Una introducción a la teoría de cuerpos de clase

Y una aplicación al teorema de Kronecker-Weber

José Cuevas Barrientos

Resumen. Ésta es una charla para el seminario de Teoría de Cuerpos de Clase Explícita organizado por Daniel Barrera, Ricardo Menares y Patricio Pérez. Aquí presentaremos los preliminares y las nociones básicas para la teoría de cuerpos de clase, específicamente teniendo en mente como aplicación el teorema de Kronecker-Weber.

Índice

La teoría de cuerpos de clase principalmente concierne a la relación entre la clasificación de extensiones de Galois de un cuerpo base K con determinados grupos de Galois y la aritmética de K. Esta exposición principalmente sigue a Neukirch **[3]**, estableciendo primero la maquinaria de cohomología de grupos finitos y culminando en los teoremas para el caso de cuerpos locales; hay una ardua discusión respecto al enfoque pedagógico de cómo aprender teoría de cuerpos de clase en `https://mathoverflow.net/a/6943`.

Los prerrequisitos no cubiertos por la exposición son principalmente resultados básicos de cuerpos locales y globales (expuestos, por ejemplo, en Neukirch **[3]**, Ch. II), y un cierto dominio o costumbre con los métodos cohomológicos.

Fecha: 18 de abril de 2024.

1. Preliminares

1.1. Cohomología de grupos y variación en un tema de Tate.

Definición 1.1: Sea G un grupo. Un ***G-módulo (derecho)*** es un grupo abeliano A, escrito en notación multiplicativa, con una acción $a\colon A \times G \to A$ (donde $x^g := a(x, g)$) tal que para todo $g, h \in G$ y $x, y \in A$ se cumplan:

$$x^e = x, \qquad (x^g)^h = x^{gh}, \qquad (x \cdot y)^g = x^g \cdot y^g.$$

Dado un G-módulo A, para un subgrupo $H \leq G$ se define el G-submódulo de invariantes por H como:

$$A^H := \{x \in A : \forall h \in H \quad x^h = x\}.$$

Defínase el anillo $\mathbb{Z}[G]$ que, como grupo aditivo es $\mathbb{Z}[G] = \bigoplus_{g \in G} \mathbb{Z} \cdot g$, con el producto

$$\left(\sum_{g \in G} a_g g\right) \cdot \left(\sum_{h \in G} b_g g\right) = \sum_{f \in G} \left(\sum_{gh = f} a_g b_h\right) f$$

Uno puede notar que un G-módulo derecho es lo mismo que un $\mathbb{Z}[G]$-módulo derecho. A veces cuando G es un grupo infinito se suelen añadir ciertas condiciones, en forma de continuidad en torno a topologías escogidas. La elección de la notación multiplicativa se hará clara en las aplicaciones más adelante.

Lema 1.2: Sea G un grupo finito y A un G-módulo. Mirando a $\mathbb{Z}$ como un G-módulo con la acción trivial, entonces

$$A_G \cong \mathbb{Z} \otimes_{\mathbb{Z}[G]} A, \qquad A^G \cong \operatorname{Hom}_{\mathbb{Z}[G]}(\mathbb{Z}, A).$$

En consecuencia, $A \mapsto A_G$ es un funtor exacto por la derecha y $A \mapsto A^G$ es exacto por la izquierda.

Demostración: Cfr. Weibel [**5,** pág. 161], Lemma 6.1.1. □

Definición 1.3: Sea G un grupo finito. Para todo G-módulo A y todo $q \geq 0$ entero, definimos su ***q-ésimo grupo de homología*** y ***de cohomología*** resp. como:

$$H_q(G, A) := \mathsf{L}^q\, A_G = \operatorname{Tor}_q^{\mathbb{Z}[G]}(\mathbb{Z}, A), \quad H^q(G, A) := \mathsf{R}^q\, A^G = \operatorname{Ext}^q_{\mathbb{Z}[G]}(\mathbb{Z}, A).$$

Aquí, los símbolos L^q y R^q denotan el q-ésimo funtor derivado izquierdo y derecho resp.; los cuales existen puesto que toda categoría de módulos posee suficientes inyectivos y proyectivos. El lector incómodo con el álgebra homológica, igual puede revisar la teoría de (co)homología de módulos, la cual admite exposiciones elementales.

Teorema 1.4: Sea G un grupo finito. Entonces $H_1(G, \mathbb{Z}) = G^{\text{ab}}$.

DEMOSTRACIÓN: Para ello, uno debe calcularle la homología a la sucesión exacta $0 \to \mathfrak{I} \to \mathbb{Z}[G] \to \mathbb{Z} \to 0$. Ésta demostración funciona para grupos arbitrarios, vid. WEIBEL [**5,** pág. 164], Thm. 6.1.11. □

Definición 1.5: Sea G un grupo finito. Definimos el ***homomorfismo de augmentación*** como

$$\operatorname{aug}\colon \mathbb{Z}[G] \longrightarrow \mathbb{Z} \qquad \sum_{g\in G} a_g g \longmapsto \sum_{g\in G} a_g$$

y denotamos por $\mathfrak{I}_G \trianglelefteq \mathbb{Z}[G]$ al núcleo de éste homomorfismo, llamado el ***ideal de augmentación***. Dicho ideal está generado por los elementos de la forma $g-1$ para todo $g \in G$.

Dado un G-módulo A (en notación multiplicativa), definimos el ***módulo de coinvariantes*** como:

$$A_G := A/\mathfrak{I}_G A = A/\langle \{a^g/a : g \in G\}\rangle,$$

(donde $\langle - \rangle$ denota el submódulo generado).

Si $G = \langle \sigma \rangle$ es un grupo finito cíclico, entonces el ideal de augmentación es el ideal principal generado por $\sigma - 1$.

Definición 1.6: Sea G un grupo finito. Dentro de $\mathbb{Z}[G]$ definimos el ***elemento norma*** como $N_G := \sum_{g\in G} g \in \mathbb{Z}[G]$; obviaremos el subíndice «G» de no haber ambigüedad. Para todo G-módulo A (en notación multiplicativa), la acción del elemento norma determina un endomorfismo, también llamado ***endomorfismo norma***:

$$\operatorname{Nm}\colon A \xrightarrow{\times N} A \qquad a \longmapsto \prod_{g\in G} a^g.$$

El núcleo de este endomorfismo se llama la N***-torsión de*** A y se denota por

$$A[N] := \{a \in A : \operatorname{Nm}(a) = 1\}.$$

Definición 1.7: Sea G un grupo finito y sea A un G-módulo. Para $q \in \mathbb{Z}$ entero (posiblemente negativo), definimos el q***-ésimo grupo de cohomología de Tate*** de A como:

$$\widehat{H}^q(G, A) := \begin{cases} H^q(G, A), & q \geq 1, \\ A^G/NA, & q = 0, \\ A[N]/\mathfrak{I}_G A, & q = -1, \\ H_{-1-q}(G, A) & q \leq -2. \end{cases}$$

Ejemplo. Sea G un grupo finito, entonces $\widehat{H}^{-2}(G,\mathbb{Z}) = G^{\mathrm{ab}}$.

Teorema 1.8: Sea G un grupo finito y sea $0 \to A \to B \to C \to 0$ una sucesión exacta de G-módulos. Entonces induce una sucesión exacta larga en cohomología de Tate:

$$\begin{tikzcd}
 & \cdots \arrow[r] & \widehat{H}^{q-1}(G,C) \arrow[dll, bend left, "\partial"] \\
\widehat{H}^{q}(G,A) \arrow[r] & \widehat{H}^{q}(G,B) \arrow[r] & \widehat{H}^{q}(G,C) \arrow[dll, bend left, "\partial"] \\
\widehat{H}^{q+1}(G,A) \arrow[r] & \cdots &
\end{tikzcd}$$

Demostración: Cfr. Harari [**1,** pág. 31], Thm. 2.6. □

Ejemplo. Sea $G = C_m$ un grupo finito cíclico. Para calcular los grupos de homología y cohomología del G-módulo $\mathbb{Z}$, podemos emplear la siguiente sucesión:

$$0 \longleftarrow \mathbb{Z} \xleftarrow{\text{aug}} \mathbb{Z}[G] \xleftarrow{\times(\sigma-1)} \mathbb{Z}[G] \xleftarrow{\times N} \mathbb{Z}[G] \xleftarrow{\times(\sigma-1)} \mathbb{Z}[G] \longleftarrow \cdots,$$

la cual afirmamos que es exacta ya que se satisface lo siguiente:

$$(\mathbb{Z}[G])^G = N \cdot \mathbb{Z}, \qquad (\sigma - 1)N = 0, \qquad \mathfrak{I} = \{a \in \mathbb{Z}[G] : Na = 0\}.$$

De esto concluimos que

$$H_q(C_m;\mathbb{Z}) = \left\{ \begin{array}{ll} \mathbb{Z}, & q = 0 \\ \mathbb{Z}/m\mathbb{Z}, & q \geq 1, 2 \nmid q \\ 0, & q \geq 2, 2 \mid q \end{array} \right\}; \quad H^q(C_m;\mathbb{Z}) = \begin{cases} \mathbb{Z}, & q = 0 \\ 0, & q \geq 1, 2 \nmid q \\ \mathbb{Z}/m\mathbb{Z}, & q \geq 2, 2 \mid q \end{cases}$$

Aplicando la última conclusión, obtenemos que:

Teorema 1.9: Sea G un grupo finito *cíclico* generado por σ. Entonces para todo G-módulo A se cumple que:

$$\widehat{H}^q(G,A) = \begin{cases} A^G/NA, & 2 \mid q, \\ A[N]/(\sigma - 1)A, & 2 \nmid q. \end{cases}$$

Demostración: Cfr. Weibel [**5,** págs. 167 s.]. □

Corolario 1.9.1: Sea G un grupo finito cíclico y sea $0 \to A \to B \to C \to 0$ una sucesión exacta de G-módulos. Entonces induce el siguiente diagrama conmutativo exacto:

$$\begin{tikzcd}
 & \widehat{H}^0(G,A) \arrow[r] & \widehat{H}^0(G,B) \arrow[dr] & \\
\widehat{H}^{-1}(G,C) \arrow[ur] & & & \widehat{H}^0(G,C) \arrow[dl] \\
 & \widehat{H}^{-1}(G,B) \arrow[ul] & \widehat{H}^{-1}(G,A) \arrow[l] &
\end{tikzcd}$$

Demostración: Se sigue de la sucesión exacta larga en cohomología de Tate sumado al que los grupos de cohomología son 2-periódicos cuando G es cíclico. □

Definición 1.10: Sea G un grupo finito y M un G-módulo tal que

$$|\widehat{H}^{-1}(G,M)| < \infty, \qquad |\widehat{H}^0(G,M)| < \infty. \tag{1}$$

Se define su ***cociente de Herbrand*** como

$$h(G,M) := \frac{|\widehat{H}^0(G,M)|}{|\widehat{H}^{-1}(G,M)|}.$$

Por ejemplo, (1) se satisface cuando M es finito.

Proposición 1.11: Sea G un grupo cíclico y sea $0 \to A \to B \to C \to 0$ una sucesión exacta corta de G-módulos tales que (1) se satisface para dos de tres G-módulos. Entonces también se satisface para el tercero y

$$h(G,B) = h(G,A)\,h(G,C).$$

Además, para todo G-módulo finito A, se cumple que $h(G,A) = 1$.

Demostración: Denotaremos por $h^p(X) := |\widehat{H}^p(G,X)|$. Del hexágono exacto deducimos la siguiente sucesión exacta:

$$\begin{tikzcd}
0 \arrow[r] & I \arrow[r] & \widehat{H}^0(G,A) \arrow[r] & \widehat{H}^0(G,B) \arrow[r] & \widehat{H}^0(G,C) \arrow[dll, bend left] & & \\
 & & \widehat{H}^1(G,A) \arrow[r] & \widehat{H}^1(G,B) \arrow[r] & \widehat{H}^1(G,C) \arrow[r] & I \arrow[r] & 0
\end{tikzcd}$$

donde

$$I := \operatorname{im}(\widehat{H}^1(G,B) \to \widehat{H}^1(G,C)) = \ker(\widehat{H}^0(G,A) \to \widehat{H}^0(G,B)).$$

Denotando por $s := |I|$, entonces la sucesión exacta implica que tenemos la siguiente identidad en cardinalidades:

$$sh^0(B)h^1(A)h^1(C) = h^0(A)h^0(C)h^1(B)s,$$

que despejando nos da la identidad en cocientes de Herbrand. □

1.2. Cuerpos locales y ramificación.

Definición 1.12: Un ***cuerpo p-ádico*** K es una extensión finita de $\mathbb{Q}_p$; su *anillo de valuación*[1] $(\mathfrak{o}, \mathfrak{m})$ es la clausura entera de $(\mathbb{Z}_p, p\mathbb{Z}_p)$ en K.

Recíprocamente, si $L \supseteq \mathbb{Q}$ es un cuerpo numérico y $\mathfrak{p} \lhd \mathcal{O}_L$ es un primo tal que $\mathfrak{p} \cap \mathbb{Z} = p\mathbb{Z}$, entonces la completación $\mathfrak{p}$-ádica de $\mathcal{O}_L$ es un anillo de valuación $(\mathfrak{o}, \mathfrak{m})$ cuyo cuerpo de fracciones K es una extensión finita de $\mathbb{Q}_p$; es decir, es un cuerpo p-ádico.

Un *cuerpo local ultramétrico* de característica 0 es un cuerpo p-ádico para algún $p > 0$ primo; el lector incómodo con la palabra «cuerpo local» puede considerar que éste siempre es el caso.

Desde aquí en adelante fijaremos la siguiente notación: Sea K un cuerpo local ultramétrico, es decir, un cuerpo completo respecto a una métrica no arquimediana y cuyo anillo de valuación $(\mathfrak{o}_K, \mathfrak{m}_K, k)$ es un dominio de valuación discreta. Denotaremos por $v_K \colon K^\times \to \mathbb{Z}$ a la valuación discreta normalizada de K y por π a un uniformizador de $\mathfrak{o}_K$. Denotaremos por $U_K := \mathfrak{o}_K^\times$ el grupo de unidades de K, esto equivale a los $\alpha \in K$ de $v_K(\alpha) = 0$. Denotaremos por

$$U_K^{(n)} := 1 + \mathfrak{m}_K^n = \{\alpha \in U_K : v_K(\alpha - 1) \geq n\}.$$

Proposición 1.13: Sea $K \supseteq \mathbb{Q}_p$ un cuerpo p-ádico con anillo de valuación $(\mathfrak{o}, \mathfrak{p})$ y sea $e \geq 1$ el entero, tal que $p\mathfrak{o} = \mathfrak{p}^e$. Entonces las series formales de potencias

$$\exp(x) := 1 + x + \frac{x^2}{2!} + \frac{x^3}{3!} + \cdots, \qquad \log(1+x) := x - \frac{x^2}{2} + \frac{x^3}{3} - \cdots$$

establecen isomorfismos (topológicos), uno el inverso del otro:

$$\mathfrak{p}^n \underset{\log}{\overset{\exp}{\rightleftarrows}} U_K^{(n)}$$

para todo $n > e/(p-1)$.

Demostración: La condición $n > e/(p-1)$ está exclusivamente para que las series formales de exp y log converjan $\mathfrak{p}$-ádicamente. El que sean continuos es claro y el que determinen homomorfismos es mera álgebra de series formales. El que uno sea la inversa del otro es un cálculo, detallado en Neukirch [**3,** pág. 137], Prop. II.5.5. □

2. Cohomología de Galois

Ésta sección está fuertemente inspirada en los capítulos 4 y 5 de Neukirch [**3**]. Otra posible referencia es el libro de Serre [**4**].

[1] Se llama así porque $\mathfrak{o}$ es noetheriano y $\mathfrak{m}$ es el único ideal maximal de $\mathfrak{o}$. También el nombre se justifica si introducimos las nociones de «valuación» o «valor absoluto».

Definición 2.1: Una extensión algebraica L/k se dice ***cíclica*** (resp. ***abeliana***) si está contenida en una extensión de Galois $k \subseteq L \subseteq F$ tal que $\mathrm{Gal}(F/k)$ es un grupo cíclico (resp. abeliano). Una extensión L/k se dice ***ciclotómica*** si L está contenido en una extensión generada por raíces de la unidad.

NEUKIRCH [**3**] se refiere al siguiente teorema como el «axioma de la teoría de cuerpos de clase»:

Teorema 2.2: Sea L/K una extensión cíclica de cuerpos locales ultramétricos, se cumplen:

$$\left|\widehat{H}^q\big(\mathrm{Gal}(L/K), L^\times\big)\right| = \begin{cases} [L:K], & q = 0, \\ 1, & q = -1. \end{cases}$$

DEMOSTRACIÓN: Denótese $G := \mathrm{Gal}(L/K)$. El caso $q = -1$ se reduce a probar que para todo $\alpha \in L^\times$ de $\mathrm{Nm}_{L/K}(\alpha) = 1$, existe $\beta \in L^\times$ tal que $\alpha = \sigma(\beta)/\beta$, lo cual es el teorema 90 de Hilbert (cfr. NEUKIRCH [**3,** pág. 281], Prop. IV.3.5).

Para el caso $q = 0$, consideramos la sucesión exacta

$$0 \longrightarrow U_L \hookrightarrow L^\times \xrightarrow{v_L} \mathbb{Z} \longrightarrow 0.$$

Es fácil calcular que $h(G, \mathbb{Z}) = [L : K]$, por lo que por la identidad en cocientes de Herbrand, basta probar que $h(G, U_L) = 1$.

Para ello, sea $\alpha \in L$ tal que $\{\alpha^\sigma : \sigma \in G\}$ sea una K-base de L (teorema de la base normal), y defínase el G-módulo $M := \sum_{\sigma\in G} \alpha^\sigma \mathcal{O}_K$ que es abierto, y sean

$$V_n := 1 + \pi^n M \subseteq U_K$$

los cuales son G-submódulos de índice finito, por lo que la sucesión exacta $1 \to V_n \to U_K \to U_K/V_n \to 1$ comprueba que $h(G, U_K) = h(G, V_n)$. Para ver que $\widehat{H}^{-1}(G, V_n) = 1$ empleamos el teorema 90 de Hilbert y argumentamos el por qué el β lo podemos escoger dentro de V_n. Para ver que $\widehat{H}^0(G, V_n) = 1$ □

Definición 2.3: Si L/k es una extensión finita, llamamos el ***grupo de normas*** de L/k a

$$\mathrm{Nm}_{L/k}(L^\times) = \{\mathrm{Nm}_{L/k}(\beta) : \beta \in L^\times\}.$$

Los siguientes dos resultados son piedras angulares de la teoría de cuerpos de clase. El segundo puede interpretarse como una conexión de Galois.

Teorema 2.4 (ley de reciprocidad local): Sea L/K una extensión finita de Galois entre cuerpos locales ultramétricos. Existe un isomorfismo canónico:

$$r_{L/K}\colon\ \mathrm{Gal}(L/K)^{\mathrm{ab}} \longrightarrow K^\times / \operatorname{Nm}_{L/K} L^\times = \widehat{H}^0(\mathrm{Gal}(L/K), L^\times).$$

Demostración: Vamos a hacer la prueba cuando $\mathrm{Gal}(L/K)$ es cíclico.

Consideremos la sucesión exacta $0 \longrightarrow U_L \hookrightarrow L^\times \xrightarrow{v_L} \mathbb{Z} \longrightarrow 0$ de $\mathrm{Gal}(L/K)$-módulos. Luego, podemos aplicar el corolario 1.9.1 para obtener el diagrama exacto:

$$\begin{tikzcd}
 & \widehat{H}^0(G,U_L) \arrow[r] & \widehat{H}^0(G,L^\times) \arrow[dr, "\varphi"] & \\
\widehat{H}^{-1}(G,\mathbb{Z}) \arrow[ur] & & & \widehat{H}^0(G,\mathbb{Z}) \arrow[dl] \\
 & \widehat{H}^{-1}(G,L^\times) \arrow[ul, "\psi"] & \widehat{H}^{-1}(G,U_L) \arrow[l] &
\end{tikzcd}$$

Por un cálculo, sabemos que $\widehat{H}^0(G,\mathbb{Z}) \cong G^{\mathrm{ab}}$, por lo que nos interesaría que φ fuese un isomorfismo. Ahora bien, $\widehat{H}^{-1}(G,L^\times) = 0$ por el teorema anterior y $\widehat{H}^{-1}(G,\mathbb{Z})$ es un cociente de la N-torsión de $\mathbb{Z}$, el cual es fácil ver que también es nulo. Así que ψ es un isomorfismo, por lo que $\widehat{H}^0(G,U_L)$ y $\widehat{H}^{-1}(G,U_L)$ son nulos.

La idea es reducir el caso general al caso de extensiones cíclicas, para lo cual véase Neukirch [**3,** págs. 300 s.]. □

Definición 2.5: Sea L/K una extensión finita de Galois entre cuerpos locales ultramétricos. Definimos el ***símbolo de Artin local*** como el epimorfismo

$$(-, L/K)\colon K^\times \longrightarrow \mathrm{Gal}(L/K)^{\mathrm{ab}}$$

dado por la composición de la proyección $K^\times / \operatorname{Nm}_{L/K} L^\times$ con $r_{L/K}^{-1}$.

Definición 2.6: Sea K un cuerpo local ultramétrico. Dotamos a $K^\times$ de la ***topología de la norma***: para cada $\alpha \in K^\times$ las clases laterales $\alpha \operatorname{Nm}_{L/K} L^\times$ forman una base de entornos de a, donde L/K recorre las extensiones finitas de Galois.

Para diferenciar, la topología subespacio sobre $K^\times$ será referida como la *usual*. La ventaja de la topología de la norma es que $\operatorname{Nm}_{L/K} L^\times \leq K^\times$ son subgrupos abiertos.

Lema 2.6.A: Sea K un cuerpo local ultramétrico, y sea $H \leq K^\times$ un subgrupo. Son equivalentes:

1. El conjunto H es abierto en la topología de la norma.
2. El conjunto H es cerrado en la topología de la norma y tiene índice finito.

3. El conjunto H es abierto en la topología usual y tiene índice finito.

Demostración: 2 $\implies$ 1. Trivial, pues su complemento es la unión de sus finitas clases laterales restantes.

1 $\implies$ 2. El conjunto H es cerrado pues

$$H^c = \bigcup_{\substack{a \in K^\times \\ aH \neq H}} aH,$$

es abierto por ser unión de abiertos. Ahora bien, por definición de la topología de la norma, $H \supseteq \mathcal{N} = \operatorname{Nm}_{L/K} L^\times$, donde L/K es una extensión finita de Galois, y $\mathcal{N}$ tiene índice finito por la ley de reciprocidad local.

1 $\implies$ 3. Sea $V \subseteq K^\times$ abierto en la topología de la norma, de modo que contiene a un grupo de normas $\operatorname{Nm}_{L/K} L^\times$ de una extensión finita de Galois y, en consecuente, también a $\operatorname{Nm}_{L/K} U_L$. Ahora bien, U_L es compacto, de modo que $\operatorname{Nm}_{L/K} U_L$ también, así que es cerrado, pero también tiene índice finito en U_K el cual es abierto en $K^\times$. Así que $\operatorname{Nm}_{L/K} U_L$ es abierto en U_K, y por tanto V es un entorno de $1 \in K^\times$; trasladando se verifica sobre un punto cualquiera.

3 $\implies$ 1. Esta es la implicación difícil, vid. Neukirch [**3,** págs. 321 ss.] para más detalles. □

Lema 2.6.B: Sea K un cuerpo local ultramétrico y sea L/K una extensión finita. Entonces su grupo de normas $\operatorname{Nm}_{L/K} L^\times$ es exactamente el mismo que el de su subextensión abeliana maximal $E \subseteq L$.

Teorema 2.7 (de existencia): Sea K un cuerpo local ultramétrico. La aplicación

$$L \longmapsto \mathcal{N}_L := \operatorname{Nm}_{L/K} L^\times$$

establece una biyección entre extensiones abelianas finitas de K y subgrupos abiertos de índice finito en $K^\times$, con respecto a la topología usual. Además:

$$L \subseteq F \iff \mathcal{N}_L \supseteq \mathcal{N}_F, \qquad \mathcal{N}_{LF} = \mathcal{N}_L \cap \mathcal{N}_F, \qquad \mathcal{N}_{L\cap F} = \mathcal{N}_L \mathcal{N}_F.$$

Demostración: Por el lema anterior, probaremos la equivalencia con subgrupos abiertos de $K^\times$ en la topología de la norma.

Es claro de la transitividad de la norma que $\mathcal{N}_{LF} \subseteq \mathcal{N}_L \cap \mathcal{N}_F$. También es claro que

$$\begin{aligned} \mathcal{N}_L \subseteq \mathcal{N}_F &\iff \mathcal{N}_L \cap \mathcal{N}_F = \mathcal{N}_{LF} = \mathcal{N}_F \\ &\iff [LF : K] = [F : K] \iff L \subseteq F, \end{aligned}$$

donde en la penúltima equivalencia empleamos la ley de reciprocidad local. Esto prueba que la aplicación $\mathcal{N}_{-}$ es inyectiva.

Sea $\mathcal{N} \leq K^\times$ un subgrupo abierto en la topología de la norma, de modo que existe una extensión abeliana finita F/K tal que $\mathcal{N} \supseteq \mathcal{N}_F = \operatorname{Nm}_{F/K} F^\times$, luego $(\mathcal{N}, F/K) = \mathrm{Gal}(F/L)$ para algún subcuerpo $K \subseteq L \subseteq F$, de modo que $\mathcal{N}$ es el núcleo de $(-, L/K)\colon K^\times \to \mathrm{Gal}(L/K)$; lo que prueba que $L \mapsto \mathcal{N}_L$ es sobreyectiva.

Finalmente como $L \cap F \subseteq L$ y $L \cap F \subseteq F$ obtenemos que $\mathcal{N}_{L\cap F} \supseteq \mathcal{N}_L \mathcal{N}_F$. Como $\mathcal{N}_L\mathcal{N}_F$ es abierto (¿por qué?), existe $M \supseteq K$ tal que $\mathcal{N}_L\mathcal{N}_F = \mathcal{N}_M$ y, como $\mathcal{N}_M \supseteq \mathcal{N}_L$, entonces $M \subseteq L \cap F$. Concluimos pues

$$\mathcal{N}_L\mathcal{N}_F = \mathcal{N}_M \supseteq \mathcal{N}_{L\cap F} \supseteq \mathcal{N}_L\mathcal{N}_F. \qquad \square$$

También al teorema anterior a veces le llaman el «teorema fundamental de la teoría de cuerpos de clase»; parte de la razón tiene que ver con el siguiente corolario que ofrece otra lectura al teorema:

Corolario 2.7.1: El símbolo de Artin local establece un isomorfismo topológico $\widehat{K^\times} \to \mathrm{Gal}(K^{\mathrm{ab}}/K)$, donde K^{ab} es la extensión abeliana maximal de K y donde $\widehat{K^\times}$ es la completación profinita de $K^\times$ dotado de la topología de la norma. En consecuencia:

$$\mathrm{Gal}(K^{\mathrm{ab}}/K) \cong \widehat{\mathbb{Z}} \times U_K.$$

La siguiente demostración emplea la teoría de los grupos profinitos; el lector interesado está referido al resumen de Harari [**1,** págs. 65 ss.], §4.1 o al exhaustivo texto sobre grupos profinitos de Wilson [**6**].

Demostración: El símbolo de Artin local nos da un epimorfismo continuo $K^\times \to \mathrm{Gal}(L/K)$ para toda extensión abeliana finita, luego induce, en el límite, un homomorfismo continuo $K^\times \to \mathrm{Gal}(K^{\mathrm{ab}}/K)$ que, en cocientes por subgrupos abiertos, induce un isomorfismo, y concluimos pues

$$\widehat{K^\times} = \varprojlim_{U \triangleleft_o K^\times} K^\times/U = \varprojlim_{L} \mathrm{Gal}(L/K) = \mathrm{Gal}(K^{\mathrm{ab}}/K).$$

El otro isomorfismo es porque $K^\times = \mathbb{Z} \times U_K$. $\square$

2.1. Aplicación: El teorema de Kronecker-Weber.

Proposición 2.8: El grupo de normas de $\mathbb{Q}_p(\zeta_{p^n})/\mathbb{Q}_p$ es $(p) \times U_{\mathbb{Q}_p}^{(n)}$.

Demostración: La extensión $\mathbb{Q}_p(\zeta_{p^n})/\mathbb{Q}_p$ tiene grado $p^{n-1}(p-1)$, lo cual ha de ser el índice del grupo de normas en $\mathbb{Q}_p^\times$ por la ley de reciprocidad local. Por la proposición 1.13 tenemos el siguiente isomorfismo topológico

$$\exp\colon \mathfrak{p}_K^m \longrightarrow U_K^{(m)},$$

donde $K = \mathbb{Q}_p$, para todo $m \geq 1$ cuando $p > 2$ y para todo $m \geq 2$ cuando $p = 2$. Considere la función

$$\varphi\colon \mathfrak{p}_K^m \to \mathfrak{p}_K^{m+n-1}, \qquad x \mapsto p^{n-1}(p-1)x,$$

la cual establece claramente un isomorfismo y así construimos el siguiente diagrama conmutativo:

$$\begin{tikzcd}
\mathfrak{p}_K^m \arrow[r, "\exp", "\sim"'] \arrow[d, "\varphi"'] & U_K^{(m)} \arrow[d, dashed, "\exists!\psi"] \\
\mathfrak{p}_K^{m+n-1} \arrow[r, "\sim", "\exp"'] & U_K^{(m+n-1)}
\end{tikzcd}$$

donde $\psi(z) = z^{p^{n-1}(p-1)} = \operatorname{Nm}_{L/K}(z)$ y donde $L := \mathbb{Q}_p(\zeta_{p^n})$. Como además $\operatorname{Nm}_{L/K}(1-\zeta_{p^n}) = p$, entonces concluimos que $(p)\times U_K^{(n)} \subseteq \operatorname{Nm}_{L/K} L^\times$. Finalmente, la igualdad se deduce de que ambos grupos tienen índice $p^{n-1}(p-1)$ en $K^\times$. $\square$

Corolario 2.8.1 (Kronecker-Weber local): Toda extensión abeliana finita $L/\mathbb{Q}_p$ es ciclotómica. En consecuencia, la extensión abeliana maximal $\mathbb{Q}_p^{\text{ab}}/\mathbb{Q}_p$ está generada por adjuntar todas las raíces de la unidad.

Demostración: Sea $L \supseteq K := \mathbb{Q}_p$ una extensión abeliana finita de Galois, entonces existen enteros f, n tales que $(p^f)\times U_K^{(n)} \subseteq \operatorname{Nm}_{L/K} L^\times$. Escribamos dicho subgrupo como

$$(p^f) \times U_K^{(n)} = \big((p^f) \times U_K\big) \cap \big((p) \times U_K^{(n)}\big),$$

por el teorema de existencia vemos que su cuerpo de clases es el composito entre el cuerpo de clases de $(p) \times U_K^{(n)}$; el cual por la proposición anterior es $\mathbb{Q}_p(\zeta_{p^n})$, y el cuerpo de clases de $(p^f) \times U_K$; el cual es $\mathbb{Q}_p(\zeta_{p^f-1})$, por lo que

$$L \subseteq \mathbb{Q}_p\left(\zeta_{(p^f-1)p^n}\right). \qquad \square$$

Teorema 2.9 (Kronecker-Weber): Toda extensión abeliana finita $L/\mathbb{Q}$ es ciclotómica.

Demostración: Sea $L \neq \mathbb{Q}$ una extensión abeliana. Sea S el conjunto de los primos $p \in \mathbb{Z}$ en los cuales L se ramifica, el cual es no vacío por el teorema de Hermite-Minkowski; sea $\mathfrak{p} \mid p$ un primo de $\mathcal{O}_L$ y denótese por $L_\mathfrak{p}$ la completación $\mathfrak{p}$-ádica. Como la extensión $L_\mathfrak{p}/\mathbb{Q}_p$ es abeliana, existe n_p tal que $L_\mathfrak{p} \subseteq \mathbb{Q}_p(\zeta_{a_p})$. Sea e_p tal que $p^{e_p} \mid n_p$, pero $p^{e_p+1} \nmid n_p$; entonces definimos

$$n := \prod_{p\in S} p^{e_p}.$$

Sea $\mathfrak{P} \mid \mathfrak{p}$ en M, entonces

$$M_\mathfrak{P} = L_\mathfrak{p}(\zeta_n) = \mathbb{Q}_p(\zeta_{p^{e_p}n'}) = \mathbb{Q}_p(\zeta_{p^{e_p}})\mathbb{Q}_p(\zeta_{n'}),$$

donde $p \nmid n'$. Se cumple que $\mathbb{Q}_p(\zeta_{n'}) = M_{\mathfrak{P}} \cap \mathbb{Q}_p^{\mathrm{nr}}$, por lo que el grupo de inercia $I_p(M_{\mathfrak{P}}/\mathbb{Q}_p)$ es isomorfo al grupo $\mathrm{Gal}(\mathbb{Q}_p(\zeta_{p^{e_p}})/\mathbb{Q}_p)$, el cual tiene cardinalidad $\phi(p^{e_p}) = p^{e_p-1}(p-1)$. Sea I el subgrupo de $\mathrm{Gal}(M/\mathbb{Q})$ generado por todos los I_p's; el cuerpo fijo de I es no ramificado sobre $\mathbb{Q}$, por lo que es el mismo $\mathbb{Q}$ y, por tanto, $I = \mathrm{Gal}(M/\mathbb{Q})$. Contemos:

$$[M:\mathbb{Q}] = |I| \leq \prod_{p\in S} |I_p(M_{\mathfrak{P}}/\mathbb{Q}_p)| = \prod_{p\in S} \phi(p^{e_p}) = \phi(n) = [\mathbb{Q}(\zeta_n):\mathbb{Q}],$$

de esta igualdad de grados se sigue que $M = \mathbb{Q}(\zeta_n) \supseteq L$. □

Apéndice A. Comentarios adicionales

A.1. Teoremas avanzados. La «ley de reciprocidad local» (teorema 2.4) puede considerarse como un caso particular del siguiente teorema:

Teorema A.1 (Tate-Nakayama): Sea G un grupo finito y sea A un G-módulo. Para cada primo p sea G_p un p-subgrupo de Sylow de G tales que:

1. $H^1(G_p, A) = 0$.
2. $|H^2(G_p, A)| = |G_p|$.

Entonces para cada subgrupo $H \leq G$ existe un isomorfismo para cada $q \in \mathbb{Z}$:

$$\widehat{H}^q(H, G) \cong \widehat{H}^{q+2}(H, A).$$

Demostración: Vid. Harari [**1,** pág. 62], Thm. 3.14. El enunciado allí es más preciso también, podemos hacer explícito el isomorfismo. □

Nótese que el teorema 2.2 precisamente indica que las dos condiciones para el teorema de Tate-Nakayama se satisfacen.

Para probar el lema fundamental (2.6.A) podemos recurrir a la *teoría de Lubin-Tate*, que involucra un tipo de series formales de potencias llamadas «leyes de grupo formal». Con ella obtenemos la existencia del siguiente cuerpo:

Teorema A.2: Para cada uniformizador π de un cuerpo local ultramétrico existe una sucesión de extensiones de cuerpo:

$$K \subseteq K_\pi^1 \subseteq K_\pi^2 \subseteq \cdots \subseteq K_\pi$$

tales que K_π/K es una extensión abeliana, $\mathrm{Gal}(K_\pi/K_\pi^n) \cong U_K^n$ y para todo n se cumple que $\pi \in \mathcal{N}_{K_\pi^n}$ está en el grupo de normas.

Demostración: Vid. Harari [**1,** págs. 152 s.], Thm. 11.13. □

Para la reciprocidad global (e.g. sobre $\mathbb{Q}$ y no $\mathbb{Q}_p$) uno debe recurrir a la bella teoría de idèles y adèles, las cuales están presentadas en varios textos (e.g., Neukirch [**3**], §VI.1-VI.3; o Harari [**1**], §12.3 y §13.1), pero que lamentablemente no alcanzan a cubrirse en detalle aquí.

A.2. Notas históricas. La «ley de reciprocidad local» y el «teorema de existencia» (teorema 2.7) fueron ambos demostrados por el japonés Teiji Takagi en [**16**] (1920) y [**17**] (1922). El isomorfismo fue explicitado por el francés Emil Artin mediante el símbolo de Artin, introducido primero en [**7**] (1924); para ello, Artin necesitó esperar cuatro años a la salida del teorema de densidad de Chebotarev para lograr su teorema de reciprocidad en [**8**] (1927).

Curiosamente, la teoría de cuerpos de clases *global* precedió a la teoría *local*, la cual fue desarrollada conjuntamente por Schmidt [**15**] (1930) y Chevalley [**9**] (1933). El francés Herbrand [**10**] (1931) fue uno de los impulsores de la cohomología de grupos como medio para el estudio local de la teoría de cuerpos de clase; esto, por supuesto, estaría en sincronía con la filosofía adoptada más adelante por la escuela francesa (Chevalley, Grothendieck, Serre, Weil, *etc.*). No obstante, algunos métodos cohomológicos son un tanto abstractos y «pierden» información acerca de los isomorfismos involucrados; esta fue una de las dificultades a superar por la teoría de Lubin y Tate [**13**] (1965).

El teorema de Kronecker-Weber fue conjeturado por Kronecker [**12**] (1853) y más tarde fue supuestamente demostrado por Weber [**18**] (1886) y [**19**] (1887); no obstante, existe cierto debate acerca de si las pruebas de ambos habrán contenido errores de cierto tipo (cfr. Neumann [**14**]). La demostración de Hilbert [**11**] (1896) es generalmente reconocida como «completa» y autores afirman que fue la *verdadera* primera demostración del teorema de Kronecker-Weber; sin entrar en controversias, podemos afirmar que las ideas de Hilbert fueron indiscutiblemente influyentes y sirvieron de inspiración para desarrollar a fondo la teoría de cuerpos de clase.

Las notas históricas son gracias a Hasse [**2**].

Referencias

1. Harari, D. *Galois Cohomology and Class Field Theory* (Springer-Verlag, 2020).
2. Hasse, H. *History of Class Field Theory* en *Algebraic Number Theory* (eds. Cassels, J. W. S. y Fröhlich, A.) (Academic Press, 1967), 305-347.
3. Neukirch, J. *Algebraic Number Theory* trad. por Schappacher, N. (Springer-Verlag Berlin Heidelberg, 1992).
4. Serre, J.-P. *Local fields* trad. por Greenberg, M. J. (Springer-Verlag, 1980).
5. Weibel, C. A. *An introduction to homological algebra Cambridge Studies in Advanced Mathematics* **38** (Cambridge University Press, 1994).
6. Wilson, J. S. *Profinite groups* (Oxford University Press, 1999).

Artículos y documentos históricos

7. Artin, E. Über eine neue Art von L-Reihen. *Abh. Math. Semin. Univ. Hamburg* **3,** 89-108 (1924).
8. Artin, E. Beweis des allgemeinen Reziprozitätsgesetzes. *Abh. Math. Semin. Univ. Hamburg* **5,** 46-51 (1927).

9. Chevalley, C. La théorie du symbote de restes normiques. *J. reine angew. Math.* **169,** 140-157. doi:10.1515/crll.1933.169.140 (1933).
10. Herbrand, J. Sur la théorie des groupes de décomposition, d'inertie et de ramification. *J. Math. pures appl.* **10,** 481-498 (1931).
11. Hilbert, D. Ein neuer Beweis des Kronecker'schen Fundamentalsatzes über Abel'sche Zahlkörper. *Nachr. Ges. Wiss. Göttingen,* 29-39. https://eudml.org/doc/58336 (1896).
12. Kronecker, L. Über die algebraisch auflösbaren Gleichungen I. *Sber. preuss. Akad. Wiss.,* 365-374 (1853).
13. Lubin, J. y Tate, J. Formal Complex Multiplication in Local Fields. *Ann. Math.* doi:10.2307/1970622 (1965).
14. Neumann, O. Two proofs of the Kronecker-Weber theorem "according to Kronecker, and Weber". *J. reine angew. Math.* **323,** 105-126. doi:10.1515/crll.1981.323.105 (1981).
15. Schmidt, F. K. Zur Klassenkörpertheorie im Kleinen. *J. reine angew. Math.* **162,** 155-168. doi:10.1515/crll.1930.162.155 (1930).
16. Takagi, T. Über eine Theorie des relativ-Abel'schen Zahlkörpers. *J. Coll. Sci. imp. Univ. Tokyo* **41,** 1-133 (1920).
17. Takagi, T. Über das Reziprozitätsgesetz in einem beliebigen algebraischen Zahlkörpers. *J. Coll. Sci. imp. Univ. Tokyo* **44,** 1-50 (1922).
18. Weber, H. Theorie der Abel'schen Zahlkorper I. *Acta math. Stockh.* **8,** 193-263 (1886).
19. Weber, H. Theorie der Abel'schen Zahlkorper II. *Acta math. Stockh.* **9,** 105-130 (1887).

Correo electrónico: josecuevasbtos@uc.cl

Departamento de Matemáticas, Pontificia Universidad Católica de Chile. Facultad de Matemáticas, 4860 Av. Vicuña Mackenna, Macul, RM, Chile
URL: josecuevas.xyz