TEORÍA DE CUERPOS DE CLASES

PATRICIO PÉREZ PIÑA

1. Ramificación

Sea K un cuerpo de números. Los ideales primos de $\mathcal{O}_K$ serán llamados primos finitos de K y por otra parte, los morfismos $\sigma\colon K \to \mathbb{C}$ serán denominados primos infinitos de K. Diremos que un primo finito $\mathfrak{p}$ de K es ramificado en una extensión de cuerpos de números L/K si existe un primo finito $\mathfrak{P}$ de L tal que $\mathfrak{p} \subseteq \mathfrak{P}^2$. En caso contrario decimos que $\mathfrak{p}$ es no ramificado. Un primo infinito $\sigma\colon K \to \mathbb{C}$ es real si $\sigma(K) \subset \mathbb{R}$ y es complejo en el caso contrario. Decimos que $\sigma\colon K \to \mathbb{C}$ es ramificado en L/K si es real y existe un primo infinito y complejo $\widetilde{\sigma}$ de L tal que $\widetilde{\sigma}|_K = \sigma$. Naturalemente, de no ocurrir lo anterior decimos que σ es no ramificado.[1]

2. Teoría de cuerpos de clases(CFT)

Definición 2.1. Dado K un cuerpo de números K, un módulo en K es un producto formal

$$\mathfrak{m} = \prod_{\mathfrak{p}} \mathfrak{p}^{n_\mathfrak{p}},$$

donde $\mathfrak{p}$ recorre todos los primos de K, los enteros $n_\mathfrak{p}$ son no negativos, $n_\mathfrak{p} = 0$ salvo un número finito de primos, $n_\mathfrak{p} = 0$ si $\mathfrak{p}$ es complejo y $n_\mathfrak{p} \leq 1$ si $\mathfrak{p}$ es real.

Observaciones 2.2.

1. Si $\mathfrak{m}$ es un módulo en K, entonces $\mathfrak{m} = \mathfrak{m}_0\mathfrak{m}_\infty$, donde $\mathfrak{m}_0$ se identifica con un ideal de $\mathcal{O}_K$ y $\mathfrak{m}_\infty$ es un producto finito de primos infinitos y reales de K.
2. Como caso particular, si K es puramente imaginario entonces todo módulo $\mathfrak{m}$ es igual a $\mathfrak{m}_0$.
3. Cuando $n_\mathfrak{p} = 0$ para todo primo $\mathfrak{p}$ escribimos $\mathfrak{m} = 1$.
4. Decimos que un módulo $\mathfrak{m}$ divide $\mathfrak{n}$ si para todo primo $\mathfrak{p}$, los exponentes de $\mathfrak{m}$ en $\mathfrak{p}$ son menores o iguales a los de $\mathfrak{n}$.

Definición 2.3. Sea $\mathfrak{m}$ un módulo en K. El grupo $I_K(\mathfrak{m})$ es el conjunto de todos los ideales fraccionarios de $\mathcal{O}_K$ que son primos relativos con $\mathfrak{m}$ junto a la multiplicación como su ley interna. Denotaremos por $P_{K,1}(\mathfrak{m})$ al subgrupo $\{\alpha\mathcal{O}_K \mid \alpha \equiv 1 \mod \mathfrak{m}_0 \text{ y } \sigma(\alpha) > 0 \text{ para todo } \sigma \mid \mathfrak{m}_\infty\}$[2].

Ejemplo 2.4. Tenemos que $-4\mathbb{Z} \in P_{\mathbb{Q},1}(3\mathbb{Z}\infty)$ porque $-4\mathbb{Z} = 4\mathbb{Z}$ y además $4 \equiv 1 \mod 3$ con $4 > 0$. También se tiene $-5\mathbb{Z} \in P_{\mathbb{Q},1}(3\mathbb{Z})$ porque $-5 \equiv 1 \mod 3$ y $\infty \nmid 3\mathbb{Z}$.

En adelante, para evitar sobrenotación identificaremos los ideales de $\mathbb{Z}$ con sus generadores, así por ejemplo $P_{\mathbb{Q},1}(3\infty) := P_{\mathbb{Q},1}(3\mathbb{Z}\infty)$.

Observación 2.5. Detengámonos en la condición $\alpha \equiv 1 \mod \mathfrak{m}_0$ y $\sigma(\alpha) > 0$ para todo $\sigma \mid \mathfrak{m}_\infty$. Lo primero equivale a decir que $\alpha \equiv 1 \mod \mathfrak{p}^{n_\mathfrak{p}}$ para todo $\mathfrak{p} \mid \mathfrak{m}_0$, o sea que para cada uno de estos primos, α pertenece a $1 + \mathfrak{p}^{n_\mathfrak{p}}$, vecindad de 1 en $K_\mathfrak{p}^*$, el grupo multiplicativo de la completación de K en $\mathfrak{p}$. Respecto a las condiciones de positividad, tenemos que para $\sigma \mid \mathfrak{m}_\infty$, $\sigma(\alpha)$ está en $\mathbb{R}^*_{>0}$, vecindad de 1 en $\mathbb{R}^*$, el grupo multiplicativo de la completación de K en σ. Luego, podemos pensar en $P_{K,1}(\mathfrak{m})$ como el conjunto de ideales principales de $\mathcal{O}_K$ que admite un generador lo suficientemente cerca de 1 en $K_\mathfrak{p}^*$ para todo primo $\mathfrak{p} \mid \mathfrak{m}$. Notar que $\mathbb{C}^*$ es conexo y por ello, respecto a los primos infinitos, solo nos preocupamos por aquellos reales.

Proposición 2.6. *Sea K un cuerpo de números. Entonces $[I_K(\mathfrak{m}) : P_{K,1}(\mathfrak{m})] < \infty$.*

Antes de comentar la demostración en general, estudiemos algunos ejemplos.

Ejemplo 2.7. Sea m un entero positivo. Entonces $[I_\mathbb{Q}(m\infty) : P_{\mathbb{Q},1}(m\infty)] = \varphi(m)$.

[1] La ramificación de los primos infinitos varía según la fuente.

[2] Esta condición sobre α se puede encontrar en algunas fuentes con la notación $\alpha \equiv 1 \mod {}^*\mathfrak{m}$ o $\alpha \equiv^* 1 \mod \mathfrak{m}$

Demostración: Tenemos que

$$P_{\mathbb{Q},1}(m\infty) = \left\{ \frac{a}{b}\mathbb{Z} \mid \text{m.c.d}(m,a) = \text{m.c.d}(m,b) = 1,\ a \equiv b \mod m, \frac{a}{b} > 0 \right\}.$$

Sea $\Phi\colon I_{\mathbb{Q}}(m\infty) \to (\mathbb{Z}/m\mathbb{Z})^*$ el mapa definido por $\frac{a}{b}\mathbb{Z} \mapsto ab^{-1} \mod m$, cuando $\frac{a}{b} > 0$ y $\text{m.c.d}(m,a) = \text{m.c.d}(m,b) = 1$. Luego Φ es sobreyectiva y $\ker\Phi = P_{K,1}(m\infty)$ por lo que $[I_{\mathbb{Q}}(m\infty) : P_{\mathbb{Q},1}(m\infty)] = \varphi(m)$.

□

Ejemplo 2.8. Sea K un cuerpo cuadrático imaginario. Entonces $[I_K(\mathfrak{m}) : P_{K,1}(\mathfrak{m})] < \infty$ para todo módulo $\mathfrak{m}$ en K.

Demostración: El mapa $(\mathcal{O}_K/\mathfrak{m})^* \to I_K(\mathfrak{m}) \cap P_K/P_{K,1}(\mathfrak{m})$ dado por $(a \mod \mathfrak{m}) \mapsto (a\mathcal{O}_K \mod P_{K,1}(\mathfrak{m}))$ es un morfismo sobreyectivo bien definido gracias a que K no posee primos infinitos reales. En efecto, si $a \equiv b \mod \mathfrak{m}$ con $a\mathcal{O}_K$ y $b\mathcal{O}_K$ no compartiendo primos en común con $\mathfrak{m}$, entonces $a\mathcal{O}_K b^{-1}\mathcal{O}_K = ab^{-1}\mathcal{O}_K \in P_{K,1}(\mathfrak{m})$ ya que $ab^{-1} \equiv 1 \mod \mathfrak{m}$. Como el grupo $(\mathcal{O}_K/\mathfrak{m})^*$ es finito, tenemos que $I_K(\mathfrak{m}) \cap P_K/P_{K,1}(\mathfrak{m})$ es finito. Considerando la sucesión exacta

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

se concluye que $I_K(\mathfrak{m})/P_{K,1}(\mathfrak{m})$ es finito pues I_K/P_K lo es (con cardinal h_K).

□

Ahora indicamos cómo sería el proceder para demostrar el caso general. Para ello, se recurre al hecho de que todo cuerpo de números tiene número de clases finito y el siguiente

Teorema 2.9 (Teorema de Aproximación)**.** *Sean* $|\ \ |_1, \ldots, |\ \ |_n$ *valuaciones dos a dos no equivalentes de un cuerpo* K *y sean* $a_1, \ldots a_n \in K$ *elementos dados. Entonces para todo* $\varepsilon > 0$ *existe* $x \in K$ *tal que*

$$|x - a_i|_i < \varepsilon \quad \textit{para todo } i=1,\ldots,n.$$

Demostración: Ver [Neu99, Chapter II, Theorem 3.4]. □

Como consecuencia del teorema anterior y el Teorema chino de los restos, se puede mostrar que $I_K(\mathfrak{m})/P_K(\mathfrak{m})$ es isomorfo a I_K/P_K (notar la similitud con la charla de Sebastian R.). Así, al tener que $[I_K(\mathfrak{m}) : P_{K,1}(\mathfrak{m})] = [I_K(\mathfrak{m}) : P_K(\mathfrak{m})][P_K(\mathfrak{m}) : P_{K,1}(\mathfrak{m})]$, basta verificar que $[P_K(\mathfrak{m}) : P_{K,1}(\mathfrak{m})]$ es finito. Sean $K_{\mathfrak{m}} := \{\alpha \in K^* \mid \alpha\mathcal{O}_K \in P_K(\mathfrak{m})\}$ y $K_{\mathfrak{m},1} := \{\alpha \in K_{\mathfrak{m}} \mid \alpha\mathcal{O}_K \in P_{K,1}(\mathfrak{m})\}$. Entonces el mapa $\iota\colon K^* \to I_K$ que envía α en $\alpha\mathcal{O}_K$ induce morfismos sobreyectivos $K_{\mathfrak{m}} \twoheadrightarrow P_K(\mathfrak{m})$ y $K_{\mathfrak{m},1} \twoheadrightarrow P_{K,1}(\mathfrak{m})$. Luego podemos reducirnos a probar que $[K_{\mathfrak{m}} : K_{\mathfrak{m},1}] < \infty$ porque $[P_K(\mathfrak{m}) : P_{K,1}(\mathfrak{m})] = [K_{\mathfrak{m}} : K_{\mathfrak{m},1} \ker\iota]$.

Otra consecuencia del Teorema de aproximación es que el morfismo diagonal

$$K_{\mathfrak{m}}/K_{\mathfrak{m},1} \to \prod_{\mathfrak{p}|\mathfrak{m}} K_{\mathfrak{p}^{n_\mathfrak{p}}}/K_{\mathfrak{p}^{n_\mathfrak{p}},1},$$

es un isomorfismo y por tanto nos reducimos a mostrar que $[K_{\mathfrak{p}^{n_\mathfrak{p}}} : K_{\mathfrak{p}^{n_\mathfrak{p}},1}] < \infty$ para todo $\mathfrak{p} \mid \mathfrak{m}$. Cuando $\mathfrak{p}$ es real $n_p = 1$ y $[K_\mathfrak{p} : K_{\mathfrak{p},1}] = [\mathbb{R}^* : \mathbb{R}^*_{>0}] = 2$. Por otra parte, cuando $\mathfrak{p}$ es un primo finito, $K_{\mathfrak{p}^{n_\mathfrak{p}}} = (\mathcal{O}_{K,\mathfrak{p}})^*$ y $K_{\mathfrak{p}^{n_\mathfrak{p}},1} = 1 + \mathfrak{p}^{n_p}\mathcal{O}_{K,\mathfrak{p}}$, luego $K_{\mathfrak{p}^{n_\mathfrak{p}}}/K_{\mathfrak{p}^{n_\mathfrak{p}}} \cong (\mathcal{O}_{K,\mathfrak{p}}/\mathfrak{p}^{n_\mathfrak{p}})^*$ y este último grupo es finito. Para los detalles ver [Jan96, Chapter IV, §1].

Definición 2.10. Sea $\mathfrak{m}$ un módulo del cuerpo de números K y H un subgrupo de $I_K(\mathfrak{m})$. Decimos que H es un subgrupo de congruencias para $\mathfrak{m}$ si $P_{K,1}(\mathfrak{m}) \subseteq H \subseteq I_K(\mathfrak{m})$. El grupo cociente $I_K(\mathfrak{m})/H$ recibe el nombre de grupo de clases generalizado para $\mathfrak{m}$.

Ejemplo 2.11. El grupo de clases $Cl(\mathcal{O}_K)$ es un grupo de clases generalizado para $\mathfrak{m} = 1$. Es el cociente entre $I_K(\mathfrak{m}) = I_K$ y el subgrupo de congruencias $P_{K,1}(\mathfrak{m}) = P_K$.

Ejemplo 2.12. Más generalmente, sea $\mathcal{O}$ un orden dentro de K, un cuerpo cuadrático imaginario, y de conductor f. Entonces $C(\mathcal{O})$ es un grupo de clases generalizado para el módulo $\mathfrak{f} = f\mathcal{O}_K$ pues $C(\mathcal{O}) \cong I_K(\mathfrak{f})/P_{K,\mathbb{Z}}(f)$ y $P_{K,1}(\mathfrak{f}) \subset P_{K,1}(f)$.

Ejemplo 2.13. De acuerdo a la demostración en el ejemplo 2.7, si m es un entero positivo, entonces el grupo $(\mathbb{Z}/m\mathbb{Z})^*$ es un grupo de clases generalizado para $\mathfrak{m} = m\infty$.

La importancia de estos grupos de clases generalizados radica en que ellos constituyen todos los grupos de Galois de las extensiones abelianas del cuerpo de números K. En cierto sentido, toda la información acerca de las extensiones abelianas de K se encuentra codificada en I_K. Para hacer esta afirmación de una manera más precisa, necesitamos recordar el símbolo de Artin.

Sea L/K una extensión abeliana y $\mathfrak{m}$ un módulo en K tal que $\mathfrak{m}_0$ es divisible por todos los primos finitos que ramifican en L. Para un primo finito $\mathfrak{p}$ no dividiendo a $\mathfrak{m}_0$, tenemos que $\mathfrak{p}$ es

no ramificado y denotamos por $\left(\frac{L/K}{\mathfrak{p}}\right)$ al único elemento σ de $\mathrm{Gal}(L/K)$ tal que $\sigma(\alpha) \equiv \alpha^{N(\mathfrak{p})}$ mód $\mathfrak{P}$ para todo $\alpha \in \mathcal{O}_L$ y $\mathfrak{P} \mid \mathfrak{p}$. En otras palabras, el único σ que induce el automorfismo de Frobenius en $\mathcal{O}_L/\mathfrak{P}$ para algún $\mathfrak{P} \mid \mathfrak{p}$.

Utilizando la unicidad en la descomposición como producto de ideales primos en $\mathcal{O}_K$, extendemos el símbolo de Artin a un morfismo $\Phi_{L/K}(\mathfrak{m})\colon I_K(\mathfrak{m}) \to \mathrm{Gal}(L/K)$ llamado el mapa de Artin.

Teorema 2.14 (Teorema de Reciprocidad de Artin)**.** *Sea L/K una extensión abeliana y $\mathfrak{m}$ un modulo en K divisible por todos los primos de K que ramifican en L, finitos e infinitos. Entonces*

1. *$\Phi_{L/K}(\mathfrak{m})$ es sobreyectivo.*
2. *Si los exponentes $n_{\mathfrak{p}}$ de $\mathfrak{m}$ son lo suficientemente grandes, entonces $\ker \Phi_{L/K}(\mathfrak{m})$ es un subgrupo de congruencias para $\mathfrak{m}$.*

Demostración: Ver [Jan96, Chapter V, Theorem 5.8]. □

Corolario 2.15. *Sea L/K una extensión abeliana, entonces $\mathrm{Gal}(L/K)$ es un grupo de clases de ideales generalizados para $\mathfrak{m}$.*

Demostración: Por el Teorema de reciprocidad de Artin, $\mathrm{Gal}(L/K) \cong I_K(\mathfrak{m})/\ker \Phi_{L/K}(\mathfrak{m})$ para algún ideal $\mathfrak{m}$ dividido por todos los primos que ramifican en L/K. □

Lema 2.16. *Sea L/K una extensión abeliana y $L = K(\alpha)$ para algún $\alpha \in \mathcal{O}_L$. Sea $f(x)$ el polinomio minimal de α sobre K, $f(x) \in \mathcal{O}_K[x]$. Si $\mathfrak{p}$ es un primo en $\mathcal{O}_K$ y $f(x)$ es separable módulo $\mathfrak{p}$, entonces $\mathfrak{p}$ no ramifica en L.*

Ejemplo 2.17. Sea m un entero positivo, ζ_m una raíz primitiva m-ésima de la unidad, $L = \mathbb{Q}(\zeta_m)$, $K = \mathbb{Q}$ y $\mathfrak{m} = m\infty$. Entonces existe un isomorfismo natural $\chi\colon \mathrm{Gal}(L/K) \to (\mathbb{Z}/m\mathbb{Z})^*$ dado por $\sigma(\zeta_m) = \zeta_m^{\chi(\sigma)}$. El mapa de Artin $\Phi_{L/K}(\mathfrak{m})$ está bien definido y $\chi \circ \Phi_{L/K}(\mathfrak{m})$ es exactamente el morfismo Φ descrito en el ejemplo 2.7.

Demostración: Si p es un primo racional que no divide a $\mathfrak{m}$, entonces $x^m - 1$ es separable en $\mathbb{Z}/p\mathbb{Z}$. Esto tiene dos consecuencias importantes, la primera es que de acuerdo con el lema 2.16, p es un primo no ramificado en L, por lo que $\Phi_{L/K}(\mathfrak{m})$ está bien definido, y la segunda es que $1, \ldots, \zeta_m^{m-1}$ son elementos distintos módulo $\mathfrak{P}$, para todo primo $\mathfrak{P}$ de L conteniendo a p. Para calcular $\chi \circ \Phi_{L/K}(\mathfrak{m})$, es suficiente ver las imágenes de los primos $p\mathbb{Z}$ con $p \nmid m$. Por definición del símbolo de Artin,

$$\left(\left(\Phi_{L/K}(\mathfrak{m})\right)(p\mathbb{Z})\right)(\zeta_m) \equiv \zeta_m^p \mod \mathfrak{P},$$

para todo $\mathfrak{P} \mid p\mathbb{Z}$. Entonces, dada la observación acerca de las potencias de ζ_m, tenemos que la congruencia anterior es de hecho una igualdad y así $\chi \circ \Phi_{L/K}(\mathfrak{m})(p\mathbb{Z}) = p \mod m$, lo cual concluye la demostración. Observar que

$$\ker \Phi_{L/\mathbb{Q}}(m\infty) = P_{\mathbb{Q},1}(m\infty).$$

□

Teorema 2.18 (Teorema de existencia)**.** *Sea K un cuerpo de números, $\mathfrak{m}$ un módulo en K y H un subgrupo de congruencia para $\mathfrak{m}$. Entonces existe una única extensión abeliana L/K en la cual todos los primos que ramifican son divisores de $\mathfrak{m}$ y tal que $\ker \Phi_{L/K}(\mathfrak{m}) = H$.*

Demostración: Ver [Jan96, Chapter V, Theorem 9.16]. □

Observación 2.19. Como consecuencia del Teorema de Existencia, podemos considerar extensiones abelianas de K con un grupo de Galois dado y ramificación restringida a un conjunto finito de primos dados.

Corolario 2.20. *Sean L/K y M/K extensiones abelianas de cuerpos de números. Entonces $L \subseteq M$ si y solo si*

$$P_{K,1}(\mathfrak{m}) \subseteq \ker \Phi_{M/K}(\mathfrak{m}) \subseteq \ker \Phi_{L/K}(\mathfrak{m}),$$

para algún módulo $\mathfrak{m}$ en K divisible por aquellos primos que ramifican en L o en M.

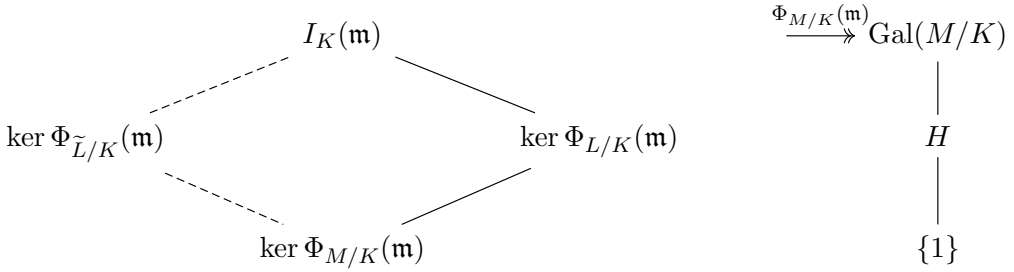
Demostración: Asuma que $L \subseteq M$ y sea $r_{M/L}\colon \mathrm{Gal}(M/K) \to \mathrm{Gal}(L/K)$ la restricción. Por el Teorema de reciprocidad de Artin, existe $\mathfrak{m}$, modulo de K divisible por los primos que ramifican M (en particular por los que ramifican en L) tal que $P_{K,1}(\mathfrak{m}) \subseteq \ker \Phi_{M/K}(\mathfrak{m})$. Por la observación sobre los primos que ramifican en L, se tiene que $\Phi_{L/K}(\mathfrak{m})$ está bien definido y luego, si notamos que $r_{M/L} \circ \Phi_{M/K}(\mathfrak{m}) = \Phi_{L/K}(\mathfrak{m})$, encontramos que

$$P_{K,1}(\mathfrak{m}) \subseteq \ker \Phi_{M/K}(\mathfrak{m}) \subseteq \ker \Phi_{L/K}(\mathfrak{m}).$$

Para la otra dirección asumimos estas contenciones para algún $\mathfrak{m}$ como en el enunciado. Entonces $H := \Phi_{M/K}(\mathfrak{m})\left(\ker \Phi_{L/K}(\mathfrak{m})\right)$ es un subgrupo de $\mathrm{Gal}(M/K)$ y por lo tanto le corresponde una subextensión de M/K, digamos $\widetilde{L}$, tal que $\mathrm{Gal}(M/\widetilde{L}) = H$. Luego

$$P_{K,1}(\mathfrak{m}) \subseteq \ker \Phi_{M/K}(\mathfrak{m}) \subseteq \ker \Phi_{\widetilde{L}/K}(\mathfrak{m}),$$

pero $\Phi_{M/K}(\mathfrak{m})\left(\ker \Phi_{\widetilde{L}/K}(\mathfrak{m})\right) = \mathrm{Gal}(M/\widetilde{L}) = H$ por lo que $\ker \Phi_{\widetilde{L}/K}(\mathfrak{m}) = \ker \Phi_{L/K}(\mathfrak{m})$. Concluimos que $L = \widetilde{L} \subseteq M$ por el Teorema de existencia. □



Lema 2.21. *Sea L/K una extensión abeliana y $\mathfrak{m}$ modulo divisible por todos los primos que ramifican en L/K. Si $P_{K,1}(\mathfrak{m}) \subseteq \ker \Phi_{L/K}(\mathfrak{m})$ y $\mathfrak{m} \mid \mathfrak{n}$ entonces $P_{K,1}(\mathfrak{n}) \subseteq \ker \Phi_{L/K}(\mathfrak{n})$.*

Demostración: Si $\iota : I_K(\mathfrak{n}) \to I_K(\mathfrak{m})$ es la inclusión natural, entonces $\Phi_{L/K}(\mathfrak{n}) = \Phi_{L/K}(\mathfrak{m}) \circ \iota$. Luego

$$P_{K,1}(\mathfrak{n}) \subseteq P_{K,1}(\mathfrak{m}) \cap I_K(\mathfrak{n}) \subseteq \ker(\Phi_{L/K}(\mathfrak{m})) \cap I_K(\mathfrak{n}) = \ker(\Phi_{L/K}(\mathfrak{n})).$$

□

Corolario 2.22 (Teorema de Kronecker-Weber)**.** *Sea $L/\mathbb{Q}$ una extensión abeliana. Entonces existe un entero positivo m tal que $L \subseteq \mathbb{Q}(\zeta_m)$.*

Demostración: Por el Teorema de reciprocidad de Artin existe un módulo $\mathfrak{m}$ en $\mathbb{Q}$ divisible por todos los primos que ramifican en L y tal que $P_{\mathbb{Q},1} \subseteq \ker \Phi_{L/\mathbb{Q}}(\mathfrak{m})$. Por el lema 2.21 podemos asumir que $\mathfrak{m} = m\infty$ para algún entero positivo m. Ahora bien, por el ejemplo 2.17 sabemos que $P_{\mathbb{Q},1}(\mathfrak{m}) = \ker \Phi_{\mathbb{Q}(\zeta_m)/\mathbb{Q}}(\mathfrak{m})$ y por el corolario 2.20 esto implica que $L \subseteq \mathbb{Q}(\zeta_m)$. □

Definición 2.23. Sea K un cuerpo de números y $\mathfrak{m} = 1$. Por el Teorema de existencia para el subgrupo de conguencias $P_{K,1}(\mathfrak{m})$, existe una única extensión abeliana H/K, la cual es no ramificada y cumple

$$I_K/P_K \cong \mathrm{Gal}(H/K).$$

El cuerpo H se denomina el cuerpo de clases de Hilbert de K.

Teorema 2.24 (Teorema del conductor)**.** *Sea L/K una extensión abeliana de cuerpos de números. Entonces existe un módulo $\mathfrak{f} = \mathfrak{f}(L/K)$ en K tal que*

1. *Un primo $\mathfrak{p}$ en K ramifica en L si y solo si $\mathfrak{p} \mid \mathfrak{f}$.*
2. *Si $\mathfrak{m}$ es un módulo divisible por todos los primos ramificados en L/K, entonces $\ker \Phi_{L/K}(\mathfrak{m})$ es un subgrupo de congruencias para $\mathfrak{m}$ si y solamente si $\mathfrak{f} \mid \mathfrak{m}$.*

Demostración: Ver [Jan96, Chapter V, §6 Theorem 12.7]. □

Corolario 2.25. *El cuerpo de clases de Hilbert de K es la máxima extensión abeliana y no ramificada de K.*

Demostración: Por la primera parte del Teorema del conductor, si M/K es una extensión abeliana no ramificada entonces $\mathfrak{f}(M/K) = 1$. Ahora bien, la segunda parte del mismo nos indica que $\ker\left(\Phi_{M/K}(1)\right)$ es un grupo de congruencias para 1. Luego

$$P_{K,1}(1) = \ker\left(\Phi_{H/K}(1)\right) \subseteq \ker\left(\Phi_{M/K}(1)\right),$$

de donde $M \subseteq H$ por el corolario 2.20. □

Definición 2.26. Sea K un cuerpo de números y $\mathfrak{m}$ un módulo en K. Por el Teorema de existencia para el subgrupo de congruencias $P_{K,1}(\mathfrak{m})$, existe una única extensión abeliana $K_\mathfrak{m}/K$ cuyos primos ramificados dividen a $\mathfrak{m}$ y tal que

$$P_{K,1}(\mathfrak{m}) = \ker \Phi_{K_\mathfrak{m}/K}(\mathfrak{m}).$$

El cuerpo $K_\mathfrak{m}$ se llama el cuerpo de clases de rayos del módulo $\mathfrak{m}$.

Ejemplo 2.27. De acuerdo con el ejemplo 2.17, para m un entero positivo se tiene $\mathbb{Q}_{m\infty} = \mathbb{Q}(\zeta_m)$.

Ejemplo 2.28. Sea $m > 2$ un entero. Entonces

$$\mathbb{Q}_m = \mathbb{Q}(\zeta_m + \zeta_m^{-1}),$$

el maximo subcuerpo real de $\mathbb{Q}_{m\infty} = \mathbb{Q}(\zeta_m)$.

Demostración: Podemos asumir que $\zeta_m = e^{\frac{2\pi i}{m}}$. Entonces $\zeta_m + \zeta_m^{-1} = \zeta_m + \overline{\zeta_m} = 2\cos(\frac{2\pi}{m}) \in \mathbb{R}$ por lo que $\mathbb{Q}(\zeta_m + \zeta_m^{-1}) \subseteq \mathbb{Q}(\zeta_m) \cap \mathbb{R}$ y entonces $2 \leq [\mathbb{Q}(\zeta_m) : \mathbb{Q}(\zeta_m + \zeta_m^{-1})]$ $(m > 2)$. Escribamos $\eta := \cos(\frac{2\pi}{m})$, entonces $\mathbb{Q}(\eta) = \mathbb{Q}(\zeta_m + \zeta_m^{-1})$ y la identidad $\cos^2 + \sin^2 = 1$ nos muestra que ζ_m satisface el polinomio

$$(x - \eta)^2 = \eta^2 - 1 \in \mathbb{Q}(\eta)[x],$$

de donde $[\mathbb{Q}(\zeta_m) : \mathbb{Q}(\eta)] = 2$ y $\mathbb{Q}(\eta) = \mathbb{Q}(\zeta_m) \cap \mathbb{R}$. De lo anterior, m es un módulo en $\mathbb{Q}$ divisible por todos los primos que ramifican en $\mathbb{Q}(\eta)$ y luego $\Phi_{\mathbb{Q}(\eta),\mathbb{Q}}(m)$ está bien definido. Como $\chi(\mathrm{Gal}(\mathbb{Q}(\zeta_m))/\mathbb{Q}(\eta)) = \{\pm 1\} \in (\mathbb{Z}/m\mathbb{Z})^*$, existe un isomorfismo $\overline{\chi}$ tal que el diagrama

$$\begin{array}{ccccc} I_\mathbb{Q}(m\infty) & \xrightarrow{\Phi_\mathbb{Q}^{\mathbb{Q}(\zeta_m)}(m\infty)} & \mathrm{Gal}(\mathbb{Q}(\zeta_m)/\mathbb{Q}) & \xrightarrow{\chi} & (\mathbb{Z}/m\mathbb{Z})^* \\ \uparrow & \searrow^{\Phi_\mathbb{Q}^{\mathbb{Q}(\eta)}(m\infty)} & \downarrow{\scriptstyle r_{\mathbb{Q}(\zeta_m)/\mathbb{Q}(\eta)}} & & \downarrow \\ I_\mathbb{Q}(m) & \xrightarrow[\Phi_\mathbb{Q}^{\mathbb{Q}(\eta)}(m)]{} & \mathrm{Gal}(\mathbb{Q}(\eta)/\mathbb{Q}) & \xrightarrow{\overline{\chi}} & (\mathbb{Z}/m\mathbb{Z})^*/\{\pm 1\}, \end{array}$$ [3]

es conmutativo. Con dicho diagrama y el ejemplo 2.17 podemos calcular el mapa

$$I_\mathbb{Q}(m) \xrightarrow{\Phi_\mathbb{Q}^{\mathbb{Q}(\eta)}(m)} \mathrm{Gal}(\mathbb{Q}(\eta)/\mathbb{Q}) \xrightarrow{\overline{\chi}} (\mathbb{Z}/m\mathbb{Z})^*/\{\pm 1\},$$

el cual resulta ser $\frac{a}{b}\mathbb{Z} \mapsto \{\pm ab^{-1} \mod m\}$ cuando $\frac{a}{b} > 0$ y $\mathrm{m.c.d}(m, a) = \mathrm{m.c.d}(m, b) = 1$. Luego $\ker \Phi_{\mathbb{Q}(\eta)/\mathbb{Q}}(m) = P_{K,1}(m)$ y esto termina la demostración. □

Es importante señalar que, tal como lo indica el siguiente ejemplo, no es es cierto en general que el conductor $\mathfrak{f}(K_\mathfrak{m}/K)$ sea $\mathfrak{m}$.

Ejemplo 2.29. Sea m un entero positivo. Entonces

$$\mathfrak{f}(\mathbb{Q}(\zeta_m)/\mathbb{Q}) = \begin{cases} 1 & \text{si } m \leq 2, \\ \frac{m}{2}\infty & \text{si } m = 2n \text{ con } n \text{ impar}, \\ m\infty & \text{en otro caso.} \end{cases}$$

Demostración: Si $m \leq 2$, entonces $\mathbb{Q} = \mathbb{Q}(\zeta_m)$ y $\mathfrak{f}(\mathbb{Q}/\mathbb{Q}) = 1$. Si $m > 2$ entonces $\mathbb{Q}(\zeta_m)$ no es real y por lo tanto $\mathfrak{f} = n\infty$ para algún n en $\mathbb{Z}$. Sabemos que $m\infty$ es divisible por todos los primos ramificados en $\mathbb{Q}(\zeta_m)$ y que $\ker \Phi_{\mathbb{Q}(\zeta_m)/\mathbb{Q}} = P_{\mathbb{Q},1}(m\infty)$ es un subgrupo de congruencias, luego por el Teorema del conductor $\mathfrak{f} \mid m\infty$ y por lo tanto $n \mid m$. De esto último nos interesa resaltar que $\varphi(n) \mid \varphi(m)$.

Por otra parte, ya que $\ker \Phi_{\mathbb{Q}(\zeta_n)/\mathbb{Q}}(n\infty) = P_{\mathbb{Q},1}(n\infty)$ y $\Phi_{\mathbb{Q}(\zeta_n)/\mathbb{Q}}(m\infty) = \Phi_{\mathbb{Q}(\zeta_n)/\mathbb{Q}}(n\infty) \circ \iota$, con $\iota \colon I_\mathbb{Q}(m\infty) \to I_\mathbb{Q}(n\infty)$ la inclusión natural, tenemos que

$$\ker \Phi_{\mathbb{Q}(\zeta_n)/\mathbb{Q}}(m\infty) = P_{\mathbb{Q},1}(n\infty) \cap I_\mathbb{Q}(m\infty) = P_{\mathbb{Q},1}(m\infty) = \ker \Phi_{\mathbb{Q}(\zeta_m)/\mathbb{Q}}(m\infty),$$

de donde $\mathbb{Q}(\zeta_m) \subseteq \mathbb{Q}(\zeta_n)$ por el corolario 2.20 y así $\varphi(n) = \varphi(m)$. Si m no es el doble de un número impar entonces $n = m$ y luego $\mathfrak{f} = m\infty$. Si m sí es de esta forma, entonces $\mathbb{Q}(\zeta_m) = \mathbb{Q}(\zeta_{\frac{m}{2}})$ y por lo tanto $\mathfrak{f} = \mathfrak{f}(\mathbb{Q}(\zeta_{\frac{m}{2}})/\mathbb{Q}) = \frac{m}{2}\infty$ por el caso anterior. □

Proposición 2.30. *Sea L/K una extensión abeliana de cuerpos de números. El conductor $\mathfrak{f} = \mathfrak{f}(L/K)$ es el máximo común divisor entre aquellos módulos $\mathfrak{m}$ en K tal que $L \subseteq K_\mathfrak{m}$.*

[3] Hemos cambiado ligeramente la notación del mapa de Artin

Demostración: Asumamos que $L \subseteq K_{\mathfrak{m}}$, entonces L es no ramificado fuera de $\mathfrak{m}$ y por lo tanto $\Phi_{L/K}(\mathfrak{m})$ y $\Phi_{K_{\mathfrak{m}}/K}(\mathfrak{m})$ están bien definidas. Además $\Phi_{L/K}(\mathfrak{m}) = r_{K_{\mathfrak{m}}/L} \circ \Phi_{K_{\mathfrak{m}}/K}(\mathfrak{m})$ por lo que

$$P_{K,1}(\mathfrak{m}) = \ker \Phi_{K_{\mathfrak{m}}/K}(\mathfrak{m}) \subseteq \ker \Phi_{L/K}(\mathfrak{m}),$$

de donde $\Phi_{L/K}(\mathfrak{m})$ es un subgrupo de congruencias para $\mathfrak{m}$. Por el Teorema del conductor esto equivale a $\mathfrak{f} \mid \mathfrak{m}$. Por el mismo Teorema se tiene que $L \subseteq K_{\mathfrak{f}}$ por lo que todo divisor común de los $\mathfrak{m}$ tal que $L \subseteq K_{\mathfrak{m}}$ debe dividir en particular a $\mathfrak{f}$. □

Corolario 2.31. *Sea L/K una extensión abeliana de cuerpos de números. Si $\mathfrak{f} = \mathfrak{f}(L/K)$, entonces $K_{\mathfrak{f}}$ es el menor cuerpo de clases de rayos que contiene a L.*

Demostración: Directo de juntar la proposición anterior, el segundo punto del Teorema del conductor y el corolario 2.20. □

Corolario 2.32. *Sea $L/\mathbb{Q}$ una extensión abeliana. Si f es el menor entero positivo m tal que $L \subseteq \mathbb{Q}(\zeta_m)$, entonces*

$$\mathfrak{f}(L/\mathbb{Q}) = \begin{cases} f & \text{si } L \text{ es real,} \\ f\infty & \text{si } L \text{ no es real.} \end{cases}$$

Demostración: Escribamos $\mathfrak{f}(L/\mathbb{Q}) = f_0 \mathfrak{f}_\infty$. Entonces $L \subseteq \mathbb{Q}_{\mathfrak{f}} = \mathbb{Q}(\zeta_{f_0})$ por lo que $f \leq f_0$. Ahora recordemos que $\mathbb{Q}(\zeta_f) = \mathbb{Q}_{f\infty}$ por lo tanto $\mathfrak{f} \mid f\infty$, de donde $f_0 = f$. El resultado final se concluye ya que ∞ divide a f_∞ si y solo si ∞ ramifica en L, lo cual se tiene si y solo si L no es real. □

3. CFT y Leyes de Reciprocidad

Sea n un entero positivo, K un cuerpo de números conteniendo a ζ, raíz primitiva n-ésima de la unidad, y $\mathfrak{p}$ un ideal primo de $\mathcal{O}_K$ relativamente primo con $n\mathcal{O}_K$. Como $x^n - 1$ es un polinomio separable módulo $\mathfrak{p}$, tenemos que $1, \zeta, ..., \zeta^{n-1}$ son todos diferentes en $(\mathcal{O}_K/\mathfrak{p})^*$ y por ende n divide a $|\,(\mathcal{O}_K/\mathfrak{p})^*\,| = N(\mathfrak{p}) - 1$.

Sea $\alpha \in \mathcal{O}_K$ primo relativo a $\mathfrak{p}$. Entonces $\alpha^{\frac{N(\mathfrak{p})-1}{n}}$ es una solución a la ecuación $x^n - 1 \equiv 0$ mód $\mathfrak{p}$. Luego existe un única potencia de ζ tal que $\alpha^{\frac{N(\mathfrak{p})-1}{n}} \equiv \zeta^i \mod \mathfrak{p}$. Dicha raíz de una unidad se conoce como el n-ésimo símbolo de Legendre $\left(\frac{\alpha}{\mathfrak{p}}\right)_n$. Este símbolo es una generalización del símbolo de Legendre usual y en este caso también tenemos

Proposición 3.1. *Sea K un cuerpo de números conteniendo una raíz primitiva n-ésima de la unidad y $\mathfrak{p}$ un primo de $\mathcal{O}_K$ que no contiene a n. Entonces*

$$\left(\frac{\alpha}{\mathfrak{p}}\right)_n = 1 \text{ si y solamente si } x^n \equiv \alpha \mod \mathfrak{p} \text{ tiene solución.}$$

Demostración: El hecho clave es que $(\mathcal{O}_K/\mathfrak{p})^*$ es un grupo cíclico generado por algún elemento γ. Si $\alpha \equiv (\gamma^t)^n \mod \mathfrak{p}$ para algún entero positivo t, entonces

$$\left(\frac{\alpha}{\mathfrak{p}}\right)_n \equiv \alpha^{\frac{N(\mathfrak{p})-1}{n}} \equiv \gamma^{(N(p)-1)t} \equiv 1 \mod \mathfrak{p}.$$

Del lado contrario, si $\alpha \equiv \gamma^k \mod \mathfrak{p}$ y $\left(\frac{\alpha}{\mathfrak{p}}\right)_n = 1$, entonces $\gamma^{\frac{(N(\mathfrak{p})-1)k}{n}} \equiv 1 \mod \mathfrak{p}$. Esto implica que $\frac{(N(\mathfrak{p})-1)k}{n} \equiv 0 \mod N(\mathfrak{p}) - 1$, de donde k es un múltiplo de n. □

El símbolo de Legendre puede ser extendido a cualquier ideal $\mathfrak{a}$ de $\mathcal{O}_K$ que sea primo relativo a n. Específicamente hacemos

$$\left(\frac{\alpha}{\mathfrak{a}}\right)_n := \prod_{\mathfrak{p}\mid\mathfrak{a}} \left(\frac{\alpha}{\mathfrak{p}}\right)_n^{n_{\mathfrak{p}}(\mathfrak{a})},$$

donde $\mathfrak{a} = \prod_{\mathfrak{p}} \mathfrak{p}^{n_{\mathfrak{p}}(\mathfrak{a})}$.

Así, si $\mathfrak{m}$ es un módulo en K que es divisible por todos los primos que dividen a $n\mathcal{O}_K$, el símbolo de Legendre induce un morfismo

$$I_K(\mathfrak{m}) \to \mu_n,$$

donde $\mu_n \subset \mathbb{C}^*$ es el grupo de raíces n-ésimas de la unidad.

Recordar que si $L = K(\sqrt[n]{\alpha})$ para algún $\alpha \in K$, entonces existe una inyección natural $\mathrm{Gal}(L/K) \hookrightarrow \mu_n$, dado por $\sigma \mapsto \zeta$ si y solo si $\sigma(\sqrt[n]{\alpha}) = \zeta\sqrt[n]{\alpha}$.

Teorema 3.2 (Reciprocidad Débil)**.** *Sea K un cuerpo de números conteniendo una raíz n-ésima de la unidad, $L = K(\sqrt[n]{\alpha})$ con $\alpha \in \mathcal{O}_K$ un elemento no nulo. Asuma que $\mathfrak{m}$ es un módulo en K divisible por todos los primos que contienen a $n\alpha$ y además asuma que $\ker \Phi_{L/K}(\mathfrak{m})$ es un subgrupo de congruencias para $\mathfrak{m}$. Entonces existe un diagrama conmutativo*

$$\begin{array}{ccc} I_K(\mathfrak{m}) & \xrightarrow{\Phi_{L/K}(\mathfrak{m})} & \mathrm{Gal}(L/K) \\ & \searrow^{\left(\frac{\alpha}{\cdot}\right)_n} & \downarrow \\ & & \mu_n \end{array}$$

donde $\mathrm{Gal}(L/K) \hookrightarrow \mu_n$ es la inyección natural. Así, si G es la imagen de $\mathrm{Gal}(L/K)$ en μ_n, entonces el n-ésimo símbolo de Legendre induce un morfismo sobreyectivo

$$\left(\frac{\alpha}{\cdot}\right)_n : I_K(\mathfrak{m})/P_{K,1}(\mathfrak{m}) \twoheadrightarrow G \subset \mu_n.$$

Demostración: Para probar que el diagrama es commutativo, es sufiente probarlo para ideales primos $\mathfrak{p} \in I_K(\mathfrak{m})$. Es decir, debemos probar que

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

Como en el ejemplo 2.17, es suficiente probar la igualdad anterior módulo algún primo $\mathfrak{P}$ de L arriba de $\mathfrak{p}$. Sea $\mathfrak{P}$ como hemos mencionado, entonces

$$\left(\frac{L/K}{\mathfrak{p}}\right)(\sqrt[n]{\alpha}) \equiv \sqrt[n]{\alpha}^{N(\mathfrak{p})} \equiv \alpha^{\frac{N(\mathfrak{p})-1}{n}} \sqrt[n]{\alpha} \equiv \left(\frac{\alpha}{\mathfrak{p}}\right) \sqrt[n]{\alpha} \mod \mathfrak{P},$$

de donde concluímos la commutatividad del diagrama.

Para la última conclusión del teorema solo debemos notar que como consecuencia de lo anterior y de que $\ker \Phi_{L/K}(\mathfrak{m})$ sea un subgrupo de congruencias para $\mathfrak{m}$ tenemos

$$P_{K,1}(\mathfrak{m}) \subseteq \ker \Phi_{L/K}(\mathfrak{m}) = \ker \left(\frac{\alpha}{\cdot}\right)$$

□

Las leyes de reciprocidad cuadráticas, conjeturadas por Euler y Legendre y siendo posteriormente demostradas por Gauss, pueden ser consideradas como los primeros hallazgos hacia la Teoría de cuerpos de clases. En adelante estudiaremos cuál es la relación entre esta teoría y dichas leyes. Para ello, nos basaremos en [Wym72].

Lema 3.3. *Sean p y q primos distintos. Entonces p se escinde completamente en $\mathbb{Q}(\sqrt{q})$ si y solo si $\left(\frac{q}{p}\right)_2 = 1$.*

Demostración: El primo p es no ramificado en $\mathbb{Q}(\sqrt{q})$ por lo que p se escinde completamente si y solo si el grado de inercia f de p es 1. Pero f es igual al orden de elemento Frobenius $\left(\frac{\mathbb{Q}(\sqrt{q})/\mathbb{Q}}{p}\right) = \Phi_{\mathbb{Q}(\sqrt{q})/\mathbb{Q}}(q\infty)(p)$. Así, el primo p se escinde completamente si y solo si $\Phi_{\mathbb{Q}(\sqrt{q})/\mathbb{Q}}(q\infty)(p)$ es trivial en $\mathrm{Gal}(\mathbb{Q}(\sqrt{q})/\mathbb{Q})$, lo cual de acuerdo a la reciprocidad débil equivale a $\left(\frac{q}{p}\right)_2 = 1 \in \mu_2$. □

Así, para determinar el conjunto de los primos racionales p que se escinden completamente en $\mathbb{Q}(\sqrt{q})$, debemos calcular el valor $\left(\frac{q}{p}\right)_2$, lo cual en un principio requiere infinitas verificaciones. Sin embargo, en nuestro problema q es fijo y p es quien varía por lo que las esperanzas son que de algún modo podamos reducirnos a estudiar el símbolo $\left(\frac{\cdot}{q}\right)_2$ que depende solamente de las finitas clases módulo q.

Teorema 3.4 (Ley de reciprocidad cuadrática)**.** *Sean p y q dos primos racionales distintos e impares. Entonces*

$$\left(\frac{p}{q}\right)_2 \left(\frac{q}{p}\right)_2 = (-1)^{\frac{(p-1)(q-1)}{4}}.$$

Sabiendo que $\left(\frac{-1}{p}\right)_2 = (-1)^{\frac{p-1}{2}}$ y denotando $p^* := (-1)^{\frac{p-1}{2}} p$, es sencillo demostrar que el enunciado del teorema equivale a

$$\left(\frac{p^*}{q}\right)_2 = \left(\frac{q}{p}\right)_2.$$

Lema 3.5. *Sea p un primo racional impar. Sea K un cuerpo cuadrático en el cual el único primo finito que ramifica es p. Entonces $K = \mathbb{Q}(\sqrt{p^*})$.*

Demostración: Escribamos $K = \mathbb{Q}(\sqrt{d_K})$. Un primo ramifica K si y solamente si divide a d_K por lo tanto $d_K \not\equiv 0 \mod 4$. Entonces $d_K \equiv 1 \mod 4$ y es libre de cuadrados. Dado que solamente p ramifica en K obtenemos que $d_K = \pm p$. De esto se concluye que $d_K = p^*$ ya que $p^* = p$ si $p \equiv 1 \mod 4$ y $p^* = -p$ si $p \equiv 3 \mod 4$. □

Demostración: (del teorema) Como $\mathrm{Gal}(\mathbb{Q}(\zeta_p)/\mathbb{Q})$ es cíclico de orden $p-1$, sabemos que existe una única subextensión K de grado 2 sobre $\mathbb{Q}$. De la contención $K \subseteq \mathbb{Q}(\zeta_p)$ y el lema 3.5 obtenemos que $K = \mathbb{Q}(\sqrt{p^*})$. El módulo $\mathfrak{m} = 2p\infty$ en $\mathbb{Q}$ es divisible por los primos que contienen a $2p^*$ y por corolario 2.20 con $L = K$ y $M = \mathbb{Q}(\zeta_p) = \mathbb{Q}(\zeta_{2p})$ tenemos $P_{K,1}(2p\infty) \subseteq \ker \Phi_{K/\mathbb{Q}}(2p\infty)$, luego podemos aplicar el teorema de reciprocidad débil para obtener un morfismo sobreyectivo

$$\left(\frac{p^*}{\cdot}\right)_2 : I_{\mathbb{Q}}(2p\infty)/P_{\mathbb{Q},1}(2p\infty) \to \{\pm 1\} \subset \mu_2.$$

Sin embargo tenemos isomorfismos $I_{\mathbb{Q}}(2p\infty)/P_{\mathbb{Q},1}(2p\infty) \xrightarrow{\sim} (\mathbb{Z}/2p\mathbb{Z})^* \xrightarrow{\sim} (\mathbb{Z}/p\mathbb{Z})^*$ siendo el primero el morfismo $\frac{a}{b}\mathbb{Z} \mapsto ab^{-1} \mod 2p$ cuando $\frac{a}{b} > 0$ y $(2p, a) = (2p, b) = 1$ y el segundo siendo $a \mod 2p \mapsto a \mod p$. Entonces $\left(\frac{p^*}{\cdot}\right)_2$ induce el único morfismo sobreyectivo entre el grupo cíclico $(\mathbb{Z}/p\mathbb{Z})^*$ y $\{\pm 1\}$. Sin embargo el símbolo de Legendre $\left(\frac{\cdot}{p}\right)_2$ también es un morfismo sobreyectivo entre los mismo grupos, de donde

$$\left(\frac{p^*}{q}\right)_2 = \left(\frac{q}{p}\right)_2,$$

para todo primo $q \neq p$ impar. □

Observación 3.6. La ley de reciprocidad cuadrática para primos p y q impares equivale a

1. Si $q \equiv 1 \mod 4$, entonces $\left(\frac{q}{p}\right)_2 = \left(\frac{p}{q}\right)_2$.
2. Si $q \equiv 3 \mod 4$, entonces

$$\left(\frac{q}{p}\right)_2 = \begin{cases} \left(\frac{p}{q}\right)_2 & \text{si } p \equiv 1 \mod 4 \\ -\left(\frac{p}{q}\right)_2 & \text{si } p \equiv 3 \mod 4 \end{cases}.$$

Proposición 3.7. *(Ley de reciprocidad cuadrática para 2) Sea p un número primo distinto a 2, entonces*

$$\left(\frac{2}{p}\right)_2 = (-1)^{\frac{p^2-1}{8}}.$$

Demostración: El objetivo es el mismo que en la demostración anterior. Encontrar un módulo $\mathfrak{m}$ que satiface las hipótesis de la reciprocidad débil y describir el grupo $I_K(\mathfrak{m})/P_{K,1}(\mathfrak{m})$. En este caso la extensión L es $\mathbb{Q}(\sqrt{2})$, exactamente el cuerpo de clases de rayos de $\mathfrak{m} = 8$. Como $4 \in \mathfrak{m}$, aplicamos reciprocidad débil para obtener,

$$\left(\frac{2}{\cdot}\right)_2 : I_{\mathbb{Q}}(8)/P_{\mathbb{Q},1} \xrightarrow{\sim} \{\pm 1\}.$$

Pero por el ejemplo 2.17 sabemos que $I_{\mathbb{Q}}(8)/P_{\mathbb{Q},1} \cong (\mathbb{Z}/8\mathbb{Z})^*/\{\pm 1\}$, de donde $\left(\frac{2}{\cdot}\right)_2$ induce un isomorfismo entre $(\mathbb{Z}/8\mathbb{Z})^*/\{\pm 1\}$ y $\{\pm 1\} \subset \mu_2$. Esto fuerza a que

$$\left(\frac{2}{p}\right)_2 = (-1)^{\frac{p^2-1}{8}}.$$

□

Corolario 3.8. *Sean p y q dos primos racionales distintos e impares. Entonces*

1. *Si $q \equiv 1 \mod 4$, entonces p se escinde completamente en $\mathbb{Q}(\sqrt{q})$ si y solo si p satisface ciertas congruencias módulo q.*
2. *Si $q \equiv 3 \mod 4$, entonces p se escinde completamente en $\mathbb{Q}(\sqrt{q})$ si y solo si p satisface ciertas congruencias módulo $4q$.*

Además, p se escinde completamente en $\mathbb{Q}(\sqrt{2})$ si y solo si p satisface ciertas congruencias módulo 8.

Demostración: Directo de juntar el lema 3.3 y las leyes de reciprocidad cuadrática. □

Ejemplo 3.9. Sea $q = 17$. Como $q \equiv 1 \mod 4$ tenemos que

$$p \text{ se escinde completamente en } \mathbb{Q}(\sqrt{17}) \iff p \equiv 1, 2, 4, 8, 9, 13, 15 \text{ o } 16 \mod 17,$$

pues este es el listado de residuos cuadráticos de 17.

Ejemplo 3.10. Sea $q = 11$. Como $q \equiv 3 \mod 4$ tenemos que

$$p \equiv 1 \mod 4 \text{ se escinde completamente en } \mathbb{Q}(\sqrt{11}) \iff p \equiv 1, 3, 4, 5 \text{ o } 9 \mod 11,$$

pues este es el listado de residuos cuadráticos módulo 11. Por otra parte

$$p \equiv 3 \mod 4 \text{ se escinde completamente en } \mathbb{Q}(\sqrt{11}) \iff p \equiv 2, 6, 7, 8 \text{ o } 10 \mod 11.$$

Utilizando el Teorema chino de los restos, podemos resumir lo anterior en

$$p \text{ se escinde completamente en } \mathbb{Q}(\sqrt{11}) \iff p \equiv 1, 5, 7, 9, 19, 25, 35, 37, 39 \text{ o } 43 \mod 44.$$

En vista de lo anterior, podemos interpretar las leyes de reciprocidad cuadrática como una manera de describir los primos que se escinden completamente en el cuerpo cuadrático $\mathbb{Q}(\sqrt{q})$ en términos de congruencias modulares. En esta misma linea, otra ley de reciprocidad sería el siguiente resultado.

Proposición 3.11 (Ley de reciprocidad ciclotómica)**.** *Sea m un entero positivo. Entonces un primo p se escinde completamente en $\mathbb{Q}(\zeta_m)$ si y solo si $p \equiv 1 \mod m$.*

Demostración: Un primo p se escinde completamente si y solo si su grado de inercia f en $\mathbb{Q}(\zeta_m)/\mathbb{Q}$ es 1. Lo anterior se tiene si y solo si $p \in \ker \Phi_{\mathbb{Q}(\zeta_m)/\mathbb{Q}}(m\infty) = P_{\mathbb{Q},1}(m\infty)$ que a su vez se reinterpreta como $p \equiv 1 \mod m$. □

Para terminar mostramos que con CFT obtenemos la existencia de una ley de reciprocidad para todas las extensiones abelianas de $\mathbb{Q}$.

Proposición 3.12. *Sea $L/\mathbb{Q}$ una extensión abeliana. Entonces existe un entero positivo m tal que, salvo finitas excepciones, un primo p se escinde completamente en L si y solo si p satisface ciertas congruencias módulo m.*

Demostración: Por el Teorema de Kronocker-Weber sabemos que existe un entero positivo m tal que $L \subset \mathbb{Q}(\zeta_m)$. Denotemos nuevamente por χ al isomorfismo del ejemplo 2.17. Análogamente a lo hecho en el ejemplo 2.28, existe un isomorfismo $\overline{\chi}$ haciendo del siguiente diagrama un diagrama commutativo.

$$\begin{array}{ccccc} I_{\mathbb{Q}}(m\infty) & \xrightarrow{\Phi_{\mathbb{Q}}^{\mathbb{Q}(\zeta_m)}(m\infty)} & \mathrm{Gal}(\mathbb{Q}(\zeta_m)/\mathbb{Q}) & \xrightarrow{\chi} & (\mathbb{Z}/m\mathbb{Z})^* \\ & \searrow^{\Phi_{\mathbb{Q}}^{L}(m\infty)} & \downarrow{\scriptstyle r_{\mathbb{Q}(\zeta_m)/L}} & & \downarrow \\ & & \mathrm{Gal}(L/\mathbb{Q}) & \xrightarrow{\overline{\chi}} & (\mathbb{Z}/m\mathbb{Z})^*/H, \end{array}$$

con $H = \chi(\mathrm{Gal}(\mathbb{Q}(\zeta_m)/L))$. De aquí, tomando p no dividiendo a m tenemos que

$$\begin{aligned} p \text{ se escinde completamente en } L &\iff p \in \ker \Phi_{L/\mathbb{Q}}(m\infty) \\ &\iff \Phi_{L/\mathbb{Q}}(m\infty)(p) \text{es trivial en } \mathrm{Gal}(L/\mathbb{Q}) \\ &\iff (\overline{\chi} \circ \Phi_{L/\mathbb{Q}}(m\infty))(p) = H \\ &\iff (\chi \circ \Phi_{\mathbb{Q}(\zeta_m)/\mathbb{Q}}(m\infty))(p) \in H \\ &\iff p \mod m \in H \end{aligned}$$

□

Referencias

[Jan96] Gerald J. Janusz. *Algebraic number fields*, volume 7 of *Graduate Studies in Mathematics*. American Mathematical Society, Providence, RI, second edition, 1996. 2, 2, 2, 2

[Neu99] J. Neukirch. *Algebraic number theory*, volume 322 of *Grundlehren der Mathematischen Wissenschaften [Fundamental Principles of Mathematical Sciences]*. Springer-Verlag, Berlin, 1999. 2

[Wym72] B. F. Wyman. What is a reciprocity law? *Amer. Math. Monthly*, 79:571–586; correction, ibid. 80 (1973), 281, 1972. 3

Email address: paperez5@mat.uc.cl