ que no contenga subgrupos de $\mathbb{C}^\times$ no triviales (por ejemplo, tomar $U = B(1, \frac{1}{2})$). Como ρ es continua, entonces $\rho^{-1}(U)$ es abierto y más aún, un entorno de la identidad en G_K. Luego, existe un conjunto finito S tal que $G(S) \subseteq \rho^{-1}(U)$. Entonces $\rho(G(S)) \subseteq U$, pero como $G(S)$ es un subgrupo de G_K se tiene que $\rho(G(S))$ es un subgrupo de U y por lo tanto $\rho(G(S)) = \{1\}$. Es decir que $G(S) \subseteq H$ y por lo tanto H es abierto.

Para $n > 1$ la prueba es similar. Simplemente debemos encontrar un entorno de la matriz identidad $(n \times n)$ que no contiene subgrupos no triviales. La idea es tomar una bola centrada en la identidad de radio ε pequeño y fijo. Supongamos que tenemos un subgrupo H dentro de la bola. Todos los elementos de H resultan diagonalizables y si $M \in H$ tiene un autovalor λ entonces $|\lambda - 1| \leq \frac{1}{2}$ (para una elección de ε adecuada, que no depende de M). Pero como M es un elemento de H entonces sus potencias también, con lo cual $|\lambda^m - 1| \leq \frac{1}{2}$ para todo $m \in \mathbb{Z}$. Por lo tanto $\lambda = 1$ y M es la matriz identidad. □

Observación 2.1.2. Con la notación anterior, tenemos que

$$|\operatorname{Im}(\rho)| = |\operatorname{Im}(\tilde{\rho})| \leq |\operatorname{Gal}(L/K)| = [L : K] < \infty.$$

Por lo tanto ρ es de orden finito.

Teorema 2.1.3. Toda representación de Artin es semi-simple.

Demostración: Sea $\rho : G_K \to \mathrm{GL}_{\mathbb{C}}(V)$ una representación de Artin. Por el Teorema 2.1.1 sabemos que ρ factoriza por una extensión finita. O sea que existe L/K Galois y finita y $\tilde{\rho} : \mathrm{Gal}(L/K) \to \mathrm{GL}_{\mathbb{C}}(V)$ tal que $\rho = \tilde{\rho} \circ \mathrm{rest}$, donde $\mathrm{rest} : G_K \to \mathrm{Gal}(L/K)$ es la función restringir. Luego, el resultado sigue del Teorema de Maschke (que afirma que toda representación de un grupo finito G en un $\mathbb{C}$-espacio vectorial V tal que la característica de k no divide al orden de G es semi-simple). Ver [Mas98]. □

Observación 2.1.4. En general no vale que toda representación de Galois es semi-simple. Usamos fuertemente que $k = \mathbb{C}$. Para ver esto, tomemos $K = \mathbb{Q}$, L como el cuerpo de descomposición del polinomio $x^3 - 3x - 1$ y $k = \mathbb{F}_3$. Viendo el discriminante del polinomio es fácil notar que $\mathrm{Gal}(L/K)$ es cíclio de orden 3. Luego,

$$\rho : C_3 \cong \mathrm{Gal}(L/K) \to \mathrm{GL}_2(\mathbb{F}_3), \quad [1] \mapsto \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$$

resulta una representación de Galois que no es semi-simple, pues el subespacio $\langle (1, 0) \rangle$ es invariante pero no tiene complemento invariante.

Proposición 2.1.5. Una representación de Artin irreducible es abeliana si y sólo si es de dimensión 1. Además, con la notación del Teorema 2.1.1 tenemos en este caso que L/K es abeliana.

Demostración: Sea $\rho : G_K \to \mathrm{GL}_{\mathbb{C}}(V)$ una representación de Artin irreducible abeliana y veamos que es de dimensión 1. Sea $\sigma \in G_K$ y $v \in V$ autovector de $\rho(\sigma)$ no nulo con autovalor $\lambda \in \mathbb{C}$. Notemos que $\ker(\rho(\sigma) - \lambda Id)$ es un subespacio no trivial de V que resulta ρ-invariante. En efecto, si $w \in \ker(\rho(\sigma) - \lambda Id)$ y $\tau \in G_K$ entonces

$$\rho(\sigma)(\rho(\tau)w) = \rho(\tau)\rho(\sigma)w = \rho(\tau)\lambda w = \lambda(\rho(\tau)w),$$

donde la primera igualdad vale por ser ρ abeliana. Dicha igualdad nos dice que $\rho(\tau)w \in \ker(\rho(\sigma) - \lambda Id)$ y por lo tanto vale la afirmación.

Luego, como ρ es irreducible entonces $\ker(\rho(\sigma) - \lambda Id) = V$, es decir que todo vector es autovector de $\rho(\sigma)$. Como σ es arbitrario $\langle v \rangle$ es ρ-invariante y por lo tanto $\langle v \rangle = V$. Es decir que ρ es de dimensión 1.

La recíproca es trivial y L/K resulta abeliana porque al ser $\widetilde{\rho}$ inyectiva entonces el grupo de Galois $\mathrm{Gal}(L/K)$ es isomorfo a $\mathrm{Im}(\widetilde{\rho}) < \mathbb{C}^\times$ y $\mathbb{C}^\times$ es abeliano. □

Capítulo 3
Valores absolutos y completaciones

3.1. Números p-ádicos

En esta sección vamos a introducir la noción de números p-ádicos, donde p es un número primo. Éstos van a formar un cuerpo que extenderá a $\mathbb{Q}$. Fueron descriptos por primera vez por Kurt Hensel en 1897 y tienen un rol muy importante en el Teorema de Hasse-Minkowski, que sirve para saber si determinado tipo de ecuaciones poseen soluciones racionales. Más información se puede encontrar en [Kob84].

Dado p un número primo fijo, sabemos por el Teorema Fundamental de la Aritmética que para cada $a \in \mathbb{Z}$ existe un único $n \in \mathbb{Z}_{\geq 0}$ tal que $a = p^n r$, con $(r, p) = 1$. Esto nos permite dar la siguiente definición.

Definición 3.1.1. Definimos la **valuación p-ádica** como una función $v_p : \mathbb{Z} \setminus \{0\} \to \mathbb{Z}$ tal que

$$v_p(x) = \text{máx}\{n \in \mathbb{Z} : p^n \mid x\}$$

Notemos que $v_p(ab) = v_p(a) + v_p(b)$. Esto último nos dice que podemos extender la valuación a $\mathbb{Q}^\times$ de manera que resulte un morfismo de grupos. Finalmente, también definimos la valuación p-ádica en 0 como ∞. Es decir que tenemos $v_p : \mathbb{Q} \to \mathbb{Z} \cup \{\infty\}$ definida como

$$v_p\left(\frac{a}{b}\right) = \begin{cases} v_p(a) - v_p(b) & \text{si} \quad a \neq 0, \\ \infty & \text{si} \quad a = 0. \end{cases}$$

Esta función está bien definida porque si $a/b = c/d \in \mathbb{Q}$ entonces $ad = bc$. Luego, vale que $v_p(a) + v_p(d) = v_p(ad) = v_p(bc) = v_p(b) + v_p(c)$ (por la siguiente proposición) y por lo tanto

$$v_p\left(\frac{a}{b}\right) = v_p(a) - v_p(b) = v_p(c) - v_p(d) = v_p\left(\frac{c}{d}\right).$$

Proposición 3.1.2. Sean $x, y \in \mathbb{Q}$, entonces:

(1) $v_p(xy) = v_p(x) + v_p(y)$.

(2) $v_p(x + y) \geq \text{mín}\{v_p(x), v_p(y)\}$.

Demostración:

(1) Extendimos la función a $\mathbb{Q}^\times$ de tal manera que resulte morfismo de grupos. Supongamos ahora sin pérdida de generalidad que $x = 0$, entonces tenemos

$$v(xy) = v(0) = \infty = \infty + v(y) = v(x) + v(y).$$

(2) Supongamos que $x = \frac{r_1}{r_2}p^n$, $y = \frac{s_1}{s_2}p^m$, con $(r_i, p) = (s_i, p) = 1$ para $i = 1, 2$. Supongamos sin pérdida de generalidad que $n \leq m$. Entonces

$$x + y = \frac{r_1}{r_2}p^n + \frac{s_1}{s_2}p^m = \left(\frac{r_1 s_2 + s_1 r_2 p^{m-n}}{r_2 s_2}\right) p^n$$

Si $m - n > 0$ entonces $(p, r_1 s_2 + s_1 r_2 p^{m-n}) = (p, r_2 s_2) = 1$. Luego $v_p(x + y) = n = v_p(x)$. Si $m = n$, como $v_p(r_2 s_2) = 1$ y $v_p(r_1 s_2 + s_1 r_2) \geq 0$, tenemos entonces por inciso (1) que $v_p(x + y) \geq n = v_p(x) = v_p(y)$.

□

Observación 3.1.3. En la prueba de (2) pudimos ver algo más fuerte:

$$v_p(x + y) \geq \text{mín}\{v_p(x), v_p(y)\} \text{ y la igualdad vale si } v_p(x) \neq v_p(y).$$

Notemos ahora que esta valuación nos permite definir un valor absoluto (en el sentido usual) en $\mathbb{Q}$.

Definición 3.1.4. Dado un número primo p definimos la función $|.|_p$ en $\mathbb{Q}$ como

$$|x|_p = \begin{cases} p^{-v_p(x)} & \text{si} \quad x \neq 0, \\ 0 & \text{si} \quad x = 0. \end{cases}$$

Es fácil ver que $|.|_p$ es un valor absoluto (en el sentido usual) en $\mathbb{Q}$. Más aún, de la Observación 3.1.3 se sigue que

$$|x + y|_p \leq \text{máx}\{|x|_p, |y|_p\} \text{ y si } |x|_p \neq |y|_p \text{ entonces se verifica la igualdad.}$$

Definición 3.1.5. Diremos que dos valores absolutos $|.|_1$, $|.|_2$ en $\mathbb{Q}$ son **equivalentes** si existe alguna constante $c \in \mathbb{R}_{\geq 0}$ tal que

$$|.|_1 = |.|_2^c$$

para todo $x \in \mathbb{Q}$.

Cabe aclarar que uno podría haber definido a la norma $|\cdot|_p$ como

$$|x|_p = \begin{cases} c^{-v_p(x)} & \text{si} \quad x \neq 0, \\ 0 & \text{si} \quad x = 0. \end{cases}$$

para cualquier $c > 1$ y esta nueva norma sería equivalente a la ya definida. La razón por la cual tomamos $c = p$ la veremos en breve.

Definición 3.1.6. Llamamos **valor absoluto trivial** a la función

$$|x| = \begin{cases} 1 & \text{si} \quad x \neq 0, \\ 0 & \text{si} \quad x = 0. \end{cases}$$

Denotamos a la norma usual como $|\cdot|_\infty$. Esta notación junto con la definición anterior dan a lugar al siguiente teorema que incentiva a estudiar las normas p-ádicas.

Teorema 3.1.7. (Ostrowski) Todo valor absoluto no trivial en $\mathbb{Q}$ es equivalente a $|.|_p$ donde p es un número primo o $p = \infty$.

Demostración: Ver [Cas67, página 45], [Kob84, Teorema 1] o más en general [Sha66, páginas 278–280]. □

La relación definida en la Definición 3.1.5 resulta una relación de equivalencia. Llamaremos **lugar** a cada clase de equivalencia no trivial y al conjunto de lugares lo denotaremos como $M_{\mathbb{Q}}$. Denotaremos con la letra v a los lugares y en general a un representante del lugar v lo denotaremos como $|.|_v$. Por el Teorema de Ostrowski, si $v \in M_{\mathbb{Q}}$ entonces $|.|_v$ es equivalente a $|.|_p$ para algún primo p o para $p = \infty$. De ahora en adelante vamos a tomar a $|.|_v$ como dicha norma. A continuación, damos el lema que le da sentido tomar $c = p$ en la Definición 3.1.4.

Lema 3.1.8. (Fórmula del producto para $\mathbb{Q}$) Tomando $|.|_v$ como se dijo anteriormente se tiene que

$$\prod_{v \in M_{\mathbb{Q}}} |x|_v = 1$$

Demostración: La función

$$f(x) := \prod_{\substack{p \text{ primo}, \\ p=\infty}} |x|_p$$

está bien definida, ya que dado $x \in \mathbb{Q}$, $|x|_p = 1$ para casi todo p. Más aún, el conjunto de primos para los cuales $|x|_p \neq 1$ es exactamente el que contiene a aquellos que dividen al numerador o al denominador (asumiendo que escribimos a x como fracción irreducible). Por otro lado, $|x|_\infty = 1$ si y sólo si $x = \pm 1$.

Además, como cada norma es multiplicativa entonces f lo es y por lo tanto basta ver que la afirmación se cumple para los primos enteros. Esto último es trivial, ya que

$$f(p) = |p|_\infty |p|_p = p\frac{1}{p} = 1.$$

Queda así probada la fórmula. □

Es sabido que toda norma induce una distancia, lo que nos da a lugar a la siguiente definición.

Definición 3.1.9. Definimos la **métrica p-ádica** en $\mathbb{Q}$ como $d_p(x, y) = |x - y|_p$.

De la misma manera en la que uno completa a $\mathbb{Q}$ con la métrica usual (la euclídea) y obtiene $\mathbb{R}$, podemos completar ahora pero respecto de nuestra nueva métrica.

Definición 3.1.10. Definimos el conjunto de los **números p-ádicos** como la completación de $\mathbb{Q}$ respecto de la métrica d_p. A este conjunto lo denotaremos como $\mathbb{Q}_p$.

Es fácil ver que si completamos $\mathbb{Q}$ con dos métricas que provienen de normas equivalentes, entonces las completaciones resultan iguales. La recíproca también es cierta, es decir que $\mathbb{Q}_p$ y $\mathbb{Q}_q$ son realmente distintos como espacios topológicos si $p \neq q$, pues $p^n \to 0$ en $\mathbb{Q}_p$ mientras que $|p^n|_q = 1$.

En $\mathbb{Q}_p$ consideramos la topología inducida por la métrica p-ádica. Obviamente, considerado como espacio métrico, $\mathbb{Q}_p$ resulta completo y $\mathbb{Q}$ es denso en $\mathbb{Q}_p$. Por otro lado, $\mathbb{Q}_p$ resulta un anillo topológico con las operaciones naturales.

3.2. Valores absolutos para cuerpos aribitrarios

Veremos en esta sección que lo hecho para $\mathbb{Q}$ en la sección anterior no es más que un caso particular de lo que podemos hacer para un cuerpo de números arbitrario K. Al igual que en $\mathbb{Q}$, vamos a intentar dotar a K de una topología, que va a depender de las distintas métricas que podamos aportarle. Para la primera parte, basta tomar K un cuerpo genérico.

Definición 3.2.1. Un **valor absoluto** de K es una función $|\cdot| : K \to \mathbb{R}$ tal que:

(1) $|x| \geq 0$ para todo $x \in K$ y $|x| = 0$ si y sólo si $x = 0$.

(2) $|xy| = |x||y|$ para todos $x, y \in K$.

(3) $|x + y| \leq |x| + |y|$ para todos $x, y \in K$.

Si en vez de (3), el valor absoluto satisface la propiedad aún más fuerte

(3') $|x + y| \leq \text{máx}\{|x|, |y|\}$ para todos $x, y \in K$,

decimos que el valor absoluto es **no arquimediano**.

Observación 3.2.2. Notemos que:

(1) Podemos ver a un valor absoluto como un morfismo de grupos $|.| : K^\times \to \mathbb{R}_{\geq 0}$ que se extiende a $|0| = 0$ y que satisface (3).

(2) Si $K = \mathbb{Q}$ y p es un número primo entonces $|.|_p$ es no arquimediano.

Al igual que en $\mathbb{Q}$, siempre existe el valor absoluto trivial. De ahora en adelante nos vamos a ocupar de los valores absolutos no triviales.

Es sabido que un valor absoluto $|.|$ define una distancia $d : K \times K \to \mathbb{R}$ de la forma $d(x, y) := |x - y|$. En consecuencia, cada valor absoluto nos va a determinar una topología en nuestro cuerpo K, inducida por la métrica dada. Esto no es muy llamativo, ya que es lo mismo que ocurría para $\mathbb{Q}$, y de la misma manera, da lugar a la siguiente definición.

Definición 3.2.3. Dos valores absolutos $|.|_1, |.|_2$ en K se dicen **equivalentes** si existe $c \in \mathbb{R}_{\geq 0}$ tal que

$$|.|_1 = |.|_2^c.$$

Podemos definir una relación de equivalencia dentro del conjunto de valores absolutos. A su vez, esta nos dice que los valores absolutos equivalentes son elementos de una misma clase.

Observación 3.2.4. La clase de equivalencia del valor absoluto trivial se compone sólo de éste.

Recordemos que decimos que un valor absoluto es no arquimediano si cumple (3'). También, diremos que es **arquimediano** si no es no arquimediano. Nos gustaría hablar ahora de clases de valores absolutos arquimedianos. Para eso es necesario el siguiente lema.

Lema 3.2.5. Sean $|.|_1, |.|_2$ dos valores absolutos de K equivalentes. Entonces $|.|_1$ es arquimediano si y sólo si $|.|_2$ es arquimediano.

Demostración: Supongamos que $|.|_1$ es no arquimediano. Esto significa que vale (3'). Veamos que $|.|_2$ también lo cumple. Como $|.|_1$ y $|.|_2$ son equivalentes, existe c positivo tal que $|.|_2 = |.|_1^c$. Sean $x, y \in K$, entonces

$$|x+y|_2 = |x+y|_1^c \leq (\text{máx}\{|x|_1, |y|_1\})^c = \text{máx}\{|x|_1^c, |y|_2^c\} = \text{máx}\{|x|_2, |y|_2\}.$$

Luego, $|.|_2$ es no arquimediano. □

Definición 3.2.6. Una clase de equivalencia de valores absolutos no triviales se llamará un **lugar** de K.

Al igual que en $\mathbb{Q}$ usaremos la letra v para denotar un lugar de K, y por $|.|_v$ a un valor absoluto que lo represente.

Como lo anticipamos antes, el Lema 3.2.5 nos permite hablar de lugares arquimedianos y lugares no arquimedianos. Para preservar la analogía con $\mathbb{Q}$, a veces llamamos a los arquimedianos como **infinitos** y a los otros como **finitos**. Dado un cuerpo K, denotaremos por M_K el conjunto de todos sus lugares.

A partir de ahora K será un cuerpo de números. En el siguiente ejemplo veremos más explícitamente cómo esto generaliza el caso de $\mathbb{Q}$.

Ejemplo 3.2.7. Sea $\mathfrak{p} \subset \mathcal{O}_K$ un ideal primo. Si $x \in K^\times$, definimos $ord_\mathfrak{p}(x)$ como la máxima potencia en la que aparece $\mathfrak{p}$ en la descomposición en primos de (x), que tambien denotaremos como $v_\mathfrak{p}((x))$. Tomemos $c > 1$ un número real arbitrario y definamos el valor absoluto en K

$$|x|_\mathfrak{p} = c^{-ord_\mathfrak{p}(x)}.$$

Es fácil ver que $|.|_\mathfrak{p}$ es un valor absoluto y claramente es no arquimediano. El siguiente lema nos dice que es indiferente el valor de c que tomemos (siempre y cuando sea mayor a 1) ya que todos ellos definen valores absolutos equivalentes.

Lema 3.2.8. Sea $\mathfrak{p}$ un primo de K y $c_1, c_2 > 1$. Entonces $|x|_1 := c_1^{-ord_\mathfrak{p}(x)}$ es equivalente a $|x|_2 := c_2^{-ord_\mathfrak{p}(x)}$

Demostración: Si $t := \log_{c_1}(c_2)$ tenemos que $c_1 = c_2^t$ y por lo tanto $|.|_1 = |.|_2^t$. □

Es común tomar $c = N(\mathfrak{p})$. Llamamos a este valor absoluto **$\mathfrak{p}$-ádico** y a su clase de equivalencia la denotaremos $v_\mathfrak{p}$.

Al igual que en $\mathbb{Q}$, tenemos que primos distintos nos dan valores absolutos no equivalentes. Por otro lado también es cierto que todo valor absoluto no arquimediano en K es equivalente a uno de éstos. En el caso de $\mathbb{Q}$ esto no es otra cosa que el Teorema de Ostrowski.

Es claro que dados $x, c \in \mathbb{R}_{\geq 0}$, entonces

$$x \leq 1 \Leftrightarrow x^c \leq 1, \quad x = 1 \Leftrightarrow x^c = 1 \quad \text{y} \quad x < 1 \Leftrightarrow x^c < 1.$$

Esto nos dice que dado un lugar v finito están bien definidos los siguiente conjuntos:

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

Lema 3.2.9. Si v es un lugar finito de K, entonces:

(1) $\mathcal{O}_v$ es un subanillo de K.

(2) $\text{Frac}(\mathcal{O}_v) = K$.

(3) $\mathcal{O}_v^\times = \mathcal{U}_v$.

(4) $\mathfrak{p}_v$ es un ideal de $\mathcal{O}_v$. Más aún, $\mathcal{O}_v$ es un anillo local y $\mathfrak{p}_v$ es su ideal maximal.

Demostración:

(1) Dados $x, y \in \mathcal{O}_v$, entonces $xy \in \mathcal{O}_v$ por la propiedad (2) de la definición de valor absoluto y $x + y \in \mathcal{O}_v$ por ser éste además arquimediano (y por lo tanto satisfacer la propiedad (3') de dicha definición).

(2) Como (1) es cierta, entonces es inmediato que $\text{Frac}(\mathcal{O}_v) \subseteq K$. Recíprocamente, si $x \in K$ entonces hay dos opciones: si $|x|_v \leq 1$ entonces $x \in \mathcal{O}_v \subseteq \text{Frac}(\mathcal{O}_v)$. Caso contrario, entonces $|x|_v > 1$ y luego $|1/x|_v < 1$. Por lo tanto, $1/x \in \mathcal{O}_v$, de lo que se sigue que $x \in \text{Frac}(\mathcal{O}_v)$.

(3) Si $x \in \mathcal{O}_v^\times$ entonces por definición, $|x|_v \leq 1$. Además, como x es una unidad en $\mathcal{O}_v$ entonces $1/x \in \mathcal{O}_v$ y luego $|1/x|_v \leq 1$, lo cual implica $|x|_v \geq 1$. Por lo tanto, $|x|_v = 1$, lo que nos dice que $x \in \mathcal{U}_v$.
La recíproca (también) es trivial, porque si $|x|_v = 1$ entonces $|1/x|_v = 1$.

(4) La primera afirmación es cierta porque si $xy \in \mathfrak{p}_v$ entonces $|xy|_v \leq 1$ y luego $|x|_v < 1$ o $|y|_v < 1$. Es decir, $x \in \mathfrak{p}_v$ o $y \in \mathfrak{p}_v$.

La segunda afirmación resulta de que

$$\mathfrak{p}_v = \mathcal{O}_v \setminus \mathcal{U}_v = \mathcal{O}_v \setminus \mathcal{O}_v^\times$$

Resulta así probado el lema. □

Al anillo local $\mathcal{O}_v$ lo llamamos **anillo de enteros** de K respecto de v.

Lema 3.2.10. Sea v un lugar finito de K, entonces $\mathcal{O}_K \subseteq \mathcal{O}_v$

Demostración: Si $\alpha \in \mathcal{O}_K$, entonces $ord_v(\alpha) \geq 0$ y luego $c^{-ord_v(\alpha)} \leq 1$. □

Más aún, si para cada subconjunto S de M_K que contiende a S_∞ definimos

$$\mathcal{O}_{K,S} = \{x \in K : |x|_v \leq 1 \ \forall v \notin S\}$$

entonces se cumple que $\mathcal{O}_K = \mathcal{O}_{K,S_\infty}$.

Recordemos que dado un primo $\mathfrak{p}$ de K teníamos definido un lugar finito v cuyo representante podía ser tomado como el valor absoluto $|x|_\mathfrak{p} = c^{-\text{ord}_\mathfrak{p}(x)}$ con $c > 1$. Es claro entonces que $\mathfrak{p}_v = \mathfrak{p}$. Recíprocamente, dado un lugar finito v, si miramos el lugar que define el primo $\mathfrak{p}_v$ entonces volvemos a obtener v. Esto nos dice que hablar de lugares finitos y primos de K es

lo mismo. Por simplicidad denotaremos a veces como $\mathrm{ord}_v(x)$ a $\mathrm{ord}_{\mathfrak{p}_v}(x)$ si estamos hablando de lugares finitos en vez de primos.

En el caso $K = \mathbb{Q}$ vimos que cada lugar finito v viene dado por un primo p y obtenemos así

$$\mathcal{O}_v = \mathbb{Z}_{(p)}, \quad \mathcal{U}_v = \mathbb{Z}_{(p)}^{\times}, \quad \mathfrak{p}_v = p\mathbb{Z}_{(p)},$$

donde $\mathbb{Z}_{(p)}$ es el anillo de los enteros localizado en el ideal primo (p). Es sabido que

$$\mathbb{Z}_{(p)}/p\mathbb{Z}_{(p)} \cong \mathbb{Z}/p\mathbb{Z}.$$

En general vale que si $\mathfrak{p}$ es un primo de K que define un lugar v, entonces por el Lema 3.2.10 tenemos

$$\mathcal{O}_K \to \mathcal{O}_v \to \mathcal{O}_v \,/\, \mathfrak{p}_v$$

que resulta suryectivo y con núcleo $\mathcal{O}_K \cap \mathfrak{p}_v = \mathfrak{p}$. Por lo tanto, $\mathcal{O}_v \,/\, \mathfrak{p}_v \cong \mathcal{O}_K \,/\, \mathfrak{p}$. En particular esto nos dice que $|\, \mathcal{O}_v \,/\, \mathfrak{p}_v \,| = N(\mathfrak{p}) < \infty$.

3.3. Topología dada por un valor absoluto

Es sabido que lo hecho en $\mathbb{Q}$ para dotarlo de una topología no tiene nada en especial. De hecho, si estamos trabajando con un cuerpo K dotado de un valor absoluto $|.|$ entonces podemos definir una topología que tenga como abiertos básicos a las bolas $B(a, \delta) := \{x \in K : |x - a| < \delta\}$, donde $a \in K$ y $\delta > 0$.

Proposición 3.3.1. Dos valores absolutos en K son equivalentes si y sólo si inducen la misma topología.

Demostración: Es claro que si dos valores absolutos son equivalentes entonces definen la misma bola unidad y luego que inducen la misma topología.

Recíprocamente, supongamos que $|.|_1, |.|_2$ son dos valores absolutos que inducen la misma topología en K. Como el conjunto de los x tales que $|x|_1 < 1$ es exactamente el conjunto de los x tales que $x^n \to 0$ cuando $n \to \infty$ (con el valor absoluto $|.|_1$) y las topologías inducidas son las mismas, entonces la sucesión $\{x^n\}$ también converge a 0 con el valor absoluto $|.|_2$ y por lo tanto $|x|_1 < 1$ si y sólo si $|x|_2 < 1$. Como $|.|_1$ no es trivial entonces existe $y \in K$ tal que $|y|_1 > 1$. Sea c tal que $|y|_2 = |y|_1^c$ y veamos que $|.|_2 = |.|_1^c$.

Si $x \in K^{\times}$ entonces existe b real tal que $|x|_1 = |y|_1^b$. Veamos que $|x|_2 = |y|_2^b$. Sea m/n, $n > 0$ un número racional mayor que b. Entonces $|x|_1 = |y|_1^b < |y|_1^{m/n}$ y por lo tanto $|x^n/y^m|_1 < 1$. Luego, por lo dicho antes, $|x^n/y^m|_2 < 1$ y $|x|_2 \leq |y|_2^{m/n}$. Como vale para todos los raciones mayores a b entonces $|x|_2 \leq |y|_2^b$. Análogamente, tomando los racionales menores a b vemos que $|x|_2 \geq |y|_2^b$ y luego vale la igualdad. Así,

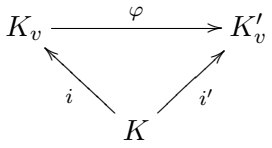
$$|x|_2 = |y|_2^b = |y|_1^{bc} = |x|_1^c.$$

Por lo tanto, $|.|_1$ y $|.|_2$ son equivalentes. □

En particular, esto prueba que la definición dada de valores absolutos equivalentes coincide con la dada para $\mathbb{Q}$.

Gracias a la Proposición 3.3.1 tenemos derecho a hablar de topologías inducidas por un lugar v de K. De la misma forma que la usual, uno puede decir que K es **completo** si toda sucesión de Cauchy converge (con el valor absoluto $|.|_v$).

Proposición 3.3.2. Dado un cuerpo K y un lugar v, existe un par (K_v, i) que consiste en un cuerpo completo K_v respecto a un valor absoluto $|.|$ y una inclusión $i : K \hookrightarrow K_v$ tal que $|x|_v = |i(x)| \ \ \forall x \in K$ y tal que K es denso en K_v. Más aún, si (K'_v, i') es otro par con esta propiedad, entonces existe un único homeomorfismo de cuerpos $\varphi : K_v \to K'_v$ que preserva el valor absoluto y hace que el siguiente diagrama sea conmutativo:



Demostración: La prueba de la existencia es esencialmente lo mismo que ocurre cuando formamos $\mathbb{R}$ completando a $\mathbb{Q}$ con la norma euclídea. Consideramos las sucesiones de Cauchy en K respecto del valor absoluto $|.|_v$ y notamos que forma un anillo, con las operaciones de suma y multiplicación componente a componente. Diremos además que una sucesión $\{x_n\}$ es equivalente a la sucesión $\{0\}$ si $\lim\limits_{n\to\infty} x_n = 0$. Luego, las sucesiones equivalentes a las nulas forman un ideal maximal. Cocientando entonces el anillo de las sucesiones de Cauchy por dicho ideal obtenemos el cuerpo K_v deseado. Resultan así dos sucesiones $\{x_n\}$ e $\{y_n\}$ en K equivalentes si $\lim\limits_{n\to\infty}(x_n - y_n) = 0$. Por un lado, es claro que K se incrusta en K_v vía la función i, que a un x lo manda a la clase de la sucesión constantemente x. Por otro lado, vamos a considerar el valor absoluto $|.|$ en K_v que se define como

$$\left|\overline{\{x_n\}}\right| := \lim_{n\to\infty} |x_n|_v.$$

Notemos que el valor absoluto está bien definido ya que como $\{|x_n|_v\}$ es una sucesión de Cauchy en $\mathbb{R}$, entonces converge y además claramente no dependen del representante que tomemos. Luego,

$$|i(x)| = \left|\overline{\{x\}}\right| = \lim_{n\to\infty} |x|_v = |x|_v.$$

Para terminar la prueba de la existencia, resta ver entonces que K_v es completo respecto a este valor absoluto. Para eso, tomemos una sucesión $\{\overline{u_n}\}$ de Cauchy en K_v con $u_n = \{x_{n,k}\}_k$ y veamos que converge. Probemos esto último en tres pasos:

(1) Para cada $n \in \mathbb{N}$ existe $v_n = \{y_{n,k}\}$ tal que $\overline{v_n} = \overline{u_n}$ y

$$| \, y_{n,p} - y_{n,q} \, | < \frac{1}{n} \quad \text{para todo} \quad p, q > 0.$$

Demostración: Como $\{x_{n,k}\}$ es de Cauchy entonces existe $N = N(n)$ tal que

$$| \, x_{n,p} - x_{n,q} \, | < \frac{1}{n} \quad \text{para todo} \quad p, q > 0.$$

Como omitir los primeros N términos de u_n no cambia la clase entonces podemos reenumerar y definir $v_n := \{y_{n,j}\}$ con $y_{n,j} = x_{n,N+j}$, que satisface lo que queríamos.

(2) $\{y_{n,1}\}$ es una sucesión de Cauchy en K.

Demostración: Dado $\varepsilon > 0$, como $\{v_n\}$ es de Cauchy, existe $N = N(\varepsilon)$ tal que

$$| \, v_n - v_m \, | = \lim_{k\to\infty} | \, y_{n,k} - y_{m,k}| < \frac{\varepsilon}{3} \tag{3.1}$$

para todo $n, m \geq N$. Sea $s > \text{máx}\{N(\varepsilon),\, 3/\varepsilon\}$. Entonces $1/s < \varepsilon/3$ y (3.1) vale para todo $n, m > s$. Ahora, viendo el límite en (3.1), existe N_1 tal que

$$| y_{n,k} - y_{m,k} | < \frac{\varepsilon}{3} \quad \text{para todo} \quad n, m > N_1.$$

Así, tomando $q := 1 + N_1$ y usando la desigualdad triangular tenemos que

$$\begin{aligned} | y_{n,1} - y_{m,1} | &\leq | y_{n,1} - y_{n,q} | + | y_{n,q} - y_{m,q} | + | y_{m,q} - y_{m,1} | \\ &\leq \frac{1}{n} + \frac{\varepsilon}{3} + \frac{1}{m} < \frac{\varepsilon}{3} + \frac{\varepsilon}{3} + \frac{\varepsilon}{3} < \varepsilon \end{aligned}$$

para todo $n, m > s$. Por lo tanto $\{y_{n,1}\}$ es de Cauchy.

(3) $\{v_n\}$ converge a $y = \{y_{n,1}\}$.

Demostración: Queremos ver que

$$| v_n - y | = \lim_{t \to \infty} | y_{n,t} - y_{t,1} | \tag{3.2}$$

tiende a 0 cuando $n \to \infty$. Dado $\varepsilon > 0$, existe M_0 tal que

$$| y_{n,1} - y_{m,1} | < \frac{\varepsilon}{2} \quad \text{para todo} \quad n, m > M_0.$$

Sea $M > \text{máx}\{M_0, 2/\varepsilon\}$. Entonces $1/M < \varepsilon/2$ y (3.2) vale para $n, m > M$. Luego, usando nuevamente la desigualdad triangular y (1), se tiene que

$$\begin{aligned} | y_{n,t} - y_{t,1} | &\leq | y_{n,t} - y_{n,1} | + | y_{n,1} - y_{t,1} | \\ &\leq \frac{1}{n} + \frac{\varepsilon}{3} < \varepsilon \end{aligned}$$

para todo $n, m > M$, probando así lo que queríamos.

Luego, como $\{v_n\}$ converge entonces $\{u_n\}$ también y queda probada la existencia.

Para ver la unicidad, supongamos que (K'_v, i') es otro par que cumple lo mismo. Dado $a = \overline{\{a_n\}} \in K_v$, entonces como $\{a_n\}$ es de Cauchy en K, $\{i'(a_n)\}$ es de Cauchy en K'_v y por lo tanto converge. Sea $\varphi : K_v \to K'_v$ como

$$\varphi(a) = \lim_{n \to \infty} i'(a_n).$$

Se puede ver que φ está bien definida, preserva el valor absoluto y que claramente $\varphi \circ i = i'$. Además preserva las operaciones de cuerpos. Análogamente existe $\phi : K'_v \to K_v$ tal que $\phi \circ i' = i$ y cumple las mismas propiedades que φ. Por lo tanto,

$$(\phi \circ \varphi)(a) = \phi\left(\lim_{n \to \infty} i'(a_n)\right) = \lim_{n \to \infty} \phi(i'(a_n)) = \lim_{n \to \infty} i(a_n) = a.$$

Es decir que $\phi \circ \varphi = Id_{K_v}$ y análogamente $\varphi \circ \phi = Id_{K'_v}$. Queda probado entonces que ϕ es un homeomorfismo de cuerpos.

Por último, si existiera $\varphi' : K_v \to K'_v$ que hace conmutar el diagrama y preserva el valor absoluto, entonces

$$\varphi'(a) = \lim_{n \to \infty} \varphi'(i(a_n)) = \lim_{n \to \infty} i'(a_n) = \varphi(a).$$

Queda así finalizada la proposición. □

Dado que para cada lugar v de K vamos a obtener uno de estos pares (salvo isomorfismo), vamos a denotar a tal par por (K_v, σ_v), donde σ_v es la inclusión de la proposición. Al valor absoluto de K_v que extiende a $|.|_v$ también la denotaremos como $|.|_v$.

Definición 3.3.3. A un par como el de la Proposición 3.3.2 lo llamaremos **completación** de K (respecto del lugar v). Más adelante, sólo nos referiremos como completación al cuerpo K_v.

Supongamos que v es un lugar arquimediano de K. Entonces $|.|_v$ en $\mathbb{Q}$ es equivalente a $|.|_\infty$ y como K_v es completo, se sigue que K_v contiene a la completación de $\mathbb{Q}$ con la norma usual, i.e., $K_v \supseteq \mathbb{R}$. Además, como K es un cuerpo de números entonces $\mathbb{C} \supseteq K_v$ y luego $K_v = \mathbb{R}$ o $K_v = \mathbb{C}$.

Vimos que un primo $\mathfrak{p}$ de K define un lugar v de K no arquimediano. Supongamos ahora que tenemos un morfismo $\sigma : K \to \mathbb{C}$. Entonces éste nos define un valor absoluto arquimediano dado por

$$|\alpha|_\sigma := |\sigma(\alpha)|.$$

En general diremos que σ es **real** si $\sigma(K) \subseteq \mathbb{R}$ y diremos que es **compleja** si no es real. Es claro entonces que si $\sigma : K \to \mathbb{C}$ es un morfismo y K_σ es la completación de K respecto de $|.|_\sigma$ resulta que $K_\sigma = \mathbb{R}$ si y sólo si σ es real.

Por definición, si σ es real entonces $\overline{\sigma} = \sigma$ y si es compleja $\overline{\sigma} \neq \sigma$. Luego, la cantidad de morfismos $\sigma : K \to \mathbb{C}$ que son complejos es par. Entonces, si K es un cuerpo de números de grado n, por teoría de Galois existen n morfismos $\sigma_i : K \to \mathbb{C}$. Suponiendo que hay r_1 reales y $2r_2$ complejos, entonces $r_1 + 2r_2 = n$.

Definición 3.3.4. Dada una extensión L de K, diremos que un morfismo real $\sigma : K \to \mathbb{C}$ ramifica en L si existe una extensión de σ a L que resulte compleja.

El siguiente teorema nos dice que lo demostrado por Ostrowski para $\mathbb{Q}$ siguen valiendo para cualquier cuerpo de números.

Teorema 3.3.5. Si K es un cuerpo de números y $|.|$ un valor absoluto de K, entonces $|.|$ es equivalente solamente a una de las siguiente posibilidades:

(1) $|.|_\sigma$ para algún morfismo $\sigma : K \to \mathbb{C}$

(2) $|.|_\mathfrak{p}$ para algún primo $\mathfrak{p}$ de K.

Demostración: Ver [Sha66, Páginas 278–280]. □

Asumiendo que el Teorema 3.3.5 es válido, entonces si v es un lugar infinito, $K_v = K_\sigma$, con $\sigma : K \to \mathbb{C}$ morfismo. Diremos que v es un lugar infinito **real** si σ es real y un lugar infinito **complejo** si σ es complejo.

Centrémonos ahora en los lugares no arquimedianos. Dado un lugar v no arquimediano, y $\mathcal{O}_K$ el anillo de enteros, denotamos momentáneamente como $\mathcal{O}_{K,v}$ a la completación de $\mathcal{O}_K$ en K_v. Definimos también a los conjuntos

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

Si $K = \mathbb{Q}$ entonces para un lugar finito dado por un primo p tenemos

$$\widehat{\mathcal{O}_v} = \mathbb{Z}_p, \quad \widehat{\mathcal{U}_v} = \mathbb{Z}_p^\times, \quad \widehat{\mathfrak{p}_v} = p\mathbb{Z}_p,$$

donde $\mathbb{Z}_p$ es el conjunto de los enteros p-ádicos.

Lema 3.3.6. Si v es finito, entonces $\widehat{\mathcal{O}_v} = \overline{\mathcal{O}}_v$ y $\widehat{\mathfrak{p}_v} = \overline{\mathfrak{p}}_v$ (clausura en K_v).

Demostración: Veamos sólo que $\widehat{\mathcal{O}_v} = \overline{\mathcal{O}}_v$. Esto se debe por un lado a que $\widehat{\mathcal{O}_v}$ es cerrado y contiene a $\mathcal{O}_v$, lo que nos dice que $\overline{\mathcal{O}}_v \subseteq \widehat{\mathcal{O}_v}$. Por otro lado, si $x \in \widehat{\mathcal{O}_v}$, entonces $x \in K_v$ y $|x|_v \leq 1$. Como K es denso en K_v, entonces existe una sucesión (x_n) en K tal que $x_n \to x$. Pero entonces si n es suficientemente grande, tenemos que

$$|x_n|_v = |x_n - x + x|_v \leq \text{máx}\{|x_n - x|_v, |x|_v\} \leq \text{máx}\{|x_n - x|_v, 1\} \leq 1.$$

Esto nos dice que para n suficientemente grande, la sucesión está en $\mathcal{O}_v$ y luego, esto nos asegura que $x \in \overline{\mathcal{O}}_v$. □

Lema 3.3.7. Si v es finito, entonces $\mathcal{O}_{K,v} = \widehat{\mathcal{O}_v}$.

Demostración: Como $\mathcal{O}_K \subseteq \mathcal{O}_v$ por el Lema 3.3.6, entonces $\mathcal{O}_{K,v} \subseteq \overline{\mathcal{O}}_v = \widehat{\mathcal{O}_v}$. Recíprocamente, si $x = \overline{\{x_n\}} \in \widehat{\mathcal{O}_v}$, entonces $|x|_v \leq 1$. Además, cambiando los primeros términos de la sucesión podemos suponer $|x_n| \leq 1 \quad \forall n \in \mathbb{N}$, i.e, $x_n \in \mathcal{O}_v$. Luego, para cada $n \in \mathbb{N}$ existe $y_n \in \mathcal{O}_K$ tal que $\overline{\{y_n\}} = \overline{\{x_n\}}$. □

Además, como es claro que $\widehat{\mathcal{O}_v} \cap K = \mathcal{O}_v$ y $\widehat{\mathfrak{p}_v} \cap K = \mathfrak{p}_v$, entonces al igual que antes tenemos un isomorfismo de los cuerpos residuales:

$$\mathcal{O}_v \,/\, \mathfrak{p}_v \cong \widehat{\mathcal{O}_v}/\widehat{\mathfrak{p}_v},$$

lo que implica a su vez que $|\widehat{\mathcal{O}_v}/\widehat{\mathfrak{p}_v}| = N(\mathfrak{p}) < \infty$.

Definición 3.3.8. Decimos que un elemento $\pi_v \in \mathfrak{p}_v$ es un **uniformizador local** o simplemente **uniformizador** si $\mathfrak{p}_v = \pi_v \mathcal{O}_v$.

Lema 3.3.9. Si v es un lugar finito, entonces $\mathfrak{p}_v$ tiene un uniformizador.

Demostración: Como $ord_v(\mathcal{O}_v) \neq \{0\}$ entonces podemos reescalar el orden (tomando un múltiplo) de forma tal que el menor valor es el 1. Luego, existe $\pi \in \mathcal{O}_v$ tal que $ord_v(\pi) = 1$. Veamos que $\pi\,\mathcal{O}_v = \mathfrak{p}_v$. Por un lado, es claro que $\pi\,\mathcal{O}_v \subseteq \mathfrak{p}_v$. Por otro lado, si $x \in \mathfrak{p}_v$ entonces

$$ord_v\left(\frac{x}{\pi}\right) \geq 0,$$

lo que implica que

$$x = \pi\frac{x}{\pi} \in \pi\,\mathcal{O}_v\,.$$

Luego, π es un uniformizador. □

Ejemplo 3.3.10. Por lo dicho antes, en el caso $K = \mathbb{Q}$ podemos tomar $\pi_p = p$.

Proposición 3.3.11. Si v es una valuación y $\pi \in \mathfrak{p}_v$ es un uniformizador entonces dado $x \in K$ no nulo existen $u \in \mathcal{U}_v$ y $r \in \mathbb{Z}$ tales que $x = \pi^r u$. Más aún, $r = ord_v(x)$.

Demostración: Supongamos primero que $x \in \mathcal{O}_v$. Por definición de uniformizador sabemos que $\mathfrak{p}_v = \pi\,\mathcal{O}_v$. Veamos que la afirmación es cierta por inducción en $ord_v(x)$.

Si $ord_v(x) = 0$, entonces $x \in \mathcal{U}_v$ y luego tomando $r = 0$ se cumple. Supongamos que vale para todo $y \in K$ que cumple que $ord_v(y) = n$. Sea ahora $x \in K$ con $ord_v(x) = n+1$. Veamos que se cumple para x.

Como $ord_v(x) > 0$, entonces $x \in \mathfrak{p}_v = \pi\,\mathcal{O}_v$. Luego,

$$ord_v\left(\frac{x}{\pi}\right) = ord_v(x) - 1 = n$$

Por hipótesis inductiva, existe $u \in \mathcal{U}_v$ tal que $x/\pi = \pi^n u$. Finalmente, $x = \pi^{n+1}u$.

Si $x \notin \mathcal{O}_v$ entonces $x^{-1} \in \mathcal{O}_v$. Vimos entonces que existen $s \in \mathbb{N} \cup \{0\}$ y $w \in \mathcal{U}_v$ tales que $x^{-1} = \pi^s w$. Luego, tomando $r := -s \in \mathbb{Z}$ y $u = w^{-1} \in \mathcal{U}_v$ resulta $x = \pi^r u$. □

Con la notación de la Proposición 3.3.11 decimos que r es el **orden** de α. Al uniformizador lo denotaremos como π si se sobreentiende sobre qué lugar nos estamos refiriendo. Notemos que el orden de un elemento α sí está bien definido, porque si $\pi'_v \in \mathfrak{p}_v$ es otro uniformizador, entonces $\pi_v/\pi'_v \in \mathcal{U}_v$.

Al igual que en $\mathbb{Q}$, podemos definir entonces un valor absoluto que sea de la forma

$$|x| = |\,\mathcal{O}_v\,/\,\mathfrak{p}_v\,|^{-r},$$

donde $r = ord_v(x)$. Cabe destacar que por lo dicho antes, $|\,\mathcal{O}_v\,/\,\mathfrak{p}_v\,| = N(\mathfrak{p}_v)$ es un número finito y más aún, potencia de un primo. Este valor absoluto definido va a estar en la clase de equivalencia del lugar v así que de ahora en adelante, este será el representante que tomaremos cuando hablemos de un lugar finito v.

Lema 3.3.12. Si v es un lugar finito entonces K_v es totalmente disconexo.

Demostración: Para ver que K_v es totalmente disconexo veamos que todas las bolas abiertas en K_v son cerradas y todas las bolas cerradas son abiertas. Esto ocurre porque la función distancia $d(x,y) = |x-y|_v$ toma valores discretos (salvo el 0), con lo cual $<$ pueden ser reemplazados por $\leq$ y $>$ por $\geq$. Para ver eso, sea $q = |\,\mathcal{O}_v\,/\,\mathfrak{p}_v\,|$ y $B(x,\delta)$ una bola en K_v. Si $\delta < 1$, entonces existe un único $k \in \mathbb{N}$ tal que $\delta \in (q^{-(k+1)}, q^{-k}]$ y luego

$$B(x,\delta) = \overline{B}(x,r) \quad \forall r \in [q^{-(k+1)}, q^k)$$

y análogamente si $\delta \geq 1$, entonces $\delta \in (q^k, q^{k+1}]$ y

$$B(x,\delta) = \overline{B}(x,r) \quad \forall r \in [q^k, q^k).$$

Recíprocamente, es claro que toda bola cerrada es abierta. □

Proposición 3.3.13. Si v es un lugar finito entonces se cumplen las siguiente propiedades:

(1) $\widehat{\mathcal{O}_v}$ es un dominio íntegro cuyo cuerpo de fracciones es K_v.

(2) $\widehat{\mathcal{O}_v}$ es un subanillo cerrado de K_v.

(3) $\widehat{\mathcal{O}_v}$ resulta completo con la métrica inducida de K_v.

(4) $\widehat{\mathcal{O}_v}$ es compacto.

(5) K_v resulta un espacio de Hausdorff localmente compacto.

(6) $\widehat{\mathcal{O}_v}$ es un anillo local con ideal maximal $\widehat{\mathfrak{p}_v}$.

Demostración:

(1) Es claro que $\widehat{\mathcal{O}_v}$ es dominio íntegro, pues si $x, y \in \widehat{\mathcal{O}_v}$ son tales que $xy = 0$, entonces $0 = |0|_v = |xy|_v = |x|_v|y|_v$. Luego, sin pérdida de generalidad, $|x|_v = 0$ y por lo tanto $x = 0$. Resulta así que $\widehat{\mathcal{O}_v}$ es un dominio íntegro. La demostración de que $\mathrm{Frac}(\widehat{\mathcal{O}_v}) = K_v$ es análoga a lo hecho en el Lema 3.2.9.

(2) $\widehat{\mathcal{O}_v} = \overline{B}(0,1)$ es cerrado por definición.

(3) Todo conjunto cerrado de un espacio completo es completo.

(4) Por inciso (2) $\widehat{\mathcal{O}_v}$ es cerrado y, por definición, es acotado en un espacio métrico. Luego, $\widehat{\mathcal{O}_v}$ es compacto.

(5) Por inciso (4) $\pi_v\widehat{\mathcal{O}_v} = \widehat{\mathfrak{p}_v}$ es compacto y por lo tanto para cada $x \in K_v$ se tiene una base de entornos compactos dada por $\{x+\pi^n\widehat{\mathcal{O}_v}\}_{n\in\mathbb{N}} = \{x+\widehat{\mathfrak{p}_v}^n\}_{n\in\mathbb{N}}$. Luego, K_v es localmente compacto y claramente es Hausdorff.

(6) Análogo a lo dicho en el Lema 3.2.9. □

Observación 3.3.14. El inciso (2) y el Lema 3.3.12 nos dicen que $\widehat{\mathcal{O}_v}$ es abierto en K_v.

Ya sabemos que $\widehat{\mathcal{O}_v}$ es un anillo y un espacio topológico. Nuestro siguiente objetivo será estudiar al conjunto $\widehat{\mathcal{U}_v} = \widehat{\mathcal{O}_v}^{\times}$ como grupo topológico. Los siguiente lemas técnicos serán utilizados para probar el Teorema 3.3.20.

Lema 3.3.15. Sea $x \in 1+\widehat{\mathfrak{p}_v}$, $q = |\widehat{\mathcal{O}_v}/\widehat{\mathfrak{p}_v}|$ y sea $s \in \mathbb{N}$ tal que $(q,s) = 1$. Entonces para cada $n \in \mathbb{N}$ existe $w_n \in \widehat{\mathcal{U}_v}$ tal que:

(1) $w_n^s \equiv x \pmod{\pi^n}$.

(2) $w_n \equiv w_{n-1} \pmod{\pi^{n-1}}$ si $n \geq 2$.

Demostración: Veamos que es cierto por inducción en n. Para $n = 1$ definimos $w_1 := 1$. Supongamos que es cierto para n. Notemos que si

$$\begin{aligned} A_n &:= (1+\widehat{\mathfrak{p}_v}^n)/(1+\widehat{\mathfrak{p}_v}^{n+1}),\\ B_n &:= (1+\widehat{\mathfrak{p}_v})/(1+\widehat{\mathfrak{p}_v}^{n+1}),\\ C_n &:= (1+\widehat{\mathfrak{p}_v})/(1+\widehat{\mathfrak{p}_v}^{n}). \end{aligned}$$

entonces la sucesión

$$1 \to A_n \xrightarrow{i_n} B_n \xrightarrow{\varphi_n} C_n \to 1$$

resulta exacta corta, donde i_n es la inclusión y φ_n es el morfismo natural que manda la clase en la clase.

En efecto, i_{n+1} es inyectica, φ_n es suryectiva y claramente $\mathrm{Im}(i_n) \subseteq \ker(\varphi_{n+1})$. Además, como

$$q^{n-1} = |C_n| = \frac{|B_n|}{|\ker(\varphi_n)|} = \frac{q^n}{|\ker(\varphi_n)|}$$

se tiene que $|\ker(\varphi_n)| = q$ y luego

$$\mathrm{Im}(i_n) = \ker(\varphi_n).$$

Ahora, como $x \in 1 + \widehat{\mathfrak{p}_v}$, por hipótesis inductiva existe $w_n \in \widehat{\mathcal{U}_v}$ tal que $w_n^s \equiv x \pmod{\pi^n}$. Entonces

$$\frac{x}{w_n^s} \equiv 1 \pmod{\pi^n} \text{ y por lo tanto } \frac{x}{w_n^s} \in 1 + \widehat{\mathfrak{p}_v}^n.$$

Como $|A_n| = q$ y $(q, s) = 1$, entonces la función $y \mapsto y^s$ es inyectiva y por lo tanto (como A_n es finito) suryectiva. Luego, existe $\alpha \in A_n$ tal que

$$\frac{x}{w_n^s} \equiv \alpha^s \pmod{\pi^{n+1}}.$$

Por lo tanto,

$$x \equiv w_n^s \alpha^s \equiv (w_n \alpha)^s \pmod{\pi^{n+1}}.$$

Finalmente, $w_{n+1} := w_n \alpha$ cumple las hipótesis. □

Observación 3.3.16. En consecuencia, la sucesión (w_n) del teorema es de Cauchy y definiendo $w := \lim_{n\to\infty} w_n$ se tiene que $w^s = x$.

Lema 3.3.17. Si p es un número primo y e es el grado de ramificación de p en K, entonces para cada $n \in \mathbb{N}$ se cumple que la sucesión

$$1 \to (1 + \widehat{\mathfrak{p}_v}^n)/(1 + \widehat{\mathfrak{p}_v}^{n+1}) \xrightarrow{i_n} (1 + \widehat{\mathfrak{p}_v}^{n-1})/(1 + \widehat{\mathfrak{p}_v}^{n+1}) \xrightarrow{\varphi_n} (1 + \widehat{\mathfrak{p}_v}^{n-1+e})/(1 + \widehat{\mathfrak{p}_v}^{n+e}) \to 1$$

es exacta corta, donde i_n la inclusión y $\varphi_n(x) = x^p$.

Demostración: Primero notemos que como e es el grado de ramificación, entonces $p = \pi^e u$, con $u \in \mathcal{U}_v$. Veamos que ϕ_n está bien definida:

Por la fórmula del Binomio de Newton, tenemos que

$$(1 + a\pi^{n-1})^p = \sum_{i=0}^{p} \binom{p}{i} (a\pi^{n-1})^i,$$

Pero como

$$\binom{p}{i} (a\pi^{n-1})^i \equiv \binom{\pi^e}{i} (a\pi^{n-1})^i \equiv 0 \pmod{\pi^{n+e}} \quad \forall i > 1$$

podemos concluir que

$$(1 + a\pi^{n-1})^p \equiv 1 + pa\pi^{n-1} \equiv 1 \pmod{\pi^{n-1+e}}.$$

Al igual que en el Lema 3.3.15, basta ver que φ_n es suryectiva. Sea $y \in 1 + \widehat{\mathfrak{p}_v}^{n-1+e}$, entonces $y = 1 + a\pi^{n-1+e}$ con $a \in \widehat{\mathcal{O}_v}$ y luego $w := 1 + a\pi^{n-1} \in 1 + \widehat{\mathfrak{p}_v}^{n-1}$. Basta ver entonces que $w^p \equiv y \pmod{\pi^{n+e}}$. Análogamente a la cuenta anterior,

$$w^p \equiv (1 + a\pi^{n-1})^p \equiv 1 + pa\pi^{n-1} \equiv y \pmod{\pi^{n+e}}.$$

Queda así probada la afirmación. □

Lema 3.3.18. Si p es un número primo y e es el grado de ramificación de p en K, entonces dado $r \in \mathbb{N}$, la sucesión

$$1 \to (1+\widehat{\mathfrak{p}_v}^{n-1})/(1+\widehat{\mathfrak{p}_v}^{n}) \xrightarrow{i_n} (1+\widehat{\mathfrak{p}_v}^{r})/(1+\widehat{\mathfrak{p}_v}^{n}) \xrightarrow{\varphi_n} (1+\widehat{\mathfrak{p}_v}^{r+e})/(1+\widehat{\mathfrak{p}_v}^{n+e-1}) \to 1$$

es exacta corta $\forall n > r$, donde i_n es la inclusión y $\varphi_n(x) = x^p$.

Notemos que el Lema 3.3.17 es un caso particular del Lema 3.3.18 tomando $n = r+2 > r$ y luego haciendo un cambio de variable.

Demostración: Lo probaremos por inducción en n.
Denotemos

$$\begin{aligned} A_n &:= (1+\widehat{\mathfrak{p}_v}^{n-1})/(1+\widehat{\mathfrak{p}_v}^{n}), \\ B_n &:= (1+\widehat{\mathfrak{p}_v}^{r})/(1+\widehat{\mathfrak{p}_v}^{n}), \\ C_n &:= (1+\widehat{\mathfrak{p}_v}^{r+e})/(1+\widehat{\mathfrak{p}_v}^{n+e-1}). \end{aligned}$$

Para $n = r+1$ resulta directo porque C_n es el grupo trivial y $A_n = B_n$. Supongamos que es cierto para n y veamos que vale para $n+1$.

Dado $x \in 1+\widehat{\mathfrak{p}_v}^{r+e}$, por hipótesis inductiva existe $w \in 1+\widehat{\mathfrak{p}_v}^{r}$ tal que $w^p \equiv x \pmod{\pi^{n+e-1}}$. Es decir que

$$\frac{x}{w^p} \equiv 1 \pmod{\pi^{n+e-1}} \quad \text{y por lo tanto} \quad \frac{x}{w^p} \in 1+\widehat{\mathfrak{p}_v}^{n+e-1}.$$

Usando ahora el Lema 3.3.17 tenemos que existe $t \in 1+\widehat{\mathfrak{p}_v}^{n-1}$ tal que

$$\frac{x}{w^p} \equiv t^p \pmod{\pi^{n+e}} \quad \text{y por lo tanto} \quad x \equiv (wt)^p \pmod{\pi^{n+e}}.$$

En particular, $x \equiv (wt)^p \pmod{\pi^{n+e-1}}$. Luego, tomando $\alpha := wt$ obtenemos que φ_{n+1} es suryectivo.

Aplicando el mismo razonamiento sobre las dimensiones de los espacios hecho en el Lema 3.3.17 se tiene que la sucesión es exacta.

□

Observación 3.3.19. Como consecuencia de lema anterior, dado $x \in 1+\widehat{\mathfrak{p}_v}^{e+1}$ existe una sucesión (w_n) en $1+\widehat{\mathfrak{p}_v}$ tal que $w_n^p \equiv x \pmod{\pi^n}$ y $w_{n+1} \equiv w_n \pmod{\pi^n}$ $\forall n \in \mathbb{N}$. Resulta entonces que (w_n) es de Cauchy y tomando $w := \lim_{n\to\infty} w_n$ tenemos que $w^p = x$.

Teorema 3.3.20. Dado H un subgrupo de $\widehat{\mathcal{U}_v}$, entonces H es abierto si y sólo si $[\widehat{\mathcal{U}_v} : H] < \infty$.

Demostración: Supongamos primero que H es un subgrupo abierto de $\mathcal{U}_v$, esto es que si $|\widehat{\mathcal{O}_v}/\widehat{\mathfrak{p}_v}| = q = p^k$ entonces existe $n \in \mathbb{N}$ tal que $B(1, q^{-n}) \subset H$, es decir que $1+\widehat{\mathfrak{p}_v}^{n} < H$. Basta ver entonces que

$$[\widehat{\mathcal{U}_v} : 1+\widehat{\mathfrak{p}_v}^{n}] < \infty.$$

Sea $\varphi : \widehat{\mathcal{U}_v} \to \left(\widehat{\mathcal{O}_v}/\widehat{\mathfrak{p}_v}^{n}\right)^{\times}$ el epimorfismo dado por $\varphi(x) = x$.

Entonces, como $\ker(\varphi) = 1+\widehat{\mathfrak{p}_v}^{n}$, resulta que

$$\widehat{\mathcal{U}_v}/\left(1+\widehat{\mathfrak{p}_v}^{n}\right) \cong \left(\widehat{\mathcal{O}_v}/\widehat{\mathfrak{p}_v}^{n}\right)^{\times}$$

y luego

$$\left[\widehat{\mathcal{U}_v} : 1 + \widehat{\mathfrak{p}_v}^n\right] = \left|\widehat{\mathcal{U}_v}/1 + \widehat{\mathfrak{p}_v}^n\right| = \left|\left(\widehat{\mathcal{O}_v}/\widehat{\mathfrak{p}_v}^n\right)^\times\right| < \infty.$$

Recíprocamente, supongamos que $[\widehat{\mathcal{U}_v} : H] = n = p^r s$ donde $p \nmid s$. Entonces por el teorema de Lagrange tenemos que dado $x \in \widehat{\mathcal{U}_v}$, $x^n \in H$. Por lo tanto,

$$\left(1 + \widehat{\mathfrak{p}_v}\right)^n < H.$$

Luego, basta ver que se cumplen las siguientes dos propiedades:

(1) $\left(1 + \widehat{\mathfrak{p}_v}\right)^s = 1 + \widehat{\mathfrak{p}_v}$.

(2) $\left(1 + \widehat{\mathfrak{p}_v}\right)^{p^r} = 1 + \widehat{\mathfrak{p}_v}^{r(e+1)}$.

En efecto, si asumimos (1) y (2), entonces

$$1 + \widehat{\mathfrak{p}_v}^{r(e+1)} = \left(1 + \widehat{\mathfrak{p}_v}\right)^{p^r} = \left(\left(1 + \widehat{\mathfrak{p}_v}\right)^s\right)^{p^r} = \left(1 + \widehat{\mathfrak{p}_v}\right)^n < H$$

y por lo tanto H es abierto.

Resta ver entonces (1) y (2):

(1) resulta directo de la Observación 3.3.16, porque dado $x \in 1 + \widehat{\mathfrak{p}_v}$ vimos que existe $w \in 1 + \widehat{\mathfrak{p}_v}$ tal que $w^s = x$. Por lo tanto

$$\left(1 + \widehat{\mathfrak{p}_v}\right)^s \supseteq 1 + \widehat{\mathfrak{p}_v}.$$

Pero la otra contención es clara, pues $1 + \widehat{\mathfrak{p}_v}$ es un subgrupo.

(2) también resulta directo porque, por la Observación 3.3.19 $(1 + \widehat{\mathfrak{p}_v})^p \supseteq 1 + \widehat{\mathfrak{p}_v}^{e+1}$ y esto implica

$$(1 + \widehat{\mathfrak{p}_v})^{p^r} \supseteq 1 + \widehat{\mathfrak{p}_v}^r.$$

Luego, es claro que vale la igualdad. □

3.4. Extensiones locales

Si L/K es una extensión finita y $w \in M_L$ entonces la restricción de $|.|_w$ a K nos define $v \in M_K$. La siguiente proposición nos dice que así se obtienen todos los lugares de K.

Proposición 3.4.1. Si L/K es una extensión finita entonces el mapa $M_L \to M_K$, $w \mapsto v$ de manera tal que $|.|_v$ es equivalente a $|.|_{w|_K}$, es suryectivo. Si $w \mapsto v$ decimos que $w|v$. En este caso el morfismo $i : K \to L$ se extiende de manera única a $K_v \to L_w$ y el siguiente diagrama es conmutativo:

$$\begin{array}{ccc} L & \xrightarrow{\sigma_w} & L_w \\ {\scriptstyle i}\uparrow & & \uparrow \\ K & \xrightarrow[\sigma_v]{} & K_v \end{array}$$

Demostración: Sea $v \in M_K$. Por el Teorema 3.3.5, si v es finito entonces proviene de un primo $\mathfrak{p}$ de K. Sea $\mathfrak{P}$ primo de L tal que $\mathfrak{P} \mid \mathfrak{p}$, entonces $\mathfrak{P}$ define $w \in M_L$. Luego, si $|x|_v = c^{-ord_{\mathfrak{p}}(x)}$, entonces

$$|x|_w = c_1^{-ord_{\mathfrak{P}}(x)} = c_1^{-ord_{\mathfrak{p}}(x)e(\mathfrak{P}\mid\mathfrak{p})} = \tilde{c}^{-ord_{\mathfrak{p}}(x)},$$

donde $\tilde{c} := c_1^{e(\mathfrak{P}\mid\mathfrak{p})}$. Por lo tanto $|.|_v$ es equivalente a $|.|_{w|_K}$ y $w|v$.

Si v es infinito entonces proviene de un morfismo $\sigma : K \to \mathbb{C}$. Como $\mathbb{C}$ es algebraicamente cerrado, σ se puede extender a L, definiendo así un lugar $w \in M_L$. Por definición, es claro que $w|v$ y, por lo tanto, el mapa es suryectivo. La existencia y unicidad de la extensión del morfismo $i : K \to L$ es análoga a la de la Proposición 3.3.2. En efecto, si $a = \overline{\{a_n\}} \in K_v$ entonces como $\{a_n\}$ es de Cauchy en K, $\{i(a_n)\}$ es de Cauchy en L. Luego, $\{\sigma_w(i(a_n))\}$ es de Cauchy en L_w y por lo tanto converge. Luego, definimos $\varphi : K_v \to L_w$ como

$$\varphi(a) = \lim_{n\to\infty} \{(\sigma_w \circ i)(a_n)\},$$

que extiende a i. □

Definición 3.4.2. Si $n = [L : K]$, entonces llamamos a $n_w = [L_w : K_v]$ el **grado local**.

Proposición 3.4.3. Sea L/K finita y separable de grado n y v un lugar finito. Entonces

$$n = \sum_{w|v} n_w.$$

Demostración: Como L/K es finita y separable entonces existe $\alpha \in L$ tal que $L = K(\alpha)$. Sea

$$m_\alpha(x) = f_1(x) \cdots f_r(x)$$

la descomposición del polinomio minimal de α en K_v en polinomios irreducibles. Como la extensión es separable, entonces cada polinomio aparece con multiplicidad 1.

Los morfismos de L en $\overline{K}_v$ se corresponden con las funciones que mandan α en las raíces de f_i. Dos morfismos van a ser conjugados si y sólo si mandan α a una raíz del mismo polinomio f_i. Además, es claro que el grado local en cada caso está dado por el grado de f_i y por lo tanto

$$n = [L : K] = \mathrm{gr}(m_\alpha) = \sum_{i=1}^{r} \mathrm{gr}(f_i) = \sum_{w|v} n_w.$$

Queda así probada la afirmación. □

Proposición 3.4.4. Sea L/K finita y separable y v un lugar finito de K. Entonces

$$N_{L/K}(x) = \prod_{w|v} N_{L_w/K_v}(x),$$
$$Tr_{L/K}(x) = \sum_{w|v} Tr_{L_w/K_v}(x).$$

Demostración: Al igual que en la demostración de la Proposición 3.4.3, existe $\alpha \in L$ tal que $L = K(\alpha)$. Sea

$$m_\alpha(x) = f_1(x) \cdots f_r(x)$$

la descomposición en K_v en polinomios irreducibles del polinomio minimal de α. Luego, $N_{L/K}(x)$ es igual a $(-1)^{\mathrm{gr}(m_\alpha)}$ veces el término independiente de m_α y de manera similar para cada f_i. Como el término independiente de m_α es el producto de los términos independientes de cada f_i, queda probada la primera afirmación. Análogamente, para el caso de la traza hay que ver el penúltimo término (ordenados de menor a mayor grado) de m_α y de cada f_i. □

Observación 3.4.5. Notemos que la proposición anterior sigue siendo cierta si tomamos v infinito, ya que en este caso, si $w|v$ entonces $L_w/K_v = \mathbb{C}/\mathbb{R}$, $\mathbb{C}/\mathbb{C}$ ó $\mathbb{R}/\mathbb{R}$. Más aún, en el primer caso $N_{L/K}$ es la norma compleja y en el segundo y el tercero es la identidad.

3.5. Valuaciones en las completaciones

Ahora, si w es una lugar finito de L sobre un lugar finito v de K entonces tenemos el siguiente diagrama conmutativo:

$$\begin{array}{ccc} \mathcal{O}_w \,/\, \mathfrak{p}_w & \xrightarrow{\cong} & \widehat{\mathcal{O}_w}/\widehat{\mathfrak{p}_w} \\ {\scriptstyle i}\uparrow & & \uparrow{\scriptstyle i} \\ \mathcal{O}_v \,/\, \mathfrak{p}_v & \xrightarrow[\cong]{} & \widehat{\mathcal{O}_v}/\widehat{\mathfrak{p}_v} \end{array}$$

Esto nos dice que el grado de ramificación $e(L|K)$ no cambia con la completación. En efecto, si v es finito definido por $\mathfrak{p}$ y $\mathfrak{p}\,\mathcal{O}_L = \mathfrak{P}_1^{e_1} \ldots \mathfrak{P}_g^{e_g}$, entonces como $\widehat{\mathcal{O}_w}/\widehat{\mathfrak{P}_w} \cong \mathcal{O}_w \,/\, \mathfrak{P}_w$ y $\widehat{\mathcal{O}_v}/\widehat{\mathfrak{p}_v} \cong \mathcal{O}_v \,/\, \mathfrak{p}_v$ se tiene que

$$f(\widehat{\mathfrak{P}_w}|\widehat{\mathfrak{p}_v}) = f(\mathfrak{P}_w \,|\, \mathfrak{p}_v) = [\mathcal{O}_L \,/\, \mathfrak{P}_i : \mathcal{O}_K \,/\, \mathfrak{p}],$$

donde la 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.

Algo similar ocurre con el índice de ramificación. Si v es un lugar finito de K, definimos el **grupo de valuación** al conjunto

$$|K|_v := \{|x|_v : x \in K^\times\},$$

que claramente resulta un grupo.

Lema 3.5.1. Dado v lugar finito de K, se tiene que $|K_v|_v = |K|_v$

Demostración: Es claro que $|K|_v \subseteq |K_v|_v$, así que veamos la otra contención. Sea $x \in K_v$. Como K es denso en K_v, existe $y \in K$ tal que $|x - y|_v < |x|_v$. Luego, como v es valuación se tiene que

$$|y|_v = |y - x + x|_v = \mín\{|y - x|_v, |x|_v\} = |x|_v,$$

por ser $|y - x|_v \neq |x|_v$, lo que prueba lo que queríamos. □

Notemos que como L/K es finita entonces L_w/K_v es finita y además separable, por estar en característica 0. Tenemos también que el siguiente diagrama es conmutativo:

$$\begin{array}{ccc} |L|_w & \xrightarrow{=} & |L_w|_w \\ {\scriptstyle i}\uparrow & & \uparrow{\scriptstyle i} \\ |K|_v & \xrightarrow[=]{} & |K_v|_v \end{array}$$

Por lo tanto, el índice de ramificación tampoco cambia en la completación. Luego, por el Teorema 1.1.23 tenemos que

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

Denotando $f(w|v) := f(\mathfrak{P}_w \,|\, \mathfrak{p}_v)$ y $e(w|v) := e(\mathfrak{P}_w \,|\, \mathfrak{p}_v)$ entonces tenemos que

$$[L_w : K_v] = e(w|v)f(w|v).$$

Si L/K es una extensión finita y separable y v es un lugar infinito de K, entonces todo lugar w de L sobre v será 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 $[L_w : K_v] = e(w|v)f(w|v)$.

3.6. Acción del grupo de Galois

Veamos primero que si E es un cuerpo de números, $\sigma : E \to \sigma(E)$ es un isomorfismo y v es un lugar de E entonces podemos definir un lugar de $\sigma(E)$, que denotaremos σv, de la siguiente forma:

$$|y|_{\sigma v} := |\sigma^{-1}(y)|_v$$

Luego, como E es denso en E_v, entonces por continuidad podemos extender σ. Luego, σ nos induce un nuevo isomorfismo en la completación, únicamente determinado por continuidad, que también denotaremos como σ. Es decir, tenemos un isomorfismo $\sigma : E_v \to \sigma(E)_{\sigma v}$.

Supongamos ahora que L/K es finita y Galois con grupo de Galois $G = \mathrm{Gal}(L/K)$. Si $\sigma \in G$ entonces $\sigma : L \to L$ es un isomorfismo por definición. Notemos que si $w \in M_L$ es finito, entonces sabemos que está dado por un primo $\mathfrak{P}$ de L. Entonces si $y = \sigma(x),\ x \in L$, supongamos sin pérdida de generalidad que

$$(x) = \mathfrak{P}_1^{e_1} \cdots \mathfrak{P}_g^{e_g},\ \text{con}\ \mathfrak{P} = \mathfrak{P}_1,\ e_1 \geq 0.$$

Entonces $|y|_{\sigma w} = c^{-e_1}$. Por otro lado, tenemos que

$$(y) = \sigma(\mathfrak{P}_1)^{e_1} \cdots \sigma(\mathfrak{P}_g)^{e_g},$$

lo que nos dice que $|y|_{\sigma(\mathfrak{P}_1)} = c^{-e_1} = |y|_{\sigma w}$. Esto en particular nos dice que si w es finito, entonces σw también. Si w es infinito, entonces σw también lo es.

Por lo dicho antes, para cada lugar w de L, tenemos definida $\sigma_w : L_w \to L_{\sigma w}$ como $\{x_i\} \mapsto \{\sigma(x_i)\}$. Además, si v es un lugar de K debajo de w, entonces σ_w es un K_v-isomorfismo, pues $\sigma_{|K} = Id_K$.

Definimos el **grupo de descomposición** de w como

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

Por la cuenta hecha más arriba, resulta directo que en el caso en que w sea finito y esté dado por $\mathfrak{P}$, entonces este no es otra cosa que $D(\mathfrak{P})$. Esto nos dice que la nueva definición extiende a la anterior para los primos infinitos. De igual manera, sigue valiendo lo mismo que antes:

Lema 3.6.1. Dado $\sigma \in G$ y w primo, $D(\sigma w) = \sigma D(w)\sigma^{-1}$.

Demostración: Sea $\tilde{\sigma} \in G$, entonces

$$|y|_{\tilde{\sigma}(\sigma w)} = |\tilde{\sigma}^{-1}(y)|_{\sigma w} = |(\sigma^{-1} \circ \tilde{\sigma}^{-1})(y)|_w = |(\tilde{\sigma} \circ \sigma)^{-1}(y)|_w = |y|_{(\tilde{\sigma}\circ\sigma)(w)}.$$

Esto nos dice que $\tilde{\sigma}(\sigma w) = (\tilde{\sigma} \circ \sigma)(w)$. Supongamos ahora que $\tilde{\sigma} \in D(\sigma w)$ esto es, $\sigma w = \tilde{\sigma}(\sigma w) = (\tilde{\sigma} \circ \sigma)(w)$. Luego, $(\sigma^{-1} \circ \tilde{\sigma} \circ \sigma)(w) = w$, es decir, $(\sigma^{-1} \circ \tilde{\sigma} \circ \sigma) \in D(w)$ y por lo tanto

$$\tilde{\sigma} = \sigma \circ (\sigma^{-1} \circ \tilde{\sigma} \circ \sigma) \circ \sigma^{-1} \in \sigma D(w)\sigma^{-1}.$$

Luego, $D(\sigma w) \subseteq \sigma D(w)\sigma^{-1}$ y la recíproca es similar. □

Con lo cual el grupo de descomposición de w está determinado a menos de conjugación por el lugar v. Luego, se tiene una inyección

$$i : D(w) \to \mathrm{Gal}(L_w/K_v)$$

definida como $i(\sigma) = \sigma_w$. Notemos que para que esta inyección tenga sentido debemos ver primero que L_w/K_v es Galois.

Proposición 3.6.2. L_w/K_v es finita y Galois, y la inyección i es un isomorfismo.

Demostración: Notemos que como L/K es finita y separable entonces existe $\alpha \in L$ tal que $L = K(\alpha)$. Luego, como $K_v \subseteq L_w$ y $\alpha \in L \subseteq L_w$ entonces $K_v(\alpha) \subseteq L_w$. Además, como L es denso en L_w tenemos que L es denso en $K_v(\alpha)$.

Por otro lado, como $K_v(\alpha)/K_v$ es finita y K_v es completo entonces $K_v(\alpha)$ es completo. Luego, por Proposición 3.3.2 resulta $L_w = K_v(\alpha)$. Esto nos asegura que L_w/K_v es Galois. Veamos ahora que i es un isomorfismo. Sea $\sigma_w \in \mathrm{Gal}(L_w/K_v)$ tal que $\sigma_w = Id_{L_w}$ y $x \in L$. Luego,

$$\{x\} = \sigma_w(\{x\}) = \{\sigma(x)\}.$$

Por lo tanto, $\sigma(x) = x$ y como x era arbitrario esto implica que $\sigma = Id_L$ y por lo tanto i es inyectiva. Notemos que si v es infinito entonces la proposición es trivial, ya que $K_v = \mathbb{R}$ o $K_v = \mathbb{C}$ y por lo tanto L_w/K_v es de grado 1 ó 2. Si v es finito entonces w también y por la Proposición 1.1.29 tenemos $|D(w)| = e(\mathfrak{P} \mid \mathfrak{p})f(\mathfrak{P} \mid \mathfrak{p})$, $\mathfrak{P}$ y $\mathfrak{p}$ son respectivamente los primos que definen a w y v. Luego, por lo visto antes tenemos que $|D(w)| = |\mathrm{Gal}(L_w/K_v)|$ y por lo tanto i es suryectiva y claramente un isomorfismo. □

Como consecuencia de la Proposición 3.6.2 tenemos que

$$D(w) \cong \mathrm{Gal}(L_w/K_v).$$

Vimos que si $\mathfrak{p}$ era un primo de K entonces G actuaba transitivamente sobre los primos de L que estaban sobre $\mathfrak{p}$. No debería sorprendernos entonces que esto siga siendo cierto para un lugar v de K. La siguiente proposición nos asegura eso, generalizando lo que ya habíamos visto

Proposición 3.6.3. Sea L/K Galois y v un lugar infinito de K. Entonces G actúa transitivamente sobre los lugares w de L que están sobre v.

Demostración: Sea $\sigma : K \to \mathbb{C}$ una inmersión correspondiente a v. Si w_1 y w_2 son dos lugares infinitos de L que están sobre v correspondientes a extensiones τ_1, τ_2 de σ respectivamente, entonces existe $\varphi \in \mathrm{Gal}(L/K)$ tal que $\tau_2 = \tau_1\varphi^{-1}$. Luego,

$$|x|_{w_2} = |\tau_2(x)| = |\tau_2\varphi^{-1}(x)| = |\varphi^{-1}(x)|_{w_1} = |x|_{\varphi w_1}.$$

Por lo tanto, $w_2 = \varphi w_1$. □

Corolario 3.6.4. Sea L/K Galois, v un lugar de K y w_1, w_2 dos lugares de L que extienden a v. Entonces L_{w_1} y L_{w_2} son isomorfas.

Demostración: Sea $\sigma \in \mathrm{Gal}(L/K)$ que manda w_1 en w_2. Definimos $\varphi : L_{w_1} \to L_{w_2}$ como $\varphi(\{x_n\}) = \{\sigma(x_n)\}$. Entonces φ manda sucesiones de Cauchy en sucesiones de Cauchy y es claramente isomorfismo. □

Como las extensiones L_w/K_v son isomorfas entre sí (sobre K_v), denotaremos como L^v a cualquiera de ellas y como $G^v = \mathrm{Gal}(L^v/K_v)$. Por lo dicho antes, sabemos entonces que G^v es isomorfo a algún grupo de descomposición $D(w)$. Si suponemos ahora que L/K es abeliana, por la Proposición 6.1.1 tenemos que este grupo es único, es decir que no depende del lugar w elegido sobre v. (Notemos que la Proposición 6.1.1 nos asegura lo dicho para el caso en que v sea finito, pero el caso de v infinito es trivial).

Capítulo 4

Adèles e idèles

4.1. Adèles

Fueron definidos en primera instancia por el francés Claude Chevalley (1909-1984) con el fin de describir la teoría global de clases para extensiones infinitas, pero años después usó los idèles (que veremos en la próxima sección) para dar una conexión entre la teoría de clases global y la local.

Por una cuestión de simplicidad haremos abuso de notación escribiendo $\mathcal{O}_v$ en vez de $\widehat{\mathcal{O}_v}$, $\mathcal{U}_v$ en lugar de $\widehat{\mathcal{U}_v}$ y denotaremos S_∞ al subconjunto de M_K que consiste en todos los lugares infinitos. Para estudiar K tiene sentido pensar simultáneamente en todas las posibles completaciones que tiene y pegar de alguna forma toda esta información local para obtener datos globales. Es lógico entonces pensar en primera instancia en el producto de todos los K_v. Uno de los problemas que trae esto es que dicho producto no es en general localmente compacto. Es entonces cuando comenzamos a trabajar con los adèles.

Consideremos primero un subconjunto finito S de M_K tal que $S_\infty \subseteq S$. Podemos definir entonces al conjunto de **S-adèles** como

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

Lema 4.1.1. Si $S_\infty \subseteq S \subseteq M_K$ entonces $\mathbb{A}_K^S$ dotado de la topología producto resulta un anillo topológico (con la suma y el producto punto a punto) localmente compacto.

Demostración: Como $\mathcal{O}_v$ es compacto, el Teorema de Tíjonov nos asegura que $\prod_{v \notin S} \mathcal{O}_v$ es compacto y como K_v es localmente compacto y S es finito, entonces $\prod_{v \in S} K_v$ es localmente compacto y por lo tanto $\mathbb{A}_K^S$ lo es. Por último, que $\mathbb{A}_K^S$ es un grupo topológico resulta claro si dotamos al conjunto con el producto lugar a lugar. □

Definición 4.1.2. Definimos ahora el **anillo de adèles** como la unión de todos los S-adèles. Es decir,

$$\mathbb{A}_K := \bigcup_{\substack{S_\infty \subseteq S, \\ S \subseteq M_K}} \mathbb{A}_K^S.$$

Notemos que resulta así $\mathbb{A}_K = \{(x_v) : x_v \in \mathcal{O}_v \text{ para todo } v \text{ salvo una cantidad finita}\}$. Esto es claramente un subconjunto del producto de los K_v y se llama el **producto directo restringido** de los K_v respecto de los $\mathcal{O}_v$. Las operaciones que le dan a $\mathbb{A}_K$ la estructura de anillo son el producto y la suma lugar a lugar y la topología dada es la que tiene como base

de entornos a los entornos básicos de $\mathbb{A}_K^S$ para cada S finito que contiende a S_∞.

Resulta así que $\mathbb{A}_K$ es un anillo topológico. Para ser más explícitos, notemos que como es anillo topológico basta describir los entornos del 0. Los entornos de 0 en la topología de los adèles son los conjuntos

$$\prod_{p\notin S} \mathcal{O}_v \times \prod_{v\in S} U_v(\varepsilon),$$

donde $U_v(\varepsilon) = \{x \in K_v : |x|_v < \varepsilon\}$ y $S \supseteq S_\infty$ es finito.

Notemos que si $x \in K$ entonces $x \in K_v$ para todo $v \in M_K$ y $x \in \mathcal{O}_v$ para casi todo lugar v. Este hecho nos permite definir una inyección natural $K \hookrightarrow \mathbb{A}_K$ dada por $x \mapsto (x, x, \ldots)$. Como consecuencia, podemos ver a K como un subgrupo de $\mathbb{A}_K$. Llamaremos a los elementos de esta imagen **adèles principales**.

Lema 4.1.3. Sean $v_1, ..., v_r \in M_K$. Entonces para cada $1 \le k \le r$ existe $a_k \in K$ tal que

$$|a_k|_{v_k} > 1 \quad \text{y} \quad |a_k|_{v_l} < 1 \quad \text{si} \quad l \neq k.$$

Demostración: Basta ver el caso $k = 1$. Lo haremos por inducción en r.

Si $r = 2$, como v_1 y v_2 no son equivalentes entonces existen $\alpha, \beta \in K$ tales que $|\alpha|_{v_1} < 1$, $|\alpha|_{v_2} \ge 1$, $|\beta|_{v_1} \ge 1$ y $|\beta|_{v_2} < 1$. Sea entonces $a_1 := \beta\alpha^{-1}$.

Si $r \ge 3$, por hipótesis inductiva existe $z \in K$ tal que $|z|_{v_1} > 1$, $|z|_{v_i} < 1$ si $1 \le i \le r_1$. Además, por el caso $r = 2$ existe $w \in K$ tal que $|w|_{v_1} > 1$ y $|w|_{v_r} < 1$. Tomando ahora

$$a_1 := \begin{cases} z & \text{si} \quad |z|_{v_r} < 1, \\ z^m w & \text{si} \quad |z|_{v_r} = 1, \\ \frac{z^m}{1+z^m} w & \text{si} \quad |z|_{v_r} > 1. \end{cases}$$

donde $m \in \mathbb{N}$ es suficientemente grande queda probado el lema. □

Teorema 4.1.4. (Teorema de aproximación débil). Sean $v_1, ..., v_r \in M_K$, $x_1, ..., x_r \in K$ y $\varepsilon > 0$. Entonces existe $x \in K$ tal que $|x - x_i|_{v_i} < \varepsilon$ para todo $i = 1, ..., r$.

Demostración: Aplicando el Lema 4.1.3, tenemos que para cada $1 \le k \le r$ existe a_k tal que $|a_k|_{v_k} > 1$ y $|a_k|_{v_l} < 1$ si $l \neq k$. Luego,

$$\frac{a_k^m}{1+a_k^m} \xrightarrow{|.|_{v_k}} 1 \quad \text{y} \quad \frac{a_k^m}{1+a_k^m} \xrightarrow{|.|_{v_l}} 0 \quad \text{si } l \neq k.$$

Por lo tanto,

$$\frac{x_k a_k^m}{1+a_k^m} \xrightarrow{|.|_{v_k}} x_k \quad \text{y} \quad \frac{x_k a_k^m}{1+a_k^m} \xrightarrow{|.|_{v_l}} 0 \quad \text{si } l \neq k.$$

Así,

$$\sum_{k=1}^{r} \frac{x_k a_k^m}{1+a_k^m} \xrightarrow{|.|_{v_j}} x_j \quad \text{para todo} \quad 1 \le j \le r.$$

Luego, dado $\varepsilon > 0$ podemos tomar

$$x = \sum_{k=1}^{r} \frac{x_k a_k^m}{1+a_k^m}$$

para un m suficientemente grande. □

Observación 4.1.5. El teorema de aproximación sigue valiendo si tomamos $x_i \in K_{v_i}$ en lugar de K. Para dicho caso, podríamos tomar $x_i' \in K$ cerca de x_i y luego tomar x cerca de los x_i'. El teorema nos dice entonces que K es denso en $\prod_{i=1}^r K_{v_i}$.

Teorema 4.1.6. (Fórmula del producto) Si K es un cuerpo de números y $x \in K^\times$ entonces

$$\prod_{v \in M_K} |x|_v = 1.$$

Demostración: Sean $\sigma_1, ..., \sigma_n$ las inmersiones de K en $\mathbb{C}$. Dado $x \in K^\times$, sabemos por Teorema 1.1.17 que existen primos $\mathfrak{p}_1, ..., \mathfrak{p}_m$ y enteros $a_1, ..., a_m$ tales que $(x) = \prod_{i=1}^m \mathfrak{p}_i^{a_i}$. Por Proposición 1.1.30,

$$|N_{K/\mathbb{Q}}(x)| = N((x)) = \prod_{i=1}^m N(\mathfrak{p}_i)^{a_i}$$

y por definición, si v es un lugar finito definido por un primo $\mathfrak{q}$ entonces

$$|x|_v = \begin{cases} N(\mathfrak{p}_i)^{-a_i} & \text{si} \quad \mathfrak{q} = \mathfrak{p}_i, \\ 1 & \mathfrak{q} \neq \mathfrak{p}_i\,. \end{cases}$$

Entonces,

$$\prod_{v \in M_K} |x|_v = \prod_{i=1}^n N(\mathfrak{p}_i)^{-a_i} \prod_{i=1}^m |\sigma_i(x)| = \prod_{i=1}^n N(\mathfrak{p}_i)^{-a_i} |N_{K/\mathbb{Q}}(x)| = \prod_{i=1}^n N(\mathfrak{p}_i)^{-a_i} \prod_{i=1}^n N(\mathfrak{p}_i)^{a_i} = 1.$$

Queda así probada la afirmación. □

Teorema 4.1.7. $\mathbb{A}_K/K$ es compacto.

Demostración: [Cas67, página 64]. □

4.2. Idèles

El término "idèle" es una variación del término "ideal", cuya relación veremos más adelante. Fue también introducido por Chevalley y hace referencia a "ideal element"(abreviado id.el.) mientras que "adèle" hace referencia a "additive idele".

El conjunto de los **idèles** es por definición $\mathbb{I}_K := \mathbb{A}_K^\times$. Esto nos dice que

$$\begin{aligned} \mathbb{I}_K := \mathbb{A}_K^\times =& \{x = (x_v) \in \mathbb{A}_K : \exists y = (y_v) \in \mathbb{A}_K : xy = 1\} \\ =& \{x = (x_v) \in \mathbb{A}_K : \exists y = (y_v) \in \mathbb{A}_K : x_v y_v = 1 \quad \forall v \in M_K\} \\ =& \{x = (x_v) \in \mathbb{A}_K : x_v \in K_v^\times \ \forall v \text{ y } x_v \in \mathcal{O}_v^\times \text{ para casi todo } v\}. \end{aligned}$$

Por lo tanto $\mathbb{I}_K$ resulta el producto directo restringido de los $K_v^\times$ respecto de los $\mathcal{O}_v^\times$. La razón por la cual lo denotamos $\mathbb{I}_K$ y no simplemente $\mathbb{A}_K^\times$ es la topología. Vamos a considerar en $\mathbb{I}_K$ la topología producto, que no coincide con la heredada por la de los adèles.

Lema 4.2.1. La topología producto en $\mathbb{I}_K$ es estrictamente más fina que la inducida por $\mathbb{A}_K$.

Demostración: Sea U abierto básico de $\mathbb{A}_K^\times$ (como subespacio de $\mathbb{A}_K$). Entonces U es de la forma $\mathbb{A}_K^\times \cap V$, donde V es un abierto básico de $\mathbb{A}_K$. Luego,

$$V = \prod_{v \notin S_1} \mathcal{O}_v \times \prod_{v \in S_1} V_v$$

donde V_v es abierto de K_v y S_1 un subconjunto finito de M_K que contiene a S_∞. Miremos entonces quién es $V \cap \left(\mathbb{A}_K^S\right)^\times$ con S finito arbitrario:

$$\begin{aligned}\left(\mathbb{A}_K^S\right)^\times \cap V &= \left(\prod_{v \notin S} \mathcal{O}_v^\times \times \prod_{v \in S} K_v^\times\right) \bigcap \left(\prod_{v \notin S_1} \mathcal{O}_v \times \prod_{v \in S_1} V_v\right) \\ &= \prod_{v \notin S \cup S_1} \mathcal{O}_v^\times \times \prod_{v \in S \setminus S_1} (K_v^\times \cap \mathcal{O}_v) \times \prod_{v \in S_1 \setminus S} V_v' \times \prod_{v \in S \cap S_1} W_v'\end{aligned}$$

donde V_v' es abierto de $\mathcal{U}_v$ y $W_v^\times$ es abierto de $K_v^\times$. Además, $K_v^\times \cap \mathcal{O}_v = \mathcal{O}_v \setminus \{0\}$.

Sea entonces $S_2 = S \cup S_1$ y

$$B = \prod_{p \notin S_2} \mathcal{U}_v \times \prod_{S_2 \setminus S_\infty} [(\mathcal{O}_v \setminus \{0\}) \cap V_v' \cap W_v'] \times W_\infty'.$$

Entonces B es abierto de $\mathbb{I}_K$, porque $[(\mathcal{O}_v \setminus \{0\}) \cap V_v' \cap W_v']$ es abierto de $K_v^\times$, pues V_v' lo es, W_v' lo es (porque $\mathcal{U}_v$ es abierto de $K_v^\times$) y $\mathcal{O}_v \setminus \{0\}$ lo es.

Como claramente $B \subseteq \left(\mathbb{A}_K^S\right)^\times \cap V$, entonces $B \subseteq U$ y por lo tanto la topología de $\mathbb{I}_K$ es más fina que la de $\mathbb{A}_K^\times$.

Es estrictamente más fina porque si fuesen iguales, dado U' abierto básico de $\mathbb{I}_K$, tenemos que

$$U' = \prod_{v \notin S_3} \mathcal{O}_v^\times \times \prod_{v \in S_3} V_v$$

con S_3 finito y V_v abierto de $K_v^\times$, existe U abierto de $\mathbb{A}_K^\times$ tal que $U \subseteq U'$ donde U es como antes. Sea S finito tal que $S_1 \cup S_3 \subsetneq S$, entonces existe $v_0 \in S$ tal que $v_0 \notin S_1 \cup S_3$. Como $\left(\mathbb{A}_K^S\right)^\times \cap V \subseteq U'$ entonces $\mathcal{O}_{v_0} \setminus \{0\} = \mathcal{O}_{v_0} \cap K_{v_0}^\times = \mathcal{O}_{v_0}^\times$, lo cual lleva a un absurdo. □

La ventaja de trabajar con una topología más fina es que ahora $\mathbb{I}_K$ resulta un grupo topológico localmente compacto, ya que $\mathcal{O}_v^\times$ es compacto y por lo tanto podemos utlizar, análogamente a lo hecho con los adèles, el Teorema de Tijonov. Esto no va a ser cierto en general si consideramos la topología inducida por $\mathbb{A}_K$ ya que $K_v^\times$ no es compacto.

Notemos que dado $x \in K^\times$, entonces por definición $x \in K_v^\times$ para todo $v \in M_K$ y además $x \in \mathcal{U}_v$ para casi todo v. Luego, al igual que en el caso de los adèles, tenemos una inyección natural $K^\times \hookrightarrow \mathbb{I}_K$ dada por $x \mapsto (x, x, \ldots)$. Sin embargo, no es cierto que $\mathbb{I}_K / K^\times$ sea compacto. Aún así, este cociente tendrá un rol muy importante. Lo llamaremos **grupo de clases de idèles** y lo denotaremos como C_K.

Definición 4.2.2. Definimos la función **contenido** o **volumen** $|.| : \mathbb{I}_K \to \mathbb{R}_{>0}$ como

$$|\alpha| = \prod_v |\alpha|_v.$$

Por lo dicho antes, el producto de la derecha es finito y la función está bien definida. Si $\alpha \in \mathbb{I}_K$ decimos que tiene volumen o contenido $|\alpha|$. Al conjunto de los idèles de contenido 1 lo denotaremos como $\mathbb{I}_K^1$. Como la función contenido es un morfismo de grupos entonces tenemos que $\mathbb{I}_K^1 = \ker(|.|)$ es un subgrupo de $\mathbb{I}_K$ y además como la función es claramente suryectiva, tenemos que la siguiente sucesión es exacta corta

$$0 \to \mathbb{I}_K^1 \xrightarrow{i} \mathbb{I}_K \xrightarrow{|.|} \mathbb{R}_{>0} \to 0.$$

Para ver que dicha sucesión se parte, consideremos la función $f : \mathbb{R}_{>0} \to \mathbb{I}_K$ dada por

$$(f(x))_v = \begin{cases} 1 & v \notin S_\infty \\ x^{\frac{1}{n}} & x \in S_\infty \end{cases},$$

donde $[K : \mathbb{Q}] = n$.

Entonces es claro que $|f(x)| = |x^{\frac{1}{n}}|^n = x$ y por lo tanto la sucesión se parte, obteniendo así que

$$\mathbb{I}_K \cong \mathbb{I}_K^1 \times \mathbb{R}_{>0}.$$

Por otro lado, por la fórmula del producto sabemos que $K^\times \subseteq \mathbb{I}_K^1$. Entonces si denotamos $C_K^1 := \mathbb{I}_K^1 / K^\times$, se sigue que

$$C_K \cong C_K^1 \times \mathbb{R}_{>0}.$$

Como anticipamos antes, esto en particular nos dice que C_K no es compacto. Pero se tiene la siguiente proposición

Proposición 4.2.3. C_K^1 es compacto.

Demostración: Ver [Cas67, Página 70]. □

Ejemplo 4.2.4. Si $K = \mathbb{Q}$ y $\widehat{\mathbb{Z}} := \prod_p \mathbb{Z}_p$, entonces veamos que:

$$\mathbb{I}_{\mathbb{Q}}^1 \cong \mathbb{Q}^\times \times \widehat{\mathbb{Z}}^\times \quad \text{y} \quad C_{\mathbb{Q}}^1 \cong \widehat{\mathbb{Z}}^\times.$$

Dado $x = ((u_p p^{e_p})_p, r) \in \mathbb{I}_{\mathbb{Q}}$, donde $u_p \in \mathbb{Z}_p^\times$, $r \in \mathbb{R}^\times$ y $e_p \in \mathbb{Z}$ es nulo para casi todo p, existe un único racional

$$\alpha = \pm \prod_{p \text{ primo}} p^{-e_p} \in \mathbb{Q}^\times$$

tal que $\alpha x = (u_p') \times r'$, donde $u_p' \in \mathbb{Z}_p^\times$ y $r' \in \mathbb{R}_{>0}$.

Luego, existe un isomorfismo canónico entre $\mathbb{I}_{\mathbb{Q}}$ y $\mathbb{Q}^\times \times \widehat{\mathbb{Z}}^\times \times \mathbb{R}_{>0}$, de lo que se sigue lo que queríamos.

4.2.1. Norma de idèles

En esta sección, L/K va a ser una extensión finita y Galois con grupo de Galois G. Ya definimos en el Capítulo 1 una norma para los elementos de $L^\times$ y otra para los de I_L. Abusando aún más de la notación, vamos a definir ahora una norma

$$N_{L/K} : \mathbb{I}_L \to \mathbb{I}_K.$$

Más aún, si pensamos a $L^\times$ como subconjunto de $\mathbb{I}_L$, queremos que $N_{L/K}$ actúe como la norma ya definida allí. Es decir, queremos que extienda a la norma ya conocida. Esto es, que si $x \in L^\times$, queremos que

$$(N_{L/K}(x))_v = N_{L/K}(x) = \prod_{\sigma \in G} \sigma(x).$$

Definición 4.2.5. Definimos la **norma** $N_{L/K} : \mathbb{I}_L \to \mathbb{I}_K$ como

$$(N_{L/K}(x))_v = \prod_{w|v} N_{L_w/K_v}(x_w).$$

Con esta definición, la norma cumple lo que queríamos, por la Proposición 3.4.4 y por la Observación 3.4.5. Por lo tanto, el siguiente diagrama conmuta:

$$\begin{array}{ccc} L^\times & \xrightarrow{i} & \mathbb{I}_L \\ {\scriptstyle N_{L/K}}\downarrow & & \downarrow{\scriptstyle N_{L/K}} \\ K^\times & \xrightarrow[i]{} & \mathbb{I}_K \end{array}$$

Luego, $N_{L/K}$ induce un morfismo $N_{L/K} : C_L \to C_K$ que resulta continuo pero no necesariamente inyectivo o suryectivo.

Capítulo 5

Caracteres

El principal objetivo de este capítulo es estudiar los caracteres de Hecke. Para ello introducimos primero la noción de caracter, presentamos los caracteres de Dirichlet y finalmente los caracteres de Hecke, tanto en el contexto clásico como en el idèlico. Para este capítulo se puede ver [Shu].

Definición 5.0.1. Dado un grupo abeliano G, un **caracter** de G es un morfismo $\chi : G \to \mathbb{C}^\times$.

Durante las próximas secciones nos centraremos en caracteres de grupos abelianos finitos.

Proposición 5.0.2. Sea G un grupo abeliano finito. Entonces el conjunto de caracteres de G, denotado $\widehat{G}$, tiene una estructura natural de grupo (con el producto de funciones punto a punto), y como grupo $\widehat{G} \cong G$ de forma no canónica.

Demostración: Por el Teorema de estructuras, existen enteros $d_1, ..., d_n \in \mathbb{Z}$ tales que $d_1|d_2|\cdots|d_n$ y $G \cong \mathbb{Z}/d_1 \times \mathbb{Z}/d_2 \times \cdots \times \mathbb{Z}/d_n$. Como claramente $\widehat{G_1 \times G_2} = \widehat{G_1} \times \widehat{G_2}$, basta suponer G cíclico (de orden n digamos). En ese caso, $\langle g \rangle = G$, entonces $\chi(g)$ es una raíz n-ésima de la unidad (no necesariamente primitiva). Sea ζ_n una raíz n-ésima primitiva, luego todo caracter es una potencia del caracter $\widetilde{\chi}(g) = \zeta_n$. □

5.1. Caracteres de Dirichlet

Definición 5.1.1. Un **caracter de Dirichlet** de módulo n es un caracter del grupo $(\mathbb{Z}/n\mathbb{Z})^\times$.

Observación 5.1.2. Para todo $a \in (\mathbb{Z}/n\mathbb{Z})^\times$ se cumple que $\chi(a)$ es una raíz $\varphi(n)$-ésima de la unidad, donde φ es la función de Euler. En efecto, por el pequeño teorema de Fermat tenemos que

$$\chi(a)^{\varphi(n)} = \chi(a^{\varphi(n)}) = \chi(1) = 1.$$

Ejemplo 5.1.3. Para $n = 15$, un posible caracter de Dirchlet es $\chi : (\mathbb{Z}/15\mathbb{Z})^\times \to \mathbb{C}^\times$ dado por $\chi(2) = i$ y $\chi(7) = -i$. Resulta entonces χ unívocamente determinado y se tiene que

m	1	2	4	7	8	11	13	14
$\chi(m)$	1	i	-1	$-i$	$-i$	-1	i	1

Podemos extender el caracter a todo $\mathbb{Z}$ definiendo $\chi(a) = 0$ para los a tales que $(a, n) > 1$.

Ejemplo 5.1.4. Sean χ_3 y χ_9 los caracteres de Dirichlet de módulo 3 y 9 respectivamente definidos por $\chi_3(2) = \chi_9(2) = -1$ y luego extendidos a todo $\mathbb{Z}$ (basta saber su valor en 2 ya que éste genera tanto $(\mathbb{Z}/3\mathbb{Z})^\times$ como $(\mathbb{Z}/9\mathbb{Z})^\times$). Dado $a \in \mathbb{Z}$, por un lado se cumple que

$\chi_9(a) = \chi_3(a) = 0$ si $(a, 9) > 1$, pues un número es coprimo con 9 si y sólo si lo es con 3. Por otro lado, si $(a, 9) = 1 = (a, 3)$, entonces $\chi_9(\overline{a}) = \chi_3(\overline{a})$, donde $\overline{a}$ denota la clase de a módulo 9 en el miembro izquierdo y módulo 3 en el miembro derecho.

Esto nos dice que con conocer a χ_3 ya podemos determinar χ_9 y por lo tanto χ_3 induce a χ_9. Esto no es tan sorprendente ya que χ_9 es "igual" a χ_3:

m	1	2	3	4	5	6	7	8	0
$\chi_3(m)$	1	-1	0	1	-1	0	1	-1	0
$\chi_9(m)$	1	-1	0	1	-1	0	1	-1	0

Es decir, que χ_9 está dado por

$$\chi_9 : (\mathbb{Z}/9\mathbb{Z})^\times \to (\mathbb{Z}/3\mathbb{Z})^\times \xrightarrow{\chi_3} \mathbb{C}^\times.$$

Ejemplo 5.1.5. Sea χ_3 como en el ejemplo anterior y χ_6 el caracter de módulo 6 no trivial, i.e, tal que $\chi_6(5) = -1$. A diferencia del ejemplo anterior, ahora extendiendo los caracteres a $\mathbb{Z}$ no van a resultar iguales, ya que χ_6 se va a anular en cualquier número par, mientras que χ_3 sólo se anulará en los múltiplos de 3. Sin embargo, vale que

$$\chi_6(a) = \begin{cases} \chi_3(a) & \text{si} \quad (a, 6) = 1, \\ 0 & \text{si} \quad (a, 6) = 0. \end{cases}$$

Con lo cual, nuevamente conocer a χ_3 alcanza para determinar a χ_6. Estos dos últimos ejemplos motivan a la siguiente definición.

Definición 5.1.6. Un caracter de Dirichlet se dice **primitivo** si no es inducido por otro caracter de módulo más chico.

Proposición 5.1.7. Considerando la definición de caracter de Dirchilet extendida a $\mathbb{Z}$, si χ es un caracter de Dirichlet de módulo n y $n = \prod_{i=1}^{r} p_i^{\alpha_i}$ es su descomposición en primos, entonces

$$\chi = \prod_{i=1}^{r} \chi_i,$$

donde χ_i es un caracter de Dirichlet de módulo $p_i^{\alpha_i}$.

Demostración: Sea $a \in \mathbb{Z}$ y sean $a_i \in \mathbb{Z}$ tales que $a \equiv a_i \pmod{p_i^{\alpha_i}}$. Por el Teorema chino del resto, para cada $i \in \{1, ..., r\}$ existe $c_i \in \mathbb{Z}$ tal que

$$c_i \equiv a_i \pmod{p_i^{\alpha_i}} \quad \text{y} \quad c_i \equiv 1 \pmod{p_j^{\alpha_j}} \quad \forall j \neq i.$$

Entonces, vale que $a \equiv c_i \pmod{p_i^{\alpha_i}}$ y multiplicando a ambos lados por c_j, para todo j distinto de i, tenemos que $a \equiv c_1 \cdots c_r \pmod{p_i^{\alpha_i}}$ y por lo tanto

$$a \equiv c_1 \cdots c_r \pmod{n}.$$

Luego, si definimos $\chi_i : (\mathbb{Z}/p_i^{\alpha_i}\mathbb{Z})^\times \to \mathbb{C}^\times$ de la forma $\chi_i(a) := \chi(c_i)$ entonces se tiene que

$$(\chi_1 \cdots \chi_r)(a) = \chi_1(a) \cdots \chi_r(a) = \chi(c_1) \cdots \chi(c_r) = \chi(c_1 \cdots c_r) = \chi(a).$$

Resulta así probada la afirmación. □

Ejemplo 5.1.8. Retomando el Ejemplo 5.1.3, se tiene que $\chi = \chi_3\chi_5$, donde χ_j es de módulo j y $\chi_3(2) = -1,\ \chi_5(2) = -i$.

5.2. Caracteres de Hecke clásicos

En la presente sección daremos una presentación de lo que son los caracteres de Hecke, que van a generalizar a los de Dirichlet.

En la definición dada de caracter de Dirichlet trabajábamos con el anillo de enteros algebraicos del cuerpo de números $\mathbb{Q}$, que es $\mathcal{O}_{\mathbb{Q}} = \mathbb{Z}$. Elegíamos un número natural n y llamábamos caracter de Dirichlet (de módulo n) a un morfismo

$$\varepsilon : (\mathbb{Z}/n\mathbb{Z})^{\times} \to \mathbb{C}^{\times}.$$

Notemos que elegir un número natural n en $\mathbb{Z}$ y ver el cociente $\mathbb{Z}/n\mathbb{Z}$ es equivalente a tomar un ideal no nulo I de $\mathbb{Z}$ y mirar el cociente $\mathbb{Z}/I$, puesto que $\mathbb{Z}$ es un DIP.
En general, para un cuerpo de números K, un caracter de Dirichlet será un morfismo

$$\varepsilon : (\mathcal{O}_K/\mathfrak{f})^{\times} \to \mathbb{C}^{\times}$$

donde $\mathfrak{f}$ es un ideal entero no nulo de $\mathcal{O}_K$, que de ahora en adelante denotaremos como $\mathcal{O}$.

A su vez, $(\mathbb{Z}/n\mathbb{Z})^{\times}$ se compone de los números coprimos con n. Esta noción es generalizada con la que nos dice cuándo dos ideales son coprimos en el anillo de enteros algebraicos. Así como dado $n \in \mathbb{N}$ y $\alpha = r/s \in \mathbb{Q}^{\times}$ con $(r, s) = 1$ podemos decir que α es coprimo con n si $(n, r) = (n, s) = 1$, vimos que podemos también generalizar la idea de cuándo un ideal fraccionario es coprimo con $\mathfrak{f}$ y más aún, cuándo dos ideales fraccionarios son coprimos. Tiene sentido entonces definir a

$$K(\mathfrak{f}) := \{\alpha \in K^{\times} : ((\alpha), \mathfrak{f}) = 1\},$$

que resulta un subgrupo de $K^{\times}$. Definimos también a

$$K(\mathfrak{f})_{\mathfrak{f}} := \{\delta \in K^{\times} : v_{\mathfrak{p}}((\delta)) \geq v_{\mathfrak{p}}(\mathfrak{f}) \text{ para todo } \mathfrak{p} \text{ que aparece en } \mathfrak{f}\} \cup \{0\}.$$

Lema 5.2.1. $K(\mathfrak{f})_{\mathfrak{f}}$ cumple las siguientes propiedades:

(1) Contiene al 0.

(2) Es cerrado bajo la multiplicación por elemento de $K(\mathfrak{f})$.

(3) Es cerrado bajo la suma.

Demostración: (1) y (2) son triviales y para ver (3) basta tomar $\delta, \delta' \in K(\mathfrak{f})_{\mathfrak{f}}$ y $\mathfrak{p}$ un primo de $\mathcal{O}_K$ que aparezca en $\mathfrak{f}$. Entonces $v_{\mathfrak{p}}((\delta)) \geq v_{\mathfrak{p}}(\mathfrak{f})$ y $v_{\mathfrak{p}}((\delta')) \geq v_{\mathfrak{p}}(\mathfrak{f})$ y por lo tanto $v_{\mathfrak{p}}((\delta + \delta')) \geq v_{\mathfrak{p}}(\mathfrak{f})$. □

El lema anterior nos dice que la siguiente definición nos da una relación de equivalencia.

Definición 5.2.2. Dados $\alpha, \beta \in K(\mathfrak{f})$ diremos que α es **congruente** a β módulo $\mathfrak{f}$ si

$$\beta - \alpha \in K(\mathfrak{f})_{\mathfrak{f}}$$

y lo denotaremos como

$$\alpha \equiv \beta \mod {}^{\times}\mathfrak{f}$$

Lógicamente, se sigue cumpliendo (gracias a que $K(\mathfrak{f})\mathfrak{f}$ es cerrado por multiplicación de $K(\mathfrak{f})$) que si $\alpha, \beta, \gamma, \delta \in K(\mathfrak{f})$ son tales que

$$\alpha \equiv \beta \mod {}^{\times}\mathfrak{f} \text{ y } \gamma \equiv \delta \mod {}^{\times}\mathfrak{f}$$

entonces

$$\alpha\gamma \equiv \beta\delta \mod {}^{\times}\mathfrak{f},$$

y como caso particular,

$$\alpha \equiv \beta \mod {}^{\times}\mathfrak{f} \text{ implica } \alpha\gamma \equiv \beta\gamma \mod {}^{\times}\mathfrak{f}.$$

Gracias a estas propiedades podemos definir ahora el subgrupo $K_{\mathfrak{f}}$ de $K(\mathfrak{f})$ por el cual vamos a cocientar:

$$K_{\mathfrak{f}} := 1 + K(\mathfrak{f})\mathfrak{f} = \{\alpha \in K^{\times} : \alpha \equiv 1 \mod {}^{\times}\mathfrak{f}\} \subset K(\mathfrak{f}).$$

Ejemplo 5.2.3. En el caso en que $K = \mathbb{Q}$ tenemos que

$$\frac{a}{b} \equiv \frac{c}{d} \mod {}^{\times}n \text{ si y sólo si } \frac{a}{b} - \frac{c}{d} = n\frac{a'}{b'}$$

con $(b', n) = 1$ y

$$\begin{aligned}
\mathbb{Q}(n) &= \{\alpha \in \mathbb{Q}^{\times} : (\alpha, n) = 1\} \\
\mathbb{Q}(n)n &= \left\{n\frac{a}{b} : (b, n) = 1\right\} \\
\mathbb{Q}_n &= \{\alpha \in \mathbb{Q}^{\times} : \alpha \equiv 1 \mod {}^{\times}n\}.
\end{aligned}$$

Notemos que $K_{\mathfrak{f}}$ es un subgrupo, pues es cerrado por inversos y si $\alpha, \beta \equiv 1 \mod {}^{\times}\mathfrak{f}$, multiplicando por β^{-1} resulta que $\alpha\beta^{-1} \equiv 1 \mod {}^{\times}\mathfrak{f}$ y por lo tanto $\alpha\beta^{-1} \in K_{\mathfrak{f}}$. Además, dados $\alpha, \beta \in K(\mathfrak{f})$, la equivalencia

$$\beta - \alpha \in K(\mathfrak{f})\mathfrak{f} \iff \beta \in \alpha + K(\mathfrak{f})\mathfrak{f} = \alpha + \alpha K(\mathfrak{f})\mathfrak{f} \iff \frac{\beta}{\alpha} \in 1 + K(\mathfrak{f})\mathfrak{f} = K_{\mathfrak{f}}$$

nos dice que $\alpha \equiv \beta \mod {}^{\times}\mathfrak{f}$ es equivalente a $\beta/\alpha \in K_{\mathfrak{f}}$.

Proposición 5.2.4. Sea $\mathfrak{f}$ un ideal entero de $\mathcal{O}$. Existe un isomorfismo

$$(\mathcal{O}/\mathfrak{f})^{\times} \xrightarrow{\cong} K(\mathfrak{f})/K_{\mathfrak{f}}, \quad \alpha + \mathfrak{f} \mapsto \alpha K_{\mathfrak{f}}.$$

Demostración: Notemos que si $\alpha + \mathfrak{f} = \beta + \mathfrak{f}$ en $(\mathcal{O}/\mathfrak{f})^{\times}$ entonces $((\alpha), \mathfrak{f}) = ((\beta), \mathfrak{f}) = 1$ y $\beta - \alpha \in \mathfrak{f}$. Entonces $\alpha, \beta \in K(\mathfrak{f})$ y $\alpha \equiv \beta \mod {}^{\times}\mathfrak{f}$. Por lo tanto la función está bien definida. El núcleo de la función es

$$\begin{aligned}
&\{\alpha + \mathfrak{f} \in (\mathcal{O}/\mathfrak{f})^{\times} : \alpha \in K_{\mathfrak{f}}\} \\
=&\{\alpha + \mathfrak{f} \in (\mathcal{O}/\mathfrak{f})^{\times} : \alpha \equiv 1 \mod {}^{\times}\mathfrak{f}\} \\
=&\{\alpha + \mathfrak{f} \in (\mathcal{O}/\mathfrak{f})^{\times} : \alpha \in 1 + K(\mathfrak{f})\mathfrak{f}\}.
\end{aligned}$$

Pero $\alpha \in \mathcal{O}$, con lo cual resulta que el núcleo es

$$\{\alpha + \mathfrak{f} \in (\mathcal{O}/\mathfrak{f})^{\times} : \alpha \in 1 + \mathfrak{f}\} = 1 + \mathfrak{f}$$

y por lo tanto la función es inyectiva.

Para ver que la función es suryectica, tomamos un elemento $\alpha K_{\mathfrak{f}}$ de $K(\mathfrak{f})/K_{\mathfrak{f}}$. Sea

$$(\alpha)_{\text{neg}} = \prod_{\mathfrak{p}} \mathfrak{p}^{e_{\mathfrak{p}}}, \quad e_{\mathfrak{p}} < 0$$

el "denominador" del ideal principal (α). Por el Teorema 4.1.4, existe $\beta \in \mathcal{O}$ tal que

$$\beta \equiv 1 \pmod{\mathfrak{f}}, \qquad \beta \equiv 0 \pmod{\prod_{\mathfrak{p}} \mathfrak{p}^{-e^{\mathfrak{p}}}}.$$

Luego, $\beta \equiv 1 \mod^{\times} \mathfrak{f}$, con lo cual $\alpha\beta K_{\mathfrak{f}} = \alpha K_{\mathfrak{f}}$. Además, $\alpha\beta \in \mathcal{O}$ y es coprimo con $\mathfrak{f}$, por lo tanto el elemento $\alpha\beta + \mathfrak{f} \in (\mathcal{O}\,/\,\mathfrak{f})^{\times}$ va a parar a $\alpha K_{\mathfrak{f}} \in K(\mathfrak{f})/K_{\mathfrak{f}}$. □

Observación 5.2.5. La proposición sigue valiendo para cualquier completación no arquimediana K_v de K. En dicho caso nos queda

$$(\mathcal{O}_v\,/\mathfrak{p}_v^{e_v})^{\times} \cong \mathcal{O}_v^{\times}/(1+\mathfrak{p}_v^{e_v}),$$

que ya fue probado en la demostración del Teorema 3.3.20.

Dado un ideal entero $\mathfrak{f}$, definimos a los siguientes conjuntos:

$$\begin{aligned} I_K(\mathfrak{f}) &= \{\text{ideales fraccionarios de } K \text{ coprimos con } \mathfrak{f}\} \\ P_K(\mathfrak{f}) &= \{\text{ideales fraccionarios principales } (\alpha) \text{ de } K \text{ coprimos con } \mathfrak{f}\} \\ P_K^1(\mathfrak{f}) &= \{\text{ideales fraccionarios principales } (\alpha) \text{ de } \ K : \alpha \equiv 1 \mod^{\times} \mathfrak{f}\} \end{aligned}$$

Entonces tenemos el siguiente diagrama, en donde los segmentos verticales indican contención y los horizontales mapean un elemento α en el ideal (α).

$$\begin{array}{ccc} & & I_K(\mathfrak{f}) \\ & & \vert \\ K(\mathfrak{f}) & \hookrightarrow & P_K(\mathfrak{f}) \\ \vert & & \vert \\ K_{\mathfrak{f}} & \hookrightarrow & P_K^1(\mathfrak{f}) \end{array}$$

Así, $I_K(\mathfrak{f})$ resultará naturalmente el dominio de los caracteres clásicos de Hecke. En primera instancia esto puede ir en contra de la intuición, ya que en el caso de $K = \mathbb{Q}$ sólo vemos los ideales principales. Esto está de alguna manera escondido, ya que en ese caso todos los ideales son principales y por lo tanto $I_{\mathbb{Q}}(\mathfrak{f}) = P_{\mathbb{Q}}(\mathfrak{f})$.

Dado K cuerpo de números de grado n sobre $\mathbb{Q}$ veamos que tenemos una función natural

$$K^{\times} \to (\mathbb{R}^{\times})^{r_1} \times (\mathbb{C}^{\times})^{r_2}.$$

Sean $\sigma_1, ..., \sigma_{r_1}$ las r_1 inmersiones reales y $\tau_1, \overline{\tau}_1 ..., \tau_{r_2}, \overline{\tau}_{r_2}$ los r_2 pares de inmersiones complejas. Entonces la función

$$\alpha \mapsto (\sigma_1(\alpha), ..., \sigma_{r_1}(\alpha), \tau_1(\alpha), ..., \tau_{r_2}(\alpha))$$

es la que queríamos. Esto es equivalente a identificar a $\mathbb{R}\otimes_{\mathbb{Q}} K$ con $\mathbb{R}^{r_1}\times\mathbb{C}^{r_2}$ de la forma usual: sabemos que existe un polinomio $p(x)\in\mathbb{Q}[x]$ irreducible de grado n tal que $K=\mathbb{Q}[x]/(p(x))$. Así resulta

$$\mathbb{R}\otimes_{\mathbb{Q}} K=\mathbb{R}\otimes_{\mathbb{Q}}\mathbb{Q}[x]/(p(x))=\mathbb{R}[x]/(p(x)).$$

Entonces como $p(x)$ es irreducible sobre $\mathbb{Q}[x]$, se factoriza sobre $\mathbb{R}[x]$ como el producto de r_1 polinomios lineales y r_2 cuadráticos, donde $r_1+r_2=n$. Luego,

$$\mathbb{R}\otimes_{\mathbb{Q}} K\cong\mathbb{R}^{r_1}\times\mathbb{C}^{r_2}$$

y

$$K^\times\to(\mathbb{R}^\times)^{r_1}\times(\mathbb{C}^\times)^{r_2},\quad \alpha\mapsto 1\otimes\alpha.$$

Estamos entonces en condiciones de enunciar la primera definición de caracter de Hecke clásico.

Definición 5.2.6. Sea $\mathfrak{f}$ un ideal no nulo de $\mathcal{O}$ y

$$\chi_\infty:(\mathbb{R}^\times)^{r_1}\times(\mathbb{C}^\times)^{r_2}\to\mathbb{C}^\times$$

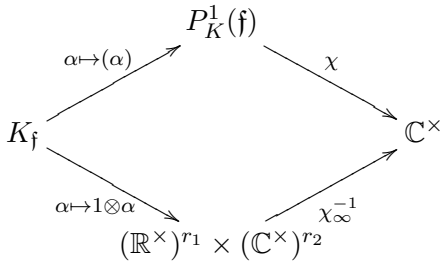
un caracter continuo. Entonces el caracter

$$\chi:I_K(\mathfrak{f})\to\mathbb{C}^\times$$

es un **caracter de Hecke con conductor $\mathfrak{f}$ y tipo-infinito** χ_∞ si

$$\chi((\alpha))=\chi_\infty^{-1}(1\otimes\alpha)\ \ \forall\alpha\in K_{\mathfrak{f}}$$

está bien definido. Esto es, que el siguiente diagrama conmute:



Observación 5.2.7. Que χ este bien definido quiere decir que si $(\alpha)=(\beta)$ con $\alpha,\beta\in K_{\mathfrak{f}}$, entonces

$$\chi((\alpha))=\chi((\beta)).$$

Pero notemos que si $(\alpha)=(\beta)$, entonces $\alpha=\beta u$ con $u\in\mathcal{O}^\times$. Entonces

$$\begin{aligned}\chi((\alpha))&=\chi_\infty^{-1}(1\otimes\alpha)=\chi_\infty^{-1}(1\otimes\beta u)\\&=\chi_\infty^{-1}(1\otimes\beta)\chi_\infty^{-1}(1\otimes u)\\&=\chi((\beta))\chi_\infty^{-1}(1\otimes u).\end{aligned}$$

Por lo tanto $\chi((\alpha))=\chi((\beta))$ si y sólo si $\chi_\infty(1\otimes u)=1\ \ \forall u\in\mathcal{O}^\times$.

En el contexto de caracteres de Hecke, los caracteres no van a ser necesariamente unitarios. Es decir, su imagen no va a estar contenida en el círculo unitario complejo $\mathbb{T}$, como vimos que sí pasaba en el caso de los caracteres de Dirichlet.

Naturalmente, un caracter de Hecke clásico con conductor $\mathfrak{f}$ es **primitivo** si no es inducido por otro caracter de Hecke clásico con conductor $\mathfrak{f}'$ que divida a $\mathfrak{f}$. Todo caracter de Hecke clásico es inducido por un único caracter de Hecke clásico primitivo. Más adelante veremos que la noción de primitividad desaparece en el contexto idélico.

Ahora notemos que si χ es un caracter de Hecke con conductor $\mathfrak{f}$ y tipo-infinito χ_∞ que determina a χ en $P_K^1(\mathfrak{f})$, entonces χ tiene además asociado un caracter de un grupo finito

$$\varepsilon : (\mathcal{O} / \mathfrak{f})^\times \to \mathbb{T}$$

tal que χ_∞ y ε determinan a χ en $P(\mathfrak{f})$. En efecto, por la Proposición 1.1.19 y la Proposición 5.2.4 se tiene que $n = |K(\mathfrak{f})/K_{\mathfrak{f}}|$ es un número finito. Entonces, dado $\alpha \in K^\times$,

$$\begin{aligned} \alpha \in K(\mathfrak{f}) &\Rightarrow \alpha^n \in K_{\mathfrak{f}} \\ &\Rightarrow \chi((\alpha))^n = \chi((\alpha^n)) = \chi_\infty^{-1}(1 \otimes \alpha^n) = \chi_\infty^{-1}(1 \otimes \alpha)^n \\ &\Rightarrow \chi((\alpha)) = \varepsilon(\alpha)\chi_\infty^{-1}(1 \otimes \alpha), \quad \text{donde } \varepsilon(\alpha)^n = 1. \end{aligned}$$

Como $\varepsilon(\alpha) = \chi((\alpha))\chi_\infty(1 \otimes \alpha)$, se sigue que $\varepsilon : K(\mathfrak{f}) \to \mathbb{T}$ es un caracter. Más aún, ε es trivial en $K_{\mathfrak{f}}$ porque χ es un caracter de Hecke clásico, así que podemos ver a ε como un caracter de $K(\mathfrak{f})/K_{\mathfrak{f}}$. Luego, como dijimos al comienzo, ε es un caracter de $(\mathcal{O} / \mathfrak{f})^\times$. Visto esto, podemos reescribir la definición de caracter de Hecke clásico.

Definición 5.2.8. Sea $\mathfrak{f}$ un ideal no nulo de $\mathcal{O}$,

$$\varepsilon : (\mathcal{O} / \mathfrak{f})^\times \to \mathbb{T}$$

un caracter y

$$\chi_\infty : (\mathbb{R}^\times)^{r_1} \times (\mathbb{C}^\times)^{r_2} \to \mathbb{C}^\times$$

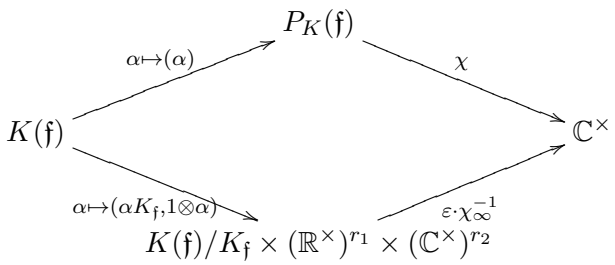
un caracter continuo. Entonces el caracter

$$\chi : I_K(\mathfrak{f}) \to \mathbb{C}^\times$$

es un **caracter de Hecke con conductor $\mathfrak{f}$, tipo-$(\mathcal{O} / \mathfrak{f})^\times$ ε y tipo-infinito** χ_∞ si

$$\chi((\alpha)) = \varepsilon(\alpha K_{\mathfrak{f}})\chi_\infty^{-1}(1 \otimes \alpha) \quad \forall \alpha \in K(\mathfrak{f})$$

está bien definido, donde ε está visto como un caracter de $K(\mathfrak{f})/K_{\mathfrak{f}}$. Esto es, que el siguiente diagrama conmute:



Observación 5.2.9. Nuevamente, que χ esté bien definido quiere decir que si $(\alpha) = (\beta)$ con $\alpha, \beta \in K(\mathfrak{f})$, entonces

$$\chi((\alpha)) = \chi((\beta)).$$

Pero como antes, si $(\alpha) = (\beta)$ entonces $\alpha = \beta u$ con $u \in \mathcal{O}^\times$. Luego

$$\begin{aligned}\chi((\alpha)) &= \varepsilon(\alpha K_{\mathfrak{f}})\chi_\infty^{-1}(1 \otimes \alpha) \\ &= \varepsilon(\beta u K_{\mathfrak{f}})\chi_\infty^{-1}(1 \otimes \beta u) \\ &= \varepsilon(\beta K_{\mathfrak{f}})\chi_\infty^{-1}(1 \otimes \beta)[\varepsilon(u K_{\mathfrak{f}})\chi_\infty^{-1}(1 \otimes u)] \\ &= \chi((\beta))[\varepsilon(u K_{\mathfrak{f}})\chi_\infty^{-1}(1 \otimes u)].\end{aligned}$$

Por lo tanto $\chi((\alpha)) = \chi((\beta))$ si y sólo si $\varepsilon(uK_{\mathfrak{f}}) = \chi_\infty(1 \otimes u) \ \ \forall u \in \mathcal{O}^\times$.

5.3. Correspondencia entre caracteres de Dirichlet y de Hecke clásicos

Como fue dicho anteriormente, los caracteres de Hecke van a resultar una generalización de los de Dirichlet. A priori uno estaría tentado en decir que los caracteres de Dirichlet se van a corresponder con caracteres de Hecke clásicos sobre $\mathbb{Q}$, pero esto no va a ser cierto. Una diferencia es que los caracteres de Dirichlet tienen orden finito, y no así los de Hecke clásicos. Veamos que existe una correspondencia entre los caracteres de Dirichlet (vistos como caracteres de $\mathbb{Q}(\mathfrak{f})/\mathbb{Q}_{\mathfrak{f}}$) y los caracteres de Hecke clásicos sobre $\mathbb{Q}$ de orden finito.

$$\begin{array}{c}\{\text{caracteres de Dirichlet}\} \longleftrightarrow \{\text{caracteres de Hecke clásicos sobre } \mathbb{Q} \text{ de orden finito}\} \\ \varepsilon(\alpha\mathbb{Q}_{\mathfrak{f}}) \quad \longleftrightarrow \quad \chi((\alpha)) = \varepsilon(\alpha\mathbb{Q}_{\mathfrak{f}})\,\chi_\infty^{-1}(\alpha)\end{array}$$

Definimos φ como la función que a un caracter de Dirichlet $\varepsilon : \mathbb{Q}(\mathfrak{f})/\mathbb{Q}_{\mathfrak{f}} :\to \mathbb{C}^\times$ lo manda al caracter de Hecke clásico $\chi = \varepsilon\chi_\infty^{-1}$, donde

$$\chi_\infty(\alpha) := \begin{cases} 1 & \text{si} \quad \varepsilon(-1\mathbb{Q}_{\mathfrak{f}}) = 1, \\ \operatorname{sgn}(\alpha) & \text{si} \quad \varepsilon(-1\mathbb{Q}_{\mathfrak{f}}) = -1. \end{cases} .$$

Recíprocamente, definimos la función ϕ que manda a un caracter de Hecke clásico sobre $\mathbb{Q}$ de orden finito, con conductor $\mathfrak{f}$, tipo-$(\mathcal{O}\,/\,\mathfrak{f})^\times$ ε y tipo-infinito χ_∞ a ε.

Claramente $\phi \circ \varphi = Id$. Veamos que $\varphi \circ \phi = Id$. Sea χ un caracter de Hecke de orden finito sobre $\mathbb{Q}$. Entonces

$$\chi(\alpha) = \varepsilon(\alpha\mathbb{Q}_{\mathfrak{f}})\,\chi_\infty^{-1}(\alpha).$$

Que χ tenga orden finito quiere decir que $\chi_\infty : \mathbb{R}^\times \to \mathbb{C}^\times$ es de orden finito. Luego, si $H := \ker(\chi_\infty)$ entonces $H < \mathbb{R}^\times$ y $[\mathbb{R}^\times : H] = n < \infty$.

Como $\mathbb{R}_{>0}$ es divisible (es decir que $\forall x \in \mathbb{R}_{>0}$ y $\forall n \in \mathbb{Z}$ no nulo existe $y \in \mathbb{R}_{>0}$ tal que $y^n = x$) entonces $\mathbb{R}_{>0} \subseteq H$, pues si $x \in \mathbb{R}_{>0}$ existe $y \in \mathbb{R}_{>0}$ tal que $x = y^n \in H$ ($[\mathbb{R}^\times : H] = n$). Luego, como $[\mathbb{R}^\times : \mathbb{R}_{>0}] = 2$, entonces $H = \mathbb{R}^\times$ o $H = \mathbb{R}_{>0}$. En particular,

$$\chi_\infty^{-1}(\alpha) = 1 \quad \forall \alpha \in \mathbb{R}_{>0}.$$

Resulta así

$$\chi_\infty(\alpha) = \chi_\infty(\alpha\,\mathrm{sgn}(\alpha))\chi_\infty(\mathrm{sgn}(\alpha)) = \chi_\infty(\mathrm{sgn}(\alpha)).$$

Como

$$1 = \chi((1)) = \chi((-1)) = \varepsilon(-1\mathbb{Q}_\mathfrak{f})\chi_\infty^{-1}(-1)$$

entonces si $\varepsilon(-1\mathbb{Q}_\mathfrak{f}) = 1$, tenemos que $\chi_\infty^{-1}(-1) = 1$ y luego $\chi_\infty(\alpha) = 1$ para todo α; y si $\varepsilon(-1\mathbb{Q}_\mathfrak{f}) = -1$ entonces $\chi_\infty^{-1}(-1) = -1$ y luego $\chi_\infty(\alpha) = \mathrm{sgn}(\alpha)$. Por lo tanto

$$\varphi \circ \phi = Id.$$

El hecho de que haya una correspondencia entre estos dos conjuntos nos lleva a la pregunta de si será cierto que ocurre lo mismo para un cuerpo genérico K. Esto no será cierto. El caso de $K = \mathbb{Q}$ funciona bien porque $\mathcal{O}_\mathbb{Q} = \mathbb{Z}$ tiene pocas unidades (1 y -1). En general, los cuerpos cuadráticos imaginarios tienen finitas unidades pero en un cuerpo de números arbitrario suele haber muchas más. Daremos a continuación un ejemplo en donde dicha correspondencia no funciona. Más precisamente, veremos que no todo caracter de Dirichlet se puede extender a uno de Hecke clásico de orden finito.

Ejemplo 5.3.1. Sea $K = \mathbb{Q}[\sqrt{7}]$. Como $7 \equiv 3$ (mód 4), entonces su anillo de enteros algebraicos es $\mathcal{O} = \mathbb{Z}[\sqrt{7}]$. Sea $\mathfrak{f} := (19, 8 - \sqrt{7})$ un ideal de $\mathcal{O}$. Notemos que $\mathfrak{f}$ resulta primo porque $\mathcal{O}/\mathfrak{f}$ es dominio íntegro. Más aún,

$$\mathcal{O}/\mathfrak{f} \cong \mathbb{F}_{19}$$

vía el isomorfismo φ que manda la clase de un número $a + b\sqrt{7}$ en la clase del número $a + 8b$. Luego, $(\mathcal{O}/\mathfrak{f})^\times \cong \mathbb{F}_{19}^\times$ es cíclico de orden 18. Más aún, $u := 8 - 3\sqrt{7}$ es una unidad y $\varphi(u) = -\overline{16} = \overline{3}$, que es un generador de $\mathbb{F}_{19}^\times$. Por lo tanto

$$(\mathcal{O}/\mathfrak{f})^\times = \langle u \rangle .$$

Por la Proposición 5.0.2, el grupo de caracteres de Dirichlet es de orden 18. Entonces, por el Teorema de Cauchy, existe un caracter de Dirichlet $\varepsilon : K(\mathfrak{f})/K_\mathfrak{f} \to \mathbb{C}^\times$ de orden 3. Sin pérdida de generalidad, podemos suponer que

$$\varepsilon(uK_\mathfrak{f}) = \zeta_3,$$

donde $\zeta_3 = \frac{-1+i\sqrt{3}}{2}$ es una raíz 3-ésima primitiva de la unidad. Sabemos que existe un monomorfismo de $\mathbb{R} \otimes_\mathbb{Q} K^\times$ en $\mathbb{R}^\times \times \mathbb{R}^\times$ vía

$$\alpha = a + b\sqrt{7} \mapsto 1 \otimes \alpha = (a + b\sqrt{7}, a - b\sqrt{7}) = (\alpha, \overline{\alpha}).$$

Veamos que ε no se puede extender porque para cada caracter $\chi_\infty : \mathbb{R}^\times \times \mathbb{R}^\times \to \mathbb{C}^\times$ de orden finito, no se cumple que

$$\varepsilon(\alpha K_\mathfrak{f}) = \chi_\infty(1 \otimes \alpha) \quad \forall \alpha \in \mathcal{O}^\times.$$

En efecto, supongamos que existe χ_∞ que sí lo cumpla. Entonces

$$\zeta_3 = \varepsilon(uK_\mathfrak{f}) = \chi_\infty(u, \overline{u}).$$

Sea $H_1 \times H_2 := \ker(\chi_\infty) < \mathbb{R}^\times \times \mathbb{R}^\times$. Esto nos dice que $(u, \overline{u})^3 \in H_1 \times H_2$ y que entonces 3 divide al índice de $H_1 \times H_2$. Por el mismo argumento que antes, como $\mathbb{R}^\times \times \mathbb{R}^\times$ es divisible, entonces

$$[\mathbb{R}^\times \times \mathbb{R}^\times : H_1 \times H_2] = 1, 2 \text{ ó } 4,$$

lo cual nos lleva a un absurdo. Por lo tanto, ε es como queríamos.

A pesar de que vimos que no podemos extender el caracter ε a $I(\mathfrak{f})$, no todo está perdido. Veamos que podemos encontrar un primo $\mathfrak{q}$ de K y $\varepsilon_\mathfrak{q} : (\mathcal{O}/\mathfrak{q})^\times \to \mathbb{C}^\times$, caracter de Dirichlet, tal que

$$\varepsilon\varepsilon_\mathfrak{q} : (\mathcal{O}/\mathfrak{q}\,\mathfrak{f})^\times \to \mathbb{C}^\times$$

sí se pueda extender a $I(\mathfrak{f}\,\mathfrak{q})$.
Dado que $\mathcal{O}^\times = \langle u, -1\rangle$, basta con ver que se cumple lo siguiente:

(1) $\varepsilon(-1K_\mathfrak{f})\,\varepsilon_\mathfrak{q}(-1K_\mathfrak{q}) = 1$.

(2) $\varepsilon(uK_\mathfrak{f})\,\varepsilon_\mathfrak{q}(uK_\mathfrak{q}) = 1$.

Además, notemos que $\varepsilon(-1K_\mathfrak{f}) = 1$, pues en caso contrario tendríamos que $\varepsilon(-1K_\mathfrak{f}) = -1$ y entonces como ε es de orden 3 resultaría que

$$1 = \varepsilon^3(-1K_\mathfrak{f}) = -1^3 = -1,$$

lo cual es absurdo. Sabiendo además que $\varepsilon(uK_\mathfrak{f}) = \zeta_3$, querríamos entonces que valgan:

(1) $\varepsilon_\mathfrak{q}(-1K_\mathfrak{q}) = 1$.

(2) $\varepsilon_\mathfrak{q}(uK_\mathfrak{q}) = \zeta_3^2$.

Tomemos $\mathfrak{q} = (5)$. Notemos que, como 7 no es un cuadrado módulo 5, entonces $x^2 - 7$ es irreducible módulo 5. Luego, $\mathfrak{q}$ es primo y

$$\mathcal{O}/\mathfrak{q} \cong \mathbb{Z}[\sqrt{7}]/(5) \cong (\mathbb{Z}/5\mathbb{Z})/(x^2 - 7) \cong \mathbb{F}_{5^2}.$$

Tenemos entonces que $(\mathcal{O}/\mathfrak{q})^\times$ es cíclico de orden 24. Además notemos que $u \in \mathcal{O}$ tiene orden 6 en el cociente $\mathcal{O}/\mathfrak{q} \cong \mathbb{F}_{5^2}$, pues

$$\begin{aligned} u^2 &= 64 - 48\sqrt{7} + 63 \equiv 2 - 3\sqrt{7} \pmod 5, \\ u^3 &= uu^2 \equiv (8 - 3\sqrt{7})(2 - 3\sqrt{7}) \equiv 79 - 20\sqrt{7} \equiv -1 \pmod 5, \\ u^6 &\equiv 1 \pmod 5 \end{aligned}$$

Luego, u tiene orden divisible por 3 y entonces existe $\varepsilon_\mathfrak{q}$ de orden 3 como queríamos.

5.4. Caracteres de Hecke

Definición 5.4.1. Un **caracter de Hecke** de K es un caracter continuo de los idèles de K que es trivial en $K^\times$. Es decir

$$\chi : \mathbb{I}_K \to \mathbb{C}^\times, \qquad \chi(K^\times) = 1.$$

Dado $\chi : \mathbb{I}_K \to \mathbb{C}^\times$ caracter de Hecke, queremos ver que podemos asociarle naturalmente un caracter de Hecke clásico.
Para cada lugar v, definimos $i_v : K_v^\times \to \mathbb{I}_K$ dado por

$$(i_v(x))_w = \begin{cases} x & \text{si } v = w \\ 1 & \text{si } v \neq w \end{cases}$$

y la función $\chi_v : K_v^\times \to \mathbb{C}^\times, \quad x \mapsto \chi(i_v(x))$.

Lema 5.4.2. Para cada lugar v de K, i_v es continua.

Demostración: Sea U un abierto básico de $\mathbb{I}_K$. Por lo visto antes, existen un conjunto S finito que contiene a S_∞ y abiertos U_v de $K_v^\times$ tales que

$$U = \prod_{v \notin S} \mathcal{O}_v^\times \times \prod_{v \in S} U_v.$$

Entonces, si v_0 es un lugar infinito se tiene que $i_{v_0}^{-1}(U) = U_{v_0}$, lo que nos dice que i_{v_0} es continua. Si v_0 es un lugar finito, tenemos que

$$i_{v_0}^{-1}(U) = \begin{cases} \mathcal{O}_{v_0}^\times & \text{si} \quad v_0 \notin S, \\ U_{v_0} & \text{si} \quad v_0 \in S. \end{cases}$$

Ambos casos nos aseguran que i_{v_0} es continua. □

Corolario 5.4.3. Para cada lugar v de K, χ_v es continuo.

Demostración: Resulta directo por ser χ_v composición de funciones continuas. □

Notemos que por la Proposición 3.3.11, para cada lugar finito v, $\chi_v : K_v^\times \to \mathbb{C}^\times$ queda determinado por su valor en $\mathcal{O}_v^\times = \mathcal{U}_v$ y en un uniformizador local π_v de $\mathfrak{p}_v$.

Lema 5.4.4. Para todo lugar finito v de K se cumple que χ_v tiene conductor. Más aún, su conductor es $\mathcal{O}_v^\times$ para casi todo v.

Demostración: Para ver la primera afirmación, necesitamos probar que existe n entero positivo tal que

$$\chi_v(1 + \pi_v^n \mathcal{O}_v) = 1.$$

Sea U un entorno abierto del 1 en $\mathbb{C}^\times$ tal que U no contiene un subgrupo no trivial de $\mathbb{C}^\times$. Entonces $\chi_v^{-1}(U)$ es abierto de K_v por el Corolario 5.4.3 y por lo tanto contiene un entorno abierto básico del 1. En otras palabras, existe n entero positivo tal que

$$1 + \pi_v^n \mathcal{O}_v \subseteq \chi_v^{-1}(U).$$

Luego, $\chi_v(1 + \pi_v^n \mathcal{O}_v) \subseteq U$. Pero como $1 + \pi^n \mathcal{O}_v$ es un subgrupo, entonces $\chi_v(1 + \pi_v^n \mathcal{O}_v)$ es un subgrupo (pues χ_v es caracter) y entonces por lo dicho antes,

$$\chi_v(1 + \pi_v^n \mathcal{O}_v) = 1.$$

Entonces χ_v tiene conductor. Denotando $1 + \pi_v^0 \mathcal{O}_v := \mathcal{O}_v^\times$ entonces podemos definir

$$e_v := \text{mín}\{n \geq 0 : \chi_v(1 + \pi_v^n \mathcal{O}_v) = 1\}.$$

Resulta así que el conductor de χ_v es $1 + \pi_v^{e_v} \mathcal{O}_v$.

Para probar la segunda afirmación debemos ver que $e_v = 0$ para casi todo v. Notemos que como χ es continua, entonces $\chi^{-1}(U)$ es abierto de $\mathbb{I}_K$ y luego contiene a un abierto básico. Es decir que existen un conjunto finito S tal que $S \supseteq S_\infty$ y abiertos U_v de $K_v^\times$ tales que

$$\chi^{-1}(U) \supseteq \prod_{v \notin S} \mathcal{O}_v^\times \times \prod_{v \in S} U_v$$

Luego, si $v_0 \notin S$ tenemos que $\chi_{v_0}(U) = \mathcal{O}_{v_0}^\times$ y entonces $U \supseteq \chi_{v_0}(\mathcal{O}_{v_0}^\times)$, lo que nos dice que $\chi_{v_0}(\mathcal{O}_{v_0}^\times) = 1$ y que por lo tanto $e_v = 0 \ \ \forall v \notin S$. □

Proposición 5.4.5. $\chi(x) = \prod_v \chi_v(x_v)$, donde $x = (x_v)$.

Demostración: Primero, notemos que el producto de la derecha tiene sentido, es decir que $\chi_v(x_v) = 1$ para casi todo v. En efecto, si $x = (x_v) \in \mathbb{I}_K$ sabemos que $x_v \in \mathcal{O}_v^\times$ para casi todo v y entonces el Lema 5.4.4 asegura lo que queríamos.

Dado $x = (x_v) \in \mathbb{I}_K$, entonces

$$x = \lim_S \prod_{v \in S} i_v(x_v),$$

donde el límite se toma sobre los conjuntos finitos de primos S. Luego, como χ es continuo se tiene que

$$\chi(x) = \lim_S \prod_{v \in S} \chi_v(x_v).$$

Pero sólo hay finitos v para los cuales $\chi_v(x_v) \neq 1$. Por lo tanto,

$$\chi(x) = \prod_v \chi_v(x_v).$$

Resulta así probada la afirmación. □

A la igualdad de la Proposición 5.4.5 la vamos a denotar como $\chi = \prod_v \chi_v$. Como consecuencia del Lema 5.4.4, si $\mathfrak{p}_v^{e_v}$ es el conductor de χ_v, entonces está bien definido

$$\mathfrak{f} := \prod_v \mathfrak{p}_v^{e_v}$$

y además resulta ser el conductor de χ.

Cabe destacar que en las definiciones de caracteres de Hecke (tanto clásicas como no), pedimos una condición de continuidad. El siguiente teorema nos dice que en caso de ser el caracter de orden finito, se satisface automáticamente la condición de continuidad si estamos trabajando con K_v.

Teorema 5.4.6. Sea v un lugar finito y $\chi : K_v^\times \to \mathbb{C}^\times$ un caracter de orden finito. Entonces χ es continuo.

Demostración: Como χ es de orden finito, la imagen es finita. Luego, existe un abierto U en $\mathbb{C}^\times$ tal que $\mathrm{Im}(\chi) \cap U = \{1\}$. Entonces $\ker(\chi) \cap \mathcal{O}_v$ tiene orden finito en $\mathcal{U}_v$. Así, usando el Teorema 3.3.20 tenemos que $\ker(\chi)$ es abierto y por lo tanto χ es continuo. □

5.5. Correspondencia entre caracteres de Hecke y caracteres de Hecke clásicos

Dado $\chi = \prod_v \chi_v$ un caracter de Hecke con conductor $\mathfrak{f} = \prod_v \mathfrak{p}_v^{e_v}$ queremos asociarle un caracter de Hecke clásico $\widetilde{\chi} : I_K(\mathfrak{f}) \to \mathbb{C}^\times$. Lo haremos de la siguiente forma:
Dado $I \in I_K(\mathfrak{f})$, por la Proposición 1.1.17, $I = \prod_{i=1}^{n} \mathfrak{p}_i^{\alpha_i}$, donde $\mathfrak{p}_i$ es un primo de $\mathcal{O}_K$, $(\mathfrak{p}_i, \mathfrak{f}) = 1$, $\alpha_i \in \mathbb{Z}$. Si $v_i := v_{\mathfrak{p}_i}$ es el lugar que define $\mathfrak{p}_i$, $\chi_i := \chi_{v_i}$ y $\pi_i := \pi_{v_i}$ es un uniformizador entonces definimos

$$\widetilde{\chi}(I) := \prod_{i=1}^{n} \chi_i(\pi_i)^{\alpha_i}.$$

Observación 5.5.1. Notemos que $\widetilde{\chi}$ no depende de la elección del uniformizador, ya que si $\widetilde{\pi}_i$ es otro uniformizador de $\mathfrak{p}_i$ entonces $\widetilde{\pi}_i/\pi_i \in \mathcal{O}_{v_i}^\times$ y como $\chi_i(\mathcal{O}_{v_i}^\times) = 1$ (pues $(\mathfrak{p}_i, \mathfrak{f}) = 1$) entonces

$$\chi_i(\widetilde{\pi}_i) = \chi_i\left(\frac{\widetilde{\pi}_i}{\pi_i}\pi_i\right) = \chi_i\left(\frac{\widetilde{\pi}_i}{\pi_i}\right)\chi_i(\pi_i) = \chi_i(\pi_i).$$

Además, $\chi_i(\pi_j) = 1$ si $i \neq j$, pues $\pi_i \in \mathcal{O}_{v_j}^\times$. Por lo tanto,

$$\widetilde{\chi}(I) = \prod_{\mathfrak{p}\,|I} \chi_{v_\mathfrak{p}}(\pi_{v_\mathfrak{p}})^{\alpha_\mathfrak{p}} = \prod_{\mathfrak{p}\,|I} \chi_{v_\mathfrak{p}}(I),$$

donde $\alpha_\mathfrak{p}$ es la potencia a la cual aparece $\mathfrak{p}$ en la descomposición en primos de I.

Claramente, $\widetilde{\chi}$ es morfismo y si $a \in K_\mathfrak{f}$ entonces $\chi_{v_\mathfrak{p}}(a) = 1$ para todo $\mathfrak{p}$ que divide a $\mathfrak{f}$. Por lo tanto,

$$\widetilde{\chi}_\infty^{-1}(1 \otimes a) = \widetilde{\chi}((a)) = \prod_{\mathfrak{p}\,|(a)} \chi_{v_\mathfrak{p}}(a) = \prod_{\mathfrak{p}} \chi_{v_\mathfrak{p}}(a) = \chi_\infty^{-1}(a).$$

Vimos entonces que $\widetilde{\chi}_\infty = \chi_\infty$ y que $\mathfrak{f}$ divide al conductor de $\widetilde{\chi}$. Veamos que $\mathfrak{f}$ es exactamente el conductor de $\widetilde{\chi}$. Para eso, debemos ver que dado $\mathfrak{p}_v$ que aparece en la factorización de $\mathfrak{f}$ existen $\alpha, \beta \in \mathcal{O}_K$ (que dependen de $\mathfrak{p}_v$) tales que $\alpha \equiv \beta \pmod{\mathfrak{p}_v^{e_v - 1}}$, $\alpha \equiv \beta \pmod{\mathfrak{p}_w^{e_w}}$ para todo $\mathfrak{p}_w$ que aparece en la factorización de $\mathfrak{f}$ con $w \neq v$ y tal que

$$\varepsilon(\alpha) \neq \varepsilon(\beta),$$

donde ε es la parte finita, i.e, $\varepsilon = \prod_{v<\infty} \chi_v$. Como

$$e_v = \min\{n : \chi_v(1 + \pi_v^n\, \mathcal{O}_v) = 1\}$$

entonces existe $\gamma \in 1 + \pi^{e_v - 1}\, \mathcal{O}_v$ tal que $\chi_v(\gamma) \neq 1$. Luego, por el Teorema 4.1.4, existe $\alpha \in \mathcal{O}_K$ tal que

$$\chi_v(\alpha) = \chi_v(\gamma) \neq 1.$$

Tomando $\beta = 1$, se cumple claramente que $\chi_v(\beta) = 1 \neq \chi_v(\alpha)$. Resulta así

$$\begin{aligned}\varepsilon(\alpha) &= \prod_{w<\infty} \chi_w(\alpha) = \prod_{w|\mathfrak{f}} \chi_w(\alpha) \\ &= \chi_v(\alpha) \prod_{\substack{w|\mathfrak{f} \\ w\neq v}} \chi_w(\alpha) = \chi_v(\alpha) \prod_{\substack{w|\mathfrak{f} \\ w\neq v}} \chi_w(\beta) \\ &\neq \chi_v(\beta) \prod_{\substack{w|\mathfrak{f} \\ w\neq v}} \chi_w(\beta) = \varepsilon(\beta).\end{aligned}$$

Por lo tanto, $\mathfrak{f}$ es el conductor de $\widetilde{\chi}$.

Recíprocamente, dado un caracter de Hecke clásico $\widetilde{\chi} : I_K(\mathfrak{f}) \to \mathbb{C}^\times$ queremos ver que podemos definir un caracter de Hecke χ.

Como $1 \otimes_{\mathbb{Q}} K_{\mathfrak{f}}$ es denso en $\mathbb{R} \otimes_{\mathbb{Q}} K$, entonces χ_∞ está totalmente determinado por $\widetilde{\chi}_\infty$. Antes de definir la parte finita, para aliviar la notación, diremos que $v \mid \mathfrak{f}$ si $\mathfrak{p}_v \mid \mathfrak{f}$. Ahora, para definir la parte finita hacemos lo siguiente:

Si $v \nmid \mathfrak{f}$, definimos χ_v como

$$\chi_v(\pi_v) := \widetilde{\chi}(\mathfrak{p}_v), \quad \chi_v(\mathcal{O}_v^\times) = 1.$$

Por otro lado, si $x \in \prod_{v|\mathfrak{f}} K_v^\times$ entonces por el Teorema 4.1.4 existe $\alpha \in K^\times$ tal que $|\alpha - x_v|_v < \varepsilon$, con

$$\varepsilon := \min_{v|\mathfrak{f}} \{|\pi_v|_v^{e_v + ord_v(x_v)}\}.$$

Entonces definimos

$$\prod_{v|\mathfrak{f}} \chi_v(x_v) := \prod_{v\nmid\mathfrak{f}} \chi_v^{-1}(\alpha)$$

precisamente para que se cumpla la propiedad que queremos. Esto es, dado $a \in K^\times$ se cumple

$$\prod_v \chi_v(a) = \prod_{v\nmid\mathfrak{f}} \chi_v(a) \prod_{v|\mathfrak{f}} \chi_v(a) = 1.$$

Luego, definiendo $\chi := \prod_v \chi_v$, se satisface la fórmula del producto. Veamos que χ está bien definido. Para eso necesitamos el siguiente lema.

Lema 5.5.2. Si $a \in K_{\mathfrak{f}}$, entonces

$$\prod_{v\nmid\mathfrak{f}} \chi_v(a) = \widetilde{\chi}((a)).$$

Demostración: Dado $a \in K_{\mathfrak{f}}$,

$$\prod_{v\nmid\mathfrak{f}} \chi_v(a) = \prod_{v\nmid\mathfrak{f}} \chi_v(\pi_v)^{v_{\mathfrak{p}_v}(a)} = \prod_{v\nmid\mathfrak{f}} \widetilde{\chi}(\mathfrak{p}_v)^{v_{\mathfrak{p}_v}(a)} = \widetilde{\chi}\left(\prod_{v\nmid\mathfrak{f}} \mathfrak{p}_v^{v_{\mathfrak{p}_v}(a)}\right) = \widetilde{\chi}((a)).$$

Resulta así probada la afirmación. □

Para ver ahora la buena definición tomemos $x \in \prod_{v \nmid \mathfrak{f}} K_v^\times$ y supongamos que $\alpha, \beta \in K^\times$ son tales que $|x_v - \alpha|_v < \varepsilon$ y $|x_v - \beta|_v < \varepsilon$. Queremos ver que

$$\prod_{v \nmid \mathfrak{f}} \chi_v^{-1}(\alpha) = \prod_{v \nmid \mathfrak{f}} \chi_v^{-1}(\beta).$$

Como $|x_v - \alpha|_v < \varepsilon$, $|x_v - \beta|_v < \varepsilon$ y v es finito entonces $|\alpha - \beta|_v < \varepsilon$. Luego, para cada v que divide a $\mathfrak{f}$ tenemos que

$$|\alpha - \beta|_v < |\pi_v|_v^{e_v + ord_v(x_v)},$$

pues v es arquimediano. Esto equivale a

$$ord_v(\alpha - \beta) > e_v + ord_v(x_v).$$

Por la Proposición 3.3.11 existe $u \in \mathcal{U}_v$ tal que $x_v = \pi_v^{ord_v(x_v)} u$. Luego,

$$\pi_v^{e_v} x_v u^{-1} = \pi_v^{e_v} \pi_v^{ord_v(x_v)} = \pi_v^{e_v + ord_v(v_v)} \mid \alpha - \beta$$

y por lo tanto $\pi_v^{e_v} x_v \mid \alpha - \beta$, es decir que $\alpha / x_v \equiv \beta / x_v \pmod{\pi_v^{e_v}}$ y entonces

$$\frac{\alpha}{\beta} \equiv \frac{\alpha / x_v}{\beta / x_v} \equiv 1 \pmod{\pi_v^{e_v}}.$$

Por lo tanto $\alpha/\beta \in K_{\mathfrak{f}}$ y luego, por el Lema 5.5.2,

$$\prod_{v \nmid \mathfrak{f}} \chi_v \left(\frac{\alpha}{\beta} \right) = \widetilde{\chi} \left(\left(\frac{\alpha}{\beta} \right) \right).$$

En consecuencia,

$$\begin{aligned} \prod_{v \nmid \mathfrak{f}} \chi_v \left(\frac{\alpha}{\beta} \right) &= \prod_{v \nmid \mathfrak{f}} \chi_v \left(\frac{\alpha}{\beta} \right) \chi_\infty \left(\frac{\alpha}{\beta} \right) \\ &= \widetilde{\chi} \left(\left(\frac{\alpha}{\beta} \right) \right) \chi_\infty \left(\frac{\alpha}{\beta} \right) \\ &= \varepsilon \left(\frac{\alpha}{\beta} \right) \widetilde{\chi}_\infty^{-1} \left(\frac{\alpha}{\beta} \right) \chi_\infty \left(\frac{\alpha}{\beta} \right) = \varepsilon \left(\frac{\alpha}{\beta} \right) = 1 \end{aligned}$$

y esto demuestra lo que buscábamos.

Resta ver que $\mathfrak{f}$ es el conductor de χ. Como el conductor de $\widetilde{\chi}$ es $\mathfrak{f} = \prod_v \mathfrak{p}_v^{e_v}$, entonces existen $\alpha, \beta \in \mathcal{O}_K$ tales que $\alpha \equiv \beta \pmod{\mathfrak{p}_v^{e_v - 1}}$ y $\widetilde{\chi}((\alpha)) \neq \widetilde{\chi}((\beta))$. Luego, $\chi((\alpha)) \neq \chi((\beta))$.

5.6. Corrrespondencia entre caracteres de Hecke y caracteres de Dirichlet

En las secciones anteriores hemos visto que cuando $K = \mathbb{Q}$ existe una biyección entre los caracteres de Dirichlet y los de Hecke clásicos de orden finito. Por otro lado, vimos también que los de Hecke clásicos se corresponden con los de Hecke. Esto nos dice que los caracteres

de Dirichlet son equivalentes a los de Hecke de orden finito. Veamos dicha correspondencia de manera explícita. Para eso, notemos que un caracter de Dirichlet

$$\chi_D : (\mathbb{Z}/N\mathbb{Z})^\times \to \mathbb{T}$$

puede ser visto como un caracter continuo

$$\chi_D : \widehat{\mathbb{Z}}^\times \to \mathbb{T},$$

ya que $(\mathbb{Z}/N\mathbb{Z})^\times$ es un cociente de $\widehat{\mathbb{Z}}^\times$ y la topología de $\widehat{\mathbb{Z}} = \varprojlim_n \mathbb{Z}/n\mathbb{Z}$ hace a χ_D continua. Luego, por el Ejemplo 4.2.4 podemos definir un caracter de Hecke $\chi_H : \mathbb{Q}^\times \times \widehat{\mathbb{Z}}^\times \times \mathbb{R}_{>0} \to \mathbb{C}^\times$ como

$$\chi_H(\alpha u t) := \chi_D(u),$$

donde $\alpha \in \mathbb{Q}^\times, u \in \widehat{\mathbb{Z}}^\times$ y $t \in \mathbb{R}_{>0}$.

Para asignarle ahora un caracter de Dirichlet a uno de Hecke de orden finito, simplemente hay que notar que todo caracter $\chi : \widehat{\mathbb{Z}}^\times \to \mathbb{C}^\times$ continuo es un caracter de Dirichlet. Eso resulta del hecho, discutido con anterioridad, de que $\mathbb{C}^\times$ tiene un entero abierto de la unidad que no contiene subgrupos no triviales.

Capítulo 6

Teoría de cuerpos de clases

En este capítulo daremos una presentación al mapa de Artin y sus propiedades y nos introduciremos en la teoría de cuerpos de clases, enunciado los resultados más importantes de la teoría global. Para detalles y demostraciones se puede consultar [Cas67] o [Jan96].

Vamos a suponer que K es un cuerpo de números de grado n y que L/K es una extensión finita de cuerpos.

6.1. El mapa de Artin

Retomando con la Sección 1.1.1, si $\mathfrak{p}$ es un primo de K y $\mathfrak{P}$ un primo de L sobre $\mathfrak{p}$ entonces por la Proposición 1.1.29 obtenemos que $D_{\mathfrak{P}}/I_{\mathfrak{P}} \cong \mathrm{Gal}(l_{\mathfrak{P}}/k_{\mathfrak{p}})$. Pero por la Proposición 1.1.19, $k_{\mathfrak{p}}$ es un cuerpo finito, digamos de q elementos. Luego, como $l_{\mathfrak{P}}/k_{\mathfrak{p}}$ es una extensión finita de cuerpos finitos tenemos por Teoría de Galois que

$$\mathrm{Gal}(l_{\mathfrak{P}}/k_{\mathfrak{p}}) = \langle Frob_q \rangle,$$

donde $Frob_q$ es el morfismo de Frobenius, i.e., $Frob_q(x) := x^q$.

Luego, existe un único elemento en $D_{\mathfrak{P}}/I_{\mathfrak{P}}$ que va a parar a $Frob_q$. A tal elemento lo denotaremos $(\mathfrak{P}, L/K)$. Dicho morfismo está además caracterizado por

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

Al morfismo $(\mathfrak{P}, L/K)$ lo llamaremos **símbolo de Artin** de $\mathfrak{P}$. Notemos que si el grupo de inercia es trivial entonces obtenemos así que $D_{\mathfrak{P}} \cong \mathrm{Gal}(l_{\mathfrak{P}}/k_{\mathfrak{p}})$. Nos centraremos a partir de ahora en este caso.

Proposición 6.1.1. Seal L/K Galois y $\mathfrak{p}$ un primo de K que no ramifica. Dado un primo $\mathfrak{P}$ de L sobre $\mathfrak{p}$ se cumple que:

(1) Si $\sigma \in \mathrm{Gal}(L/K)$ entonces $\sigma D(\mathfrak{P})\sigma^{-1} = D(\sigma(\mathfrak{P}))$ y

$$(\sigma(\mathfrak{P}), L/K) = \sigma(\mathfrak{P}, L/K)\sigma^{-1}.$$

(2) El orden de $(\mathfrak{P}, L/K)$ es el grado de inercia $f(\mathfrak{P} \mid \mathfrak{p})$.

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

Demostración:

(1) La primera afirmación es clara. Para la segunda, dado $\alpha \in \mathcal{O}_L$, por la caracterización dada del símbolo de Artin, tenemos que $(\mathfrak{P}, L/K)\sigma^{-1}(\alpha) \equiv \sigma^{-1}(\alpha)^q \pmod{\mathfrak{P}}$. Aplicando σ (que es multilpicativo) obtenemos que

$$\sigma(\mathfrak{P}, L/K)\sigma^{-1}(a) \equiv \alpha^q \pmod{\sigma(\mathfrak{P})}.$$

(2) Por inciso (2) de la Proposición 1.1.29 tenemos que $|\operatorname{Gal}(l_{\mathfrak{P}}/k_{\mathfrak{p}})| = f(\mathfrak{P} \mid \mathfrak{p})$. Como el símbolo de Artin genera dicho grupo entonces tiene orden $f(\mathfrak{P} \mid \mathfrak{p})$.

(3) Como $\mathfrak{p}$ es no ramificado por hipótesis entonces $e(\mathfrak{P} \mid \mathfrak{p}) = 1$ y por lo tanto se sigue directo de (2).

Resulta así probada la proposición. □

Notemos que (1) nos dice que los símbolos de Artin de los primos de L que están sobre un primo fijo de K son conjugados en $\operatorname{Gal}(L/K)$. Esto nos permite asignarle a cada primo de K una clase de conjugación de $\operatorname{Gal}(L/K)$. Luego, si la extensión es abeliana, entonces tenemos que la clase de conjugación que define un primo $\mathfrak{p}$ de K tiene un sólo elemento, pues si $\mathfrak{P}$ y $\mathfrak{P}'$ son dos primos en L que están sobre $\mathfrak{p}$ entonces por Teorema 1.1.25 existe $\sigma \in \operatorname{Gal}(L/K)$ tal que $\sigma(\mathfrak{P}) = \mathfrak{P}'$ y por Proposición 6.1.1,

$$(\mathfrak{P}', L/K) = \sigma(\mathfrak{P}, L/K)\sigma^{-1} = (\mathfrak{P}, L/K)\sigma\sigma^{-1} = (\mathfrak{P}, L/K).$$

A este único elemento lo llamaremos **símbolo de Artin** de $\mathfrak{p}$ y lo denotaremos por $(\mathfrak{p}, L/K)$.

Imaginémonos por un instante que estamos en el maravilloso caso en que nuestra extensión L/K no ramifica y es abeliana. Entonces, para cada primo $\mathfrak{p}$ de K tenemos definido su símbolo de Artin. Luego, utilizando la propiedad que nos garantiza la Proposición 1.1.17 podemos definir por multiplicidad a una función

$$I_K \to \operatorname{Gal}(L/K), \quad \prod_{i=1}^{r} \mathfrak{p}_i^{n_i} \mapsto \prod_{i=1}^{r} (\mathfrak{p}_i, L/K)^{n_i}.$$

Este caso resulta utópico pues, en general, las extensiones no tienen por qué ser no ramificadas. Aun así, no todo está perdido. Dado un conjunto de primos S de K, podemos definir I_K^S el subconjunto de I_K generado por los ideales que no están en S. Luego, si la extensión es abeliana y tomamos a S como el conjunto de ideales primos de K que ramifican, entonces podemos definir el **mapa de Artin** como la función

$$\begin{aligned} \psi_{L/K} : I_K^S &\to \operatorname{Gal}(L/K) \\ \prod_{\mathfrak{p} \notin S} \mathfrak{p}^{n_{\mathfrak{p}}} &\mapsto \prod_{\mathfrak{p} \notin S} (\mathfrak{p}, L/K)^{n_{\mathfrak{p}}}. \end{aligned}$$

Proposición 6.1.2. Sea $K \subseteq L \subseteq F$ una torre de extensiones finitas de Galois. Sea $\mathfrak{B}$ un primo no ramificado de F que está sobre un primo de $\mathfrak{P}$ de L, que a su vez está sobre un primo $\mathfrak{p}$ de K. Entonces:

(1) $(\mathfrak{B}, F/L) = (\mathfrak{B}, F/K)^{f(\mathfrak{P} \mid \mathfrak{p})}$.

(2) $(\mathfrak{B}, F/K)_{|_L} = (\mathfrak{P}, L/K)$.

Demostración:

(1) Sale del hecho de que el elemento de Frobenius de la extensión de arriba es elevar a la $f(\mathfrak{P} \mid \mathfrak{p})$ el elemento de Frobenius de la extensión total.

(2) Es trivial, ya que $(\mathfrak{B}, F/K)_{|_L}$ cumple la propiedad que caracteriza a $(\mathfrak{P}, L/K)$.

Queda así probada la proposición. □

Lema 6.1.3. Sean L/K y L'/K' extensiones finitas y abelianas, con $K \subseteq K'$, $L \subseteq L'$ 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:

$$\begin{array}{ccc} I_K^{S'} & \xrightarrow{\psi_{L'/K'}} & \mathrm{Gal}(L'/K') \\ {\scriptstyle N_{K'/K}}\downarrow & & \downarrow{\scriptstyle \mathrm{rest}} \\ I_K^{S} & \xrightarrow[\psi_{L/K}]{} & \mathrm{Gal}(L/K) \end{array}$$

Demostración: Sea $\mathfrak{p}'$ un ideal de K' sobre un ideal $\mathfrak{p}$ de K que no está en S'. Entonces por Definición 1.1.31, $N_{K'/K}(\mathfrak{p}') = \mathfrak{p}^{f(\mathfrak{p}' \mid \mathfrak{p})}$. Luego, se sigue que $\psi_{L/K}(\mathfrak{p})^{f(\mathfrak{p}' \mid \mathfrak{p})} = (\mathrm{rest} \circ \psi_{L'/K'})(\mathfrak{p}')$ por la Proposición 6.1.2. □

Corolario 6.1.4. Sea L/K finita y abeliana y S el conjunto de primos ramificados. Entonces $\psi_{L/K}(N_{L/K}(I_L^{S'})) = 1$, donde S' es el conjunto de primos de L que están sobre los de S.

Demostración: Directo del lema anterior, tomando $K' = L = L'$. □

Ejemplo 6.1.5. Sean $K = \mathbb{Q}$ y $L = \mathbb{Q}[\sqrt{m}]$, donde m es un entero libre de cuadrados. Es sabido que los primos que ramifican son los que dividen al discriminante de L, con lo cual si S es el conjunto de primos que ramifican, está compuesto de los primos que dividen a m si $m \equiv 1 \pmod 4$ y los primos que dividen a m más el 2 si $m \equiv 2, 3 \pmod 4$. Luego, identificando $\mathrm{Gal}(L/K)$ con $\{\pm 1\}$, el mapa de Artin está dado por

$$p \mapsto \left(\frac{m}{p}\right),$$

donde $\left(\frac{m}{p}\right)$ es el residuo cuadrático (símbolo de Legendre).

Ejemplo 6.1.6. Sean $K = \mathbb{Q}$ y $L = \mathbb{Q}[\zeta_m]$, donde ζ_m es una raíz primitiva m-ésima de la unidad. Asumamos que m es impar o múltiplo de 4 (así los primos que ramifican son precisamente los que dividen a m). Es sabido que el mapa

$$(\mathbb{Z}/m\mathbb{Z})^\times \to \mathrm{Gal}(L/K), \quad [n] \mapsto (\zeta_m \mapsto \zeta_m^n)$$

define un isomorfismo de grupos. Sea p primo que no divide a m y $\sigma \in \mathrm{Gal}(L/K)$ la imagen de $[p]$ vía el isomorfismo dado. Notemos que $\sigma(x) \equiv x^p \pmod{p\,\mathcal{O}_L} \quad \forall x \in \mathcal{O}_L$. En efecto,

como $\mathcal{O}_L = \mathbb{Z}[\zeta_m]$, dado $x \in \mathcal{O}_L$ podemos escribirlo como $x = \sum_{i=1}^{n} a_i \zeta_m^i$ con $a_i \in \mathbb{Z}$ y luego por el Pequeño Teorema de Fermat se tiene que

$$x^p \equiv \sum_{i=1}^{n} a_i^p \zeta_m^{ip} \equiv \sum_{i=1}^{n} a_i \zeta_m^{ip} \equiv \sigma(x) \pmod{p\,\mathcal{O}_L}.$$

Como $p\,\mathcal{O}_L$ está contenido en cualquier primo que esté sobre p, resulta así, por definición, que si p no divide a m entonces $(p, L/K) = [p]$. Además, si r, s son enteros positivos coprimos con m, entonces r/s define una clase $[r/s] = [r][s]^{-1} \in (\mathbb{Z}/m\mathbb{Z})^\times$. Resulta así el mapa de Artin como la composición

$$I_{\mathbb{Q}}^S \xrightarrow{(r/s)\mapsto[r/s]} (\mathbb{Z}/m\mathbb{Z})^\times \xrightarrow{[n]\mapsto(\zeta_m\mapsto\zeta_m^n)} \mathrm{Gal}(L/K).$$

6.2. Teoría global de cuerpos de clases

Definición 6.2.1. Un **módulo** $\mathfrak{m}$ en K es un producto formal

$$\mathfrak{m} = \prod_{v \notin S_\infty} \mathfrak{p}_v^{n_v} \times \prod_{v \in S_\infty} v^{n_v}$$

tal que:

(1) $n_v \geq 0$ para todo v y es 0 para casi todo v.

(2) $n_v = 0$ si v es infinito complejo.

(3) $n_v \leq 1$ si v es un lugar infinito real.

Luego, es inmediato que todo módulo $\mathfrak{m}$ es K 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 lugares reales distintos de K. Si todos los exponentes n_v son 0 entonces asumimos $\mathfrak{m} = 1$. Decimos que $v \mid \mathfrak{m}$ si $n_v > 0$.

Dado un módulo $\mathfrak{m}$ denotamos por $I_K(\mathfrak{m})$ al conjunto de todos los ideales coprimos con $\mathfrak{m}$ (es decir, coprimos con $\mathfrak{m}_0$). En otras palabras, $I_K(\mathfrak{m}) = I_K^{S(\mathfrak{m})}$, donde $S(\mathfrak{m})$ es el conjunto de primos que dividen a $\mathfrak{m}$ (finitos e infinitos).

Diremos que un elemento $\alpha \in K^\times$ es congruente a 1 módulo $\mathfrak{m}$, y lo denotaremos como $\alpha \equiv^* 1 \pmod{\mathfrak{m}}$, si $ord_v(\alpha - 1) \geq n_v$ para todo v finito que divide a $\mathfrak{m}$ y $\sigma_v(\alpha) > 0$ para los v infinitos (reales) que dividen a $\mathfrak{m}$, donde σ_v es la inmersión correspondiente v.

Si $id : K^\times \to I_K$ es la aplicación $\alpha \mapsto (\alpha)$ entonces definimos los conjuntos

$$\begin{aligned} P_K(\mathfrak{m}) &:= P_K(\mathfrak{m}_0) = \{(\alpha) : ord_v(\alpha) = 0 \ \forall v \text{ finito}, v \mid \mathfrak{m}\} \\ K_{\mathfrak{m},1} &:= \{\alpha \in K^\times : \alpha \equiv^* 1 \pmod{\mathfrak{m}}\} \\ P_{K,1}(\mathfrak{m}) &:= id(K_{\mathfrak{m},1}) \end{aligned}$$

Luego, es inmediato que $K_{\mathfrak{m}_0} \subseteq K_{\mathfrak{m},1}$ y $P_K^1(\mathfrak{m}_0) \subseteq P_{K,1}(\mathfrak{m}) \subseteq P_K(\mathfrak{m})$. Notemos además que cuando $\mathfrak{m}$ es trivial tenemos $I_K(1) = I_K$ y $P_{K,1}(1) = P_K(1) = P_K$

Ejemplo 6.2.2. Si tomamos $\mathfrak{m} = (m)\infty$ como módulo de $\mathbb{Q}$, donde $m \in \mathbb{Z}$ y ∞ es el único lugar infinito entonces si $m = p_1^{k_1} \cdots p_r^{k_r}$ tenemos que $\mathbb{Q}_{\mathfrak{m},1}$ consiste de los números raciones a/b con $a, b \in \mathbb{Z}$, $(a, m) = (b, m) = 1$, $(a/b) > 0$ tales que $ab^{-1} = 1$ en $(\mathbb{Z}/p_i^{k_i}\mathbb{Z}^\times)$ para todo $i = 1, ..., r$. Es decir, tales que $a \equiv b \pmod{m}$.

Definición 6.2.3. Definimos el **grupo de clases radial módulo** $\mathfrak{m}$ al cociente

$$C_{\mathfrak{m}} := I_K(\mathfrak{m})/P_{K,1}(\mathfrak{m}).$$

Además, decimos que un conjunto H es un **subgrupo de congruencia módulo** $\mathfrak{m}$ si cumple que $H \leq I_K(\mathfrak{m})$ y $P_{K,1}(\mathfrak{m}) \subseteq H$.

En particular, por lo visto antes tenemos que $P_{K,1}(\mathfrak{m})$ es un subgrupo de congruencia módulo $\mathfrak{m}$. En general, los subgrupos de congruencia están en correspondencia con los subgrupos de $C_{\mathfrak{m}}$ vía la proyección canónica de $I_K(\mathfrak{m})$ a $C_{\mathfrak{m}}$.

Recordemos que si L/K es finita y abeliana y S es el conjunto de los primos de K que ramifican, entonces teníamos definido el mapa de Artin $\psi_{L/K} : I_K^S \to \mathrm{Gal}(L/K)$.

Supongamos ahora que tenemos un módulo $\mathfrak{m}$ tal que $S \subseteq S(\mathfrak{m})$. Entonces $I_K(\mathfrak{m}) \subseteq I_K^S$ y por lo tanto tenemos definido el morfismo $\psi_{L/K} : I_K^S(\mathfrak{m}) \to \mathrm{Gal}(L/K)$. Esto nos lleva a la siguiente definición

Definición 6.2.4. Sea S un conjunto finito de primos de K y G un grupo finito abeliano. Un módulo $\mathfrak{m}$ en K se dice **admisible** para un morfismo $\psi : I_K^S \to G$ si $S \subseteq S(\mathfrak{m})$ y $\psi(P_{K,1}(\mathfrak{m})) = 1$. Diremos que $\psi_{L/K}$ **admite** módulo si existe un módulo admisible para ella.

Se puede ver que si $S \subseteq S'$ y $\psi : I_K^S \to G$ admite módulo entonces la restricción de ψ a $I_K^{S'}$ también admite módulo.

Luego, cabe preguntarse entonces si existirá algún módulo $\mathfrak{m}$ tal que $S(\mathfrak{m}) = S$. Esto va a ser cierto y es uno de los teoremas más importante de la teoría de clases.

Teorema 6.2.5. (Reciprocidad) Dada L/K finita y abeliana, existe un módulo $\mathfrak{m}$ de K tal que $S(\mathfrak{m}) = S$. Además, $\psi_{L/K}$ es suryectiva y $\ker(\psi_{L/K})$ es un subgrupo de congruencia para $\mathfrak{m}$ (lo que nos dice que $\psi_{L/K}(P_{K,1}(\mathfrak{m}) = 1)$).

Más aún, el núcleo es exactamente $N_{L/K}(I_L^{S'})P_{K,1}(\mathfrak{m})$, donde S' es el conjunto de primos que están sobre primos de S. Así, esto induce un isomorfismo

$$I_K(\mathfrak{m})/N_{L/K}(I_L^{S'})P_{K,1}(\mathfrak{m}) \cong \mathrm{Gal}(L/K)$$

Demostración: Ver [Jan96, Teorema 5.8]. □

Teorema 6.2.6. (Existencia) Dado $\mathfrak{m}$ un módulo de K y H un subgrupo de congruencia módulo $\mathfrak{m}$, existe una única extensión (contenida en una clausura algebraica fija de K) L/K finita abeliana, tal que los primos que ramifican dividen a $\mathfrak{m}$, y más aún, tal que $H = \ker(\psi_{L/K} : I_K(\mathfrak{m}) \to \mathrm{Gal}(L/K))$. En particular,

$$I_K(\mathfrak{m})/H \cong \mathrm{Gal}(L/K).$$

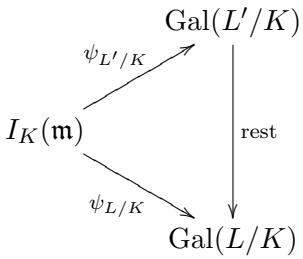
Demostración: Ver [Jan96, páginas 208–214]. □

Resulta así $\mathrm{Gal}(L/K)$ isomorfo a $C_{\mathfrak{m}}/\overline{H}$, donde $\overline{H}$ es la imagen de H en $C_{\mathfrak{m}}$. La extensión L de K dada por el teorema de existencia se llamará **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. Cuando $\mathfrak{m} = 1$, la extensión $K_{\mathfrak{m}}$ se llamará el **cuerpo de clases de Hilbert de** K.

6.3. Reinterpretación en términos de idèles

En esta sección nos encargaremos de traducir los anteriores teoremas en términos de idèles. El primero en realizar esto fue Chevalley y la razón es que la clásica manera de estudiar el mapa de Artin en términos de ideales no es muy adecuada para extensiones infinitas abelianas. Veamos por qué:

Supongamos que $K \subset L \subset L'$ es una cadena de extensiones finitas abelianas. Por el teorema de reciprocidad tenemos que existe un módulo $\mathfrak{m}$ en K tal que los primos que ramifican en la extensión L'/K son exactamente $S(\mathfrak{m})$. En particular $\mathfrak{m}$ es admisible para $\psi_{L'/K}$ y por lo tanto para $\psi_{L/K}$. Entonces, el siguiente diagrama conmuta:



Pero a medida que L' crece, el módulo $\mathfrak{m}$ va cambiando y de hecho va aumentando, ya que se incremente la cantidad de primos que ramifican. Por lo tanto $I_K(\mathfrak{m})$ se ve afectado a medida que cambiamos L'. Nuestro actual objetivo es reemplazar $I_K(\mathfrak{m})$ por algún objeto que no se altere si hacemos crecer a L'.

Sea $\mathfrak{m} = \prod_{v<\infty} \mathfrak{p}_v^{n_v} \times \prod_{v\in S_\infty} v^{n_v}$ un módulo en K. Queremos comenzar generalizando la noción de congruencia módulo $\mathfrak{m}$ a idèles.

Dado $\alpha \in K_v$, supongamos que v es finito y $n_v > 0$. Decimos que $\alpha \equiv^{\times} 1 \pmod{\mathfrak{m}_v}$ si $\alpha \in \widehat{\mathcal{O}_v}$ y $\alpha \equiv 1 \pmod{\widehat{\mathfrak{p}_v}}$. Si v es infinito real, decimos que $\alpha \equiv^{\times} 1 \pmod{\mathfrak{m}_v}$ si $\alpha > 0$.

Por último, si $\alpha \in \mathbb{I}_K$, decimos que $\alpha \equiv^{\times} 1 \pmod{\mathfrak{m}}$ si $\alpha_v \equiv^{\times} 1 \pmod{\mathfrak{m}_v}$ para todo v tal que $v|\,\mathfrak{m}$. Definimos el conjunto

$$\mathbb{I}_{\mathfrak{m}} := \{\alpha \in \mathbb{I}_K : \alpha \equiv^{\times} 1 \pmod{\mathfrak{m}}\}.$$

Así, pudimos extender la noción de congruencia, ya que visto $K^\times$ dentro de $\mathbb{I}_K$, tenemos que $\mathbb{I}_{\mathfrak{m}} \cap K^\times = K_{\mathfrak{m},1}$.

Definición 6.3.1. Definimos la función $id : \mathbb{I}_K \to I_K$ como

$$x \mapsto \prod_{v<\infty} \mathfrak{p}_v^{ord_v(x_v)}.$$

Notemos que la función está bien definida porque como $x \in \mathbb{I}_K$ entonces $ord_v(x_v) = 0$ para casi todo v. Además, es claro que los idèles principales van a parar a P_K, con lo cual tenemos un morfismo $C_K \hookrightarrow Cl(K)$. Se puede ver que dicho morfismo es suryectivo y su núcleo es exactamente

$$\mathbb{I}_{S_\infty} = \prod_{v<\infty} \mathcal{O}_v^\times \times \prod_{v\in S_\infty} K_v^\times,$$

con lo cual, tenemos definido entonces un isomorfismo

$$C_K/\mathbb{I}_{S_\infty} \cong Cl(K)$$

Esta función es probablemente la primera conexión que tenemos entre idèles e ideales. Por otro lado, si restringimos la función a $\mathbb{I}_{\mathfrak{m}}$ obtenemos $id : \mathbb{I}_{\mathfrak{m}} \to I_K(\mathfrak{m})$. Queremos estudiar ahora más sobre esta función. Para eso, vamos a definir para cada lugar v el conjunto

$$W_{\mathfrak{m}}(v) := \begin{cases} \{\alpha \in K_v^\times : \alpha \equiv^\times 1 \pmod{\mathfrak{m}}\} & \text{si} \quad v \mid \mathfrak{m}, \\ \mathcal{U}_v & \text{si} \quad v \nmid \mathfrak{m},\ v < \infty, \\ K_v^\times & \text{si} \quad v \nmid \mathfrak{m},\ v \in S_\infty. \end{cases}$$

Esto es equivalente a definir $W_{\mathfrak{m}}(v)$ como

$$W_{\mathfrak{m}}(v) = \begin{cases} 1 + \widehat{\mathfrak{p}_v}^{n_v} & \text{si} \quad v < \infty, \\ \mathbb{R}_{\geq 0} & \text{si} \quad v \mid \mathfrak{m}, v \text{ es real}, \\ \mathbb{R}^\times & \text{si} \quad v \nmid \mathfrak{m},\ v \text{ es real}, \\ \mathbb{C}^\times & \text{si} \quad v \text{ es complejo}. \end{cases}$$

Es claro entonces que

$$\mathbb{I}_{\mathfrak{m}} = \prod_{v \mid \mathfrak{m}} W_{\mathfrak{m}}(v) \times \prod_{v \nmid \mathfrak{m}}{}' K_v^\times.$$

Definición 6.3.2. Si $\mathfrak{m}$ es un módulo de K, definimos el conjunto

$$W_{\mathfrak{m}} := \prod_v W_{\mathfrak{m}}(v).$$

Proposición 6.3.3. Con la notación usada, vale:

(1) $id : \mathbb{I}_{\mathfrak{m}} \to I_K(\mathfrak{m})$ define un isomorfismo

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

(2) $\mathbb{I}_{\mathfrak{m}} \hookrightarrow \mathbb{I}_K$ define un isomorfismo

$$\mathbb{I}_{\mathfrak{m}} / K_{\mathfrak{m},1} \xrightarrow{\cong} C_K.$$

Demostración:

(1) Por definición de $P_{K,1}(\mathfrak{m})$ se tiene que $\mathbb{I}_{\mathfrak{m}} / K_{\mathfrak{m},1} \hookrightarrow C_{\mathfrak{m}}$ y por definición de $W_{\mathfrak{m}}$ se tiene que éste es el núcleo del morfismo. Luego, como el morfismo es suryectivo, vale el isomorfismo buscado.

(2) Como el núcleo del morfismo $\mathbb{I}_{\mathfrak{m}} \to \mathbb{I}_K / K^\times$ es $\mathbb{I}_{\mathfrak{m}} \cap K^\times = K_{\mathfrak{m},1}$, sólo resta ver que

$$\mathbb{I}_{\mathfrak{m}} / K_{\mathfrak{m},1} \to \mathbb{I}_K / P_K$$

es suryectiva. Sea $x \in \mathbb{I}_K$, y sea $M = \min\{|x_v|_v : v \mid \mathfrak{m}\}$. Sea $\varepsilon > 0$ suficientemente chico para que si $a \in \mathbb{I}_K$ es tal que $|a_v - 1|_v < \varepsilon / M$ para todo $v \mid \mathfrak{m}$ entonces $a \in \mathbb{I}_{\mathfrak{m}}$. Por el Teorema de 4.1.4, existe $\alpha \in K^\times$ tal que $|x_v - \alpha|_v < \varepsilon$ para todo $v \mid \mathfrak{m}$. Entonces $|(\alpha / x_v) - 1|_v < \varepsilon / |x_v|_v \leq \varepsilon / M$, con lo cual $y := \alpha / x$ es un elemento de $\mathbb{I}_{\mathfrak{m}}$; también lo será por lo tanto $1/y$ y se sigue la suryectividad.

Resulta así probada la proposición. □

Usando este pasaje de idèles a ideales, todo grupo radial $C_{\mathfrak{m}}$ se puede ver como cociente del grupo de clases de idèles C_K. Sea

$$\mathbb{I}_{K,S} := \{x \in \mathbb{I}_K : x_v = 1 \ \ \forall v \in S\}.$$

La siguiente proposición nos proporcionará una herramienta fundamental para la conexión entre idèles e ideales.

Proposición 6.3.4. Sea S un conjunto finito de primos de K, G un grupo abeliano finito y $\psi : I_K^S \to G$ un morfismo que admite un módulo $\mathfrak{m}$. Entonces existe un único morfismo $\phi : \mathbb{I}_K \to G$ tal que:

(1) ϕ es continuo al considerar en G la topología discreta,

(2) $\phi(K^\times) = 1$,

(3) $\phi(x) = \psi(id(x)) \quad \forall x \in \mathbb{I}_{K,S(\mathfrak{m})}$.

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.

Demostración: Como ψ se factoriza por $C_{\mathfrak{m}}$, podemos considerarlo como un morfismo $\psi : C_m \to G$. Notemos que en la cadena de morfismos

$$C_K \to \mathbb{I}_{\mathfrak{m}}/K_{\mathfrak{m},1} \to \mathbb{I}_{\mathfrak{m}}/K_{\mathfrak{m},1}W_{\mathfrak{m}} \to C_{\mathfrak{m}}$$

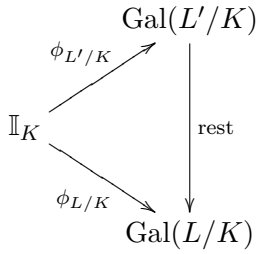
las flechas de los extremos son isomorfismos (por la proposición anterior) y la del medio es suryectiva. Luego, vía esta cadena encontramos un morfismo $\phi : \mathbb{I}_K \to G$ tal que $\phi(K^\times) = 1$. Éste es continuo, pues al anularse en $W_{\mathfrak{m}}$ el núcleo es abierto y cumple (3). La unicidad se sigue de que $K^\times \mathbb{I}_{K,S(\mathfrak{m})}$ es denso en $\mathbb{I}_K$.

Si $\phi : \mathbb{I}_K \to G$ es continuo y $\phi(K^\times) = 1$ entonces el núcleo de ϕ es un subgrupo abierto de $\mathbb{I}_K$. Luego, existe un módulo $\mathfrak{m}$ contenido en el núcleo (propiedad que caracteriza a los subgrupos abiertos de $\mathbb{I}_K$) y entonces $\phi(W_{\mathfrak{m}}) = 1$.

Componiendo con la misma cadena de morfismos de antes obtenemos un morfismo de $C_{\mathfrak{m}}$ en G. Por último, componiendo con la proyección natural conseguimos un morfismo $\psi : I_K(\mathfrak{m}) \to G$ que se factoriza por $C_{\mathfrak{m}}$. Tomando $S = S(\mathfrak{m})$ tenemos lo que buscábamos. □

Luego, por el Teorema 6.2.5, dada un extensión de cuerpos de números L/K finita y abeliana, existe un morfismo $\phi_{L/K} : \mathbb{I}_K \to \mathrm{Gal}(L/K)$ continuo tal que $\phi_{L/K}(K^\times) = 1$ y tal que $\phi_{L/K}(x) = \psi_{L/K}(id(x)) \ \ \forall x \in \mathbb{I}_{K,S}$, donde S es el conjunto de los primos que ramifican. En este caso diremos que **la ley de reciprocidad se cumple** y a $\phi_{L/K}$ también lo llamaremos **mapa de Artin** o mapa de Artin idélico. Notemos que este morfismo sí cumple lo que queríamos, porque ahora si tenemos $K \subset L \subset L'$ una cadena de extensiones finitas abelianas

entonces el siguiente diagrama conmuta:



Pero ahora $\mathbb{I}_K$ no cambia a medida que aumenta L' y por lo tanto tenemos definido un morfismo $\phi_K : \mathbb{I}_K \to \mathrm{Gal}(K^{\mathrm{ab}}/K)$, donde K^{ab} es la clausura abeliana de K, que la podemos tomar como la unión de todas las extensiones finitas abelianas de K dentro de una clausura algebraica fija. Dicho morfismo resulta suryectivo y continuo, considerando en $\mathrm{Gal}(K^{\mathrm{ab}}/K)$ la topología profinita. Más aún, el núcleo de ϕ_K es la componente conexa de la identidad D_K en C_K, de donde se obtiene un isomorfismo canónico

$$C_K/D_K \cong \mathrm{Gal}(K^{\mathrm{ab}}/K).$$

Vimos que $K^\times \subseteq \ker(\phi_{L/K})$ pero ahora nos gustaría saber quién es exactamente el núcleo de $\phi_{L/K}$. Para eso necesitamos una herramienta que sirva de conexión entre los ideales y los idèles. Dicha herramienta será la norma. Ya definimos la norma para idèles e ideales y vimos que en ambos casos se extiende la función norma $N_{L/K} : L^\times \to K^\times$. Más precisamente, tenemos que los diagramas

$$\begin{array}{ccc} L^\times & \xrightarrow{i} & \mathbb{I}_L \\ {\scriptstyle N_{L/K}}\downarrow & & \downarrow{\scriptstyle N_{L/K}} \\ K^\times & \xrightarrow[i]{} & \mathbb{I}_K \end{array} \qquad \begin{array}{ccc} L^\times & \xrightarrow{id} & I_L \\ {\scriptstyle N_{L/K}}\downarrow & & \downarrow{\scriptstyle N_{L/K}} \\ K^\times & \xrightarrow[id]{} & I_K \end{array}$$

conmutan, lo que nos motiva a querer probar el siguiente lema.

Lema 6.3.5. El siguiente diagrama es conmutativo:

$$\begin{array}{ccc} \mathbb{I}_L & \xrightarrow{id} & I_L \\ {\scriptstyle N_{L/K}}\downarrow & & \downarrow{\scriptstyle N_{L/K}} \\ \mathbb{I}_K & \xrightarrow[id]{} & I_K \end{array}$$

Demostración: Sea $x = (x_w) \in \mathbb{I}_L$. Por un lado, $id(x) = \prod_{w<\infty} \mathfrak{p}_w^{ord_w(x_w)}$, con lo cual $N_{L/K}(id(x)) = \prod_{w<\infty} N_{L/K}(\mathfrak{p}_w)^{ord_w(x_w)}$. Si w es finito, $N_{L/K}(\mathfrak{p}_w) = \mathfrak{p}_v^{f(w|v)}$, donde v es el primo debajo de w. Luego, tenemos que

$$N_{L/K}(id(x)) = \prod_{w<\infty} \mathfrak{p}_v^{f(w|v)}\, ord_v(x_w).$$

Por otro lado, si $y = N_{L/K}(x)$ entonces $y_v = \prod_{w|v} N_{L_w/K_v}(x_w)$. Queremos calcular $id(y) = \prod_{v<\infty} \mathfrak{p}_v^{ord_v(y_v)}$. Notemos que

$$ord_v(y_v) = \sum_{w|v} ord_v(N_{L_w/K_v} x_w) \quad \text{y} \quad ord_v(N_{L_w/K_v}(x_w)) = \frac{1}{e(w|v)} ord_w(N_{L_w/K_v}(x_w)),$$

pues $N_{L_w/K_v}(x_w) \in K_v$. Así, obtenemos que

$$ord_v(N_{L_w/K_v}(x_w)) = \frac{1}{e(w|v)} \sum_{\sigma \in \mathrm{Gal}(L_w/K_v)} ord_w(\sigma(x_w)).$$

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

$$ord_w(N_{L_w/K_v}(x_w)) = f(w|v)ord_w(x_w).$$

Luego,

$$id(N_{L/K}(x)) = id(y) = \prod_{v<\infty} \mathfrak{p}_v^{\sum_{w|v} f(w|v)ord_w(x_w)} = \prod_{w<\infty} \mathfrak{p}_w^{f(w|v)ord_w(x_w)} = N_{L/K}(id(x)).$$

Queda así probada la afirmación. □

Corolario 6.3.6. El siguiente diagrama es conmutativo:

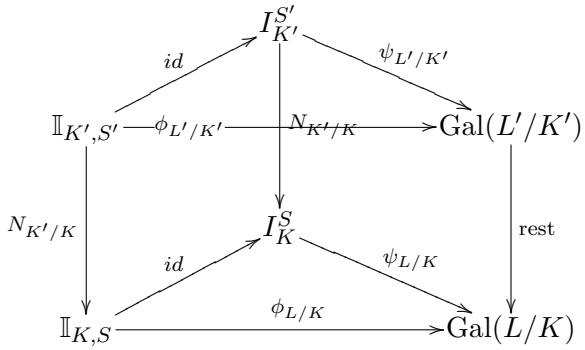
$$\begin{array}{ccc} C_L & \xrightarrow{id} & Cl(L) \\ {\scriptstyle N_{L/K}}\downarrow & & \downarrow{\scriptstyle N_{L/K}} \\ C_K & \xrightarrow[id]{} & Cl(K) \end{array}$$

Demostración: Directo del lema anterior. □

Proposición 6.3.7. Sean L/K y L'/K' extensiones finitas y abelianas, con $K \subseteq K'$, $L \subseteq L'$ finitas. Supongamos que se cumple la ley de reciprocidad para L/K y L'/K'. Entonces el siguiente diagrama es conmutativo:

$$\begin{array}{ccc} \mathbb{I}_{K'} & \xrightarrow{\phi_{L'/K'}} & \mathrm{Gal}(L'/K') \\ {\scriptstyle N_{K'/K}}\downarrow & & \downarrow{\scriptstyle \mathrm{rest}} \\ \mathbb{I}_K & \xrightarrow[\phi_{L/K}]{} & \mathrm{Gal}(L/K) \end{array}$$

Demostración: Sea S un conjunto finito de primos de K suficientemente grande y sea S' el conjunto de primos de K' que están sobre los primos de S. Consideremos el siguiente diagrama:



El paralelogramo de la izquierda conmuta por el Lema 6.3.5 y el de la derecha por el Lema 6.1.3. Los triángulos superior e inferior conmutan por las propiedades del mapa de Artin. Luego, el rectángulo frontal conmuta, y por lo tanto rest $\circ\, \phi_{L'/K'}$ coincide con $\phi_{L/K} \circ N_{K'/K}$ en $\mathbb{I}_{K',S'}$. Como las dos funciones son triviales en $(K')^\times$ por la Proposición 6.3.4, entonces también coinciden en $(K')^\times \mathbb{I}_{K',S'}$, que es denso en $\mathbb{I}_{K'}$ por el Teorema 4.1.4. Luego, como ambas funciones son continuas, coinciden en $\mathbb{I}_{K'}$, que es lo que queríamos ver. □

Corolario 6.3.8. Sea L/K finita abeliana tal que cumple la ley de reciprocidad. Entonces

$$\phi_{L/K}(N_{L/K}(\mathbb{I}_L)) = 1$$

Demostración: Basta tomar $K' = L' = L$ en la proposición anterior. □

Como además dijimos que $\phi_{L/K}(K^\times) = 1$ y $\phi_{L/K}$ es morfismo, entonces

$$\phi_{L/K}(K^\times N_{L/K}(\mathbb{I}_L)) = 1.$$

Reformulando ahora el Teorema 6.2.5 en términos de idèles, obtenemos el siguiente teorema, que nos dice que el núcleo de $\phi_{L/K}$ es exactamente $K^\times N_{L/K}(\mathbb{I}_L)$.

Teorema 6.3.9. El morfismo $\phi_{L/K} : \mathbb{I}_K \to \mathrm{Gal}(L/K)$ es suryectivo y $\ker(\phi_{L/K}) = K^\times N_{L/K}(\mathbb{I}_L)$. Si vemos a $\phi_{L/K}$ como $\phi_{L/K} : C_K \to \mathrm{Gal}(L/K)$ entonces su núcleo es $N_{L/K}(C_L)$.

La primera afirmación nos dice que

$$\mathbb{I}_K / K^\times N_{L/K}(\mathbb{I}_L) \cong \mathrm{Gal}(L/K)$$

y la segunda nos dice que

$$C_K / N_{L/K}(C_L) \cong \mathrm{Gal}(L/K).$$

6.4. Teoría local de cuerpos de clases

Recordemos que para cada lugar v tenemos $i_v : K_v^\times \hookrightarrow \mathbb{I}_K$, $x \mapsto (1, ..., 1, x, 1, ..., 1)$. Definimos $\phi_v : K_v^\times \to \mathrm{Gal}(L/K)$ como $\phi_v := \phi_{L/K} \circ i_v$.

Proposición 6.4.1. Si F es una subextensión de L_v/K_v, entonces

$$\phi_v(N_{F/K_v} F^\times) \subseteq \mathrm{Gal}(L_v/F)$$

(viendo a este último como subgrupo de G).

Demostración: Como $M = L \cap F$ es el cuerpo fijo en L/K del subgrupo de $\mathrm{Gal}(L/K)$ que le corresponde a $\mathrm{Gal}(L^v/F)$ vía la identificación del grupo de Galois local con el grupo de descomposición, entonces $\mathrm{Gal}(L/M)$ se identifica con $\mathrm{Gal}(L^v/F)$. Resulta entonces que $F = M_w$, para algún lugar w de M que esté sobre v. Entonces, considerando el siguiente diagrama

$$\begin{array}{ccc} F = M_w & \xrightarrow{i_w} & \mathbb{I}_M \\ {\scriptstyle N_{F/K_v}}\downarrow & & \downarrow{\scriptstyle N_{M/K}} \\ K_v & \xrightarrow[i_v]{} & \mathbb{I}_K \end{array}$$

y usando la Proposición 6.3.7 con $M = K'$ y $L = L'$ tenemos que

$$\phi_v(N_{F/K_v}F^\times) \subseteq \phi_{L/K}(N_{M/K}\mathbb{I}_M) \subseteq \mathrm{Gal}(L/M),$$

que se identifica con $\mathrm{Gal}(L_v/F)$. □

Corolario 6.4.2. $\phi_v(N_{L^v/K_v}((L^v)^\times)) = 1$.

Demostración: Basta tomar $F = L_v$ en la proposición anterior. □

Dado $x = (x_v) \in \mathbb{I}_K$, entonces

$$x = \lim_S \prod_{v\in S} i_v(x_v),$$

donde el límite se toma sobre los conjuntos finitos de primos S. Luego, como $\phi_{L/K}$ es continuo se tiene que

$$\phi_{L/K}(x) = \lim_S \prod_{v\in S} \phi_v(x_v).$$

Como $\phi_v(x_v) = 1$ para casi todo v, entonces

$$\phi_{L/K}(x) = \prod_v \phi_v(x_v).$$

Llamaremos a ϕ_v el **mapa de Artin local**. Vimos entonces que si conocemos el mapa de Artin (global) podemos determinar para cada v al mapa de Artin local y se puede ver también que vale la recíproca. Es decir que si conocemos el mapa de Artin local para cada v entonces podemos generar el mapa de Artin.

Notemos que definimos el mapa de Artin local a partir del mapa de Artin $\phi_{L/K}$. Como se dijo anteriormente, es común definir en primera instancia el mapa de Artin local para cada lugar y partir de éstos formar el mapa de Artin. Para ver el desarrolo independiente de la teoría local de cuerpos de clases se recomienda [Cas67].

Capítulo 7

Correspondencia de Langlands

7.1. Correspondencia de Langlands en dimensión 1

En la presente sección expondremos el objetivo que fue propuesto al comienzo del trabajo: estudiar la correspondencia de Langlands en dimensión 1. Ésta se compone en primera instancia por la conexión entre los caracteres de Hecke y la representaciones de Artin y en segunda instancia por un caso más general.

7.1.1. Correspondencia entre caracteres de Hecke de orden finito y representaciones de Artin

Supongamos que $\rho : G_K \to \mathbb{C}^\times$ es una representación de Artin abeliana. Sean L/K extensión finita y $\tilde{\rho} : \mathrm{Gal}(L/K) \to \mathbb{C}^\times$ como en el Teorema 2.1.1. Por la Proposición 2.1.5, L/K es abeliana. Luego, por el Teorema 6.2.5, existe $\phi_{L/K} : \mathbb{I}_K \to \mathrm{Gal}(L/K)$ morfismo suryectivo. Entonces podemos definir un morfismo $\chi := \chi_\rho$ como

$$\chi_\rho : \mathbb{I}_K \xrightarrow{\phi_{L/K}} \mathrm{Gal}(L/K) \xrightarrow{\tilde{\rho}} \mathbb{C}^\times,$$

es decir, $\chi = \rho \circ \phi_{L/K}$. Veamos que χ es un caracter de Hecke de orden finito. Por un lado, χ es morfismo, pues $\phi_{L/K}$ y ρ lo son y además, $\chi(K^\times) = \tilde{\rho}(\phi_{L/K}(K^\times)) = \tilde{\rho}(1) = 1$. Por otro lado, χ es de orden finito, pues ρ lo es (por Observación 2.1.2). Entonces, como $\phi_{L/K}$ y $\tilde{\rho}$ son continuas, χ resulta un caracter de Hecke de orden finito.

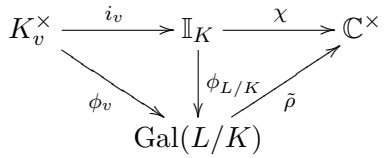
Luego, como χ es un caracter de Hecke entonces para cada lugar v existe un caracter $\chi_v : K_v^\times \to \mathbb{C}^\times$ tal que

$$\chi = \prod_v \chi_v.$$

Cabe preguntarse entonces si es posible determinar quién es χ_v para cada v. Recordemos que χ_v está definido por

$$\chi_v : K_v^\times \xrightarrow{i_v} \mathbb{I}_K \xrightarrow{\chi} \mathbb{C}^\times.$$

Pero como el siguiente diagrama es conmutativo,



entonces $\chi_v = K_v^\times \xrightarrow{\phi_v} \mathrm{Gal}(L/K) \xrightarrow{\tilde{\rho}} \mathbb{C}^\times$ y por lo tanto $\chi = \prod_v (\tilde{\rho} \circ \phi_v)$. Notemos entonces que

$$\begin{aligned}\chi_v(\pi_v) &= \rho(\phi_v(\pi_v)) = \rho(\phi_{L/K}(1, ..., \pi_v, ..., 1)) \\ &= \rho\left(\psi_{L/K}\left(\mathfrak{p}_v^{ord_v(\pi_v)}\right)\right) = \rho(\psi_{L/K}(\mathfrak{p}_v)) \\ &= \rho\left((\mathfrak{p}_v, L/K)\right).\end{aligned}$$

Esto nos dice que, en los primos que no ramifican, χ_v está unívocamente determinado por la imagen $(\mathfrak{p}_v, L/K)$ vía la representación. A su vez, por la fórmula del producto, éstos nos determinan a los caracteres locales que provienen de primos que sí ramifican.

Recíprocamente, dado $\chi : \mathbb{I}_K \to \mathbb{C}^\times$ un caracter de Hecke de orden finito, sabemos que este corresponde a un caracter de Hecke clásico de orden finito $\widetilde{\chi} : I_K(\mathfrak{f}) \to \mathbb{C}^\times$ de conductor $\mathfrak{f}$, tipo-$(\mathcal{O}_K / \mathfrak{f})^\times$ ε y tipo-infinito χ_∞, donde $\mathfrak{f}$ es el conductor de χ que hace que sea primitivo.

Como χ es de orden finito, entonces χ_∞ es de orden finito. Luego, como $(\mathbb{R}_{>0})^{r_1} \times (\mathbb{C}^\times)^{r_2}$ es divisible, razonando análogamente a lo hecho en la Sección 5.3 tenemos que

$$\chi_\infty\left((\mathbb{R}_{>0})^{r_1} \times (\mathbb{C}^\times)^{r_2}\right) = 1.$$

Más aún, si $\{\sigma_i\}_{i=1}^{r_1}$ son los morfismos reales sabemos que cada uno es trivial o es la función signo. Sin pérdida de generalidad, supongamos que $\sigma_i = \mathrm{sgn}$ para todo $1 \leq i \leq m$ y $\sigma_i = 1$ para todo $m+1 \leq i \leq r_1$, para cierto m.

Veamos que si definimos

$$\mathfrak{m}_0 := \mathfrak{f}, \quad \mathfrak{m}_\infty := \prod_{i=1}^{m} v_i \quad \text{y} \quad H := \ker(\widetilde{\chi})$$

(donde $v_i = v_{\sigma_i}$) entonces H resulta un subgrupo de congruencia módulo $\mathfrak{m} := \mathfrak{m}_0\,\mathfrak{m}_\infty$. En efecto, $H < I_K(\mathfrak{f})$, con lo cual resta ver que $P_{K,1}(\mathfrak{m}) \subseteq H$. Dado $(\alpha) \in P_{K,1}(\mathfrak{m})$, sabemos por definición que $\alpha \in K_{\mathfrak{m},1}$. En particular, $\alpha \in K_\mathfrak{f}$ y por lo tanto $\widetilde{\chi}((\alpha)) = \chi_\infty^{-1}(1 \otimes \alpha)$. Como $\alpha \in K_{\mathfrak{m},1}$ entonces $\sigma_i(\alpha) > 0$ si $1 \leq i \leq m$. Luego, si $\{\tau_i, \overline{\tau}_i\}_{i=1}^{r_2}$ son los morfismos complejos,

$$\chi_\infty(1 \otimes \alpha) = \chi_\infty(\sigma_1(\alpha), ..., \sigma_{r_1}(\alpha), \tau_1(\alpha), \overline{\tau}_1(\alpha), ..., \tau_{r_2}(\alpha), \overline{\tau}_{r_2}(\alpha)) = 1,$$

y por lo tanto $(\alpha) \in H$. Así, $P_{K,1}(\mathfrak{m}) \subseteq H$.

Luego, por el Teorema 6.2.6 tenemos que existe una extensión L/K finita y abeliana tal que los morfismos que ramifican son los que dividen a $\mathfrak{m}_\infty$, i.e., son $\sigma_1, ..., \sigma_m$; los primos que ramifican son exactamente los que dividen a $\mathfrak{f}$ y $\mathrm{Gal}(L/K) \cong I_K(\mathfrak{f})/\ker(\widetilde{\chi})$. Definimos entonces

$$\tilde{\rho} : \mathrm{Gal}(L/K) \xrightarrow{\cong} I_K(\mathfrak{f})/\ker(\widetilde{\chi}) \xrightarrow{\widetilde{\chi}} \mathbb{C}^\times$$

y a $\rho_\chi := \tilde{\rho} \circ \mathrm{rest} : G_K \to \mathbb{C}^\times$ que resulta ser una representación de Artin abeliana. Así, tenemos una biyección entre los dos conjuntos:

$$\begin{array}{ccc} \{\text{Representaciones de Artin abelianas}\} & \longleftrightarrow & \{\text{Caracteres de Hecke de orden finito}\} \\ \rho & \longrightarrow & \chi_\rho \\ \rho_\chi & \longleftarrow & \chi \end{array}$$

ESCRIBIR BIEN LA CORRESPONDENCIA: CREO QUE SERIA DE REPRESENTACIONES DE ARTIN ABELIANAS IRREDUCIBLES (Y CUÁNDO USO QUE SEA IRRED?)

7.1.2. Caso general

Notemos que tanto los caracteres de Hecke como las representaciones de Artin de dimensión 1 tienen como espacio de llegada a $\mathbb{C}^\times$. Sabemos que el conjunto de los complejos se obtiene tomando la clausura algebraica de $\mathbb{R}$, que es la completación de $\mathbb{Q}$ en el lugar del infinito. Esto nos dice que si uno reemplaza al lugar del infinito por uno generado por un primo p, debería reemplazar a $\mathbb{C}$ por $\overline{\mathbb{Q}}_p$. Cabe destacar que, a diferencia de $\mathbb{C}$, $\overline{\mathbb{Q}}_p$ no es completo.

Recordemos que cuando introdujimos la noción de representación de Galois, tomábamos un espacio vectorial V sobre un cuerpo topológico k. En el caso de representacion de Artin tomábamos $k = \mathbb{C}$. El Teorema 2.1.1 nos dice que la representaciones de Artin son interesantes pero que si trabajamos con ellas, sólo vamos a obtener información de las extensiones finitas de $\mathbb{Q}$. Es por eso que hay que considerar también representaciones en espacios vectoriales sobre $\overline{\mathbb{Q}}_p$. Eso da lugar a la siguiente definición.

Definición 7.1.1. Una **representación p-ádica** es una representación de Galois con $k = \overline{\mathbb{Q}}_p$.

Al igual que con las representaciones de Artin, nos vamos a concentrar en las representaciones p-ádicas de dimensión 1.

Ejemplo 7.1.2. Para $K = \mathbb{Q}$ y p primo vamos a definir una representanción p-ádica

$$\rho_p : G_{\mathbb{Q}} \to \mathbb{Z}_p^\times \subseteq \overline{\mathbb{Q}}_p^\times.$$

Para cada $n \geq 1$ sea $K_n = \mathbb{Q}(\zeta_{p^n})$, donde ζ_{p^n} es la raíz p^n-ésima primitiva de la unidad. Sabemos que $\mathrm{Gal}(K_n/\mathbb{Q}) \cong (\mathbb{Z}/p^n\mathbb{Z})^\times$. Más aún, el mapa

$$\mathrm{Gal}(K_{n+1}/\mathbb{Q}) \xrightarrow{\text{rest}} \mathrm{Gal}(K_n/\mathbb{Q})$$

está dado por la reducción módulo p^n de $(\mathbb{Z}/p^{n+1}\mathbb{Z})^\times$ a $(\mathbb{Z}/p^n\mathbb{Z})^\times$. Luego, para cada $n \geq 1$ tenemos definido el morfismo

$$\rho_{p,n} : G_{\mathbb{Q}} \xrightarrow{\text{rest}} \mathrm{Gal}(K_n/\mathbb{Q}) \xrightarrow{\cong} (\mathbb{Z}/p^n\mathbb{Z})^\times.$$

Por lo dicho antes, estos morfismos se "pegan" bien, i.e, $\rho_{p,n+1}(\sigma) \equiv \rho_{p,n}(\sigma) \pmod{p^n}$ y por lo tanto mediante ellas podemos construir una representación p-ádica $\rho_p : G_{\mathbb{Q}} \to \mathbb{Z}_p^\times$ dada por

$$\rho_p(\sigma) \equiv \rho_{p,n}(\sigma) \pmod{p^n} \quad \forall n \geq 1.$$

Esta representación se llama **caracter ciclotómico p-ádico** y otra manera equivalente de definirla es la siguiente.

Notemos que dada $\sigma \in G_{\mathbb{Q}}$, $\sigma(\zeta_{p^n})$ es otra raíz p^n-ésima primitiva de la unidad y por lo tanto $\sigma(\zeta_{p^n}) = \zeta_{p^n}^{a_n}$, para algún entero a_n tal que $1 \leq a_n < p^n$ con $(a_n, p) = 1$. Esto nos dice que a_n es una unidad módulo p^n y además

$$\sigma(\zeta_{p^{n-1}}) = \sigma(\zeta_{p^n}^p) = \zeta_{p^n}^{pa_n} = \zeta_{p^{n-1}}^{a_n}.$$

Por lo tanto, $a_n \equiv a_{n-1} \pmod{p^{n-1}}$. Así, podemos definir

$$\rho_p(\sigma) = \varprojlim a_n \in \mathbb{Z}_p^\times.$$

No es sorprendente que definamos como **caracter de Hecke p-ádico** a un morfismo continuo $\chi : \mathbb{I}_K \to \overline{\mathbb{Q}}_p^\times$ tal que $\chi(K^\times) = 1$.

El Ejemplo 7.1.2 nos muestra que existen representaciones p-ádicas que no son de orden finito, aunque sí pueden definirse como límite de caracteres de orden finito. En general, si $\rho : G_K \to \overline{\mathbb{Q}}_p^\times$ es una representanción p-ádica entonces como G_K es compacto, $\mathrm{Im}(\rho)$ está contenida en $\mathcal{O}_F^\times$ para alguna extensión finita $F/\mathbb{Q}_p$ (Ver [Con, Teorema 1]). Como $\mathcal{O}_F^\times$ es profinito, las representanciones p-ádicas son límites de caracteres de orden finito (al igual que antes). Por otro lado, la imagen de caracteres de Hecke p-ádico también está contenida en $\mathcal{O}_F^\times$ para alguna extensión $F/\mathbb{Q}_p$ finita. Luego, al igual que antes tenemos una correspondencia

$$\{\text{Representaciones de Galois } p\text{-ádicas de dimensión } 1\} \longleftrightarrow \{\text{Caracteres de Hecke } p\text{-ádicos}\}$$

Más información se puede ver en [Sno10]. A pesar de que $\overline{\mathbb{Q}}_p$ no es completo, cualquier representación continua cae en una extensión finita, y dichas extensiones sí son finitas, por eso no es preciso trabajar con cuerpos más generales. Lo mismo vale para espacios de dimensión finita sobre $\overline{\mathbb{Q}}_p$.

7.2. Correspondencia de Langlands en dimensión n

La correspondencia antes descripta da una biyección entre representaciones de Galois irreducibles de dimensión 1 (que son abelianas) y ciertas funciones del grupo de idèles. La pregunta natural es qué pasa con representaciones irreducibles de dimensión más grande. El programa de Langlands predice una correspondencia (muy explícita) para cualquier tipo de representaciones. En particular, si miramos una representación $\rho : G_{\mathbb{Q}} \to \mathrm{GL}_n(k)$, donde $k = \mathbb{C}$ o $\overline{\mathbb{Q}}_p$, entonces las mismas están en correspondencia con las llamadas "representaciones automorfas". Éstas, son representaciones irreducibles del grupo $\mathrm{GL}_n(\mathbb{A}_{\mathbb{Q}})$ en espacios vectoriales (complejos) de dimensión infinita, que satisfacen varias propiedades. Una propiedad importante, es que dichas representaciones se obtienen (por medio de un producto restringido) a partir de representaciones de $\mathrm{GL}_n(\mathbb{Q}_v)$ para cada lugar v de $\mathbb{Q}$. La correspondencia de Langlands no sólo dice que ambos mundos están relacionados, sino que da información precisa que caracteriza unívocamente los objetos de un lado con los del otro (en el caso abeliano, el caracter local de Hecke está determinado unívocamente por su valor en el uniformizador local). Así, para dimensiones más grandes, dado un primo p no ramificado de ρ, el polinomio característico de $\rho\left((\mathfrak{p}, \overline{\mathbb{Q}}/\mathbb{Q})\right)$ determina univocamente a la representación de $\mathrm{GL}_n(\mathbb{Q}_{\mathfrak{p}})$ correspondiente (donde $\mathfrak{p}$ es cualquier primo que esté sobre p).

El primer caso no abeliano corresponde a mirar representaciones de dimensión 2, es decir, $\rho : G_{\mathbb{Q}} \to \mathrm{GL}_2(k)$, las cuales corresponden a formas automorfas del grupo GL_2, también llamadas "formas modulares". En el caso en que la representación ρ es "impar" (esto es que la imagen de conjugación compleja tiene determinante -1), dicha correspondencia está demostrada gracias a los trabajos de Wiles, Taylor-Wiles y la demostración de Khare-Wintenberger de las conjeturas de Serre (ver [Wil95], [Wil03] o [Win04]). El caso de representaciones pares, está completamente abierto (y debería corresponder a las llamadas formas de Maass).

Si queremos considerar grupos reductivos G generales (en lugar del grupo GL_n), la conjeturas de Langlands también predicen qué formas automorfas hay que considerar, pero ya las representaciones automorfas no son del grupo $G(\mathbb{A}_{\mathbb{Q}})$, sino del grupo de Langlands asociado

a G (cuyo grupo de Lie subyacente es el grupo dual, obtenido al mirar el dual del retículo de raíces). Esto fue notado ya por Langlands al describir la correspondencia.

Por último, queremos mencionar que podemos reemplazar $\mathbb{C}$ o $\overline{\mathbb{Q}}_p$ por un cuerpo finito $k = \mathbb{F}_q$, y existe una correspondencia de Langlands en este caso también, aunque al día de hoy quedan varios problemas por resolver en dicho caso.

Bibliografía

[Apo76] Tom M. Apostol. *Introduction to analytic number theory.* Springer-Verlag, New York-Heidelberg, 1976. Undergraduate Texts in Mathematics.

[Cas67] A. Cassels, J. & Frölich. *Algebraic Number Theory.* Academic Press Inc. (London) Ltd., 1967.

[Con] K. Conrand. Compact subgroups of $\mathrm{GL}_n(\overline{Q}_p)$. Disponible en `https://kconrad.math.uconn.edu/blurbs/gradnumthy/GLnQpbar.pdf`.

[Cox12] David A. Cox. *Galois theory.* Pure and Applied Mathematics (Hoboken). John Wiley & Sons, Inc, Hoboken, NJ, second edition, 2012.

[Cox13] David A. Cox. *Primes of the form $x^2 + ny^2$.* Pure and Applied Mathematics (Hoboken). John Wiley & Sons, Inc., Hoboken, NJ, second edition, 2013. Fermat, class field theory, and complex multiplication.

[Hec37] E. Hecke. Über modulfunktionen und die dirichletschen reihen mit eulerscher produktentwicklung. i. *Mathematische Annalen*, 1937.

[Jan96] Gerald J. Janusz. *Algebraic number fields*, volume 7 of *Graduate Studies in Mathematics.* American Mathematical Society, Providence, RI, second edition, 1996.

[Kob84] Neal Koblitz. *p-adic numbers, p-adic analysis, and zeta-functions*, volume 58 of *Graduate Texts in Mathematics.* Springer-Verlag, New York, second edition, 1984.

[Lan94] Serge Lang. *Algebraic number theory*, volume 110 of *Graduate Texts in Mathematics.* Springer-Verlag, New York, second edition, 1994.

[Lan02] Serge Lang. *Algebra*, volume 211 of *Graduate Texts in Mathematics.* Springer-Verlag, New York, third edition, 2002.

[Mar77] D. Marcus. *Number Fields.* Graduate Texts in Mathematics. 1977.

[Mas98] Heinrich Maschke. *Ueber den arithmetischen Charakter der Coeffienten der Substitutionen endlicher linearer Substitutionsgruppen.* Math. Ann., 1898.

[Mil13] J.S. Milne. Class field theory (v4.02), 2013. Disponible en `www.jmilne.org/math/`.

[Mil17] J.S. Milne. Algebraic number theory (v3.07), 2017. Disponible en `www.jmilne.org/math/`.

[Mil18] J.S. Milne. Fields and galois theory (v4.60), 2018. Disponible en `www.jmilne.org/math/`.

[Pac18] L. Dieulefait & A. Pacetti. Representaciones de galois, 2018. Disponible en `http://www.famaf.unc.edu.ar/~apacetti/agra3/RepGal.pdf`.

[Sha66] V. I. Borevich & I. R. Shafarevich. *Number Theory.* Academic Press, New York, 1966.

[Shu] J. Shurman. Hecke characters clasically and idèllically. Disponible en `https://people.reed.edu/~jerry/361/lectures/heckechar.pdf`.

[Sno10] Andrew Snowden. Hecke characters and galois characters, 2010. Disponible en `http://virtualmath1.stanford.edu/~conrad/modseminar/pdf/L11.pdf`.

[Wil95] A. Wiles. Modular elliptic curves and fermat's last theorem. *Ann. of Math. (2)*, 1995.

[Wil03] R. Taylor & A. Wiles. Ring-theoretic properties of certain hecke algebras. *Ann. of Math. (2)*, 2003.

[Win04] C. Khare & J.P. Wintenberg. On serre's reciprocity conjecture for 2-dimensional mod p representations of g_q., 2004.

Los abajo firmantes, miembros del Tribunal de Evaluación de tesis, damos Fe que el presente ejemplar impreso, se corresponde con el aprobado por este Tribunal