ARITMÉTICA DE CUERPOS GLOBALES
(característica cero)

Joan Nualart (UB)

Study group: the geometric Langlands correspondence

14 de enero de 2010

CRM, Bellaterra (Barcelona)

Aritmética de cuerpos globales (char 0).

§1. Cuerpos de números:

- Cuerpo de números: K cuerpo t.q. $K/\mathbb{Q}$ finito.

  $\overline{K}$: clausura alg. de K.

1.1. Anillos de enteros:

Def: B anillo, $A \subseteq B$ subanillo.
Un elemento $b \in B$ se llama entero sobre A si b es raíz de un polinomio mónico con coeficientes en A. La extensión B/A se dice entera cuando todo elemento de B es entero sobre A.

Prop: B/A ext. de anillos y $b \in B$. Son equivalentes:
(i) b es entero sobre A
(ii) El anillo $A[b]$ és un A-módulo f.g.

Cor: B anillo, $A \subseteq B$ subanillo. El conjunto de los elementos de B que son enteros sobre A es un subanillo de B que contiene A. Este subanillo se denomina la clausura entera de A en B.

Def: B anillo, $A \subseteq B$ subanillo.
Se dice que A es enteramente cerrado en B cuando A es su propia clausura entera en B.

Prop: B/A ext. de anillos i C la clausura entera de A en B. Entonces C es enteramente cerrado en B.

- **Def** (Anillo de enteros): Un entero alg. és un elemento de $\overline{\mathbb{Q}}$ que es entero sobre $\mathbb{Z}$. Si K es un cuerpo de números, la clausura entera de $\mathbb{Z}$ en K, $\mathcal{O}_K$, se llama el anillo de enteros de K; es el anillo formado por todos los elementos de K que son enteros algebraicos.

Ejemplos: (i) $\mathbb{Z}[i] \subset \mathbb{Q}(i)$

(ii) $\mathbb{Z}\left[\frac{1+\sqrt{-3}}{2}\right] \subset \mathbb{Q}(\sqrt{-3})$

- **Prop:** El anillo de enteros de un cuerpo de números es un dominio noetheriano, enteramente cerrado y de dimensión 1 (↳ todo ideal primo no nulo es maximal)

  (II) es un anillo de Dedekind.

- **Thm:** Todo ideal $\mathfrak{a}$ de $\mathcal{O}$ no trivial admite una factorización

$$\mathfrak{a} = \mathfrak{p}_1 \cdots \mathfrak{p}_r, \quad \mathfrak{p}_i \subseteq \mathcal{O} \text{ ideales primos no nulos}$$

que es única módulo el orden de los factores.

- **Def:** Un ideal fraccionario $\mathfrak{a}$ de K es un $\mathcal{O}$-submódulo no nulo f.g. de K. (equiv. si $\exists c \in \mathcal{O}, c \neq 0$, t.q. $c\mathfrak{a} \subseteq \mathcal{O}$ es un ideal de $\mathcal{O}$)

  . Un ideal fraccionario se denomina principal cuando es de la forma $a\mathcal{O}$, $a \in K^\times$.

- **Prop:** Los ideales fraccionarios forman un grupo abeliano libre respecto de la multiplicación. El elemento identidad es $(1) = \mathcal{O}$ y el inverso de $\mathfrak{a}$ es

$$\mathfrak{a}^{-1} = \{x \in K \mid x\mathfrak{a} \subseteq \mathcal{O}\}.$$

Los ideales primos no nulos de $\mathcal{O}$ forman un sistema de generadores libres de este grupo.

- **Def:** El grupo de ideales fraccionarios no nulos de $\mathcal{O}$ se llama el grupo de ideales de K. El grupo cociente de este grupo de ideales por el subgrupo de los ideales fraccionarios principales se denomina el grupo de clases de ideales de K. lo designamos Cl_K.

$$1 \longrightarrow \mathcal{O}^* \longrightarrow K^* \longrightarrow I(K) \longrightarrow Cl_K \longrightarrow 1 \text{ exacta}$$

grupo de ideales principales P_K $\quad 0 \to K^*/\mathcal{O}^* \to$ grupo de ideales fracc.

- **Teorema (Dirichlet)**: $Cl(k)$ es un grupo abeliano finito.

- **1.2. Ramificación**: k cuerpo de números, $\mathcal{O}_k$ anillo de enteros
  L cuerpo de números, $\mathcal{O}_L$ anillo de enteros.
  $L|k$.

$\mathfrak{p} \neq 0$ ideal primo de $\mathcal{O}_k$ ($\mathfrak{p}\mathcal{O}_L \neq \mathcal{O}_L$) descompone en $\mathcal{O}_L$ como

$$\mathfrak{p}\mathcal{O}_L = \mathfrak{P}_1^{e_1} \cdots \mathfrak{P}_g^{e_g}$$

Decimos que $\mathfrak{P}_1, \dots, \mathfrak{P}_g$ son los primos de $\mathcal{O}_L$ sobre $\mathfrak{p}$ y lo escribimos $\mathfrak{P}_i | \mathfrak{p}$.

e_i es el índice de ramificación

$f_i = [\underbrace{\mathcal{O}_L/\mathfrak{P}_i : \mathcal{O}_k/\mathfrak{p}}_{\text{ext. de cuerpos}}]$ es el grado residual.

Prop: $\sum_{i=1}^{g} e_i f_i = n = [L:k]$.

~~**Prop**: El número de primos de~~

Def: $\mathfrak{p} = \mathfrak{P}_1^{e_1} \cdots \mathfrak{P}_g^{e_g}$ decimos que:

- descompone completamente en L si $g = n = [L:k]$ ($\Rightarrow e_i = f_i = 1 \ \forall i$)

Decimos $\mathfrak{P}_i$ es no ramificado si $e_i = 1$ y ramificado si $e_i > 1$.
totalmente ramificado si además $f_i = 1$

$\mathfrak{p}$ se dice no ramificado si todos los $\mathfrak{P}_i$ lo son, y ramificado si no.

$L|k$ se dice no ramificado si todos los primos $\mathfrak{p}$ de k son no ramificados en L.

Prop: El número de primos de k ramificados en L es finito.

Si $L|k$ es de Galois,

Prop: $Gal(L|k)$ actúa transitivamente en el cjto de todos los primos $\mathfrak{P}$ de $\mathcal{O}_L$ sobre $\mathfrak{p}$.
(los primos sobre $\mathfrak{p}$ son conjugados)

Def: $\mathfrak{P}|\mathfrak{p}$, $D(\mathfrak{P}|\mathfrak{p}) = \{\sigma \in Gal(L|k) \mid \sigma(\mathfrak{P}) = \mathfrak{P}\} \subset Gal(L|k)$ subgrupo de descomposición de $\mathfrak{P}|\mathfrak{p}$.

Propiedades: · $[Gal(L|k) : D(\mathfrak{P}|\mathfrak{p})] = g$

· $D(\mathfrak{P}|\mathfrak{p}) \simeq Gal(L_{\mathfrak{P}}|k_{\mathfrak{p}})$ canónicamente

1.3. Idèles y adèles:

k cuerpo de números

Def (Plaza): Una plaza de k es una clase de equiv. de ~~valoraciones~~ valores absolutos de k. Las plazas definidas por ~~valoraciones~~ valores absolutos no arquimedianas se llaman plazas finitas y están en corresp. biyectiva con los ideales primos de $\mathcal{O}_k$. Las plazas definidas por ~~valoraciones~~ valores absolutos arquimedianas se llaman plazas infinitas y se corresponden con los r_1 inmersiones reales $k \hookrightarrow \mathbb{R}$ y con los r_2 parejas de inmersiones complejas no reales $k \hookrightarrow \mathbb{C}$. Está claro que $[k:\mathbb{Q}] = r_1 + 2r_2$

Para cada plaza $\mathfrak{p}$ de k y cada entero $u_{\mathfrak{p}} \geq 0$, que se supone $u_{\mathfrak{p}} \in \{0,1\}$ si $\mathfrak{p}|\infty$, definimos:

$$U_{\mathfrak{p}}^{(u_{\mathfrak{p}})} = \begin{cases} 1+\mathfrak{p}^{u_{\mathfrak{p}}}, & u_{\mathfrak{p}} > 0 \\ U_{k_{\mathfrak{p}}}, & u_{\mathfrak{p}} = 0,\ \mathfrak{p} \nmid \infty \\ \mathbb{R}^\times, & \mathfrak{p} \text{ real y } u_{\mathfrak{p}} = 0 \\ \mathbb{R}_+^\times, & \mathfrak{p} \text{ real y } u_{\mathfrak{p}} = 1 \\ \mathbb{C}^\times, & \mathfrak{p} \text{ complejo.} \end{cases}$$

Def: Anillo de adèles: $\mathbb{A}_k = \{(\alpha_{\mathfrak{p}}) \in \prod_{\mathfrak{p}} k_{\mathfrak{p}} : \alpha_{\mathfrak{p}} \in \mathcal{O}_{\mathfrak{p}} \text{ c.p.t.}\}$

Grupo de idèles: $\mathbb{I}_k = \mathbb{A}_k^\times = \{(\alpha_{\mathfrak{p}}) \in \prod_{\mathfrak{p}} k_{\mathfrak{p}}^\times : \alpha_{\mathfrak{p}} \in U_{\mathfrak{p}} \text{ c.p.t.}\}$

Grupo de S-idèles: $\mathbb{I}_k^S = \prod_{\mathfrak{p} \in S} k_{\mathfrak{p}}^\times \times \prod_{\mathfrak{p} \notin S} U_{\mathfrak{p}}$

S cjto finito de plazas

Obs: $\mathbb{I}_k = \bigcup_S \mathbb{I}_k^S$.

$\mathbb{A}_K$ es un anillo topológico

$\mathbb{I}_K$ es un grupo topológico loc. compacto.

$K^\times \hookrightarrow \mathbb{I}_K$ $\quad x \longmapsto (x_\mathfrak{p})_\mathfrak{p}$, $x_\mathfrak{p} = x$ $\forall \mathfrak{p}$ identifico $K^\times$ con un subgrupo discreto y cerrado de $\mathbb{I}_K$, el subgrupo de idèles principales.

El grupo topológico cociente $C_K := \mathbb{I}_K / K^\times$ (top. cociente) es el grupo de clases de idèles de K (grupo abeliano infinito)

Tenemos una aplicación natural que a cada idèle le asigna un ideal fraccionario:

$$\begin{aligned} \mathbb{I}_K &\longrightarrow I_K \\ \alpha = (\alpha_\mathfrak{p})_\mathfrak{p} &\longmapsto (\alpha) = \prod_{\mathfrak{p} \nmid \infty} \mathfrak{p}^{v_\mathfrak{p}(\alpha_\mathfrak{p})} \end{aligned}$$

Esta aplicación es exhaustiva y tiene núcleo $\mathbb{I}_K^{S_\infty}$.

Prop: i) El grupo de clases de ideales de K es un cociente de su grupo de clases de idèles:

$$C_K \Big/ \left(\mathbb{I}_K^{S_\infty} K^\times / K^\times \right) \simeq \mathbb{I}_K \Big/ \mathbb{I}_K^{S_\infty} K^\times \simeq Cl_K.$$

ii) Si S es un cjto de plazas suficientemente grande $C_K \simeq \mathbb{I}_K^S K^\times / K^\times$.

Def: $\mathfrak{m} = \prod_{\mathfrak{p} \nmid \infty} \mathfrak{p}^{\mu_\mathfrak{p}}$ ideal entero de K. Consideremos el subgpo de idèles $\mathbb{I}_K^{\mathfrak{m}} = \prod_\mathfrak{p} U_\mathfrak{p}^{(\mu_\mathfrak{p})}$.

- $I_K^{\mathfrak{m}}$ gpo de ideales fracc. de K primos con $\mathfrak{m}$.
- $P_K^{\mathfrak{m}} = \{(\alpha) \in P_K : \alpha \equiv 1 \pmod{\mathfrak{m}}, \alpha \text{ tot positivo}\}$ (subgpo de ideales princ.)
- $Cl_K^{\mathfrak{m}}$ = grupo de clases de rayas de ideales mod $\mathfrak{m}$.

$C_K^{\mathfrak{m}} = \mathbb{I}_K^{\mathfrak{m}} K^\times / K^\times$ subgpo de cong. mod $\mathfrak{m}$.

$Cl_K^{\mathfrak{m}} = C_K / C_K^{\mathfrak{m}}$ grupo ~~de cla~~ radial de clases de idèles mod $\mathfrak{m}$

Prop: $H \subset C_k$ subgrupo. H es cerrado y de índice $< \infty$
$\Leftrightarrow \exists$ ideal $\mathfrak{m}$ entero t.q. $H \supseteq C_k^{\mathfrak{m}}$.

Prop: $I_k \longrightarrow I_k$ induce un isomorfismo

$$Cl_k^{\mathfrak{m}} \simeq C_k^{\mathfrak{m}}.$$

$L|k$ ext. finita de cuerpos de números. Entonces,

$$I_k \hookrightarrow I_L$$
$$\alpha = (\alpha_p)_p \longmapsto \alpha' = (\alpha'_{\mathfrak{P}}) \text{ t.q. } \alpha'_{\mathfrak{P}} = \alpha_p \in k_p^\times \subseteq L_{\mathfrak{P}}^\times \text{ si } \mathfrak{P}|p$$

Si $L|k$ Galois, todo $\sigma \in Gal(L|k)$ induce un automorfismo
$\sigma : I_L \to I_L$ y se cumple,

$$I_L^{Gal(L|k)} = I_k.$$

además, $N_{L|k} : I_L \longrightarrow I_k$

$$\alpha = (\alpha_{\mathfrak{P}})_{\mathfrak{P}} \longmapsto N_{L|k}(\alpha) = (N_{L|k}(\alpha))_p$$

donde $N_{L|k}(\alpha)_p = \prod_{\mathfrak{P}|p} N_{L_{\mathfrak{P}}|k_p}(\alpha_{\mathfrak{P}})$

es un homomorfismo análogo a la norma entre cuerpos de números o cuerpos locales.

§ 2. Teoría global de cuerpos de clases:

2.1. Símbolo de Hilbert. Fórmula del producto:

Sea n entero ≥ 2 y k cuerpo de números que contiene el grupo μ_n de raíces n-ésimas de la unidad.

$\forall p$ plaza de k, $(\ ,\ )_p : k_p^\times \times k_p^\times \longrightarrow \mu_n$
símbolo de Hilbert n-ésimo.

- **Tma (Fórmula del producto):** $\forall a, b \in k^\times$,

$$\prod_p (a,b)_p = 1.$$

? **Aplicación:** Símbolo de residuos de potencias n-ésimas.

- $\left(\frac{a}{\mathfrak{P}}\right) = (\pi, a)_p$, donde $\mathfrak{P}$ primo de k, $\mathfrak{P} \nmid n$
$a \in U_p \subset k_p^\times$
π elemento primo de k_p

es independiente de la elección de π

y $\left(\frac{a}{\mathfrak{p}}\right) \equiv a^{(q-1)/n} \pmod{\mathfrak{p}}$, $q = N(\mathfrak{p})$

En particular,

$$\left(\frac{a}{\mathfrak{p}}\right) = 1 \iff a = \alpha^n \pmod{\mathfrak{p}}.$$

(Generalización del símbolo de Legendre).

- $\mathfrak{b} = \prod_{\mathfrak{p} \nmid n} \mathfrak{p}^{\nu_\mathfrak{p}}$, a primo con $\mathfrak{b}$

$$\left(\frac{a}{\mathfrak{b}}\right) = \prod_{\mathfrak{p} \nmid n} \underbrace{\left(\frac{a}{\mathfrak{p}}\right)^{\nu_\mathfrak{p}}}_{= 1 \text{ si } \nu_\mathfrak{p} = 0}$$

es mult. en ambos argumentos y si $\mathfrak{b} = (b)$ lo escribimos $\left(\frac{a}{\mathfrak{b}}\right) = \left(\frac{a}{b}\right)$.

(Generalización del símbolo de Jacobi)

Thm (Ley de reciprocidad para potencias n-ésimas):

$a, b \in k^\times$ coprimos y primos con n,

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

Dem: Fórmula del producto /

(Generalización de la ley de reciprocidad cuadrática)

2.2. Grupo de Brauer de $\mathbb{Q}$ y de un cuerpo de números

k cuerpo de números

$Br(k) = \{ A \mid A \text{ } k\text{-álg central y simple} \} / \sim$

donde $A \sim A' \iff \exists n, m$ enteros positivos tq $A \otimes M_n(k) \simeq A' \otimes M_m(k)$.

que tiene estructura de grupo con la operación $\otimes$:

$$[A] \otimes [B] = [A \otimes_k B].$$

L

- Sea k cuerpo de números y L/k ext. no nec. finita. Entonces, existe un morfismo de grupos:

$$\begin{aligned} Br(k) &\longrightarrow Br(L) \\ [A] &\longmapsto [A \otimes_k L] \end{aligned}$$

Denotamos $Br(L|k)$ el núcleo de este morfismo que, por definición, es

$$\{[A]\ k\text{-alg. c.s} \mid A \otimes_k L \text{ es alg. de matrices}\}.$$

entonces, $Br(k) = \bigcup_{\bar{k}|L|k} Br(L|k)$.

(*) · Tma: $0 \to Br(k) \to \bigoplus_{\mathbb{Q}/\mathbb{Z}} Br(k_p) \xrightarrow{\Sigma} \mathbb{Q}/\mathbb{Z} \to 0$

$[A] \longmapsto (\ [A \otimes_k k_p]\ )_p$

es exacto.

→ Los invariantes locales de una clase global satisfacen una relación.

→ Relación con el símbolo de Hilbert:

Sea k cuerpo de números tq $\mu_u \subset k$.

$\forall a, b \in k^\times$ i ζ raíz primitiva u-ésima de la unidad, sea $A(a,b;\zeta)$ la k-alg. con generadores i, j tq $i^u = a$, $j^u = b$, $ij = \zeta ji$. Entonces, $A(a,b;\zeta)$ es central y simple y la clase en $Br(k_v)$ representada por $A(a,b;\zeta)$ es de u-torsión y viene dada mediante la identificación $Br(k_v) \simeq \mathbb{Q}/\mathbb{Z}$ y la elección de una raíz primitiva u-ésima de la unidad, por $(a,b)_v$.

Interpretación cohomológica:

· $L|k$ de Galois (finita)

· Def: $H^2(L|k) := H^2(Gal(L|k), L^\times)$.

· Tma: 1) $H^2(L|k) \simeq Br(L|k)$

2) $H^2(\bar{k}|k) \simeq Br(k)$.

Dem (Idea): 1) $\Rightarrow$ 2) ✓

1) A/k alg. c.s. tq $\exists L|k$ finito de Galois con $[A:k] = [L:k]^2$

Tma Skolem-Noether $\Rightarrow \forall \sigma \in Gal(L|k)$, $\exists e_\sigma \in A$ tq. $\sigma a = e_\sigma a e_\sigma^{-1}$ $\forall a \in L$

y e_σ está determinado módulo multiplicación por $L^\times$.

Entonces, $e_\sigma e_\tau = \varphi(\sigma,\tau)\, e_{\sigma\tau}$, $\varphi(\sigma,\tau) \in L^\times$

$\rightsquigarrow$ φ 2-cociclo y diferentes e_σ dan lugar a un cociclo cohomólogo

$\rightsquigarrow$ $\varphi \in H^2(L|k)$

Recíprocamente, dado $\varphi : Gal(L|k) \times Gal(L|k) \to L^\times$ 2-cociclo

Definimos $A(\varphi)$ como el L-e.v. con base $(e_\sigma)_{\sigma \in Gal(L|k)}$

y multiplicación $\sigma a = e_\sigma a e_\sigma^{-1}$

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

$\rightsquigarrow$ $\begin{cases} e_1 \text{ identidad por la multiplicación} \\ e_\rho(e_\sigma e_\tau) = (e_\rho e_\sigma) e_\tau \text{ por 2-cociclo.} \end{cases}$

$\to$ $A(\varphi)$ k-alg con $L \simeq L e_1 \subset A(\varphi)$ que és c.s. $=$

$\downarrow$

- $\circledast \iff 0 \to H^2(\bar{k}|k) \to \bigoplus_{\mathcal{P}} H^2(\bar{k}_\mathcal{P}|k_\mathcal{P}) \to \mathbb{Q}/\mathbb{Z} \to 0$. exacta

2.3. Ley de reciprocidad global y símbolo de Artin:

Thm (Ley de reciprocidad de Artin): $L|k$ ext. finita y abeliana de cuerpos de números.

(i) $\exists$ isomorfismo canónico $r_{L|k} : Gal(L|k) \to C_k/N_{L|k} C_L$ llamado reciprocidad.

(ii) El isomorfismo inverso de $r_{L|k}$,

$(\ , L|k) : C_k/N_{L|k} C_L \longrightarrow Gal(L|k)$ define el símbolo global de residuos nórmicos.

Obs: C_k juega el papel en la teoría global de $k^\times$ en la teoría local.

Compatibilidad entre las teorías local y global:

$L_\mathfrak{p}$ completado de L respecto de $\mathfrak{P}|\mathfrak{p}$.

Entonces, $\exists$ diagrama conmutativo

$$\begin{array}{ccc} k_\mathfrak{p}^\times & \xrightarrow{(\,,L_\mathfrak{p}|k_\mathfrak{p})} & Gal(L_\mathfrak{p}|k_\mathfrak{p}) \\ i\downarrow & /\!/\!/ & \downarrow i \\ C_k & \xrightarrow[(\,,L|k)]{} & Gal(L|k) \end{array}$$

donde $i: k_\mathfrak{p}^\times \longrightarrow C_k$

$$a_\mathfrak{p} \longmapsto (\ldots, 1, 1, a_\mathfrak{p}, 1, 1, \ldots)$$

En otras palabras, dado $\alpha = (\alpha_\mathfrak{p}) \in \mathbb{I}_k$,

$$(\alpha, L|k) = \prod (\alpha_\mathfrak{p}, L_\mathfrak{p}|k_\mathfrak{p})$$

Obs: • Si $\alpha \in k^\times$, $\prod (\alpha_\mathfrak{p}, L_\mathfrak{p}|k_\mathfrak{p}) = 1$ $\Big| \Rightarrow$ Fórmula del producto para el símb. de Hilb.

• $(a, k(\sqrt[n]{b})|k)\sqrt[n]{b} = (a,b)_\mathfrak{p}\sqrt[n]{b}$

Teorema (existencia): La aplicación $L \longmapsto N_L = N_{L|k} C_L$ establece una biyección entre el cjto de ext. abelianas finitas de k y el cjto de los subgrupos de C_k cerrados y de índice finito. Se cumple que:

- $L_1 \subseteq L_2 \iff N_{L_1} \supset N_{L_2}$
- $N_{L_1 L_2} = N_{L_1} \cap N_{L_2}$
- $N_{L_1 \cap L_2} = N_{L_1} N_{L_2}$.

Def: $H \subset C_k$ subgpo cerrado y de índice finito. La ext. ab. corresp. mediante el Teo de exist. se llama cuerpo de clases de H. Si $H = C_k^m$ es el subgpo de cong. mod m, entonces el cuerpo k^m corresp. se llama cuerpo de clases radiales módulo m. Por lo tanto

$$Gal(k^m/k) \simeq Cl_k^m.$$

Si $m = (1)$ se obtiene el cuerpo de clases de Hilbert $\equiv$ ext. ab. no ramificada max de k.

Cuerpos de clases y ramificación

Def: $\forall L|k$ fin. ab. $\exists k^m|L$. m se llama un módulo de def. de $L|k$. El conductor de $L|k$, $f_{L|k}$, es el mcd de todos los mod. de definición, i.e. el menor módulo ~~de def~~ tq $k \subseteq L \subseteq k^{f_{L|k}}$.

Prop: $L|k$ fin. ab., $f_\mathfrak{p}$ cond. de $L_\mathfrak{P}|k_\mathfrak{p}$. Entonces,

$$f_{L|k} = \prod_{\mathfrak{p}|\infty} f_\mathfrak{p}$$

$\Rightarrow$ un primo finito $\mathfrak{p}$ ramifica en $L \Leftrightarrow \mathfrak{p} \mid f_{L|k}$.

(Descripción $U^{(i)} \leftrightarrow G^i$ de la teoría local.)

Símbolo de Artin (Reinterpretación de la ley de reciprocidad mediante ideales)

$L|k$ no ramif. en $\mathfrak{p}$, primo finito de k.

$\mathrm{Gal}(L_\mathfrak{P}|k_\mathfrak{p}) \subseteq \mathrm{Gal}(L|k)$ cíclico y tiene un generador distinguido, $\varphi_\mathfrak{P}$, el automorfismo de Frobenius.

Si $L|k$ ab., $\varphi_\mathfrak{p} := (\pi_\mathfrak{p}, L_\mathfrak{P}|k_\mathfrak{p}) =: \left(\frac{L|k}{\mathfrak{p}}\right)$.

Entonces, para un ideal $\mathfrak{a} = \prod \mathfrak{p}^{v_\mathfrak{p}}$ de $\mathcal{O}_k$ no div. por ningún primo ramificado, definimos el símbolo de Artin de $\mathfrak{a}$:

$$\left(\frac{L|k}{\mathfrak{a}}\right) = \prod_{\mathfrak{p}|\mathfrak{a}} \left(\frac{L|k}{\mathfrak{p}}\right)^{v_\mathfrak{p}(\mathfrak{a})}$$

(Generalización del símbolo de Kronecker)

De este modo,

$$\begin{array}{ccccccc} 1 \to & N_{L|k} C_L & \to & C_k & \xrightarrow{(\,,L|k)} & \mathrm{Gal}(L|k) \to 1 \\ & \downarrow & & \downarrow & & \downarrow \mathrm{id} \\ 1 \to & H^m/P_k^m & \to & Cl_k^m & \xrightarrow{\left(\frac{L|k}{\cdot}\right)} & \mathrm{Gal}(L|k) \to 1 \end{array}$$

donde $H^m := (N_{L|k} I_k^m) P_k^m$.

Teorema (Ley de descomposición)

$L|k$ ob. de grado n, $\mathfrak{p}$ primo de k no ramif. en L

$\mathfrak{m}$ mod. de def de $L|k$ tq $\mathfrak{p} \nmid \mathfrak{m}$.

Si f es el mínimo entero tq $\mathfrak{p}^f \in (N_{L|k} I_L^{\mathfrak{m}}) P_k^{\mathfrak{m}}$, entonces

$\mathfrak{p}\mathcal{O}_L = \mathfrak{P}_1 \cdots \mathfrak{P}_g$, donde $g = \frac{n}{f}$ y el grado residual de cada primo $\mathfrak{P}|\mathfrak{p}$ es f.

$\Downarrow$

- $\mathfrak{p}$ descompone completamente en el cuerpo de clases de Hilbert de $k \Leftrightarrow$ es principal en k.
- Todo ideal de k ext. al cuerpo de clases de Hilbert de k se convierte en principal. Esta propiedad caracteriza al cuerpo de clases de Hilbert

2.4. Extensión abeliana maximal de $\mathbb{Q}$ y de un cuerpo de números

Thm (Kronecker-Weber): Toda ext. finita y abeliana $L|\mathbb{Q}$ es ciclotomica, i.e. $\exists m$ tq $L \subset \mathbb{Q}(\mu_m)$.

Cor: La ext. ab. maximal de $\mathbb{Q}$ es $\mathbb{Q}(\mu_\infty)$

y $\mathrm{Gal}(\mathbb{Q}(\mu_\infty)|\mathbb{Q}) = \varprojlim_m \mathrm{Gal}(\mathbb{Q}(\mu_m)|\mathbb{Q}) = \varprojlim_m \left(\mathbb{Z}/m\mathbb{Z}\right)^\times$

$\simeq \prod_p \mathbb{Z}_p^\times$.

En general, para un cuerpo de números k,

$\mathrm{Gal}(k^{ab}|k) = \varprojlim_m C_k/C_k^m = \hat{C}_k$ ← completación profinita.

2.5. Idea de la demostración de la ley de reciprocidad: por vía cohomológica

Obj: $\exists \varnothing: C_k/N_{L|k} C_L \xrightarrow{\sim} G = \mathrm{Gal}(L|k)$ tq sus componentes locales son los símbolos locales.

Idea: Definir $\varnothing$ o partir de esta propiedad y comprobar que cumple todas las propiedades.

$\forall \mathfrak{p}$ primo de k, $\mathfrak{P} \mid \mathfrak{p}$ primo de L

$$\begin{array}{ccc} k_{\mathfrak{p}}^{\times} & \xrightarrow{\varphi_{\mathfrak{p}}} & Gal(L_{\mathfrak{P}} \mid k_{\mathfrak{p}}) \\ \downarrow i & /\!/\!/ & \downarrow i \\ \mathbb{I}_k & \xrightarrow[\varphi]{} & Gal(L|k) \end{array}$$

L

① $H^0(G, \mathbb{I}_L) = \mathbb{I}_k$, $H^r(G, \mathbb{I}_L) \simeq \bigoplus_{\mathfrak{p}} H^r(G^{\mathfrak{P}}, L^{\mathfrak{P}^\times})$

donde $\mathfrak{P} \mid \mathfrak{p}$, $G^{\mathfrak{P}}$ gpo de desc. y $L^{\mathfrak{P}} = L_{\mathfrak{P}}$.

② Primera desigualdad: $\dfrac{(C_k : N_{L|k} C_L)}{|H^1(G, C_L)|} = [L:k]$.

$L|k$ cíclica.

$\Rightarrow (C_k : N C_L) \geq [L:k]$.

③ $\forall L|k$ abeliana, $Gal(L|k)$ está generado por elementos de Frobenius.

④ Segunda desigualdad: $L|k$ fin de Galois, $G = Gal(L|k)$

a) $(C_k : N_{L|k} C_L) \mid [L:k]$.

b) $H^1(G, C_L) = 0$.

c) $H^2(G, C_L)$ finito y su orden divide $[L:k]$.

$\mathbb{I}_k$.

⑤ a) $L|k$ fin. ab. $\varphi(k^\times) = 1$

b) $L|k$ fin. Gal., $\sum inv_v(\alpha) = 0 \quad \forall \alpha \in H^2(L|k)$.

$$\left[\begin{array}{l} 5a \Rightarrow \ker \varphi \supset k^\times \\ N_{L|k}(\mathbb{I}_L) \subset \ker \varphi \\ 3 \Rightarrow \varphi \text{ exh.} \end{array} \;\middle|\; \searrow \overset{④}{\Longrightarrow} \varphi \text{ iso.} \right]$$

⑥ Teoría de kummer $\Rightarrow$ fmla de exist.