Teoría de Cuerpos de clases

Patricio Pérez Piña

Seminario CM

1er semestre, 2020

Hoy

1. Previos a CFT
2. Resultados de la Teoría de cuerpos de clases:
    1. Teorema de reciprocidad de Artin
    2. Teorema de existencia.
    3. Teorema del conductor.
3. Algunas consecuencias
    1. Teorema de Kronecker-Weber.
    2. Existencia Cuerpos de clases de rayos.
4. CFT y leyes de reciprocidad.

Módulos en un cuerpo de números

Un **módulo** $\mathfrak{m}$ en K es un producto formal

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

donde

1. El valor $\mathfrak{p}$ recorre todos los primos (finitos e infinitos) de K,
2. Los exponentes $n_{\mathfrak{p}}$ son enteros no negativos,
3. Salvo un número finitos de excepciones $n_{\mathfrak{p}} = 0$,
4. Además, $n_{\mathfrak{p}} = 0$ si $\mathfrak{p}$ es complejo y $n_{\mathfrak{p}} \leq 1$ si $\mathfrak{p}$ es real.

Módulos en un cuerpo de números

- Ejemplos y observaciones:
  1. $2\mathbb{Z} \cdot (5\mathbb{Z})^2 \cdot \infty$ es un módulo en $\mathbb{Q}$.
  2. $17\mathbb{Z} \cdot \infty^2$ **NO** es un módulo en $\mathbb{Q}$.
  3. Si $\sigma : \mathbb{Q}(i) \to \mathbb{C}$ es un primo infinito arriba de ∞, entonces $(1+i)\mathbb{Z}[i] \cdot \sigma$ **NO** es un módulo en $\mathbb{Q}[i]$.
  4. Todo módulo en un cuerpo K totalmente imaginario se identifica con un ideal de $\mathcal{O}_K$.
  5. Más generalmente, todo módulo en un cuerpo de números K se escribe de la forma $\mathfrak{m} = \mathfrak{m}_0\mathfrak{m}_\infty$ donde $\mathfrak{m}_0$ se identifica con un ideal de $\mathcal{O}_K$ y $\mathfrak{m}_\infty$ es un producto finito de primos reales de K.
- Denotamos por 1 al módulo cuyos exponentes $n_\mathfrak{p} = 0$ para todo $\mathfrak{p}$.
- En adelante a los módulos $\mathfrak{m}$ en $\mathbb{Q}$ los escribimos de la forma $\mathfrak{m} = m\infty^r$, cuando $\mathfrak{m}_0 = m\mathbb{Z}$ y $r \in \{0, 1\}$.
- Ejemplo: Con esta notación el módulo del ejemplo 1 se denota por 50∞.

Dos grupos de ideales: $I_K(\mathfrak{m})$ y $P_{K,1}(\mathfrak{m})$

Sea $\mathfrak{m}$ un módulo en K. Definimos

$$I_K(\mathfrak{m}) = \{\text{ideales fraccionarios de } \mathcal{O}_K \text{ primos relativos a } \mathfrak{m}_0\},$$

y

$$P_{K,1}(\mathfrak{m}) = \{\alpha\mathcal{O}_K \mid \alpha \equiv 1 \mod \mathfrak{m}_0 \text{ y } \sigma(\alpha) > 0 \text{ para todo } \sigma \mid \mathfrak{m}_\infty\}.$$

Por ejemplo

1. El ideal $-4\mathbb{Z}$ pertenece a $P_{\mathbb{Q},1}(3\infty)$ porque $-4\mathbb{Z} = 4\mathbb{Z}$ y además $4 \equiv 1 \mod 3$ con $4 > 0$.
2. El ideal $-5\mathbb{Z}$ **NO** pertenece a $P_{\mathbb{Q},1}(3\infty)$ porque $5 \not\equiv 1 \mod 3$ y $-5 \equiv 1 \mod 3$ PERO $-5 \not> 0$.
3. El ideal $-5\mathbb{Z}$ pertenece a $P_{\mathbb{Q},1}(3)$ porque $-5 \equiv 1 \mod 3$ y $\infty \nmid 3$.

Un teorema de finitud

- **Teorema:** El índice $[I_K(\mathfrak{m}) : P_{K,1}(\mathfrak{m})]$ es finito.
- La demostración del caso general es consecuencia del Teorema de Aproximación, la finitud del grupo de clases I_K/P_K y un isomorfismo $I_K(\mathfrak{m})/P_K(\mathfrak{m}) \cong I_K/P_K$.
- Podemos estudiar casos más sencillos:
- **Proposición:** Sea $m > 0$. Entonces $[I_{\mathbb{Q}}(m\infty) : P_{\mathbb{Q},1}(m\infty)] = \varphi(m)$.
- Dem: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 $\Phi\colon I_{\mathbb{Q}}(m\infty) \to (\mathbb{Z}/m\mathbb{Z})^*$ definido por $\frac{a}{b}\mathbb{Z} \mapsto ab^{-1} \mod m$, cuando $\frac{a}{b} > 0$ y $\text{m.c.d}(m,a) = \text{m.c.d}(m,b) = 1$.
- Entonces $\ker \Phi = P_{\mathbb{Q},1}(m\infty)$ y como Φ es sobreyectiva se tiene que $[I_{\mathbb{Q}}(m\infty) : P_{\mathbb{Q},1}(m\infty)] = \varphi(m)$. □

Un teorema de finitud

- **Proposición:** 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: Sea

$$(\mathcal{O}_K/\mathfrak{m})^* \to I_K(\mathfrak{m}) \cap P_K/P_{K,1}(\mathfrak{m})$$

dado por $(a \mod \mathfrak{m}) \mapsto (a\mathcal{O}_K \mod P_{K,1}(\mathfrak{m}))$.

- Sean $\overline{a}, \overline{b} \in (\mathcal{O}_K/\mathfrak{m})^*$ con $a \equiv b \mod \mathfrak{m}$, entonces $a\mathcal{O}_K b^{-1}\mathcal{O}_K = ab^{-1}\mathcal{O}_K \in P_{K,1}(\mathfrak{m})$ ya que $ab^{-1} \equiv 1 \mod \mathfrak{m}$ y no hay condición al infinito!.
- La sobreyectividad del mapa implica 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. □

Grupos de clases generalizados

- **Definición:** 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: Tomando $\mathfrak{m} = 1$ y $H = P_K = P_{K,1}(\mathfrak{m})$ recuperamos el grupo de clases usual.
- Ejemplo: Si $K = \mathbb{Q}$, entonces $(\mathbb{Z}/m\mathbb{Z})^*$ "es" un grupo de clases generalizado para $\mathfrak{m} = m\infty$.
- Ejemplo: Sea $\mathcal{O}$ un orden de conductor f dentro de K un cuerpo cuadrático imaginario. Entonces $C(\mathcal{O})$ es un grupo de clases generalizado para $\mathfrak{f} = f\mathcal{O}_K$ pues $C(\mathcal{O}) \cong I_K(\mathfrak{f})/P_{K,\mathbb{Z}}(f)$ y $P_{K,1}(\mathfrak{f}) \subset P_{K,\mathbb{Z}}(f)$.

Teorema de Reciprocidad de Artin

- **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. El mapa de Artin $\Phi_{L/K}(\mathfrak{m})\colon I_K(\mathfrak{m}) \to \mathrm{Gal}(L/K)$ 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 $\mathfrak{m}$.
- **Corolario** Sea L/K una extensión abeliana de cuerpos de números, entonces $\mathrm{Gal}(L/K)$ es un grupo de clases generalizado para algún módulo $\mathfrak{m}$ en K.
- Demostración del corolario: Tomar $H = \ker \Phi_{L/K}(\mathfrak{m})$ con $\mathfrak{m}$ como en el Teorema. □

Un ejemplo de mapa de Artin

- Recuerdo: Sea m un entero positivo, ζ_m una raíz primitiva m-ésima de la unidad, $L = \mathbb{Q}(\zeta_m)$, $K = \mathbb{Q}$. Entonces existe un isomorfismo

$$\chi\colon \mathrm{Gal}(L/K) \to (\mathbb{Z}/m\mathbb{Z})^*\,, \text{ dado por } \sigma(\zeta_m) = \zeta_m^{\chi(\sigma)}.$$

- Ejemplo: Si $\mathfrak{m} = m\infty$, entonces 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 previamente definido en un ejemplo.
- Demostración: Sea p no dividiendo a 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 $\mathfrak{P} \mid p\mathbb{Z}$ en L.
- Entonces $\chi \circ \Phi_{L/K}(\mathfrak{m})(p\mathbb{Z}) = p \mod m$ por definición de χ y esto termina la prueba. □

Teorema de Existencia

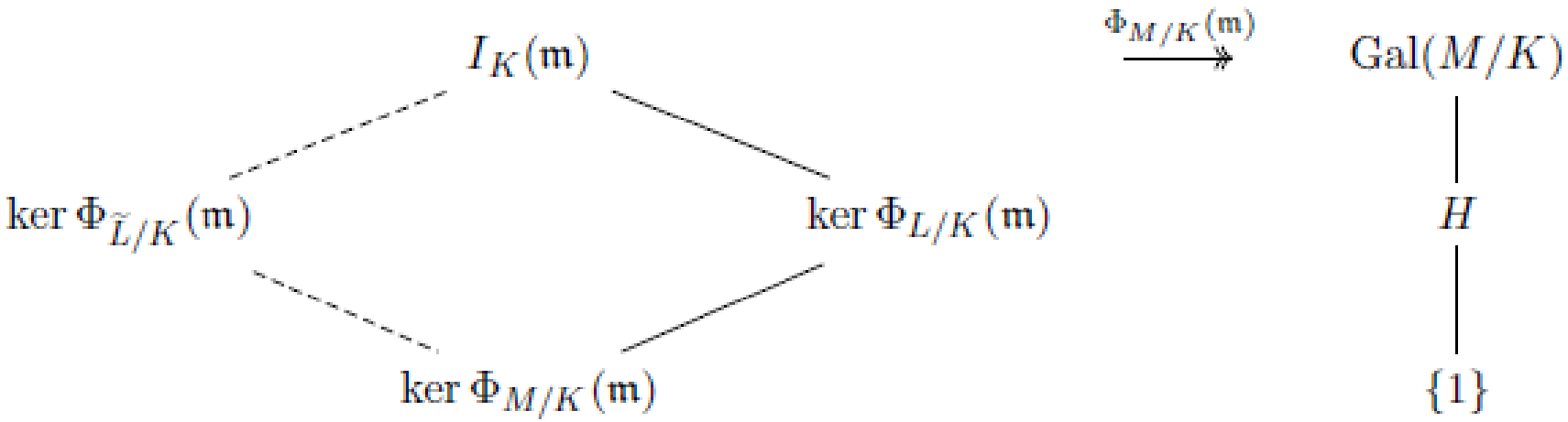
- **Teorema de Existencia:** Sea K un cuerpo de números, $\mathfrak{m}$ un módulo en K y H un subgrupo de congruencia para $\mathfrak{m}$. Entonces existe una única extensión abeliana L/K en la cual todos los primos que ramifican son divisores de $\mathfrak{m}$ y tal que $\ker \Phi_{L/K}(\mathfrak{m}) = H$.
- **Corolario:** 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: Supongamos que $L \subseteq M$ y sea $\mathfrak{m}$ módulo en K como en el Teorema de Reciprocidad para la extensión M/K. Entonces $\mathrm{res}_{M/L} \circ \Phi_{M/K}(\mathfrak{m}) = \Phi_{L/K}(\mathfrak{m})$ y luego

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

Teorema de Existencia



- Para la condición suficiente sea $H := \Phi_{M/K}(\mathfrak{m})\left(\ker \Phi_{L/K}(\mathfrak{m})\right)$.
- 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 $\Phi_{M/K}(\mathfrak{m})\left(\ker \Phi_{\widetilde{L}/K}(\mathfrak{m})\right) = \mathrm{Gal}(M/\widetilde{L}) = H$.
- Entonces $\ker \Phi_{\widetilde{L}/K}(\mathfrak{m}) = \ker \Phi_{L/K}(\mathfrak{m})$.
- Concluimos $L = \widetilde{L} \subseteq M$ por el Teorema de existencia. □

Kronecker-Weber y Cuerpos de clases de rayos

- **Corolario: Teorema de Kronocker-Weber** Sea $L/\mathbb{Q}$ una extensión abeliana. Entonces existe un entero m tal que $L \subseteq \mathbb{Q}(\zeta_m)$.
- Demostración: Por el Teorema de Reciprocidad de Artin existe $\mathfrak{m} = m\infty$ módulo en $\mathbb{Q}$ tal que $P_{\mathbb{Q},1}(\mathfrak{m}) \subseteq \ker \Phi_{L/\mathbb{Q}}(\mathfrak{m})$.
- Recordar que $\chi \circ \Phi_{\mathbb{Q}(\zeta_m)/\mathbb{Q}}(\mathfrak{m}) = \Phi$ con $\ker \Phi = P_{\mathbb{Q},1}(\mathfrak{m})$ por lo que $\ker \Phi_{\mathbb{Q}(\zeta_m)/\mathbb{Q}}(\mathfrak{m}) = P_{\mathbb{Q},1}(\mathfrak{m})$ (χ es un isomorfismo).
- El corolario anterior implica que $L \subseteq \mathbb{Q}(\zeta_m)$. □
- **Definición:** 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 $\mathfrak{m}$.

Cuerpos de clases de rayos y el conductor

- Ejemplo: Para m un entero positivo se tiene $\mathbb{Q}_{m\infty} = \mathbb{Q}(\zeta_m)$.
- Ejemplo: Sea $m > 2$ un entero, entonces $\mathbb{Q}_m = \mathbb{Q}(\zeta_m + \zeta_m^{-1})$.
- **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 $\mathfrak{f} \mid \mathfrak{m}$.
- **Definición:** El módulo $\mathfrak{f}(L/K)$ se conoce como el **conductor** de L/K.
- **Corolario:** K_1 es el **cuerpo de clases de Hilbert** de K.
- Demostración: K_1 es no ramificada pues solo ramifica en divisores de $\mathfrak{m} = 1$. Si L/K es abeliana y no ramificada entonces $\mathfrak{f}(L/K) = 1$ y luego $\ker \Phi_{K_1/K}(1) = P_{K,1}(1) \subseteq \ker \Phi_{L/K}(1)$.
- El cuerpo $K = \mathbb{Q}(\sqrt{17601097}, \sqrt{17380678572159893})$ tiene una extensión de Galois no ramificada e infinita (No es abeliana! $K_1 = K$).

El conductor

- Ejemplo: Sea m un entero positivo. Entonces

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

- **Proposición:** 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 $L \subseteq K_{\mathfrak{m}}$.
- **Corolario** Si $\mathfrak{f} = \mathfrak{f}(L/K)$, entonces $K_{\mathfrak{f}}$ es el menor cuerpo de clases de rayos que contiene a L.
- Ejemplo: Sea $L/\mathbb{Q}$ una extensión abeliana. Si f es el menor entero positivo m tal que $L \subseteq \mathbb{Q}(\zeta_m)$, entonces

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

El símbolo de Legendre

- Sea n un entero positivo y K un cuerpo de números conteniendo a ζ, raíz primitiva n-ésima de la unidad.
- Sea $\mathfrak{p}$ 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 tanto n divide a $|\,(\mathcal{O}_K/\mathfrak{p})^*\,| = N(\mathfrak{p}) - 1$.
- Si $\alpha \in \mathcal{O}_K$ primo relativo a $\mathfrak{p}$, como $\alpha^{\frac{N(\mathfrak{p})-1}{n}}$ es una solución a la ecuación $x^n - 1 \equiv 0 \mod \mathfrak{p}$, existe un única potencia de ζ tal que

$$\alpha^{\frac{N(\mathfrak{p})-1}{n}} \equiv \zeta^i \mod \mathfrak{p}.$$

- **Definición:** Dicha raíz de una unidad se conoce como el n-**ésimo símbolo de Legendre** $\left(\frac{\alpha}{\mathfrak{p}}\right)_n$.

El símbolo de Legendre

- **Proposición:** 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: Usar que $(\mathcal{O}_K/\mathfrak{p})^*$ es cíclico. □

- 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 $\sigma(\sqrt[n]{\alpha}) = \zeta\sqrt[n]{\alpha}$.

Reciprocidad débil

- **Teorema de 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.
- **Corolario:** Si G es la imagen de $\mathrm{Gal}(L/K)$ en μ_n, entonces el n-ésimo símbolo de Legendre induce un morfismo sobreyectivo

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

Ley de Reciprocidad cuadrática

- Demostración: Es suficiente mostrar la conmutatividad del diagrama en los primos $\mathfrak{p} \in I_K(\mathfrak{m})$. Tenemos

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

□

- **Lema:** 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: Sea p no ramificado en $\mathbb{Q}(\sqrt{q})$. Entonces p se escinde completamente si y solo si su grado de inercia es 1. Pero el grado de inercia es el orden del Frobenius en p. Es decir, necesitamos que $\Phi_{\mathbb{Q}(\sqrt{q})/\mathbb{Q}}(p)$ sea trivial. Por la reciproidad débil esto equivale a $\left(\frac{q}{p}\right)_2 = 1$. □
- Si fijamos el cuerpo $\mathbb{Q}(\sqrt{q})$ y variamos p no es molesto que la verificación no dependa de las clases módulo q?

Leyes de Reciprocidad cuadrática

- **Ley de Reciprocidad cuadrática:** Sean p y q dos primos racionales distintos e impares. Entonces

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

donde $p^* := (-1)^{\frac{p-1}{2}} p$.

- **Lema:** 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: Escribir $K = \mathbb{Q}(\sqrt{d_K})$. □
- Demostración del Teorema: Como $\mathrm{Gal}(\mathbb{Q}(\zeta_p)/\mathbb{Q})$ es cíclico de orden $p-1$, existe una única subextensión K de grado 2 sobre $\mathbb{Q}$. Como $K \subseteq \mathbb{Q}(\zeta_p)$, del lema anterior obtenemos que $K = \mathbb{Q}(\sqrt{p^*})$.
- Como $K \subseteq \mathbb{Q}(\zeta_p) = \mathbb{Q}(\zeta_{2p})$, entonces $P_{K,1}(2p\infty) \subseteq \ker \Phi_{K/\mathbb{Q}}(2p\infty)$.
- El teorema de reciprocidad débil implica

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

Leyes de Reciprocidad

- (continuación demostración) Por otra parte $I_{\mathbb{Q}}(2p\infty)/P_{\mathbb{Q},1}(2p\infty) \xrightarrow{\sim} (\mathbb{Z}/2p\mathbb{Z})^* \xrightarrow{\sim} (\mathbb{Z}/p\mathbb{Z})^*$. Entonces $\left(\frac{p^*}{\cdot}\right)_2$ induce el único morfismo sobreyectivo entre el grupo cíclico $(\mathbb{Z}/p\mathbb{Z})^*$ y $\{\pm 1\}$. Pero $\left(\frac{\cdot}{p}\right)_2$ satisface la misma propiedad y por tanto $\left(\frac{p^*}{q}\right)_2 = \left(\frac{q}{p}\right)_2$. para todo primo $q \neq p$ impar. □
- **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: Análoga. Aplicar Teorema de reciprocidad débil a la extensión $\mathbb{Q}(\sqrt{2})/\mathbb{Q}$. □

Leyes de Reciprocidad?

- **Observación:** 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 $\left(\frac{q}{p}\right)_2 = \begin{cases} \left(\frac{p}{q}\right)_2 & \text{si } p \equiv 1 \mod 4 \\ -\left(\frac{p}{q}\right)_2 & \text{si } p \equiv 3 \mod 4 \end{cases}$.
- **Corolario:** Sean p y q dos primos racionales distintos e impares.
  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.
- Ejemplo: Sea $q = 17$. Como $q \equiv 1 \mod 4$ tenemos que

  p 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.

Leyes de Reciprocidad?

- Ejemplo: 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

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

- Con el Teorema chino de los restos, resumimos todo lo anterior en

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

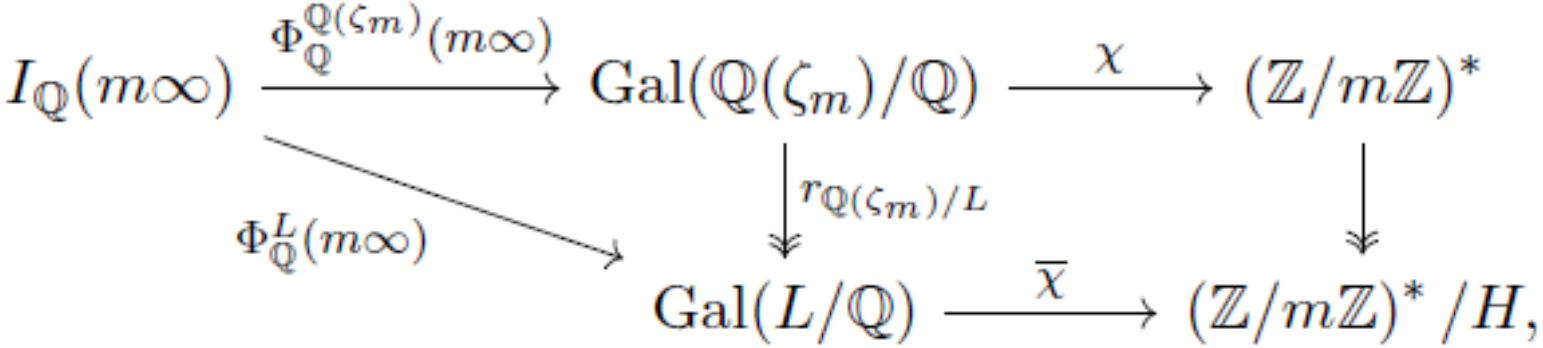
- Las leyes de reciprocidad serían resultados que describen los primos que se escinden completamente en términos de congruencias.

"Ley de Reciprocidad"

- **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 no ramificado 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 $p \equiv 1 \mod m$. □
- **Ley de reciprocidad para extensiones abelianas de $\mathbb{Q}$:** 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.

"Ley de Reciprocidad"

- Demostración: Kronecker-Weber nos dice que $L \subseteq \mathbb{Q}(\zeta_m)$. Tenemos un diagrama conmutativo



  con $H = \chi(\mathrm{Gal}(\mathbb{Q}(\zeta_m)/L))$ y $\overline{\chi}$ el isomorfismo inducido por χ.
- Tomando p no dividiendo a m tenemos que

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