Teoría de Cuerpos de Clase

Mario Ignacio Lagunas Diaz

1. Introducción

En el presente documento se presentara la teoría de cuerpos de clase para cuerpos de números (globales), la exposición se centrara en la formulación clásica de la teoría basándose siguiendo el libro de Cox [1], pero se mencionarán aspectos de la versión adélica, en particular para hablar sobre la ley de reciprocidad asociada al símbolo de Hilbert que aparece en el libro de Neukirch [2].

El foco será en los principales teoremas: la ley de reciprocidad general de Artin y el teorema de existencia, más que en sus demostraciones. La teoría de cuerpos de clase tiene como objetivo principal clasificar todas las extensiones abelianas de un cuerpo de números K dado, consiguiendo una relación entre subgrupos de un objeto asociado al cuerpo K y sus extensiones abelianas. Otro objetivo, la primera motivación de la teoría, es entender como se factorizan los primos en una extensión (abeliana) de cuerpos de números L/K, en particular que primos $\mathfrak{p}$ escinden completamente en K, esto estaría determinado por una ley de reciprocidad.

De hecho la definición original de lo que es un cuerpo de clases asociado a un subgrupo H del grupo de clases de ideales $\mathcal{C}_K$ de K es una extensión abeliana L de K tal que ningún primo de K ramifica en L y tal que los primos de K que escinden completamente en L son exactamente los que están dentro de H.

La ley de reciprocidad cuadrática, uno de los teoremas más importantes de la teoría de números, se puede entender como el comienzo de la teoría de cuerpos de clase. De hecho, uno de los objetivos que tenían los matemáticos que se dedicaron a desarrollar el área era obtener la versión más general posible de este fenómeno, esta es la ley de reciprocidad de Artin. Luego de enunciar los principales teoremas de la teoría de cuerpos de clase, se explicara la ley de reciprocidad de n-potencias que se puede obtener como una consecuencia de la ley de reciprocidad de Artin.

2. Teoremas Principales de la Teoría

La teoría se trata en cierta parte de encontrar cuerpos análogos a lo que son los cuerpos ciclotómicos en el caso de los números racionales, es decir que cumplan una condición como la del teorema de Kronecker-Weber mencionado en el documento anterior, estos serán los llamados cuerpos de clase de rayos asociado a un módulo, la idea central es que las extensiones abelianas de un cuerpo de números K pueden ser descritos por grupos de clases de ideales generalizados.

Definición: Sea $K/\mathbb{Q}$ un cuerpo de números, un módulo $\mathfrak{m}$ de K es un producto formal:

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

sobre todos los lugares $\mathfrak{p}$ de K,donde:

- $n_\mathfrak{p} \geq 0$, y para todos, salvo finitos $n_\mathfrak{p}$, se tiene $n_\mathfrak{p} = 0$
- $n_\mathfrak{p} = 0$, si $\mathfrak{p}$ es infinito complejo
- $n_\mathfrak{p} \leq 1$, si $\mathfrak{p}$ es infinito real

Así $\mathfrak{m} = \mathfrak{m}_0\mathfrak{m}_\infty$, donde $\mathfrak{m}_0$ es un ideal de $\mathcal{O}_K$ y $\mathfrak{m}_\infty$ es un producto de lugares infinitos de K. Cuando $n_\mathfrak{p} = 0$ para todo $\mathfrak{p}$ lugar de K, se escribe $\mathfrak{m} = 1$.

Dado un módulo $\mathfrak{m}$ de K, consideramos $\mathcal{I}_K(\mathfrak{m})$ el grupo de $\mathcal{O}_K$-ideales fraccionarios relativamente primos a $\mathfrak{m}$, y $\mathcal{P}_K(\mathfrak{m})$ el subgrupo de $\mathcal{I}_K(\mathfrak{m})$ generado por los ideales principales $\alpha\mathcal{O}_K$, donde $\alpha \in \mathcal{O}_K$ satisface:

$$\alpha \equiv 1 \pmod{\mathfrak{m}_0}$$

y $\sigma(\alpha) > 0$ para todo primo infinito real σ diviendo a $\mathfrak{m}_\infty$

Definición: Un subgrupo $H \subseteq \mathcal{I}_K(\mathfrak{m})$ se llama un subgrupo de congruencia para $\mathfrak{m}$ si satisface:

$$\mathcal{P}_K(\mathfrak{m}) \subseteq H \subseteq \mathcal{I}_K(\mathfrak{m})$$

En este caso el cuociente $\mathcal{I}_K(\mathfrak{m})/H$ se llama un grupo de clases de ideales generalizado, esto debido a que si tomamos $\mathfrak{m} = 1$ y $H = \mathcal{P}_K(1) = \mathcal{P}_K$ (el subgrupo de ideales fraccionarios principales) obtenemos $\mathcal{I}_K(1)/\mathcal{P}_K(1) = \mathcal{I}_K/\mathcal{P}_K = \mathcal{C}_K$, el grupo de clases de ideales de K (esto ya que la condición sobre los ideales se vuelve vacía).

Sea L/K una extensión abeliana de K, Sea $\mathfrak{m}$ un módulo de K divisible por todos los primos de K ramificados en L. Dado un primo $\mathfrak{p}$ que no divida a $\mathfrak{m}$, tenemos el morfismo de Artin:

$$\Phi_\mathfrak{m} \colon \mathcal{I}_K(\mathfrak{m}) \to \mathrm{Gal}(L/K) \tag{1}$$

restringido a los $\mathcal{O}_K$-ideales fraccionarios relativamente primos a $\mathfrak{m}$. Se recuerda que este morfismo se obtiene asignando a cada primo $\mathfrak{p}$ de K, que no se ramifique en L, el automorfismo de Frobenius $\left(\dfrac{L/K}{\mathfrak{p}}\right)$, y extendiendolo a $\mathcal{I}_K(\mathfrak{m})$. Esto se puede ya que el primo $\mathfrak{p}$ al no dividir a $\mathfrak{m}$ no se ramifica en L.

Con estos conceptos se puede enunciar el Teorema de Reciprocidad de Artin.

Teorema: (Ley de Reciprocidad de Artin) Sea L/K una extensión abeliana, y sea $\mathfrak{m}$ un módulo divisible por todos los primos de K (finitos o infinitos) que se ramifican en L, luego:

- El mapa de Artin $\Phi_\mathfrak{m}$ es sobreyectivo
- Si los exponentes de los primos finitos diviendo a m son suficientemente grandes, luego $\ker(\Phi_\mathfrak{m})$ es un subgrupo de congruencia para m, esto es:

  $$\mathcal{P}_K(\mathfrak{m}) \subseteq \ker(\Phi_\mathfrak{m}) \subseteq \mathcal{I}_K(\mathfrak{m})$$

  $$\mathcal{I}_K(\mathfrak{m})/\ker(\Phi_\mathfrak{m}) \simeq \mathrm{Gal}(L/K)$$

  En otras palabras, esto muestra que $\mathrm{Gal}(L/K)$ es un grupo de clases de ideales generalizado para el módulo $\mathfrak{m}$.

Sea m un número natural, $L = \mathbb{Q}(\zeta_m)$, $K = \mathbb{Q}$, y $\mathfrak{m} = m\infty$, usando la identificación $\mathrm{Gal}(\mathbb{Q}(\zeta_m)/\mathbb{Q}) \simeq (\mathbb{Z}/m\mathbb{Z})^*$, tenemos que:

$$\Phi_{\mathfrak{m}} \colon \mathcal{I}_{\mathbb{Q}}(\mathfrak{m}) \to (\mathbb{Z}/m\mathbb{Z})^*$$

puede ser descrito de la siguiente manera: dado $\frac{a}{b}\mathbb{Z} \in \mathcal{I}_{\mathbb{Q}}(\mathfrak{m})$, podemos asumir $\frac{a}{b} > 0$ y $\gcd(a, m) = \gcd(b, m) = 1$, luego:

$$\Phi_{\mathfrak{m}}(\frac{a}{b}\mathbb{Z}) = [a]\,[b]^{-1} \in (\mathbb{Z}/m\mathbb{Z})^*$$

De esto sigue facílmente que:

$$\ker(\Phi_{\mathfrak{m}}) = \mathcal{P}_{\mathbb{Q}}(\mathfrak{m})$$

Falta precisar que significa la condición de expontentes suficientemente grandes en el teorema de reciprocidad. Notar que si $\mathfrak{m}$ es un módulo de K tal que $\mathcal{P}_{\mathbb{K}}(\mathfrak{m}) \subseteq \ker(\Phi_{\mathfrak{m}})$ y $\mathfrak{n}$ es cualquier módulo de K que divida a $\mathfrak{m}$, entonces $\mathcal{P}_{\mathbb{K}}(\mathfrak{n}) \subseteq \ker(\Phi_{\mathfrak{n}})$. Así $\mathrm{Gal}(L/K)$ es un grupo de clases de ideales generalizado para infinitos módulos.

Por esta razón nos interesa saber cual si existe un módulo $\mathfrak{m}$ mejor que los demás, este será el conductor asociado a una extensión abeliana L/K de cuerpos de números.

Teorema: (del Conductor) Sea L/K una extensión abeliana. Luego existe un módulo $\mathfrak{f} = \mathfrak{f}(L/K)$ tal que:

- Un primo de K (finitos o infinito) se ramifica en L si y solo si divide a $\mathfrak{f}$.
- Sea $\mathfrak{m}$ un módulo divisible por todos los primos que ramifican en L. Luego $\ker(\Phi_{\mathfrak{m}})$ es un subgrupo de congruencia para $\mathfrak{m}$ si $\mathfrak{f} \mid \mathfrak{m}$.

Así esto nos permite precisar la condición de expontentes suficientemente grandes que aparece en la ley de reciprocidad, un tal módulo $\mathfrak{m}$ será suficientemente grande si es dividido por el conductor de la extensión. El conductor $\mathfrak{f}$ de una extensión L/K se puede definir en términos de sus completaciones.

Definición (Conductor Local): Sea L/K extensión abeliana finita de un cuerpo local K (extensión finita de $\mathbb{Q}_p$), $\mathfrak{p}_K$ el ideal primo de su anillo de enteros $\mathcal{O}_K$, y sea n el mínimo número ≥ 0 tal que $U_K^{(n)} \subseteq N_{L/K}L^*$, luego el ideal $\mathfrak{f} = \mathfrak{p}_K^n$ se llama el conductor (local) de L/K. Aquí $U_K^{(n)} = 1 + \mathfrak{p}_K^n$ para $n > 0$ y $U_K^{(0)} = U_K$, el grupo de unidades de $\mathcal{O}_K$.

Proposición: una extensión abeliana (local) L/K es no ramificada si y sólo si su conductor (local) $\mathfrak{f} = 1$.

Demostración: Si L/K es no ramificada, luego $U_K = N_{L/K}U_L$ (en otras palabras $\mathrm{H}^0(\mathrm{Gal}(L/K), U_L) = 1$), luego $U_K \subseteq N_{L/K}L^*$, por lo que $\mathfrak{f} = 1$.

Si $\mathfrak{f} = 1$, luego $U_K \subseteq N_{L/K}L^*$ y $\pi_K^n \in N_{L/K}L^*$ con $n = [L : K]$, donde π_K es un elemento primo de $\mathcal{O}_K$, $(\pi_K) = \mathfrak{p}_K$. Si M/K es la extensión no ramificado de grado n, luego $N_{M/K}M^* = U_K \times (\pi_K^n) \subseteq N_{L/K}L^*$, por lo que $L \subseteq M$, por lo que L/K es no ramificada.

Dicho esto, el conductor $\mathfrak{f}(L/K)$ de una extensión abeliana de cuerpos de números L/K cumple:

$$\mathfrak{f}(L/K) = \prod_{\mathfrak{p}} \mathfrak{f}_{\mathfrak{p}}$$

sobre todos los lugares $\mathfrak{p}$ de K. Para los lugares finitos $\mathfrak{f}_{\mathfrak{p}}$ es el conductor local de $L_{\mathfrak{B}}/K_{\mathfrak{p}}$, donde $\mathfrak{B}$ es un ideal primo de L sobre $\mathfrak{p}$. Para los lugares infinitos $\mathfrak{f}_{\mathfrak{p}} = \mathfrak{p}$ si $L_{\mathfrak{B}} \neq K_{\mathfrak{p}}$, y $\mathfrak{f}_{\mathfrak{p}} = 1$ si $L_{\mathfrak{B}} = K_{\mathfrak{p}}$. El hecho de que la extensión L/K sea galoisiana nos asegura que la definición no depende del primo $\mathfrak{B}$ sobre $\mathfrak{p}$ escogido, por la transitividad de la acción del grupo de Galois, las distintas completaciones son isomorfas.

El teorema de existencia consigue el objetivo de relacionar extensiones abelianas con subgrupos de congruencia, y asegura la existencia de un cuerpo de clase para todo subgrupo de congruencia.

Teorema: (De la existencia) Sea $\mathfrak{m}$ un módulo de K, y sea H un subgrupo de congruencia para $\mathfrak{m}$:

$$\mathcal{P}_K(\mathfrak{m}) \subseteq H \subseteq \mathcal{I}_K(\mathfrak{m})$$

Luego existe una única extensión abeliana L de K, tal que todos los primos de K ramificados en L, dividen a $\mathfrak{m}$, y tal que si:

$$\Phi_{\mathfrak{m}} \colon \mathcal{I}_K(\mathfrak{m}) \to \mathrm{Gal}(L/K)$$

es el morfismo de Artin de L/K sobre $\mathfrak{m}$, se tiene $H = \ker(\Phi_{\mathfrak{m}})$.

Corolario: Sea L y M una extensión abeliana de K. Luego $L \subseteq M$ si y solo si existe un módulo $\mathfrak{m}$, divisible por todos los primos de K ramificados en L o M, tal que:

$$\mathcal{P}_K(\mathfrak{m}) \subseteq \ker(\Phi_{M/K,\mathfrak{m}}) \subseteq \ker(\Phi_{L/K,\mathfrak{m}})$$

Demostración: Si $L \subseteq M$ y $r_{M/L} \colon \mathrm{Gal}(M/K) \to \mathrm{Gal}(L/K)$ el morfismo de restricción. Existe un módulo $\mathfrak{m}$ tal que $\ker(\Phi_{L/K,\mathfrak{m}})$ y $\ker(\Phi_{M/K,\mathfrak{m}})$ son ambas subgrupos de congruencia para $\mathfrak{m}$ (basta tomar el mínimo común múltiplo entre los conductores de ambas extensiones). Además $r_{M/L} \circ \Phi_{M/K,\mathfrak{m}} = \Phi_{L/K,\mathfrak{m}}$, por lo que se tiene:

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

Por otro lado, supongamos que:

$$\mathcal{P}_K(\mathfrak{m}) \subseteq \ker(\Phi_{M/K,\mathfrak{m}}) \subseteq \ker(\Phi_{L/K,\mathfrak{m}})$$

El subgrupo $\ker(\Phi_{L/K,\mathfrak{m}}) \subseteq \mathcal{I}_K(\mathfrak{m})$ tiene imagen H en $\mathrm{Gal}(M/K)$ bajo $\Phi_{M/K,\mathfrak{m}}$, luego podemos tomar el cuerpo fijo $K \subseteq E_L \subseteq M$ asociado al subgrupo H de $\mathrm{Gal}(M/K)$, pero $E_L \subseteq M$, por lo que:

$$r_{M/E_L} \circ \Phi_{M/K,\mathfrak{m}} = \Phi_{E_L/K,\mathfrak{m}}$$

Así, $\ker(\Phi_{E_L/K,\mathfrak{m}}) = \ker(\Phi_{L/K,\mathfrak{m}})$, solo hay que evaluar y usar esta identidad y la relacionada con $r_{M/L}$. Luego por la unicidad dada por el teorema de existencia, se tiene que $L = E_L \subseteq M$.

A continuación, utilizaremos los teoremas presentados para probar el Teorema de Kronecker-Weber sin utilizar Kronecker-Weber Local.

Teorema: (Kronecker-Weber) Sea L una extensión abeliana de $\mathbb{Q}$, luego $L \subseteq \mathbb{Q}(\zeta_m)$, para algún m número natural, donde ζ_m es una m-ésima raíz de la unidad.

Demostración: Por el teorema de Artin, existe un módulo $\mathfrak{m}$ tal que:

$$\mathcal{P}_{\mathbb{Q}}(\mathfrak{m}) \subseteq \ker(\Phi_{L/\mathbb{Q},\mathfrak{m}})$$

donde se puede tomar $\mathfrak{m} = m\infty$, donde m es un número natural, esto ya que todo módulo en $\mathbb{Q}$ divide a un módulo de esta forma. Por lo que:

$$\mathcal{P}_{\mathbb{Q}}(\mathfrak{m}) = \ker(\Phi_{\mathbb{Q}(\zeta_m)/\mathbb{Q},\mathfrak{m}}) \subseteq \ker(\Phi_{L/K,\mathfrak{m}})$$

Así por el corolario recién probado, se tiene que $L \subseteq \mathbb{Q}(\zeta_m)$.

Por otro lado, si aplicamos el teorema de existencia con $\mathfrak{m} = 1$ con $H = \mathcal{P}_K(1) = \mathcal{P}_K$, obtenemos la única extensión abeliana K_1/K no ramificada con $\mathrm{Gal}(K_1/K) \simeq \mathcal{C}l_K$, el grupo de clases de ideales de K, K_1 es el cuerpo de clase de Hilbert de K.

Proposición: K_1 es la máxima extensión abeliana no ramificada de K.

Demostración: Sea M/K una extensión abeliana no ramificada de K, luego $\mathfrak{f}(M/K) = 1$, así por el teorema de reciprocidad de Artin, $\ker(\Phi_{M/K,1})$ es un subgrupo de congruencia para el módulo $\mathfrak{m} = 1$:

$$\ker(\Phi_{K_1/K,1}) = \mathcal{P}_{\mathbb{Q}}(\mathfrak{m}) \subseteq \ker(\Phi_{M/K,1})$$

A partir del corolario se concluye que $M \subseteq K_1$, toda extensión abeliana no ramificada M de K está dentro de K_1, esto es K_1 es la extensión abeliana no ramificada maximal, el cuerpo de clase de Hilbert.

Sea $\mathfrak{m}$ un módulo de un cuerpo de números K, luego existe una única extensión abeliana $K_{\mathfrak{m}}$ de K tal que $\mathcal{P}_K(\mathfrak{m}) = \ker(\Phi_{K_{\mathfrak{m}}/K,\mathfrak{m}})$, K_m se llama el cuerpo de clases de rayos para el módulo $\mathfrak{m}$. Esta noción generaliza los cuerpos ciclotómicos y el cuerpo de clase de Hilbert en un solo concepto, y nos da un concepto de extensión maximal de K.

Teorema: (Ley de Descomposición) Sea L/K una extensión abeliana de grado n y sea $\mathfrak{p}$ primo de K no ramificado en L, sea $\mathfrak{m}$ un módulo de K tal que $\mathfrak{f}(L/K) \mid \mathfrak{m}$ con $\mathfrak{p} \nmid \mathfrak{m}$, y sea $H^{\mathfrak{m}} = \ker(\Phi_{\mathfrak{m}})$ el grupo de congruencia asociado, luego el grado de inercia $f_{\mathfrak{p}}$ es igual al orden de $\mathfrak{p}$ en $\mathcal{I}_K(\mathfrak{m})/H^{\mathfrak{m}}$.

Demostración: El grado de inercia $f_{\mathfrak{p}}$ es igual al orden del automorfismo de Frobenius $\Phi_{L/K,\mathfrak{m}}(\mathfrak{p})$ asociado al primo $\mathfrak{p}$, luego por el isomorfismo inducido por el morfismo de Artin, se tiene que $f_{\mathfrak{p}}$ es exactamente el orden de $\mathfrak{p}$ en $\mathcal{I}_K(\mathfrak{m})/H^{\mathfrak{m}}$.

De esto se obtiene, en particular, que los primos que escinden completamente son exactamente los primos dentro de $H^{\mathfrak{m}}$ esta propiedad de los subgrupos de congruencia fue una de las primeras nociones que tuvo Hilbert para formular la teoría de cuerpos de clase. Hilbert también conjeturó el siguiente resultado:

Teorema: (Del ideal principal) Sea K un cuerpo de números, en el cuerpo de clases de Hilbert K_1 todo ideal α de $\mathcal{O}_K$ se vuelve principal en $\mathcal{O}_{K_1}$, esto es:

$$\alpha\mathcal{O}_{K_1} = a\mathcal{O}_{K_1}$$

Para algún $a \in \mathcal{O}_{K_1}$.

Uno de los detalles interesantes de este teorema es que se demostró gracias a que Emil Artin lo redujo a un problema puramente de teoría de grupos:

Teorema: Sea G un grupo finitamente generado, si $(G : G') < \infty$, se tiene que:

$$Ver_{G/G'} \colon G/G' \to G'/G'' = 0$$

es el homomorfismo trivial, donde G' denota el conmutador del grupo G, y si G es un grupo y H con $(G : H) = n$ finito, entonces $Ver_{G/H}$ se define de la siguiente manera:

Tomamos un conjunto de representantes $x_1, ..., x_n$ de clases laterales izquierdas de H en G, así $G = \cup x_i H$. Sea $y \in G$, luego para todo $1 \leq i \leq n$, $yx_i = x_j h_i$ con $h_i \in H$. Luego se define:

$$Ver(y \pmod{G'}) = \prod_{i=1}^{n} h_i \pmod{H'}.$$

La demostración de este resultado y su relación con el teorema del ideal principal se encuentra en el Capítulo 6, Sección 7, Página 410 de [2].

3. Leyes de Reciprocidad

En esta sección se presentara la ley de reciprocidad general de n-potencias, con este fin definiremos primero el símbolo de Hilbert:

Sea K un cuerpo local (extensión finita de $\mathbb{Q}_p$, con ideal primo $\mathfrak{p}$, y $q = p^r$ el orden de su cuerpo residual) que contiene el grupo μ_n de n-ésimas raíces de la unidad. Así se puede usar la teoría de Kummer sobre K y la teoría local de cuerpos de clase. Sea $L = K(\sqrt[n]{K^*})$ la extensión abeliana maximal de exponente n.

$$N_{L/K} L^* = K^{*n}$$

donde K^{*n} es el subgrupo de n-potencias de K, claramente $K^{*n} \subseteq N_{L/K} L^*$, y:

$$| \, K^*/N_{L/K} L^* \, | = | \, \mathrm{Gal}(L/K) \, | = | \, K^*/K^{*n} \, |$$

Por teoría local de cuerpos de clase, tenemos un isomorfismo:

$$\mathrm{Gal}(L/K) \simeq K^*/K^{*n}$$

Por el otro lado, por teoría de Kummer tenemos un isomorfismo:

$$\mathrm{Hom}(\mathrm{Gal}(L/K), \mu_n) \simeq K^*/K^{*n}$$

donde los homomorfismos son de grupos abelianos.

Así la función evaluar:

$$\mathrm{Gal}(L/K) \times \mathrm{Hom}(\mathrm{Gal}(L/K), \mu_n) \to \mu_n, \quad (\sigma, \chi) \to \chi(\sigma)$$

Aplicando los isomorfismos en cada coordenada, se obtiene un mapa bilineal no-degenerado (en el sentido multiplicativo) llamado el símbolo de Hilbert:

$$\left(\frac{\cdot}{\mathfrak{p}}\right) \colon K^*/K^{*n} \times K^*/K^{*n} \to \mu_n$$

Por razones que serán evidentes luego (completaciones en lugares infinitos) nos interesa lo que sucede cuando $K = \mathbb{R}$, siguiendo el mismo procedimiento, tenemos dos posibilidades, $n = 1$, donde:

$$\left(\frac{a,b}{\mathfrak{p}}\right) = 1 \quad \text{Para todo } a, b \in \mathbb{R}$$

y $n = 2$, donde:

$$\left(\frac{a,b}{\mathfrak{p}}\right) = (-1)^{\frac{sgn(a)-1}{2}\frac{sgn(b)-1}{2}} \quad \text{Para todo } a, b \in \mathbb{R}$$

Aquí el primo $\mathfrak{p}$ es simbolico. Esto se calcula de igual manera usando el símbolo del residuo de la norma de la teoría local de cuerpos de clase para $K = \mathbb{R}$

A continuación se enuncian propiedades del símbolo de Hilbert.

Proposición:

- $\left(\frac{aa',b}{\mathfrak{p}}\right) = \left(\frac{a,b}{\mathfrak{p}}\right)\left(\frac{a',b}{\mathfrak{p}}\right)$
- $\left(\frac{a,bb'}{\mathfrak{p}}\right) = \left(\frac{a,b}{\mathfrak{p}}\right)\left(\frac{a,b'}{\mathfrak{p}}\right)$
- $\left(\frac{a,bb'}{\mathfrak{p}}\right) = 1 \iff a$ es una norma de la extensión $K(\sqrt[n]{b})/K$
- $\left(\frac{a,b}{\mathfrak{p}}\right) = \left(\frac{b,a}{\mathfrak{p}}\right)^{-1}$

Demostración: Ver demostración en el Capitulo 5, Sección 3, Página 334 de [2].

Sabemos que $U_K = \mu_{q-1} \times U_K^{(1)}$, por lo que toda unidad $u \in U_K$ tiene una descomposición única:

$$u = \omega(u)\,\langle u \rangle$$

con $\omega(u) \in \mu_{q-1}$ y $\langle u \rangle \in U_K^{(1)}$, y $u \equiv \omega(u) (\text{mod } \mathfrak{p})$.

Teorema: Si $(n, p) = 1$ y $a, b \in K^*$, luego:

$$\left(\frac{a,b}{\mathfrak{p}}\right) = \omega((-1)^{\alpha\beta}\frac{b^\alpha}{a^\beta})^{\frac{q-1}{n}}$$

donde $\alpha = v_K(a), \beta = v_K(b)$

Demostración: Ver demostración en el Capitulo 5, Sección 3, Página 335 de [2].

A partir de esto, se concluye que si $(n, p) = 1$ y $u, v \in U_K$, entonces:

$$\left(\frac{u,v}{\mathfrak{p}}\right) = 1$$

,y que si π es un elemento primo de K, entonces:

$$\left(\frac{\pi,u}{\mathfrak{p}}\right) = \omega(u)^{\frac{q-1}{n}}$$

y por tanto, no depende del elemento primo π escogido.

Así podemos definir:

$$\left(\frac{u}{\mathfrak{p}}\right) = \left(\frac{\pi, u}{\mathfrak{p}}\right)$$

Este es el n-ésimo símbolo de Legendre.

Proposición: Sea $(n, p) = 1$ y $u \in U_K$. Luego:

$$\left(\frac{u}{\mathfrak{p}}\right) = 1 \iff u \text{ es una } n\text{-ésima potencia mod } \mathfrak{p}$$

Demostración: Sea $\zeta \in U_K$ una $q-1$-ésima raíz de la unidad y sea $m = \frac{q-1}{n}$. Luego ζ^n es una m-ésima raíz de la unidad y:

$$\left(\frac{u}{\mathfrak{p}}\right) = \omega(u)^m = 1 \iff \omega(u) \in \mu_m \iff \omega(u) = (\zeta^n)^i \iff u \equiv \omega(u) \equiv (\zeta^i)^n (\text{mod } \mathfrak{p})$$

Desde ahora K será un cuerpo (global) de números que contenga al grupo de n-ésimas raíces de la unidad μ_n, para algún n natural. Usaremos el símbolo de Hilbert para la completación $K_\mathfrak{p}$, donde $\mathfrak{p}$ es un lugar de K.

$$\left(\frac{,}{\mathfrak{p}}\right) : K_\mathfrak{p} \times K_\mathfrak{p} \to \mu_n$$

Hilbert obtuvo una interesante relación entre los símbolos sobre cada completación:

Teorema: (Fórmula del Producto de Hilbert) Si $a, b \in K^*$, luego:

$$\prod_\mathfrak{p} \left(\frac{a, b}{\mathfrak{p}}\right) = 1$$

donde el producto es sobre todos los lugares $\mathfrak{p}$ de K.

Demostración: El resultado es una conclusión trivial de la reciprocidad general de Artin obtenida sobre los ideles, los detalles se pueden encontrar en el Capítulo 6 de [2].

Definición: Sea $\mathfrak{b} = \prod_\mathfrak{p} \mathfrak{p}^{v_\mathfrak{p}}$ un ideal de K coprimo a n y sea $a \in K$ coprimo a β, se define el símbolo del residuo de la n-potencia:

$$\left(\frac{a}{\mathfrak{b}}\right)_n = \prod_{\mathfrak{p} \nmid n} \left(\frac{a}{\mathfrak{p}}\right)_n^{v_\mathfrak{p}}$$

donde el producto es sobre todos los lugares de K que no dividen a n.

Si $\mathfrak{b} = (b)$ es un ideal principal, se escribe $\left(\frac{a}{\mathfrak{b}}\right)_n = \left(\frac{a}{b}\right)_n$.

Teorema: (Ley de Reciprocidad General de n-potencias) Si $a, b \in K^*$ son coprimos entre si y a n (con respecto a su factorización en ideales primos), luego:

$$\left(\frac{a}{b}\right)_n \left(\frac{b}{a}\right)_n^{-1} = \prod_{\mathfrak{p} \mid n\infty} \left(\frac{a, b}{\mathfrak{p}}\right)$$

donde el producto es sobre todos los lugares infinitos de K y los lugares de K que dividen a n.

Demostración: Si $\mathfrak{p} \nmid bn\infty$, sea $a = u\pi^{v_\mathfrak{p}(a)}$, donde π es un elemento primo de $K_\mathfrak{p}$ y $u \in U_\mathfrak{p}$, el grupo de unidades de $\mathcal{O}_{K_\mathfrak{p}}$.

$$\left(\frac{b}{\mathfrak{p}}\right)_n^{v_\mathfrak{p}(a)} = \left(\frac{\pi, b}{\mathfrak{p}}\right)^{v_\mathfrak{p}(a)} = \left(\frac{\pi, b}{\mathfrak{p}}\right)^{v_\mathfrak{p}(a)} \left(\frac{u, b}{\mathfrak{p}}\right) = \left(\frac{a, b}{\mathfrak{p}}\right)$$

Esto ya que $\left(\frac{u, b}{\mathfrak{p}}\right) = 1$ cuando $u, b \in U_\mathfrak{p}$. Por esta misma razón si $\mathfrak{p} \nmid abn\infty$, luego $a \in U_\mathfrak{p}$ y por lo tanto:

$$\left(\frac{a, b}{\mathfrak{p}}\right) = 1 \quad \text{Para } \mathfrak{p} \nmid abn\infty$$

Usando lo recién mencionado y la fórmula del producto de Hilbert, obtenemos:

$$\begin{aligned}
\left(\frac{a}{b}\right)_n \left(\frac{b}{a}\right)_n^{-1} &= \prod_{\mathfrak{p}|(b)} \left(\frac{a}{\mathfrak{p}}\right)^{v_\mathfrak{p}(b)} \prod_{\mathfrak{p}|(a)} \left(\frac{b}{\mathfrak{p}}\right)^{-v_\mathfrak{p}(a)} \\
&= \prod_{\mathfrak{p}|(b)} \left(\frac{b, a}{\mathfrak{p}}\right) \prod_{\mathfrak{p}|(a)} \left(\frac{a, b}{\mathfrak{p}}\right)^{-1} \\
&= \prod_{\mathfrak{p}|(ab)} \left(\frac{b, a}{\mathfrak{p}}\right) = \prod_{\mathfrak{p} \nmid n\infty} \left(\frac{b, a}{\mathfrak{p}}\right) = \prod_{\mathfrak{p}|n\infty} \left(\frac{b, a}{\mathfrak{p}}\right)
\end{aligned}$$

Visto de esta manera, la reciprocidad para un exponente n general es una consecuencia sencilla de la Reciprocidad General de Artin. Así lo único que falta es calcular explícitamente los símbolos de Hilbert $\left(\frac{a, b}{\mathfrak{p}}\right)$ para $\mathfrak{p} \mid n\infty$.

En el Capítulo 5 Sección 3 de [2] se calcula el caso $K = \mathbb{Q}$ y $n = 2$, donde se obtiene que si a,b son enteros impares relativamente primos, entonces:

$$\left(\frac{a, b}{2}\right) = (-1)^{\frac{a-1}{2}\frac{b-1}{2}}, \quad \left(\frac{2, a}{2}\right) = (-1)^{\frac{a^2-1}{8}}$$

De esto se obtiene una versión un poco más general de la clásica reciprocidad cuadrática.

Teorema: (Ley de Reciprocidad Cuadrática) Sean a, b enteros impares coprimos, entonces:

$$\left(\frac{a}{b}\right)\left(\frac{b}{a}\right) = (-1)^{\frac{a-1}{2}\frac{b-1}{2}} (-1)^{\frac{sgn(a)-1}{2}\frac{sgn(b)-1}{2}}$$

para b impar positivo, se tiene además que:

$$\left(\frac{-1}{b}\right) = (-1)^{\frac{b-1}{2}}, \quad \left(\frac{2}{b}\right) = (-1)^{\frac{b^2-1}{8}}$$

Demostración: Para probar la última afirmación usamos la fórmula del producto:

$$\left(\frac{2}{b}\right) = \prod_{\mathfrak{p} \neq 2,\infty} \left(\frac{p, 2}{p}\right)^{v_\mathfrak{p}(b)} = \prod_{\mathfrak{p} \neq 2,\infty} \left(\frac{b, 2}{p}\right) = \left(\frac{2, b}{2}\right)\left(\frac{2, b}{\infty}\right) = (-1)^{\frac{b^2-1}{8}}$$

El símbolo $\left(\frac{a}{b}\right)$ coincide con el símbolo de Jacobi, y en el caso en que b es un número primo determina si a es un residuo cuadrático módulo b.

Referencias

[1] D.A. Cox. *Primes of the Form x2+ny2: Fermat, Class Field Theory, and Complex Multiplication*. Pure and Applied Mathematics: A Wiley Series of Texts, Monographs and Tracts. Wiley, 2014.

[2] J Neukirch. *Algebraic Number Theory*. Grundlehren der mathematischen Wissenschaften. Springer Berlin Heidelberg, 2013.