Trabajo monográfico

Teoría de cuerpo de clases y sus aplicaciones

Pablo Maurente

April 2022

Orientador:

Gonzalo Tornaría

Licenciatura en Matemática
Universidad de la República
Montevideo, Uruguay

Índice general

Introducción

El tema de estudio en esta monografía será teoría de cuerpo de clases, y sus aplicaciones. La teoría de cuerpos de clases es la rama de la teoría de números que estudia las extensiones de cuerpos de números abelianas, el programa de Langlands es su generalización, donde se estudian las extensiones de cuerpos en general. A lo largo de este documento veremos por qué es más fácil estudiar las extensiones abelianas, esto se verá claramente con el teorema de limitación de norma, el cual nos dirá que dado un cuerpo K y una extensión L, sea L^{ab} la mayor extensión abeliana de K dentro de L, entonces $Nm(L) = Nm(L^{ab})$; esto no nos deja diferenciar entre ambas extensiones con las herramientas que presentaremos más adelante.

A lo largo del estudio de la teoría de cuerpo de clases han existido varios enfoques. El primero fue el de Kronecker (comenzando aproximadamente en 1850), su motivación fue estudiar la factorización de polinomios y la densidad de primos, además de conjeturar el Teorema de Kronecker-Weber, el cual dice que, toda extensión abeliana de $\mathbb{Q}$ esta contenida en $Q(\zeta_m)$ con ζ_m una raíz m-ésima de la unidad. Años después Weber daría una prueba de dicho teorema, aunque incompleta, a esto se le debe el nombre. Posteriormente, Hilbert daría una prueba completa de dicho teorema, e introduciría el símbolo de Hilbert, el cual estudiaremos en esta monografía. Todo esto desarrolló la teoría de cuerpo de clases con cuerpos globales, donde un cuerpo global es una extensión finita de $\mathbb{Q}$. Una vez desarrollada la teoría global, se comenzaron a estudiar los cuerpos locales, donde un cuerpo local es un cuerpo completo con respecto a la topología inducida por una valuación discreta y su cuerpo residual es finito, en nuestro caso serán extensiones finitas de $\mathbb{Q}_{\mathfrak{p}}$. Partiendo de la teoría global, Hasse, Brauer y Noether entre otros, desarrollaron la teoría de cuerpo de clases local.

Sin embargo, posterior a este enfoque Tate introduciría la cohomología de Tate para estudiar la teoría de cuerpos local, y deducir la teoría de cuerpos global con la heurística que se empezaba a usar en esa época (1950) de entender los problemas de manera local, estudiándolo en cada completación p-ádica, y utilizando ideles (idea desarrollada por Chevalley en 1936), se desarrolló la teoría de cuerpo de clases global, la esencia de usar los ideles es que se estudia el problema en cada localización del cuerpo (cada completacion con respecto a una norma p-ádica) y en los ideles se puede ver lo anterior, pero en todas las localizaciones a la vez, de ahí sacar conclusiones sobre el cuerpo global, a esto se le llamó principio local-global. Será sobre este segundo enfoque que se tratará este trabajo, recopilando resultados importantes, en algunos casos omitiremos sus demostraciones, y dando algunas aplicaciones de la teoría de cuerpo de clases.

Esta monografía constará de tres capítulos, en el primero introduciremos la cohomología de Tate, para esto necesitaremos algunas definiciones más básicas de álgebra homológica, por tanto, comenzaremos definiendo cohomología y homología de un grupo G, y algunas herramientas que necesitaremos mas adelante como el cup product, los homomorfismos Inflación y Restricción. Una vez tengamos estas herramientas podremos definir la cohomología de Tate, además de enunciar y demostrar el Teorema de Tate, el cual nos facilitara el estudio de la cohomología de Tate, y nos dejará ver como la cohomología de Tate logra unificar de manera útil para nosotros la homología y la cohomología.

Una vez que poseamos estas herramientas, las aplicaremos para estudiar los cuerpos locales y sus extensiones, durante esta sección calcularemos la cohomología de las extensiones ramificadas, y daremos una idea del cálculo de la cohomología para extensiones no ramificadas, para esto construiremos el mapa invariante. Dicho mapa nos dará un isomorfismo entre el segundo grupo de cohomología de K^{un}, que es la extensión no ramificada más grande de K, o sea, el cuerpo que contiene a toda extensión no ramificada de K, con $\mathbb{Q}/\mathbb{Z}$. Además, este mapa nos dará el isomorfismo entre los grupos de cohomología de las extensiones de K, que estarán contenidas en K^{un} y los subgrupos de $\mathbb{Q}/\mathbb{Z}$. Posteriormente, definiremos el mapa local de Artin, el cual nos dirá que $\mathrm{Gal}(L/K)^{ab} \simeq K^{\times}/\mathrm{Nm}_{L/K}(L^{\times})$. Para describir este mapa nos será muy útil haber definido anteriormente el mapa invariante.

En la última sección de este primer capítulo, definiremos el grupo de Brauer e interpretaremos la cohomología en términos del grupo de Brauer. Para esto introduciremos las álgebras centrales simples sobre un cuerpo K y la relación de similaridad que es una relación de equivalencia, una vez tengamos estas definiciones, podemos definir un producto el cual respetara las clases de equivalencia, y el conjunto de clases de similaridad con dicho producto, será el antes mencionado grupo de Brauer. Al final de la sección veremos algunos grupos de Brauer particulares, sobre K finito, $K = \mathbb{R}$ y cuerpos locales no arquimedeanos.

En el capítulo 2 comenzaremos introduciendo el Ray Class Group, para esto necesitaremos la noción de módulo, el cual por ahora pensaremos como un producto de primos o lugares del cuerpo, una vez tengamos esta noción podremos definir el Ray Class Group. Además, daremos algunos ejemplos de este grupo utilizando extensiones cuadráticas. Posteriormente, definiremos el elemento de Frobenius, el cual será el generador del grupo de descomposición, dada una extensión L de K definiremos el grupo de descomposición $D(\mathfrak{B}) = \{\tau \in G \mid \tau\mathfrak{B} = \mathfrak{B}\}$ donde $\mathfrak{B}$ es un ideal en L sobre un ideal primo $\mathfrak{p}$ en el cuerpo K.

Una vez tengamos estas definiciones, definiremos el mapa global de Artin, el cual será la versión global del mapa local de Artin definido en el capítulo anterior. Calcularemos el mapa global de Artin en algunos cuerpos particulares para fijar ideas sobre su funcionamiento. Ahora nos interesaría obtener un isomorfismo del mismo tipo que nos daba el mapa local de Artin, sin embargo, el mapa global de Artin no es un isomorfismo. Para eso enunciaremos la Ley de reciprocidad, la cual nos dará un isomorfismo entre $\mathrm{Gal}(L/K)$ y $I^{S(\mathfrak{m})}/i(K_{\mathfrak{m},1}).\mathrm{Nm}(I_L^{S(\mathfrak{m})})$, donde $S(\mathfrak{m})$ es el conjunto de ideales primos que dividen al módulo $\mathfrak{m}$, y el mapa i es $i(a) = (a)$, manda un elemento en el ideal generado por ese elemento. Este será el primer teorema que enunciaremos de CFT global,

en esta misma sección enunciaremos el teorema de limitación de norma el cual ya fue mencionado anteriormente.

En este punto nos interesaría combinar la parte local y la global. Para eso introduciremos los ideles, estos fueron introducidos por Chevalley, el grupo de ideles de K es $\{(x_v)_v \mid x_v \in K_v \text{ y } x_v \in \mathcal{O}_v \text{ para casi todo } v\}$ donde v son los lugares o primos de K. De manera intuitiva estamos mirando todos los lugares de k a la vez. Lo que haremos será entender los teoremas que ya vimos en términos de ideales en el lenguaje de los ideles, y ver que tanto se pueden generalizar estos teoremas, es decir, ver cuál es la ventaja de usar ideles.

En el capítulo 3 culminaremos la monografía viendo algunas aplicaciones de CFT. Estudiaremos 3 problemas, el primero será cuando una n-ésima potencia local es global. Veremos que dado un cuerpo de números que contiene una n-ésima raíz de la unidad. Un elemento no nulo de K es una n-ésima potencia en K, si es una n-ésima potencia en K_v para casi todo v primo. Para probar este teorema necesitaremos algunos resultados de teoría de números analítica, los cuales enunciaremos sin demostración. Otro de los problemas que estudiaremos será el principio local-global de normas, para esto tendremos el Teorema de la norma de Hasse. Dada una extensión cíclica L/K de un cuerpo de números y sea $a \in K^*$, entonces la imagen de $a \in K_v$ es una norma de L_v para casi todo v, y si es una norma para todo v, entonces es una norma en K.

Finalizaremos el capítulo y la monografía estudiando leyes de reciprocidad, para esto introduciremos el símbolo de Legendre y veremos la ley de reciprocidad cuadrática como primera aproximación al problema. Posteriormente, generalizaremos el símbolo de Legendre, dando el símbolo de potencia residual. Definiremos el símbolo de Hilbert, para esto nos será útil el mapa invariante definido anteriormente. Una vez que tengamos esto, podremos usar el símbolo de Hilbert y alguna de sus propiedades para demostrar la ley de reciprocidad. Por ultimo, veremos la reciprocidad cúbica de Eisenstein, y algunas aplicaciones de estos resultados, entre las cuales estará una demostración del Teorema de Fermat para primos menores que 3×10^9.

Capítulo 1

Teoría de cuerpo de clases local

1. Cohomología de Tate

Esta sección será puramente preliminar dando resultados que necesitaremos más adelante, daremos algunos preliminares básicos sobre cohomología para poder definir la cohomología de Tate, comenzaremos definiendo qué es la cohomología y la homología de un G-módulo, siendo G un grupo.

1.1. Definición de cohomología de grupos.

Definición 1.1. Diremos que M es un $G-$modulo si M es un grupo abeliano y G actúa sobre M de manera tal que

1. $g(m+n) = gm + gn \; \forall m, n \in M$ y $g \in G$
2. $g'g(m) = g'(gm) \; \forall m \in M$ y $\forall g, g'$
3. $1m = m \; \forall m \in M$

Definición 1.2. Para un G-módulo M, definimos

$$M^G = \{m \in M \mid gm = m \; \forall g \in G\}.$$

El functor $M \mapsto M^G : \mathrm{Mod}_G \to Ab$ es exacto a izquierda, i.e., si $0 \to M' \to M \to M'' \to 0$ es exacta, entonces $0 \to M'^G \to M^G \to M''^G$ es exacta.

Dado que la categoría de los G-módulos tiene suficientes inyectivos, podemos aplicar la teoría de los functores derivados en esta situación. Una resolución inyectiva de un G-módulo M es una sucesión exacta de la forma $0 \to M \to I^0 \to I^1 \to \cdots$, donde los I^j son todos inyectivos. Remitirse a [**Mil20**, Capitulo 2] por mas detalles.

Sea M un G-módulo, elegimos una resolución inyectiva

$$0 \to M \to I^0 \to I^1 \to I^2 \to \cdots$$

de M. El complejo

$$0 \xrightarrow{d^{-1}} \left(I^0\right)^G \xrightarrow{d^0} \left(I^1\right)^G \to \cdots \xrightarrow{d^{r-1}} \left(I^r\right)^G \xrightarrow{d^r} \left(I^{r+1}\right)^G \to \cdots$$

no necesariamente es exacto, lo cual da lugar a la siguiente definición.

Definición 1.3. Definiremos el r-ésimo grupo de cohomología de G con coeficientes en M como

$$H^r(G, M) = \frac{\mathrm{Ker}\,(d^r)}{\mathrm{Im}\,(d^{r-1})}.$$

Proposición 1.4. *Se cumplen las siguientes propiedades*

1. $H^0(G, M) = M^G$

2. *Dada una sucesión exacta corta de G-módulos*

$$0 \to M' \to M \to M'' \to 0$$

da lugar a una sucesión exacta larga

$$0 \to H^0\left(G, M'\right) \to \cdots \to H^r(G, M) \to H^r\left(G, M''\right) \overset{\delta^r}{\to} H^{r+1}\left(G, M'\right) \to \cdots .$$

Descripción de la Cohomología de grupos por medio de cocadenas.

DEFINICIÓN 1.5. Llamaremos una $r-$cocadena homogénea a una función $\varphi : G^{r+1} \to M$ tal que cumpla lo siguiente

$$\varphi(gg_0, ..., gg_r) = g(\varphi(g_0, ..., g_r)) \; \forall g, g_0, ..., g_r \in G.$$

Notaremos al conjunto de las $r-$cocadenas homogéneas como $\tilde{C}^r(G, M)$. Definimos el mapa borde $\tilde{d}^r : \tilde{C}^r(G, M) \to \tilde{C}^{r+1}(G, M)$ de la siguiente manera

$$(\tilde{d}^r\varphi)(g_0, ..., g_{r+1}) = \sum (-1)^i \varphi(g_0, ..., \widehat{g_i}, ..., g_{r+1}).$$

Esta cadena nos da una manera explicita de calcular el $r-$ésimo grupo de cohomología como

$$H^r(G, M) \simeq \frac{Ker(\tilde{d}^r)}{Im(\tilde{d}^{r-1})}.$$

Una cocadena homogénea $\varphi : G^{r+1} \to M$ es determinada por sus valores en los elementos $(1, g_1, g_1g_2, ..., g_1...g_r)$. Por tanto definimos el grupo $C^r(G, M)$ de r-cocadenas no homogéneas de G con valores en M, el cual consiste de todas las funciones $\varphi : G^r \to M$. Tomaremos $G^0 = \{1\}$, por lo tanto $C^0(G, M) = M$. Definimos

$$d^r : C^r(G, M) \to C^{r+1}(G, M)$$

por $(d^r\varphi)(g_1, \cdots, g_{r+1}) =$

$$g_1\varphi(g_2, ..., g_{r+1}) + \sum_{j=1}^{r} (-1)^j \varphi(g_1, ..., g_jg_{j+1}, ..., g_{r+1}) + (-1)^{r+1}\varphi(g_1, ..., g_r).$$

Definimos

$$Z^r(G, M) = Ker(d^r) \textbf{ grupo de r-cociclos}$$
$$B^r(G, M) = Im(d^{r-1}) \textbf{ grupo de r-cobordes (r-coboundaries)}$$

Podemos describir el $r-$ésimo grupo de cohomología como

$$H^r(G, M) \simeq \frac{Z^r(G, M)}{B^r(G, M)}.$$

Las tres maneras en las que definimos cohomología son isomorfas, dependiendo del contexto en el cual estemos trabajando en el futuro usaremos la definición mas útil.

A continuación daremos una descripción del mapa borde δ^r usando cocadenas. Sea $0 \to M \to N \to P \to 0$ una sucesión exacta de G-módulos. El mapa borde

$$\delta^r : H^r(G, P) \to H^{r+1}(G, M)$$

tiene la siguiente descripción: sea $\gamma \in H^r(G, P)$ representado por el r-cociclo $\phi : G^r \to P$. El mapa de N en P es sobre, por tanto, existe una r-cocadena $\tilde{\phi} : G^r \to N$ que levanta a ϕ, como $d\phi = 0$, $d\tilde{\phi}$ toma valores en M, este es el cociclo que representa a $\delta^r\gamma$.

Calculando una cohomología importante.
Sea L una extensión de Galois finita de K, y sea $G = \mathrm{Gal}(L/K)$. Entonces L y $L^\times$ son G-módulos.

PROPOSICIÓN 1.6. *Sea L/K una extensión de Galois finita con grupo de Galois G. Entonces $H^1(G, L^\times) = 0$*

DEMOSTRACIÓN. Sea $\varphi : G \to L^\times$ un $1-$cociclo, por tanto,

$$\varphi(\sigma\tau) = \sigma(\varphi(\tau)).\varphi(\sigma),\ \forall \sigma, \tau \in G$$

usando la independencia lineal de los automorfismos de L, se tiene que existe $x \in L^\times$ tal que

$$0 \neq y = \sum_{\sigma \in G} \varphi(\sigma).\sigma(x).$$

Luego para $\theta \in G$

$$\theta(y) = \sum_{\sigma \in G} (\theta\varphi)(\sigma)(\theta\sigma)(x) = \sum_{\sigma \in G} \varphi(\theta\sigma)\varphi(\theta)^{-1}(\theta\sigma)(x) = \varphi(\theta)^{-1}y$$

por lo tanto, φ satisface $\varphi(\theta) = \theta(y)^{-1}y$, o sea que φ es un $1-$coborde. Probando que $Z^1(G, L^\times) \simeq B^1(G, L^\times)$ □

Algunos homomorfismos importantes.
Definimos $Ind_H^G(M) = \{\varphi : G \to M \mid \varphi(hg) = h\varphi(g) \forall h \in H\ \forall g \in G\}$. $Ind_H^G(M)$ tiene estructura de G-módulo con $(\varphi + \varphi')(x) = \varphi(x) + \varphi'(x)$ y $g\varphi(x) = \varphi(xg)$. Ahora enunciaremos el lema de Shapiro.

LEMA 1.7. *(Shapiro) Sea G un grupo y H un subgrupo de G, $\forall M$ H-módulo, existe un isomorfismo canónico $H^r(G, Ind_H^G(M)) \xrightarrow{\simeq} H^r(H, M)\ \forall r \leq 0$.*

DEMOSTRACIÓN. Ver Proposición 1.11 de [**Mil20**]. □

El **homomorfismo Restricción** se construirá de la siguiente manera. Sea $M \to Ind_H^G(M)$ el homomorfismo de G-módulos que envía m al mapa $g \mapsto gm$. Esto induce el homomorfismo

$$H^r(G, M) \to H^r(G, Ind_H^G(M)),$$

por el lema de Shapiro tenemos un isomorfismo de $H^r(G, Ind_H^G(M)) \xrightarrow{\simeq} H^r(H, M)$ definiremos el homomorfismo Restricción como la composición de los dos homomorfismos anteriores

$$Res : H^r(G, M) \to H^r(H, M).$$

Una manera explicita de construir el homomorfismo Restricción es la siguiente. Sea $\phi \in H^r(G, M)$, y sea φ una $r-$cocadena de G que toma valores en M, tal que representa a ϕ, podemos restringir φ a H^r, esto nos da una $r-$cocadena de H que toma valores en M, la cual representa la clase de $Res(\phi)$

El **homomorfismo Inflación**. Sea H un subgrupo normal de G, sea $\alpha : G \to G/H$ la proyección, y sea $\beta : M^H \hookrightarrow M$. Sea $\phi \in H^r(G/H, M^H)$ representado por φ un $r-$cociclo de de G/H que toma valores en M^H, φ es fijado por la acción de H ya

que $M^H = \{m \in M : h(m) = m \forall h \in H\}$. Sea $\tilde{\varphi}$ un levantado de φ en G tal que $\tilde{\varphi}(g) = \varphi(gH)$, por tanto, $h\tilde{\varphi}(g) = \tilde{\varphi}(g)$. Definimos

$$Inf : H^r(G/H, M^H) \to H^r(G, M) \text{ como } Inf(\phi) = \overline{\beta(\tilde{\varphi})}$$

donde $\overline{\beta(\tilde{\varphi})}$ es la clase de $\beta(\tilde{\varphi})$ en $H^r(G, M)$.

El **homomorfismo Corestricción**. Sea H un subgrupo de G de índice finito y sea S un conjunto de representantes de las coclases a izquierda de H. Entonces $G = \bigcup_{s\in S} sH$. Dado M un G-módulo, definimos la función norma de la siguiente manera

$$Nm_{G/H}m = \sum_{s\in S} sm.$$

$Nm_{G/H}$ es un homomorfismo de $M^H \to M^G$, esto nos da un homomorfismo de los grupos de cohomología

$$Cor : H^r(H, M) \to H^r(G, M)$$

para todo r de la siguiente manera. Para todo G-modúlo M tomamos

$$\varphi \mapsto \sum_{s\in S} s\varphi(s^{-1}) : Ind_H^G(M) \to M.$$

Componiendo con el isomorfismo del lema de Shapiro obtenemos el homomorfismo corestricción

$$H^r(H, M) \xrightarrow{\simeq} H^r(G, Ind_H^G(M)) \to H^r(G, M).$$

1.2. Cup Product. Para dos G-módulos M y N, escribimos $M \otimes N$ para $M \otimes_{\mathbb{Z}} N$ como G-módulo con

$$g(m \otimes n) = gm \otimes gn,\ g \in G,\ m \in M,\ n \in N.$$

Proposición 1.8. *Existe una y solo una familia de apareamientos bi-aditivos*

$$(m, n) \mapsto m \cup n : H^r(G, M) \times H^s(G, N) \to H^{r+s}(G, M \otimes N)$$

tal que

1. *para r=s=0, el apareamiento es*
$$(m, n) \to m \otimes n : M^G \otimes N^G \to (M \otimes N)^G;$$
2. *Si* $0 \to M' \to M \to M'' \to 0$ *es una sucesión exacta de G-módulos tal que*
$$0 \to M' \otimes N \to M \otimes N \to M'' \otimes N \to 0$$
es exacta, entonces
$$(\delta m'') \cup n = \delta(m'' \cup n), m'' \in H^r(G, M''), n \in H^s(G, N);$$
Donde δ *es el homomorfismo* $H^r(G, M'') \to H^{r+1}(G, M')$ *o* $H^{r+s}(G, M'' \otimes N) \to H^{r+s+1}(G, M' \otimes N)$
3. *Si* $0 \to N' \to N \to N'' \to 0$ *es una sucesión exacta de G-módulos tal que*
$$0 \to M' \otimes N \to M \otimes N \to M'' \otimes N \to 0$$
es exacta, entonces
$$m \cup \delta n'' = (-1)^r \delta(m \cup n''), m \in H^r(G, M), n'' \in H^s(G, N'').$$

Proposición 1.9. *El producto cup cumple las siguientes propiedades*

- $(x \cup y) \cup z = x \cup (y \cup z)$
- $x \cup y = (-1)^{rs} y \cup x$
- $Res(x \cup y) = Res(x) \cup Res(y)$
- $Cor(x \cup Res(y)) = Cor(x) \cup y$
- $Inf(x \cup y) = Inf(x) \cup Inf(y)$

1.3. Definición de homología de grupos. Dado un G-módulo M, sea M_G el cociente mas grande de M sobre el que G actúa trivialmente. Por tanto M_G es el cociente de M por el subgrupo generado por

$$\{gm - m \mid g \in G, m \in M\}.$$

El functor

$$M \mapsto M_G : \mathbf{Mod}_G \to \mathbf{Ab}$$

es exacto a derecha, es decir, si

$$0 \to M' \to M \to M'' \to 0$$

es exacto, entonces

$$M'_G \to M_G \to M''_G \to 0$$

es exacto.

Sea M un G-módulo, elegimos una resolución proyectiva, podemos hacerlo pues la categoría de $G-$módulos tiene suficientes proyectivos

$$\cdots \longrightarrow P_2 \longrightarrow P_1 \longrightarrow P_0 \longrightarrow M \longrightarrow 0$$

de M. El complejo

$$\cdots \longrightarrow (P_2)_G \xrightarrow{d_2} (P_1)_G \xrightarrow{d_1} (P_0)_G \longrightarrow 0$$

no necesariamente es exacto, por tanto definimos

$$H_r(G, M) = \frac{\operatorname{Ker}(d_r)}{\operatorname{Im}(d_{r+1})}$$

como el r-ésimo grupo de Homología de G con coeficientes en M.

Proposición 1.10. *Se cumplen las siguientes propiedades*

1. $H_0(G, M) = M_G$;
2. *Una sucesión exacta corta de G-módulos*

$$0 \to M' \to M \to M'' \to 0$$

da lugar a una sucesión exacta larga

$$\cdots \to H_r(G, M) \to H_r\left(G, M''\right) \xrightarrow{\delta_r} H_{r-1}\left(G, M'\right) \to \cdots \to H_0\left(G, M''\right) \to 0.$$

1.4. Cohomología de Tate. Supongamos que G es un grupo finito.

Para un G-módulo, definimos el mapa norma $\mathrm{Nm}_G : M \to M$ de la siguiente manera

$$m \mapsto \sum_{g \in G} gm.$$

Sea $g' \in G$. Como g recorre todos los elementos de G, $g'(Nm_G(m)) = Nm_G(m) = Nm_G(g'm)$. Entonces

$$\mathrm{Im}\,(\mathrm{Nm}_G) \subset M^G, \quad I_G M \subset \mathrm{Ker}\,\mathrm{Nm}_G.$$

Donde I_G es el ideal de aumentación, $I_G = ker(\sum_{\sigma \in G} n_\sigma \sigma \mapsto \sum_{\sigma \in G} n_\sigma)$, este ideal (de $\mathbb{Z}[G]$) es generado por $\{\sigma - 1 : \sigma \in G\}$.

Por tanto, obtenemos el siguiente diagrama conmutativo

$$\begin{array}{ccccccccc} & & & & M & \xrightarrow{Nm_G} & M & & \\ & & & & \downarrow & & \uparrow & & \\ 0 & \longrightarrow & Ker(Nm_G)/I_G M & \longrightarrow & M/I_G M & \longrightarrow & M^G & \longrightarrow & M^G/Nm_G(M) \longrightarrow 0 \end{array}$$

Como $H_0(G, M) = M/I_G M$ y $H^0(G, M) = M^G$, la fila inferior puede ser reescrita como

$$0 \to \mathrm{Ker}\,(\mathrm{Nm}_G)\,/I_G M \to H_0(G, M) \xrightarrow{\mathrm{Nm}_G} H^0(G, M) \to M^G/\mathrm{Nm}_G(M) \to 0$$

Definición 1.11. Tate definió

$$H_T^r(G, M) = \begin{cases} H^r(G, M) & r > 0 \\ M^G/Nm_G(M) & r = 0 \\ Ker(Nm_G)/I_G M & r = -1 \\ H_{-r-1}(G, M) & r < -1 \end{cases}$$

por tanto la sucesión exacta ahora se convierte en

$$0 \to H_T^{-1}(G, M) \to H_0(G, M) \xrightarrow{\mathrm{Nm}_G} H^0(G, M) \to H_T^0(G, M) \to 0.$$

Los grupos $H_T^r(G, M)$ son conocidos como grupos de Cohomología de Tate.

Proposición 1.12. *Dada una sucesión exacta corta de G-módulos*

$$0 \to M' \to M \to M'' \to 0.$$

Obtenemos la siguiente sucesión exacta larga

$$\cdots \to H_T^r(G, M') \to H_T^r(G, M) \to H_T^r(G, M'') \xrightarrow{\delta} H_T^{r+1}(G, M) \to \cdots .$$

Dos resultados importantes.

TEOREMA 1.13. *Sea G un grupo finito, y sea M un G-módulo. Si*

$$H^1(H, M) = 0 = H^2(H, M)$$

para todo subgrupo H de G, entonces $H_T^r(G, M) = 0$ para todo $r \in \mathbb{Z}$

DEMOSTRACIÓN. Ver Teorema 3.10 de [**Mil20**]. □

TEOREMA 1.14. *Teorema de Tate*
Sea G un grupo finito y sea C un G-módulo. Supongamos que para todo subgrupo H de G (incluyendo H=G)

1. $H^1(H, C) = 0$
2. $H^2(H, C)$ *es un grupo cíclico de orden igual a* $|H|$

Entonces, para todo r, existe un isomorfismo

$$H_T^r(G, \mathbb{Z}) \to H_T^{r+2}(G, C)$$

dependiendo solo de la elección del un generador para $H^2(G, C)$

DEMOSTRACIÓN. Ver Teorema 3.11 de [**Mil20**]. □

2. Teoría de cuerpos de clases local

Sea K un cuerpo local, es decir que K es un cuerpo local si es un cuerpo y además es completo con la topología inducida por una valuación discreta y su cuerpo residual es finito. En nuestro caso, los cuerpos locales que utilizaremos siempre serán una completación de un cuerpo de números con respecto a normas p-ádicas. De ahora en adelante llamaremos $H^2(L/K)$ a $H^2(\mathrm{Gal}(L/K), L^\times)$. En la siguiente sección veremos una interpretación de $H^2(L/K)$ como el grupo de Brauer de L/K.

2.1. Cohomología de extensiones no ramificadas. En el inicio de esta sección describiremos la cohomología de las extensiones no ramificadas, las cuales son mas fáciles de estudiar que las ramificadas. Para esto estudiaremos la cohomología de las unidades, la cual nos sera útil para entender la cohomología de L.
La cohomología de las unidades.

PROPOSICIÓN 2.1. *Sea L/K una extensión finita no ramificada con grupo de Galois G, y sea U_L el grupo de unidades en L. Entonces*

$$H_T^r(G, U_L) = 0 \text{ para todo } r$$

DEMOSTRACIÓN. Si π es un primo de L, entonces todo elemento de $L^\times$ puede ser escrito únicamente como $\alpha = u\pi^m$ con $u \in U_L, m \in \mathbb{Z}$. Por tanto

$$L^\times = U_L.\pi^{\mathbb{Z}} \simeq U_L \times \mathbb{Z}$$

Como L es no ramificada sobre K, podemos elegir $\pi \in K$, entonces $\tau(\alpha) = \tau(u\pi^m) = (\tau u)\pi^m$ para todo $\tau \in G$, y por tanto 2.1 se convierte en una descomposición de G-módulos cuando tenemos G actuando trivialmente sobre $\pi^{\mathbb{Z}} \simeq \mathbb{Z}$. Por tanto $H^r(G, U_L)$ es un sumando de $H^r(G, L^\times)$.

Tenemos que $H^1(G, L^\times) = 0$ por el Teorema 90 de Hilbert. Como G es cíclico, para completar la prueba de la proposición, es suficiente ver que $H^0_T(G, U_L) = 0$. Para eso usaremos la siguiente proposición. □

PROPOSICIÓN 2.2. *Sea L/K extensión finita no ramificada. Entonces el mapa norma $Nm_{L/K} : U_L \to U_K$ es sobreyectivo.*

Necesitaremos los siguientes lemas para demostrar la proposición. Sean l y k los cuerpos residuales de L y K. Como L/K es no ramificada, la acción de G sobre O_L define un isomorfismo $G \simeq \mathrm{Gal}(l/k)$.

LEMA 2.3. *Para $m > 0$, sea $U_L^{(m)} = 1 + \mathrm{m}_L^m$. Entonces*

$$U_L/U_L^{(1)} \xrightarrow{\simeq} l^\times$$
$$U_L^{(m)}/U_L^{(m+1)} \xrightarrow{\simeq} l$$

como G-módulos.

DEMOSTRACIÓN. Sea π un primo de K, por tanto es primo en L, y $U_L^{(m)} = \{1 + a\pi^m \mid a \in O_L\}$
Los mapas

$$u \mapsto u \bmod m_L : U_L \to l^\times$$
$$1 + a\pi^m \mapsto a \bmod m_L : U_L^{(m)} \to l$$

inducen los isomorfismos requeridos. □

LEMA 2.4. *Para todo r, $H^r_T(G, l^\times) = 0$. En particular, el mapa norma $l^\times \to k^\times$ es sobreyectivo.*

DEMOSTRACIÓN. Mirar Lema 1.4 del capitulo 3 de [**Mil20**] □

LEMA 2.5. *El grupo $H^r_T(G, l) = 0$ para todo r. En particular, el mapa traza $l \to k$ es sobreyectivo.*

DEMOSTRACIÓN. Mirar Lema 1.5 del capitulo 3 de [**Mil20**] □

Utilizaremos los lemas anteriores sin dar las pruebas.

DEMOSTRACIÓN DE LA PROPOSICIÓN 2.2. Ahora demostraremos la proposición anterior utilizando los lemas. Tenemos los siguientes diagramas conmutativos

$$\begin{array}{ccc} U_L & \longrightarrow & l^\times \\ \downarrow{\scriptstyle Nm} & & \downarrow{\scriptstyle Nm} \\ U_K & \longrightarrow & k^\times \end{array} \qquad \begin{array}{ccc} U_L^{(m)} & \longrightarrow & l \\ \downarrow{\scriptstyle Nm} & & \downarrow{\scriptstyle Tr} \\ U_K^{(m)} & \longrightarrow & k \end{array}$$

Consideremos un $u \in U_K$. Como el mapa Norma $l^\times \to k^\times$ es sobreyectivo, existe un $v_0 \in U_L$ tal que $Nm(v_0)$ y u tiene la misma imagen en $k^\times$, lo que es igual a que $u/Nm(v_0) \in U_K^{(1)}$. Como el mapa Traza de $l \to k$ es sobreyectivo, existe un $v_1 \in U_L^{(1)}$ tal que $Nm(v_1) \equiv u/Nm(v_0) \bmod U_K^{(2)}$. Continuando con este razonamiento, obtenemos una sucesión de $v_0, v_1, v_2, ..., v_i \in U_L^{(i)}$, tal que $u/Nm(\prod_{j=0}^i v_j) \in U_K^{(i+1)}$. Sea $v = lim_{m\to\infty} \prod_{j=0}^m v_j$. Entonces $u/Nm(v) \in \bigcap U_K^{(i)} = 1$. □

El mapa invariante.
Sea L una extensión de K no ramificada, y $G = \mathrm{Gal}(L/K)$.

Como $H^2(G, U_L) = 0 = H^3(G, U_L)$, la sucesión de cohomología de la sucesión exacta corta

$$0 \longrightarrow U_L \longrightarrow L^\times \xrightarrow{ord_L} \mathbb{Z} \longrightarrow 0$$

nos da el siguiente isomorfismo

$$H^2(G, L^\times) \xrightarrow[\simeq]{H^2(ord_L)} H^2(G, \mathbb{Z}).$$

Los grupos $H^r(G, \mathbb{Q})$ son de torsión para $r > 0$ y únicamente divisible porque $\mathbb{Q}$ lo es, y por tanto son triviales. Por tanto la sucesión de cohomología de la sucesión exacta corta

$$0 \longrightarrow \mathbb{Z} \longrightarrow \mathbb{Q} \longrightarrow \mathbb{Q}/\mathbb{Z} \longrightarrow 0$$

nos da un isomorfismo (G actuando trivialmente)

$$H^1(G, \mathbb{Q}/\mathbb{Z}) \xrightarrow{\delta} H^2(G, \mathbb{Z}) \ .$$

Sabiendo que

$$H^1(G, \mathbb{Q}/\mathbb{Z}) \simeq \mathrm{Hom}_{cts}(G, \mathbb{Q}/\mathbb{Z})$$

y que G tiene un generador topológico canónico, el elemento de Frobenius $\sigma = Frob_{L/K}$. La composición de

$$H^2(L/K) \xrightarrow{ord_L} H^2(G, \mathbb{Z}) \xleftarrow[\delta]{} H^1(G, \mathbb{Q}/\mathbb{Z}) \simeq \mathrm{Hom}_{cts}(G, \mathbb{Q}/\mathbb{Z}) \xrightarrow{f \mapsto f(\sigma)} \mathbb{Q}/\mathbb{Z}$$

es llamado el **mapa invariante**

$$inv_{L/K} : H^2(L/K) \to \mathbb{Q}/\mathbb{Z}$$

Teorema 2.6. *Existe un único isomorfismo*

$$inv_K : H^2(K^{un}/K) \to \mathbb{Q}/\mathbb{Z}$$

con la propiedad tal que para toda extensión $L \subset K$ de grado n sobre K, inv_K induce el isomorfismo

$$inv_{L/K} : H^2(L/K) \to \frac{1}{[L:K]}\mathbb{Z}/\mathbb{Z}$$

La prueba del teorema es una consecuencia de la discusión anterior.

Proposición 2.7. *Sea L una extensión finita de K de grado n, y sean K^{un} y L^{un} las extensiones mas grandes no ramificadas de K y L. Entonces el siguiente diagrama conmuta*

$$\begin{array}{ccc} H^2(K^{un}/K) & \xrightarrow{Res} & H^2(L^{un}/L) \\ \downarrow{\scriptstyle inv_K} & & \downarrow{\scriptstyle inv_L} \\ \mathbb{Q}/\mathbb{Z} & \xrightarrow{\quad n \quad} & \mathbb{Q}/\mathbb{Z} \end{array}$$

Demostración. La extensión no ramificada mas grande es un cuerpo local obtenido por adjuntar todas las m-esimas raíz de la unidad para m no divisible por la característica del cuerpo residual.Por tanto, $L^{un} = L.K^{un}$ y por tanto el mapa

$$\tau \mapsto \tau \mid K^{un} : \mathrm{Gal}(L^{un}/L) \to \mathrm{Gal}(K^{un}/K)$$

es inyectivo. El mapa Res en el diagrama anterior es definido por la compatibilidad de los homomorfismos

$$\mathrm{Gal}(K^{un}) \leftarrow \mathrm{Gal}(L^{un}/L)$$

$$K^{un\times} \to L^{un\times}$$

Sea $\Gamma_K = \mathrm{Gal}(K^{un}/K)$ y $\Gamma_L = \mathrm{Gal}(L^{un}/L)$, y consideramos el siguiente diagrama

$$\begin{array}{ccccc} H^2(K^{un}/K) & \xrightarrow{ord_K} & H^2(\Gamma_K,\mathbb{Z}) & \xleftarrow[\delta]{} & H^1(\Gamma_K,\mathbb{Q}/\mathbb{Z}) \xrightarrow{g\mapsto g(\sigma_K)} \mathbb{Q}/\mathbb{Z} \\ \downarrow Res & & \downarrow eRes & & \downarrow eRes \quad \downarrow fe \\ H^2(L^{un}/L) & \xrightarrow{ord_L} & H^1(\Gamma_L,\mathbb{Z}) & \xleftarrow[\delta]{} & H^1(\Gamma_L,\mathbb{Q}/\mathbb{Z}) \xrightarrow{g\mapsto g(\sigma_L)} \mathbb{Q}/\mathbb{Z} \end{array}$$

Donde e es el índice de ramificación de L/K y f es el grado de inercia (grado de la extensión de los cuerpos residuales). El primer cuadrado es obtenido del cuadrado conmutativo

$$\begin{array}{ccc} K^{un\times} & \xrightarrow{ord_K} & \mathbb{Z} \\ \downarrow & & \downarrow e \\ L^{un\times} & \xrightarrow{ord_L} & \mathbb{Z} \end{array}$$

El segundo cuadrado expresa el hecho de que el mapa restricción conmuta con el mapa γ. Aparte de el factor "e", el tercer cuadrado es

$$\begin{array}{ccc} \mathrm{Hom}(\Gamma_K,\mathbb{Q}/\mathbb{Z}) & \xrightarrow{g\mapsto g(\sigma_K)} & \mathbb{Q}/\mathbb{Z} \\ \downarrow g\mapsto g\mid\Gamma_L & & \downarrow f \\ \mathrm{Hom}(\Gamma_L,\mathbb{Q}/\mathbb{Z}) & \xrightarrow{g\mapsto g(\sigma_L)} & \mathbb{Q}/\mathbb{Z} \end{array}$$

El elemento de Frobenius σ_K y σ_L son determinados por el hecho que induce $x \mapsto x^q$ y $x \mapsto x^{q^f}$ respectivamente sobre los cuerpos residuales, donde $q = |k|$ y $q^f = |l|$, por tanto $\sigma_L \mid K^{un} = \sigma_K^f$. Ahora es claro que estos cuadrados conmutan, y $n = ef$, esto prueba la proposición. □

Mapa Local de Artin.
Sea L una extensión finita no ramificada de K con grupo de Galois G, y sea n=[L:K]. La clase local fundamental $u_{L/K}$ es el elemento de $H^2(L/K)$ mapeado por el generador $\frac{1}{[L:K]}$ de $\frac{1}{[L:K]}\mathbb{Z}/\mathbb{Z}$ por el mapa invariante $inv_{L/K} : H^2(L/K) \xrightarrow{\simeq} \frac{1}{[L:K]}\mathbb{Z}/\mathbb{Z}$. El par $(G, L^\times)$ satisface las hipótesis del Teorema de Tate, y por tanto su producto cup con la clase fundamental $u_{L/K}$ define un isomorfismo

$$H_T^r(G,\mathbb{Z}) \to H_T^{r+2}(G, L^\times)$$

para todo $r \in \mathbb{Z}$. Para $r = -2$, esto se convierte en

$$\begin{array}{ccc} H^{-2}(G,\mathbb{Z}) & \xrightarrow{\simeq} & H^0(G,L^\times) \\ \| & & \| \\ G & & K^\times/Nm(L^\times) \end{array}$$

Ahora calcularemos este mapa explícitamente.

Un un elemento primo π de K es también un primo de L, y define la siguiente descomposición

$$L^\times = U_L.\pi^{\mathbb{Z}} \simeq U_L \times \mathbb{Z}$$

de G-módulos. Entonces

$$H^r(G,L^\times) \simeq H^r(G,U_L) \oplus H^r(G,\pi^{\mathbb{Z}})$$

Eligiendo un generador σ de G, y sea $f \in H^1(G,\mathbb{Q}/\mathbb{Z}) \simeq \mathrm{Hom}(G,\mathbb{Q}/\mathbb{Z})$ el elemento tal que $f(\sigma^i) = \frac{i}{n} \bmod \mathbb{Z}$ para todo i. Genera $H^1(G,\mathbb{Q}/\mathbb{Z})$.
De la sucesión exacta

$$0 \to \mathbb{Z} \to \mathbb{Q} \to \mathbb{Q}/\mathbb{Z} \to 0$$

como $H^r(G,\mathbb{Q}) = 0$ para todo r, obtenemos un isomorfismo

$$\delta : H^1(G,\mathbb{Q}/\mathbb{Z}) \to H^2(G,\mathbb{Z})$$

De acuerdo a la descripción dada en la anterior sección anterior sobre el mapa δ, para construir δf, primero elegimos un levantamiento de f por una 1-cocadena $\tilde{f} : G \to \mathbb{Q}$. Tomamos $\tilde{f}$ el mapa $\sigma^i \mapsto \frac{i}{n}$, donde $0 \le i < n-1$. Entonces

$$d\tilde{f}(\sigma^i,\sigma^j) = \sigma^i\tilde{f}(\sigma^j) - \tilde{f}(\sigma^{i+j}) + \tilde{f}(\sigma^i) = \begin{cases} 0 \ si \ i+j \le n-1 \\ 1 \ si \ i+j > n-1 \end{cases}$$

Cuando identificamos $\mathbb{Z} \simeq \pi^{\mathbb{Z}} \subset L^\times$, encontramos que la clase fundamental $u_{L/K} \in H^2(G,L^\times)$ es representada por el cociclo

$$\varphi(\sigma^i,\sigma^j) = \begin{cases} 1 \ si \ i+j \le n-1 \\ \pi \ si \ i+j > n-1 \end{cases}$$

De la sucesión exacta

$$0 \to I \to \mathbb{Z}[G] \to \mathbb{Z} \to 0$$

$$0 \to L^\times \to L^\times(\varphi) \to I \to 0$$

obtendremos los mapas borde

$$H^{-2}(G,\mathbb{Z}) \to H^{-1}(G,I),$$

$$H^{-1}(G,I) \to H^0(G,L^\times).$$

Los cuales son isomorfismos porque $\mathbb{Z}[G]$ y $L^\times(\varphi)$ tienen Cohomología trivial. Como $L^\times(\varphi)$ es el módulo de descomposición de $L^\times \oplus \bigoplus_{\sigma\in G,\sigma\neq 1}\mathbb{Z}x_\sigma$ de φ.

Finalmente $H^{-2}(G,\mathbb{Z}) = H_1(G,\mathbb{Z}) \simeq G$, donde la primer igualdad es por definición, y la segunda porque $H_1(G,\mathbb{Z}) \simeq G^{ab}$, en este caso el grupo ya era abeliano.

PROPOSICIÓN 2.8. *Bajo la composición de los mapas*

$$\begin{array}{ccc} H^{-2}(G,\mathbb{Z}) & \xrightarrow{\simeq} & H^0(G,L^\times) \\ \| & & \| \\ G & & K^\times/Nm(L^\times) \end{array}$$

el elemento de Frobenius $\sigma \in G$ mapea en la clase de π en $K^\times/Nm(L^\times)$.

Notar que como todas las unidades en K son normas de $L^\times$, la clase de π mod $Nm(L^\times)$ es independiente de la elección del primo π. Por otro lado, el G-módulo $L^\times(\varphi)$ y el mapa dependen de la elección de el generador σ para G.

DEMOSTRACIÓN. De la construcción del isomorfismo $H^{-2}(G,\mathbb{Z}) \simeq G$, podemos ver que la imagen de σ bajo el mapa borde $H^{-2}(G,\mathbb{Z}) \to H^{-1}(G,I_G) \subset I_G/I_G^2$ es representado por $\sigma - 1$

El mapa borde $H^{-1}(G,I_G) \to H^0(G,L^\times)$ es dado por el lema de la serpiente de el diagrama

$$\begin{array}{ccccccccc} & & & & & & H^{-1}(G,I_G) & & \\ & & & & & & \downarrow & & \\ & & (L^\times)_G & \longrightarrow & L^\times(\varphi)_G & \longrightarrow & (I_G)_G & \longrightarrow & 0 \\ & & \downarrow & & \downarrow & & \downarrow & & \\ 0 & \longrightarrow & L^{\times G} & \longrightarrow & L^\times(\varphi)^G & \longrightarrow & (I_G)^G & & \\ & & \downarrow & & & & & & \\ & & H^0(G,L^\times) & & & & & & \end{array}$$

Los mapas verticales son $Nm_G = \sum_{i=0}^{n-1} \sigma^i$. El elemento $(\sigma-1)+(I_G)^2$ es la imagen de $X_\sigma + I.L^\times(\varphi)$ en $L^\times(\varphi)_G$, y $Nm_G(x_\sigma + I.L^\times(\varphi)$ es la suma de los elementos

$$x_\sigma = x_\sigma$$

$$x_\sigma = x_{\sigma^2} - x_\sigma + \varphi(\sigma,\sigma)$$

$$\cdots \quad \cdots$$

$$\sigma^{n-1}x_\sigma = x_1 - x_{\sigma^{n-1}} + \varphi(\sigma,\sigma^{n-1})$$

Donde $x_1 = \varphi(1,1) = 1$ y que $+$ sobre el factor $L^\times$ de $L(\varphi)$ es ., entonces encontramos que

$$Nm_G(x_\sigma) = \prod_{i=1}^{n-1} \varphi(\sigma,\sigma^i) = \pi$$

Esto completa la prueba. □

2.2. Cohomología de extensiones ramificadas. Por el Teorema 90 de Hilbert, la sucesión es exacta

$$0 \to H^2(L/K) \xrightarrow{Inf} H^2(E/K) \xrightarrow{Res} H^2(E/L)$$

para cualquier extensión de Galois $E \subset L \subset K$.

TEOREMA 2.9. *Para todo cuerpo local K, existe un isomorfismo canónico*

$$inv_K : H^2(K^{al}/K) \to \mathbb{Q}/\mathbb{Z}$$

Sea L una extensión de Galois de K de grado $n < \infty$. Entonces el diagrama

$$\begin{array}{ccccccc} 0 & \longrightarrow & H^2(L/K) & \longrightarrow & H^2(K^{al}/K) & \xrightarrow{Res} & H^2(K^{al}/L) \\ & & & & \downarrow{\scriptstyle inv_K} & & \downarrow{\scriptstyle Inv_L} \\ 0 & \longrightarrow & \frac{1}{n}\mathbb{Z}/\mathbb{Z} & \longrightarrow & \mathbb{Q}/\mathbb{Z} & \xrightarrow{n} & \mathbb{Q}/\mathbb{Z} \end{array}$$

conmuta, y por tanto define un isomorfismo

$$inv_{L/K} : H^2(L/K) \to \frac{1}{n}\mathbb{Z}/\mathbb{Z}$$

LEMA 2.10. *Si L/K es Galois de grado finito n, entonces $H^2(L/K)$ contiene un subgrupo canónicamente isomorfo a $\frac{1}{n}\mathbb{Z}/\mathbb{Z}$.*

DEMOSTRACIÓN. Consideremos el diagrama

$$\begin{array}{ccccccc} 0 & \longrightarrow & Ker(Res) & \longrightarrow & H^2(K^{un}/K) & \xrightarrow{Res} & H^2(L^{un}/L) \\ & & \downarrow & & \downarrow{\scriptstyle Inf} & & \downarrow{\scriptstyle Inf} \\ 0 & \longrightarrow & H^2(L/K) & \longrightarrow & H^2(K^{al}/K) & \xrightarrow{Res} & H^2(K^{al}/K) \end{array}$$

Ya que los mapas inflación son inyectivos, así también es el primer mapa vertical, por el teorema visto en la sección anterior, vimos que el kernel de el mapa restricción es canónicamente isomorfo a $\frac{1}{n}\mathbb{Z}/\mathbb{Z}$. Terminando la prueba. □

Para completar la prueba del teorema falta ver que el mapa $\frac{1}{n}\mathbb{Z}/\mathbb{Z} \hookrightarrow H^2(L/K)$ es un isomorfismo. Para eso enunciaremos algunos lemas que usaremos.

LEMA 2.11. *Sea L una extensión de Galois finita de K con grupo G. Entonces existe un subgrupo abierto V de O_L, estable por G, tal que $H^r(G, V) = 0 \forall r > 0$*

LEMA 2.12. *Sea L,K, y G como en el lema anterior. Entonces existe un subgrupo abierto V de U_L estable por G tal que $H^r(G, V) = 0 \forall r > 0$*

LEMA 2.13. *Sea L/K una extensión cíclica de grado n, entonces $h(U_L) = 1$ y $h(L^\times) = n$*

LEMA 2.14. *Sea L una extensión de Galois finita de orden n, entonces $H^2(L/K)$ tiene orden n*

DEMOSTRACIÓN. Sabemos que el orden de $H^2(L/K)$ es divisible por n, y que es igual a n si L/K es cíclica. Probemos el lema por inducción sobre [L:K]. Porque el grupo $\mathrm{Gal}(L/K)$ es soluble, existe una extensión de Galois K'/K con $L \supsetneq K' \supsetneq K$. De la sucesión exacta

$$0 \to H^2(K'/K) \to H^2(L/K) \to H^2(L/K')$$

vemos que

$$|H^2(L/K)| \leq |H^2(K'/K) \mid . \mid H^2(L/K') \mid = n$$

□

DEMOSTRACIÓN DEL TEOREMA 2.9. Del diagrama en la prueba de 2.10 podemos ver que para toda extensión finita de Galois L de K, el subgrupo $H^2(L/K)$ de $H^2(K^{al}/K)$ esta contenido en $H^2(K^{un}/K)$. Por tanto $H^2(K^{al}/K) = \bigcup H^2(L/K)$, probando que el mapa inflación $H^2(K^{un}/K) \to H^2(K^{al}/K)$ es un isomorfismo. Componiendo la inversa de esto con el mapa invariante $inv_K : H^2(K^{un}/K) \to \mathbb{Q}/\mathbb{Z}$ del Teorema 2.1. □

Mapa Local de Artin.
El par $(G, L^\times)$ satisface las hipótesis del Teorema de Tate, y por tanto tenemos el siguiente resultado.

TEOREMA 2.15. *Para toda extensión de Galois finita L/K de cuerpos locales y $r \in \mathbb{Z}$, el homomorfismo*

$$H_T^r(Gal(L/K), \mathbb{Z}) \to H_T^{r+2}(Gal(L/K), L^\times)$$

definido por $x \mapsto x \cup u_{L/K}$ es un isomorfismo. Cuando $r = -2$, esto se convierte en

$$Gal(L/K)^{ab} \simeq K^\times / Nm_{L/K}(L^\times)$$

Llamaremos al mapa inverso

$$\phi_{L/K} : K^\times / Nm_{L/K}(L^\times) \xrightarrow{\simeq} Gal(L/K)^{ab}$$

y lo llamamos el ***Mapa local de Artin****, o* ***Mapa de reciprocidad local****.*

Si $L \supset E \supset K$ Con L/K Galois, entonces el homomorfismo en el teorema conmuta con Res y Cor. Para probar el resultado para Res debemos ver que

$$Res(x \cup u_{L/K}) = Res(x) \cup u_{L/K}$$

Para todo $x \in H_T^r(\mathrm{Gal}(L/K), L^\times$. Pero esto es una propiedad estándar del cup-product.

Si $L \supset E \supset K$ Con L/K Galois y E/K Galois, $x \in H^r(\mathrm{Gal}(E/K), E^\times)$ con $r \geq 1$, entonces

$$\mathrm{Inf}(x \cup u_{E/K}) = [L : E]\mathrm{Inf}(x) \cup u_{L/K}$$

De vuelta esta es una propiedad básica del cup-product.

LEMA 2.16. *Sea $L \supset E \supset K$ cuerpos locales con L/K Galois. Entonces los diagramas conmutan*

$$\begin{array}{ccc} E^\times & \xrightarrow{\phi_{L/E}} & Gal(L/E)^{ab} \\ \downarrow{\scriptstyle Nm_{E/K}} & & \downarrow \\ K^\times & \xrightarrow{\phi_{L/K}} & Gal(L/K)^{ab} \end{array} \qquad \begin{array}{ccc} E^\times & \xrightarrow{\phi_{L/E}} & Gal(L/E)^{ab} \\ \uparrow & & \uparrow{\scriptstyle Ver} \\ K^\times & \xrightarrow{\phi_{L/K}} & Gal(L/K)^{ab} \end{array}$$

OBSERVACIÓN 2.17. Sea $L \supset E \supset K$ cuerpos locales con L/K y E/K Galois. Entonces el diagrama conmuta

$$\begin{array}{ccc} K^\times & \xrightarrow{\phi_{L/K}} & \mathrm{Gal}(L/K)^{ab} \\ & \searrow^{\phi_{E/K}} & \downarrow \\ & & \mathrm{Gal}(E/K)^{ab}. \end{array}$$

En particular si $L \supset E \supset K$ es una torre de extensiones abelianas de K, entonces $\phi|L/K(a)|_E = \phi_{E/K}(a), \forall a \in K^\times$, y por tanto podemos definir $\psi_K : K^\times \to \mathrm{Gal}(K^{ab}/K)$ como el homomorfismo tal que, para cada extensión abeliana finita L/K, $\phi_K(a)|L = \psi_{L/K}(a)$

TEOREMA 2.18. *Para todo cuerpo local K, existe un homomorfsimo (mapa local de Artin)*

$$\phi_K : K^\times \to Gal(K^{ab}/K)$$

con las siguientes propiedades

1. *para todo primo $\pi \in K, \phi_K(\pi)|K^{un} = Frob_K$;*
2. *para toda extensión abeliana finita L de K, $Nm_{L/K}(L^\times)$ esta contenido en el kernel de $a \mapsto \phi_K(a)|L$ y ϕ_K induce un isomorfismo*

$$\phi_{L/K} : K^\times / Nm_{L/K}(L^\times) \to Gal(L/K)$$

Descripción alternativa de el mapa local de Artin.
Sea L/K una extensión abeliana finita con grupo de Galois G, y sea $u_{L/K}$ en $H^2(G, L^\times)$ la clase fundamental. El mapa local de Artin $\phi_{L/K}$ es el inverso del isomorfismo

$$x \mapsto x \cup u_{L/K} : H_T^{-2}(G, \mathbb{Z}) \to H_T^0(G, L^\times)$$

Esta definición es difícil para trabajar porque el producto cup involucra grupos de homología y de cohomología no tienen una descripción simple como para trabajar con ella. Interpretaremos de vuelta este mapa puramente en términos de grupo de cohomología. Consideramos el emparejamiento de producto cup

$$H^0(G, L^\times) \times H^2(G, \mathbb{Z}) \to H^2(G, L^\times) \xrightarrow{inv_{L/K}} \mathbb{Q}/\mathbb{Z}$$

Dado un elemento $a \in H^0(G, L^\times) = K^\times$ y una clase $c \in H^2(G, \mathbb{Z})$ representada por el cociclo $f : G \times G \to \mathbb{Z}$, el producto cup $a \cup c$ es representado por el cociclo $(\sigma, \tau) \mapsto a^{f(\sigma,\tau)}$. Recordando que tenemos un isomorfismo

$$\mathrm{Hom}(G, \mathbb{Q}/\mathbb{Z}) = H^1(G, \mathbb{Q}/\mathbb{Z}) \xrightarrow{\delta} H^2(G, \mathbb{Z}).$$

PROPOSICIÓN 2.19. *Para todo $\chi \in Hom_{cts}(G, \mathbb{Q}/\mathbb{Z})$ y $a \in K^\times$,*

$$\chi(\phi_{L/K}(a)) = inv_K(a \cup \delta_\chi).$$

Usando esto podemos obtener otra descripción del mapa de Artin.

LEMA 2.20. *Si L/K es no ramificada, $\phi_{L/K}$ manda $a \in K^\times \mapsto Frob^{ord_K(a)}$*

Demostración. Recordemos que inv_K es definido por la composición

$$H^2(G, L^\times) \xrightarrow{H^2(ord)} H^2(G, \mathbb{Z}) \xleftarrow{\delta} \mathrm{Hom}(G, \mathbb{Q}/\mathbb{Z}) \xrightarrow{\chi \mapsto \chi(\sigma)} \mathbb{Q}/\mathbb{Z}$$

Por la functorialidad del producto cup

$$ord(a \cup \delta_\chi) = ord(a) \cup \delta_\chi, a \in K^\times, \chi \in \mathrm{Hom}(G, \mathbb{Q}/\mathbb{Z})$$

donde, a la izquierda ord denota el mapa sobre H^2 inducido por $ord_L : L^\times \twoheadrightarrow \mathbb{Z}$. Sea $a \in H^0(G, L^\times) = K^\times$, y sea $m = ord_L(a)$. Para cada $\chi \in \mathrm{Hom}(G, \mathbb{Q}/\mathbb{Z})$, en el diagrama de arriba,

$$a \cup \delta_\chi \mapsto ord(a) \cup \delta_\chi \mapsto m_\chi \mapsto \chi(\sigma^m),\ \sigma = Frob.$$

Por tanto $inv_K(a \cup \delta_\chi) = \chi(\sigma^m)$. Combinándolo con la proposición anterior vemos que

$$\chi(\phi(\alpha)) = \chi(\sigma^{ord(\alpha)})$$

para todo $\chi \in \mathrm{Hom}(G, \mathbb{Q}/\mathbb{Z})$ y por tanto $\phi(\alpha) = \sigma^{ord(\alpha)}$.

Para cada carácter $\chi \in G$, obtenemos un carácter $a \mapsto inv_K(a \cup \delta_\chi)$ de $K^\times$. Por dualidad obtenemos un mapa $K^\times \to G$. Este mapa es $\phi_{L/K} : K^\times \to \mathrm{Gal}(L/K)$ □

3. Grupo de Brauer

En esta sección daremos una interpretación al grupo $H^2(L/K)$, para eso definiremos el grupo de Brauer. En el resto de la sección usaremos las siguientes nociones. Una K-álgebra A es un anillo que contiene a K en su centro y su dimensión es finita como K-espacio vectorial. A no necesariamente tiene que ser conmutativo, por ejemplo $M_n(K)$ el álgebra de las matrices $n \times n$ sobre K. Una K-subálgebra de una K-álgebra es un subanillo que contiene a K. Un homomorfismo de K-álgebras $\varphi : A \to B$ es un homomorfismo de anillos con la propiedad $\varphi(a) = a \forall a \in K$. Definimos el opuesto A^{op} de una K-álgebra A como el álgebra con el mismo conjunto y la misma suma, pero la multiplicación $\bullet$ definida por $\alpha \bullet \beta = \beta * \alpha$ donde * denota la multiplicación en A. Sea $e_1, ..., e_n$ una base de A como K-espacio vectorial. Entonces

$$e_i e_j = \sum_l a_{ij}^l e_l$$

para algunos $a_{ij}^l \in K$, llamados constantes de estructura de A relativas a la base $(e_i)_i$. Una vez elegida la base, el álgebra queda únicamente determinada por sus constantes de estructura.

3.1. Definición de grupo de Brauer. Entenderemos por un A-módulo, a un A-módulo V a izquierda finitamente generado. En particular, esto significa que $1v = v$ para todo $v \in V$. Tal V es además de dimensión finita cuando lo pensamos como K-espacio vectorial, y por tanto tomamos un A-módulo es lo mismo que dar un K-espacio vectorial de dimensión finita con un homomorfismo de K-álgebras $A \to End_K(V)$, una representación de A en V. El módulo es fiel si este homomorfismo es inyectivo, es decir, si $\alpha x = 0$ para todo $x \in V$ implica $\alpha = 0$.

Un A-módulo V es simple si es no trivial y no contiene un A-submódulo excepto el 0, y es semisimple si es isomorfo a la suma directa de A-módulos simples. Es indescomponible si no puede ser escrito como la suma directa de dos A-módulos no nulos. Por tanto un

módulo simple es semisimple, y un módulo indescomponible es semisimple si y solo si es simple.

Sea${}_AA$, A como un A-módulo a izquierda. La multiplicación a derecha $x \mapsto xa$ sobre ${}_AA$ por un elemento a de A es un A-lineal endomorfismo de ${}_AA$. Más aún, cada mapa A-lineal $\varphi :_A A \to_A A$ es de esta forma con $a = \varphi(1)$. Por tanto

$$\varphi \mapsto \varphi(1) : End_A({}_AA) \xrightarrow{\simeq} A \text{ (como K-espacios vectoriales)}$$

Sea φ_a el mapa $x \mapsto xa$. Entonces

$$(\varphi_a \circ \varphi_b)(1) = \varphi_a(\varphi_b(1)) = \varphi_a(b) = ba = \varphi_{ba}(1)$$

y por tanto,

$$End_A({}_AA) \simeq A^{op} \text{ (como K-álgebras).}$$

Mas en general, si V es un A-módulo libre de rango n, entonces una elección de una base para V determina un isomorfismo

$$End_A(V) \to M_n(A^{op}).$$

Una K-álgebra A es llamada semisimple si todo A-módulo es semisimple. Como cada A-módulo es n cociente de una suma directa de copias de ${}_AA$, es suficiente verificar que el A-módulo ${}_AA$ es semisimple.

Una K-álgebra A es llamada simple si no contiene ideales propios a ambos lados además de 0.

Observación 3.1. El kernel de un homomorfismo $f : A \to B$ de K-álgebras es un ideal en A que no contiene a 1. Por tanto, si A es simple, entonces f es inyectivo.

Observación 3.2. Una K-álgebra es llamada un álgebra de división si todo elemento no nulo a de A tiene un inverso. Por tanto un álgebra de división satisface todos los axiomas para ser un cuerpo excepto la conmutatividad. Claramente, un álgebra de división no tiene ideales propios, a derecha, izquierda o ambos lados, y por tanto es simple.

Observación 3.3. Para $a, b \in K^\times$, sea $H(a, b)$ la K-álgebra con base 1,i,j,ij (como K-espacio vectorial) y con la multiplicación determinada por

$$i^2 = a,\ j^2 = b,\ ij = -ji$$

Entonces H(a,b) es una K-álgebra, llamada el álgebra de cuaterniones sobre K. Por ejemplo, si $K = \mathbb{R}$, entonces H(-1,-1) es el álgebra de cuaterniones usual. Se puede ver que H(a,b) es además un anillo de división o es isomorfos a $M_2(K)$. En particular es simple.

Dado A una K-subálgebra de una K-álgebra B. El centralizador de A en B es

$$C_B(A) = \{b \in B \mid ba = ab\ \forall a \in A\}$$

Esto también es una K-subálgebra de B.

Observación 3.4. En los siguientes ejemplos, el centralizador es tomado en $M_n(K)$

1. Sea A el conjunto de las matrices escalares, o sea, $A = KI_n$. Claramente $C(A) = M_n(K)$

2. Sea $A = M_n(K)$ entonces C(A) es el centro de $M_n(K)$. Sea e_{ij} la matriz con 1 en la (i,j) posición y 0 en el resto de las posiciones. Por tanto
$$e_{ij}e_{lm} = \begin{cases} e_{im} \text{ si } j = l \\ 0 \text{ si } j \neq l \end{cases}$$
Sea $\alpha = (a_{ij}) \in M_n(K)$. Entonces $\alpha = \sum_{i,j} a_{ij}e_{ij}$, y por tanto $\alpha e_{lm} = \sum_i a_{il}e_{im}$ y $e_{lm}\alpha = \sum_j a_{mj}e_{lj}$. Si α esta en el centro de $M_n(K)$, entonces $\alpha e_{lm} = e_{lm}\alpha$, y por tanto $a_{il} = 0$ para $i \neq l, a_{m_j} = 0$ para $j \neq m$, y $a_{ll} = a_{mm}$. De esto sigue que el centro de $M_n(K)$ es K
3. Sea A el conjunto de matrices diagonales en $M_n(K)$. En este caso, C(A)=A

TEOREMA 3.5. *(Teorema del doble centralizador)*
Sea A una K-álgebra,y sea V un A-módulo semisimple fiel. Entonces C(C(A))=A.

DEMOSTRACIÓN. Sea $D = C(A)$ y $B = C(D)$. Claramente $A \subset B$, y la inclusión reversa sigue del siguiente lema cuando tomamos $v_1, ..., v_n$ que generen V como K-espacio vectorial. □

LEMA 3.6. *Para todo $v_1, ..., v_n \in V$ y $b \in B$, existe un $a \in A$ tal que*
$$av_1 = bv_1,\ av_2 = bv_2,\ ...,\ av_n - bv_n.$$

No daremos la demostración de este lema.

LEMA 3.7. *(Lema de Schur) El álgebra de endomorfismo de un A-módulo simple es un álgebra de división.*

DEMOSTRACIÓN. Sea γ un mapa A-lineal $S \to S$. Entonces $Ker(\gamma)$ es un A-submódulo de S, y por tanto es S o 0. En el primer caso, γ es cero, y en el segundo caso es un isomorfismo, o sea, tiene un inverso que además es A-lineal. □

TEOREMA 3.8. *(Weddeburn)*
Toda K-álgebra simple A es isomorfa a $M_n(D)$ para algún n y alguna K-álgebra de división D

DEMOSTRACIÓN. Elegimos un A-módulo simple S, por ejemplo, algún ideal minimal a izquierda de A. Entonces A actúa fielmente sobre S, porque el kernel de $A \to End_K(S)$ es un ideal a ambos lados de A que no contiene al 1, y por tanto es 0.

Sea D el centralizador de A en el K-álgebra $End_K(S)$ de mapas K-lineales $S \to S$. De acuerdo con el Teorema del doble centralizador, el centralizador de D en $End_K(S)$ es A, o sea, $A = End_D(S)$. EL lema de Schur implica que D es un álgebra de división. Por tanto, S es un D-módulo libre, decimos $S \approx D^n$, y por tanto $End_D(S) \approx M_n(D^{op})$. □

Producto tensorial de álgebras.
Sean A y B K-álgebras, y sea $A \otimes_K B$ el producto tensorial de A y B como K-espacios vectoriales. Existe una única K-bilineal multiplicación sobre $A \otimes_K B$ tal que
$$(a \otimes b)(a' \otimes b') = aa' \otimes bb',\ a, a' \in A,\ b, b' \in B.$$
Cuando identificamos K con $K.(1 \otimes 1) \subset A \otimes_K B$, entonces $A \otimes_K B$ se convierte en una K-álgebra. Si $(e_i)_i$ y $(f_j)_j$ son bases de A y B como K-espacios vectoriales, entonces $(e_i \otimes f_j)_{i,j}$ es una base para $A \otimes_K B$, y las constantes de estructura para $A \otimes_K B$ pueden

ser obtenidos de los de A y B por la formula obvia. Usaremos que el producto tensorial es conmutativo en el sentido que, para dos K-álgebras A y B, el mapa $a \otimes b \mapsto b \otimes a$ extiende a un isomorfismo de K-álgebras

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

y que son asociativos en el sentido que, para tres K-álgebras A, B y C, el mapa $a \otimes (b \otimes c) \mapsto (a \otimes b) \otimes c$ extiende a un isomorfismo de K-álgebras

$$A \otimes_K (B \otimes_K C) \to (A \otimes_K B) \otimes_K C.$$

Observación 3.9. Para toda K-álgebra A

$$A \otimes_K M_n(K) \simeq M_n(A)$$

Para ver esto, notar que un anillo B que contiene un subanillo R en su centro es isomorfo a $M_n(R)$ si y solo si este admite una base $(e_{ij})1 \leq i, j \leq n$ a la izquierda como R-módulo tal que

$$e_{ij}e_{lm} = \begin{cases} e_{im} \text{ si } j = l \\ 0 \text{ si } j \neq l \end{cases}$$

Si (e_{ij}) es la base estándar para $M_n(K)$, entonces $(1 \otimes e_{ij}$ es una A-base para $A \otimes M_n(K)$ con la propiedad correcta.
Mas en general

$$A \otimes_K M_n(A') \simeq M_n(A \otimes_K A')$$

para todas K-álgebras A y A'

Observación 3.10. Para m,n, $M_m(K) \otimes M_n(K) \sim M_{mn}(K)$. Para ver esto, notemos que $M_m(K) \otimes_K M_n(K) \sim M_m(M_n(K))$, y una matriz $m \times m$ tal que sus entradas son matrices $n \times n$ es una matriz $mn \times mn$. Alternativamente, sea (e_{ij}) y $(f_{i'j'})$ una base estándar para $M_m(K)$ y $M_n(K)$, y chequeamos que $(e_{ij} \otimes f_{i'j'})$ tiene la propiedad de multiplicación correcta.

La siguiente proposición muestra que el centralizador de un producto tensorial de subálgebras es el producto de los centralizadores.

Proposición 3.11. *Sea A y A' K-álgebras, con subálgebras B y B', y sea $C(B)$ y $C(B')$ los centralizadores de B y B' en A y A' respectivamente. Entonces el centralizador de $B \otimes_K B'$ en $A \otimes_K A'$ es $C(B) \otimes_K C(B')$, o sea,*

$$C_{A \otimes_K A'}(B \otimes_K B') = C_A(B) \otimes_K C_{A'}(B')$$

Demostración. Claramente $C(B \otimes_K B') \supset C(B) \otimes_K C(B')$
Sea $(f_i)_i$ una base para A' como K-espacio vectorial. Entonces $(1 \otimes f_i)_i$ es una base para $A \otimes_K A'$ como un A-módulo, y por tanto un elemento $\alpha \in A \otimes_K A'$ puede ser escrito de manera unica como $\alpha = \sum_i \alpha_i \otimes f_i$, $\alpha_i \in A$. Sea $\beta \in B$, entonces α conmuta con $\beta \otimes 1$ si y solo si $\beta\alpha_i = \alpha_i\beta \; \forall i$. Por tanto, el centralizador de $B \otimes 1$ en $A \otimes A'$ es $C(B) \otimes A'$. Similarmente, el centralizador de $1 \otimes B'$ en $C(B) \otimes A'$ es $C(B) \otimes C(B')$.

Claramente, $C(B \otimes B') \subset C(B \otimes 1)$, por tanto $C(B \otimes B')$ esta contenido en $C(B) \otimes A'$, y esta contenido en el centralizador de $1 \otimes B'$ en $C(B) \otimes A'$, que es $C(B) \otimes C(B')$.
Esto termina la prueba □

En particular, el centro de un producto tensorial de dos K-álgebras es el producto tensorial de sus centros: $Z(A \otimes_K B) = Z(A) \otimes_K Z(B)$

COROLARIO 3.12. *El centro de una K-álgebra simple es un cuerpo.*

DEMOSTRACIÓN. Obviamente, el centro de un álgebra de división es un cuerpo, pero el teorema de Wedderburn muestra que toda K-álgebra simple es isomorfa a $M_n(D)$ para algún álgebra de división D. Ahora $M_n(D) \simeq M_n(K) \otimes_K D$, y por tanto $Z(M_n(D)) \simeq K \otimes_K Z(D) \simeq Z(D)$ □

Una K-álgebra es llamada central si su centro es K, y una K-álgebra que es central y simple, se dice un álgebra central simple. El corolario muestra que toda K-álgebra simple es central simple sobre alguna extensión finita de K.

LEMA 3.13. *Sea A una K-álgebra, y sea D un álgebra de división con centro K. Entonces cualquier ideal a ambos lados I en $A \otimes D$ es generado como D-módulo a izquierda por $a = I \cap (A \otimes 1)$.*

PROPOSICIÓN 3.14. *El producto tensorial de dos K-álgebras simples, con al menos una central, es también simple.*

DEMOSTRACIÓN. Por el teo de Weddeburn, podemos suponer que una de las álgebras es $M_n(D)$, donde D es un álgebra de división con centro K. Sea A la segunda K-álgebra simple. En el lema enunciado antes, podemos ver que $A \otimes_K D$ es simple. Por tanto, $A \otimes_K D \approx M_m(D')$ con D' un álgebra de división, y por tanto

$$A \otimes_K M_n(D) \simeq M_n(A \otimes_K D) \approx M_n(M_m(D')) \approx M_{mn}(D'),$$

que es simple □

COROLARIO 3.15. *El producto tensorial de dos K-álgebras centrales simples es un K-álgebra central simple*

DEMOSTRACIÓN. Combinar Proposiciones 3.11 y 3.14 □

Sea A un álgebra central simple sobre K, y tomemos V a A como K-espacio vectorial. Entonces la multiplicación a izquierda hace que V se convierta en un A-módulo a izquierda, y la multiplicación a derecha convierte a V en un A-módulo a derecha, o lo que es lo mismo un A^{op}-módulo a izquierda. De la universalidad del producto tensorial, obtenemos un homomorfismo

$$a \otimes A' \mapsto (v \mapsto ava') : A \otimes_K A^{op} \to End_K(V)$$

Como $A \otimes_K A^{op}$ es simple y el kernel de los homorfismos no contienen al 1, por tanto es inyectivo. Podemos ver que

$$[A \otimes_K A^{op} : K] = [A : K]^2 = (dimV)^2 = [End_K(V) : K]$$

y por tanto el homomorfismo es un isomorfismo. Hemos probado el siguiente resultado.

COROLARIO 3.16. *Para una K-álgebra central simple A,*

$$A \otimes_K A^{op} \simeq End_K(A) \approx M_n(K),\ n = [A : K]$$

Definición de el grupo de Brauer.
Sean A y B álgebras centrales simples sobre K. Diremos que A y B son similares, $A \sim B$, si $A \otimes_K M_n(K) \approx B \otimes_K M_m(K)$ para algún m y n. Esta es una relación de equivalencia, es obvio que es reflexiva y simétrica, y es transitiva por la observación 3.10. Definimos Br(K) como el conjunto de clases de similaridad de álgebras centrales simples sobre K, y escribimos [A] la clase de similaridad de A. Para clases [A] y [B], definimos

$$[A][B] = [A \otimes_K B]$$

Esto esta bien definido (o sea,$A \sim A'$ y $B \sim B'$, entonces $A \otimes_K B \sim A' \otimes_K B'$), la asociatividad y conmutatividad vienen dadas porque el producto tensorial es asociativo y conmutativo. Para todo n, $[M_n(K)]$ es un elemento identidad, y como $A \otimes_K A^{op} \simeq M_n(K)$ [A] tiene $[A^{op}]$ como su inverso. Por tanto Br(K) es un grupo abeliano, llamado el grupo de Brauer de K.

Observación 3.17.

1. Si K es algebraicamente cerrado, entonces Br(K)=0. Para probar esto veamos que toda álgebra de división central D sobre K es igual K. Sea $\alpha \in D$, y sea $K[\alpha]$ la subálgebra de D generada por K y α. Entonces $K[\alpha]$ es un cuerpo conmutativo de grado finito sobre K (porque es un dominio integral de grado finito sobre K). Por tanto $K[\alpha] = K$, y $\alpha \in K$. Como α era arbitrario, esto muestra que D=K.
2. Frobenius mostró que el álgebra de cuaterniones de Hamilton es la única álgebra de división central sobre $\mathbb{R}$. Por tanto, el grupo de Brauer de $\mathbb{R}$ es cíclico de orden 2, igual a $\{[\mathbb{R}], [\mathbb{H}]\}$
3. Wedderburn mostró que toda álgebra de división finita es conmutativa. Por tanto, el grupo de Brauer de cuerpos finitos es trivial.
4. Hasse mostró que el grupo de Brauer de un cuerpo no arquimedeano local es canónicamente isomorfo a $\mathbb{Q}/\mathbb{Z}$.
5. Albert, Brauer, Hasse, y Noether mostraron que, para un cuerpo de números K, hay una sucesión exacta

$$0 \to Br(K) \to \bigotimes_v Br(K_v) \xrightarrow{\sum} \mathbb{Q}/\mathbb{Z} \to 0$$

La suma es sobre todos los primos de K (incluidos los primos infinitos).

Proposición 3.18. *Sea A un álgebra central simple sobre K, y sea L una extensión de K (no necesariamente finita). Entonces $A \otimes_K L$ es un álgebra central simple sobre L.*

Demostración. El mismo argumento que en la prueba de 3.11 muestra que el centro de $A \otimes_K L$ es $K \otimes_K L = K$. Además, la prueba del lema 3.13 no usa que D es de dimensión finita sobre K. Por tanto, cuando A es un álgebra de división, todo ideal a ambos lados en $A \otimes_K L$ es generado como un A-módulo por su intersección con L, y por tanto es 0 o $A \otimes_K L$. En el caso general, $A \approx M_n(D)$, y por tanto

$$\begin{aligned} A \otimes_K L \approx M_n(D) \otimes_K L &\simeq (M_n(K) \otimes_K D) \otimes_K L \\ &\simeq M_n(K) \otimes_K (D \otimes_K L) \\ &\simeq M_n(D \otimes_K L) \\ &\simeq M_n(L) \otimes_L (D \otimes_K L) \end{aligned}$$

el cual es simple □

COROLARIO 3.19. *Para una K-álgebra central simple A sobre K, $[A : K]$ es un cuadrado.*

DEMOSTRACIÓN. Claramente $[A : K] = [A \otimes_K K^{al} : K^{al}]$ y $A \otimes_K K^{al} \approx M_n(K^{al})$ para todo n. □

Sea L una extensión de K. Entonces

$$M_n(K) \otimes L \simeq M_n(L)$$

y

$$(A \otimes_K L) \otimes_L (A' \otimes_K L) = A \otimes_K (L \otimes_L (A' \otimes_K L)) = (A \otimes_K A') \otimes_K L.$$

Por tanto el mapa $A \mapsto A \otimes_K L$ define un homomorfismo

$$Br(K) \to Br(L)$$

Denotaremos el kernel del homomorfismo por $Br(L/K)$, esto consiste de las clases de similaridad representadas por una K-álgebra central simple A tal que la L-álgebra $A \otimes_K L$ es un álgebra de matrices. □

Un álgebra central simple A es llamada split por L, y L es llamado un splitting field para A, si $A \otimes_K L$ es un álgebra de matrices por L. Por tanto $Br(L/K)$ consiste de los elementos de Br(K) split por L.

PROPOSICIÓN 3.20. *Para un cuerpo K, $Br(K) = \bigcup Br(L/K)$, donde L corre sobre las extensiones finitas de K contenida en alguna clausura algebraica fija.*

DEMOSTRACIÓN. Tenemos que ver que una K-álgebra central simple sobre K es split por una extensión finita de K.
Sabemos que $A \otimes_K K^{al} \approx M_n(K^{al})$, o sea, que existe una base $(e_{ij})_{1 \leq i,j, \leq n}$ para $A \otimes_K K^{al}$ tal que $e_{ij}e_{lm} = \delta_{jl}e_{im}$ para todos i,j,l,m. Como $A \otimes_K K^{al} = \bigcup_{[L:K]<\infty} A \otimes_K L$, todos los e_{ij} se encuentran en $A \otimes_K L$ para algún L, de esto se sigue que $A \otimes_K K \approx M_n(K)$ □

3.2. El grupo de Brauer y la cohomología. Ahora veremos que dada una extensión de Galois L/K, existe un isomorfismo natural $H^2(L/K) \simeq Br(L/K)$

Subcuerpos maximales.
Necesitaremos una variante del Teorema del doble centralizador en el cual $M_n(K)$ es remplazado por un álgebra central simple.

TEOREMA 3.21. *Sea B una K-subálgebra simple de una K-álgebra central simple A. Entonces el centralizador C=C(B) de B en A es simple, y B es el centralizador de C. más aún*

$$[B : K][C : K] = [A : K]$$

DEMOSTRACIÓN. Ver Teorema 3.1 de [**Mil20**] □

Álgebras centrales simples y 2-cociclos.
De aquí en adelante necesitaremos el siguiente teorema

TEOREMA 3.22. *(Noether-Skolem)*
Dados $f, g : A \to B$ homomorfismos entre K-álgebras. Si A es simple y B es central simple, entonces existe un elemento invertible $b \in B$ tal que $f(a) = bg(a)b^{-1}$.

DEMOSTRACIÓN. Mirar Teorema 2.10 de [**Mil20**] □

Fijada una extensión de Galois finita L de K, y sea $G = \mathrm{Gal}(L/K)$. Definimos $\mathcal{A}(L/K)$ como la clase de álgebras centrales simples A sobre K que contienen a L y de grado $[A : K] = [L : K]^2$ (por tanto, L es el centralizador en A).

Fijado un $A \in \mathcal{A}(L/K)$. Para todo $\sigma \in G$ el Teorema de Noether-Skolem, muestra que existe un elemento $e_\sigma \in A$ tal que

$$\sigma a = e_\sigma a e_\sigma^{-1} \; \forall a \in L.$$

Mas aún, e_σ es determinado por la ecuación anterior hasta la multiplicación por un elemento de $L^\times$, porque si f_σ tiene la misma propiedad, entonces $f_\sigma^{-1} e_\sigma$ centraliza L. Notar que la ecuación puede ser escrita como ‘

$$e_\sigma.a = \sigma a.e_\sigma \; \forall a \in L.$$

Claramente $e_\sigma e_\tau$ tiene la propiedad 3.2 para $\sigma\tau$, y por tanto

$$e_\sigma e_\tau = \varphi(\sigma, \tau) e_{\sigma\tau}$$

para algún $\varphi(\sigma, \tau) \in L^\times$. Notar que

$$e_\rho(e_\sigma e_\tau) = e_\rho(\varphi(\sigma, \tau) e_{\sigma\tau}) = \rho\varphi(\sigma, \tau).\varphi(\rho, \sigma\tau).e_{\rho\sigma\tau}$$

y

$$(e_\rho e_\sigma)e_\tau = \varphi(\rho, \sigma) e_{\rho\sigma} e_\tau = \varphi(\rho, \sigma)\varphi(\rho\sigma, \tau).e_{\rho\sigma\tau}.$$

Por tanto la ley de asociatividad implica que φ es un 2-cociclo. Además es un 2-cociclo normalizado si $e_1 = 1$. Una elección diferente de e_σ's lleva a un 2-cociclo de cohomología, y por tanto tenemos bien definido el mapa $A \mapsto \gamma(A) : \mathcal{A}(L/K) \to H^2(L/K)$.

TEOREMA 3.23. *El mapa $\gamma : \mathcal{A}(L/K) \to H^2(L/K)$ es sobreyectivo, y sus fibras son las clases de isomorfismo*

Primero necesitaremos el siguiente lema.

LEMA 3.24. *Sea $A \in \mathcal{A}(L/K)$, y definimos e_σ que satisfaga 3.2. Entonces el conjunto $(e_\sigma)_{\sigma \in G}$ es una base para A como espacio vectorial a izquierda sobre L.*

DEMOSTRACIÓN. Ahora A es únicamente determinado por la siguiente propiedad: $A \supset L$; $(e_\sigma)_{\sigma \in G}$ es una base para A como L-espacio vectorial; multiplicación en A satisface la ecuación 3.2 y 3.2.

Sea $A' \in \mathcal{A}(L/K)$ y supongamos que $\gamma(A) = \gamma(A')$. La condición implica que podemos elegir una base (e_σ) y (e'_σ) para A y A' satisfaciendo 3.2 y 3.2 con el mismo 2-cociclo φ. El mapa $\sum a_\sigma e_\sigma \mapsto \sum a_\sigma e'_\sigma : A \to A'$ es un isomorfismo de K-álgebras.

Ahora supongamos que A y A' son elementos isomorfos de $\mathcal{A}(L/K)$. El Teorema de Noether-Skolem nos permite elegir el isomorfismo $f : A \to A'$ tal que $f(L) = L$ y $f|L$ es

el mapa identidad. Si e_σ satisface 3.2 para A, entonces $f(e_\sigma)$ satisface 3.2 para A'. Con la opción de (e_σ) y $(f(e_\sigma))$, A y A' define el mismo cociclo.

Esto muestra que el mapa $A \mapsto \gamma(A)$ define una inyección

$$\mathcal{A}(L/K)/ker(\gamma) \xrightarrow{\approx} H^2(L/K)$$

Para ver que el mapa es sobreyectivo, construiremos la inversa.

Sea $\varphi : G \times G \to L^\times$ un 2-cociclo normalizado. Defino $A(\varphi)$ como el L-espacio vectorial con base $(e_\sigma)_{\sigma \in G}$ con la multiplicación dada por 3.2 y 3.2. Entonces e_1 es un elemento identidad para la multiplicación, y la condición de cociclo muestra que

$$e_\rho(e_\sigma e_\tau) = (e_\rho e_\sigma)e_\tau$$

De esto sigue que $A(\varphi)$ es una K-álgebra. Identificamos L con el subcuerpo Le_1 de $A(\varphi)$. □

LEMA 3.25. *El álgebra $A(\varphi)$ es central simple sobre K.*

DEMOSTRACIÓN. Sea φ y φ' 2-cociclos de cohomología, o sea,

$$a(\sigma).\sigma a(\tau).\varphi'(\sigma,\tau) = a(\sigma\tau).\varphi(\sigma,\tau)$$

para algún mapa $a : G \to L'$. Se ve inmediatamente que $A(\varphi) \to A(\varphi')$ enviando e_σ en $a(\sigma)e'_\sigma$ es un isomorfismo de K-álgebras. Por tanto $\varphi \mapsto A(\varphi)$ define un mapa $H^2(L/K) \to \mathcal{A}(L/K)/\approx$, el cual es el inverso de $A \mapsto \gamma(A)$. Esto completa la prueba del teorema. □

Las álgebras $A(\varphi)$ son llamadas álgebras de producto cruzado. Antes de que existieran los grupos de cohomología, los 2-cociclos $\varphi : G \times G \to L^\times$ eran llamados conjuntos de factores.

TEOREMA 3.26. *Para cada extensión de Galois L/K, el mapa $\varphi \mapsto [A(\varphi)]$ define un isomorfismo de grupos abelianos $H^2(L/K) \to Br(L/K)$.*

DEMOSTRACIÓN. Para mostrar que este mapa es biyectivo, es suficiente ver que el mapa $A \mapsto [A] : \mathcal{A}(L/K)/\approx \to Br(L/K)$ es biyectivo.

Si A y A' son K-álgebras centrales simples similares, entonces existe un álgebra de división D tal que $A \sim D \sim A'$, decimos que $A \approx M_n(D), A' \approx M_{n'}(D)$. Pero si $[A : K] = [A' : K]$, entonces $n = n'$, y por tanto $A \approx A'$. Esto prueba que el mapa $\mathcal{A}(L/K)/\approx \to Br(L/K)$ es inyectivo, y mirar Corolario 3.6 de [**Mil20**, capítulo 3] que es sobreyectivo. □

LEMA 3.27. *Para cualquier par de 2-cociclos φ y φ', $A(\varphi + \varphi') \sim A(\varphi) \otimes_K A(\varphi')$.*

DEMOSTRACIÓN. Ver Lema 3.15 de [**Mil20**]. □

COROLARIO 3.28. *Sea K^{al} una clausura algebraica separable de K, existe un único isomorfismo canónico $Br(K) \to H^2(K^{al}/K)$*

DEMOSTRACIÓN. Para cualquier torre de cuerpos $E \supset L \supset K$ con E y L extensiones finitas y de Galois sobre K, el diagrama

$$\begin{array}{ccc} H^2(L/K) & \xrightarrow{Inf} & H^2(E/K) \\ \downarrow & & \downarrow \\ Br(L/K) & \hookrightarrow & Br(E/K) \end{array}$$

conmuta (el mapa vertical envía φ en $[A(\varphi)]$). Ahora usamos que

$$Br(K) = \bigcup Br(L/K)$$

$$H^2(K^{al}/K) = \bigcup H^2(L/K)$$

donde ambas uniones recorren todas las extensiones de Galois L de K contenidas en K^{al}. □

COROLARIO 3.29. *Para todo cuerpo K, Br(K) es de torsión, y para toda extensión finita L/K, Br(L/K) es a lo sumo de orden [L:K].*

DEMOSTRACIÓN. El mismo enunciado es verdadero para los grupos de cohomología. □

3.3. El grupo de Brauer de algunos cuerpos particulares. Los resultados de esta sección permitirán interpretar algunos resultados anteriores en términos del Grupo de Brauer.

Cuerpos finitos.
Sea K un cuerpo finito, ya vimos que, para toda extensión finita L de K, $H^2(L/K) = 0$ y por tanto Br(K)=0. El siguiente resultado es una prueba directa de este hecho.

TEOREMA 3.30. *(Wedderburn) Toda álgebra de división finita es conmutativa*

DEMOSTRACIÓN. Sea D un álgebra de división finita con centro K, y sea $[D : K] = n^2$. Cada elemento de D esta contenido en un subcuerpo $K[\alpha] \subset D$, y por tanto es un subcuerpo maximal. Cada subcuerpo maximal de D tiene q^n elementos. Son todos isomorfos, entonces son conjugados. Por tanto, para un subcuerpo maximal L, $D^\times = \bigcup \alpha L^\times \alpha^{-1}$, pero un grupo finito no puede ser la unión de conjugados de un subgrupo propio, y por tanto D=L. □

Los Reales.
Sea $G = \mathrm{Gal}(\mathbb{C}/\mathbb{R}) = \{1, \sigma\}$. Entonces

$$H^2(\mathbb{C}/\mathbb{R}) \simeq H^0_T(G, \mathbb{C}^\times) = \mathbb{R}^\times / Nm_G(\mathbb{C}^\times) = \{\pm\},$$

y por tanto $Br(\mathbb{C}/\mathbb{R})$ es un grupo cíclico de orden 2. El elemento no nulo de $H^2(\mathbb{C}/\mathbb{R})$ es representado por el 2-cociclo $\varphi : G \times G \to \mathbb{C}^\times$,

$$\varphi(\rho, \tau) = \begin{cases} -1 \text{ si } \rho = \sigma = \tau \\ 1 \text{ en otro caso.} \end{cases}$$

Sea $\mathbb{H}$ el álgebra de cuaterniones usual sobre $\mathbb{R}$. Entonces el mapa $\mathbb{C}$-lineal $A(\varphi) \to \mathbb{H}$ enviando $x_\sigma \mapsto j$ es un isomorfismo de $\mathbb{R}$-álgebras. De esto se sigue que toda álgebra

central simple sobre $\mathbb{R}$ es isomorfa a un álgebra de matrices sobre $\mathbb{R}$ o a un álgebra de matrices sobre $\mathbb{H}$.

Cuerpos locales no arquimedeanos.

Sea K un cuerpo local no arquimedeano. En la sección anterior definimos el isomorfismo $inv_K : H^2(K^{al}/K) \simeq \mathbb{Q}/\mathbb{Z}$ y por tanto el isomorfismo $Br(K) \simeq \mathbb{Q}/\mathbb{Z}$. Explicaremos como construir este isomorfismo de manera directa.

Sea D un álgebra central simple sobre K, y sea $n^2 = [D : K]$. Para cada subcuerpo L de D conteniendo a K, el valor absoluto $|\ .\ |$ tiene una única extensión a L. Cada elemento $\alpha \in D$ esta contenido en un subcuerpo de D, por ejemplo, $K[\alpha]$, el valor absoluto $|\ .\ |$ tiene una única extensión para D, $|\ .\ |$ sigue siendo un valor absoluto no arquimedeano. Es decir

1. $|\alpha| = 0 \Longleftrightarrow \alpha = 0$;
2. $\forall \alpha,\ \beta \in D, |\alpha\beta| = |\alpha||\beta|$;
3. $\forall \alpha,\ \beta \in D, |\alpha + \beta| \leq max\{|\alpha|, |\beta|\}$.

Sea q el cardinal del cuerpo residual k de K, definimos $ord(\alpha)$ para $\alpha \in D$ por la formula

$$|\alpha| = (1/q)^{ord(\alpha)}$$

Entonces ord extiende la valuación ord_K sobre K a D.Para cualquier subcuerpo L de D conteniendo a K, $[L : K] \leq n$ y por tanto $ord(L^\times) \subset n^{-1}\mathbb{Z}$. Además $ord(D^\times) \subset n^{-1}\mathbb{Z}$.

Sea

$$\mathcal{O}_D = \{\alpha \in D \mid ord(\alpha) \geq 0\}$$
$$\mathfrak{B} = \{\alpha \in D \mid ord(\alpha) > 0\}$$

$\mathcal{O}_D$ es un subanillo en D, llamado el anillo de enteros. Para cada subcuerpo L de D conteniendo a K, $\mathcal{O}_D \cap L = \mathcal{O}_L$ y por tanto $\mathcal{O}_D$ consiste de los elementos de D que son integrales sobre $\mathcal{O}_K$. Además $\mathfrak{B}$ es un ideal maximal a ambos lados en $\mathcal{O}_D$, y las potencias son los únicos ideales a ambos lados en D. Por tanto $\mathfrak{B}^e = \mathfrak{p}\mathcal{O}_D$ para algún e. Entonces $ord(D^\times) = e^{-1}\mathbb{Z}$, y por tanto $e \leq n$.

Claramente, los elementos de $\mathcal{O}_D$ que no están en $\mathfrak{B}$ son unidades. Por tanto, definimos $d = \mathcal{O}_D/\mathfrak{B}$ es un álgebra de división, y por tanto un cuerpo. Sea f su grado sobre k. Escribimos d como $d = k[a]$. Podemos levantar a a un elemento $\alpha \in \mathcal{O}_D$. Como $[K[\alpha] : K] \leq n$ tenemos que $f \leq n$.

El mismo argumento en el caso conmutativo muestra que $n^2 = ef$, $\mathcal{O}_D$ es un $\mathcal{O}_K$-módulo libre de algún rango m. Como $\mathcal{O}_D \otimes_{\mathcal{O}_K} K = D$, $m = n^2$. más aún, como $\mathcal{O}_D \otimes_{\mathcal{O}_K} k = \mathcal{O}_D/\mathfrak{p}\mathcal{O}_D$, es además libre de dimensión n^2 sobre k. Ahora consideramos la filtración de k-espacios vectoriales

$$\mathcal{O}_D \supset \mathfrak{B} \supset \mathfrak{B}^2 \supset ... \supset \mathfrak{B}^e = \mathfrak{p}\mathcal{O}_D.$$

De nuestra definición de f, $\mathcal{O}_D/\mathfrak{B} = d$ tiene dimensión f como k-espacio vectorial, los cocientes siguientes son de dimensión 1 como espacio vectorial sobre d. Por tanto $\mathcal{O}_D/\mathfrak{p}\mathcal{O}_D$ tiene dimensión ef sobre k, entonces $ef = n^2$.

Como $e \leq n$, $f \leq n$, la igualdad $ef = n^2$ implica que $e = f = n$. En particular, cada álgebra de división central diferente de K es ramificada. De vuelta, escribimos $d = k[a]$, y levantamos a a un elemento $\alpha \in D$. Entonces $K[\alpha]$ es un cuerpo con cuerpo residual d, y por tanto $[K[\alpha] : K] \geq [d : k] = n$. Por tanto $K[\alpha]$ tiene grado n sobre K y es no ramificado. Este es un subcuerpo maximal, y por tanto split en D. Tenemos que ver que

cada elemento de Br(K) es split por una extensión no ramificada, o sea, $Br(K)$ es igual a un subrgrupo de $Br(K^{un}/K)$.

Definimos el mapa

$$inv_K : Br(K) \to \mathbb{Q}/\mathbb{Z}.$$

Un elemento de $Br(K)$ es representado por un álgebra de división central D sobre K. De acuerdo a lo probado, existe un subcuerpo maximal L de D que es no ramificado sobre K. Sea σ el automorfismo de Frobenius de L. De acuerdo al Teorema de Noether-Skoelem, existe un elemento $\alpha \in D$ tal que $\sigma x = \alpha x \alpha^{-1} \forall x \in L$. Si α' además tiene esta propiedad, entonces $\alpha' = c\alpha$ para algún $c \in L$, y por tanto

$$ord(\alpha') = ord(c) + ord(\alpha) \equiv ord(\alpha) \bmod \mathbb{Z}.$$

Definimos

$$inv_K(D) = ord(\alpha) \bmod \mathbb{Z}$$

Esto depende solo de la clase de isomorfismo de D.

Observación 3.31. Sea L una extensión no ramificada de K de grado n, y sea σ el automorfismo de Frobenius de L/K, por tanto $G = \mathrm{Gal}(L/K) = \{\sigma^i \mid 0 \leq i \leq n-1\}$. Sea φ el 2-cociclo

$$\varphi(\sigma^i, \sigma^j) = \begin{cases} 1 \ si \ i+j \leq n-1 \\ \pi \ si \ i+j > n-1. \end{cases}$$

Donde π es un primo de K. El álgebra con producto cruzado $A(\varphi) = \bigoplus_{0 \leq i \leq n-1} Le_i$ con la multiplicación determinada por

$$e_i.a = \sigma^i a.e_i \, \forall a \in L$$

y

$$e_i e_j = \begin{cases} e_{i+j} \ si \ i+j \leq n-1 \\ \pi e_{i+j-n} \ si \ i+j > n-1. \end{cases}$$

Identificamos L con un subcuerpo de $A(\varphi)$ identificando e_0 con 1. Como $e_1 a e_1^{-1} = \sigma a \forall a \in L$, podemos usar e_1 para calcular el invariante de $A(\varphi)$. De acuerdo a las reglas de arriba, $e_1^n = e_{n-1}e_1 = \pi e_0 = \pi$. Por tanto

$$inv_K(A(\varphi)) = ord(e_1) = \frac{1}{n} ord(e_1^n) = \frac{1}{n} ord(\pi) = \frac{1}{n}$$

como era esperado.

Proposición 3.32. *El mapa $inv_K : Br(K) \to \mathbb{Q}/\mathbb{Z}$ define una biyección.*

Demostración. Sea L una extensión no ramificada de K de grado n (contenida en K^{al}), y sea l/k los cuerpos residuales correspondientes. Como el mapa norma $l \to k$, $l^\times \to k^\times$ son sobreyectivos, y U_L tiene una filtración cuyos cocientes son $l^\times$ 0 l, esto nos decía que el mapa norma de $U_L \to U_K$ es sobreyectivo. Por tanto, $H_T^0(G, U_L) = 0$, y esto implica que $H^2(G, U_L) = 0$. Para $L^\times = U_L \times \pi^{\mathbb{Z}}$ para algún primo $\pi \in K$

$$H^2(L/K) = H^2(G, \pi^{\mathbb{Z}}).$$

Consideremos la sucesión de cohomología de

$$0 \longrightarrow \mathbb{Z} \longrightarrow \mathbb{Q} \longrightarrow \mathbb{Q}/\mathbb{Z} \longrightarrow 0$$

muestra que $H^2(G, \pi^{\mathbb{Z}}$ es cíclico de orden n y es generado por la clase del cociclo φ considerado en el ultimo ejemplo. Por tanto, $Br(L/K)$ es cíclico de orden n, y es generado por $[A(\varphi)]$. Esto dice que $inv_K : Br(K^{un}/K) \to \mathbb{Q}/\mathbb{Z}$ es un isomorfismo, y por lo visto arriba $Br(K^{un}/K) = Br(K^{al}/K)$. □

Observación 3.33.

1. El cálculo del ultimo ejemplo muestra que el mapa invariante definido en esta sección coincide con el definido en la sección anterior usando cohomología. En particular, esto muestra que el mapa es un homomorfismo.
2. El cálculo del ejemplo muestra que $inv_K(A(\varphi^i)) = \frac{1}{n} \bmod \mathbb{Z}$. supongamos que i es coprimo a n, entonces $A(\varphi^i)$ es un álgebra de división central. Si no, entonces $(A(\varphi^i)) \sim M_r(D)$ para algún álgebra de división central D de grado m^2 para algún $m < n$, y $inv_K(A(\varphi^i)) = inv_K(D) \in \frac{1}{m}\mathbb{Z}/\mathbb{Z}$, lo cual es una contradicción. Se sigue cada álgebra de división central sobre K es isomorfa para exactamente un álgebra de división de la forma $A(\varphi^i)$ para algún $n \geq 1$ y algún i coprimo a n. En particular, para un álgebra de división central D, el orden de [D] en Br(K) es $\sqrt{[D : K]}$.
3. Sea D un álgebra de división central de grado n^2 sobre K. Como el mapa $Br(K) \to Br(L)$ multiplica al invariante por $[L : K]$, D es split para toda extensión L de K de grado n. Por tanto cada L puede ser metido en D. En otras palabras, todo polinomio irreducible en K[X] de grado n tiene una raíz en D.

Capítulo 2

Teoría de cuerpo de clases global

En este capítulo, enunciaremos y explicaremos algunos resultados importantes de la teoría de cuerpos global. Fijemos algunas cosas antes de comenzar, definiremos un primo de K como una clase de equivalencia de valores absolutos no triviales en K. Hay dos tipos de primos, los primos finitos, que pueden ser identificados con los ideales primos de O_K, y los primos infinitos. Un primo infinito real puede ser identificado con una inmersión de $K \hookrightarrow \mathbb{R}$, y uno complejo con un par de inmersiones conjugadas de $K \hookrightarrow \mathbb{C}$. Usaremos $\mathfrak{p}$ o v para denotar un primo, finito o infinito. Usaremos S para denotar un conjunto finito de primos de K. S_∞ para los primos infinitos.

La completación de K para un primo $\mathfrak{p}$ es denotada por $K_\mathfrak{p}$, y la inclusión $K \hookrightarrow K_\mathfrak{p}$ es denotada por $a \mapsto a_\mathfrak{p}$.

1. Ray Class Group

Sea $I = I_K$ el grupo de ideales fraccionales en K. Para un conjunto finito S de primos de K, definimos I^S el subgrupo de I generado por los ideales primos que no están en S. Cada elemento $\mathfrak{a}$ de I^S se factoriza de manera única como

$$\mathfrak{a} = \prod \mathfrak{p}_i^{n_i},\ \mathfrak{p}_i \notin S,\ n_i \in \mathbb{Z}$$

y por tanto I^S puede ser identificado con el grupo abeliano libre generado por los ideales primos que no están en S. Definimos

$$K^S = \{a \in K^\times \mid (a) \in I^S\} = \{a \in K^\times \mid ord_\mathfrak{p}(a) = 0\ \forall \mathfrak{p} \in S \text{ finitos }\}.$$

Sea $i : K^S \to I^S$ el mapa que manda un elemento $a \in K^S$ en el ideal $a\mathcal{O}_K$.

Por ejemplo, si $K = \mathbb{Q}$ y S es el conjunto de primos dividiendo un entero n, I^S es el conjunto de ideales fraccionales

$$\{(r/s) \mid r, s \in \mathbb{Z},\ mcd(r, n) = 1 = mcd(s, n)\}$$

y

$$\mathbb{Q}^S = \{r/s \mid r, s \in \mathbb{Z},\ mcd(r, n) = 1 = mcd(s, n)\}.$$

En este caso, el mapa natural $\mathbb{Q}^S \to I^S$ es sobreyectivo con kernel $\{\pm 1\}$.

Lema 1.1. *Para todo conjunto finito S de ideales primos en $\mathcal{O}_K$, la sucesión*

$$0 \to U_K \to K^S \to I^S \to C \to 0$$

es exacta, donde $U_K = \mathcal{O}_K^\times$ y $C = \frac{I}{i(K^\times)}$

Demostración. Para ver que $I^S \to C$ es sobreyectivo, tenemos que ver que cada clase de ideales de C es representada por un ideal en I^S. Sea $\mathfrak{a} \in C$. Entonces $\mathfrak{a} = \mathfrak{b}\mathfrak{c}^{-1}$ con $\mathfrak{b}$ y $\mathfrak{c}$ ideales integrales, y para algún $c \in \mathfrak{c}$, $\mathfrak{a}(c) = \mathfrak{b}.\mathfrak{c}^{-1}.(c)$ es integral, y por tanto

podemos suponer que $\mathfrak{a}$ es un ideal integral. Escribimos $a = \prod_{\mathfrak{p}\in S} \mathfrak{p}^{n(\mathfrak{p})}\mathfrak{b}$, donde $\mathfrak{b} \in I^S$. Para cada $\mathfrak{p} \in S$, elegimos un $\pi_\mathfrak{p} \in \mathfrak{p} \setminus \mathfrak{p}^2$, por tanto $ord_\mathfrak{p}(\pi_\mathfrak{p}) = 1$. Por el teorema chino de los restos, existe un $a \in \mathcal{O}_K$ tal que

$$a \equiv \pi_\mathfrak{p}^{n(\mathfrak{p})} \bmod \mathfrak{p}^{n(\mathfrak{p})+1} \, \forall \mathfrak{p} \in S.$$

Estas congruencias implican que $ord_\mathfrak{p}(a) = n(\mathfrak{p})$ para todo $\mathfrak{p} \in S$, y por tanto $(a) = \prod_{\mathfrak{p}\in S} \mathfrak{p}^{n(\mathfrak{p})}\mathfrak{b}'$ con $\mathfrak{b}' \in I^S$. Ahora $a^{-1}\mathfrak{a} \in I^S$ y representa la misma clase que $\mathfrak{a}$ en C.

Siguiendo, si $\mathfrak{a} \in I^S$ es mandado en el elemento trivial en C, entonces $\mathfrak{a} = (\alpha)$ para algún $\alpha \in K^S$, y α es único a menos de unidades. Esto prueba que la sucesión es exacta. □

Observación 1.2. Toda clase en C es representada por un ideal integral $\mathfrak{a} \in I^S$: supongamos que la clase es representada por $\mathfrak{a} \in I^S$, escribimos $\mathfrak{a} = \mathfrak{b}\mathfrak{c}^{-1}$ con $\mathfrak{b}, \mathfrak{c}$ ideales integrales en I^S, elegimos un $c \in \mathfrak{c} \cap K^S$ no nulo, notemos que $c\mathfrak{a}$ es integral.

Definición 1.3. Un módulo para K es una función

$$m : \{\text{primos de K}\} \to \mathbb{Z}$$

tal que

1. $m(\mathfrak{p}) \geq 0 \, \forall \mathfrak{p}$, y $m(\mathfrak{p}) = 0$ para todo primo menos una cantidad finita,
2. Si $\mathfrak{p}$ es real, entonces $m(\mathfrak{p}) = 0$ o 1,
3. Si $\mathfrak{p}$ es complejo entonces $m(\mathfrak{p}) = 0$.

Usualmente escribiremos

$$\mathfrak{m} = \prod_\mathfrak{p} \mathfrak{p}^{m(\mathfrak{p})}.$$

Un módulo $\mathfrak{m} = \prod \mathfrak{p}^{m(\mathfrak{p})}$ se dice que divide a un módulo $\mathfrak{n} = \prod \mathfrak{p}^{n(\mathfrak{p})}$ si $m(\mathfrak{p}) \leq n(\mathfrak{p})$ para todo $\mathfrak{p}$. En particular, un primo $\mathfrak{p}$ divide a un módulo $\mathfrak{m}$ si y solo si $\mathfrak{m}(\mathfrak{p}) > 0$.

Un módulo $\mathfrak{m}$ puede ser escrito como

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

donde $\mathfrak{m}_\infty$ es un producto de primos reales y $\mathfrak{m}_0$ es producto de potencias positivas de ideales primos, y por tanto puede ser identificado con un ideal en $\mathcal{O}_K$.

1.1. Definición de Ray Class Group. Para un módulo $\mathfrak{m}$, definimos $K_{\mathfrak{m},1}$ como el conjunto de los $a \in K^\times$ tal que

$$\begin{cases} ord_\mathfrak{p}(a-1) \geq m(\mathfrak{p}) \text{ para todo } \mathfrak{p} \text{ finito dividiendo } \mathfrak{m} \\ a_\mathfrak{p} > 0 \text{ para todo primo real dividiendo } \mathfrak{m} \end{cases}$$

Notar que

$$ord_\mathfrak{p}(a-1) \geq m(\mathfrak{p}) \Leftrightarrow \pi^{m(\mathfrak{p})} \mid (a_\mathfrak{p} - 1) \Leftrightarrow a \mapsto 1 \text{ en } (\mathcal{O}_\mathfrak{p}/\mathfrak{p}^{m(\mathfrak{p})}\times) \simeq (\widehat{\mathcal{O}}_\mathfrak{p}/\widehat{\mathfrak{p}}^{m(\mathfrak{p})\times})$$

donde π es un primo en $K_\mathfrak{p}$ de K para $\mathfrak{p}$.

Sea $S(\mathfrak{m}) = \{\text{primos dividiendo } \mathfrak{m}\}$. Para cualquier $a \in K_{\mathfrak{m},1}$ y un ideal primo $\mathfrak{p}$ dividiendo $\mathfrak{m}$, $ord_\mathfrak{p}(a-1) > 0 = ord_\mathfrak{p}(1)$, y por tanto

$$ord_\mathfrak{p}(a) = ord_\mathfrak{p}((a-1)+1) = 0.$$

Por tanto, para todo $a \in K_{\mathfrak{m},1}$, el ideal (a) se encuentra en $I^{S(\mathfrak{m})}$. Sea i el mapa $a \mapsto (a) : K_{m,1} \to I^{S(\mathfrak{m})}$. El cociente

$$C_{\mathfrak{m}} = I^{S(\mathfrak{m})}/i(K_{m,1})$$

es llamado el **Ray class group del módulo** $\mathfrak{m}$.

Ejemplo 1.4. Sea $\mathfrak{m} = (2)^3.(17)^2.(19).\infty$ es un módulo para $\mathbb{Q}$ tal que $\mathfrak{m}_0 = (2)^3.(17)^2.(19)$ y $\mathfrak{m}_\infty = \infty$. Más aún, $\mathbb{Q}_{\mathfrak{m},1}$ consiste de los racionales positivos a tales que

$$\begin{cases} ord_2(a-1) \geq 3 \\ ord_{17}(a-1) \geq 2 \\ ord_{19}(a-1) \geq 1. \end{cases}$$

La condición sobre 2 nos dice que a es el cociente de dos enteros impares, $a = b/c$, y que la imagen de a bc^{-1} en $(\mathbb{Z}/8\mathbb{Z})^\times$ es 1. Las otras condiciones pueden ser expresadas de manera similar.

Lema 1.5. *Sea S un conjunto finito de ideales primos de K. Entonces cada elemento $\alpha \in K^S$ puede ser escrito como $\alpha = a/b$ con $a, b \in \mathcal{O}_K \cap K^S$*

Demostración. Como $\alpha \in K^S, (\alpha) = \mathfrak{a}/\mathfrak{b}$ con $\mathfrak{a}, \mathfrak{b}$ ideales integrales está en I^S. Claramente $\mathfrak{a}, \mathfrak{b}$ representan el mismo elemento $\mathcal{C}$ en el grupo de clases de ideales, y de acuerdo con la Observación 1.2 podemos elegir un ideal integral $\mathfrak{c} \in I^S$ para representar $\mathcal{C}^{-1}$. Ahora $(\alpha) = \mathfrak{ac}/\mathfrak{bc} = (a)/(b)$ para algún $a, b \in \mathcal{O}_K \cap K^S$ □

Proposición 1.6. *Toda clase en $C_{\mathfrak{m}}$ es representada por un ideal integral $\mathfrak{a}$, y dos ideales integrales $\mathfrak{a}$ y $\mathfrak{b}$ representan la misma clase en $C_{\mathfrak{m}}$ si y solo si existen $a, b \in \mathcal{O}_K$ tal que $a\mathfrak{a} = b\mathfrak{b}$ y*

$$a \equiv b \equiv 1 \; mod\, \mathfrak{m}_0$$

a y b tienen el mismo signo para todo primo real dividiendo $\mathfrak{m}$

Demostración. Supongamos que la clase es representada por $\mathfrak{a} \in I^S$, y sea $\mathfrak{a} = \mathfrak{bc}^{-1}$ con $\mathfrak{a}, \mathfrak{b}$ son ideales integrales en I^S. El teorema chino de los restos muestra que existe un $c \in \mathfrak{c} \cap K_{\mathfrak{m}_0,1}$ no nulos, y por el teorema de aproximación fuerte nos muestra que c puede ser elegido > 0 para todos los primos reales. Ahora $c\mathfrak{a}$ es integral y representa la misma clase $\mathfrak{a}$ en $C_{\mathfrak{m}}$. La segunda parte del enunciado se sigue del Lema 1.5 □

Observación 1.7. El grupo de clases de ideales puede ser identificado con el conjunto de ideales integrales módulo la relación equivalencia: $\mathfrak{a} \sim \mathfrak{b}$ si y solo si $a\mathfrak{a} = b\mathfrak{b}$ para algún $a, b \in \mathcal{O}_K$ no nulos.

Teorema 1.8. *Para cada módulo $\mathfrak{m}$ de K, existe una sucesión exacta*

$$0 \to U/U_{\mathfrak{m},1} \to K_{\mathfrak{m}}/K_{\mathfrak{m},1} \to C_{\mathfrak{m}} \to C \to 0$$

y isomorfismos canónicos

$$K_{\mathfrak{m}}/K_{\mathfrak{m},1} \simeq \prod_{\mathfrak{p} \mid \mathfrak{m}\, \mathfrak{p}\ reales} \{\pm\} \times \prod_{\mathfrak{p} \mid \mathfrak{m}\, \mathfrak{p}\ finitos} (\mathcal{O}_K/\mathfrak{p}^{m(\mathfrak{p})})^\times \simeq \prod_{\mathfrak{p} \mid \mathfrak{m}\, \mathfrak{p}\ reales} \{\pm\} \times (\mathcal{O}_K/\mathfrak{m}_0)^\times$$

donde

$$K_{\mathfrak{m}} = K^{S(\mathfrak{m})} = \{\alpha \in K^\times \mid ord_{\mathfrak{p}}(\alpha) = 0 \; \forall \mathfrak{p} \mid \mathfrak{m}\}$$

$$U = \mathcal{O}_K^\times, \text{ grupo de las unidades en } K$$
$$U_{\mathfrak{m},1} = U \cap K_{\mathfrak{m},1}$$

Por tanto, $C_\mathfrak{m}$ es un grupo de orden finito

$$h_\mathfrak{m} = h * [U : U_{\mathfrak{m},1}]^{-1} * 2^{r_0} * Nm(\mathfrak{m}_0) * \prod_{\mathfrak{p} \mid \mathfrak{m}_0} (1 - \frac{1}{Nm(\mathfrak{p})}),$$

donde r_0 es el número de primos reales que dividen a $\mathfrak{m}$ y h es el número de clases de ideales de K (orden de C, el grupo de clases de ideales).

Demostración. La inclusión $I^{S(\mathfrak{m})} \hookrightarrow I$ define un homorfismo $C_\mathfrak{m} \to C$. Considerando el par de mapas

$$K_{\mathfrak{m},1} \xrightarrow{f} K_\mathfrak{m} \xrightarrow{g} I^{S(\mathfrak{m})}.$$

De acuerdo al Lema 1.1, el kernel y cokernel de g son U y C respectivamente. El cokernel de $g \circ f$ es $C_\mathfrak{m}$ y su kernel es $K_{\mathfrak{m},1} \cap U = U_{\mathfrak{m},1}$. Finalmente, f es inyectivo. Por tanto, la sucesión de kernel-cokernel de el par de mapas es

$$0 \to U_{\mathfrak{m},1} \to U \to K_\mathfrak{m}/K_{\mathfrak{m},1} \to C_\mathfrak{m} \to C \to 0.$$

Ahora demostraremos que $K_\mathfrak{m}$ es canónicamente isomorfo al grupo dado. Sea $\mathfrak{p}$ un primo dividiendo $\mathfrak{m}$. Si $\mathfrak{p}$ es real, asignamos $\alpha \in K_\mathfrak{m}$ al signo de $\alpha_\mathfrak{p}$ (recordando que un primo real es una inmersión $K \hookrightarrow \mathbb{R}$, y que $\alpha \mapsto \alpha_\mathfrak{p}$). Si $\mathfrak{p}$ es un primo finito, es decir es un ideal primo de $\mathcal{O}_K$, entonces mandamos $\alpha \in K_\mathfrak{m}$ en $[a][b]^{-1} \in (\mathcal{O}_K/\mathfrak{p}^{m(\mathfrak{p})})^\times$, donde a,b son los del lema. Como a y b son coprimos a $\mathfrak{p}$, sus clases [a] y [b] en $\mathcal{O}_K/\mathfrak{p}^{m(\mathfrak{p})}$ son invertibles, por tanto esto tiene sentido. El teorema de aproximación débil muestra que el mapa $K_\mathfrak{m} \to \prod\{\pm\} \times \prod(\mathcal{O}_K/\mathfrak{p}^{m(\mathfrak{p})})$ es sobreyectivo, y su kernel es $K_{\mathfrak{m},1}$.

El teorema chino de los restos nos da el isomorfismo de anillos

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

y por tanto el isomorfismo de grupos

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

Esto completa la prueba del isomorfismo.

Ahora resta calcular el orden de los grupos. Notar que $\mathcal{O}_K/\mathfrak{p}^m$ es un anillo local con ideal maximal $\mathfrak{p}/\mathfrak{p}^m$, y las unidades son los elementos que no están en $\mathfrak{p}/\mathfrak{p}^m$. La filtración

$$(\mathcal{O}_K/\mathfrak{p}^m)^\times \subset (1+\mathfrak{p})/\mathfrak{p}^m \subset \cdots \subset (1+\mathfrak{p}^{m-1})/\mathfrak{p}^m \subset 0$$

tiene cocientes isomorfos a

$$k^\times, k, \cdots, k,\ k \overset{\text{def}}{=} \mathcal{O}_K/\mathfrak{p}$$

y por tanto $(\mathcal{O}_K/\mathfrak{p}^m)^\times$ tiene orden $(q-1)q^{m-1}$ con $q = [\mathcal{O}_K, \mathfrak{p}] \overset{\text{def}}{=} Nm(\mathfrak{p})$. Esto muestra que

$$[C_\mathfrak{m} : 1] = [C : 1].[K_\mathfrak{m} : K_{\mathfrak{m},1}].[U_\mathfrak{m} : U_{\mathfrak{m},1}]^{-1}$$

es igual a la expresión del enunciado del teorema. □

Ejemplo 1.9.

1. Si $\mathfrak{m} = 1$, entonces $C_{\mathfrak{m}} = C$.
2. Cuando $\mathfrak{m}$ es producto de primos reales, $C_{\mathfrak{m}}$ es el Narrow class group y la sucesión exacta es

$$0 \to U/U_+ \to K^\times/K_+ \to C_{\mathfrak{m}} \to C \to 1$$

donde K_+ es el grupo de elementos positivos, U_+ es el grupo de todas las unidades positivas. Más aún, $K^\times/K_+ \simeq \prod_{\text{preales}}\{\pm\}$, y por tanto el kernel de $C_{\mathfrak{m}} \to C$ es el conjunto de posibles signos módulo los que vienen de las unidades.

Para $\mathbb{Q}$, el Narrow class group es trivial. Para $\mathbb{Q}[\sqrt{d}]$, $d > 0$, hay dos primos reales y $U = \{\pm\epsilon^m \mid m \in \mathbb{Z}\} \simeq (\mathbb{Z}/2\mathbb{Z}) \times \mathbb{Z}$, donde ϵ es una unidad fundamental. Sea $\bar{\epsilon}$ el conjugado de ϵ. Entonces $h_{\mathfrak{m}} = 2h$ *o* h dependiendo de si $\epsilon\, y\, \bar{\epsilon}$ tienen el mismo signo o diferente. Notar que $Nm(\epsilon) = +1$ si los signos son iguales, y -1 si son diferentes. Para algunos valores de d tenemos

(1)

d	h	ϵ	$Nm(\epsilon)$
2	1	$1+\sqrt{2}$	-1
3	1	$2+\sqrt{3}$	1
5	1	$(1+\sqrt{5})/2$	-1
6	1	$5+2\sqrt{6}$	1

Por tanto $\mathbb{Q}[\sqrt{3}]$ y $\mathbb{Q}[\sqrt{6}]$ tienen número de clases 1 y número de clases narrow 2, mientras que para $\mathbb{Q}[\sqrt{2}]$ y $\mathbb{Q}[\sqrt{5}]$ ambos números de clases son 1.
3. Para el cuerpo $\mathbb{Q}$ y el módulo (m), la sucesión se convierte en

$$0 \to \{\pm 1\} \to (\mathbb{Z}/m\mathbb{Z})^\times \to C_{\mathfrak{m}} \to 0.$$

Para el módulo $\infty(\mathfrak{m})$, la sucesión se convierte en

$$0 \to \{\pm 1\} \to \{\pm\} \times (\mathbb{Z}/m\mathbb{Z})^\times \to C_{\mathfrak{m}} \to 0.$$

1.2. El elemento de Frobenius. Sea K un cuerpo de números, y sea L una extensión Galois finita sobre K con grupo G. Sea $\mathfrak{p}$ un ideal de K, y sea $\mathfrak{B}$ un ideal de L sobre $\mathfrak{p}$. El grupo de descomposición $D(\mathfrak{B})$ es definido por

$$\{\tau \in G \mid \tau\mathfrak{B} = \mathfrak{B}\}.$$

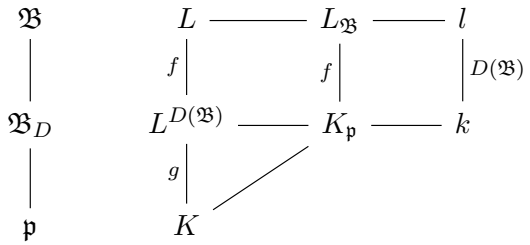
Equivalentemente, es el conjunto de elementos de G que cuya acción es continua para la topología $\mathfrak{B}$-ádica, y por tanto extiende a la completación de $L_{\mathfrak{B}}$. De esta forma obtenemos un isomorfismo

$$D(\mathfrak{B}) \to \mathrm{Gal}(L_{\mathfrak{B}}/K_{\mathfrak{p}}).$$

Asumamos $\mathfrak{B}$ es no ramificado sobre $\mathfrak{p}$. Entonces la acción de $\mathrm{Gal}(L_{\mathfrak{B}}/K_{\mathfrak{p}})$ en $\mathcal{O}_L$ induce un isomorfismo

$$\mathrm{Gal}(L_{\mathfrak{B}}/K_{\mathfrak{p}}) \to \mathrm{Gal}(l/k)$$

donde l y k son los cuerpos residuales.



El grupo Gal(l/k) es cíclico con un generador canónico, el elemento de Frobenius $x \mapsto x^q$, donde $q = |k|$. Por tanto $D(\mathfrak{B})$ es cíclico, y el generador corresponde al elemento de Frobenius en Gal(l/k) es llamado el elemento de Frobenius $(\mathfrak{B}, L/K)$ para $\mathfrak{B}$. Este es el único elemento $\sigma \in \text{Gal}(L/K)$ que satisface las siguientes condiciones

1. $\sigma \in D(\mathfrak{B})$, o sea, $\sigma\mathfrak{B} = \mathfrak{B}$;
2. $\forall \alpha \in \mathcal{O}_L$, $\sigma\alpha \equiv \alpha^q \ (mod\, \mathfrak{B})$ con el q anterior.

Veamos algunas propiedades básicas de $(\mathfrak{B}, L/K)$

Observación 1.10. Sea $\tau\mathfrak{B}$ otro primo dividiendo a $\mathfrak{p}$. Entonces tenemos $D(\tau\mathfrak{B}) = \tau D(\mathfrak{B})\tau^{-1}$, y

$$(\tau\mathfrak{B}, L/K) = \tau(\mathfrak{B}, L/K)\tau^{-1}$$

Demostración. Si $\rho \in D(\mathfrak{B})$, entonces

$$\tau\rho\tau^{-1}(\tau\mathfrak{B}) = \tau\rho\mathfrak{B} = \tau\mathfrak{B}$$

y por tanto $\tau\rho\tau^{-1} \in D(\tau\mathfrak{B})$. Entonces $\tau D(\mathfrak{B})\tau^{-1} \subset D(\tau\mathfrak{B})$, y tienen el mismo orden, pro tanto son iguales.

Sea $\alpha \in \mathcal{O}_L$ y sea $\sigma = (\mathfrak{B}, L/K)$; entonces

$$\tau\sigma\tau^{-1}(\alpha) = \tau((\tau^{-1}\alpha)^q + a), \text{ para algún } a \in \mathfrak{B}, \ y$$

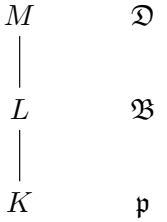
$$\tau((\tau^{-1}\alpha)^q + a) = \alpha^q + \tau\alpha \equiv \alpha^q \ (mod \tau\mathfrak{B})$$

Como G actúa transitivamente sobre los primos dividiendo $\mathfrak{p}$, esto implica que

$$\{(\mathfrak{B}, L/L) \mid \mathfrak{B} \mid \mathfrak{p}\}$$

es una clase de conjugación en G, la cual notaremos como $(\mathfrak{p}, L/K)$. Cuando L/K es abeliano, $(\mathfrak{p}, L/K)$ contiene un único elemento, este es un elemento de Gal(L/K). □

Observación 1.11. Consideremos una torre de cuerpos



y asumamos que $\mathfrak{D}$ es no ramificado sobre $\mathfrak{p}$; entonces

$$(\mathfrak{D}, M/L) = (\mathfrak{D}, M/K)^{f(\mathfrak{B}/\mathfrak{p})}.$$

DEMOSTRACIÓN. Sea $k(\mathfrak{D}) \supset k(\mathfrak{B}) \supset k(\mathfrak{p})$ la torre de cuerpos residuales. Entonces $f(\mathfrak{B}/\mathfrak{p}) = [k(\mathfrak{B}) : k(\mathfrak{p})]$, y el elemento de Frobenius en $\mathrm{Gal}(k(\mathfrak{D})/k(\mathfrak{B}))$ es la $f(\mathfrak{B}/\mathfrak{p})$-ésima potencia de el Frobenius de $Galf(k(\mathfrak{D})/k(\mathfrak{p}))$. □

OBSERVACIÓN 1.12. Si en la observación anterior L es Galois sobre K, entonces

$$(\mathfrak{D}, M/K) \mid L = (\mathfrak{B}, L/K).$$

2. Principales resultados de CFT en términos de ideales

Sea L/K una extensión Galois abeliana finita de grupo G.

Para todo conjunto finito S de primos de K conteniendo a todos los primos ramificados en L, tenemos el siguiente homomorfismo

$$\Psi_{L/K} : I^S \to \mathrm{Gal}(L/K) \mid \mathfrak{p}_1{}^{n_1} \cdots \mathfrak{p}_t{}^{n_t} \mapsto \prod (\mathfrak{p}_i, L/K)^{n_i}$$

llamado el mapa global de Artin(o mapa de reciprocidad).

EJEMPLO 2.1. Sea $K = \mathbb{Q}[\sqrt{m}]$ donde m es libre de cuadrados. El conjunto S de primos finitos que ramifican en K consiste de los primos que dividen m si $m \equiv 1 \pmod 4$ y los primos que dividen a m y 2 en otro caso. Identificamos $\mathrm{Gal}(K/\mathbb{Q}) \simeq \{\pm 1\}$. El mapa de Artin es el homomorfismo determinado por

$$p \mapsto \left(\frac{m}{p}\right) : I^S \to \mathrm{Gal}(K/\mathbb{Q})$$

donde $\left(\frac{m}{p}\right)$ es el símbolo de Legendre.

EJEMPLO 2.2. Sea $L = \mathbb{Q}[\zeta_m]$, donde ζ_m es una m-ésima raíz de la unidad. Asumamos que m es impar o divisible por 4 (o sea que los primos que ramifican en L son los primos que dividen a m). El mapa que envía un entero n coprimo con m al automorfismo $\zeta \mapsto \zeta^n$ de L define un isomorfismo $(\mathbb{Z}/m\mathbb{Z})^\times \to \mathrm{Gal}(L/\mathbb{Q})$. Para p no dividiendo a n, $(p, L/K) = [p]$. Si r y s son enteros positivos coprimos a m, entonces r/s define una clase $[r/s] = [r][s]^{-1} \in (\mathbb{Z}/m\mathbb{Z})^\times$, y el mapa de Artin es la composición de

$$I^S \xrightarrow{(r/s)\mapsto[r/s]} (\mathbb{Z}/m\mathbb{Z})^\times \xrightarrow{[n]\mapsto(\zeta\mapsto\zeta^n)} \mathrm{Gal}(L/\mathbb{Q}).$$

PROPOSICIÓN 2.3. *Sea L una extensión abeliana de K, y sea K' un cuerpo intermedio, o sea, $L \supset K' \supset K$. Entonces el siguiente diagrama conmuta*

$$\begin{array}{ccc} I^S_{K'} & \xrightarrow{\Psi_{L/K'}} & Gal(L/K^\times) \\ \downarrow Nm & & \downarrow \\ I^S_K & \xrightarrow{\Psi_{L/K}} & Gal(L/K) \end{array}$$

Donde S es algún conjunto finito de ideales primos de K en el cual están contenidos todos los primos que ramifican en L, y además el conjunto de primos de K' sobre primos de S.

DEMOSTRACIÓN. Sea $\mathfrak{p}'$ un ideal primo de K' sobre un ideal primo $\mathfrak{p}$ de K que no esta en S. Entonces $Nm_{K'/K}(\mathfrak{p}') = \mathfrak{p}^{f(\mathfrak{p}'/\mathfrak{p})}$, y tenemos que ver que $\Psi_{L/K'}(\mathfrak{p}') = \Psi_{L/K}(\mathfrak{p}^{f(\mathfrak{p}'/\mathfrak{p})})$, es decir, que $(\mathfrak{B}, L/K') = (\mathfrak{B}, L/K)^{f(\mathfrak{p}'/\mathfrak{p})}$ para cada ideal primo $\mathfrak{B}$ de L sobre $\mathfrak{p}$. Pero esto ya fue probado. □

COROLARIO 2.4. *Para toda extensión abeliana finita L de K, $Nm_{L/K}(I_L^S)$ esta contenido en el kernel de $\Psi_{L/K} : I^S \to Gal(L/K)$.*

DEMOSTRACIÓN. Tomar $K' = L$ en el diagrama anterior. □

Por tanto el mapa de Artin induce un homomorfismo

$$\Psi_{L/K} : I_K^S/Nm(I_L^S) \to \mathrm{Gal}(L/K)$$

donde L/K es una extensión abeliana finita. El grupo $I^S/Nm(I_L^S)$ es infinito (porque infinitos primos no descomponen), y por tanto $\Psi_{L/K}$ no puede ser inyectivo.

Sea S un conjunto finito de primos de K. Diremos que un homomorfismo $\Psi : I^S \to G$ admite un módulo si existe un módulo $\mathfrak{m}$ con $S(\mathfrak{m}) \supset S$ tal que $\Psi(i(K_{m,1})) = 0$. Por tanto Ψ admite un módulo si y solo factoriza por $C_{\mathfrak{m}}$ para algún $\mathfrak{m}$ con $S(\mathfrak{m}) \supset S$.

TEOREMA 2.5. *(Ley de Reciprocidad)*
Sea L una extensión abeliana finita de K, y sea S el conjunto de primos de K que ramifican en L. Entonces el mapa de Artin $\Psi : I^S \to Gal(L/K)$ admite un módulo $\mathfrak{m}$ con $S(\mathfrak{m}) = S$, y esto define un isomorfismo

$$I_K^{S(\mathfrak{m})}/i(K_{\mathfrak{m},1}).Nm(I_L^{S(\mathfrak{m})}) \to Gal(L/K).$$

Un módulo como el del teorema es llamado un módulo de definición para L.

Escribimos $I_K^{\mathfrak{m}}$ el grupo de $S(\mathfrak{m})$-ideales en K, y $I_L^{\mathfrak{m}}$ para el grupo de $S(\mathfrak{m})'$-ideales en L, donde $S(\mathfrak{m})'$ son los primos sobre en L sobre los primos en $S(\mathfrak{m})$. Llamamos a un subgrupo H de $I_K^{\mathfrak{m}}$ un subgrupo de congruencia módulo $\mathfrak{m}$ si

$$I_K^{\mathfrak{m}} \supset H \supset i(K_{\mathfrak{m},1}).$$

TEOREMA 2.6. *(Teorema de existencia)*
Dado un subgrupo de congruencia módulo $\mathfrak{m}$, existe una extensión abeliana finita L/K, no ramificada sobre todos los primos que no dividen a $\mathfrak{m}$ con $H = i(K_{\mathfrak{m},1}).Nm_{L/K}(I_L^{\mathfrak{m}})$.

Notar que para H y L como en el teorema, el mapa de Artin $\Psi_{L/K}$ induce un isomorfismo

$$I^{S(\mathfrak{m})}/H \to \mathrm{Gal}(L/K).$$

En particular, para cada módulo $\mathfrak{m}$ existe un cuerpo $L_{\mathfrak{m}}$, llamado el Ray class field módulo $\mathfrak{m}$ tal que el mapa de Artin define un isomorfismo $C_{\mathfrak{m}} \to \mathrm{Gal}(L_{\mathfrak{m}}/k)$. Para un cuerpo $L \subset L_{\mathfrak{m}}$, tenemos

$$Nm(C_{L,\mathfrak{m}}) = i(K_{\mathfrak{m},1}).Nm(I_L^{\mathfrak{m}}) \bmod i(K_{\mathfrak{m},1}).$$

COROLARIO 2.7. *Dado un módulo $\mathfrak{m}$. Entonces el mapa $L \mapsto Nm(C_{L,\mathfrak{m}})$ es una biyección de el conjunto de extensiones abelianas contenidas en $L_{\mathfrak{m}}$ y los subgrupos de $C_{\mathfrak{m}}$. Más aún,*

$$L_1 \subset L_2 \Leftrightarrow Nm(C_{L_1,\mathfrak{m}}) \supset Nm(C_{L_2,\mathfrak{m}});$$
$$Nm(C_{L_1.L_2.\mathfrak{m}}) = Nm(C_{L_1,\mathfrak{m}}) \cap Nm(C_{L_2,\mathfrak{m}});$$

$$Nm(C_{L_1\cap L_2,\mathfrak{m}}) = Nm(C_{L_1}).Nm(C_{L_2,\mathfrak{m}}).$$

Observación 2.8. Sea L/K una extensión con grupo de Galois G. De acuerdo con la ley de reciprocidad, existe un módulo $\mathfrak{m}$ con soporte el conjunto de primos de K que ramifican en L tal que el mapa de Artin $\Psi_{L/K} : I^{S(\mathfrak{m})} \to G$ toma valor 1 en $i(K_{\mathfrak{m},1})$. Considerando el mapa dado por el Teorema 1.8

$$(\mathcal{O}_K/\mathfrak{p}^{m(\mathfrak{p})})^\times \hookrightarrow K_{\mathfrak{m}}/K_{\mathfrak{m},1} \xrightarrow{i} C_{\mathfrak{m}} \xrightarrow{\Psi_{L/K}} G.$$

Tenemos un entero $\mathfrak{f}(\mathfrak{p}) \leq m(\mathfrak{p})$ tal que este mapa factoriza por $(\mathcal{O}_K/\mathfrak{p}^{\mathfrak{f}(\mathfrak{p})\times})$. El módulo $\mathfrak{f}(L/K) = \mathfrak{m}_\infty \prod \mathfrak{p}^{\mathfrak{f}(\mathfrak{p})}$ es entonces el módulo mas chico tal que $\Psi_{L/K}$ factoriza por C_f, este es llamado el conductor de L/K. El conductor $f(L/K)$ es divisible por exactamente los primos que ramifican en L.

Los subcuerpos de el Ray Class field $L_{\mathfrak{m}}$ conteniendo K son los que tienen conductor $\mathfrak{f} \mid \mathfrak{m}$. Toda extensión abeliana de K esta contenida en $L_{\mathfrak{m}}$ para algún $\mathfrak{m}$.

Ejemplo 2.9. El Ray class group para el módulo $\mathfrak{m} = 1$ es el grupo de clases de ideales, y el Ray class field correspondiente es el Hilbert class field; esta es la extensión abeliana maximal de K que es no ramificada para todos los primos, incluyendo los primos reales. Por ejemplo, el Hilbert class field de $\mathbb{Q}$ es $\mathbb{Q}$ (porque tiene número de clases 1). El Hilbert class field de $\mathbb{Q}[\sqrt{-5}]$ es $\mathbb{Q}[\sqrt{-1}, \sqrt{-5}]$, 2 y 5 ramifican en $\mathbb{Q}[\sqrt{-1}]$ y solo 5 ramifica en $\mathbb{Q}[\sqrt{5}]$, de esto se sigue que los primos de $\mathbb{Q}[\sqrt{-5}]$ dividiendo 2 y 5 no ramifica en $\mathbb{Q}[\sqrt{-1}, \sqrt{-5}]$.

Ejemplo 2.10. Sea $\mathfrak{m}$ un entero positivo impar o divisible por 4. El Ray class field para $(\mathfrak{m})$ es $\mathbb{Q}[\zeta_m + \overline{\zeta}_m]$, y el Ray class field para $\infty\mathfrak{m}$ es $\mathbb{Q}[\zeta_m]$. Por tanto la ley de reciprocidad implica el teorema de Kronecker-Weber: toda extensión abeliana de $\mathbb{Q}$ tiene conductor dividiendo $\infty(\mathfrak{m})$ para algún $\mathfrak{m}$, y por tanto esta contenido en una extensión ciclotómica.

Ejemplo 2.11. Sea d un entero libre de cuadrados. Calculamos el conductor de $K = \mathbb{Q}[\sqrt{d}]$ sobre $\mathbb{Q}$ encontrando el m mas pequeño tal que $\mathbb{Q}[\sqrt{d}] \subset \mathbb{Q}[\zeta_m]$.

Primero, consideremos un primo impar p. Entonces $\mathrm{Gal}(\mathbb{Q}[\zeta_p]/\mathbb{Q}) \simeq (\mathbb{Z}/p\mathbb{Z})^\times$ es cíclica de orden p-1, y por tanto tiene un único grupo cociente de orden 2. Por tanto, $\mathbb{Q}[\zeta_p]$ contiene un único cuerpo cuadrático, que debido a que solo puede ser ramificado sobre p, debe ser igual a $\mathbb{Q}[\sqrt{p^*}]$, donde $p^* = (-1)^{\frac{p-1}{2}} p$

Segundo, notar que $\zeta_8 = (1+i)/\sqrt{2}$, y por tanto $\zeta_8 + \overline{\zeta}_8 = \sqrt{2}$. Por tanto $\mathbb{Q}[\sqrt{2}] \subset \mathbb{Q}[\zeta_8]$.

Sea n el producto de primos impares dividiendo d (por tanto $d = \pm n \; o \; \pm 2n$). Por tanto, tenemos

$$\mathbb{Q}[\sqrt{d}] \subset \mathbb{Q}[\zeta_n] \; si \; d \equiv 1 \bmod 4$$
$$\mathbb{Q}[\sqrt{d}] \subset \mathbb{Q}[\zeta_{4n}] \; si \; d \equiv 3 \bmod 4$$
$$\mathbb{Q}[\sqrt{d}] \subset \mathbb{Q}[\zeta_{8n}] \; si \; d \equiv 2 \bmod 4$$

en cada caso, este es el cuerpo ciclotómico mas pequeño que contiene a $\mathbb{Q}[\sqrt{d}]$. Por ejemplo, notar que $d = p_1 \cdots p_r$, $d \equiv 1 \bmod 4$, implica que $d = p_1^* \cdots p_r^*$, y por tanto $\mathbb{Q}[\sqrt{d}] \subset \mathbb{Q}[\zeta_n]$. Además notar que si d es impar, entonces $\mathbb{Q}[\sqrt{d}]$ no esta contenido en

$\mathbb{Q}[\zeta_{4n}]$ porque de lo contrario $\mathbb{Q}[\zeta_{4n}]$ contendría a $i, \sqrt{d}, \sqrt{d/2}$, y por tanto contendría a $i, \sqrt{2}, \zeta_8$.

Concluimos que el conducto de $\mathbb{Q}[\sqrt{d}]$ es $|\Delta_{K/\mathbb{Q}}|$ o $\infty|\Delta_{K/\mathbb{Q}}|$ dependiendo de si $d > 0$ o $d < 0$, donde $|\Delta_{K/\mathbb{Q}}|$ es el discriminante de $K/\mathbb{Q}$.

OBSERVACIÓN 2.12. Para una extensión abeliana finita L/K y un módulo $\mathfrak{m}$ con $S(\mathfrak{m})$ igual al conjunto de primos de K que ramifican en L, sea

$$T(L/K, \mathfrak{m}) = i(K_{\mathfrak{m},1}).Nm_{L/K}(I_L^{S(\mathfrak{m})}) \subset I_K.$$

Takagi mostró que para $\mathfrak{m}$ suficientemente divisible (de hecho, para todo $\mathfrak{m}$ divisible por el conductor $\mathfrak{f}$ de L/K), el grupo $T(L/K, \mathfrak{m})$ es independiente de $\mathfrak{m}$ y $I_K^{S(\mathfrak{m})}/T(L/K, \mathfrak{m}) \simeq \mathrm{Gal}(L/K)$. Por esta razón, $T(L/K, \mathfrak{m})$ es llamado el grupo de Takagi de L/K donde $\mathfrak{f}|\mathfrak{m}$. Artin mostró que el grupo de Takagi es el kernel del mapa $a \mapsto (a, L/K) : I_K^{S(\mathfrak{m})} \to \mathrm{Gal}(L/K)$.

A continuación veremos un resultado el cual nos dice que esta manera de clasificar las extensiones finitas abelianas, o sea, asignarle a L el grupo $H = i(K_{\mathfrak{m},1}).Nm(I_L^{S(\mathfrak{m})})$ para un módulo $\mathfrak{m}$ suficientemente grande, no puede ser extendida a extensiones finitas no abelianas.

TEOREMA 2.13. *Teorema de limitación de norma.*
Sea L una extensión finita de K, y sea L'/K la subextensión maximal abeliana de L/K. Para cada módulo $\mathfrak{m}$ para L'/K,

$$i(K_{\mathfrak{m},1}).Nm_{L/K}(I_L^{S(\mathfrak{m})}) = i(K_{\mathfrak{m},1}).Nm_{L'/K}(I_{L'}^{S(\mathfrak{m})}).$$

Por ejemplo, si L es una extensión cúbica de K que no es Galois sobre K, entonces $L' = K$, y por tanto

$$i(K_{\mathfrak{m},1}).Nm_{L/K}(I_L^{S(\mathfrak{m})}) = I_K^{S(\mathfrak{m})}.$$

Ley de reciprocidad.

Supongamos K contiene a la n-ésima raíz de 1, y sea $a \in K$. Si $\sqrt[n]{a}$ es una raíz de $X^n - a$, entonces el resto de raíces son de la forma $\zeta\sqrt[n]{a}$ donde ζ es una n-ésima raíz de 1. Por tanto $L = K[\sqrt[n]{a}]$ es Galois sobre K, y $\sigma\sqrt[n]{a} = \zeta\sqrt[n]{a}$ para alguna n-ésima raíz de 1.

Si $\mathfrak{p}$ es un ideal primo de K que es coprimo a n y a, entonces $\mathfrak{p}$ es no ramificado en L, y podemos definir una n-ésima raíz $(\frac{a}{n})_n$ de 1 por la formula

$$(\mathfrak{p}, L/K)(\sqrt[n]{a}) = \left(\frac{a}{\mathfrak{p}}\right)_n \sqrt[n]{a}.$$

Se puede ver que

$$\left(\frac{a}{\mathfrak{p}}\right)_n = 1 \Leftrightarrow \text{ a es una n-ésima potencia módulo}\mathfrak{p}$$

y por tanto $\left(\frac{a}{\mathfrak{p}}\right)_n$ generaliza el símbolo de residuo cuadrático. Por esta razón $\left(\frac{a}{\mathfrak{p}}\right)_n$ es llamado símbolo de potencia residual. La ley de reciprocidad de Artin implica que se conocen todas las leyes de reciprocidad para este símbolo, y por tanto, esto puede

ser visto como una generalización de la reciprocidad a cuerpos sin raíces de la unidad. Veremos esto mas en detalle en el capítulo final.

3. Ideles

Grupos topológicos.
Un grupo G con una topología es llamado un grupo topológico si los mapas

$$g, g' \mapsto gg' : G \times G \to G \ , \ g \mapsto g^{-1} : G \to G$$

son continuos. El mapa traslación

$$g \mapsto ag : G \to G$$

es un homeomorfismo.

En general, para determinar una topología sobre un conjunto tenemos que dar una base de entornos de cada punto, que es lo mismo que dar una base de entornos para el 1, ya que el mapa traslación es un homeomorfismo, la topología sobre un grupo topológico es determinado por un sistema de entornos de 1.

Ideles.
Escribiremos v un primo de K. Entonces:

$|.|_v$ = el valor absoluto normalizado para v;
K_v = la completación de K para v;
$\mathfrak{p}_v$ = el ideal primo correspondiente en $\mathcal{O}_K$, cuando v es finito;
$\mathcal{O}_v$ = el anillo de enteros en K_v;
$U_v = \mathcal{O}_v^\times$;
$\widehat{\mathfrak{p}}_v$ = la completación de $\mathfrak{p}_v$= ideal maximal en $\mathcal{O}_v$.

Recordemos que, para todo v, K_v es localmente compacto, $\mathcal{O}_v$ es un entorno compacto de 0. También $K_v^\times$ es compacto, de hecho

$$1 + \widehat{\mathfrak{p}}_v \supset 1 + \widehat{\mathfrak{p}}_v^2 \supset 1 + \widehat{\mathfrak{p}}_v^3 \supset \cdots$$

es una base de entornos de 1 que consiste de subgrupos compactos abiertos.

Queremos combinar todos los grupos $K_v^\times$ en un gran espacio topológico, pero $\prod K_v^\times$ no es localmente compacto. En lugar de eso, definiremos el grupo de ideles como

$$\mathbb{I}_K = \{(a_v) \in \prod K_v^\times | a_v \in \mathcal{O}_v^\times \text{ para todo menos una cantidad finita de v's}\}.$$

De aquí en adelante notaremos $\mathbb{I}$ a $\mathbb{I}_K$.

Para un conjunto finito S de primos que incluye todos los primos infinitos, sea

$$\mathbb{I}_S = \prod_{v \in S} K_v^\times \times \prod_{v \notin S} \mathcal{O}_v^\times$$

con la topología producto. El primer factor es un producto finito de espacios localmente compactos, y por tanto es localmente compacto, y el segundo es un producto de espacios compactos, luego es compacto. Por tanto $\mathbb{I}_S$ es localmente compacto. Notar que

$$\mathbb{I} = \bigcup \mathbb{I}_S.$$

Queremos darle una topología a $\mathbb{I}$ tal que cada $\mathbb{I}_S$ es abierto en $\mathbb{I}$ y herede la topología producto. Lo haremos dando una base para los abiertos que consiste de los conjuntos de forma $\prod_v V_v$ con V_v abiertos en $K_v^\times$ para todo v y $V_v = \mathcal{O}_v^\times$ para todos menos una

cantidad finita de $v's$. Una intersección de dos conjuntos de esta forma contiene a un tercero de esta misma forma, y por tanto forman una base para una topología. Es claro que la topología tiene la propiedad que queremos, y más aún $\mathbb{I}$ tiene estructura de un grupo topológico. El siguiente conjunto forma una base de entornos de 1, para cada conjunto finito de primos $S \supset S_\infty$ y $\epsilon > 0$, define

$$U(S,\epsilon) = \{(a_v) \mid |a_v - 1|_v < \epsilon,\ v \in S,\ |a_v|_v = 1,\ \forall v \notin S\}.$$

Observación 3.1. Existe un homorfismo canónico sobreyectivo Id

$$(a_v) \mapsto \prod_{v\ finito} \mathfrak{p}_v^{ord_{\mathfrak{p}}(a_v)} : \mathbb{I}_K \to I_K$$

cuyo kernel es $\mathbb{I}_{S_\infty}$.

Podemos pensar a los ideles como un engrosamiento de los ideales, estos incluyen factores para los primos infinitos, e incluye las unidades para todos los primos finitos. Notar que $\mathbb{I}/\mathbb{I}_{S_\infty}$ es una suma directa contable de sumas de $\mathbb{Z}$ con la topología discreta, pero $\prod K_v^\times/\mathbb{I}_{S_\infty}$ es un producto directo de contable copias de $\mathbb{Z}$, por tanto es incontable.

Observación 3.2. Existe un homomorfismo canónico inyectivo (diagonal)

$$a \mapsto (a, a, a, \cdots, a) : K^\times \to \mathbb{I}_K.$$

Esta imagen es discreta. Como tenemos grupos, es suficiente probar que $1 \in K^\times$ es abierto en la topología inducida. Sea $U = U(S,\epsilon)$ con S conjunto finito conteniendo a S_∞ y $1 > \epsilon > 0$. Para cada $a \in K^\times \cap U$

$$\begin{cases} |a-1|_v < \epsilon\ \forall v \in S \\ |a|_v = 1\ \forall\ v \notin S. \end{cases}$$

La segunda condición implica que

$$|a-1|_v \leq max(|a|_v, |-1|_v) \leq 1.$$

Por tanto, si $a \in K^\times \cap U$, entonces $\prod_v |a-1|_v < \epsilon^{|S|} < 1$, lo cual contradice la formula del producto, a menos que $a = 1$.

Definición 3.3. El cociente $\mathbf{C} = \mathbb{I}/K^\times$ es llamado el grupo de clase de ideles de K. Esto no es compacto.

Observación 3.4. Existe un homomorfismo inyectivo canónico

$$a \mapsto (1, ..., 1, a, 1, ..., 1) : K_v^\times \to \mathbb{I}_K$$

(a en el v-ésimo lugar). La topología inducida sobre $K_v^\times$ es la topología natural, porque

$$U(S,\epsilon) \cap K_v^\times = \left\{ \begin{array}{c} |a-1|_v < \epsilon\ \forall v \in S \\ |a|_v = 1\ \forall\ v \notin S \end{array} \right\}$$

y tales conjuntos forman una base de entornos de 1 en $K_v^\times$.

Observación 3.5. Existe un homomorfismo canónico sobreyectivo

$$a = (a_v) \mapsto c(a) = \prod |a_v|_v : \mathbb{I} \to \mathbb{R}_{>0}.$$

La imagen de a es llamada el contenido de a. Definimos

$$\mathbb{I}^1 = Ker(c) = \{a \in \mathbb{I} \mid c(a) = 1\}.$$

Notar que, por la formula del producto, $K^\times \subset \mathbb{I}^1$. El cociente $\mathbb{I}/K^\times$ no puede ser compacto porque este mapa es sobreyectivo sobre $\mathbb{R}_{>0}$, pero se puede probar que $\mathbb{I}^1/K^\times$ es compacto.

DEFINICIÓN 3.6. Definimos $\mathbb{I}_f$ de la misma manera que $\mathbb{I}$, excepto que solo usaremos los primos finito. Ahora llamamos $\mathbb{I}_f$ al grupo de ideles finitos. Tenemos

$$\prod_{v\ finito} \mathcal{O}_v^\times \subset \mathbb{I}_f \subset \prod_{v\ finito} K_v^\times.$$

El subgrupo $\prod \mathcal{O}_v^\times$ es abierto y compacto en $\mathbb{I}_f$, y $\mathbb{I}_f/\prod \mathcal{O}_v^\times = I$ (el grupo de ideales de K).

De vuelta tenemos un morfismo diagonal de $K^\times$ en $\mathbb{I}_f$, pero esta vez la topología inducida sobre $K^\times$ tiene la siguiente descripción: $U_K = \mathcal{O}_K^\times$ es abierto, y una base de entornos de 1 es formado por los subgrupos de U_K de índice finito (esto no es trivial). En particular, $K^\times$ es un subgrupo discreto de $\mathbb{I}_f \Leftrightarrow U_K\ es\ finito \Leftrightarrow K = \mathbb{Q}$ o un cuerpo cuadrático imaginario.

3.1. Ray Class group en términos de ideles. Tenemos que ver que el grupo de clases $C_K = I/i(K^\times)$ puede ser un cociente de $\mathbb{I}$, queremos mostrar lo mismo para $C_\mathfrak{m}$.

Sea $\mathfrak{m}$ un módulo. Para $\mathfrak{p}|\mathfrak{m}$, sea

$$W_\mathfrak{m}(\mathfrak{p}) = \begin{cases} \mathbb{R}_{>0} & \mathfrak{p}\ real \\ 1 + \hat{\mathfrak{p}}^{m(\mathfrak{p})} & \mathfrak{p}\ finito. \end{cases}$$

Por tanto, en cada caso, $W_\mathfrak{m}(\mathfrak{p})$ es un entorno de 1 en $K_\mathfrak{p}^\times$.

Definimos $\mathbb{I}_\mathfrak{m}$ como el conjunto de ideles $(a_\mathfrak{p})_\mathfrak{p}$ tal que $a_\mathfrak{p} \in W_\mathfrak{m}(\mathfrak{p})$ para todo $\mathfrak{p}|\mathfrak{m}$:

$$\mathbb{I}_\mathfrak{m} = \left(\prod_{\mathfrak{p}\nmid\mathfrak{m}} K_\mathfrak{p}^\times \times \prod_{\mathfrak{p}|\mathfrak{m}} W_\mathfrak{m}(\mathfrak{p}) \right) \bigcap \mathbb{I}.$$

En otras palabras, $\mathbb{I}_\mathfrak{m}$ consiste de las familias $(a_\mathfrak{p})_\mathfrak{p}$ indexadas por los primos de K tales que

$$\begin{cases} a_\mathfrak{p} \in K_\mathfrak{p}^\times\ \forall\ \mathfrak{p} \\ a_\mathfrak{p} \in \mathcal{O}_\mathfrak{p}^\times \text{ para casi todo } \mathfrak{p} \\ a_\mathfrak{p} \in W_\mathfrak{m}(\mathfrak{p})\ \forall\ \mathfrak{p}|\mathfrak{m}. \end{cases}$$

Definimos $W_\mathfrak{m}$ como el conjunto de ideles $(a_\mathfrak{p})_\mathfrak{p}$ en $\mathbb{I}_\mathfrak{m}$ tal que $a_\mathfrak{p}$ es una unidad para todo $\mathfrak{p}$ no divisor de $\mathfrak{m}$:

$$W_\mathfrak{m} = \prod_{\substack{\mathfrak{p}\nmid\mathfrak{m} \\ \mathfrak{p}\ \text{finito}}} K_\mathfrak{p}^\times \times \prod_{\mathfrak{p}|\mathfrak{m}} W_\mathfrak{m}(\mathfrak{p}) \times \prod_{\substack{\mathfrak{p}\nmid\mathfrak{m} \\ \mathfrak{p}\ \text{finito}}} U_\mathfrak{p}$$

O sea, $W_\mathfrak{m}$ consiste de las familias $(a_\mathfrak{p})_\mathfrak{p}$ indexado por los primos de K tales que

$$\begin{cases} a_\mathfrak{p} \in K_\mathfrak{p}^\times\ \forall\ \mathfrak{p}\ infinito \\ a_\mathfrak{p} \in \mathcal{O}_\mathfrak{p}^\times \forall \mathfrak{p}\ finito \\ a_\mathfrak{p} \in W_\mathfrak{m}(\mathfrak{p})\ \forall\ \mathfrak{p}|\mathfrak{m} \end{cases}$$

Notamos que

$$K_{\mathfrak{m},1} = K^\times \cap \prod_{\mathfrak{p}|\mathfrak{m}} W_{\mathfrak{m}}(\mathfrak{p}) \text{ intersección dentro de } \prod_{\mathfrak{p}|\mathfrak{m}} K_{\mathfrak{p}}^\times,$$

y que

$$K_{\mathfrak{m},1} = K^\times \cap \mathbb{I}_{\mathfrak{m}} \text{ intersección dentro de } \mathbb{I}.$$

PROPOSICIÓN 3.7. *Sea $\mathfrak{m}$ un módulo de K.*

1. *El mapa $id : \mathbb{I}_{\mathfrak{m}} \to I^{S(\mathfrak{m})}$ define un isomorfismo*
$$\mathbb{I}_{\mathfrak{m}}/K_{\mathfrak{m},1}.W_{\mathfrak{m}} \xrightarrow{\simeq} C_{\mathfrak{m}}$$
2. *La inclusión $\mathbb{I}_{\mathfrak{m}} \hookrightarrow \mathbb{I}$ define un isomorfismo:*
$$\mathbb{I}_{\mathfrak{m}}/K_{\mathfrak{m},1} \to \mathfrak{I}/K^\times$$

DEMOSTRACIÓN.

1. Consideremos el par de mapas
$$K_{\mathfrak{m},1} \to \mathbb{I}_{\mathfrak{m}} \xrightarrow{id} I^{S(\mathfrak{m})}.$$
El primer mapa es inyectivo, y el segundo es sobreyectivo con kernel $W_{\mathfrak{m}}$, y por tanto la sucesión kernel-cokernel de el par de mapas es
$$W_{\mathfrak{m}} \to \mathbb{I}_{\mathfrak{m}}/K_{\mathfrak{m},1} \to C_{\mathfrak{m}} \to 1.$$
Esto prueba la primer parte de la proposición.
2. El kernel de $\mathbb{I}_{\mathfrak{m}} \to \mathbb{I}/K^\times$ es $K^\times \cap \mathbb{I}_{\mathfrak{m}}$ (intersección en $\mathbb{I}$), veamos que es $K_{\mathfrak{m},1}$. Por eso la inclusión define una inyección
$$\mathbb{I}_{\mathfrak{m}}/K_{\mathfrak{m},1} \hookrightarrow \mathbb{I}/K^\times.$$
Para la sobreyectividad, aplicamos el teorema de aproximación débil. Sea $S = S(\mathfrak{m})$ y sea $\mathbf{a} = (a_v) \in \mathbb{I}$. Si elegimos $b \in K$ muy cerca de $a_v \in K_v^\times$ para todo $v \in S$, entonces a_v/b estará cerca de 1 en $K + v^\times$ para todo $v \in S$, podemos elegir b tal que $a_v/b \in W_{\mathfrak{m}}(\mathfrak{p})$ para todo $v \in S$. Por ejemplo, para un primo real $v \in S$, solo necesitamos elegir b para tener el mismo signo que a_v en K_v. Entonces $\mathbf{a}/b \in \mathbb{I}_{\mathfrak{m}}$, y se asigna a $\mathbf{a}$ en $\mathbb{I}/K^\times$.

□

Caracteres de ideales y de ideles.
Sea $S \supset S_\infty$ un conjunto finito de primos de K, y sea G un grupo abeliano finito. Diremos que un homomorfismo

$$\Psi : I^G \to G$$

admite un módulo si existe un módulo $\mathfrak{m}$ con soporte en S tal que $\Psi(i(K_{\mathfrak{m},1})) = 1$. Para toda extensión abeliana L/K, Artin mostró que el mapa de Artin

$$I^S \to \mathrm{Gal}(L/K)$$

admite un módulo.

PROPOSICIÓN 3.8. *Si $\Psi : I^S \to G$ admite un módulo, entonces existe un único homomorfismo $\phi : \mathbb{I} \to G$ tal que:*

1. *ϕ es continuo (G con topología discreta);*
2. *$\phi(K^\times) = 1$;*
3. *$\phi(\mathbf{a}) = \Psi(id(\mathbf{a}))$ para todo $\mathbf{a} \in \mathbb{I}^S = \{\mathbf{a} \mid a_v = 1 \, \forall \, v \in S\}$.*

Más aún, cada homomorfismo continuo $\phi : \mathbb{I} \to G$ cumpliendo el segundo ítem viene de un Ψ.

Demostración. Como Ψ admite un módulo $\mathfrak{m}$, factoriza por $I^{\mathfrak{m}}/i(K_{\mathfrak{m},1}) = C_{\mathfrak{m}}$. Por tanto, tenemos el siguiente diagrama

$$\begin{array}{ccccc} & & I^{\mathfrak{m}} & \longrightarrow & C_{\mathfrak{m}} \xrightarrow{\Psi} G \\ & & & & \simeq\uparrow \\ & & \mathbb{I}_{\mathfrak{m}}/K_{\mathfrak{m},1} & \longrightarrow & \mathbb{I}_{\mathfrak{m}}/K_{\mathfrak{m},1}W_{\mathfrak{m}} \\ & & \downarrow\simeq & & \\ \mathbb{I} & \longrightarrow & \mathbb{I}/K^\times. & & \end{array}$$

Los isomorfismos vienen de la proposición anterior, y el resto de mapas son mapas cocientes. Definimos $\phi : \mathbb{I} \to G$ como la composición. Esto tiene las propiedades 1 y 2, y además tiene la propiedad

$$\phi(\mathbf{a}) = \Psi(id(\mathbf{a})) \, \forall \, \mathbf{a} \in \mathbb{I}_{\mathfrak{m}}$$

y por tanto, tiene la propiedad 3.

Para probar que el mapa es únicamente determinado por 1,2 y 3, es suficiente probar que $\mathbb{I}^S K^\times$ es denso en $\mathbb{I}$, pero esto se sigue del teorema de aproximación débil: sea $\mathbf{a} \in \mathbb{I}$; elegimos $b \in K^\times$ muy cerca de a_v para $v \in S$, y sea $\mathbf{a}'$ el elemento de $\mathbb{I}^S$ tal que $a'_v b = a_v$ para todo $v \notin S$. Entonces $\mathbf{a}'b \in \mathbb{I}^S.K$ y es cercano a $\mathbf{a}$ en $\mathbb{I}$.

Por el contrario, sea $\phi : \mathbb{I} \to G$ un mapa continuo. El kernel contiene un entorno abierto de 1, y por tanto $U(S, \epsilon) \subset Ker(\phi)$ para algún S y ϵ. Consideremos un primo finito v. La restricción de $\phi|_{K_v^\times}$ es un mapa continuo $\mathbb{R}^\times \to G$ o $\mathbb{C}^\times \to G$. Claramente, la componente conexa de $K_v^\times$ que contiene a 1, llamada, $\mathbb{R}_{>0}$ o $\mathbb{C}^\times$, tiene a 1 como imagen, y por tanto esta en el kernel. Combinando estas observaciones, vemos que el kernel de ϕ contiene a $W_{\mathfrak{m}}$ para algún $\mathfrak{m}$.

Ahora podemos usar el diagrama del inicio de vuelta. Dado un homomorfismo $\phi : \mathbb{I}/K^\times \to G$, puede ser 'restricto' a un homomorfismo $\mathbb{I}_{\mathfrak{m}}/K_{\mathfrak{m},1} \to G$. Este homomorfismo es trivial sobre $W_{\mathfrak{m}}$, y por tanto factoriza a través de $\mathbb{I}_{\mathfrak{m}}/K_{\mathfrak{m},1}W_{\mathfrak{m}}$. El homomorfismo puede ser transferido a $C_{\mathfrak{m}}$, y compuesto con $\mathbb{I} \twoheadrightarrow C_{\mathfrak{m}}$. Este es Ψ que estábamos buscando. □

Observación 3.9. Sea G un grupo topológico conmutativo. Definimos un homomorfismo $\Psi : I^S \to G$ admisible si para cada entorno N de 1 en G, existe un módulo $\mathfrak{m}$ tal que $\Psi(i(K_{\mathfrak{m},1})) \subset N$. Entonces cada homomorfismo admisible Ψ define un homomorfismo $\phi : \mathbb{I} \to G$ que satisface las tres condiciones de la proposición. Más aún, si G es completo y no tiene subgrupos pequeños, lo cual significa que existe un entorno de 1 conteniendo un subgrupo no trivial, entonces cada homomorfismo continuo $\phi : \mathbb{I} \to G$ satisfaciendo la segunda condición viene de un Ψ admisible. La prueba es la misma que la de la proposición.

El grupo S^1 $G = \{z \in \mathbb{C} \mid |z| = 1\}$ es completo y no tiene subgrupos pequeños. El $\Psi : I^S \to G$ admisible, y el correspondiente ϕ, son llamados caracteres de Hecke.

Observación 3.10. Dado Ψ elegimos un $\mathfrak{m}$, y construiremos ϕ. En la practica, es mas usual para identificar ϕ utilizar que satisface las tres condiciones de la proposición anterior. Para esto las siguientes observaciones son útiles.

1. Sea $\mathbf{a} = (a_v)$ un idele tal que $a_v = 1$ para todo primo finito y $a_v > 0$ para todo primo real; Entonces $\phi(\mathbf{a}) = 1$. Para ver esto, notar que la topología inducida sobre $\prod_{v|\infty} K_v^\times$ como un subgrupo de $\mathbb{I}$ es la topología natural. Por tanto, la restricción de ϕ es trivial sobre la componente conexa que contiene a 1.
2. Sea $\mathbf{a} = (a_v)$ un idele tal que $a_v = 1$ para todo $v \in S$ y a_v es una unidad para todo $v \notin S$; entonces $\phi(\mathbf{a}) = 1$.
3. Si $\mathbf{a}$ es "cercano a 1", $\phi(\mathbf{a}) = 1$. De hecho, esto se deriva de la primer condición, en vista de que G tiene topología discreta.
4. Combinando las tres propiedades, encontramos que si $\mathbf{a} = (a_v)$ es tal que
$$\begin{cases} a_v > 0 \,\forall\, v \; real \\ a_v \; es \; cercano \; a \; 1 \; cuando \; v \in S \; es \; finito \\ a_v \; es \; una \; unidad \; cuando \; v \notin S \end{cases}$$
el $\phi(\mathbf{a}) = 1$.

Ejemplo 3.11. Sea $L = \mathbb{Q}[\zeta_p]$, y sea Ψ el mapa de Artin
$$I^S \to (\mathbb{Z}/p\mathbb{Z})^\times \to \mathrm{Gal}(L/\mathbb{Q}),\ S = \{p, \infty\}.$$
Recordemos que el primer mapa envía el ideal representado por $(r/s), r, s > 0$, $(p, r) = 1 = (p, s)$, a $[r][s]^{-1}$, y que el segundo envía $[m] \mapsto (\zeta \mapsto \zeta^m)$. Para cualquier primo $l \neq p$, el mapa envía (l) al automorfismo de Frobenius para l, $\zeta \mapsto \zeta^l$. Sea $\phi : \mathbb{I} \to \mathrm{Gal}(L/\mathbb{Q})$ el homomorfismo correspondiente a Ψ como en la proposición. Deseamos determinar ϕ de manera explicita.

Sea $\mathbf{a} = (a_\infty, a_2, ..., a_p, ..., a_l, ...)$ un idele de $\mathbb{Q}$. Si $a_\infty = 1 = a_p$, entonces $\phi(\mathbf{a}) = \Psi(id(\mathbf{a}))$.Por tanto $\phi(\mathbf{a}) = \zeta_p^m$ donde $m = \prod l^{ord_l(a_l)}$.

Consideramos $\mathbf{p} = (1, ..., 1., p, 1, ...)$ con p en la p-ésima posición. Entonces
$$\mathbf{p}/p = (p^{-1}, ..., p^{-1}, 1, p^{-1}, ...).$$
De acuerdo a la observación 4, $\phi(\mathbf{p}/p) = 1$, y por tanto
$$\phi(\mathbf{p}) = \phi(\mathbf{p}/p)\phi(p) = 1.$$
Consideramos $\mathbf{a} = (1, ..., 1, u, 1, ...), u \in \mathbb{Z}_p^\times$, u en la posición p-ésima. Escribimos
$$u^{-1} = a_0 + a_1 p + \cdots + a_s p^s + \cdots,\ 0 \leq a_i < p,\ a_i \in \mathbb{Z}$$
y sea $c = a_0 + \cdots + a_s p^s \in \mathbb{Z}$. Notar que $c > 0$. Entonces $uc \in 1 + p^{s+1}\mathbb{Z}_p$, para un s suficientemente grande esto es cercano a 1. Escribimos
$$\mathbf{a}c = (c, c, ..., c, \overset{l|c}{l}, c, ..., \overset{p}{uc}, c, ...)(1, ..., 1, \overset{l|c}{c}, 1, ...).$$
El primer factor es $\mathbf{a}c$ excepto que tenemos movida las componentes para los primos l dividiendo a c para el segundo factor. Para un s grande, ϕ del primer factor es 1 por 4. El segundo factor esta en $\mathbb{I}^S$, y la descripción que tenemos de $\phi|\mathbb{I}^S$ muestra que ϕ envía ζ en ζ^c. En conclusión,
$$\phi(\mathbf{a})(\zeta) = \zeta^c = \zeta^{u^{-1}}.$$

Consideremos $\mathbf{a} = (-1, 1, ..., 1)$. Entonces

$$-\mathbf{a} = (1, -1, ..., -1, \overset{p}{1}, -1, ...)(1, ..., 1, \overset{p}{-1}, 1, ...)$$

y

$$\phi(\mathbf{a}) = \phi(-\mathbf{a})\phi(1, ..., 1, -1, 1, ...).$$

De acuerdo a 3.11, $\phi(\mathbf{a})(\zeta) = \zeta^{-1}$.

Como ϕ es un homomorfismo, esto completa su descripción.

3.2. Norma de ideles. Sea L una extensión finita de K un cuerpo de números, sea v un primo de K. Recordemos que existe un isomorfismo canónico

$$L \otimes_K K_v \to \prod_{w|v} L_w.$$

De esto se sigue que para cada $\alpha \in L$,

$$Nm_{L/K}\alpha = \prod_{w|v} Nm_{L_w/K_v}\alpha \ (igualdad\ en\ K_v).$$

Para un idele $\mathbf{a} = (a_w) \in \mathbb{I}_L$, define $Nm_{L/K}(\mathbf{a})$ como el idele $\mathbf{b} \in \mathbb{I}_K$ con $b_v = \prod_{w|v} Nm_{L_w/K_v} a_w$. La anterior observación muestra que el cuadrado de la izquierda en el siguiente diagrama conmuta, y es fácil ver que el cuadrado de la derecha también lo hace

$$\begin{array}{ccccc} L^\times & \longrightarrow & \mathbb{I}_L & \xrightarrow{id} & I_L \\ \downarrow{\scriptstyle Nm_{L/K}} & & \downarrow{\scriptstyle Nm_{L/K}} & & \downarrow{\scriptstyle Nm_{L/K}} \\ K^\times & \longrightarrow & \mathbb{I}_K & \xrightarrow{id} & I_K. \end{array}$$

Por tanto obtenemos el siguiente diagrama

$$\begin{array}{ccc} C_L & \longrightarrow & C_L \\ \downarrow{\scriptstyle Nm_{L/K}} & & \downarrow{\scriptstyle Nm_{L/K}} \\ C_K & \longrightarrow & C_K. \end{array}$$

Donde C_K es el grupo de clases de ideles $\mathbb{I}/K^\times$; C_K= el grupo de clases de ideales $I/i(K^\times)$

Proposición 3.12. *Si L/K es una extensión finita de un cuerpo local de característica cero, entonces*

1. $Nm_{L/K}(L^\times) = \mathbb{R}_{>0}$ *(caso* $K = \mathbb{R}, L = \mathbb{C}$
2. $Nm_{L/K}(L^\times) \supset 1 + \mathfrak{p}_K^{\mathfrak{m}}$ *para algún* $\mathfrak{m}$ *(caso K no arquimedeano)*
3. $Nm_{L/K}(L^\times) \supset \mathcal{O}_K^\times$ *(caso K no arquimedeano y L/K es no ramificado)*

Demostración. Ver Proposición 4.12 de las notas de Class Field Theory de J.S. Milne □

4. Principales resultados de CFT en términos de ideles

Los principales teoremas de CFT en términos de ideales son muy explícitos, y, para algunos propósitos, son muy útiles. Aunque tienen algunas desventajas. Fijado un módulo $\mathfrak{m}$, la teoría describe solo las extensiones abelianas cuyo conductor divide a $\mathfrak{m}$. En particular, esto no provee una descripción de las extensiones abelianas infinitas de K. Los enunciados de estos teoremas en términos de ideles permiten considerar extensiones abelianas infinitas, o, lo que es lo mismo, todas las extensiones abelianas finitas simultáneamente. Esto además nos permite ver la relación entre el mapa local de Artin y el mapa global de Artin.

Sea L una extensión finita de K. Sea v un primo de K, y sea w un primo de L sobre v. Recordemos que el grupo de descomposición $D(w)$ de w es el subgrupo

$$D(w) = \{\sigma \in \mathrm{Gal}(L/K) \mid \sigma w = w\}.$$

Estos elementos extienden únicamente a automorfismos de L_w/K_w, y $D(\sigma) \simeq \mathrm{Gal}(L_w/K_w)$. CFT local provee un homomorfismo (el mapa local de Artin)

$$\phi_v : K_v^\times \to D(w) \subset G.$$

LEMA 4.1. *El subgrupo $D(w) \subset G$ y el mapa ϕ_v son independientes de la elección del primo $w|v$.*

DEMOSTRACIÓN. Cualquier otro primo sobre v es de la forma σw para algún $\sigma \in G$, y $\sigma : L \to L$ extiende por continuidad a un homomorfismo $\sigma : L_w \to L_{\sigma w}$ fijando K_v. Tenemos

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

el cual es igual a $D(w)$ porque G es conmutativo.

Sea Ω y Ω' extensiones abelianas maximales de K_v conteniendo L_w y $L_{\sigma w}$ respectivamente. De CFT local, obtenemos el mapa local de Artin $\phi_v : K^\times \to \mathrm{Gal}(\Omega/K_v)$ y $\phi'_v : K^\times \to \mathrm{Gal}(\Omega'/K_v)$. La elección de un isomorfismo $\widetilde{\sigma} : \Omega \to \Omega'$ determina un isomorfismo

$$\rho \mapsto \widetilde{\sigma} \circ \rho \circ \widetilde{\sigma}^{-1} : \mathrm{Gal}(\Omega/K_v) \to \mathrm{Gal}(\Omega'/K_v)$$

que es independiente de $\widetilde{\sigma}$. más aún, su composición con ϕ_v es ϕ'_v. □

PROPOSICIÓN 4.2. *Existe un único homomorfismo $\phi_K : \mathbb{I} \to Gal(K^{ab}/K)$ con la siguiente propiedad: para todo $L \subset K^{ab}$ finito sobre K y cualquier primo $w \in L$ sobre un primo $v \in K$, el siguiente diagrama conmuta*

$$\begin{array}{ccc} K_v^\times & \xrightarrow{\phi_v} & Gal(L_w/K_v) \\ \downarrow & & \downarrow \\ \mathbb{I}_K & \xrightarrow{\mathbf{a}\mapsto\phi_K(\mathbf{a})|_L} & Gal(L/K) \end{array}$$

DEMOSTRACIÓN. Sea $\mathbf{a} \in \mathbb{I}$, y sea $L \subset K^{ab}$ una extensión finita sobre K. Si $a_v \in U_v$ y L_w/K_v es no ramificada, entonces $\phi_v(a_v) = 1$. Por tanto, $\phi_v(a_v) = 1$ excepto para una cantidad finita de primos, y por tanto podemos definir

$$\Phi_{L/K}(\mathbf{a}) = \prod_v \phi_v(a_v).$$

Claramente, $\phi_{L/K}$ es el único homomorfismo que hace que el diagrama conmute.

Si $L' \supset L$, entonces las propiedades del mapa local de Artin muestra que $\phi_{L'/K}(\mathbf{a})|_L = \phi_{L/K}(\mathbf{a})$. Por tanto existe un único homomorfismo $\phi : \mathbb{I} \to \mathrm{Gal}(K^{ab}/K)$ tal que $\phi(\mathbf{a})|_L = \phi_{L/K}(\mathbf{a})$ para todo $L \subset K^{ab}$, con L finito sobre K.

De vuelta, las propiedades del mapa local de Artin muestra que, para toda torre de cuerpos $K \subset K' \subset L \subset K^{ab}$ con L finito sobre K,

$$\begin{array}{ccc} \mathbb{I}_{K'}^S & \xrightarrow{\phi_{L/K'}} & \mathrm{Gal}(L/K') \\ \downarrow Nm & & \downarrow \\ \mathbb{I}_K^S & \xrightarrow{\phi_{L/K}} & \mathrm{Gal}(L/K) \end{array}$$

conmuta. Al tomar $K' = L$, encontramos que $Nm_{L/L}(\mathbb{I}_L^S)$ esta contenido en el kernel de $\phi_{L/K}$. En particular, el kernel de $\phi_{L/K}$ contiene un subgrupo abierto de $\mathbb{I}_K^S$, y esto implica que ϕ_K es continuo. □

Teorema 4.3. *Ley de Reciprocidad.*
El homomorfismo $\phi_K : \mathbb{I}_K \to Gal(K^{ab}/K)$ tiene las siguientes propiedades

1. $\phi_K(K^\times) = 1$*;*
2. *para cada extensión abeliana finita L de K, ϕ_K define un isomorfismo*

$$\phi_{L/K} : \mathbb{I}_K/(K^\times.Nm(\mathbb{I}_L)) \to Gal(L/K).$$

En la prueba de la Proposición vimos que $\phi_{L/K}(Nm(\mathbb{I}_L)) = 1$, y por tanto vemos que $\phi_{L/K}$ factoriza a través de $\mathbb{I}_K/K^\times.Nm(\mathbb{I}_L)$. La segunda propiedad puede ser vista como: ϕ define un isomorfismo

$$\phi_{L/K} : C_K/Nm(C_L) \to Gal(L/K)$$

Teorema 4.4. *Teorema de existencia.*
Fijada una clausura algebraica K^{al} de K; para cada subgrupo abierto $N \subset C_K$ de índice finito, existe una única extensión abeliana L de K contenida en K^{al} tal que $Nm_{L/K}C_L = N$.

Un subgrupo de C_K es un grupo norma si es de la forma $Nm(C_L)$ para alguna extensión abeliana finita L de K. El teorema de existencia muestra que los grupos norma son exactamente los subgrupos abiertos de índice finito en C_K. Si N es un grupo de este tipo, entonces la extensión abeliana finita L de K tal que $Nm(C_L) = N$, i.e., $N = Ker(\phi_{L/K})$, es llamado el cuerpo de clases de K perteneciente a N (class field of K belonging to N).

Corolario 4.5. *El mapa $L \mapsto Nm(C_L)$ es una biyección de el conjunto de extensiones abelianas de K al conjunto de subgrupos abiertos de índice finito en C_K. más aún,*

$$L_1 \subset L_2 \Leftrightarrow Nm(C_{L_1}) \supset Nm(C_{L_2})$$
$$Nm(C_{L_1.L_2}) = Nm(C_{L_1}) \cap Nm(C_{L_2})$$
$$Nm(C_{L_1 \cap L_2}) = Nm(C_{L_1}).Nm(C_{L_2})$$

Observación 4.6.

1. En el caso de un cuerpo de números, el mapa
$$\phi_K : \mathbb{I}_K \to \mathrm{Gal}(K^{ab}/K)$$
es sobreyectivo. Para una primo infinito v de K, escribimos K_v^+ la componente conexa de $K_v^\times$ que contiene a 1; Por tanto K_v^+ es isomorfo a $\mathbb{C}^\times$ o $\mathbb{R}_{>0}$ de acuerdo a si v es complejo o real. Claramente $\prod_{v|\infty} K_v^+ \subset Ker(\phi_K)$. Por definición $K^\times \subset Ker(\phi_K)$, y por tanto $K^\times.(\prod_{v|\infty} K_v^+) \subset Ker(\phi_K)$. Pero ϕ_K es un homomorfismo continuo y $\mathrm{Gal}(K^{ab}/K)$ es Hausdorff, y por tanto el Kernel es un subgrupo cerrado. Entonces $Ker(\phi_K)$ contiene a la clausura de $K^\times.(\prod_{v|\infty} K_v^+)$. Es un teorema que esto exactamente es el kernel. La imagen de la clausura de $K^\times.(\prod_{v|\infty} K_v^+)$ en C_K es la componente conexa de C_K que contiene a 1.

   Para cualquier extensión abeliana finita $L \supset K$ el mapa de Artin define un isomorfismo $C_K/Nm(C_L) \to \mathrm{Gal}(L/K)$.
2. En el caso de cuerpos de funciones , el mapa de Artin $\phi_K : \mathbb{I}_K/K^\times \to \mathrm{Gal}(K^{ab}/K)$ es inyectivo, pero no es sobreyectivo.

Capítulo 3

Aplicaciones de CFT

En este capitulo usaremos algunos de los resultados que vimos en los capítulos anteriores para ver aplicaciones de CFT. Nos centraremos en 3 problemas, en los cuales usaremos fuertemente la heurística local-global, la cual nos permitirá un mejor estudio de los problemas.

1. Potencias locales, potencias globales

Es un problema interesante ver cuando una potencia local se convierte en global. Es obvio que si $a \in K$ un cuerpo de números es una potencia n-ésima, entonces $a \in K_v$ también lo es para cualquier v. Comenzaremos viendo el siguiente teorema.

TEOREMA 1.1. *Sea K un cuerpo de números que contiene una raíz n-ésima de la unidad. Un elemento no nulo en K es una n-ésima potencia si lo es en K_V para casi todo primo v.*

DEMOSTRACIÓN. Recordemos que, para un cuerpo k que contiene una raíz n-ésima de la unidad, un polinomio $X^n - a$ descompone completamente en $k[x]$ si tiene una raíz en k. Sea a un elemento no nulo de K, y sea β una raíz n-ésima de a en alguna extensión. Si a es una n-ésima potencia en K_v para casi todo v, entonces $X^n - a$ descompone completamente en $K_v[x]$ para casi todo v, y por tanto v descompone completamente en $K[\beta]$. Esto se cumple para casi todo v, viendo que $K[\beta] = K$. □

Para esto ultimo podemos utilizar el siguiente teorema, el cual no demostraremos.

TEOREMA 1.2. *Sea L una extensión finita de K, y sea M su clausura de Galois. Entonces el conjunto de ideales primos de K que descomponen completamente en L tienen densidad 1/[M:K]*

OBSERVACIÓN 1.3. Usando este resultado el teorema probado es mas fuerte, ya que solo basta con que sea potencia n-ésima para un conjunto de primos de densidad mayor a 1/2.

TEOREMA 1.4. *Sea K un cuerpo de números, y sea n un entero tal que $K[\zeta_{2^t}]$ es cíclico sobre K, donde 2^t es la mayor potencia de 2 que divide a n. Un elemento no nulo de K es una n-ésima potencia en K si es una n-ésima potencia en K_v para casi todo v.*

DEMOSTRACIÓN. Paso 1. Es suficiente probar el teorema con n una potencia de un primo. Supongamos $n = n_1 n_2$ con n_1, n_2 coprimos, y asumamos que el teorema se cumple para ambos. Entonces un elemento no nulo $a \in K$ que es una n-ésima potencia en K_v

para casi todo v es una n_1 y n_2-ésima potencia en K, por tanto, $a = b^{n_1} = c^{n_2}$. Ahora, existen enteros r y s tales que $rn_1 + sn_2 = 1$, y por tanto

$$a = a^{rn_1}a^{sn_2} = c^{rn_1n_2}b^{sn_1n_2} \in K^{\times n}.$$

Paso 2. El teorema es cierto si n es una potencia de un primo p y $K[\zeta_n]/K$ es una extensión cíclica de orden una p-potencia. Sea $K' = K[\zeta_n]$, y sea a un elemento no nulo de K que se convierte en una n-ésima potencia en K_v para casi todo v. De acuerdo al Teorema 1.1, a se convierte en una n-ésima potencia en K', por tanto, $a = \beta^n$, y por tanto

$$X^n - a = \prod_{j=0}^{n-1}(X - \beta\zeta_n^j) \text{ en } K'[X].$$

Sea

$$X^n - a = \prod_i f_i(X)$$

la descomposición de $X^n - a$ en factores irreducibles en $K[X]$. Para cada i, elegimos una raíz $\beta_i = \beta\zeta_n^{j(i)}$ de $f_i(X)$. Entonces $K[\beta_i] \subset K'$, por tanto $K[\beta_i]$ es una extensión abeliana de K, en particular, es Galois sobre K, entonces es el cuerpo de descomposición de $f_i(X)$. Sea v un primo de K tal que a es una n-ésima potencia en K_v. Por hipótesis, $X^n - a$ tiene una raíz en K_v, y por tanto al menos uno de los $f_i(X)$ tiene una raíz en K_v. Para un i particular, v descompone completamente en $K[\beta_i]$. Entonces vemos que cada $v \notin S$ descompone completamente en al menos uno de los cuerpos $K[\beta_i]$, pero diferentes v pueden descomponer en diferentes cuerpos, no podemos concluir nada de esto. Para ver que todos los v descomponen en un solo $K[\beta_i]$ tenemos que usar la hipótesis que K' es cíclica de orden una potencia de primo sobre K. Esta hipótesis implica que los cuerpos intermedios están linealmente ordenados.

$$K' \supset \cdots \supset K_3 \supset K_2 \supset K_1 \supset K.$$

Elegimos i_0 tal que $K[\beta_{i_0}]$ es la mas pequeña de el $K[\beta_i]$. Entonces cada $v \notin S$ descompone completamente en un cuerpo conteniendo a $K[\beta_{i_0}]$, y por tanto en $K[\beta_{i_0}] = K$, y $X^n - a$ tiene al menos una raíz de K.

Paso 3. El teorema es cierto. Después del primer paso, podemos asumir que $n = p^r$, y después del paso 2 que p es impar. Supongamos que a es una n-ésima potencia en K_v para casi todo v. Como $K[\zeta_{p^r}]$ es cíclica de orden p-potencia sobre $K[\zeta_p]$, el paso 3 muestra que a se convierte en una n-ésima potencia en $K[\zeta_p]$, notamos, $a = b^n$. Tomando normas, encontramos que a^d es una n-ésima potencia en $K^\times$, donde $d = [K[\zeta_p] : K] < p$. Pero d es coprimo a p, y eso implica que a es una n-ésima potencia en $K^\times$ (sabemos que $a^d = 1$ en $K^\times/K^{\times p^r}$, y esto implica que $a = 1$ en $K^\times/K^{\times p^r}$). □

2. Principio local global para normas

El principio local-global (o de Hasse) pregunta si una afirmación sobre un cuerpo de números es cierta si es cierta para todas las completaciónes de K. Aquí veremos uno de estos principios local-global.

2.1. Normas.

TEOREMA 2.1. *(Teorema de la norma de Hasse)*
Sea L/K una extensión cíclica de un cuerpo de números, y sea $a \in K^\times$. Entonces la imagen de $a \in K_v$ es una norma de L^v para casi todo v, y si es una norma para todo v, entonces es una norma en K.

DEMOSTRACIÓN. Para esta prueba asumiremos sin probarlo que $H^1(G, C_L) = 0$. Por la periodicidad de la cohomología de grupos cíclicos, esto implica que $H_T^{-1}(G, C_L) = 0$. Por tanto, de la sucesión de cohomología de

$$1 \to L^\times \to \mathbb{I}_L \to C_L \to 0$$

encontramos que

$$H_T^0(G, L^\times) \to H_T^0(G, \mathbb{I}_L)$$

es inyectivo. Pero este es el mapa

$$K^\times / Nm(L^\times) \to \bigotimes_v K_v^\times / Nm(L^{v\times}).$$

□

3. Leyes de reciprocidad altas

Recordemos que, dado p un primo impar y a coprimo a p, el símbolo de Legendre (o símbolo de reciprocidad cuadrática)

$$\left(\frac{a}{p}\right) = \begin{cases} 1 \textit{ si } a \textit{ es un cuadrado modulo } p \\ -1 \textit{ otro caso.} \end{cases}$$

El grupo $\mathbb{F}_p^\times$ es cíclico de orden $p-1$ con -1 el único elemento de orden 2. Por tanto, para $u \in \mathbb{F}_p^\times$, $u^{\frac{p-1}{2}}$ es 1 o -1 de acuerdo a si u es un cuadrado o no, y por tanto $\left(\frac{a}{p}\right)$ es la única raíz de 1 tal que

$$\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} \; mod\, p$$

La ley de reciprocidad cuadrática, dice que para p y q primos impares

$$\left(\frac{q}{p}\right)\left(\frac{p}{q}\right) = (-1)^{\frac{p-1}{2}\frac{q-1}{2}}.$$

Además

$$\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}}, \; \left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}.$$

Para $\alpha \in \mathbb{Z}[i]$ y $\pi \in \mathbb{Z}[i]$ un primo, Gauss definió $\left(\frac{\alpha}{\pi}\right)$ (símbolo de residuo cuartico) como la única raíz 4^{ta} de 1 tal que

$$\left(\frac{\alpha}{\pi}\right) \equiv \alpha^{\frac{\mathbb{N}\pi-1}{4}} \; mod\, \pi$$

y probo una ley de reciprocidad cuártica para este símbolo. Luego Eisenstein probo una ley de reciprocidad cubica. Artin observó que su teorema implica toda posible ley de reciprocidad, y por tanto puede ser considerado como una "ley de reciprocidad para cuerpos que no contienen una n-ésima raíz de 1". En el resto de esta sección explicaremos esta observación.

3.1. Símbolo de potencia residual. Sea K un cuerpo de números conteniendo una raíz n-ésima de la unidad. Para cada conjunto finito $a, b, ...$ de elementos de K, definimos $S(a, b, ...)$ como el conjunto de ideales primos de K tales que $ord_{\mathfrak{p}}(n) \neq 0$, o $ord_{\mathfrak{p}}(a) \neq 0$, o $ord_{\mathfrak{p}}(b) \neq 0, ...$ En particular, S en si consiste solamente de los divisores de n.

Recordemos que el discriminante de $X^n - 1$ es divisible solo por los primos que dividen a n. Por tanto $X^n - 1$ tiene n raíces distintas en $\mathbb{F}_p^{al}$ para cada $p \nmid n$, y el mapa

$$\zeta \mapsto \zeta \, mod \, \mathfrak{p} : \mu_n(K) \to \mu_n(\mathcal{O}_K/\mathfrak{p})$$

es biyectivo para cada ideal primo $\mathfrak{p} \nmid n$. Para cada primo $\mathfrak{p}$, sea $q = \mathbb{N}\mathfrak{p} = (\mathcal{O}_K : \mathfrak{p})$. Entonces $\mathbb{F}_q^\times$ es cíclico de orden $q-1$, y por tanto $n|q-1$ y $\zeta^{\frac{q-1}{n}} \in \mu_n \subset \mathbb{F}_q^\times$.

Para $a \in K^\times$ y $\mathfrak{p} \notin S(a)$, definimos $\left(\frac{a}{\mathfrak{p}}\right)$ como la única raíz de la unidad tal que

$$\left(\frac{a}{\mathfrak{p}}\right) \equiv a^{\frac{\mathbb{N}\mathfrak{p}-1}{n}} \, mod \, \mathfrak{p}.$$

1. Para todo $a, b \in K^\times$ y $\mathfrak{p} \notin S(a, b)$,
$$\left(\frac{ab}{\mathfrak{p}}\right) = \left(\frac{a}{\mathfrak{p}}\right)\left(\frac{b}{\mathfrak{p}}\right)$$
esto es obvio por definición.
2. Para $a \in K^\times$ y $\mathfrak{p} \notin S(a)$, los siguientes enunciados son equivalentes:
   a) $\left(\frac{a}{\mathfrak{p}}\right) = 1$;
   b) a es una n-ésima potencia en $\mathcal{O}_K/\mathfrak{p}$
   c) a es una n-ésima potencia en $K_{\mathfrak{p}}$
   La equivalencia de a y b salen de la exactitud de
$$1 \to \mathbb{F}_q^{\times n} \to \mathbb{F}_q^\times \xrightarrow{x \mapsto x^{\frac{q-1}{n}}} \mu_n \to 1, \; q = \mathbb{N}\mathfrak{p}.$$
   Si $X^n - a$ tiene una solución modulo $\mathfrak{p}$, entonces el lema de Hensel muestra que tenemos una solución en $K_{\mathfrak{p}}$. Contrariamente, si $a = \alpha^n$, $\alpha \in K_{\mathfrak{p}}$, entonces $ord_{\mathfrak{p}}(\alpha) = \frac{1}{n} ord_{\mathfrak{p}}(a) = 0$, y por tanto $\alpha \in \mathcal{O}_{K_{\mathfrak{p}}}$. El mapa $\mathcal{O}_K \to \mathcal{O}_{K_{\mathfrak{p}}}/\mathfrak{p}$ es sobreyectivo, y por tanto es un $\alpha_0 \in \mathcal{O}_K$ enviado a α modulo $\mathfrak{p}$.

   Lo extendemos enviando $\mathfrak{p} \mapsto \left(\frac{a}{\mathfrak{p}}\right)$ a $I^{S(a)}$ por linealidad: por tanto, para $\mathfrak{b} = \prod \mathfrak{p}_i^{r_i} \in I^{S(a)}$,
$$\left(\frac{a}{\mathfrak{b}}\right) = \prod \left(\frac{a}{\mathfrak{p}_i}\right)^{r_i}$$
   abreviaremos $\left(\frac{a}{(b)}\right)$ a $\left(\frac{a}{b}\right)$.

   Para una extensión abeliana L/K en la cual los primos en S' no ramifican, $\Psi_{L/K} : I^S \to Gal(L/K)$ denota el mapa de Artin
3. Para cada $a \in K^\times$ y $\mathfrak{b} \in I^{S(a)}$,
$$\Psi_{K[a^{\frac{1}{n}}]/K}(\mathfrak{b})(a^{\frac{1}{n}}) = \left(\frac{a}{\mathfrak{b}}\right) a^{\frac{1}{n}}.$$

De teoría de Galois, sabemos que hay una raíz n-ésima de 1 $\zeta(\mathfrak{b})$ tal que

$$\Psi(\mathfrak{b})(a^{\frac{1}{n}}) = \zeta(\mathfrak{b}).a^{\frac{1}{n}}$$

y que el mapa $\mathfrak{b} \mapsto \zeta(\mathfrak{b})$ es un homomorfismo. Por tanto, esto es suficiente para probar la igualdad con $\mathfrak{b} = \mathfrak{p}$, un ideal primo. Por definición

$$\Psi(\mathfrak{p})(x) \equiv x^{\mathbb{N}\mathfrak{p}} \, mod \, \mathfrak{p}.$$

De

$$\Psi(\mathfrak{p})(a^{\frac{1}{n}}) = \zeta(\mathfrak{p}).a^{\frac{1}{n}}$$

encontramos que

$$\zeta(\mathfrak{p}).a^{\frac{1}{n}} \equiv a^{\frac{\mathbb{N}\mathfrak{p}}{n}} \, mod \, \mathfrak{p}$$

de donde se sigue que $\zeta(\mathfrak{p}) = \left(\frac{a}{\mathfrak{p}}\right)$.

4. Sea $a \in \mathcal{O}_K$, y sea $\mathfrak{b}$ un ideal integral en $I^{S(a)}$. Si $a' \in \mathcal{O}_K, a' \equiv a \, mod \, \mathfrak{b}$, entonces $\mathfrak{b} \in I^{S(a')}$ y

$$\left(\frac{a}{\mathfrak{b}}\right) = \left(\frac{a'}{\mathfrak{b}}\right).$$

Para cada ideal primo $\mathfrak{p}$ dividiendo a $\mathfrak{b}$,$a' \equiv a \, mod \, \mathfrak{p}$, y por tanto $\left(\frac{a}{\mathfrak{p}}\right) = \left(\frac{a'}{\mathfrak{p}}\right)$.

5. Sea $a \in K^\times$. Existe un modulo $\mathfrak{m}$ con soporte $S(a)$ tal que $\left(\frac{a}{\mathfrak{b}}\right)$ depende solo de la clase de $\mathfrak{b}$ en el Ray class group C_m.

3.2. El símbolo de Hilbert. Sea K_v un cuerpo local conteniendo una raíz n-ésima de la unidad. El símbolo de Hilbert es un pairing

$$a, b \mapsto (a, b)_v : K_v^\times / K_v^{\times n} \times K_v^\times / K_v^{\times n} \to \mu_n,$$

donde μ_n es el grupo de raíces n-ésimas de 1 en K_v. Probablemente la manera mas natural de definir esto es con el producto cup

$$H^1(G, \mu_n) \times H^1(G, \mu_n) \to H^2(G, \mu_n \otimes \mu_n), \; G = Gal(K^{al}/K)$$

seguido por el isomorfismo

$$H^2(G, \mu_n \otimes \mu_n) = H^2(G, \mu_n) \otimes \mu_n \to \mu_n$$

definido por el mapa invariante inv_v. Sin embargo, en el espíritu de los 20 y 30, se define en términos de álgebras centrales simples.

Recordemos que para cada $a, b \in K_v^\times$, definimos $A(a, b; \zeta)$ como la K_v-álgebra con generadores i,j y relaciones

$$i^n = a, \; j^n = b, \; ij = \zeta ji.$$

Esto es un álgebra central simple de grado n sobre K_v. En el caso que $n = 2$, $A(a, b; -1)$ es el álgebra de cuaterniones $H(a, b)$. Definimos

$$(a, b)_v = \zeta^{-n.inv_v([A(a,b;\zeta)]}$$

donde $[A(a, b; \zeta)]$ es la clase de $A(a, b; \zeta)$ en $Br(K_v)$. Como $A(a, b; \zeta)$ es split para un cuerpo de grado n, su invariante es un elemento de $\frac{1}{n}\mathbb{Z}/\mathbb{Z}$, y por tanto $n.inv_v([A(a, b; \zeta)])$ es un elemento de $\mathbb{Z}/n\mathbb{Z}$. Claramente el isomorfismo de clases de $A(a, b; \zeta)$ depende solo de a y b como elementos de $K_v^\times / K_v^{\times n}$, y por tanto tenemos un pairing

$$K_v^\times / K_v^{\times n} \times K_v^\times / K_v^{\times n} \to \mu_n$$

Sin embargo, no es obvio que el pairing es bilineal.

Observación 3.1.

1. Para todo a,b
$$A(b,a;\zeta) \approx A(a,b;\zeta^{-1}) \approx A(a,b;\zeta)^{op}.$$
Por tanto
$$(b,a)_v = (a,b)_v^{-1}.$$
Por definición $A(b,a;\zeta)$ es la K_v-álgebra con generadores i', j' y relaciones $i'^n = b$, $j'^n = a$, y $i'j' = \zeta j'i'$. El mapa $i' \mapsto j$, $j' \mapsto i$ es un isomorfismo $A(b,a;\zeta) \to A(a,b;\zeta^{-1})$. El mapa $i \mapsto i$, $j \mapsto j$ es un isomorfismo $A(a,b;\zeta)^{op} \to A(a,b;\zeta)$.
2. Sea $a, b \in K^\times$. Sea $v \notin S(a), (a,b)_v = \left(\frac{a}{\mathfrak{p}_v}\right)^{0ord_v(b)}$.

   Por simplicidad, asumiremos que $A(a,b;\zeta)$ es un álgebra de división. Recordemos que para calcular el invariante de un álgebra de división central D sobre un cuerpo local K_v,tenemos que
   a) elegir un cuerpo maximal no ramificado $L \subset D$.
   b) Encontrar un elemento $\beta \in D$ tal que $\alpha \mapsto \beta\alpha\beta^{-1}$ es el automorfismo de Frobenius de L.
   c) Sea $inv_v([D]) = ord_v(\beta)$.

   Aplicamos esto con $L = K_v[i] = K_v[a^{\frac{1}{n}}]$. Notamos que, como $v \notin S(a)$, esta extensión es no ramificada. Sea $\left(\frac{a}{\mathfrak{p}_v}\right) = \zeta^r$, por tanto $(\mathfrak{p}, L/K_v)(i) = \zeta^r i$. Dado que $jij^{-1} = \zeta^{-1}i$, vemos que podemos tomar $\beta = j^{-r}$. Entonces $\beta^n = b^{-r}$, se sigue que $ord_v(\beta) = -\frac{r}{n}ord_v(b)$. Por tanto
$$(a,b)_v = \zeta^{-ninv_v(A(a,b;\zeta))} = \zeta^{r.ord_v(b)} = \left(\frac{a}{\mathfrak{p}_v}\right)^{ord_v(b)}.$$
3. $$(a,b)_v = \frac{\phi_v(b)(a^{\frac{1}{n}})}{a^{\frac{1}{n}}}$$
para todo a, b, v.
4. Para $a, b \in K^\times$,
$$\prod_v (a,b)_v = 1.$$
Para esto hay que mirar la prueba de la Ley de Reciprocidad, en dicha prueba se ve que, para cada $\beta \in Br(K)$, $\sum inv_v(\beta) = 0$. En particular, $\sum inv_v(A(a,b;\zeta)) = 0$, y esto implica la formula.

   Para $a, b \in K^\times$, definimos
$$\left(\frac{a}{b}\right) = \prod_{v \notin S(a)} \left(\frac{a}{v}\right)^{ord_v(b)} = \left(\frac{a}{(b)^{S(a)}}\right)$$
donde $(b)^{S(a)}$ es el ideal en $I^{S(a)}$ generado por b. El símbolo $\left(\frac{a}{b}\right)$ es multiplicativo en b, pero $\left(\frac{aa'}{b}\right) = \left(\frac{a}{b}\right)\left(\frac{a'}{b}\right)$ no siempre se cumplirá a menos que $S(b) \cap S(a,a') = S$.

TEOREMA 3.2. *Ley de Reciprocidad.*
Sean $a, b \in K^\times$ tales que $S(a) \cap S(b) = S$ (por ejemplo a y b coprimos). Entonces

$$\left(\frac{a}{b}\right)\left(\frac{b}{a}\right)^{-1} = \prod_{v \in S}(b,a)_v.$$

DEMOSTRACIÓN. Sea $S'(a) = S(a) \setminus S$ y $S'(b) = S(b) \setminus S$. Nuestra suposición es que $S'(a)$ y $S'(b)$ son disjuntos. Entonces

$$\left(\frac{a}{b}\right) = \prod_{v \in S'(b)} \left(\frac{a}{\mathfrak{p}_v}\right)^{ord_v(b)} = \prod_{v \in S'(b)} (a,b)_v$$

y

$$\left(\frac{b}{a}\right) = \prod_{v \in S'(a)} \left(\frac{b}{\mathfrak{p}_v}\right)^{ord_v(a)} = \prod_{v \in S'(a)} (b,a)_v$$

Por tanto

$$\left(\frac{a}{b}\right)\left(\frac{b}{a}\right)^{-1} = \prod_{v \in S'(a) \cup S'(b)} (a,b)_v$$

Para $v \notin S \cup S'(a) \cup S'(b)$, $(a,b)_v = 1$, y por la formula del producto vemos que

$$\prod_{v \in S'(a) \cup S'(b)} (a,b)_v \times \prod_{v \in S}(a,b)_v = 1$$

□

Para obtener una formula completamente explicita, resta calcular el símbolo de Hilbert para $v \in S$. Para los primos infinitos, estos es fácil: si v es complejo, entonces $(a,b)_v = 1$ siempre, y si v es real, entonces

$$(a,b)_v = 1 \iff X^2 - aY^2 - bZ^2 \; representa \; 0 \iff a > 0 \, o \, b > 0$$

Para $K = \mathbb{Q}$ y $n = 2$,

$$(u2^r, v2^s)_2 = (-1)^{\frac{u-1}{2}\frac{v-1}{2} + r\frac{v^2-1}{8} + s\frac{u^2-1}{8}},$$

donde u, v son unidades 2-ádicas, y el exponente debe interpretarse modulo 2. Aplicando esto a los pares (p,q) con ambos primos impares, $(2,p)$ con p primo impar, y a $(-1,p)$ con p primo impar, se obtiene la ley de reciprocidad cuadrática clásica.

Para p un primo impar y $K = \mathbb{Q}[\zeta]$ con ζ una raíz primitiva p-ésima de la unidad, entonces se puede hacer el símbolo de Hilbert $(a,b)_p$ de manera explicita. Recordemos que p es totalmente ramificado en K y $(p) = (\pi)^{p-1}$, donde $\pi = 1 - \zeta$. Sea K_π la completación de K para (π), sea U_i el grupo de unidades en K_π congruente a 1 mod π^i. Tenemos una filtración

$$\mathcal{O}_{K_\pi}^\times \supset U_1 \supset U_2 \supset \cdots \supset U_{p+1} \supset \cdots .$$

Si $u \in U_{p+1}$, entonces u es una p-ésima potencia en K_π. De esto, se puede deducir que $K_\pi^\times / K_\pi^{\times p}$ es generado libremente (como un $\mathbb{F}_p$-espacio vectorial) por los elementos

$$\pi, \zeta, 1 - \pi^2, ..., 1 - \pi^p$$

Sea $\eta_i = 1 - \pi^i$, $i \geq 1$.

PROPOSICIÓN 3.3. *El Hilbert pairing*

$$a, b \mapsto (a, b)_\pi : K_\pi^\times \times K_\pi^\times \to \mu_p$$

es el único pairing simétrico satisfaciendo

1. $(\eta_i, \eta_j)_\pi = (\eta_i, \eta_{i+j})_\pi (\eta_{i+j}, \eta_j)_\pi (\eta_{i+j}, \pi)_\pi^{-j}$ *para todo* $i, j \geq 1$;
2. $(\eta_i, \pi)_\pi = \begin{cases} 1 \text{ si } 1 \leq i \leq p-1 \\ \zeta \text{ si } i = p \end{cases}$
3. $(.,.)_\pi = 1$ *en* $U_i \times U_j$ *si* $i + j \geq p + 1$.

EJEMPLO 3.4. (Ley de reciprocidad cubica ; Eisenstein). Sea $p = 3$, $K = \mathbb{Q}[\zeta]$, $\zeta = \frac{-1+\sqrt{3}}{2}$, y $\pi = -\zeta\sqrt{3}$. Entonces $\mathcal{O}_K = \mathbb{Z}[\zeta]$, y cada elemento no nulo de $\mathcal{O}_K$ puede ser escrito de la forma $\zeta^i \pi^j a$ con $a \equiv \pm 1 \, mod \, 3\mathcal{O}_K$. En este caso, la ley de reciprocidad se convierte en

$$\left(\frac{a}{b}\right) = \left(\frac{b}{a}\right)$$

si a y b son coprimos y congruentes con $\pm 1 \, mod \, 3\mathcal{O}_K$, y

$$\begin{cases} \left(\frac{\zeta}{a}\right) = \zeta^{-m-n} \\ \left(\frac{\pi}{a}\right) = \zeta^m \end{cases}$$

si $a = \pm(1 + 3(m + n\zeta))$.

Notamos que, si $a \in \mathbb{Z}$, entonces $a \equiv \pm 1 \, mod \, 3\mathcal{O}_K$ es automático.

Aplicación. Fijemos un primo impar p y una raíz p-ésima ζ de la unidad. Si x, y, z son enteros tales que $x^p + y^p = z^p$, entonces

$$\prod_{i=0}^{p-1} (x + \zeta^i y) = z^p.$$

Podemos suponer que x, y, z no tienen factores en común. Si $p \nmid xyz$, entonces los elementos $x + \zeta^i y \in \mathbb{Z}[\zeta]$ son coprimos. Por tanto, cada uno genera un ideal que es una p-ésima potencia y lo mismo es cierto para

$$\alpha = \frac{x + \zeta y}{x + y} = 1 - \frac{y\pi}{x + y}, \; \pi = 1 - \zeta.$$

Por tanto $\left(\frac{\beta}{\alpha}\right) = 1$ para todo $\beta \in \mathbb{Z}[\zeta]$ coprimo a α.

TEOREMA 3.5. *Sea* x, y, z *enteros positivos coprimos tales que* $p \nmid xyz$ *y* $x^p + y^p = z^p$. *Para cada primo* q *dividiendo* xyz, $q^{p-1} \equiv 1 \, mod \, p^2$.

DEMOSTRACIÓN. En este caso, la ley de reciprocidad se convierte en

$$\left(\frac{\beta}{\alpha}\right)\left(\frac{\alpha}{\beta}\right)^{-1} = \zeta^{Tr_{\mathbb{Q}[\zeta]*\mathbb{Q}(\eta)}},$$

donde $\eta = \frac{\beta-1}{p}\frac{\alpha-1}{\pi}$. Aplicamos esta ecuación con $\beta = q^{p-1}$. Sin pérdida de generalidad, podemos asumir que $q|y$, por tanto que $\alpha \equiv 1 \, mod \, q$ y $\left(\frac{\alpha}{q}\right) = 1$. Más aún,

$$Tr(\eta) = \frac{q^{p-1}-1}{p} Tr(\frac{\alpha-1}{\pi}),$$

pero

$$Tr(\frac{\alpha-1}{\pi}) = Tr(-\frac{y}{x+y}) = -\frac{y}{x+y}(p-1),$$

que no es divisible por p. Por tanto $\frac{q^{p-1}-1}{p}$ es divisible por p. □

Corolario 3.6. *(Condición de Wieferich) Si $X^p + Y^p = Z^p$ admite una solución x, y, z con x, y, z enteros positivos no divisibles por p, entonces $2^{p-1} \equiv 1 \, mod \, p^2$.*

Demostración. Si $x^p + y^p = z^p$, entonces al menos uno es par. □

Un argumento similar(con un β diferente) prueba la condición de Mirimanoff: $3^{p-1} \neq 1 \, mod \, p^2$.

Los únicos primos $< 3 \times 10^9$ que satisfacen la condición de Wieferich son 1093 y 3511, y no cumplen la condición de Mirimanoff. Esto prueba el primer caso del ultimo teorema de Fermat para $p < 3 \times 10^9$.

Bibliografía

[Con01] Keith Conrad. History of class field theory.
Disponible en kconrad.math.uconn.edu/blurbs/gradnumthy/cfthistory.pdf, 2001.

[Mil20] J.S. Milne. Class field theory (v4.03), 2020.
Disponible en www.jmilne.org/math/.

[Wei16] Jared Weinstein. Reciprocity laws and galois representations: recent breakthroughs. *Bulletin of the American Mathematical Society*, 53(1):1–39, 2016.

[Wym72] Bostwick F Wyman. What is a reciprocity law? *The American Mathematical Monthly*, 79(6):571–586, 1972.