MAT 529 : Aritmética

Referencias

1. Jürgen NEUKIRCH, "Algebraic Number Theory"
2. Pierre SAMUEL, "Algebraic Theory of Numbers"
3. Jean-Pierre SERRE, "Local Fields"

El curso estará dividido en 3 grandes tópicos:

I. Anillos de Enteros y Teoría de Galois
II. Anillos de Dedekind y Valuaciones
III. Geometría de Números

Parte I: Anillos de Enteros y Teoría de Galois

§ 1. Recuerdos de Álgebra Abstracta

Sea A un anillo conmutativo. Recordemos que una A-álgebra es un anillo B junto con un morfismo $\rho_B : A \to B$, que permite definir una estructura de A-módulo en B

$$A \times B \longrightarrow B, \quad (a,b) \mapsto a \cdot b := \rho_B(a)b$$

y de tal suerte que el producto en B es A-bilineal. Además, $\rho_B(1_A) \overset{\text{def}}{=} 1_B$.

Ejemplos: ① Todo anillo conmutativo con unidad (eg. $\mathbb{Z}/n\mathbb{Z}$) es una $\mathbb{Z}$-álgebra.
② $M_n(A)$ es una A-álgebra.
③ El anillo de polinomios $A[X_1, \ldots, X_n]$ es una A-álgebra.
④ Si B es una A-álgebra conmutativa y C una B-álgebra, entonces C es una A-alg.

Def: Sean B y C dos A-álgebras. Un morfismo de anillos $\varphi : B \to C$ es un morfismo de A-álgebras si es A-lineal, ie, si $\varphi \circ \rho_B = \rho_C$.

$$\begin{tikzcd} B \arrow[rr, "\varphi"] & & C \\ & A \arrow[ul, "\rho_B"] \arrow[ur, "\rho_C"'] & \end{tikzcd}$$

Def: Sea B una A-álgebra. Un subanillo $C \subseteq B$ es una subálgebra si $\operatorname{Im}(\rho_B) \subseteq C$. En ese caso, $\rho_C : A \to C$, $a \mapsto \rho_B(a)$ define una estructura de A-álgebra en C.

Ejemplos: ① Si $\{A_i\}_{i\in I} \subseteq B$ son subalgebras, $\bigcap_{i\in I} A_i \subseteq B$ también lo es.
② Si B es una A-álgebra y $X \subseteq B$ es un subconjunto, entonces

$$\langle X \rangle_{A\text{-alg}} := \bigcap_{\substack{C \subseteq B \text{ subalg} \\ \text{tq } X \subseteq C}} C$$ es el subalg. de B generada por X.

En part, si $\alpha_1, \ldots, \alpha_n \in B$ entonces escribimos $A[\alpha_1, \ldots, \alpha_n] := \langle \{\alpha_1, \ldots, \alpha_n\} \rangle_{A\text{-alg}}$.

Recuerdo (división euclideana): Sean $F, G \in A[X]$ con $G = \sum_{i=0}^{d} a_i X^i$ tal que $a_d \in A^*$ (ie, coef. líder invertible). Entonces, $\exists!\ Q, R \in A[X]$ tales que

$$F = GQ + R \quad \text{con} \quad \deg(R) < \deg(Q).$$

Por ejemplo, si $F \in A[X]$ y $a \in A$ entonces $R = F(a) \in A \subseteq A[X]$ es el resto de la división de F por $X - a$.

Corolario importante: Sea $F \in A[X]$ con coeficiente líder 1. Entonces, $A[X]/\langle F \rangle$ es un A-módulo libre con base dada por $(\bar{1}, \bar{X}, \bar{X}^2, \ldots, \bar{X}^{\deg(F)-1})$.

Def: Sea $P \in A[X]$, $\alpha \in A$ y $m \in \mathbb{N}^{\geq 1}$. Decimos que α es:
① Una raíz de multiplicidad $\geq m$ de P si $(X-\alpha)^m \mid P$.
② Una raíz de multiplicidad m de P si $(X-\alpha)^m \mid P$ pero $(X-\alpha)^{m+1} \nmid P$.

Prop: Sea A un dominio entero (ie, $\forall a,b \in A$, $ab = 0 \Rightarrow a = 0$ o $b = 0$), sean $\alpha_1, \dots, \alpha_r \in A$ distintos y $P \in A[X] \setminus \{0\}$. Son equivalentes:
① α_i es raíz de mult. $\geq m_i$ de P para todo $i \in \{1, \dots, r\}$.
② $\prod_{i=1}^{r} (X-\alpha_i)^{m_i} \mid P$.
En tal caso, $\sum_{i=1}^{r} m_i \leq \deg(P)$.

Un objetivo de la teoría de cuerpos es escribir polinomios como producto de raíces.

Def: Sea A un dominio entero y $P \in A[X]$. Decimos que P escinde (split) si $P = 0$ o si $P = u(X-\alpha_1)\cdots(X-\alpha_d)$ con $u \in A \setminus \{0\}$ y $\alpha_1, \dots, \alpha_d \in A$.

Obs útil: Un cálculo directo muestra que para todos $\alpha_1, \dots, \alpha_d \in A$ se tiene
$$\prod_{i=1}^{d} (X-\alpha_i) = \sum_{i=0}^{d} (-1)^i \sigma_i(\alpha_1, \dots, \alpha_d) X^{d-i} \quad \text{con } \sigma_i(x_1, \dots, x_d) := \sum_{1 \leq j_1 < \dots < j_i \leq d} \prod_{k=1}^{i} x_{j_k} \text{ y } \sigma_0 \equiv 1$$

Def: Un cuerpo $\mathbb{K}$ es algebraicamente cerrado si:
① Todo $P \in \mathbb{K}[X]$ de $\deg(P) \geq 1$ tiene una raíz en $\mathbb{K}$.
$\Updownarrow$
② Todo $P \in \mathbb{K}[X]$ escinde.
$\Updownarrow$
③ Los polinomios irreducibles de $\mathbb{K}[X]$ son aquellos de grado 1.

Ejemplo: $\mathbb{R}$ no es alg. cerrado, pero $\mathbb{C}$ sí lo es.

§2. Clausura integral

Sea M un A-módulo. Decimos que M es:
① Fiel si $\mathrm{Ann}(M) := \{a \in A \mid am = 0 \ \forall m \in M\}$ es $\{0\}$.
② Finitamente generado si $M = \langle X \rangle_{A\text{-mod}}$ con $X = \{m_1, \dots, m_r\} \subseteq M$ conj. finito
$\iff \exists r \in \mathbb{N}$ y $A^r \twoheadrightarrow M$ sobreyectivo y A-lineal.

$\boxed{\text{Ejercicio}}$ Probar que un A-álgebra B es fiel $\iff \rho_B : A \hookrightarrow B$ es inyectivo.

Teorema: Sea B una A-álgebra y sea $\alpha \in B$. Son equivalentes:
① Existe $P = X^n + \sum_{i=0}^{n-1} a_i X^i$ polinomio mónico en $A[X]$ tal que $P(\alpha) = 0$.
② La subálgebra $A[\alpha] \subseteq B$ es un A-módulo finitamente generado.
③ Existe $C \subseteq B$ subálgebra tq $\alpha \in C$ y tq C es un A-módulo fin. generado.
④ Existe un $A[\alpha]$-módulo fiel M tal que, visto como A-módulo, es fin. generado.
Si estas condiciones se cumplen, decimos que $\alpha \in B$ es entero sobre A.

Obs: Si B es una A-álgebra conmutativa (eg. $B = A[\alpha]$) y M un B-módulo, entonces M es un A-módulo vía $A \times M \longrightarrow M$, $(a,m) \longmapsto a \cdot m := \rho_B(a)m$.

Dem: ① ⇒ ② Sea $ev_\alpha : A[X] \to B$, $F \mapsto F(\alpha)$ morfismos de A-álgebras con $\mathrm{Im}(ev_\alpha) \overset{\text{def}}{=} A[\alpha]$. Como $P \in \ker(ev_\alpha)$, $\exists!\ \overline{ev}_\alpha : A[X]/\langle P\rangle \twoheadrightarrow A[\alpha]$ inducido. Como P tiene coef. líder 1, $A^n \xrightarrow{\sim} A[X]/\langle P\rangle$, $(a_0,\dots,a_{n-1}) \mapsto \sum_{i=0}^{n-1} a_i \overline{X}^i$ es un isomorfismo. Luego, $\exists\ A^n \twoheadrightarrow A[\alpha]$ sobreyectivo ✓ ② ⇒ ③ : $C := A[\alpha]$ ✓
③ ⇒ ④ : $M = C$ es un $A[\alpha]$-módulo fiel ✓ Veamos ④ ⇒ ① :
Sea M un $A[\alpha]$-módulo fiel tq M es A-mód. fin. generado por $\{e_1,\dots,e_m\}$.
Como $\alpha e_j \in M$ para todo j, podemos escribir

$$(*) \begin{cases} \alpha e_1 = a_{11} e_1 + \dots + a_{1m} e_m \\ \vdots \\ \alpha e_m = a_{m1} e_1 + \dots + a_{mm} e_m \end{cases} \qquad \text{con } N := (a_{ij}) \in M_m(A)$$

Sea $Q := \alpha I_m - N \in M_m(A[\alpha])$ y $\widetilde{Q} \in M_m(A[\alpha])$ tq $Q\widetilde{Q} = \widetilde{Q}Q = \det(Q) I_m$.
Dada $\mathcal{U} = (u_{ij}) \in M_m(A[\alpha])$, la aplicación $\gamma_{\mathcal{U}} : M^m \to M^m$, $(m_1,\dots,m_m) \mapsto \left(\sum_{j=1}^m u_{ij} m_j\right)_{1\le i\le m}$ verifica $\gamma_{\mathcal{U}V} = \gamma_{\mathcal{U}} \circ \gamma_V$ y $\gamma_{aI_m} = a\, \mathrm{Id}_{M^m}$ para $a \in A[\alpha]$.
⇒ si $d = \det(Q)$ entonces:

$$(de_1,\dots,de_m) = d(e_1,\dots,e_m) = \gamma_{dI_m}(e_1,\dots,e_m) = \gamma_{\widetilde{Q}Q}(e_1,\dots,e_m) = \gamma_{\widetilde{Q}}\big(\overbrace{\gamma_Q(e_1,\dots,e_m)}^{=0 \text{ por } (*)}\big) = 0$$

Así, $(de_1,\dots,de_m) = 0$ y luego $dm = 0$ $\forall m \in M$ ⇒ $d \equiv 0$ (pues M es $A[\alpha]$-mod fiel !). Si $P := \det(X\cdot I_m - N) \in A[X]$ (mónico !), entonces $d = P(\alpha) = 0$ ✓ ■

Ejemplo: ① $\alpha = \sqrt{2} \in \mathbb{R}$ es entero sobre $\mathbb{Z}$, pues $\alpha^2 - 2 = 0$.
② Sea B una A-álgebra tq B es un A-módulo fin. gen. Entonces, todo $\alpha \in B$ es entero sobre A (por la condición ② del Teorema).

Def: Sea B una A-álgebra conmutativa. La clausura integral de A en B está dada por $\widetilde{A} := \{b \in B,\ b \text{ es entero sobre } A\}$.

Obs: ① $\rho_B(A) \subseteq \widetilde{A} \subseteq B$.
② Sea B una A-álg. conmutativa y C una B-álgebra (ie, $A \xrightarrow{\rho_B} B \xrightarrow{\rho_C} C$).
Si $\alpha \in C$ es entero sobre A, entonces α es entero sobre B. (Ejercicio).

Ejercicio importante Sea B una A-álgebra conmutativa. Supongamos que B es un A-módulo fin. generado por $\{e_1,\dots,e_m\}$ y que M es un B-módulo fin. generado por $\{f_1,\dots,f_n\}$. Probar que $\{e_i f_j,\ 1\le i\le m,\ 1\le j\le n\}$ es un conjunto generador de M como A-módulo. ⚠ En part, M es un A-módulo fin. generado !

Lema útil: Sea B una A-alg. conmutativa y sea C una B-álgebra. Sea $\alpha \in C$. Sup. que B es un A-módulo fin. generado y que $\alpha \in C$ es entero sobre B (ie, $B[\alpha]$ es un B-mód. fin. generado). Entonces, $B[\alpha]$ es un A-módulo fin. generado y luego $\alpha \in C$ es entero sobre A.

Dem: El Ejercicio anterior, aplicado a $M = B[\alpha]$, implica que $B[\alpha]$ es un A-módulo fin. generado (y luego $A[\alpha]$ también, ie, α es entero sobre A). ■

Prop: Sea B una A-álgebra conmutativa y $\tilde{A} \subseteq B$ la clausura integral de A en B. Entonces, $\tilde{A}$ es una subálgebra de B.

Dem: $\rho_B(A) \subseteq \tilde{A}$ (pues $a \in A$ es raíz de $P = X - a$). Sean $\alpha, \beta \in \tilde{A}$. Como β es entero sobre A, también es entero sobre $A[\alpha]$. Luego, el Lema útil implica que $A[\alpha][\beta] \overset{def}{=} A[\alpha,\beta]$ es un A-módulo fin. generado. Dado que $\alpha \pm \beta$, $\alpha\beta \in A[\alpha,\beta]$ tenemos, por el ítem ③ del Teorema, que son enteros sobre A y luego $\tilde{A} \subseteq B$ es una subalgebra. ■

$\boxed{\text{Ejercicio}}$ Encontrar $P \in \mathbb{Z}[X]$ mónico tal que $P(\sqrt{2}+\sqrt{3}) = 0$.

Obs: La misma prueba anterior muestra que si $\alpha_1, \dots, \alpha_m \in \tilde{A}$ entonces el A-módulo $A[\alpha_1, \dots, \alpha_m] \subseteq B$ es finitamente generado.

$\boxed{\text{Ejercicio importante}}$ Probar que $\tilde{\tilde{A}} = \tilde{A}$, ie, si $\alpha \in B$ es entero sobre $\tilde{A}$ entonces necesariamente $\alpha \in \tilde{A}$.

Def: Sea A un dominio entero y $\mathbb{K} = Fr(A)$ su cuerpo de fracciones. Decimos que A es <u>integralmente cerrado</u> si la clausura integral de A en $\mathbb{K}$ coincide con A, ie, $\tilde{A} = A \subseteq \mathbb{K}$.

Prop (Gauss): Sea A un dominio de factorización única. Entonces, A es integralmente cerrado.

Dem: Sea $x \in \mathbb{K} = Fr(A)$ entero sobre A, ie, $\exists\, P = X^n + \sum_{i=0}^{n-1} a_i X^i \in A[X]$ tq $P(x) = 0$ y veamos que $x \in A$:
Si $x = p/q$ con $p \in A$, $q \in A \setminus \{0\}$ y $mcd(p,q) = 1$ entonces $P(x) = 0$ equivale a $p^n + a_{n-1} q p^{n-1} + \dots + a_0 q^n = 0 \Rightarrow q \mid p^n$ y luego $q \mid 1$ (pues $mcd(q, p^n) = 1$) ie, $q \in A^\times$. Así, $x = pq^{-1} \in A$ ✓ ■

Ejemplo: ① $\mathbb{Z}$ es integralmente cerrado, donde $\mathbb{K} = Fr(\mathbb{Z}) \overset{def}{=} \mathbb{Q}$.
② $\mathbb{Z}[i\sqrt{3}]$ <u>no</u> es dominio de factorización única, pues <u>no</u> es integralmente cerrado: $\mathbb{Z}[i\sqrt{3}] \subsetneq \mathbb{Z}\left[\frac{1+i\sqrt{3}}{2}\right]$ donde $j := \frac{1+i\sqrt{3}}{2}$ cumple $j^2 + j + 1 = 0$.

§3. <u>Extensiones de cuerpos y Anillos de enteros</u>

En esta sección, denotamos por $\mathbb{K}$ un cuerpo arbitrario.

Def: Sea B una $\mathbb{K}$-álgebra y $\alpha \in B$ entero sobre $\mathbb{K}$. Consideremos
$$ev_\alpha : \mathbb{K}[X] \to B, \quad P \mapsto P(\alpha)$$
El único generador de $\ker(ev_\alpha)$ con coef. líder 1 es llamado el <u>polinomio minimal</u> de α, y se denota $\mu_\alpha^{\mathbb{K}}$ o bien μ_α.

Obs: ① Si $P \in \mathbb{K}[X]$ es tq $P(\alpha) = 0$, entonces P es múltiplo de μ_α.
② μ_α es el polinomio minimal de la aplicación $\mathbb{K}$-lineal $m_\alpha : B \to B$, $x \mapsto \alpha x$.

En efecto, si $P \in \mathbb{K}[X]$ entonces $P(m_\alpha) = m_{P(\alpha)}$.

Terminología (Teoría de cuerpos)

① Una extensión de $\mathbb{K}$ es una $\mathbb{K}$-álgebra $\rho_{\mathbb{L}} : \mathbb{K} \hookrightarrow \mathbb{L}$ con $\mathbb{L}$ un cuerpo. En tal caso, escribimos $\mathbb{L}/\mathbb{K}$.

② Sea $\mathbb{L}/\mathbb{K}$ extensión de cuerpos. Decimos que $\alpha \in \mathbb{L}$ es algebraico sobre $\mathbb{K}$ si es entero $/\mathbb{K}$, en caso contrario decimos que es trascendente. Decimos que $\mathbb{L}/\mathbb{K}$ es una extensión algebraica si todo $\alpha \in \mathbb{L}$ es algebraico$/\mathbb{K}$.

③ El grado de la extensión de cuerpos $\mathbb{L}/\mathbb{K}$ es $[\mathbb{L}:\mathbb{K}] := \dim_{\mathbb{K}}(\mathbb{L})$. Decimos que $\mathbb{L}/\mathbb{K}$ es una extensión finita si $[\mathbb{L}:\mathbb{K}] < +\infty$.

Observación / Ejercicio: Lo discutido en secciones anteriores implica:

① $\mathbb{L}/\mathbb{K}$ finita $\Rightarrow$ $\mathbb{L}/\mathbb{K}$ algebraica.

② Si $\mathbb{M}/\mathbb{L}/\mathbb{K}$ entonces $[\mathbb{M}:\mathbb{K}] = [\mathbb{M}:\mathbb{L}][\mathbb{L}:\mathbb{K}]$.

③ Si $\alpha \in \mathbb{L}/\mathbb{K}$ algebraico sobre $\mathbb{K}$, entonces $\mu_\alpha^{\mathbb{K}} \in \mathbb{K}[X]$ irreducible y además $\mathbb{K}[X]/\langle \mu_\alpha^{\mathbb{K}} \rangle \xrightarrow{\sim} \mathbb{K}[\alpha] =: \mathbb{K}(\alpha)$. En part, $[\mathbb{K}(\alpha):\mathbb{K}] = \deg(\mu_\alpha^{\mathbb{K}})$.

Hecho (Steinitz, 1910): Sea $\mathbb{K}$ un cuerpo. Entonces, $\exists\, \Omega/\mathbb{K}$ extensión con Ω alg. cerrado. Más aún, si Ω_1 y Ω_2 son dos de estas extensiones entonces existe $\Omega_1 \xrightarrow{\sim} \Omega_2$ isom. de $\mathbb{K}$-álgebras. Decimos que Ω es una clausura algebraica de $\mathbb{K}$.

Ej: $\overline{\mathbb{Q}} := \{\alpha \in \mathbb{C},\ \alpha$ algebraico sobre $\mathbb{Q}\}$ es una clausura algebraica de $\mathbb{Q}$.

Def: Sea $\mathbb{L}/\mathbb{K}$ extensión finita y $\alpha \in \mathbb{L}$. Sea $m_\alpha : \mathbb{L} \to \mathbb{L}$, $x \mapsto \alpha x$ $\mathbb{K}$-lineal, y definamos $\chi_\alpha^{\mathbb{K}} := \chi_{m_\alpha}$ (pol. característico), $\mathrm{Tr}_{\mathbb{L}/\mathbb{K}}(\alpha) := \mathrm{Tr}(m_\alpha)$, $N_{\mathbb{L}/\mathbb{K}}(\alpha) := \det(m_\alpha)$.

"norma"

Obs: ① $\mathrm{Tr}_{\mathbb{L}/\mathbb{K}} : \mathbb{L} \to \mathbb{K}$ es $\mathbb{K}$-lineal.

② $N_{\mathbb{L}/\mathbb{K}}(\alpha\beta) = N_{\mathbb{L}/\mathbb{K}}(\alpha) N_{\mathbb{L}/\mathbb{K}}(\beta)$ $\forall \alpha, \beta \in \mathbb{L}$ y $N_{\mathbb{L}/\mathbb{K}}(a) = a^{[\mathbb{L}:\mathbb{K}]}$ si $a \in \mathbb{K}$.

La siguiente es una de las definiciones más importantes del curso!

Def: Un cuerpo de números $\mathbb{K}$ es una extensión finita de $\mathbb{Q}$. En tal caso, el anillo de enteros de $\mathbb{K}$ es la clausura integral $\mathcal{O}_{\mathbb{K}} := \widetilde{\mathbb{Z}}$ de $\mathbb{Z}$ en $\mathbb{K}$.

Prop: Sea $A \subseteq \mathbb{K} = \mathrm{Fr}(A)$ un dominio entero integralmente cerrado, sea $\mathbb{L}/\mathbb{K}$ extensión finita, y sea $\alpha \in \mathbb{L}$ entero sobre A. Entonces:

① $\chi_\alpha^{\mathbb{K}} \in A[X]$ y $\mu_\alpha^{\mathbb{K}} \in A[X]$.

② $\mathrm{Tr}_{\mathbb{L}/\mathbb{K}}(\alpha) \in A$ y $N_{\mathbb{L}/\mathbb{K}}(\alpha) \in A$.

Dem: Sea $\Omega/\mathbb{L}$ extensión con Ω alg. cerrado, y escribamos $\mu_\alpha^{\mathbb{K}} = \prod_{i=1}^{d}(X - \alpha_i)$ en $\Omega[X]$. Sea $P = X^n + \sum_{i=0}^{n-1} a_i X^i \in A[X]$ tq $P(\alpha) = 0$. Luego, $\mu_\alpha^{\mathbb{K}} \mid P$ en $\mathbb{K}[X]$ y en particular $\alpha_1, \dots, \alpha_d \in \Omega$ son enteros sobre A. Por otra parte:

$$\mu_\alpha^{\mathbb{K}} = \prod_{i=1}^{d}(X - \alpha_i) = X^d + \sum_{i=1}^{d} \underbrace{(-1)^i \sigma_i(\alpha_1, \dots, \alpha_d)}_{\text{enteros sobre } A} X^{d-i} \Rightarrow \mu_\alpha^{\mathbb{K}} \in \mathbb{K}[X] \text{ tiene coeficientes}$$

enteros sobre A $\underset{\tilde{A} = A \text{ en } \mathbb{K}}{\Rightarrow}$ $\mu_\alpha^{\mathbb{K}} \in A[X]$.

Por Álgebra Lineal (Cayley - Hamilton): $\mu_\alpha^{\mathbb{K}} \mid \chi_\alpha^{\mathbb{K}} \mid (\mu_\alpha^{\mathbb{K}})^{[\mathbb{L}:\mathbb{K}]}$ con $[\mathbb{L}:\mathbb{K}] = \dim_{\mathbb{K}} \mathbb{L}$.
Como $\mu_\alpha^{\mathbb{K}}, \chi_\alpha^{\mathbb{K}} \in \mathbb{K}[X]$ tienen coef. líder 1 y $\mu_\alpha^{\mathbb{K}}$ es irreducible, entonces necesariamente $\chi_\alpha^{\mathbb{K}} = (\mu_\alpha^{\mathbb{K}})^r$ para cierto $r \in \{1, \dots, d\} \Rightarrow \chi_\alpha^{\mathbb{K}} \in A[X]$ ✓
En part, $\chi_\alpha^{\mathbb{K}} \overset{\text{def}}{=} \det(XI_d - m_\alpha) = X^d - \mathrm{Tr}_{\mathbb{L}/\mathbb{K}}(\alpha) X^{d-1} + \dots + (-1)^d N_{\mathbb{L}/\mathbb{K}}(\alpha) \in A[X]$. ■

Observaciones útiles: Con la notación anterior, tenemos que:

① $\deg(\chi_\alpha^{\mathbb{K}}) = [\mathbb{L}:\mathbb{K}]$ y $\deg(\mu_\alpha^{\mathbb{K}}) = [\mathbb{K}(\alpha):\mathbb{K}]$. Luego, $\boxed{\chi_\alpha^{\mathbb{K}} = (\mu_\alpha^{\mathbb{K}})^{[\mathbb{L}:\mathbb{K}(\alpha)]}}$

② Si $\alpha_1, \dots, \alpha_d \in \Omega$ (alg. cerrado) son las raíces de $\mu_\alpha^{\mathbb{K}}$ contadas con multipl. entonces $\mathrm{Tr}_{\mathbb{L}/\mathbb{K}}(\alpha) = [\mathbb{L}:\mathbb{K}(\alpha)] \sum_{i=1}^{d} \alpha_i$ y $N_{\mathbb{L}/\mathbb{K}}(\alpha) = \left(\prod_{i=1}^{d} \alpha_i\right)^{[\mathbb{L}:\mathbb{K}(\alpha)]}$ en Ω.

Ejemplo: Si $\mathbb{L}/\mathbb{K}$ es una extensión cuadrática, ie, $[\mathbb{L}:\mathbb{K}] = 2$, con $\mathbb{K} = \mathrm{Fr}(A)$ tal que A integralmente cerrado, entonces:

$$\alpha \in \mathbb{L} \text{ es entero sobre } A \iff \mathrm{Tr}_{\mathbb{L}/\mathbb{K}}(\alpha) \in A \text{ y } N_{\mathbb{L}/\mathbb{K}}(\alpha) \in A$$

$\chi_\alpha^{\mathbb{K}}(\alpha) = 0$

En efecto, si $\mathrm{Tr}_{\mathbb{L}/\mathbb{K}}(\alpha), N_{\mathbb{L}/\mathbb{K}}(\alpha) \in A \Rightarrow \chi_\alpha^{\mathbb{K}} = X^2 - \mathrm{Tr}_{\mathbb{L}/\mathbb{K}}(\alpha) X + N_{\mathbb{L}/\mathbb{K}}(\alpha) \in A[X]$

Lema útil: Sea $A \subseteq \mathbb{K} = \mathrm{Fr}(A)$ dominio entero y $\mathbb{L}/\mathbb{K}$ extensión finita. Entonces, para todo $\alpha \in \mathbb{L}$, $\exists\, q \in A \setminus \{0\}$ tal que $q\alpha$ es entero sobre A.

Dem: Sea $P = \mu_\alpha^{\mathbb{K}} = X^d + \sum_{i=0}^{d-1} c_i X^i \in \mathbb{K}[X]$ con $c_i = \frac{a_i}{q}$ con $a_i \in A, q \in A \setminus \{0\}$.
Así, $q^d P(\alpha) = 0 \iff (q\alpha)^d + \sum_{i=0}^{d-1} b_i (q\alpha)^i = 0$ con $b_i = a_i q^{d-1-i} \in A$ ✓ ■

⚠ Consecuencia: Sea $A \subseteq \mathbb{K} = \mathrm{Fr}(A)$ dom. entero, $\mathbb{L}/\mathbb{K}$ extensión finita y $B := \widetilde{A} \subseteq \mathbb{L}$ la clausura integral de A en $\mathbb{L}$. Entonces, $\mathbb{L} = \mathrm{Fr}(B)$ pues todo $\alpha \in \mathbb{L}$ se escribe como $\alpha = b/a$ con $b \in B$ y $a \in A \setminus \{0\}$.
En particular, si $\mathbb{K}/\mathbb{Q}$ cuerpo de números entonces $\mathbb{K} = \mathrm{Fr}(\mathcal{O}_{\mathbb{K}})$.

Def: Sea $A \subseteq \mathbb{K} = \mathrm{Fr}(A)$ dominio entero. Un ideal fraccionario de $\mathbb{K}$ (resp. a A) es un A-submódulo $I \subseteq \mathbb{K}$ tal que $\exists\, c \in A \setminus \{0\}$ tal que $cI \subseteq A$.

Ejemplos: ① $\frac{1}{3}\mathbb{Z} = \{\frac{a}{3}, a \in \mathbb{Z}\} \subseteq \mathbb{Q}$ es un ideal fraccionario de $\mathbb{Q}$ (resp. a $\mathbb{Z}$).
② Si $\alpha \in \mathbb{K}$ entonces $\langle \alpha \rangle := \langle \alpha \rangle_{A\text{-mód}} \subseteq \mathbb{K}$ es un ideal fraccionario, pues si $q \in A$ es tal que $q\alpha \in A$ entonces $q\langle \alpha \rangle = \langle q\alpha \rangle \subseteq A$ (ideal usual!).
Diremos que estos ideales fraccionarios son ideales fraccionarios principales.
Ejercicio: Probar que todo ideal fraccionario de $\mathbb{Q}$ es principal.
③ Todo ideal (usual) de A es un ideal fraccionario de $\mathbb{K}$.

Recuerdo de Álgebra Lineal: Sea $\mathbb{K}$ un cuerpo y $V \cong \mathbb{K}^d$ un $\mathbb{K}$-esp. vectorial. Sea $B: V \times V \to \mathbb{K}$ una forma bilineal simétrica en V. Si $\mathcal{B} = \{e_1, \dots, e_d\}$ base de V y $M_{\mathcal{B}} := (B(e_i, e_j))_{1 \le i,j \le d}$ es la matriz de B resp. a la base $\mathcal{B}$
$\Rightarrow \det(M_{\mathcal{B}'}) = \det(P)^2 \det(M_{\mathcal{B}})$ con $P = \mathrm{Mat}_{\mathcal{B}}(\mathcal{B}')$ y $\mathcal{B}'$ otra base de V.
Conclusión: $\mathrm{disc}(B) := \det(B(e_i, e_j)_{1 \le i,j \le d}) \in \mathbb{K}/\mathbb{K}^{*2}$ es indep. de la base $\mathcal{B}$ y se llama el discriminante de la forma bilineal simétrica B.

Def: Sea $A \subseteq \mathbb{K} = \mathrm{Fr}(A)$ dom. entero y $\mathbb{L}/\mathbb{K}$ ext. finita de $[\mathbb{L}:\mathbb{K}] = d$. Sea $B := \tilde{A} \subseteq \mathbb{L}$ clausura integral de A y sea $I \subseteq \mathbb{L} = \mathrm{Fr}(B)$ ideal fraccionario (resp. a B). Definimos el discriminante de I como

$$D_{B/A}(I) := \langle \det((\mathrm{Tr}_{\mathbb{L}/\mathbb{K}}(e_i e_j))_{1\le i,j\le d}),\ (e_1,\dots,e_d) \in I^d \rangle_{A\text{-mod}} \subseteq \mathbb{K}.$$

En part, definimos $d_{B/A} := D_{B/A}(B) \subseteq A$ (ideal).

Prop: $D_{B/A}(I) \subseteq \mathbb{K}$ es un ideal fraccionario resp. a A, con A integralmente cerrado.

Dem: Sea $\mathcal{B} = (e_1,\dots,e_d) \in \mathbb{L}^d$, $M_{\mathcal{B}} := (\mathrm{Tr}_{\mathbb{L}/\mathbb{K}}(e_i e_j))_{1\le i,j\le d}$ y $P = (a_{ij}) \in M_d(\mathbb{K})$. Si $\mathcal{B}' = (f_1,\dots,f_d)$ con $f_j = \sum_{i=1}^{d} a_{ij} e_i$ entonces $\det(M_{\mathcal{B}'}) = \det(P)^2 \det(M_{\mathcal{B}})$. En part, si $\mathcal{B}$ es base de $\mathbb{L}$ y $P = \mathrm{Mat}_{\mathcal{B}}(m_\alpha)$ entonces $\det(P) \overset{\text{def}}{=} N_{\mathbb{L}/\mathbb{K}}(\alpha)$.
Sea $\alpha \in B\setminus\{0\}$ tal que $\alpha I \subseteq B$, entonces toda d-tupla $\mathcal{B} = (e_1,\dots,e_d) \in I^d$ cumple $N_{\mathbb{L}/\mathbb{K}}(\alpha)^2 \det(M_{\mathcal{B}}) = \det(M_{(\alpha e_1,\dots,\alpha e_d)}) \in A$ pues $\alpha e_j \in B$ y $\mathrm{Tr}_{\mathbb{L}/\mathbb{K}}(B) \underset{\uparrow}{\subseteq} A$.
A int. cerrado
Así, $N_{\mathbb{L}/\mathbb{K}}(\alpha)^2 D_{B/A}(I) \subseteq A$ con $N_{\mathbb{L}/\mathbb{K}}(\alpha) \in A$ ✓ ■

Obs útil: Lo anterior muestra que si $I \subseteq \mathbb{L}$ ideal fraccionario y $\alpha \in \mathbb{L}$ entonces se tiene que $D_{B/A}(\alpha I) = N_{\mathbb{L}/\mathbb{K}}(\alpha)^2 D_{B/A}(I)$.

Def: Sea $\mathbb{K}$ un cuerpo de números. El discriminante de $\mathbb{K}$ es el entero $d_{\mathbb{K}} \in \mathbb{N}$ tal que $d_{\mathcal{O}_{\mathbb{K}}/\mathbb{Z}} = \langle d_{\mathbb{K}} \rangle \subseteq \mathbb{Z}$.

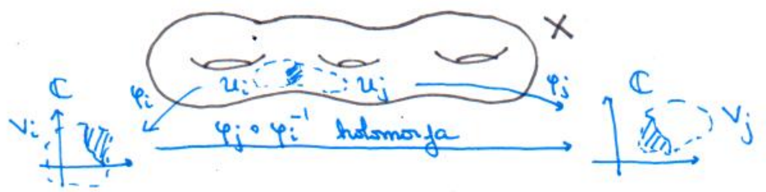
⚠ Concretamente: Si $(e_1,\dots,e_d)$ es una base (sobre $\mathbb{Z}$) del $\mathbb{Z}$-módulo $\mathcal{O}_{\mathbb{K}}$, entonces $d_{\mathbb{K}} = |\det((\mathrm{Tr}_{\mathbb{K}/\mathbb{Q}}(e_i e_j))_{1\le i,j\le d})|$.

Ejercicio* Calcular $d_{\mathbb{K}}$ para $\mathbb{K} = \mathbb{Q}(\sqrt{d})$ con $d \in \mathbb{Z}$ libre de cuadrados (cf. P. Samuel §2.5).

§4. Teoría de Galois geométrica

Esta sección es un interludio de Geometría Compleja, que busca motivar fenómenos que se replican en Teoría Algebraica de Números.

Def: Sea X un esp. topológico de Hausdorff. Un atlas complejo en X está dado por:
1. Un cubrimiento abierto $\{\mathcal{U}_i\}_{i\in I}$ de X.
2. Homeomorfismos $\{\varphi_i : \mathcal{U}_i \subseteq X \xrightarrow{\sim} V_i \subseteq \mathbb{C}\}_{i\in I}$ con $V_i \subseteq \mathbb{C}$ abiertos y tales que el "cambio de cartas" $\varphi_j \circ \varphi_i^{-1} : \varphi_i(\mathcal{U}_i \cap \mathcal{U}_j) \xrightarrow{\sim} \varphi_j(\mathcal{U}_i \cap \mathcal{U}_j)$ es holomorfo.



Obs: Dos atlas $\mathcal{A} = \{(\mathcal{U}_i, \varphi_i)\}_{i\in I}$, $\mathcal{A}' = \{(\mathcal{U}'_j, \varphi'_j)\}_{j\in J}$ son equivalentes si su unión es un atlas complejo. Lo anterior es una relación de equivalencia.

Def: Una superficie de Riemann es un espacio topológico de Hausdorff X dotado de (la clase de equivalencia de) un atlas complejo.

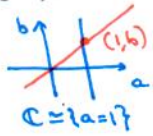
Obs (Geo. diferencial): Toda sup. de Riemann es orientable (Ec. de Cauchy-Riemann). Luego, si X es compacto entonces es difeomorfa a S^2 o suma conexa de $g \geq 1$ toros.

<u>Ejemplos</u>: ⓪ Todo abierto de una sup. de Riemann es una sup. de Riemann.

① <u>Esfera de Riemann</u>: $\mathbb{P}^1(\mathbb{C}) := \{\text{Rectas } 0 \in l = \langle (a,b) \rangle_{\mathbb{C}} =: [a,b] \text{ en } \mathbb{C}^2\}$.

La proyección $\pi : \mathbb{C}^2 \setminus \{(0,0)\} \to \mathbb{P}^1(\mathbb{C})$, $(a,b) \mapsto [a,b]$ induce una topología ✓

Sea $\mathcal{U}_1 := \{[a,b] \in \mathbb{P}^1(\mathbb{C}), a \neq 0\}$ y $\varphi_1 : \mathcal{U}_1 \xrightarrow{\sim} \mathbb{C}$, $[a,b] \mapsto \frac{b}{a}$ homeo.



con inversa $\varphi_1^{-1}(z) = [1, z]$.

Similar: $\mathcal{U}_2 = \{[a,b] \in \mathbb{P}^1(\mathbb{C}), b \neq 0\} \xrightarrow{\sim} \mathbb{C}$, $[a,b] \mapsto \frac{a}{b}$ $\rightsquigarrow \mathbb{P}^1(\mathbb{C})$ sup. de Riemann

<u>Convención</u>: Denotamos $\mathbb{C} := \varphi_1(\mathcal{U}_1)$ y $\infty := [0,1]$. Así, $\mathbb{P}^1(\mathbb{C}) = \mathbb{C} \cup \{\infty\}$.

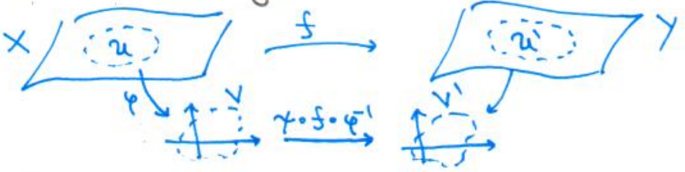
$\boxed{\text{Ejercicio}}$ Probar que $\varphi_2 \circ \varphi_1^{-1}$ está dada por $z \mapsto \frac{1}{z}$.

② <u>Toros complejos</u>: Sean $\omega_1, \omega_2 \in \mathbb{C}$ l.i./$\mathbb{R}$ y $\Lambda := \mathbb{Z}\omega_1 + \mathbb{Z}\omega_2 \simeq \mathbb{Z}^2 \subseteq \mathbb{C}$

Entonces, $\mathbb{T} := \mathbb{C}/\Lambda$ sup. de Riemann.

<u>Obs</u> (cartas): Si $\rho = \frac{1}{2}\min\{|\lambda|, \lambda \in \Lambda \setminus \{0\}\}$ y $z \in \mathbb{C}$, $\pi_z := \pi|_{D(z,\rho)} : D(z,\rho) \to \mathcal{U}_z = \pi(D(z,\rho))$ es biyectiva y $\varphi_z := \pi_z^{-1} : \mathcal{U}_z \xrightarrow{\sim} D(z,\rho) \subseteq \mathbb{C}$ carta, con $\varphi_{z_1} \circ \varphi_{z_2}^{-1}(s) = s + \omega$, cierto $\omega \in \Lambda$.

<u>Def</u>: Sean X e Y sup. de Riemann. Una función continua $f : X \to Y$ es un <u>morfismo regular</u> si para todo par de cartas $\varphi : \mathcal{U} \subseteq X \xrightarrow{\sim} V \subseteq \mathbb{C}$, $\psi : \mathcal{U}' \subseteq Y \xrightarrow{\sim} V' \subseteq \mathbb{C}$ la función $\psi \circ f \circ \varphi^{-1}$ es <u>holomorfa</u>:



Si $Y = \mathbb{C}$, decimos que $f : X \to \mathbb{C}$ es una <u>función holomorfa</u>. Si $Y = \mathbb{P}^1(\mathbb{C}) = \mathbb{C} \cup \{\infty\}$ y si $f(\mathcal{U}) \neq \{\infty\}$ para toda $\mathcal{U} \subseteq X$ componente conexa, decimos que $f : X \to \mathbb{P}^1(\mathbb{C})$ es una <u>función meromorfa</u> y definimos $\mathbb{C}(X) := \{f : X \to \mathbb{P}^1(\mathbb{C}) \text{ meromorfa}\}$.

<u>Ejemplos</u>:

① Si $P/Q \in \mathbb{C}(T) \overset{\text{def}}{=} \mathrm{Fr}(\mathbb{C}[T])$ con $P, Q \in \mathbb{C}[T]$ ($\mathrm{mcd}(P,Q) = 1$) entonces la función

$P/Q : \mathbb{P}^1(\mathbb{C}) \longrightarrow \mathbb{P}^1(\mathbb{C})$, $[1:z] \mapsto [Q(z), P(z)]$ es regular.

Por ejemplo, si $P = T^m$ y $Q = 1$, obtenemos $f : \mathbb{P}^1(\mathbb{C}) \to \mathbb{P}^1(\mathbb{C})$, $[a,b] \mapsto [a^m, b^m]$.

<u>Hecho</u>: $\mathbb{C}(\mathbb{P}^1(\mathbb{C})) \cong \mathbb{C}(T)$.

② Sean $\omega_1, \omega_2 \in \mathbb{C}$ l.i./$\mathbb{R}$, $\Lambda = \mathbb{Z}\omega_1 + \mathbb{Z}\omega_2$ y $\mathbb{T} := \mathbb{C}/\Lambda$. Se define la <u>función $\wp$ de Weierstrass</u> mediante

$$\wp(z) := \frac{1}{z^2} + \sum_{\omega \in \Lambda \setminus \{0\}} \left(\frac{1}{(z-\omega)^2} - \frac{1}{\omega^2} \right) \quad \text{para } z \in \mathbb{C}.$$

Dicha función converge uniformemente en compactos de $\mathbb{C} - \Lambda$, y cumple:

i) $\wp(-z) = \wp(z)$ $\forall z \in \mathbb{C} - \Lambda$.

ii) $\wp$ es Λ-periódica, ie, $\wp(z+\lambda) = \wp(z)$ para todo $\lambda \in \Lambda$ y $z \in \mathbb{C} - \Lambda$:

Como $\wp'(z) = -2 \sum_{\omega \in \Lambda \setminus \{0\}} \frac{1}{(z-\omega)^3} \overset{\text{def}}{=} \wp'(z+\lambda)$, $z \mapsto \wp(z+\lambda) - \wp(z)$ es constante.

Si $z = -\frac{\omega_1}{2}$ y $\lambda = \omega_1$: $\wp\left(-\frac{\omega_1}{2} + \omega_1\right) - \wp\left(-\frac{\omega_1}{2}\right) = 0$ por (i). Similar para $\lambda = \omega_2$

$\Rightarrow \wp(z+\lambda) = \wp(z)$ para $\lambda = n\omega_1 + m\omega_2 \in \Lambda$ arbitrario ✓

Así, $\wp$ induce $\wp : \mathbb{T} \to \mathbb{P}^1(\mathbb{C})$, $[z] \mapsto [1 : \wp(z)]$ si $z \notin \Lambda$ y $[0] \mapsto \infty$ holom.

<u>Hecho</u>: $\mathbb{C}(\mathbb{T}) = \mathbb{C}(\wp, \wp')$, donde $\wp' \notin \mathbb{C}(\wp)$ por paridad ! Así, $[\mathbb{C}(\mathbb{T}) : \mathbb{C}(\wp)] > 1$.

De hecho, derivando $\wp$ se verifica que

$$(\wp')^2 - 4\wp^3 + 60\, G_4(\Lambda)\wp + 140\, G_6(\Lambda) = 0 \quad \text{con } G_m(\Lambda) := \sum_{\omega \in \Lambda \setminus \{0\}} \frac{1}{\omega^m} \quad \left(\text{series de Eisenstein}\right)$$

ie, $\mathbb{C}(T)[Y] / \langle Y^2 - 4T^3 + 60 G_4(\Lambda) T + 140\, G_6(\Lambda) \rangle \xrightarrow{\sim} \mathbb{C}(\mathbb{T})$; $T \mapsto \wp$, $Y \mapsto \wp'$.

<u>Obs</u>: De manera más general, si X e Y son sup. de Riemann <u>conexas</u> y $f : X \to Y$ función regular no-constante, entonces:

1. $\mathbb{C}(X)$ es un cuerpo.
2. $f^* : \mathbb{C}(Y) \hookrightarrow \mathbb{C}(X)$, $g \mapsto g \circ f$ extensión de cuerpos !.

Usando Análisis Complejo, podemos describir morfismos regulares <u>localmente</u>:

<u>Prop</u>: Sea $f : X \to Y$ morfismo regular entre sup. de Riemann conexas no-constante. Sea $p \in X$ y $q = f(p) \in Y$. Entonces, $\exists$ carta $\varphi : \mathcal{U}_p \xrightarrow{\sim} W \subseteq \mathbb{C}$ (resp. $\psi : V_q \xrightarrow{\sim} W' \subseteq \mathbb{C}$) en torno a p (resp. a q) tales que:

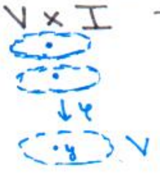
1. $\varphi(p) = 0$, $\psi(q) = 0$ y $f(\mathcal{U}_p) \subseteq V_q$.
2. $\psi \circ f \circ \varphi^{-1} : W \to W'$ está dada por $z \mapsto z^{m_p}$ donde $m_p \in \mathbb{N}^{\geq 1}$ <u>no</u> depende de la elección de dichas cartas locales.

<u>Def</u>: El entero m_p es el <u>índice de ramificación</u> de f en $p \in X$. Si $m_p > 1$ entonces decimos que $p \in X$ es un <u>punto de ramificación</u> de f.

<u>Obs</u>: Localmente f luce como $f(z) = z^m$ y luego $f'(z) = m z^{m-1} \neq 0$ si $z \neq 0$. Así, por Teo. de la función implícita, $m_z = 1$ si $z \neq 0$. Luego, el conjunto de puntos de ramificación $R_f := \{p \in X,\ m_p > 1\}$ es <u>discreto</u>. El mismo argumento muestra que $\forall y \in Y$, la <u>fibra</u> $f^{-1}(y) \subseteq X$ es un conjunto discreto.

<u>Def</u>: Sea $\varphi : X \to Y$ función continua entre esp. topológicos. Decimos que φ es un <u>revestimiento</u> (o que es <u>étale</u>) si $\forall y \in Y$ existe un abierto $y \in V \subseteq Y$ y un conjunto discreto I tal que $\exists$ homeomorfismo $\varphi^{-1}(V) \xrightarrow{\sim} V \times I$ tal que el diagrama

$$\begin{tikzcd} \varphi^{-1}(V) \arrow[rr, "\sim"] \arrow[dr, "\varphi"'] & & V \times I \arrow[dl, "pr_1"] \\ & V & \end{tikzcd}$$



$\mathrm{Card}(\varphi^{-1}(y)) = \mathrm{Card}(I)$

es conmutativo.

<u>Ej</u>: $\exp : \mathbb{C} \to \mathbb{C}^*$ (resp. $z \mapsto z^n$ de $\mathbb{C}^*$ a $\mathbb{C}^*$) es un revestimiento con $I = \mathbb{Z}$ (resp $\{1, .., n\}$).

<u>Recuerdo</u>: Una función continua $f : X \to Y$ entre espacios de Hausdorff es <u>propia</u> si es cerrada (ie, $f(Z) \subseteq Y$ cerrado para todo $Z \subseteq X$ cerrado) y $\forall y \in Y$, $f^{-1}(y) \subseteq X$ compacto. En part, si X es compacto entonces <u>toda</u> f continua es propia.

<u>Prop</u>: Sea $f : X \to Y$ morfismo regular <u>propio</u> entre sup. de Riemann conexas no-constante. Entonces, f es sobreyectivo con fibras <u>finitas</u> y la restricción

$$X \setminus f^{-1}(f(R_f)) \xrightarrow{f} Y \setminus f(R_f)$$

es un revestimiento cuyas fibras tienen <u>todas</u> el mismo cardinal, denotado $\deg(f) \in \mathbb{N}^{\geq 1}$.

Ejemplos: ① $f : \mathbb{P}^1(\mathbb{C}) \to \mathbb{P}^1(\mathbb{C})$, $[x:y] \mapsto [x^n, y^n]$ tiene $R_f = \{[0,1],[1,0]\}$ y $\deg(f) = n$.

② Sea $\mathbb{T} = \mathbb{C}/\Lambda$ con $\Lambda = \mathbb{Z}\omega_1 + \mathbb{Z}\omega_2$ y sea $\wp : \mathbb{T} \to \mathbb{P}^1(\mathbb{C})$, $[z] \mapsto \begin{cases} \infty & \text{si } z \in \Lambda \\ [1:\wp(z)] & \text{sino} \end{cases}$

donde $\wp(z) = \frac{1}{z^2} + \sum_{\lambda \in \Lambda \setminus \{0\}} \left(\frac{1}{(z-\lambda)^2} - \frac{1}{\lambda^2} \right)$ tiene un <u>polo de orden 2</u> en $z = 0$, i.e., $\wp^{-1}(\infty) = \{[0]\}$ con mult. 2. Así, para $u \in \mathbb{C}$ la ecuación $\wp([z]) = [1:u]$ "=" u tiene <u>dos</u> soluciones contando mult. Por paridad de $\wp$ si $[z]$ solución entonces $[-z]$ también (!) Luego, los puntos de ramificación son los $[z] = [-z]$, i.e., $[2z] = [0]$ en $\mathbb{T}$.

$\Rightarrow R_\wp = \{[0], [\frac{\omega_1}{2}], [\frac{\omega_2}{2}], [\frac{\omega_1+\omega_2}{2}]\}$ y $\deg(\wp) = 2$.

(!) Sea $f : X \to Y$ morfismo regular propio entre sup. de Riemann conexas no-constante.

① <u>Álgebra</u>: $f^* : \mathbb{C}(Y) \hookrightarrow \mathbb{C}(X)$, $g \mapsto g \circ f$ extensión de cuerpo de grado $[\mathbb{C}(X) : \mathbb{C}(Y)]$.

② <u>Geometría</u>: f es un revestimiento ramificado de grado $\deg(f)$.

<u>Teorema</u>: Sean X e Y sup. de Riemann <u>compactas</u> y conexas. Si $f : X \to Y$ es un morfismo regular no-constante, entonces $[\mathbb{C}(X) : \mathbb{C}(Y)] = \deg(f)$.

<u>Obs importante</u> (cf. Szamuely "Galois groups and Fundamental groups"): La analogía entre superficies de Riemann y Teoría de cuerpos puede hacerse aún más explícita:

$$\left\{ \begin{array}{l} \text{Superficies de Riemann} \\ \text{compactas conexas} \end{array} \right\} \xrightarrow{\sim} \left\{ \begin{array}{l} \text{Extensiones } \mathbb{L}/\mathbb{C} \text{ tal que } \mathbb{L} \\ \text{isom. a una extensión finita de } \mathbb{C}(T) \end{array} \right\}$$

$$X \longmapsto \mathbb{L} := \mathbb{C}(X)$$

$$(f : X \to Y) \longmapsto f^* : \mathbb{C}(Y) \hookrightarrow \mathbb{C}(X)$$

es una <u>equivalencia de categorías</u> (!).

<u>Eslogan</u>: El cuerpo $\mathbb{C}(X)$ es el cuerpo de fracciones del anillo de funciones holomorfas $\mathcal{O}(X)$. Si $\mathbb{K}/\mathbb{Q}$ cuerpo de números, entonces $\mathcal{O}_{\mathbb{K}}$ "debería lucir como un anillo de funciones".

§5. <u>Los comienzos de la Teoría de Galois</u>

La ecuación general de grado d sobre $\mathbb{C}$, $X^d + a_{d-1}X^{d-1} + \dots + a_1 X + a_0 = 0$ con $a_i \in \mathbb{C}$ puede ser resuelta explícitamente para:

① $d = 2$ (Babilonia, Siglo $\overline{\text{XVIII}}$ A.C.)

② $d = 3$ (Del Ferro, Cardano, Fontana, S. $\overline{\text{XVI}}$).

③ $d = 4$ (Ferrari, 1565).

Sin embargo, para $d \geq 5$ esto es <u>imposible</u> (Abel 1824, Galois 1832).

<u>La idea clave de Galois</u>: Sea $P \in \mathbb{Q}[X]$ y consideremos el conjunto

$$Z(P) := \{\alpha \in \mathbb{C},\ P(\alpha) = 0\},$$

y definamos $\mathbb{K}_P := \mathbb{Q}(Z(P)) \subseteq \mathbb{C}$. El <u>grupo de Galois</u> de P está dado por

$$G_P := \mathrm{Gal}(\mathbb{K}_P/\mathbb{Q}) := \{\sigma : \mathbb{K}_P \xrightarrow{\sim} \mathbb{K}_P \text{ automorfismo de cuerpos tq } \sigma(x) = x\ \forall x \in \mathbb{Q}\}$$

Como $P \in \mathbb{Q}[X]$ tiene coef. en $\mathbb{Q}$, todo $\sigma \in G_P$ cumple $P(\sigma(\alpha)) = \sigma(P(\alpha)) = 0\ \forall \alpha \in Z(P)$.

Así, todo $\sigma \in G_P$ cumple $\sigma(Z(P)) = Z(P)$ y además: "$\sigma|_{Z(P)} = \mathrm{Id}_{Z(P)} \Rightarrow \sigma = \mathrm{Id}_{\mathbb{K}_P}$".

$\Rightarrow \tau : G_P \hookrightarrow S_{\# Z(P)}$ es un morfismo de grupos <u>inyectivo</u>.

Ejemplos: ① $P = X^2+1$ con $Z(P) = \{-i, i\}$ y $\mathbb{K}_P = \mathbb{Q}(i)$ ext. cuadrática imaginaria. Cada $\sigma \in G_P$ está determinado por $\sigma(i) = \pm i$. Así, $\sigma = \mathrm{Id}_{\mathbb{K}_P}$ o $\sigma(a+ib) = a-ib$ conjugación $\Rightarrow G_P \cong \mathbb{Z}/2\mathbb{Z}$.

② Sea $n \in \mathbb{N}^{\geq 1}$ y $P = X^n - 1$, con $Z(P) = \{1, \xi_n, \xi_n^2, \dots, \xi_n^{n-1}\} =: \mu_n(\mathbb{C})$ donde $\xi_n = e^{2\pi i/n}$. Aquí, $\mathbb{K}_P = \mathbb{Q}(\xi_n)$ es el cuerpo ciclotómico (cf. P. SAMUEL §2.9) y cada $\sigma \in G_P$ está determinado por $\sigma(\xi_n) \in \mu_n(\mathbb{C})$: Dado que $\mathrm{ord}(\xi_n) = n$ en $\mathbb{C}^*$ tenemos que $\mathrm{ord}(\sigma(\xi_n)) = n$ y luego $\sigma(\xi_n) = \xi_n^k$ con $k \in \mathbb{Z}$ tq $\mathrm{mcd}(k,n) = 1$.
$\Rightarrow \varphi : (\mathbb{Z}/n\mathbb{Z})^* \hookrightarrow G_P$, $[k] \mapsto (\xi_n \mapsto \xi_n^k)$ es inyectivo. Mejor aún:

$\boxed{\text{Ejercicio}}^*$ (cf. P. Samuel §2.9) Probar que el n-ésimo polinomio ciclotómico

$$\Phi_n(X) = \prod_{\substack{1 \leq k \leq n \\ \mathrm{mcd}(k,n)=1}} (X - \xi_n^k)$$

pertenece a $\mathbb{Z}[X]$ y es irreducible en $\mathbb{Q}[X]$. En part, $\mu_{\xi_n}^{\mathbb{Q}} = \Phi_n$.

Obs: veremos luego que esto implica $|G_P| = |(\mathbb{Z}/n\mathbb{Z})^*|$, ie, φ es un isomorfismo.

③ Sea $P = X^5 - 6X + 3 \in \mathbb{Q}[X]$ irreducible. Analizando la función $P(x)$ se deduce que P tiene 3 raíces reales $x_1 < x_2 < x_3$ y dos complejas $x_4, x_5 = \overline{x_4}$. La extensión $\mathbb{K}_P/\mathbb{Q}$ tiene grupo de Galois $G_P \leq S_5$ y la conjugación $z \mapsto \overline{z}$ actúa como la transposición $(4,5)$. Más adelante veremos que la acción $G_P \curvearrowright Z(P)$ es transitiva y luego $\exists\, \sigma \in G_P$ de orden 5 que (reemplazando σ por σ^m si fuera necesario) envía 4 en 5. Reordenando x_1, x_2, x_3 si fuera necesario, podemos asumir $\sigma = (1,2,3,4,5)$ y luego $G_P \supseteq \langle (1,2,3,4,5), (4,5) \rangle \cong S_5$, ie, $G_P \cong S_5$.

Teorema (Galois): Sea $P \in \mathbb{Q}[X]$. La ecuación $P(X) = 0$ puede ser resuelta (usando radicales) $\Leftrightarrow$ G_P es un grupo soluble, ie, $\exists$ una torre de subgrupos
$\{e\} = G_0 \triangleleft G_1 \triangleleft \dots \triangleleft G_m = G_P$ con $G_i/G_{i-1} \cong \mathbb{Z}/d_i\mathbb{Z}$ grupo cíclico.

Ejemplo: $P = X^5 - 6X + 3$ tiene $G_P \cong S_5$ con $A_5 \ntrianglelefteq S_5$. Dado que A_5 es un grupo simple no-abeliano, $P=0$ no puede resolverse usando radicales!

Problema abierto: Dado G un grupo finito, $\exists\, P \in \mathbb{Q}[X]$ (explícito) tal que $G_P \cong G$? (Problema de Galois inverso).

§6. Extensiones separables

En todo lo que sigue, $\mathbb{K}$ es un cuerpo y $\overline{\mathbb{K}}$ es una clausura algebraica de $\mathbb{K}$.

Notación y Terminología: Sea $\mathbb{L}/\mathbb{K}$ extensión algebraica.

① Definimos $\Sigma_{\mathbb{L}/\mathbb{K}} := \{\sigma : \mathbb{L} \hookrightarrow \overline{\mathbb{K}}$ morfismos de $\mathbb{K}$-extensiones$\}$.

② Decimos que $\mathbb{L}/\mathbb{K}$ es primitiva si $\exists\, \alpha \in \mathbb{L}$ tal que $\mathbb{L} = \mathbb{K}(\alpha)$.

③ Si $\sigma : \mathbb{L} \hookrightarrow \overline{\mathbb{K}}$ en $\Sigma_{\mathbb{L}/\mathbb{K}}$, entonces σ induce $\sigma : \mathbb{L}[X] \hookrightarrow \overline{\mathbb{K}}[X]$
$$\sum a_i X^i \mapsto \sum \sigma(a_i) X^i$$

Recuerdo: Si $\exists\, n \geq 2$ tq $n \cdot 1 = 0$ en $\mathbb{K}$, entonces el menor entero $\mathrm{char}(\mathbb{K}) \in \mathbb{N}^{\geq 2}$ con dicha propiedad es la característica de $\mathbb{K}$, y $p = \mathrm{char}(\mathbb{K})$ primo. Sino $\mathrm{char}(\mathbb{K}) = 0$.

Lema: Sean $\mathbb{M}/\mathbb{L}/\mathbb{K}$ ext. algebraicas y sup. $\mathbb{M}=\mathbb{L}(\alpha)$ primitiva, $\alpha\in\mathbb{M}$. Si $\sigma:\mathbb{L}\hookrightarrow\overline{\mathbb{K}}$ en $\Sigma_{\mathbb{L}/\mathbb{K}}$, entonces hay una biyección

$$\{\tau:\mathbb{M}\hookrightarrow\overline{\mathbb{K}} \text{ en } \Sigma_{\mathbb{M}/\mathbb{K}} \text{ tq } \tau|_{\mathbb{L}}=\sigma\} \xrightarrow{\sim} \{\beta\in\overline{\mathbb{K}} \text{ tq } \sigma(\mu_\alpha^{\mathbb{L}})(\beta)=0\},\ \tau\mapsto\tau(\alpha).$$

Dem: Sea $\tau:\mathbb{M}\hookrightarrow\overline{\mathbb{K}}$ en $\Sigma_{\mathbb{M}/\mathbb{K}}$ tq $\tau|_{\mathbb{L}}=\sigma$. Dado que $\mu_\alpha^{\mathbb{L}}(\alpha)=0$ en $\mathbb{M}\supseteq\mathbb{L}$ se tiene $\tau(\mu_\alpha^{\mathbb{L}}(\alpha))=0=\tau(\mu_\alpha^{\mathbb{L}})(\tau(\alpha))=\sigma(\mu_\alpha^{\mathbb{L}})(\tau(\alpha))$, i.e., $\tau\mapsto\tau(\alpha)$ bien def. Como $\mathbb{M}=\mathbb{L}(\alpha)$, $\tau\mapsto\tau(\alpha)$ es inyectiva ✓ Si $\beta\in\overline{\mathbb{K}}$ cumple $\sigma(\mu_\alpha^{\mathbb{L}})(\beta)=0$ entonces construimos $\tau=\tau_\beta:\mathbb{M}\hookrightarrow\overline{\mathbb{K}}$ con $\tau|_{\mathbb{L}}=\sigma$ mediante:

$$\begin{tikzcd}
\mathbb{L}[X]/\langle\mu_\alpha^{\mathbb{L}}\rangle \arrow[r, "ev_\beta"] & \overline{\mathbb{K}} \\
\mathbb{L}(\alpha)=\mathbb{M} \arrow[u, "\simeq"', "\varphi"] \arrow[ur] &
\end{tikzcd}$$

$\tau=ev_\beta\circ\varphi^{-1}$ inducido por $[P]\mapsto P(\beta)$. ■

Prop: Sea $P\in\mathbb{K}[X]$ irreducible no-constante. Son equivalentes:

① $\mathrm{Card}(\{\beta\in\overline{\mathbb{K}} \text{ tq } P(\beta)=0\})\neq\deg(P)$.

② $P'=0$ (← "derivada formal": $\frac{d}{dX}(X^n):=nX^{n-1}$)

③ $p=\mathrm{char}(\mathbb{K})>0$ y $\exists\, Q\in\mathbb{K}[X]$ irreducible con $P(X)=Q(X^p)$.

Dem: ①⇔②: Sea $\beta\in\overline{\mathbb{K}}$ tq $(X-\beta)^2\mid P$ y escribamos $P=(X-\beta)Q$ en $\overline{\mathbb{K}}[X]$ con $P(\beta)=P'(\beta)=0$. Así, $P'\in\langle P\rangle=\ker(ev_\beta:\mathbb{K}[X]\to\overline{\mathbb{K}},\ F\mapsto F(\beta))$ y luego $P\mid P'\Rightarrow P'=0$ pues $\deg(P')\leq\deg(P)-1$ ✓ Recíprocamente, si $P'=0$ y $\beta\in\overline{\mathbb{K}}$ es raíz de P con $P=(X-\beta)Q$ en $\overline{\mathbb{K}}[X]$ entonces $P'=0\Rightarrow Q(\beta)=0$ y luego $(X-\beta)^2\mid P$. Así, $\mathrm{Card}(\{\beta\in\overline{\mathbb{K}} \text{ tq } P(\beta)=0\})<\deg(P)$ ✓

②⇔③: Sea $P=\sum_{i=0}^{d}a_iX^i$ con $a_d\neq0$ y sup. que $P'=0$. Entonces, $ia_i=0$ en $\mathbb{K}$ $\forall i\in\{0,\dots,d\}$. Luego, para $a_i\neq0$ tenemos $i=0$ en $\mathbb{K}$ y en particular $p=\mathrm{char}(\mathbb{K})>0$ divide a d. Así, para $a_i\neq0$ se tiene $p\mid i$ en $\mathbb{Z}$ y luego P es de la forma $P=\sum_{j=0}^{d/p}a_{pj}X^{pj}=Q(X^p)$ con $Q:=\sum_{j=0}^{d/p}a_{pj}X^j$ irreducible ✓ Recíprocamente, si $P(X)=Q(X^p)\Rightarrow P'=pX^{p-1}Q'(X^p)\equiv0$ en $\mathbb{K}[X]$ ■

Def: Sea $\mathbb{K}$ un cuerpo de $\mathrm{char}(\mathbb{K})=p>0$. Se define el endomorfismo de Frobenius como $Fr:\mathbb{K}\hookrightarrow\mathbb{K}$, $a\mapsto a^p$, verificando $Fr(ab)=Fr(a)Fr(b)$ y $Fr(a+b)=Fr(a)+Fr(b)$!

Ejercicio Sea $\mathbb{K}:=\mathbb{F}_p(T)$. Probar que $Fr:\mathbb{K}\hookrightarrow\mathbb{K}$ no es sobreyectivo.

Def: Sea $\mathbb{K}$ un cuerpo. Decimos que $\mathbb{K}$ es un cuerpo perfecto si $\mathrm{char}(\mathbb{K})=0$ o si $\mathrm{char}(\mathbb{K})=p>0$ y $Fr:\mathbb{K}\xrightarrow{\sim}\mathbb{K}$, $a\mapsto a^p$ es un automorfismo (eg. si $\mathbb{K}$ es finito).

Corolario: Sea $\mathbb{K}$ un cuerpo perfecto, y sea $P\in\mathbb{K}[X]$ irreducible. Entonces, se tiene que $\mathrm{Card}(\{\beta\in\overline{\mathbb{K}} \text{ tq } P(\beta)=0\})=\deg(P)$.

Dem: Por la Proposición anterior, basta considerar $\mathrm{char}(\mathbb{K})=p>0$ y $P=\sum_{j=0}^{d/p}a_{pj}X^{pj}$ con $a_{pj}\in\mathbb{K}$. Como $\mathbb{K}$ es perfecto, $\exists\, b_j\in\mathbb{K}$ tq $a_{pj}=b_j^p$ y luego:

$$P=\sum_{j=0}^{d/p}b_j^pX^{pj}=\Big(\sum_{j=0}^{d/p}b_jX^j\Big)^p$$ no sería irreducible ↯ ■

Teorema: Sea $\mathbb{L}/\mathbb{K}$ extensión algebraica. Entonces, $\Sigma_{\mathbb{L}/\mathbb{K}} \neq \emptyset$.

Idea de Dem: Si $\mathbb{L}/\mathbb{K}$ ext. finita $\Rightarrow \exists\, \alpha_1, \dots, \alpha_m \in \mathbb{L}$ tq $\mathbb{L} = \mathbb{K}(\alpha_1, \dots, \alpha_m)$ y concluimos usando inductivamente el lema probado anteriormente.
Si $\mathbb{L}/\mathbb{K}$ es infinita, el lema de Zorn aplicado al conjunto parcialmente ordenado
$$\{(\mathbb{M}, \sigma) \text{ donde } \mathbb{L}/\mathbb{M} \text{ y donde } \sigma \in \Sigma_{\mathbb{M}/\mathbb{K}}\}$$
permite construir $\sigma_{max} : \mathbb{M}_{max} = \mathbb{L} \hookrightarrow \overline{\mathbb{K}}$ en $\Sigma_{\mathbb{L}/\mathbb{K}}$ ✓ ■

Def: Sea $\mathbb{L}/\mathbb{K}$ una extensión algebraica. El grado de separabilidad de $\mathbb{L}$ sobre $\mathbb{K}$ es
$$[\mathbb{L}:\mathbb{K}]_s := \mathrm{Card}(\Sigma_{\mathbb{L}/\mathbb{K}}) \in \mathbb{N}^{\geq 1} \cup \{+\infty\}$$
Además, es indep. de la elección de la clausura algebraica $\overline{\mathbb{K}}$ de $\mathbb{K}$.

Ejemplo principal: Sup. $\mathbb{L} = \mathbb{K}(\alpha)$ extensión primitiva y algebraica. El Lema anterior (aplicado a $\mathbb{K}(\alpha)/\mathbb{K}/\mathbb{K}$) implica que
$$[\mathbb{K}(\alpha):\mathbb{K}]_s = \mathrm{Card}(\{\beta \in \overline{\mathbb{K}} \text{ tq } \mu_\alpha^{\mathbb{K}}(\beta) = 0\}).$$
En part, si $\mathbb{K}$ es un cuerpo perfecto entonces $[\mathbb{K}(\alpha):\mathbb{K}]_s = [\mathbb{K}(\alpha):\mathbb{K}]$.

Teorema: Sean $\mathbb{M}/\mathbb{L}/\mathbb{K}$ extensiones algebraicas, entonces $[\mathbb{M}:\mathbb{K}]_s = [\mathbb{M}:\mathbb{L}]_s [\mathbb{L}:\mathbb{K}]_s$.
En part, $[\mathbb{M}:\mathbb{K}]_s < +\infty \iff [\mathbb{M}:\mathbb{L}]_s$ y $[\mathbb{L}:\mathbb{K}]_s$ son finitos.

Dem: Considerar la restricción $R : \Sigma_{\mathbb{M}/\mathbb{K}} \longrightarrow \Sigma_{\mathbb{L}/\mathbb{K}}$, $\tau \mapsto \tau|_{\mathbb{L}}$ y fijemos un $\sigma : \mathbb{L} \hookrightarrow \overline{\mathbb{K}}$ en $\Sigma_{\mathbb{L}/\mathbb{K}}$. En part, usando σ, $\overline{\mathbb{K}}$ es una clausura alg. de $\mathbb{L}$ y luego $\Sigma_{\mathbb{M}/\mathbb{L}} \simeq \{\tau : \mathbb{M} \hookrightarrow \overline{\mathbb{L}} := \overline{\mathbb{K}} \text{ morfismo de } \mathbb{L}\text{-álg. con } \tau|_{\mathbb{L}} = \sigma\} \overset{\text{def}}{=} R^{-1}(\{\sigma\})$.
Así, $\mathrm{Card}(R^{-1}(\{\sigma\})) = [\mathbb{M}:\mathbb{L}]_s$ y luego $\mathrm{Card}(\Sigma_{\mathbb{M}/\mathbb{K}}) = [\mathbb{M}:\mathbb{L}]_s\, \mathrm{Card}(\Sigma_{\mathbb{L}/\mathbb{K}})$ ✓ ■

Def: Sea $\mathbb{K}$ un cuerpo. Decimos que:
1. $P \in \mathbb{K}[X] \setminus \{0\}$ es separable si $\deg(P) = \mathrm{Card}(\{\beta \in \overline{\mathbb{K}} \text{ tq } P(\beta) = 0\})$.
2. $\alpha \in \mathbb{L}/\mathbb{K}$ algebraico sobre $\mathbb{K}$ es separable sobre $\mathbb{K}$ si $\mu_\alpha^{\mathbb{K}}$ es separable.
3. Una extensión algebraica $\mathbb{L}/\mathbb{K}$ es una extensión separable si todo $\alpha \in \mathbb{L}$ es separable sobre $\mathbb{K}$.

Notación: La característica exponencial de $\mathbb{K}$ es $\exp.\mathrm{char}(\mathbb{K}) := \begin{cases} 1 & \text{si } \mathrm{char}(\mathbb{K}) = 0 \\ p & \text{si } \mathrm{char}(\mathbb{K}) = p > 0 \end{cases}$

⚠ **Obs**: Sean $\mathbb{M}/\mathbb{L}/\mathbb{K}$ ext. algebraicas y sea $\alpha \in \mathbb{M}$. Entonces, como $\mu_\alpha^{\mathbb{L}} \mid \mu_\alpha^{\mathbb{K}}$:
$$\alpha \in \mathbb{M} \text{ separable sobre } \mathbb{K} \Rightarrow \alpha \in \mathbb{M} \text{ separable sobre } \mathbb{L}$$

Prop: Sea $\mathbb{L}/\mathbb{K}$ extensión finita. Entonces, $[\mathbb{L}:\mathbb{K}]_s$ divide a $[\mathbb{L}:\mathbb{K}]$ y el grado de inseparabilidad $[\mathbb{L}:\mathbb{K}]_i := [\mathbb{L}:\mathbb{K}]/[\mathbb{L}:\mathbb{K}]_s$ es una potencia de $\exp.\mathrm{char}(\mathbb{K})$.
Más aún, $\mathbb{L}/\mathbb{K}$ es separable $\iff [\mathbb{L}:\mathbb{K}]_s = [\mathbb{L}:\mathbb{K}]$.

Dem: Sup. primero que $\mathbb{L} = \mathbb{K}(\alpha)$ extensión primitiva y sea $\mu_\alpha^{\mathbb{K}} = \sum_{i=0}^{d} a_i X^i$ con $a_d = 1 \neq 0$. Ya vimos que si $\mathrm{char}(\mathbb{K}) = 0 \Rightarrow [\mathbb{L}:\mathbb{K}]_s = [\mathbb{L}:\mathbb{K}]$ ✓
Sup. que $\mathrm{char}(\mathbb{K}) = p > 0$ y definamos $r := \max\{m \text{ tq } \{j,\ a_j \neq 0\} \subseteq p^m \mathbb{Z}\} \in \mathbb{N}$.
Así, p^r divide a $d = \deg(\mu_\alpha^{\mathbb{K}}) = [\mathbb{L}:\mathbb{K}]$. Veamos que $[\mathbb{L}:\mathbb{K}]_i = p^r$:

Por def. de r, tenemos $\mu_\alpha^{\mathbb{K}} = \sum_{i=0}^{d/p^r} a_{ip^r} X^{ip^r} = Q(X^{p^r})$ con $Q \in \mathbb{K}[X]$ irred.
Por maximalidad de r, $Q' \neq 0$ y, como $\overline{\mathbb{K}}$ perfecto, $Fr : \overline{\mathbb{K}} \simeq \overline{\mathbb{K}}$ automorfismo.
Luego, $\Sigma_{\mathbb{L}/\mathbb{K}} \overset{1:1}{\longleftrightarrow} \{\beta \in \overline{\mathbb{K}}, \mu_\alpha^{\mathbb{K}}(\beta) = 0\} \overset{1:1}{\longleftrightarrow} \{\gamma \in \overline{\mathbb{K}}, Q(\gamma) = 0\}$ son biyecciones
$\beta \longmapsto \beta^{p^r}$
$\Rightarrow \text{Card}(\Sigma_{\mathbb{L}/\mathbb{K}}) = \text{Card}(\{\gamma \in \overline{\mathbb{K}}, Q(\gamma) = 0\}) = \deg(Q)$ (pues $Q' \neq 0$).
Como $\mu_\alpha^{\mathbb{K}} = Q(X^{p^r})$, $[\mathbb{L} : \mathbb{K}]_s = \deg(Q) = \deg(\mu_\alpha^{\mathbb{K}})/p^r = [\mathbb{L} : \mathbb{K}]/p^r$ ✓

Para el caso general en que $\mathbb{L} = \mathbb{K}(\alpha_1, \dots, \alpha_m)$, con $\alpha_i \in \mathbb{L}$, escribimos $\mathbb{K}_0 := \mathbb{K}$ y $\mathbb{K}_i := \mathbb{K}(\alpha_1, \dots, \alpha_i)$ con $i \in \{1, \dots, m\}$. Como $[\mathbb{L} : \mathbb{K}] = \prod_{i=1}^m [\mathbb{K}_i : \mathbb{K}_{i-1}]$ y $[\mathbb{L} : \mathbb{K}]_s = \prod_{i=1}^m [\mathbb{K}_i : \mathbb{K}_{i-1}]_s$, basta aplicar lo anterior a cada extensión $\mathbb{K}_i/\mathbb{K}_{i-1}$ ✓

Veamos finalmente que $\mathbb{L}/\mathbb{K}$ separable $\Leftrightarrow [\mathbb{L} : \mathbb{K}]_s = [\mathbb{L} : \mathbb{K}]$:
($\Rightarrow$) Como $\mu_\alpha^{\mathbb{K}_i} \mid \mu_\alpha^{\mathbb{K}}$ en $\mathbb{K}_i[X]$ para todo $\alpha \in \mathbb{L}$, tenemos que α_{i+1} es separable sobre $\mathbb{K}_i$ y luego $[\mathbb{K}_{i+1} : \mathbb{K}_i]_s = [\mathbb{K}_{i+1} : \mathbb{K}_i]$ (cf. Ejemplo principal). Así, tenemos que $[\mathbb{L} : \mathbb{K}]_s = [\mathbb{L} : \mathbb{K}]$ ✓
($\Leftarrow$) Sea $\alpha \in \mathbb{L}$. Basta verificar que $[\mathbb{K}(\alpha) : \mathbb{K}]_s = [\mathbb{K}(\alpha) : \mathbb{K}]$ (cf. Ejemplo principal). En general, $[\mathbb{K}(\alpha) : \mathbb{K}]_s \leq [\mathbb{K}(\alpha) : \mathbb{K}]$ y $[\mathbb{L} : \mathbb{K}(\alpha)]_s \leq [\mathbb{L} : \mathbb{K}(\alpha)]$ y luego
$[\mathbb{L} : \mathbb{K}(\alpha)][\mathbb{K}(\alpha) : \mathbb{K}] = [\mathbb{L} : \mathbb{K}] \overset{\text{hip}}{=} [\mathbb{L} : \mathbb{K}]_s = [\mathbb{L} : \mathbb{K}(\alpha)]_s [\mathbb{K}(\alpha) : \mathbb{K}]_s \Rightarrow \alpha$ separable ■

Def: Sea $\mathbb{L}/\mathbb{K}$ una extensión algebraica. La subextensión $\mathbb{L}/\mathbb{L}'/\mathbb{K}$ definida por
$$\mathbb{L}' := \{\alpha \in \mathbb{L} \text{ tal que } \alpha \text{ es separable sobre } \mathbb{K}\}$$
se llama la clausura separable de $\mathbb{K}$ relativa a $\mathbb{L}$.

Ejercicio Probar que $\mathbb{K} \subseteq \mathbb{L}'$ y que $\mathbb{L}'$ es un cuerpo.
(Indicación: si $\alpha, \beta \in \mathbb{L}$ separables sobre $\mathbb{K}$, analizar la extensión $\alpha \pm \beta, \alpha\beta \in \mathbb{K}(\alpha,\beta)/\mathbb{K}$).

Terminología: Sea $\mathbb{M}/\mathbb{K}$ extensión y $\mathbb{L}_1, \mathbb{L}_2 \subseteq \mathbb{M}$ subextensiones. Definimos la composición de $\mathbb{L}_1$ y $\mathbb{L}_2$ como $\mathbb{L}_1\mathbb{L}_2 := \mathbb{K}(\mathbb{L}_1 \cup \mathbb{L}_2) \subseteq \mathbb{M}$.

Corolario: Sea $\mathbb{M}/\mathbb{K}$ una extensión y $\mathbb{L}_1, \mathbb{L}_2 \subseteq \mathbb{M}$ subextensiones. Supongamos que $\mathbb{L}_1/\mathbb{K}$ y $\mathbb{L}_2/\mathbb{K}$ son separables, entonces $\mathbb{L}_1 \cap \mathbb{L}_2/\mathbb{K}$ y $\mathbb{L}_1\mathbb{L}_2/\mathbb{K}$ también.

Dem: Si $\mathbb{M}'$ es la clausura separable de $\mathbb{K}$ resp. a $\mathbb{M}$, entonces $\mathbb{L}_1, \mathbb{L}_2 \subseteq \mathbb{M}'$ y luego $\mathbb{L}_1 \cap \mathbb{L}_2 \subseteq \mathbb{M}'$ y $\mathbb{L}_1\mathbb{L}_2 \subseteq \mathbb{M}'$ ■

Prop: Sean $\mathbb{M}/\mathbb{L}/\mathbb{K}$ extensiones algebraicas. Entonces,
$$\mathbb{M}/\mathbb{K} \text{ separable} \Leftrightarrow \mathbb{M}/\mathbb{L} \text{ y } \mathbb{L}/\mathbb{K} \text{ son separables.}$$

Dem: ($\Rightarrow$) $\alpha \in \mathbb{M}$ separable$/\mathbb{K} \Rightarrow \alpha$ separable$/\mathbb{L}$ pues $\mu_\alpha^{\mathbb{L}} \mid \mu_\alpha^{\mathbb{K}}$ ✓
($\Leftarrow$) Sea $\alpha \in \mathbb{M}$, separable$/\mathbb{L}$ por hipótesis, y veamos que es separable$/\mathbb{K}$:
Escribamos $\mu_{\mathbb{L}}^{\alpha} = X^d + \sum_{i=0}^{d-1} a_i X^i$ con $a_i \in \mathbb{L} \Rightarrow \mu_{\mathbb{L}}^{\alpha} \in \mathbb{K}(a_0, \dots, a_{d-1})[X]$ irreducible (sino, sería reducible sobre $\mathbb{L}$) $\Rightarrow \mu^{\alpha}_{\mathbb{K}(a_0, \dots, a_{d-1})} = \mu_{\mathbb{L}}^{\alpha}$ y así α separable$/\mathbb{K}(a_0, \dots, a_{d-1})$
$\overset{\text{def}}{\Rightarrow} [\mathbb{K}(a_0, \dots, a_{d-1}, \alpha) : \mathbb{K}(a_0, \dots, a_{d-1})]_s = [\mathbb{K}(a_0, \dots, a_{d-1}, \alpha) : \mathbb{K}(a_0, \dots, a_{d-1})]$ y como $[\mathbb{K}(a_0, \dots, a_{d-1}) : \mathbb{K}]_s = [\mathbb{K}(a_0, \dots, a_{d-1}) : \mathbb{K}]$ (pues $\mathbb{L}/\mathbb{K}$ separable) se deduce que $\alpha \in \mathbb{K}(a_0, \dots, a_{d-1}, \alpha)/\mathbb{K}$ es una extensión separable ✓ ■

Prop: Sea $\mathbb{L}/\mathbb{K}$ extensión finita y sea $\mathbb{L}'/\mathbb{K}$ la clausura separable de $\mathbb{K}$ resp. $\mathbb{L}$. Entonces, $[\mathbb{L}':\mathbb{K}] = [\mathbb{L}:\mathbb{K}]_s$ y en particular $[\mathbb{L}:\mathbb{K}]_i = [\mathbb{L}:\mathbb{L}']$ y $[\mathbb{L}:\mathbb{L}']_s = 1$.

Dem: Tenemos $[\mathbb{L}':\mathbb{K}] \overset{\text{def}}{=} [\mathbb{L}':\mathbb{K}]_s \leq [\mathbb{L}:\mathbb{L}']_s[\mathbb{L}':\mathbb{K}]_s = [\mathbb{L}:\mathbb{K}]_s$. Sea $\alpha \in \mathbb{L}$ y recordemos (ver pág 14) que $\exists\, r \in \mathbb{N}$ y $Q \in \mathbb{K}[X]$ irred con $Q' \neq 0$ tal que $\mu_\alpha^{\mathbb{K}} = Q(X^{p^r})$, con $p = $ exp. char$(\mathbb{K})$, y luego $\beta := \alpha^{p^r} \in \mathbb{L}'$ es separable $/\mathbb{K}$.
Notar que $\alpha \in \mathbb{L}$ es raíz de $X^{p^r} - \beta \in \mathbb{L}'[X]$ y que $X^{p^r} - \beta = (X-\alpha)^{p^r}$ en $\mathbb{L}[X]$ $\Rightarrow$ si $\mathbb{L}' \subseteq \mathbb{M} \subseteq \mathbb{L}$ subextensión, entonces $\mu_\alpha^{\mathbb{M}} \mid (X-\alpha)^{p^r}$ en $\mathbb{L}[X]$ y luego $[\mathbb{M}(\alpha):\mathbb{M}]_s \overset{\text{def}}{=} 1$ (pues α es la única raíz multiple).
Finalmente, si $\alpha_1, \dots, \alpha_m \in \mathbb{L}$ son tales que $\mathbb{L} = \mathbb{L}'(\alpha_1, \dots, \alpha_m)$ entonces:

$$[\mathbb{L}:\mathbb{L}']_s = \prod_{i=1}^{m} \underbrace{[\mathbb{L}'(\alpha_1,\dots,\alpha_{i-1})(\alpha_i) : \mathbb{L}'(\alpha_1,\dots,\alpha_{i-1})]_s}_{=1} = 1 \Rightarrow [\mathbb{L}:\mathbb{K}]_s = [\mathbb{L}':\mathbb{K}]_s = [\mathbb{L}':\mathbb{K}] \quad \blacksquare$$

Resumen: Toda extensión algebraica finita $\mathbb{L}/\mathbb{K}$ se descompone como

$$\begin{tikzcd}
\mathbb{L} \arrow[dr, dash, "\text{puramente inseparable, ie, } {[\mathbb{L}:\mathbb{L}']_s = 1}"] \arrow[dd, dash, "\text{algebraica}"'] & \\
 & \mathbb{L}' \arrow[dl, dash, "\text{separable}"] \\
\mathbb{K} &
\end{tikzcd}$$

Aquí, $\exists\, \beta_1, \dots, \beta_m \in \mathbb{L}'$ y $r_1, \dots, r_m \in \mathbb{N}$ tales que $\mathbb{L} = \mathbb{L}'\left(\sqrt[p^{r_1}]{\beta_1}, \dots, \sqrt[p^{r_m}]{\beta_m}\right)$.

Teorema del Elemento Primitivo (Emil Artin ≈ 1930): Sea $\mathbb{L}/\mathbb{K}$ una extensión finita y separable. Entonces, $\exists\, \alpha \in \mathbb{L}$ tal que $\mathbb{L} = \mathbb{K}(\alpha)$.

Dem: Si $\mathbb{K}$ cuerpo finito, entonces $\mathbb{L}$ también. Por Teoría de Grupos y Anillos, $\mathbb{L}^*$ es un grupo cíclico finito, ie, $\mathbb{L}^* = \langle \alpha \rangle$ y luego $\mathbb{L} = \mathbb{K}(\alpha)$ ✓
Sup. $\mathbb{L} = \mathbb{K}(\alpha_1, \dots, \alpha_m)$ y $\mathbb{K}$ cuerpo infinito. Por inducción en m, basta considerar $\mathbb{L} = \mathbb{K}(\alpha, \beta)$ con $\alpha, \beta \in \mathbb{L}$. Consideremos el polinomio

$$P := \prod_{\substack{\sigma, \sigma' \in \Sigma_{\mathbb{L}/\mathbb{K}} \\ \sigma \neq \sigma'}} \left(X(\sigma(\beta) - \sigma'(\beta)) + (\sigma(\alpha) - \sigma'(\alpha)) \right) \in \overline{\mathbb{K}}[X]$$

con $P \neq 0$ pues si $\sigma \neq \sigma'$ entonces $\sigma(\alpha) \neq \sigma'(\alpha)$ o $\sigma(\beta) \neq \sigma'(\beta)$ (pues $\mathbb{L} = \mathbb{K}(\alpha,\beta)$).
Así, como $\mathbb{K}$ infinito, $\exists\, \lambda \in \mathbb{K}$ tq $P(\lambda) \neq 0$ y definamos $\gamma := \alpha + \lambda\beta$

$$\Rightarrow P(\lambda) = \prod_{\sigma \neq \sigma'} \left(\sigma(\alpha) + \lambda\sigma(\beta) - \sigma'(\alpha) - \lambda\sigma'(\beta)\right) \overset{\text{def}}{=} \prod_{\sigma \neq \sigma'} \left(\sigma(\gamma) - \sigma'(\gamma)\right) \neq 0$$

Así, para todos $\sigma, \sigma' \in \Sigma_{\mathbb{L}/\mathbb{K}}$ con $\sigma \neq \sigma'$ se tiene $\sigma(\gamma) \neq \sigma'(\gamma)$, ie, la restricción $\Sigma_{\mathbb{L}/\mathbb{K}} \hookrightarrow \Sigma_{\mathbb{K}(\gamma)/\mathbb{K}}$, $\sigma \mapsto \sigma|_{\mathbb{K}(\gamma)}$ es inyectiva $(\star)$. Luego:

$$[\mathbb{K}(\gamma):\mathbb{K}] \overset{\text{def}}{\geq} [\mathbb{K}(\gamma):\mathbb{K}]_s \overset{(\star)}{\geq} [\mathbb{L}:\mathbb{K}]_s \overset{\text{hip}}{=} [\mathbb{L}:\mathbb{K}] \overset{\gamma \in \mathbb{L}}{\Longrightarrow} \mathbb{L} = \mathbb{K}(\gamma) \quad \blacksquare$$

⚠ El Teorema del Elemento Primitivo es FALSO sin la hipótesis de separabilidad.
Por ejemplo si $\mathbb{K} = \mathbb{F}_p(X,Y)$ y $\mathbb{L} = \mathbb{K}(\sqrt[p]{X}, \sqrt[p]{Y})$, con $[\mathbb{L}:\mathbb{K}] = p^2$, entonces todo $\alpha \in \mathbb{L}$ cumple que $\alpha^p \in \mathbb{K}$ (pues $(a+b)^p = a^p + b^p$) $\Rightarrow [\mathbb{K}(\alpha):\mathbb{K}] \leq p < p^2$.

Ejercicio Sea $\mathbb{K} = \mathbb{F}_p(T)$ y $\mathbb{L} := \mathbb{K}[X]/\langle X^p - X + T \rangle$. Probar que $\mathbb{L}/\mathbb{K}$ es una extensión separable de grado $[\mathbb{L}:\mathbb{K}] = p$.

§7. Extensiones normales

Def: Sea $\{P_i\}_{i\in I} \subseteq \mathbb{K}[X]$ familia arbitraria de polinomios. Un cuerpo de descomposición de los $\{P_i\}_{i\in I}$ sobre $\mathbb{K}$ es una extensión $\mathbb{L}/\mathbb{K}$ que cumple:
① P_i escinde en $\mathbb{L}[X]$ para todo $i\in I$.
② $\mathbb{L} = \mathbb{K}(\{\beta\in\mathbb{L}$ tq $\exists\, i\in I$ con $P_i(\beta)=0\})$ ($\Rightarrow \mathbb{L}/\mathbb{K}$ ext. algebraica).

Prop: Sea $\{P_i\}_{i\in I} \subseteq \mathbb{K}[X]$ familia arbitraria de polinomios. Entonces:
① $\exists!$ subextensión $\mathbb{K}\subseteq\mathbb{L}\subseteq\overline{\mathbb{K}}$ tq $\mathbb{L}$ es un cuerpo de descomposición de los $\{P_i\}_{i\in I}$.
② Para todo cuerpo de descomposición $\mathbb{L}'/\mathbb{K}$ de $\{P_i\}_{i\in I}$ y todo $\sigma:\mathbb{L}'\hookrightarrow\overline{\mathbb{K}}$ en $\underbrace{\Sigma_{\mathbb{L}'/\mathbb{K}}}_{\neq\emptyset \text{ pues } \mathbb{L}'/\mathbb{K} \text{ ext. algebraica!}}$ se tiene que $\sigma(\mathbb{L}')=\mathbb{L}$. Así, $\mathbb{L}\cong\mathbb{L}'$ son $\mathbb{K}$-isomorfos.

Dem: Sea $Z := \{\beta\in\overline{\mathbb{K}}$ tq $\exists\, i\in I,\ P_i(\beta)=0\}\subseteq\overline{\mathbb{K}}$, entonces $\mathbb{L}:=\mathbb{K}(Z)\subseteq\overline{\mathbb{K}}$ es la única subextensión de $\overline{\mathbb{K}}$ que es cuerpo de descomposición de los $\{P_i\}_{i\in I}$ $\Rightarrow$ ① ✓
Para ②, notar que $\sigma:\mathbb{L}'\hookrightarrow\overline{\mathbb{K}}$ induce un $\mathbb{K}$-isomorfismo $\mathbb{L}'\cong\sigma(\mathbb{L}')\subseteq\overline{\mathbb{K}}$ y luego $\sigma(\mathbb{L}')$ es un cuerpo de descomp. de $\{P_i\}_{i\in I}$ en $\overline{\mathbb{K}}$ $\overset{①}{\Rightarrow}$ $\sigma(\mathbb{L}')=\mathbb{L}$ ✓ ■

Ejemplos: ① $\mathbb{K}=\mathbb{Q}$ y $\overline{\mathbb{K}}=\overline{\mathbb{Q}}\subseteq\mathbb{C}$. Si $P=X^2-2$ entonces $\mathbb{L}=\mathbb{Q}(\sqrt{2})\subseteq\overline{\mathbb{Q}}$ es cuerpo de descomp. de P. El cuerpo $\mathbb{L}'=\mathbb{Q}[X]/\langle X^2-2\rangle$ también, con $\mathbb{L}\cong\mathbb{L}'$.
② (E. Moore, 1893): Sea $n\in\mathbb{N}^{\geq 1}$, p un número primo y $q:=p^n$. Consideremos $F:=X^q-X\in\mathbb{F}_p[X]$ polinomio separable (pues $F'=-1\neq 0$) y sea $\mathbb{F}_p\subseteq\mathbb{L}\subseteq\overline{\mathbb{F}_p}$ su cuerpo de descomposición. Dado que $(ab)^q=a^qb^q$ y $(a+b)^q=a^q+b^q$ en $\overline{\mathbb{F}_p}$, el conjunto de las q raíces de F en $\overline{\mathbb{F}_p}$ es un cuerpo y luego coincide con $\mathbb{L}$
$\Rightarrow \mathbb{F}_q := \mathbb{L}\subseteq\overline{\mathbb{F}_p}$ es el único cuerpo (salvo isom.) con $q=p^n$ elementos.

Teorema/Definición: Una extensión algebraica $\mathbb{L}/\mathbb{K}$ es una extensión normal si cumple alguna de las sgtes condiciones equivalentes:
① Para todas $\sigma,\sigma':\mathbb{L}\hookrightarrow\overline{\mathbb{K}}$ en $\Sigma_{\mathbb{L}/\mathbb{K}}$, se tiene $\sigma(\mathbb{L})=\sigma'(\mathbb{L})$.
② Para todo $P\in\mathbb{K}[X]$ irred, si P tiene una raíz en $\mathbb{L}$ entonces P escinde en $\mathbb{L}$.
③ $\exists\,\{P_i\}_{i\in I}\subseteq\mathbb{K}[X]$ familia de pol. tal que $\mathbb{L}$ es su cuerpo de descomposición sobre $\mathbb{K}$.

Dem: ③ $\Rightarrow$ ① (Prop. anterior) y ② $\Rightarrow$ ③ (considerar $\{\mu_\alpha^{\mathbb{K}}\}_{\alpha\in\mathbb{L}}$, donde $\mu_\alpha^{\mathbb{K}}(\alpha)=0$).
Basta probar ① $\Rightarrow$ ②: Sea $P\in\mathbb{K}[X]$ irred. y $\alpha\in\mathbb{L}$ con $P(\alpha)=0$. La composición

$$\begin{array}{ccccc}\Sigma_{\mathbb{L}/\mathbb{K}} & \twoheadrightarrow & \Sigma_{\mathbb{K}(\alpha)/\mathbb{K}} & \xrightarrow{\sim} & Z(P):=\{\beta\in\overline{\mathbb{K}}, P(\beta)=0\} \\ \sigma & \longmapsto & \sigma|_{\mathbb{K}(\alpha)}\ ;\ \tau & \longmapsto & \tau(\alpha)\end{array}$$

es sobreyectiva. Así, para $\beta\in Z(P)$ existe $\sigma=\sigma_\beta:\mathbb{L}\hookrightarrow\overline{\mathbb{K}}$ en $\Sigma_{\mathbb{L}/\mathbb{K}}$ tq $\sigma_\beta(\alpha)=\beta$.
Fijemos cualquier $\sigma\in\Sigma_{\mathbb{L}/\mathbb{K}}$ $\overset{①}{\Rightarrow}$ $\sigma(\mathbb{L})=\sigma_\beta(\mathbb{L})\ni\beta$ para todo $\beta\in Z(P)$. Así, si escribimos $\gamma_\beta:=\sigma^{-1}(\beta)\in\mathbb{L}$ y $P=a\prod_{\beta\in Z(P)}(X-\beta)^{m_\beta}\in\overline{\mathbb{K}}[X]$ con $a\in\mathbb{K}$ coef. líder
$\Rightarrow P=a\prod_{\beta\in Z(P)}(X-\gamma_\beta)^{m_\beta}\in\mathbb{L}[X]$ escinde en $\mathbb{L}$ ✓ ■

Ejemplos: ① $\overline{\mathbb{K}}/\mathbb{K}$ es una extensión normal (cumple ②).
② $\mathbb{Q}(\sqrt{d})/\mathbb{Q}$ es una extensión normal, con $d\in\mathbb{Z}$ libre de cuadrados (cumple ②).

③ $\mathbb{Q}(\sqrt[4]{2})/\mathbb{Q}$ no es normal, pues $\mathbb{Q}(\sqrt[4]{2}) \subseteq \mathbb{R} \subseteq \mathbb{C}$ donde $\mathbb{C}$ clausura alg. de $\mathbb{Q}$ y $\sigma : \mathbb{Q}(\sqrt[4]{2}) \hookrightarrow \mathbb{C}$. Por otro lado, $\mathbb{Q}[X]/\langle X^4-2\rangle \cong \mathbb{Q}(\sqrt[4]{2}) \cong \mathbb{Q}(i\sqrt[4]{2})$ y así $\sigma' : \mathbb{Q}(\sqrt[4]{2}) \xrightarrow{\sim} \mathbb{Q}(i\sqrt[4]{2}) \hookrightarrow \mathbb{C}$ cumple $\sigma(\mathbb{Q}(\sqrt[4]{2})) \neq \sigma'(\mathbb{Q}(\sqrt[4]{2}))$.

$\boxed{\text{Ejercicio}}$ Probar que $\mathbb{Q}(\sqrt[4]{2})/\mathbb{Q}$ no es normal analizando $P = X^4 - 2 \in \mathbb{Q}[X]$.

Prop: Sea $\mathbb{M}/\mathbb{K}$ una extensión y $\mathbb{L}_1, \mathbb{L}_2 \subseteq \mathbb{M}$ subextensiones. Supongamos que $\mathbb{L}_1/\mathbb{K}$ y $\mathbb{L}_2/\mathbb{K}$ son extensiones normales, entonces $\mathbb{L}_1 \cap \mathbb{L}_2/\mathbb{K}$ y $\mathbb{L}_1\mathbb{L}_2/\mathbb{K}$ también.

Dem: $\mathbb{L}_1 \cap \mathbb{L}_2/\mathbb{K}$ es normal por el ítem ② del Teorema. Por otro lado, si $\sigma, \sigma' \in \Sigma_{\mathbb{L}_1\mathbb{L}_2/\mathbb{K}}$ entonces $\sigma'(\mathbb{L}_1\mathbb{L}_2) = \sigma'(\mathbb{L}_1)\sigma'(\mathbb{L}_2) \overset{①}{=} \sigma(\mathbb{L}_1)\sigma(\mathbb{L}_2) = \sigma(\mathbb{L}_1\mathbb{L}_2)$ ✓ ■

⚠ Sean $\mathbb{M}/\mathbb{L}/\mathbb{K}$ extensiones algebraicas. En general:

①
$$\begin{tikzcd}[column sep=small] \mathbb{M} \arrow[dr, dash, "\text{normal}"] \arrow[dd, dash, "\cancel{\text{normal}}"'] & \\ & \mathbb{L} \arrow[dl, dash, "\text{normal}"] \\ \mathbb{K} & \end{tikzcd}$$

Eg. $\mathbb{Q} \subseteq \mathbb{Q}(\sqrt{2}) \subseteq \mathbb{Q}(\sqrt[4]{2})$ donde $\mathbb{Q}(\sqrt{2})/\mathbb{Q}$ (resp. $\mathbb{Q}(\sqrt[4]{2})/\mathbb{Q}(\sqrt{2})$) normal pues es cuerpo de descomposición de X^2-2 (resp. $X^2-\sqrt{2}$).

②
$$\begin{tikzcd}[column sep=small] \mathbb{M} \arrow[dr, dash] \arrow[dd, dash, "\text{normal}"'] & \\ & \mathbb{L} \arrow[dl, dash, "\cancel{\text{normal}}"] \\ \mathbb{K} & \end{tikzcd}$$

Eg. $\mathbb{Q} \subseteq \mathbb{Q}(\sqrt[4]{2}) \subseteq \mathbb{Q}(i, \sqrt[4]{2})$ donde $\mathbb{Q}(i,\sqrt[4]{2})/\mathbb{Q}$ (resp. $\mathbb{Q}(i,\sqrt[4]{2})/\mathbb{Q}(\sqrt[4]{2})$) normal pues es cuerpo de descomposición de X^4-2 (resp. X^2+1).

③
$$\begin{tikzcd}[column sep=small] \mathbb{M} \arrow[dr, dash, "\text{normal} ✓"] \arrow[dd, dash, "\text{normal}"'] & \\ & \mathbb{L} \arrow[dl, dash] \\ \mathbb{K} & \end{tikzcd}$$

Pues si $\mathbb{M}$ cuerpo de descomposición de $\{P_i\}_{i\in I} \subseteq \mathbb{K}[X]$ sobre $\mathbb{K}$ $\Rightarrow \mathbb{M}$ cuerpo de descomp. de $\{P_i\}_{i\in I} \subseteq \mathbb{L}[X]$ sobre $\mathbb{L}$ (pues $\mathbb{K} \subseteq \mathbb{L}$).

Def: Sea $\mathbb{L}/\mathbb{K}$ una extensión algebraica. Sea $\mathbb{L}^n$ un cuerpo de descomposición de $\{\mu_\alpha^{\mathbb{K}}\}_{\alpha\in\mathbb{L}}$ sobre $\mathbb{K}$. Luego, $\mathbb{L}^n/\mathbb{L}/\mathbb{K}$ y $\mathbb{L}^n/\mathbb{L}$ es una clausura normal de $\mathbb{L}$ sobre $\mathbb{K}$.

Ejemplo: $\mathbb{K} = \mathbb{Q} \subseteq \mathbb{L} = \mathbb{Q}(\sqrt[4]{2}) \subseteq \mathbb{L}^n = \mathbb{Q}(i, \sqrt[4]{2}) \subseteq \overline{\mathbb{K}} = \overline{\mathbb{Q}} \subseteq \mathbb{C}$.

Prop: Sea $\mathbb{L}/\mathbb{K}$ ext. algebraica y $\mathbb{L}^n/\mathbb{L}$ una clausura normal de $\mathbb{L}$ sobre $\mathbb{K}$. Entonces:
① $\mathbb{L}^n/\mathbb{K}$ es una extensión normal ($\Rightarrow \mathbb{L}^n/\mathbb{L}$ extensión normal).
② $\mathbb{L}^n$ es la "extensión más pequeña de $\mathbb{L}$ normal sobre $\mathbb{K}$", ie, para toda $\mathbb{M}/\mathbb{L}$ ext. normal sobre $\mathbb{K}$, $\exists\, \mathbb{L}^n \hookrightarrow \mathbb{M}$ morfismo de $\mathbb{L}$-extensiones.

Dem: ① $\mathbb{L}^n$ es un cuerpo de descomposición $\Rightarrow \mathbb{L}^n/\mathbb{K}$ normal ✓ Para ②, primero notar que $\exists\, \mathbb{L} \hookrightarrow \mathbb{L}^n$ morfismo de $\mathbb{K}$-extensiones: si $\sigma : \mathbb{L} \hookrightarrow \overline{\mathbb{K}}$ en $\Sigma_{\mathbb{L}/\mathbb{K}}$ y $\tau : \mathbb{L}^n \hookrightarrow \overline{\mathbb{K}}$ en $\Sigma_{\mathbb{L}^n/\mathbb{K}}$ entonces $\tau(\mathbb{L}^n) \overset{\text{def}}{=} \mathbb{K}(\{\beta \in \overline{\mathbb{K}}, \exists\, \alpha \in \mathbb{L} \text{ tq } \mu_\alpha^{\mathbb{K}}(\beta) = 0\})$.
$\Rightarrow$ Todo $\alpha \in \mathbb{L}$ es tal que $\mu_\alpha^{\mathbb{K}}(\sigma(\alpha)) = 0$, ie, $\sigma(\alpha) \in \tau(\mathbb{L}^n)$ y así $\tau^{-1}\circ\sigma : \mathbb{L} \hookrightarrow \mathbb{L}^n$ ✓
Más generalmente, si $\mathbb{M}/\mathbb{L}$ normal sobre $\mathbb{K}$ y $\varphi : \mathbb{M} \hookrightarrow \overline{\mathbb{K}}$ en $\Sigma_{\mathbb{M}/\mathbb{K}}$ tq $\varphi|_{\mathbb{L}} = \sigma$ entonces todo $\alpha \in \mathbb{L}$ define $\varphi(\alpha) = \sigma(\alpha)$ raíz de $\mu_\alpha^{\mathbb{K}}$ en $\varphi(\mathbb{M})$. Dado que $\mathbb{M}/\mathbb{K}$ extensión normal, $\mu_\alpha^{\mathbb{K}}$ escinde sobre $\varphi(\mathbb{M}) \subseteq \overline{\mathbb{K}}$ y luego $\tau(\mathbb{L}^n) \subseteq \varphi(\mathbb{M})$.
$\Rightarrow \varphi^{-1}\circ\tau : \mathbb{L}^n \hookrightarrow \mathbb{M}$ morfismo de $\mathbb{L}$-extensiones ✓ ■

Ejemplo (cf. Teoría de Galois clásica): Si $P \in \mathbb{Q}[X]$ irreducible y $Z(P) = \{\alpha \in \mathbb{C}, P(\alpha) = 0\}$, entonces $\mathbb{K}_P := \mathbb{Q}(Z(P)) \subseteq \mathbb{C}$ es un cuerpo de números y $\mathbb{K}_P/\mathbb{Q}$ extensión normal.

$\boxed{\text{Ejercicio}}$ Sea $\mathbb{L}/\mathbb{K}$ extensión con $[\mathbb{L}:\mathbb{K}] = 2$ (ie, cuadrática). Probar que $\mathbb{L}/\mathbb{K}$ es normal.

§8. Extensiones de Galois

Def: Una extensión algebraica $\mathbb{L}/\mathbb{K}$ es una extensión de Galois (o extensión galoisiana) si es una extensión separable y normal.

Prop: Sea $\mathbb{M}/\mathbb{K}$ una extensión algebraica y $\mathbb{L}_1, \mathbb{L}_2 \subseteq \mathbb{M}$ subextensiones. Si $\mathbb{L}_1/\mathbb{K}$ y $\mathbb{L}_2/\mathbb{K}$ son extensiones de Galois, entonces $\mathbb{L}_1 \cap \mathbb{L}_2/\mathbb{K}$ y $\mathbb{L}_1\mathbb{L}_2/\mathbb{K}$ también.

Ejemplos: ① Si $\mathrm{char}(\mathbb{K}) = 0$, Galois $\Longleftrightarrow$ Normal.

② Si $P \in \mathbb{Q}[X]$ irreducible y $Z(P) = \{\alpha \in \mathbb{C}, P(\alpha) = 0\}$, entonces $\mathbb{K}_P/\mathbb{Q}$ es una extensión de Galois, donde $\mathbb{K}_P = \mathbb{Q}(Z(P))$ cuerpo de números asociado a $Z(P)$.

$\boxed{\text{Ejercicio útil}}$ Probar que si $\mathbb{L}/\mathbb{K}$ es una extensión de cuerpos finitos, entonces es Galois.

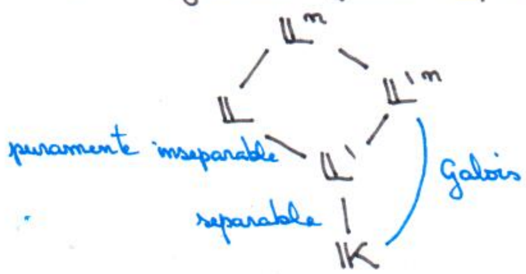
Ejemplo importante: Sea $\mathbb{K}^s$ la clausura separable de $\mathbb{K}$ relativa a $\overline{\mathbb{K}}$, llamada (una) clausura separable de $\mathbb{K}$. Entonces, $\mathbb{K}^s/\mathbb{K}$ es una extensión de Galois:

Para ver que $\mathbb{K}^s/\mathbb{K}$ es normal consideremos $\alpha \in \mathbb{K}^s$, donde $\mu_\alpha^{\mathbb{K}} \in \mathbb{K}[X]$ irreducible y separable. En part, toda raíz de $\mu_\alpha^{\mathbb{K}}$ en $\overline{\mathbb{K}}$ es separable$/\mathbb{K}$ y luego pertenece a $\mathbb{K}^s$ $\Rightarrow \mu_\alpha^{\mathbb{K}}$ escinde en $\mathbb{K}^s$ y concluimos que $\mathbb{K}^s$ es cuerpo de descomp. de $\{\mu_\alpha^{\mathbb{K}}\}_{\alpha \in \mathbb{K}^s}$ ✓

Prop: Sea $\mathbb{L}/\mathbb{K}$ extensión separable y sea $\mathbb{L}^n/\mathbb{L}$ la clausura normal de $\mathbb{L}/\mathbb{K}$. Entonces, $\mathbb{L}^n/\mathbb{K}$ es una extensión de Galois.

Dem: Sabemos que $\mathbb{L}^n/\mathbb{K}$ es una extensión normal (por definición). Para ver que es separable notar que $\mathbb{L}^n \overset{\text{def}}{=} \mathbb{K}(\{\beta \in \mathbb{L}^n, \exists\, \alpha \in \mathbb{L} \text{ tq } \mu_\alpha^{\mathbb{K}}(\beta) = 0\})$ y cada β es separable pues $\mu_\alpha^{\mathbb{K}}$ lo es (pues $\mathbb{L}/\mathbb{K}$ separable). ∎

Resumen: Toda extensión algebraica finita $\mathbb{L}/\mathbb{K}$ se descompone como



Def: Sea $\mathbb{L}/\mathbb{K}$ una extensión de Galois. El grupo de Galois de la extensión $\mathbb{L}/\mathbb{K}$ es

$$\mathrm{Gal}(\mathbb{L}/\mathbb{K}) := \{\sigma : \mathbb{L} \xrightarrow{\sim} \mathbb{L} \text{ automorfismo de cuerpos } \mathbb{K}\text{-lineal}\}$$

Prop: Sea $\mathbb{L}/\mathbb{K}$ extensión de Galois y sea $\tau_0 : \mathbb{L} \hookrightarrow \overline{\mathbb{K}}$ en $\Sigma_{\mathbb{L}/\mathbb{K}}$ fijo. Entonces,

$$\mathrm{Gal}(\mathbb{L}/\mathbb{K}) \xrightarrow{\sim} \Sigma_{\mathbb{L}/\mathbb{K}}, \quad \sigma \longmapsto \tau_0 \circ \sigma$$

es una biyección. En part, si $\mathbb{L}/\mathbb{K}$ es finita entonces $|\mathrm{Gal}(\mathbb{L}/\mathbb{K})| = [\mathbb{L} : \mathbb{K}]$.

Dem: La aplicación $\mathrm{Gal}(\mathbb{L}/\mathbb{K}) \times \Sigma_{\mathbb{L}/\mathbb{K}} \to \Sigma_{\mathbb{L}/\mathbb{K}}$, $(\sigma, \tau) \mapsto \tau \circ \sigma^{-1}$ define una acción (izquierda) $\mathrm{Gal}(\mathbb{L}/\mathbb{K}) \curvearrowright \Sigma_{\mathbb{L}/\mathbb{K}}$. El estabilizador de $\tau \in \Sigma_{\mathbb{L}/\mathbb{K}}$ es trivial pues (como τ inyectiva) $\sigma \cdot \tau = \tau \circ \sigma^{-1} = \tau \Rightarrow \sigma = \mathrm{Id}_{\mathbb{L}}$ ✓ Además, la acción es transitiva: si $\tau, \tau' \in \Sigma_{\mathbb{L}/\mathbb{K}}$ entonces $\tau(\mathbb{L}) = \tau'(\mathbb{L}) \subseteq \overline{\mathbb{K}}$ (pues $\mathbb{L}/\mathbb{K}$ normal!) y luego $\sigma := \tau'^{-1} \circ \tau : \mathbb{L} \xrightarrow{\sim} \mathbb{L}$ en $\mathrm{Gal}(\mathbb{L}/\mathbb{K})$ cumple $\tau = \tau' \circ \sigma$ ✓ (Rec: $G/G_x \simeq G \cdot x$) ∎

Teorema Fundamental de la Teoría de Galois: Sea $\mathbb{M}/\mathbb{K}$ una extensión de Galois finita. Entonces, hay una biyección estrictamente decreciente (resp. a la inclusión)

$$\{\mathbb{L}/\mathbb{K} \text{ subextensión de } \mathbb{M}\} \xrightarrow{\sim} \{\text{Subgrupos de } Gal(\mathbb{M}/\mathbb{K})\}$$
$$\mathbb{L} \longmapsto Gal(\mathbb{M}/\mathbb{L})$$
$$\mathbb{M}^H \longleftarrow H$$

Más aún, para toda subextensión $\mathbb{L}/\mathbb{K}$ de $\mathbb{M}$ y todo $\sigma \in Gal(\mathbb{M}/\mathbb{K})$ se tiene que $Gal(\mathbb{M}/\sigma(\mathbb{L})) = \sigma\, Gal(\mathbb{M}/\mathbb{L})\,\sigma^{-1}$ y luego $\mathbb{L}/\mathbb{K}$ ext. de Galois $\Leftrightarrow Gal(\mathbb{M}/\mathbb{L}) \trianglelefteq Gal(\mathbb{M}/\mathbb{K})$. Además, en este último caso $Gal(\mathbb{M}/\mathbb{K})/Gal(\mathbb{M}/\mathbb{L}) \xrightarrow{\sim} Gal(\mathbb{L}/\mathbb{K})$ es un isomorfismo, inducido por la restricción $Gal(\mathbb{M}/\mathbb{K}) \to Gal(\mathbb{L}/\mathbb{K})$, $\sigma \mapsto \sigma|_{\mathbb{L}}$.

Así, obtenemos un diccionario entre Teoría de Grupos y Teoría de Cuerpos:

Cuerpos	Grupos
Subextensiones $\mathbb{L}$ de $\mathbb{M}$	subgrupos H de $Gal(\mathbb{M}/\mathbb{K})$
$\mathbb{L}$	$Gal(\mathbb{M}/\mathbb{L})$
$\mathbb{M}^H$	H
$\mathbb{M}^{H_1} \subseteq \mathbb{M}^{H_2}$	$H_2 \leq H_1$
$[\mathbb{M}:\mathbb{L}]$	$\lvert Gal(\mathbb{M}/\mathbb{L})\rvert$
$[\mathbb{L}:\mathbb{K}]$	$[Gal(\mathbb{M}/\mathbb{K}) : Gal(\mathbb{M}/\mathbb{L})]$
$\mathbb{L}_1 \cap \mathbb{L}_2$	$\langle H_1 \cup H_2 \rangle$
$\mathbb{L}_1 \mathbb{L}_2$	$H_1 \cap H_2$
$\mathbb{L}/\mathbb{K}$ ext. de Galois	$H \trianglelefteq Gal(\mathbb{M}/\mathbb{K})$ subgrupo normal

Obs útiles: En el contexto del Teorema anterior, se tiene que:

① $\mathbb{M}/\mathbb{K}$ Galois $\Rightarrow \mathbb{M}/\mathbb{L}$ Galois y $Gal(\mathbb{M}/\mathbb{L}) \overset{\text{def}}{=} \{\sigma \in Gal(\mathbb{M}/\mathbb{K}) \text{ tq } \sigma|_{\mathbb{L}} = Id_{\mathbb{L}}\} \leq Gal(\mathbb{M}/\mathbb{K})$

② Si $H \leq Gal(\mathbb{M}/\mathbb{K})$ el cuerpo fijo de H

$$\mathbb{M}^H := \{\alpha \in \mathbb{M} \text{ tq } \sigma(\alpha) = \alpha \text{ para todo } \sigma \in H\}$$

es un subcuerpo de $\mathbb{M}$ y $\mathbb{K} \subseteq \mathbb{M}^H$.

③ Tanto $\mathbb{L} \mapsto Gal(\mathbb{M}/\mathbb{L})$ como $H \mapsto \mathbb{M}^H$ son decrecientes. Más aún, dado que $\lvert Gal(\mathbb{M}/\mathbb{L})\rvert = [\mathbb{M}:\mathbb{L}]$ se tiene que son estrictamente decrecientes ($\Rightarrow$ inyectivos ✓).

④ Si $\mathbb{L}/\mathbb{K}$ es una subextensión de $\mathbb{M}/\mathbb{K}$ y $\tau \in Gal(\mathbb{M}/\mathbb{K})$ entonces:

$$\begin{aligned} Gal(\mathbb{M}/\tau(\mathbb{L})) &\overset{\text{def}}{=} \{\sigma \in Gal(\mathbb{M}/\mathbb{K}) \text{ tq } \sigma(\tau(\alpha)) = \tau(\alpha)\ \forall \alpha \in \mathbb{L}\} \\ &= \{\sigma \in Gal(\mathbb{M}/\mathbb{K}) \text{ tq } (\tau^{-1}\circ\sigma\circ\tau)(\alpha) = \alpha\ \forall \alpha \in \mathbb{L}\} \\ &= \{\sigma \in Gal(\mathbb{M}/\mathbb{K}) \text{ tq } \tau^{-1}\circ\sigma\circ\tau \in Gal(\mathbb{M}/\mathbb{L})\} \overset{\text{def}}{=} \tau\, Gal(\mathbb{M}/\mathbb{L})\,\tau^{-1} \end{aligned}$$

Lema: Sea $\mathbb{L}/\mathbb{K}$ extensión de Galois, entonces $\mathbb{L}^{Gal(\mathbb{L}/\mathbb{K})} = \mathbb{K}$.

Dem: Por def, $\mathbb{K} \subseteq \mathbb{L}^{Gal(\mathbb{L}/\mathbb{K})}$. Sea $\alpha \in \mathbb{L}^{Gal(\mathbb{L}/\mathbb{K})}$ y fijemos $\tau_0 : \mathbb{L} \hookrightarrow \overline{\mathbb{K}}$ en $\Sigma_{\mathbb{L}/\mathbb{K}}$. Hay una aplicación sobreyectiva $Gal(\mathbb{L}/\mathbb{K}) \xrightarrow{\sim} \Sigma_{\mathbb{L}/\mathbb{K}} \twoheadrightarrow \Sigma_{\mathbb{K}(\alpha)/\mathbb{K}}$, $\sigma \mapsto (\tau_0\circ\sigma)|_{\mathbb{K}(\alpha)}$ donde $\Sigma_{\mathbb{K}(\alpha)/\mathbb{K}} \xrightarrow{\sim} \{\beta \in \overline{\mathbb{K}},\ \mu_\alpha^{\mathbb{K}}(\beta) = 0\}$, $\tau \mapsto \tau(\alpha)$. Dado que $\sigma(\alpha) = \alpha\ \forall \sigma \in Gal(\mathbb{L}/\mathbb{K})$ tenemos que $\tau_0(\alpha)$ es la única raíz de $\mu_\alpha^{\mathbb{K}}$ en $\overline{\mathbb{K}}$. Como $\mathbb{L}/\mathbb{K}$ es separable, esto implica que $\deg(\mu_\alpha^{\mathbb{K}}) = 1$, ie, $[\mathbb{K}(\alpha):\mathbb{K}] = 1$ y luego $\alpha \in \mathbb{K}$ ✓ ∎

Así, la biyectividad en el Teo. Fundamental de la Teoría de Galois es consecuencia de:

Teorema (Artin, 1942): Sea $\mathbb{M}$ un cuerpo y G un subgrupo finito del grupo $\mathrm{Aut}(\mathbb{M})$ de automorfismos de cuerpo de $\mathbb{M}$. Entonces, $\mathbb{M}/\mathbb{M}^G$ es una extensión de Galois con $\mathrm{Gal}(\mathbb{M}/\mathbb{M}^G) = G$, y en particular $[\mathbb{M}:\mathbb{M}^G] = |G|$.

Dem: Sea $\mathbb{L} := \mathbb{M}^G$. Sea $\alpha \in \mathbb{M}$ y sea $G\cdot\alpha \subseteq \mathbb{M}$ la órbita de α por G. Se define $P_\alpha := \prod_{\beta\in G\alpha}(X-\beta) \in \mathbb{M}[X]$ y notamos que $G \curvearrowright \mathbb{M}[X]$ por $\sigma(\sum a_iX^i) = \sum \sigma(a_i)X^i$
$\Rightarrow \mathbb{M}[X]^G = \{\sum a_iX^i \in \mathbb{M}[X] \text{ tq } \sigma(a_i)=a_i \ \forall \sigma\in G, \forall i\in\mathbb{N}\} \overset{\text{df}}{=} \mathbb{L}[X]$.

En particular, $\sigma(P_\alpha) = \prod_{\beta\in G\alpha}(X-\sigma(\beta)) = P_\alpha$ (pues $G\cdot\alpha \xrightarrow{\sim} G\cdot\alpha$, $\beta\mapsto\sigma(\beta)$ biyección) para todo $\sigma\in G$ y luego $P_\alpha \in \mathbb{L}[X]$, con $P_\alpha(\alpha)=0$ y donde todas las raíces de P_α tienen multiplicidad 1 en $\mathbb{M}$ $\Rightarrow \mu_\alpha^{\mathbb{L}} \mid P_\alpha$ tiene raíces simples y escinde en $\mathbb{M}$
$\Rightarrow$ Todo $\alpha\in\mathbb{M}$ es separable sobre $\mathbb{L}$ y $\mathbb{M}$ cuerpo de descomp. de $\{\mu_\alpha^{\mathbb{L}}\}_{\alpha\in\mathbb{M}}$, y luego $\mathbb{M}/\mathbb{L}$ es separable y normal, i.e., de Galois ✓ Por construcción, $G \subseteq \mathrm{Gal}(\mathbb{M}/\mathbb{L})$ ✓
Por otro lado: Para todo $\alpha\in\mathbb{M}$, $[\mathbb{L}(\alpha):\mathbb{L}] = \deg(\mu_\alpha^{\mathbb{L}}) \le \deg(P_\alpha) = |G\cdot\alpha| \le |G|$
Sea $\mathbb{L}\subseteq\mathbb{L}'\subseteq\mathbb{M}$ subcuerpo de $\mathbb{M}$. Si $\mathbb{L}'/\mathbb{L}$ es finita entonces, dado que $\mathbb{L}'/\mathbb{L}$ es separable (cf. §6, pág 14), $\exists\, \alpha\in\mathbb{L}'$ "elemento primitivo" con $\mathbb{L}' = \mathbb{L}(\alpha)$ y luego $[\mathbb{L}':\mathbb{L}] \le |G|$. Esto último implica que $\mathbb{M}/\mathbb{L}$ es finita y luego $[\mathbb{M}:\mathbb{L}] \le |G|$ (en caso contrario, $\exists \{\alpha_i\}_{i\in\mathbb{N}} \subseteq \mathbb{M}$ sucesión de elementos con $\alpha_i \notin \mathbb{L}(\alpha_0,\dots,\alpha_{i-1})$ y por ende $[\mathbb{L}(\alpha_0,\dots,\alpha_i):\mathbb{L}] \to +\infty$ con $i\to+\infty$ ↯ pues está acotado por $|G|$)
$\Rightarrow |\mathrm{Gal}(\mathbb{M}/\mathbb{L})| = [\mathbb{M}:\mathbb{L}] \le |G|$ y luego $G = \mathrm{Gal}(\mathbb{M}/\mathbb{L})$ ✓ ■

Dem del Teo Fundamental: Por todo lo anterior, sólo basta probar que si $\mathbb{K}\subseteq\mathbb{L}\subseteq\mathbb{M}$ (con $\mathbb{M}/\mathbb{K}$ Galois) entonces $\mathbb{L}/\mathbb{K}$ Galois $\iff \mathrm{Gal}(\mathbb{M}/\mathbb{L}) \trianglelefteq \mathrm{Gal}(\mathbb{M}/\mathbb{K})$:
Sup. $\mathbb{M} \overset{\tau_0}{\hookrightarrow} \overline{\mathbb{K}}$ en $\Sigma_{\mathbb{M}/\mathbb{K}}$ fijo. Entonces, $\mathbb{L}/\mathbb{K}$ Galois $\iff \tau(\mathbb{L}) = \tau_0(\mathbb{L}) \ \forall \tau\in\Sigma_{\mathbb{M}/\mathbb{K}}$
$\iff \forall\sigma\in\mathrm{Gal}(\mathbb{M}/\mathbb{K}),\ (\tau_0\circ\sigma)(\mathbb{L}) = \tau_0(\mathbb{L}) \iff \forall\sigma\in\mathrm{Gal}(\mathbb{M}/\mathbb{K}),\ \sigma(\mathbb{L}) = \mathbb{L}$
$\iff \forall\sigma\in\mathrm{Gal}(\mathbb{M}/\mathbb{K}),\ \mathrm{Gal}(\mathbb{M}/\sigma(\mathbb{L})) = \sigma\,\mathrm{Gal}(\mathbb{M}/\mathbb{L})\,\sigma^{-1} = \mathrm{Gal}(\mathbb{M}/\mathbb{L}) \overset{\text{df}}{\iff} \mathrm{Gal}(\mathbb{M}/\mathbb{L})$ normal
Por último, notamos que en tal caso $\mathrm{Gal}(\mathbb{M}/\mathbb{K}) \to \mathrm{Gal}(\mathbb{L}/\mathbb{K})$, $\sigma\mapsto\sigma|_{\mathbb{L}}$ es un morfismo de grupos con kernel $\mathrm{Gal}(\mathbb{M}/\mathbb{L})$ y que es sobreyectivo puesto que
$|\mathrm{Gal}(\mathbb{M}/\mathbb{K})/\mathrm{Gal}(\mathbb{M}/\mathbb{L})| = [\mathbb{M}:\mathbb{K}]/[\mathbb{M}:\mathbb{L}] = [\mathbb{L}:\mathbb{K}] = |\mathrm{Gal}(\mathbb{L}/\mathbb{K})|$ ✓ ■

Alternativamente, la sobreyectividad se puede deducir del siguiente resultado más general:

Prop útil: Sea $\mathbb{M}/\mathbb{K}$ extensión de Galois y $\mathbb{K}\subseteq\mathbb{L}\subseteq\mathbb{M}$ subextensión. Si $\sigma:\mathbb{L}\hookrightarrow\mathbb{M}$ es un morfismo de $\mathbb{K}$-extensiones, $\exists\, \tau\in\mathrm{Gal}(\mathbb{M}/\mathbb{K})$ tal que $\tau|_{\mathbb{L}} = \sigma$ (cf. Hahn-Banach)

Dem.: Sea $\tau_0 : \mathbb{M}\hookrightarrow\overline{\mathbb{K}}$ en $\Sigma_{\mathbb{M}/\mathbb{K}}$. Como $\Sigma_{\mathbb{M}/\mathbb{K}} \to \Sigma_{\mathbb{L}/\mathbb{K}}$, $\rho\mapsto\rho|_{\mathbb{L}}$ sobreyectivo, $\exists\, \rho : \mathbb{M}\hookrightarrow\overline{\mathbb{K}}$ en $\Sigma_{\mathbb{M}/\mathbb{K}}$ tq $\rho|_{\mathbb{L}} = \tau_0\circ\sigma : \mathbb{L}\hookrightarrow\overline{\mathbb{K}}$. Por otra parte, como $\mathbb{M}/\mathbb{K}$ es extensión de Galois, $\exists\, \tau\in\mathrm{Gal}(\mathbb{M}/\mathbb{K})$ tq $\rho = \tau_0\circ\tau \Rightarrow \rho|_{\mathbb{L}} = \tau_0\circ\tau|_{\mathbb{L}} = \tau_0\circ\sigma$ y así $\tau|_{\mathbb{L}} = \sigma$ ✓ ■

Una consecuencia importante de lo anterior es el hecho que el grupo de Galois actúa transitivamente en el conjunto de raíces de polinomios minimales:

Corolario: Sea $\mathbb{M}/\mathbb{K}$ una extensión de Galois y sea $\alpha\in\mathbb{M}$. Entonces: $\mathrm{Gal}(\mathbb{M}/\mathbb{K})\cdot\alpha = \{\beta\in\mathbb{M},\ \mu_\alpha^{\mathbb{K}}(\beta)=0\}$ y así $\mu_\alpha^{\mathbb{K}} = \prod_{\beta\in \mathrm{Gal}(\mathbb{M}/\mathbb{K})\cdot\alpha}(X-\beta)$ en $\mathbb{M}[X]$.

Dem: Tenemos que $\mathrm{Gal}(\mathbb{M}/\mathbb{K})\cdot\alpha\subseteq\{\beta\in\mathbb{M},\ \mu_\alpha^{\mathbb{K}}(\beta)=0\}$ pues $\sigma(\mu_\alpha^{\mathbb{K}}(\alpha))=\mu_\alpha^{\mathbb{K}}(\sigma(\alpha)) = 0$ $\forall\sigma\in\mathrm{Gal}(\mathbb{M}/\mathbb{K})$. Recíprocamente, si $\beta\in\mathbb{M}$ es tal que $\mu_\alpha^{\mathbb{K}}(\beta)=0$ entonces $\mathbb{K}(\alpha)\underset{\sigma}{\overset{\sim}{\rightarrow}}\mathbb{K}(\beta)$, $\alpha\mapsto\beta$ y la Prop. anterior implica que $\exists\tau\in\mathrm{Gal}(\mathbb{M}/\mathbb{K})$ tq $\tau|_{\mathbb{K}(\alpha)}=\sigma$, ie, $\beta=\tau(\alpha)$ ✓ Finalmente, dado que $\mu_\alpha^{\mathbb{K}}$ tiene una raíz en $\mathbb{M}$ entonces $\mu_\alpha^{\mathbb{K}}$ escinde en $\mathbb{M}$ (pues $\mathbb{M}/\mathbb{K}$ normal) con raíces simples ($\mathbb{M}/\mathbb{K}$ sep.) ∎

Corolario: Sea $\mathbb{M}/\mathbb{K}$ una extensión de Galois finita. Entonces, para todo $\alpha\in\mathbb{M}$ se tiene que $\chi_\alpha^{\mathbb{K}} = \prod_{\sigma\in\mathrm{Gal}(\mathbb{M}/\mathbb{K})}(X-\sigma(\alpha))$ y luego

$$\mathrm{Tr}_{\mathbb{M}/\mathbb{K}}(\alpha) = \sum_{\sigma\in\mathrm{Gal}(\mathbb{M}/\mathbb{K})}\sigma(\alpha) \quad \text{y} \quad N_{\mathbb{M}/\mathbb{K}}(\alpha) = \prod_{\sigma\in\mathrm{Gal}(\mathbb{M}/\mathbb{K})}\sigma(\alpha).$$

Dem: Notar que $\prod_{\sigma\in\mathrm{Gal}(\mathbb{M}/\mathbb{K})}(X-\sigma(\alpha)) = \prod_{\beta\in\mathrm{Gal}(\mathbb{M}/\mathbb{K})\cdot\alpha}(X-\beta)^{\mathrm{Card}(\{\sigma\in\mathrm{Gal}(\mathbb{M}/\mathbb{K}),\ \sigma(\alpha)=\beta\})}$

Por otro lado, la función $\mathrm{Gal}(\mathbb{M}/\mathbb{K})\twoheadrightarrow\mathrm{Gal}(\mathbb{M}/\mathbb{K})\cdot\alpha$, $\sigma\mapsto\sigma(\alpha)$ tiene fibras de cardinal $|\mathrm{Stab}(\alpha)|\overset{\text{def}}{=}|\{\sigma\in\mathrm{Gal}(\mathbb{M}/\mathbb{K}),\ \sigma(\alpha)=\alpha\}| = |\mathrm{Gal}(\mathbb{M}/\mathbb{K}(\alpha))| = [\mathbb{M}:\mathbb{K}(\alpha)]$

$\Rightarrow \prod_{\sigma\in\mathrm{Gal}(\mathbb{M}/\mathbb{K})}(X-\sigma(\alpha)) = \prod_{\beta\in\mathrm{Gal}(\mathbb{M}/\mathbb{K})\cdot\alpha}(X-\beta)^{[\mathbb{M}:\mathbb{K}(\alpha)]} = (\mu_\alpha^{\mathbb{K}})^{[\mathbb{M}:\mathbb{K}(\alpha)]} = \chi_\alpha^{\mathbb{K}}$ ✓ ∎

$\boxed{\text{Ejercicio}}$ Sea $\mathbb{K}=\mathbb{Q}(\sqrt{2})$. Calcular $\mathrm{Tr}_{\mathbb{K}/\mathbb{Q}}(\alpha)$ y $N_{\mathbb{K}/\mathbb{Q}}(\alpha)$ para todo $\alpha\in\mathbb{K}$.

Ejemplo importante: Sea $\mathbb{K}$ un cuerpo finito de $\mathrm{char}(\mathbb{K})=p>0$ de cardinal $q=p^n$. Sea $\mathbb{L}/\mathbb{K}$ una extensión finita de $[\mathbb{L}:\mathbb{K}]=d$. Entonces, $\mathbb{L}/\mathbb{K}$ es una extensión de Galois y $\mathrm{Gal}(\mathbb{L}/\mathbb{K})=\langle \mathrm{Fr}_q\rangle$ es cíclico con $\mathrm{Fr}_q:\mathbb{L}\to\mathbb{L}$, $a\mapsto a^q$:

En efecto, $\mathrm{Fr}_q=\mathrm{Fr}_{p^n}=(\mathrm{Fr}_p)^n$ es un automorfismo de $\mathbb{L}$ y para todo $k\in\{1,\dots,d\}$ se tiene $\mathbb{L}^{(\mathrm{Fr}_q)^k}\overset{\text{def}}{=}\{x\in\mathbb{L},\ x^{q^k}-x=0\}$ es un subcuerpo de cardinal $\leq q^k$.

Si $k=1$, entonces $\mathbb{K}\subseteq\mathbb{L}^{\mathrm{Fr}_q}$ y luego $\mathbb{K}=\mathbb{L}^{\mathrm{Fr}_q}$ ✓ ($\overset{\text{Artin}}{\Longrightarrow}$ $\mathbb{L}/\mathbb{K}$ Galois).

Además, si $k\in\{1,\dots,d-1\}$ entonces $\mathbb{L}^{(\mathrm{Fr}_q)^k}\neq\mathbb{L}$ y $\mathbb{L}^{(\mathrm{Fr}_q)^d}=\mathbb{L}$ (pues $|\mathbb{L}|=q^d$)

$\Rightarrow \mathrm{Fr}_q\in\mathrm{Gal}(\mathbb{L}/\mathbb{K})$ y $\mathrm{ord}(\mathrm{Fr}_q)=[\mathbb{L}:\mathbb{K}]=|\mathrm{Gal}(\mathbb{L}/\mathbb{K})|\Rightarrow\mathrm{Gal}(\mathbb{L}/\mathbb{K})=\langle\mathrm{Fr}_q\rangle$.

⚠ Sea $A\subseteq\mathbb{K}=\mathrm{Fr}(A)$ un dominio entero y $\mathbb{L}/\mathbb{K}$ extensión de Galois finita. Si $B:=\tilde{A}\subseteq\mathbb{L}$ es la clausura integral de A en $\mathbb{L}$ entonces $\sigma(B)=B$ para todo $\sigma\in\mathrm{Gal}(\mathbb{L}/\mathbb{K})$ (pues $\sigma(x^d+\sum a_i x^i)=\sigma(x)^d+\sum a_i\sigma(x)^i$ si $a_i\in A\subseteq\mathbb{K}$). Así, tenemos que $\mathrm{Gal}(\mathbb{L}/\mathbb{K})\curvearrowright B$.

$\boxed{\text{Ejercicio}}$ Sea $m\in\mathbb{N}^{\geq1}$ y $\xi_m:=e^{2\pi i/m}$ raíz primitiva de la unidad. Demostrar de manera rigurosa que hay un isomorfismo $\mathrm{Gal}(\mathbb{Q}(\xi_m)/\mathbb{Q})\cong(\mathbb{Z}/m\mathbb{Z})^*$ (cf. §5, pág 11). Usar lo anterior para calcular $N_{\mathbb{Q}(j)/\mathbb{Q}}$ y $\mathrm{Tr}_{\mathbb{Q}(j)/\mathbb{Q}}$ donde $j:=e^{2\pi i/3}$.

Parte II: Anillos de Dedekind y Valuaciones

§9. Recuerdos sobre Localización y Anillos Noetherianos

La construcción de $\mathbb{Q}$ a partir de $\mathbb{Z}$ se generaliza a anillos más generales:

Def: Sea A anillo conmutativo. Un subconjunto $S \subseteq A$ es *multiplicativo* si $1 \in S$ y si $a, b \in S$ entonces $ab \in S$. En tal caso, definimos en $A \times S$ la rel. de equivalencia

$$(a,s) \sim (a',s') \iff \exists t \in S \text{ tal que } t(as' - a's) = 0 \text{ en } A$$

La *localización* de A resp. a S es el anillo $A_S := (A \times S)/\sim$, donde $\frac{a}{s} := [(a,s)] \in A_S$

Obs: ① Notar que $0 \in S$ (ie, podemos "dividir por 0") $\iff A_S = 0$ (tomar $t = 0$!).

② La aplicación $i_S : A \to A_S$, $a \mapsto \frac{a}{1}$ permite ver A_S como A-álgebra, y $a \in \ker(i_S)$ $\iff \frac{a}{1} = \frac{0}{1}$ en $A_S \overset{\text{def}}{\iff} \exists t \in S$ tq $ta = 0$. En part, si $0 \notin S$ y si definimos $\mathrm{zdiv}(A) := \{a \in A \text{ tq } \exists b \neq 0 \text{ con } ab = 0\}$ entonces $i_S : A \hookrightarrow A_S$ inyectivo $\iff S \cap \mathrm{zdiv}(A) = \emptyset$.

Ejemplos más usados: Sea A un anillo y $S \subseteq A$ multiplicativo.

① Si $S = \{1\}$ entonces $A_S \cong A$.

② Si S dominio y $S = A \setminus \{0\}$ entonces $A_S \overset{\text{def}}{=} \mathrm{Fr}(A)$ cuerpo de fracciones. En part, si $T \subseteq A \setminus \{0\}$ multiplicativo $\Rightarrow A \overset{i_T}{\hookrightarrow} A_T \hookrightarrow \mathrm{Fr}(A)$ son subanillos.

③ Sea $\mathfrak{p} \subseteq A$ ideal primo $\overset{\text{def}}{\iff} S := A \setminus \mathfrak{p}$ multiplicativo. Entonces, la *localización* de A en $\mathfrak{p}$ es $A_\mathfrak{p} := A_S$, y así $\frac{a}{s} \in A_\mathfrak{p}$ si $a \in A$ y $s \notin \mathfrak{p}$.

④ Si $f \in A$ y $S = \{f^m\}_{m \in \mathbb{N}}$ entonces $A_f := A_S$ y $\frac{a}{f^m} \in A_f$ con $a \in A$ y $m \in \mathbb{N}$.

Hecho: Sea $S \subseteq A$ multiplicativo y $i_S : A \to A_S$ la localización corresp. Entonces:

① Para todo ideal $I \subseteq A$, tenemos $i_S(I) = \{\frac{a}{s} \text{ con } a \in I \text{ y } s \in S\}$.

② Para todo ideal $J \subseteq A_S$, tenemos $i_S(i_S^{-1}(J)) = J$.

③ Hay una biyección

$$\{\text{Ideales primos en } A_S\} \overset{1:1}{\longleftrightarrow} \{\text{Ideales primos } \mathfrak{p} \subseteq A \text{ con } \mathfrak{p} \cap S = \emptyset\}$$
$$\mathfrak{q} \longmapsto i_S^{-1}(\mathfrak{q})$$
$$i_S(\mathfrak{p}) \longleftarrow\!\shortmid \mathfrak{p}$$

Notación: Sea A anillo conmutativo. El *espectro* de A es $\mathrm{Spec}(A) := \{\mathfrak{p} \subseteq A \text{ ideal primo}\}$.

El conjunto $\mathrm{Spec}(A)$ se puede dotar de una *topología*:

$$X \subseteq \mathrm{Spec}(A) \text{ es \emph{cerrado}} \overset{\text{def}}{\iff} \exists I \subseteq A \text{ ideal tq } X = V(I) := \{\mathfrak{p} \in \mathrm{Spec}(A), I \subseteq \mathfrak{p}\}$$

Así, los *abiertos* son los $U_I := \mathrm{Spec}(A) \setminus V(I)$. Esta es la *topología de Zariski* de $\mathrm{Spec}(A)$.

Obs: ① Con esta notación, hay una biyección $\mathrm{Spec}(A_S) \overset{1:1}{\longleftrightarrow} \{\mathfrak{p} \in \mathrm{Spec}(A) \text{ tq } \mathfrak{p} \cap S = \emptyset\}$

② Si $\varphi : A \to B$ es un morfismo de anillos conmutativos, entonces

$$\varphi^* : \mathrm{Spec}(B) \to \mathrm{Spec}(A), \; \mathfrak{q} \mapsto \varphi^{-1}(\mathfrak{q})$$

está bien def (pues $A/\varphi^{-1}(\mathfrak{q}) \hookrightarrow B/\mathfrak{q}$ es inyectivo y $B/\mathfrak{q}$ es un *dominio*).

Ejemplo importante: Sea $\mathfrak{p} \subseteq A$ ideal primo y $i_\mathfrak{p} : A \to A_\mathfrak{p}$ localización en $\mathfrak{p}$. Si denotamos $IA_\mathfrak{p} := i_\mathfrak{p}(I)$ para todo $I \subseteq A$ ideal, entonces hay una biyección

$$\{\text{Ideales primos } \mathfrak{q} \subseteq A \text{ tq } \mathfrak{q} \subseteq \mathfrak{p}\} \xrightarrow{\sim} \{\text{Ideales primos en } A_\mathfrak{p}\}, \; \mathfrak{q} \mapsto \mathfrak{q}A_\mathfrak{p}$$

Def: Un anillo conmutativo A es un anillo local si posee un único ideal maximal $\mathfrak{m} \subseteq A$. El cuerpo $\kappa := A/\mathfrak{m}$ es el cuerpo residual de $(A, \mathfrak{m})$.

Ejemplo principal: Si $\mathfrak{p} \subseteq A$ ideal primo, entonces $A_\mathfrak{p}$ es un anillo local con ideal maximal $\mathfrak{p}A_\mathfrak{p} = \{\frac{a}{s}$ con $a \in \mathfrak{p}$ y $s \notin \mathfrak{p}\}$ y cuerpo residual $\kappa(\mathfrak{p}) := A_\mathfrak{p}/\mathfrak{p}A_\mathfrak{p}$:
En efecto, el ejemplo anterior implica que todo ideal primo de $A_\mathfrak{p}$ está contenido en $\mathfrak{p}A_\mathfrak{p}$ (pues $\mathfrak{q} \subseteq \mathfrak{p} \Rightarrow \mathfrak{q}A_\mathfrak{p} \subseteq \mathfrak{p}A_\mathfrak{p} \subsetneq A_\mathfrak{p}$) y luego $\mathfrak{p}A_\mathfrak{p}$ es el único ideal maximal ✓

Subejemplo: Si $A = \mathbb{Z}$, entonces:
i) Si $\mathfrak{p} = \langle 0 \rangle \Rightarrow A_\mathfrak{p} = \mathbb{Q}$ y $\kappa(\mathfrak{p}) = \mathbb{Q}$.
ii) Si $\mathfrak{p} = \langle p \rangle$ con p primo $\Rightarrow A_\mathfrak{p} = \{\frac{a}{b}$ con $a \in \mathbb{Z}$ y $p \nmid b\}$ y $\kappa(\mathfrak{p}) \cong \mathbb{F}_p$

Def: Sea A un anillo y M un A-módulo. Decimos que M es noetheriano si cumple alguna de las sgtes propiedades equivalentes:
① Todo submódulo $N \subseteq M$ es finitamente generado.
② Toda cadena creciente de submódulos de M
$$N_1 \subseteq N_2 \subseteq N_3 \subseteq \ldots \subseteq N_k \subseteq N_{k+1} \subseteq \ldots$$
es estacionaria, ie, $\exists\, \ell \geq 1$ tq $N_\ell = N_{\ell+1} = N_{\ell+2} = \ldots$ (ie, $N_m = N_\ell \ \forall m \geq \ell$)
③ Toda familia no-vacía de submódulos $\{N_\lambda\}_{\lambda \in \Lambda} \subseteq M$ posee un elemento maximal.

Obs/Recuerdo: Si $M = A$ es el A-módulo libre de rango 1, entonces un submódulo $I \subseteq A$ es lo mismo que un ideal de A.

Def: Un anillo A es noetheriano si el A-módulo $M = A$ es noetheriano, ie, las condiciones ①, ②, ③ se cumplen para ideales de A.

Prop: Sea A un anillo, M un A-módulo y $N \subseteq M$ un submódulo. Entonces,
$$M \text{ noetheriano} \iff N \text{ y } M/N \text{ son noetherianos}.$$

Corolario: Sea M un A-módulo y $\{N_i\}_{i=1,\ldots,r} \subseteq M$ familia finita de submódulos. Si N_i es noetheriano para todo $i \in \{1,\ldots,r\}$ entonces $\sum_{i=1}^{r} N_i \overset{\text{def}}{=} \langle N_1 \cup \ldots \cup N_r \rangle_{A\text{-mod}}$ también. Si $\{M_j\}_{j=1,\ldots,s}$ es una familia finita de A-módulos noetherianos, entonces la suma directa $\bigoplus_{j=1}^{s} M_j \simeq M_1 \times \ldots \times M_s$ también lo es.

$\boxed{\text{Ejercicio importante}}$ Sea A un anillo noetheriano. Probar que todo A-módulo finitamente generado M es noetheriano. [Indicación: $\exists\, A^n \twoheadrightarrow M$ sobreyectivo]

Ejemplos: ① Todo cuerpo $\mathbb{K}$ es noetheriano (pues $\langle 0 \rangle$ es el único ideal $\neq \mathbb{K}$).
② Todo anillo de ideales principales (eg. $\mathbb{Z}$ o $\mathbb{K}[X]$) es noetheriano.

Teorema (Hilbert): Sea A un anillo noetheriano, entonces $A[X]$ es noetheriano.

Prop: Sea $\varphi: A \twoheadrightarrow B$ un morfismo de anillos sobreyectivo. Entonces, si A es noetheriano entonces B es noetheriano.

$\boxed{\text{Ejercicio importante}}$ Sea A un anillo noetheriano y B una A-álgebra fin. generada. Entonces, B es un anillo noetheriano [Indicación: $\exists\, A[X_1,\ldots,X_m] \twoheadrightarrow B$ sobreyectivo].

Prop: Sea A anillo noetheriano y $S \subseteq A$ multiplicativo. Entonces, A_S es noetheriano.

Dem: La función $\{J \text{ ideal de } A_S\} \hookrightarrow \{I \text{ ideal de } A\}$, $J \mapsto i_S^{-1}(J)$ es inyectiva (pues $i_S(i_S^{-1}(J)) = J$) y creciente (pues $J_1 \subseteq J_2 \Rightarrow i_S^{-1}(J_1) \subseteq i_S^{-1}(J_2)$). Luego, toda cadena creciente de ideales en A_S induce una cadena en A, que por ende se estabiliza ∎

§10. Clausura integral en extensiones separables

Estudiar cuerpos de números nos obliga a analizar extensiones separables (no nec. de Galois).

Prop: Sea $\mathbb{L}/\mathbb{K}$ extensión finita separable. Entonces, para todo $\alpha \in \mathbb{L}$ se tiene
$$\mathrm{Tr}_{\mathbb{L}/\mathbb{K}}(\alpha) = \sum_{\sigma \in \Sigma_{\mathbb{L}/\mathbb{K}}} \sigma(\alpha) \text{ en } \overline{\mathbb{K}}.$$

Dem: Sea $Z := Z(\mu_\alpha^{\mathbb{K}}) = \{\beta \in \overline{\mathbb{K}},\ \mu_\alpha^{\mathbb{K}}(\beta) = 0\}$, entonces $\mathrm{Tr}_{\mathbb{L}/\mathbb{K}}(\alpha) = [\mathbb{L} : \mathbb{K}(\alpha)] \sum_{\beta \in Z} \beta$ en $\overline{\mathbb{K}}$. Así, basta notar que $\Sigma_{\mathbb{L}/\mathbb{K}} \twoheadrightarrow \Sigma_{\mathbb{K}(\alpha)/\mathbb{K}} \overset{\sim}{\longleftrightarrow} Z(\mu_\alpha^{\mathbb{K}})$, $\sigma \mapsto \sigma(\alpha)$ es sobreyectiva y todas sus fibras tienen cardinal $[\mathbb{L} : \mathbb{K}]_s / [\mathbb{K}(\alpha) : \mathbb{K}]_s = [\mathbb{L} : \mathbb{K}(\alpha)]_s = [\mathbb{L} : \mathbb{K}(\alpha)]$ ✓ ∎

Lema de Dedekind (independencia de caracteres): Sea G un grupo y $\mathbb{K}$ un cuerpo. Entonces, el grupo de caracteres $\mathrm{Hom}_{gr}(G, \mathbb{K}^*)$ es un conj. $\mathbb{K}$-l.i. de funciones de G en $\mathbb{K}$.

Dem: Sup que $\exists\ \lambda_1 \chi_1 + \ldots + \lambda_r \chi_r = 0$ con $\chi_i : G \to \mathbb{K}^*$ diferentes y con $(\lambda_1, \ldots, \lambda_r) \in \mathbb{K}^r \setminus \{0\}$. Asumamos $r \geq 2$ minimal, y luego $\lambda_i \neq 0\ \forall i$. Como $\chi_1 \neq \chi_2$, $\exists h \in G$ tq $\chi_1(h) \neq \chi_2(h)$. Además, notemos que:
$$\forall g \in G,\ \lambda_1 \chi_1(g) + \ldots + \lambda_r \chi_r(g) = 0 \ /\cdot \chi_1(h) \Rightarrow \lambda_1 \chi_1(g)\chi_1(h) + \ldots + \lambda_r \chi_r(g)\chi_1(h) = 0 \quad (*)$$
$$\Downarrow$$
$$\lambda_1 \chi_1(gh) + \ldots + \lambda_r \chi_r(gh) = 0 \iff \lambda_1 \chi_1(g)\chi_1(h) + \ldots + \lambda_r \chi_r(g)\chi_r(h) = 0 \quad (**)$$
$$\overset{(**)-(*)}{\Longrightarrow} \overbrace{\lambda_2 (\chi_2(h) - \chi_1(h))}^{\neq 0} \chi_2 + \ldots + \lambda_r (\chi_r(h) - \chi_1(h)) \chi_r \equiv 0 \ \lightning \ (r \text{ minimal!}) \ ∎$$

Corolario: Si $\mathbb{K}$ y $\mathbb{L}$ son cuerpos, el conjunto de funciones $\mathrm{Hom}_{cuerpos}(\mathbb{K}, \mathbb{L})$ es $\mathbb{L}$-l.i.

Dem: Considerar $G = \mathbb{K}^*$ y notar que $\varphi \in \mathrm{Hom}_{cuerpos}(\mathbb{K}, \mathbb{L})$ induce $\varphi : \mathbb{K}^* \to \mathbb{L}^*$ ∎

Corolario: Sea $\mathbb{L}/\mathbb{K}$ extensión finita separable de grado $d = [\mathbb{L} : \mathbb{K}]$ y sea $(e_1, \ldots, e_d)$ una $\mathbb{K}$-base de $\mathbb{L}$. Si escribimos $\Sigma_{\mathbb{L}/\mathbb{K}} = \{\sigma_1, \ldots, \sigma_d\}$ entonces $\det((\sigma_i(e_j))_{1 \leq i,j \leq d}) \neq 0$.

Dem: $\det((\sigma_i(e_j))_{1 \leq i,j \leq d}) = 0 \Rightarrow \exists (\lambda_1, \ldots, \lambda_d) \in \mathbb{K}^d \setminus \{0\}$ tq $\sum_{i=1}^d \lambda_i \sigma_i(e_j) = 0\ \forall j \in \{1, \ldots, d\}$
$\overset{(e_1, \ldots, e_d) \text{ base}}{\Longrightarrow} \lambda_1 \sigma_1 + \ldots + \lambda_d \sigma_d \equiv 0$, contradiciendo el Corolario anterior ∎

Teorema (Fórmula del discriminante): Sea $\mathbb{L}/\mathbb{K}$ extensión finita separable con $d = [\mathbb{L} : \mathbb{K}]$. Sea $(e_1, \ldots, e_d)$ una $\mathbb{K}$-base de $\mathbb{L}$ y sea $\Sigma_{\mathbb{L}/\mathbb{K}} = \{\sigma_1, \ldots, \sigma_d\}$, entonces:
$$\det((\mathrm{Tr}_{\mathbb{L}/\mathbb{K}}(e_i e_j))_{1 \leq i,j \leq d}) = \det((\sigma_i(e_j))_{1 \leq i,j \leq d})^2 \neq 0.$$

Dem: Sea $M := (\sigma_i(e_j))_{1 \leq i,j \leq d}$. Entonces, el coef. (i,j) de ${}^tMM$ está dado por
$$c_{ij} = \sum_{\sigma \in \Sigma_{\mathbb{L}/\mathbb{K}}} \sigma(e_i)\sigma(e_j) = \sum_{\sigma \in \Sigma_{\mathbb{L}/\mathbb{K}}} \sigma(e_i e_j) \overset{\text{Prop}}{=} \mathrm{Tr}(e_i e_j) \text{ pues } \mathbb{L}/\mathbb{K} \text{ finita separable} \ ∎$$

Lo anterior permite probar la sgte caracterización "numérica" de separabilidad:

Prop: Sea $\mathbb{L}/\mathbb{K}$ extensión finita de cuerpos. Son equivalentes:
1. $\mathbb{L}/\mathbb{K}$ es una extensión separable.
2. La forma bilineal $\mathrm{Tr}_{\mathbb{L}/\mathbb{K}} : \mathbb{L} \times \mathbb{L} \to \mathbb{K}$, $(x,y) \mapsto \mathrm{Tr}_{\mathbb{L}/\mathbb{K}}(xy)$ es no-degenerada.
3. $\mathrm{Tr}_{\mathbb{L}/\mathbb{K}} \neq 0$ (i.e. $\exists x \in \mathbb{L}$ tal que $\mathrm{Tr}_{\mathbb{L}/\mathbb{K}}(x) \neq 0$).

Dem: ① $\Rightarrow$ ② por la Fórmula del discriminante, y ② $\Rightarrow$ ③ ✓ Veamos ③ $\Rightarrow$ ① (contrarecíproco):

Sup. que $\mathbb{L}/\mathbb{K}$ no es separable, y sea $p = \mathrm{char}(\mathbb{K}) > 0$. Veamos que $\mathrm{Tr}_{\mathbb{L}/\mathbb{K}}(\alpha) = 0$ $\forall \alpha \in \mathbb{L}$: Sea $\alpha \in \mathbb{L}$ y $Z := \{\beta \in \overline{\mathbb{K}},\ \mu_\alpha^{\mathbb{K}}(\beta) = 0\}$. Escribamos $\mu_\alpha^{\mathbb{K}} = \left(\prod_{\beta\in Z}(X-\beta)\right)^{p^r}$ en $\overline{\mathbb{K}}[X]$ para cierto $r \geq 0$. Entonces, $\mathrm{Tr}_{\mathbb{L}/\mathbb{K}}(\alpha) = [\mathbb{L} : \mathbb{K}(\alpha)]\, p^r \sum_{\beta\in Z} \beta$ en $\overline{\mathbb{K}}$.

(a) Si α separable $/\mathbb{K}$ (ie, $r = 0$) $\Leftrightarrow$ $[\mathbb{K}(\alpha) : \mathbb{K}]_s = [\mathbb{K}(\alpha) : \mathbb{K}]$, y luego $[\mathbb{L} : \mathbb{K}]_i$ se escribe como $p^\alpha = [\mathbb{L} : \mathbb{K}]_i \overset{\text{def}}{=} [\mathbb{L} : \mathbb{K}]/[\mathbb{L} : \mathbb{K}]_s = [\mathbb{L} : \mathbb{K}(\alpha)]/[\mathbb{L} : \mathbb{K}(\alpha)]_s$ y en. p divide a $[\mathbb{L} : \mathbb{K}(\alpha)]$ $\Rightarrow$ $\mathrm{Tr}_{\mathbb{L}/\mathbb{K}}(\alpha) = 0$ ✓

(b) Si α no es separable $/\mathbb{K}$ (ie, $r \geq 1$) entonces $p^r > 1$ y luego $\mathrm{Tr}_{\mathbb{L}/\mathbb{K}}(\alpha) = 0$ ✓ ■

Teorema: Sea $A \subseteq \mathbb{K} = \mathrm{Fr}(A)$ dominio entero integralmente cerrado, sea $\mathbb{L}/\mathbb{K}$ extensión finita y $B = \tilde{A} \subseteq \mathbb{L}$ clausura integral de A en $\mathbb{L}$. Si $\mathbb{L}/\mathbb{K}$ es separable entonces $M_1 \subseteq B \subseteq M_2$ donde $M_1 \cong M_2 \cong A^d$ son A-módulos libres de rango $d = [\mathbb{L} : \mathbb{K}]$.

Dem: Para todo $x \in \mathbb{L}$ existe $a \in A\setminus\{0\}$ tal que $ax \in B$. Así, podemos escoger una base $(e_1, \dots, e_d)$ de $\mathbb{L}$ con $e_i \in B$. Por otra parte, dado que $\mathrm{Tr}_{\mathbb{L}/\mathbb{K}} : \mathbb{L}\times\mathbb{L} \to \mathbb{K}$ es no-degenerada, $\exists!$ base $(f_1, \dots, f_d)$ de $\mathbb{L}$ tal que $\mathrm{Tr}_{\mathbb{L}/\mathbb{K}}(e_i f_j) = \delta_{ij}$. "base dual".
Más generalmente, si $M \subseteq \mathbb{L}$ es un A-módulo entonces definimos el A-módulo

$$M^\vee := \{x \in \mathbb{L} \text{ tal que } \mathrm{Tr}_{\mathbb{L}/\mathbb{K}}(xy) \in A \text{ para todo } y \in M\}.$$

Así, $M \subseteq N$ implica que $N^\vee \subseteq M^\vee$ y $(\langle e_1, \dots, e_d\rangle_{A\text{-mod}})^\vee \overset{\text{def}}{=} \langle f_1, \dots, f_d\rangle_{A\text{-mod}}$.
Con esta notación, y dado que $\mathrm{Tr}_{\mathbb{L}/\mathbb{K}}(B) \subseteq A$, tenemos que $B \subseteq B^\vee$. Así, concluimos que $M_1 := \langle e_1, \dots, e_d\rangle_A \subseteq B \subseteq B^\vee \subseteq M_1^\vee = \langle f_1, \dots, f_d\rangle_A =: M_2$ con $M_1 \cong M_2 \cong A^d$ ✓ ■

Recuerdo / Hecho (Teorema de la base adaptada): Sea A un dominio de ideales principales (ie, todo ideal $I = \langle a\rangle \subseteq A$ está generado por 1 elemento) y sea $M \cong A^d$ un A-módulo libre de $\mathrm{rg}(M) = d$. Si $N \subseteq M$ submódulo, entonces $\exists r \in \mathbb{N}$ y $a_1, \dots, a_r \in A\setminus\{0\}$ tales que $a_1 | a_2 | \cdots | a_r$ y una base $(e_1, \dots, e_d)$ de M tq $(a_1 e_1, \dots, a_r e_r)$ es una base de N. En part, $N \cong A^r$ es libre de rango $r \leq d$.

Corolario: Siguiendo la notación e hipótesis del Teorema anterior, tenemos que:
① Si A es noetheriano, entonces B es noetheriano.
② Si A es un anillo de ideales principales, entonces $B \cong A^d$ es un A-módulo libre de rango $d = [\mathbb{L} : \mathbb{K}]$. Más aún, todo ideal fraccionario $\underset{\{0\}\neq}{I} \subseteq \mathbb{L}$ resp. a B es $\cong A^d$.

Dem: ① Como $B \subseteq M_2$ submódulo del A-módulo $M_2 \cong A^d$ fin. generado ($\Rightarrow M_2$ noetheriano) tenemos que B es un A-módulo noetheriano, y luego todo ideal ($\Leftrightarrow$ sub-B-módulo) $I \subseteq B$ es un A-módulo fin. generado, ie, $I = \langle b_1, \dots, b_q\rangle_{A\text{-mod}}$ $\Rightarrow$ $I = \langle b_1, \dots, b_q\rangle$ como ideal ✓
② Por el Teo. de la base adaptada $B \subseteq M_2 \cong A^d$ es libre y $\mathrm{rg}(M_1) = d \leq \mathrm{rg}(B) \leq \mathrm{rg}(M_2) = d$
$\Rightarrow B \cong A^d$ libre de rango d ✓
Más generalmente, si $I \subseteq \mathbb{L}$ ideal fraccionario resp. a B, entonces $\exists\, \alpha \in B\setminus\{0\}$ tal que $\alpha I \subseteq B \cong A^d$ y por def. de ideal fraccionario si $b \in I\setminus\{0\}$ se tiene $bB \subseteq I$. Así:

$$A^d \cong B \xrightarrow[\sim]{\cdot b} bB \subseteq I \subseteq \alpha^{-1}B \xrightarrow[\sim]{\cdot\alpha} B \cong A^d \underset{\text{adaptada}}{\overset{\text{Teo base}}{\Longrightarrow}} I \cong A^d \text{ es libre de } \mathrm{rg}(I) = d$$ ■

⚠ Consecuencia: Sea $A = \mathbb{Z}$ con $\mathrm{Fr}(\mathbb{Z}) = \mathbb{Q}$. Así, para todo cuerpo de números $\mathbb{K}/\mathbb{Q}$ el anillo de enteros $\mathcal{O}_{\mathbb{K}}$ es un $\mathbb{Z}$-módulo libre de rango $[\mathbb{K}:\mathbb{Q}]$. Más generalmente, todo ideal fraccionario no-nulo $I \subseteq \mathbb{K}$ (resp. a $\mathcal{O}_{\mathbb{K}}$) es un $\mathbb{Z}$-módulo libre de rango $d = [\mathbb{K}:\mathbb{Q}]$, i.e., $I \cong \mathbb{Z}^d$. En part, si $(e_1, \dots, e_d)$ es una $\mathbb{Z}$-base de $I \subseteq \mathbb{K}$ entonces $D_{\mathcal{O}_{\mathbb{K}}/\mathbb{Z}}(I) = \langle \det((\mathrm{Tr}_{\mathbb{K}/\mathbb{Q}}(e_i e_j))_{1 \le i,j \le d}) \rangle_{\mathbb{Z}\text{-mod}} \subseteq \mathbb{K}$.

§11. Anillos de Dedekind

Los anillos de Dedekind son una versión algebraica de variedades (suaves) de dimensión ≤ 1. Se puede probar que si C es una curva algebraica afín suave e irreducible sobre $\mathbb{C}$ (y luego C es una sup. de Riemann) entonces su anillo de funciones regulares $\mathcal{O}(C)$ es un ejemplo de un anillo de Dedekind. Veremos que $\mathcal{O}_{\mathbb{K}}$ también es un ejemplo!

Def: Un anillo conmutativo A es un anillo de Dedekind si verifica que:
① A es un dominio entero, noetheriano e integralmente cerrado; y además
② Todo ideal primo no-nulo $\mathfrak{p} \subseteq A$ es maximal.

Ejemplo: Sea A un dominio de ideales principales. Entonces, A es un dominio de factorización única (aquí, $a \mid b \Leftrightarrow \langle a \rangle \supseteq \langle b \rangle$) y luego A es integralmente cerrado (cf. §2). Dado que ② se verifica para dominios de ideales principales, A es un anillo de Dedekind. En part, $A = \mathbb{Z}$ y $A = \mathbb{K}$ cuerpo son anillos de Dedekind.

Observación: La dimensión de Krull de un anillo conmutativo A es

$$\dim_{\text{Krull}}(A) := \sup \left\{ n \in \mathbb{N},\ \begin{matrix}\exists\, \mathfrak{p}_0 \subsetneq \mathfrak{p}_1 \subsetneq \dots \subsetneq \mathfrak{p}_n \subsetneq A \\ \text{cadena de ideales primos en } A\end{matrix} \right\} \in \mathbb{N} \cup \{+\infty\}$$

Entonces:
① Si $\mathbb{K}$ es un cuerpo entonces $\dim_{\text{Krull}}(\mathbb{K}) = 0$. Más aún, $\dim_{\text{Krull}}(\mathbb{K}[x_1, \dots, x_n]) = n$ gracias a un resultado de Noether.
② Si A es un anillo de Dedekind $\overset{\text{cond } ②}{\Longrightarrow} \dim_{\text{Krull}}(A) \le 1$.

Def: Sea $A \subseteq \mathbb{K} = \mathrm{Fr}(A)$ un dominio entero. Sean $I, J \subseteq \mathbb{K}$ ideales fraccionarios (resp. a A), entonces definimos el producto de I y J como el ideal fraccionario

$$IJ := \left\{ \sum_{i=1}^{n} a_i b_i \ ;\ n \in \mathbb{N},\ a_i \in I \ \text{y}\ b_i \in J \right\} \subseteq \mathbb{K}.$$

Aquí, si a (resp. b) en $A \setminus \{0\}$ cumple $aI \subseteq A$ (resp. $bJ \subseteq A$) entonces $ab\,IJ \subseteq A$.

Obs: Si A es integralmente cerrado y $x, y \in \mathbb{K}$, entonces $\langle x \rangle \cdot \langle y \rangle = \langle xy \rangle \subseteq \mathbb{K}$.

Notación: Sea $A \subseteq \mathbb{K} = \mathrm{Fr}(A)$ un dominio entero. Denotamos por

$$\mathcal{I}(A) := \{ I \subseteq \mathbb{K} \text{ ideal fraccionario no-nulo} \}$$

que, dotado de la mult. de ideales, es un monoide conmutativo (ie, el producto es asociativo, conmutativo y tiene al ideal A como neutro). Denotamos por $\mathcal{P}r(A) \subseteq \mathcal{I}(A)$ al submonoide formado por ideales fraccionarios principales, ie, de la forma $\langle x \rangle$ con $x \in \mathbb{K}^*$.

Obs: Dado que todo ideal (usual) de A es un ideal fraccionario de $\mathbb{K}$, se tiene en particular que $\mathrm{Spec}(A)^* \overset{\text{def}}{=} \{ \mathfrak{p} \subseteq A \text{ ideal primo no-nulo} \}$ es un subconjunto de $\mathcal{I}(A)$.

Teorema (Grupo de clases de ideales): Sea A un anillo de Dedekind. Entonces:

① Para todo $I \in \mathcal{I}(A)$ existe una única función $\mathrm{Spec}(A)^* \to \mathbb{Z}$, $\mathfrak{p} \mapsto v_\mathfrak{p}(I)$ tal que:

(a) El conjunto $\{\mathfrak{p} \in \mathrm{Spec}(A)^*, v_\mathfrak{p}(I) \neq 0\}$ es finito.

(b) $I = \prod_{\mathfrak{p} \in \mathrm{Spec}(A)^*} \mathfrak{p}^{v_\mathfrak{p}(I)}$

② $\mathcal{I}(A)$ es un grupo, donde el inverso de $I \in \mathcal{I}(A)$ está dado por

$$I^{-1} := \{x \in \mathbb{K} = \mathrm{Fr}(A) \text{ tal que } xy \in A \text{ para todo } y \in I\}$$

En part, $\langle x\rangle^{-1} = \langle x^{-1}\rangle$ para $x \in \mathbb{K}^*$ y luego $\mathrm{Pr}(A) \subseteq \mathcal{I}(A)$ es un subgrupo.

El grupo abeliano cociente $\mathrm{Cl}(A) := \mathcal{I}(A)/\mathrm{Pr}(A)$ es el grupo de clases de ideales de A.

Cultura general (Geometría Algebraica): $\mathrm{Cl}(A) \cong \mathrm{Pic}(\mathrm{Spec}(A))$ "grupo de Picard".

Necesitamos de varios lemas previos para demostrar el Teorema anterior:

Lema 1: Sea $\mathfrak{p} \subseteq A$ un ideal primo de un anillo abeliano A. Sean $I_1, \dots, I_r \subseteq A$ ideales tal que $I_1 \cdots I_r \subseteq \mathfrak{p}$. Entonces, $\exists\, i \in \{1, \dots, r\}$ tal que $I_i \subseteq \mathfrak{p}$.

Dem: Sino, $I_i \not\subseteq \mathfrak{p}$ $\forall i$ y luego $\exists\, x_i \in I_i \setminus \mathfrak{p} \Rightarrow x_1 \cdots x_r \in I_1 \cdots I_r \subseteq \mathfrak{p} \underset{\mathfrak{p} \text{ primo}}{\Rightarrow} \exists\, x_j \in \mathfrak{p}$ ↯ ■

Lema 2: Sea $A \subseteq \mathbb{K} = \mathrm{Fr}(A)$ dominio entero y sea $I \subseteq \mathbb{K}$ ideal fraccionario no-nulo. Entonces, $I^{-1} = \{x \in \mathbb{K}, xy \in A \text{ para todo } y \in I\}$ es ideal fraccionario y $I^{-1}I = A$.

Dem: $I^{-1} \subseteq \mathbb{K}$ es un A-submódulo y todo $a \in I \setminus \{0\}$ cumple $aI^{-1} \subseteq A$ ✓ ■

Lema 3: Sea $A \subseteq \mathbb{K} = \mathrm{Fr}(A)$ dominio entero y sea $I \in \mathcal{I}(A)$ invertible, ie, $\exists\, J \in \mathcal{I}(A)$ tal que $IJ = A$. Entonces, $J = I^{-1}$.

Dem: Como $IJ = A$, $\forall x \in I$ y $\forall y \in J$ se tiene $xy \in A$, ie, $J \subseteq I^{-1}$. Así, tenemos que $A = IJ \subseteq II^{-1} \subseteq A$ ($\Rightarrow II^{-1} = I^{-1}I = A$) y así $I^{-1} = I^{-1}IJ = A \cdot J = J$ ■

Lema 4: Sea A un dominio entero noetheriano. Entonces, todo ideal no-nulo $I \subseteq A$ contiene un producto de ideales primos no-nulos.

Dem: Sea X el conjunto de ideales no-nulos en A que no contienen un producto de ideales primos no-nulos. Si $X \neq \emptyset$, al ser A noetheriano, entonces posee un elemento maximal $0 \neq I \subsetneq A$ que por hipótesis no es primo.

$\Rightarrow \exists\, x, y \notin I$ con $xy \in I$. Sea $I_1 := \langle I, x\rangle$ y $I_2 := \langle I, y\rangle$, con $I \subsetneq I_j$.

Como $I \in X$ maximal, $I_1, I_2 \notin X$ y luego $\exists\, \mathfrak{p}_1, \dots, \mathfrak{p}_r, \mathfrak{q}_1, \dots, \mathfrak{q}_s \in \mathrm{Spec}(A)$ no-nulos tal que $\mathfrak{p}_1 \cdots \mathfrak{p}_r \subseteq I_1$ y $\mathfrak{q}_1 \cdots \mathfrak{q}_s \subseteq I_2 \Rightarrow \mathfrak{p}_1 \cdots \mathfrak{p}_r \mathfrak{q}_1 \cdots \mathfrak{q}_s \subseteq I_1 I_2 \subseteq I$ ↯ ■

Lema 5: Sea A un anillo de Dedekind que no sea un cuerpo, y sea $\mathfrak{m} \subsetneq A$ ideal primo (ie, maximal) no-nulo. Entonces, $\mathfrak{m}\mathfrak{m}^{-1} = A$, ie, $\mathfrak{m} \in \mathcal{I}(A)$ es invertible.

Dem: Vimos que $\mathfrak{m}\mathfrak{m}^{-1} \subseteq A$ es un ideal y dado que $1 \in \mathfrak{m}^{-1} \subseteq \mathbb{K} = \mathrm{Fr}(A)$, $\mathfrak{m} \subseteq \mathfrak{m}\mathfrak{m}^{-1}$.

Dado que $\mathfrak{m}$ maximal, $\mathfrak{m}\mathfrak{m}^{-1} = \mathfrak{m}$ o $\mathfrak{m}\mathfrak{m}^{-1} = A$. Sup, por contradicción, $\mathfrak{m}\mathfrak{m}^{-1} = \mathfrak{m}$ y sea $x \in \mathfrak{m}^{-1} \subseteq \mathbb{K}$. Así, $x\mathfrak{m} \subseteq \mathfrak{m}$ y más aún $x^n \mathfrak{m} \subseteq \mathfrak{m}$ $\forall n \in \mathbb{N}$.

Por otro lado, si $d \in \mathfrak{m} \setminus \{0\}$ entonces $x^n d \in A$ y luego $d\, A[x] \subseteq A \overset{A \text{ noeth.}}{\Longrightarrow} A[x]$ fin. gen ie, $x \in \mathbb{K}$ es entero sobre A y luego $x \in A$ (pues A int. cerrado). Así, $A \underset{\text{def}}{\subseteq} \mathfrak{m}^{-1} \subseteq A$ y luego $\mathfrak{m}^{-1} = A$. Para llegar a una contradicción, construiremos $x \in \mathfrak{m}^{-1}$ con $x \notin A$:

Sea $d \in \mathfrak{m} \setminus \{0\} \overset{\text{Lema 4}}{\Longrightarrow} \exists\, \mathfrak{p}_1, \dots, \mathfrak{p}_r$ primos no-nulos, con r minimal, tal que $\mathfrak{p}_1 \cdots \mathfrak{p}_r \subseteq \langle d\rangle \subseteq \mathfrak{m}$

$\overset{\text{Lema 1}}{\Rightarrow} \exists\, i \in \{1,\dots,r\}$ tq $\mathfrak{p}_i \subseteq \mathfrak{m} \subsetneq A$; e.g. $\mathfrak{p}_1 \subseteq \mathfrak{m}$ y como $\mathfrak{p}_1$ maximal, $\mathfrak{p}_1 = \mathfrak{m}$.
Sea $I := \mathfrak{p}_2 \cdots \mathfrak{p}_r$, entonces $\mathfrak{p}_1 I = \mathfrak{m} I \subseteq \langle d \rangle$ y, como r minimal, $I \not\subseteq \langle d \rangle$.
Sea $c \in I \setminus \langle d \rangle \Rightarrow c\mathfrak{m} \subseteq \mathfrak{m} I \subseteq \langle d \rangle$ y así $\frac{c}{d}\mathfrak{m} \subseteq \langle \frac{d}{d} \rangle = \langle 1 \rangle \overset{\text{dy}}{=} A$, i.e., $\frac{c}{d} \in \mathfrak{m}^{-1}$
Sin embargo, $c \notin \langle d \rangle$ y luego $d \nmid c$ y así $\frac{c}{d} \notin A$ ↯ pues $\mathfrak{m}^{-1} = A$ ■

Lema 6: Sea A un anillo de Dedekind. Entonces, todo ideal no-nulo $I \subseteq A$ es el producto de ideales primos. Aquí, por convención : A es el producto de cero ideales primos.

Dem: Sea X el conj. de ideales no-nulos en A que no se escriben como producto de ideales primos. Si $X \neq \emptyset$, como A noetheriano, $\exists\, 0 \neq I \subsetneq A$ elemento maximal en X que por dy. no es un ideal primo (ie, no es maximal) $\Rightarrow \exists\, \mathfrak{m} \subsetneq A$ maximal tal que $I \subseteq \mathfrak{m}$.
$\Rightarrow I\mathfrak{m}^{-1} \subseteq \mathfrak{m}\mathfrak{m}^{-1} = A$ y $I \subseteq I\mathfrak{m}^{-1}$ (pues $1 \in \mathfrak{m}^{-1}$). Si $I\mathfrak{m}^{-1} = \prod_{j=1}^{r} \mathfrak{p}_j$ producto de primos entonces $I = I\mathfrak{m}\mathfrak{m}^{-1} = \mathfrak{m}\prod_{j=1}^{r}\mathfrak{p}_j$ también y luego $I\mathfrak{m}^{-1} \in X$. Como I maximal, entonces $I = I\mathfrak{m}^{-1}$. Finalmente, si $x \in \mathfrak{m}^{-1}$ y $d \in I \setminus \{0\} \subseteq \mathfrak{m} \setminus \{0\} \overset{\text{Lema 5}}{\Rightarrow} dA[x] \subseteq A$ y así $x \in A$
$\Rightarrow \mathfrak{m}^{-1} = A$ lo cual es una contradicción (cf. Lema 5). Así, $X = \emptyset$ ■

Recuerdo/Notación: Sea A un anillo conmutativo y M un A-módulo. Si Λ es un conjunto arbitrario, se define
$$M^{(\Lambda)} := \{ (m_\lambda)_{\lambda \in \Lambda} \in M^{\Lambda} \text{, el conj. } \{\lambda \in \Lambda,\ m_\lambda \neq 0\} \text{ es } \underline{\text{finito}} \} \overset{\text{dy}}{=} \bigoplus_{\lambda \in \Lambda} M$$

Dem del Teorema (Grupo de clases): Probemos primero la existencia y unicidad de la escritura como producto de primos para $I \in \mathcal{I}(A)$ ideal fraccionario no-nulo: sea $a \in A \setminus \{0\}$ tq $aI \subseteq A$ es un ideal y escribamos (por Lema 6) $\langle a \rangle = \mathfrak{p}_1 \cdots \mathfrak{p}_r$ y $aI = \mathfrak{q}_1 \cdots \mathfrak{q}_s$, y en particular (por Lema 5) $\langle a \rangle \cdot \mathfrak{p}_1^{-1} \cdots \mathfrak{p}_r^{-1} = A \Rightarrow I = \mathfrak{p}_1^{-1} \cdots \mathfrak{p}_r^{-1} \mathfrak{q}_1 \cdots \mathfrak{q}_s$ ✓
Para la unicidad, consideremos dos escrituras $\prod_{\mathfrak{p} \in \operatorname{Spec}(A)^*} \mathfrak{p}^{m_\mathfrak{p}} = \prod_{\mathfrak{p} \in \operatorname{Spec}(A)^*} \mathfrak{p}^{n_\mathfrak{p}}$ donde los conjuntos $\{\mathfrak{p},\ m_\mathfrak{p} \neq 0\}$ y $\{\mathfrak{p},\ n_\mathfrak{p} \neq 0\}$ son finitos, ie, $(m_\mathfrak{p})_\mathfrak{p}, (n_\mathfrak{p})_\mathfrak{p} \in \mathbb{Z}^{(\operatorname{Spec}(A)^*)}$.
Dado que cada $\mathfrak{p} \in \operatorname{Spec}(A)$ no-nulo es invertible (por Lema 5), podemos reacomodar los exponentes negativos y obtener $\mathfrak{p}_1^{m_1} \cdots \mathfrak{p}_r^{m_r} = \mathfrak{q}_1^{n_1} \cdots \mathfrak{q}_s^{n_s}$ para ciertos $m_i, n_i \in \mathbb{N}^{\geq 1}$ y donde $\{\mathfrak{p}_1, \dots, \mathfrak{p}_r\} \cap \{\mathfrak{q}_1, \dots, \mathfrak{q}_s\} = \emptyset$ (*). Podemos asumir que $r \geq s$ y que $r \geq 1$ es minimal.
Así, $\mathfrak{p}_1^{m_1} \cdots \mathfrak{p}_r^{m_r} \subseteq \mathfrak{p}_1$ y luego $\mathfrak{q}_1^{n_1} \cdots \mathfrak{q}_s^{n_s} \subseteq \mathfrak{p}_1 \subsetneq A$, por lo que $s \geq 1 \overset{\text{Lema 1}}{\Rightarrow} \exists\, \mathfrak{q}_i \subseteq \mathfrak{p}_1$
y como $\mathfrak{q}_i$ es máximal, deducimos que $\mathfrak{q}_i = \mathfrak{p}_1$, lo que contradice (*) ↯ Unicidad ✓
Por último, observamos que $\mathcal{I}(A)$ es un grupo pues si $I = \prod_{\mathfrak{p} \in \operatorname{Spec}(A)^*} \mathfrak{p}^{v_\mathfrak{p}(I)}$ entonces el producto $J = \prod_{\mathfrak{p} \in \operatorname{Spec}(A)^*} \mathfrak{p}^{-v_\mathfrak{p}(I)}$ es su inverso, ie, $J = I^{-1}$ (cf. Lemas 2, 3 y 5) ■

Consecuencia importante: Sea A un anillo de Dedekind. Entonces, hay un isomorfismo de grupos
$$\mathbb{Z}^{(\operatorname{Spec}(A)^*)} \xrightarrow{\sim} \mathcal{I}(A),\ (m_\mathfrak{p})_{\mathfrak{p} \in \operatorname{Spec}(A)^*} \longmapsto \prod_{\mathfrak{p} \in \operatorname{Spec}(A)^*} \mathfrak{p}^{m_\mathfrak{p}}$$
Más aún, si $\mathbb{K} = \operatorname{Fr}(A)$ entonces el homomorfismo de grupos
$$\mathbb{K}^* \longrightarrow \mathbb{Z}^{(\operatorname{Spec}(A)^*)},\ x \longmapsto (v_\mathfrak{p}(x))_{\mathfrak{p} \in \operatorname{Spec}(A)^*} \text{ donde } v_\mathfrak{p}(x) := v_\mathfrak{p}(\langle x \rangle)$$
tiene kernel A^* (las unidades de A). Así, obtenemos una sucesión exacta de grupos abelianos (ie, el kernel de cada flecha coincide con la imagen de la flecha anterior):
$$1 \longrightarrow A^* \longrightarrow \mathbb{K}^* \longrightarrow \mathbb{Z}^{(\operatorname{Spec}(A)^*)} \longrightarrow \mathcal{C}\ell(A) \overset{\text{dy}}{=} \mathcal{I}(A)/\mathcal{P}r(A) \longrightarrow 1$$

⚠ Observación importante: El isomorfismo $\mathbb{Z}^{(\operatorname{Spec}(A)^*)} \xrightarrow{\sim} \mathcal{I}(A),\ (m_\mathfrak{p})_{\mathfrak{p} \in \operatorname{Spec}(A)^*} \longmapsto \prod_{\mathfrak{p} \in \operatorname{Spec}(A)^*} \mathfrak{p}^{m_\mathfrak{p}}$ es una función decreciente respecto al orden parcial
$$(m_\mathfrak{p})_{\mathfrak{p} \in \operatorname{Spec}(A)^*} \leq (n_\mathfrak{p})_{\mathfrak{p} \in \operatorname{Spec}(A)^*} \overset{\text{dy}}{\Longleftrightarrow} m_\mathfrak{p} \leq n_\mathfrak{p} \text{ para todo } \mathfrak{p} \in \operatorname{Spec}(A)^*.$$

Lo anterior implica las siguientes fórmulas útiles:

(a) $I \subseteq J \iff v_{\mathfrak{p}}(I) \geq v_{\mathfrak{p}}(J)$ para todo $\mathfrak{p} \in \mathrm{Spec}(A)^*$.

(b) $I \subseteq A \iff v_{\mathfrak{p}}(I) \geq 0$ para todo $\mathfrak{p} \in \mathrm{Spec}(A)^*$.

(c) $v_{\mathfrak{p}}(I \cap J) = \max\{v_{\mathfrak{p}}(I), v_{\mathfrak{p}}(J)\}$.

(d) $v_{\mathfrak{p}}(I + J) = \min\{v_{\mathfrak{p}}(I), v_{\mathfrak{p}}(J)\}$ donde $I + J \overset{\text{def}}{=} \langle I, J\rangle_{A\text{-mód}} = \langle I \cup J\rangle_{A\text{-mód}}$.

<u>Recuerdo</u> (Teorema chino del resto): sea A anillo conmutativo y sean $I_1, \dots, I_r \subseteq A$ ideales tales que $I_i + I_j = A$ para todo $i \neq j$. Entonces, $\bigcap_{i=1}^{r} I_i = \prod_{i=1}^{r} I_i$ y hay un isomorfismo $A/I_1 \cdots I_r \xrightarrow{\sim} (A/I_1) \times \dots \times (A/I_r)$.

<u>Prop</u>: sea A un anillo de Dedekind y sea $I \subseteq A$ un ideal. Entonces, hay un isomorfismo de anillos $A/I \cong \prod_{\mathfrak{p} \in \mathrm{Spec}(A)} A/\mathfrak{p}^{v_{\mathfrak{p}}(I)}$.

<u>Dem</u>: Sean $\mathfrak{p}, \mathfrak{q} \subseteq A$ ideales primos con $\mathfrak{p} \neq \mathfrak{q}$ y $m = v_{\mathfrak{p}}(I)$, $n = v_{\mathfrak{q}}(I) \in \mathbb{N}^{\geq 1}$.
$\Rightarrow J := \mathfrak{p}^m + \mathfrak{q}^n$ cumple $v_{\mathfrak{r}}(J) = 0 \ \forall \mathfrak{r} \in \mathrm{Spec}(A)$ por (d), i.e., $J = A$ ✓ ■

§12. <u>Localización y extensión de Anillos de Dedekind</u>

<u>Teorema</u>: Sea A un anillo de Dedekind, $0 \notin S \subseteq A$ subconj. multiplicativo. Entonces, A_S es un anillo de Dedekind.

<u>Dem</u>: Como $0 \notin S$, $A_S \hookrightarrow \mathrm{Fr}(A)$ es un dominio entero. Además, A_S es noetheriano y la descripción explícita de ideales primos en A_S (ver §9) implica $\dim_{\mathrm{Krull}}(A_S) \leq 1$. Así, sólo basta verificar que A_S es integralmente cerrado:
Sea $x \in \mathrm{Fr}(A_S) = \mathrm{Fr}(A)$ elemento entero sobre A_S, i.e., $\exists a_i \in A$ y $\exists s_i \in S$ tales que se cumple $x^d + \sum_{i=0}^{d-1} \frac{a_i}{s_i} x^i = 0$. Sea $t := s_0 \cdots s_{d-1} \in S$ y sea $b_i := a_i \left(\prod_{j \neq i} s_j\right) t^{d-1-i} \in A$
$\Rightarrow (tx)^d + \sum_{i=0}^{d-1} b_i (tx)^i = 0$ y luego tx entero sobre A, i.e., $tx \in A \iff x \in A_S$ ■

<u>Lema</u>: Sea K un cuerpo y sea A una K-álgebra conmutativa de <u>dimensión finita</u>. Si A es un dominio (i.e., $xy = 0 \Rightarrow x = 0$ ó $y = 0$) entonces A es un cuerpo.

<u>Dem</u>: Sea $x \in A \setminus \{0\}$. Entonces $m_x : A \hookrightarrow A$, $y \mapsto xy$ es inyectivo $\overset{\dim_K(A) < +\infty}{\Longrightarrow} m_x$ sobreyectivo. Así, existe $y \in A$ tal que $xy = 1$ ■

<u>Teorema</u>: Sea $A \subseteq \mathbb{K} = \mathrm{Fr}(A)$ un anillo de Dedekind y sea $\mathbb{L}/\mathbb{K}$ una extensión <u>finita</u> y <u>separable</u>. Entonces, la clausura integral $B := \tilde{A} \subseteq \mathbb{L}$ es un anillo de Dedekind.

<u>Dem</u>: Por def, $B \subseteq \mathbb{L}$ es un dominio integralmente cerrado y sabemos que B es noetheriano. Así, basta verificar que todo ideal primo no-nulo $\mathfrak{q} \subseteq B$ es maximal, i.e., $B/\mathfrak{q}$ es un <u>cuerpo</u>:
Sea $\mathfrak{p} := \rho^{-1}_{\mathbb{L}/\mathbb{K}}(\mathfrak{q})$. Entonces, $\mathfrak{p} \overset{\text{def}}{=} \mathfrak{q} \cap \mathbb{K} = \mathfrak{q} \cap A \subseteq A$ (pues A int. cerrado) es un ideal primo de A, i.e., un ideal maximal de A puesto que $\mathfrak{p} \neq \langle 0 \rangle$ (si $x \in \mathfrak{q} \setminus \{0\}$ entonces $\mu_x^{\mathbb{K}} = X^d + \sum_{i=0}^{d-1} a_i X^i \in A[X] \Rightarrow \mu_x^{\mathbb{K}}(x) = 0$ y luego $a_0 \in \mathfrak{q} \setminus \{0\} \Rightarrow 0 \neq a_0 \in \mathfrak{p}$).
Así, $\kappa(\mathfrak{p}) := A/\mathfrak{p}$ es un cuerpo y hay un diagrama conmutativo

$$\begin{tikzcd} A \arrow[r, hook] \arrow[d] \arrow[dr, "\varphi"] & B \arrow[d] \\ A/\mathfrak{p} \arrow[r, "\exists!\, \bar{\varphi}"'] & B/\mathfrak{q} \end{tikzcd} \qquad \mathfrak{p} \subseteq \ker(\varphi)$$

Así, $B/\mathfrak{q}$ es una $\kappa(\mathfrak{p})$-álgebra y es un dominio pues $\mathfrak{q} \subseteq B$ ideal primo. Dado que B es un A-mód. noetheriano, $\exists (e_1, \dots, e_d)$ generadores $\Rightarrow B/\mathfrak{q}$ es un $\kappa(\mathfrak{p})$-e.v. de dim. <u>finita</u> generado por $([e_1], \dots, [e_d])$. Así, $B/\mathfrak{q}$ es un <u>cuerpo</u> (por Lema anterior) ✓ ■

Consecuencia: El Teorema anterior implica que si $\mathbb{K}/\mathbb{Q}$ es un cuerpo de números entonces el anillo de enteros $\mathcal{O}_{\mathbb{K}}$ es un anillo de Dedekind.

Obs práctica: Con la notación del Teorema anterior, notamos que la demostración implica que para todo $\mathfrak{q} \in \operatorname{Spec}(B)$ se tiene que $\mathfrak{p} := \mathfrak{q}|_{\mathbb{K}} = \mathfrak{q} \cap A \in \operatorname{Spec}(A)$ y que $B/\mathfrak{q}$ es una extensión finita de $A/\mathfrak{p}$.

Así, ideales primos en $\mathcal{O}_{\mathbb{K}}$ inducen ideales primos en $\mathbb{Z}$. Será de interés estudiar cuando ideales primos de $\mathbb{Z}$ inducen (o no) ideales primos en $\mathcal{O}_{\mathbb{K}}$.

Def/Prop: Sea $A \subseteq \mathbb{K} = \operatorname{Fr}(A)$ un anillo de Dedekind, sea $\mathbb{L}/\mathbb{K}$ una extensión finita separable y sea $B := \tilde{A} \subseteq \mathbb{L}$ la clausura integral de A. Si $I \subseteq \mathbb{K}$ es un ideal fraccionario resp. a A entonces IB, el B-submódulo de $\mathbb{L}$ generado por I, es un ideal fraccionario resp. a B y $\rho^*_{\mathbb{L}/\mathbb{K}} : \mathcal{I}(A) \longrightarrow \mathcal{I}(B)$, $I \longmapsto IB$ es un morfismo de grupos.

Dem: Sea $a \in A\setminus\{0\}$ tal que $aI \subseteq A$, entonces $aIB \subseteq A\cdot B = B$ ✓ Si $I, J \in \mathcal{I}(A)$ entonces $(IB)\cdot(JB) = IJB$ pues ambos son el B-mód generado por $\{xy \,;\, x \in I, y \in J\} \subseteq \mathbb{L}$ ■

Así, para entender la extensión de ideales primos de A a B (eg. de $\mathbb{Z}$ a $\mathcal{O}_{\mathbb{K}}$) necesitamos entender $\rho^*_{\mathbb{L}/\mathbb{K}}(\mathfrak{p})$ para $\mathfrak{p} \in \operatorname{Spec}(A)$.

Lema útil: Con la notación de la Definición anterior, si $\mathfrak{p} \in \operatorname{Spec}(A)$ y $\mathfrak{q} \in \operatorname{Spec}(B)$ entonces

$$v_{\mathfrak{q}}(\mathfrak{p}B) \geq 1 \iff \mathfrak{p} = \rho_{\mathbb{L}/\mathbb{K}}^{-1}(\mathfrak{q}) = \mathfrak{q} \cap A.$$

Dem: $v_{\mathfrak{q}}(\mathfrak{p}B) \geq 1 \overset{\text{def}}{\iff} \mathfrak{p}B \subseteq \mathfrak{q} \iff \rho_{\mathbb{L}/\mathbb{K}}(\mathfrak{p}) \subseteq \mathfrak{q} \iff \mathfrak{p} \subseteq \rho_{\mathbb{L}/\mathbb{K}}^{-1}(\mathfrak{q}) \overset{\mathfrak{p}\text{ maximal}}{\iff} \mathfrak{p} = \rho_{\mathbb{L}/\mathbb{K}}^{-1}(\mathfrak{q})$ ■

§13. Fórmula de Ramificación y Anillos de Valuación Discreta

Los resultados de la sección anterior motivan la sgte definición:

Def: Sea $A \subseteq \mathbb{K} = \operatorname{Fr}(A)$ anillo de Dedekind, $\mathbb{L}/\mathbb{K}$ extensión finita separable y $B := \tilde{A} \subseteq \mathbb{L}$ la clausura integral de A. Sea $\mathfrak{p} \in \operatorname{Spec}(A)^*$ y sea $\mathfrak{q} \in \operatorname{Spec}(B)^*$ entonces:

① Decimos que $\mathfrak{q} \mid \mathfrak{p}$ si $v_{\mathfrak{q}}(\mathfrak{p}B) > 0$ (ie, si $\mathfrak{p} = \mathfrak{q} \cap A$).

② Si $\mathfrak{q} \mid \mathfrak{p}$, entonces $f_{\mathfrak{q}} := [B/\mathfrak{q} : A/\mathfrak{p}] \in \mathbb{N}^{\geq 1}$ es el grado residual de $\mathfrak{q}$ sobre A.

③ El entero $e_{\mathfrak{q}} := v_{\mathfrak{q}}(\mathfrak{p}B) \in \mathbb{N}$ es el índice de ramificación de $\mathfrak{q}$ sobre A.

Notación: Sea A una κ-álgebra, donde κ es un cuerpo. Definimos $[A:\kappa] := \dim_{\kappa}(A)$. Nuestro ejemplo principal, con la notación de la Definición anterior, es $\kappa = \kappa(\mathfrak{p}) \overset{\text{def}}{=} A/\mathfrak{p}$ y $A = B/\mathfrak{p}B$: la composición $\varphi : A \hookrightarrow B \twoheadrightarrow B/\mathfrak{p}B$ cumple $\mathfrak{p} \subseteq \ker(\varphi)$ y luego $\exists!\ \hat{\varphi} : A/\mathfrak{p} = \kappa(\mathfrak{p}) \longrightarrow B/\mathfrak{p}B$. Así, $[B/\mathfrak{p}B : A/\mathfrak{p}] = \dim_{\kappa(\mathfrak{p})}(B/\mathfrak{p}B)$.

El objetivo de esta sección es probar el siguiente resultado, que permitirá extender la idea de ramificación en topología y superficies de Riemann a cuerpos de números:

Teorema (Fórmula de Ramificación): Sea $A \subseteq \mathbb{K} = \operatorname{Fr}(A)$ anillo de Dedekind, $\mathbb{L}/\mathbb{K}$ extensión finita separable y $B := \tilde{A} \subseteq \mathbb{L}$ la clausura integral de A. Entonces, para todo ideal primo $\mathfrak{p} \subseteq A$ no-nulo, se tiene que:

$$[\mathbb{L}:\mathbb{K}] = [B/\mathfrak{p}B : A/\mathfrak{p}] = \sum_{\mathfrak{q}\mid\mathfrak{p}} e_{\mathfrak{q}} f_{\mathfrak{q}}.$$

Para probarlo, necesitamos la noción de Anillo de Valuación Discreta (DVR, en inglés):

Def: Un anillo de valuación discreta es un anillo R que es un dominio entero, noetheriano e integralmente cerrado y que además posee un único ideal primo no-nulo $\mathfrak{m}_R$.

Ejemplo principal: Sea A un anillo de Dedekind y sea $\mathfrak{p} \in \mathrm{Spec}(A)$. Entonces, $A_\mathfrak{p}$ es un anillo de Dedekind y es un anillo local con único ideal maximal $\mathfrak{m}_\mathfrak{p} := \mathfrak{p} A_\mathfrak{p}$. Así, la localización $A_\mathfrak{p}$ de un anillo de Dedekind es un anillo de valuación discreta.

Obs clave: Todo anillo de valuación discreta R es un anillo de Dedekind. Más aún, $\mathrm{Spec}(R)^* = \{\mathfrak{p} \subseteq R$ ideal primo no-nulo$\} = \{\mathfrak{m}_R\}$. Así, hay un isomorfismo

$$v_{\mathfrak{m}_R} : \mathcal{I}(R) \xrightarrow{\sim} \mathbb{Z}, \quad I = \mathfrak{m}_R^n \longmapsto n$$

Def: Sea $\mathbb{K}$ un cuerpo. Una valuación discreta en $\mathbb{K}$ es una función $v : \mathbb{K} \to \mathbb{Z} \cup \{+\infty\}$ tal que se cumple:

(i) $v^{-1}(+\infty) = \{0\}$ (ie, $v(0) = +\infty$ y $v(x) \in \mathbb{Z}$ $\forall x \in \mathbb{K}^*$).

(ii) $v(xy) = v(x) + v(y)$ para todos $x, y \in \mathbb{K}$.

(iii) $v(x+y) \geq \min\{v(x), v(y)\}$ para todos $x, y \in \mathbb{K}$.

Aquí, $(+\infty) + \alpha := +\infty$ y $\min\{+\infty, \alpha\} := \alpha$.

Ejemplo importante: Sea R un anillo de valuación discreta y sea $\mathbb{K} = \mathrm{Fr}(R)$, entonces

$$v : \mathbb{K} \to \mathbb{Z} \cup \{+\infty\}, \; x \longmapsto \begin{cases} +\infty & \text{si } x = 0 \\ v_{\mathfrak{m}_R}(\langle x \rangle) & \text{si } x \neq 0 \end{cases}$$

es una valuación discreta. Más aún, $R = \{x \in \mathbb{K},\ v(x) \geq 0\}$.

Obs: ① Decimos que una valuación discreta $v : \mathbb{K} \to \mathbb{Z} \cup \{+\infty\}$ es trivial si $v(x) = 0$ para todo $x \in \mathbb{K}^*$. Si $v : \mathbb{K} \to \mathbb{Z} \cup \{+\infty\}$ es no-trivial entonces $v(\mathbb{K}^*) = d\mathbb{Z}$ para cierto $d \in \mathbb{N}^{\geq 1}$. Luego, $v' := \frac{1}{d} v : \mathbb{K} \twoheadrightarrow \mathbb{Z} \cup \{+\infty\}$ es una valuación discreta sobreyectiva.

② Sea $v : \mathbb{K} \twoheadrightarrow \mathbb{Z} \cup \{+\infty\}$ una valuación discreta (sobreyectiva) entonces

$$R_v := \{x \in \mathbb{K},\ v(x) \geq 0\}$$

es un subanillo de $\mathbb{K}$.

Lema: Sea $\mathbb{K}$ un cuerpo y sea $v : \mathbb{K} \to \mathbb{Z} \cup \{+\infty\}$ una valuación discreta. Entonces, R_v es un dominio euclideano con único ideal maximal $\mathfrak{m}_v := \{x \in \mathbb{K},\ v(x) > 0\}$. En part, si v es no-trivial entonces R_v es un anillo de valuación discreta.

Dem: Dado que $x \in \mathbb{K}$ pertenece a $R_v \Leftrightarrow v(x) \geq 0$, tenemos que $\forall a, b \in R_v$ se tiene $a | b$ en $R_v \Leftrightarrow x = \frac{b}{a} \in R_v \Leftrightarrow v(x) \geq 0 \Leftrightarrow v(b) = v(xa) = v(x) + v(a)$ con $v(b) \geq v(a)$.
Así, $a | b \Leftrightarrow v(b) \geq v(a) \geq 0$.
Notar que si v es trivial entonces $R_v = \mathbb{K}$ es euclideano ($\Leftarrow$ cuerpo) y $\mathfrak{m}_v \overset{\text{def}}{=} \langle 0 \rangle$ ✓
Sup. que v es no-trivial y veamos que $v : R_v \setminus \{0\} \to \mathbb{N}$ es una función euclideana, ie, $\forall a, b \in R_v$ con $b \neq 0$ existen $q, r \in R_v$ tal que $a = bq + r$ y $r = 0$ o bien $v(r) < v(b)$:
Si $v(a) < v(b)$ entonces $a = b \cdot 0 + a$ (ie, $q = 0, r = a$) y si $v(a) \geq v(b)$ entonces tenemos $a = b \cdot \frac{a}{b} + 0$ (ie, $q = \frac{a}{b} \in R_v$ y $r = 0$) ✓
Sea $I \subsetneq R_v$ un ideal y sup $I \neq \langle 0 \rangle$. Sea $d = \min\{v(I \setminus \{0\})\}$ y sea $a \in I$ tq $v(a) = d$.
$\Rightarrow v(a) \leq v(x)$ $\forall x \in I$, ie, $x \in \langle a \rangle$ y luego $I = \langle a \rangle = \{x \in \mathbb{K},\ v(x) \geq d\}$.
Así, $\mathfrak{m}_v := \{x \in \mathbb{K},\ v(x) \geq 1\}$ es el único ideal maximal de R_v ∎

⚠ Consecuencia: Todo anillo de valuación discreta es principal (DIP). Por ejemplo, si A es un anillo de Dedekind y $0 \neq \mathfrak{p} \subseteq A$ ideal primo, entonces $A_\mathfrak{p}$ es un DIP.

Ejemplo: Sea $p \in \mathbb{Z}$ un número primo. Dado $x \in \mathbb{Q}^*$ escribimos $x = \frac{a}{b}p^n$ con $a,b \in \mathbb{Z}$ tq $\mathrm{mcd}(a,b) = 1$ y con $p \nmid a$, $p \nmid b$. Definimos la valuación p-ádica $v_p : \mathbb{Q} \to \mathbb{Z} \cup \{+\infty\}$ como $v_p(x) = v_p\left(\frac{a}{b}p^n\right) := n \in \mathbb{Z}$.

$\boxed{\text{Ejercicio}}$ Probar que $R_v = \mathbb{Z}_{\langle p \rangle}$ y $\mathfrak{m}_v = p\mathbb{Z}_{\langle p \rangle}$.

Def: Sea $\mathbb{K}$ un cuerpo y sea $v : \mathbb{K} \twoheadrightarrow \mathbb{Z} \cup \{+\infty\}$ una valuación discreta sobreyectiva. Un parámetro local para v es cualquier $\pi \in \mathbb{K}$ tal que $v(\pi) = 1$ (ie, $\pi \in \mathfrak{m}_v$ y $\pi \notin \mathfrak{m}_v^2$). Así, $\mathfrak{m}_v = \langle \pi \rangle$ y todo ideal no-nulo en R_v es de la forma $\langle \pi^n \rangle$ con $n \in \mathbb{N}$.

Lema: Sea B un anillo de Dedekind y sea $\mathfrak{q} \in \mathrm{Spec}(B)$ no-nulo. Entonces, el cociente $\mathfrak{q}^n/\mathfrak{q}^{n+1}$ es un $B/\mathfrak{q}$-esp. vectorial de dimensión 1 para todo $n \in \mathbb{N}$.

Dem: El B-módulo $\mathfrak{q}^n/\mathfrak{q}^{n+1}$ cumple $\mathfrak{q} \subseteq \{b \in B \text{ tq } bx = 0 \ \forall x \in \mathfrak{q}^n/\mathfrak{q}^{n+1}\}$ y luego es un $B/\mathfrak{q}$-e.v. mediante $B/\mathfrak{q} \times \mathfrak{q}^n/\mathfrak{q}^{n+1} \to \mathfrak{q}^n/\mathfrak{q}^{n+1}$, $([\lambda],[x]) \mapsto [\lambda x]$. Más aún, los $B/\mathfrak{q}$-sub e.v. de $\mathfrak{q}^n/\mathfrak{q}^{n+1}$ son B-submódulos de $\mathfrak{q}^n/\mathfrak{q}^{n+1}$ y luego corresponden a B-submódulos $I \subseteq B$ (ie, ideales de B) tq $\mathfrak{q}^{n+1} \subseteq I \subseteq \mathfrak{q}^n$. Como B es un anillo de Dedekind, la factorización única de ideales implica que $I = \mathfrak{q}^n$ ó $I = \mathfrak{q}^{n+1}$, y luego $\mathfrak{q}^n/\mathfrak{q}^{n+1}$ sólo posee a $\{0\}$ y $\mathfrak{q}^n/\mathfrak{q}^{n+1}$ como sub-ev ✓ ∎

Volvamos al contexto de la Fórmula de Ramificación: $A \subseteq \mathbb{K} = \mathrm{Fr}(A)$ dominio de Dedekind, $\mathbb{L}/\mathbb{K}$ extensión finita separable y $B = \widetilde{A} \subseteq \mathbb{L}$ clausura integral de A. Dado $\mathfrak{p} \subseteq A$ ideal primo no-nulo, la estrategia será reducirnos al anillo de valuación discreta $A_\mathfrak{p}$ y en particular necesitamos comprender $\widetilde{A_\mathfrak{p}} \subseteq \mathbb{L}$ su clausura integral:

$$\begin{array}{ccccc} B & \hookrightarrow & \widetilde{A_\mathfrak{p}} & \hookrightarrow & \mathbb{L} \\ \uparrow & & \uparrow & & \uparrow \\ A & \hookrightarrow & A_\mathfrak{p} & \hookrightarrow & \mathbb{K} \end{array}$$

Lema: La clausura integral $\widetilde{A_\mathfrak{p}} \subseteq \mathbb{L}$ está dada por B_S, donde $S = A \setminus \mathfrak{p} \subseteq B$.

Dem: Sea $x \in \mathbb{L}$ entero sobre $A_\mathfrak{p}$. Entonces $x \in \mathbb{L}$ verifica una ecuación de la forma $x^d + \sum_{i=0}^{d-1} \frac{a_i}{s^{d-i}} x^i = 0$ con $a_i \in A$ y $s \in A \setminus \mathfrak{p}$ $\Rightarrow$ $(sx) \in \widetilde{A} = B$ y así $x \in B_S$ ∎

Dem. de la Fórmula de Ramificación:

Veamos primero que $[\mathbb{L} : \mathbb{K}] = [B/\mathfrak{p}B : A/\mathfrak{p}]$. Para reducirnos al caso local de anillos de valuación discreta, escribamos $A' := A_\mathfrak{p}$ y $B' := \widetilde{A_\mathfrak{p}} = B_S$ con $S = A \setminus \mathfrak{p}$.
Sabemos que A es anillo de Dedekind, por lo que
$$A'/\mathfrak{p}A' \overset{\text{def}}{=} A_\mathfrak{p}/\mathfrak{p}A_\mathfrak{p} \cong (A/\mathfrak{p})_{\mathfrak{p}A_\mathfrak{p}} \cong A/\mathfrak{p} \quad \text{pues } A/\mathfrak{p} \text{ es un cuerpo (!)}$$
Similar: $B'/\mathfrak{p}B' \cong (B/\mathfrak{p}B)_{\overline{S}}$ con $\overline{S} \subseteq B/\mathfrak{p}B$ la imagen de $S = A \setminus \mathfrak{p}$ en el cociente.
Dado que $\mathfrak{p} = \rho_{\mathbb{L}/\mathbb{K}}^{-1}(\mathfrak{p}B) = \mathfrak{p}B \cap A$, tenemos que $\mathfrak{p}B \cap S = \emptyset$ y luego $\overline{S}$ es invertible en $B/\mathfrak{p}B$ ($\boxed{\text{Ejercicio}}$). Así, $(B/\mathfrak{p}B)_{\overline{S}} \simeq B/\mathfrak{p}B$ y luego $B'/\mathfrak{p}B' \cong B/\mathfrak{p}B$.
$\Rightarrow$ Basta probar que $[\mathbb{L} : \mathbb{K}] = [B'/\mathfrak{p}B' : A'/\mathfrak{p}A']$:
Sea $d = [\mathbb{L} : \mathbb{K}]$. Entonces, B' es un A'-módulo libre de $\mathrm{rg}(B') = d$ y luego existe una base $(e_1, \ldots, e_d)$ de B' como A'-módulo. Sea $\pi \in \mathfrak{m}_{A'} \setminus \mathfrak{m}_{A'}^2$ parámetro local de A'.

Así, $m_{A'} = \mathfrak{p}A' = \langle \pi \rangle$ y $\mathfrak{p}B' = \pi B'$. Así, $(\pi e_1, \dots, \pi e_d)$ es una base de $\pi B'$
$\Rightarrow B'/\mathfrak{p}B' \simeq \bigoplus_{i=1}^{d} \langle \bar{e}_i \rangle_{A'/\mathfrak{p}A'}$ como $A'/\mathfrak{p}A'$ - módulo, y luego concluimos que
$[\mathbb{L} : \mathbb{K}] \overset{\text{dy}}{=} d = [B'/\mathfrak{p}B' : A'/\mathfrak{p}A'] = [B/\mathfrak{p}B : A/\mathfrak{p}A]$ ✓

Veamos que $[B/\mathfrak{p}B : A/\mathfrak{p}A] = \sum_{\mathfrak{q}|\mathfrak{p}} e_\mathfrak{q} f_\mathfrak{q}$: Por definición de índice de ramificación, se tiene que $\mathfrak{p}B = \prod_{\mathfrak{q}|\mathfrak{p}} \mathfrak{q}^{e_\mathfrak{q}} \Rightarrow B/\mathfrak{p}B \cong \prod_{\mathfrak{q}|\mathfrak{p}} B/\mathfrak{q}^{e_\mathfrak{q}}$ por el Teo. chino del Resto.

Sea $m \in \mathbb{N}^{\geq 1}$ y sea $\mathfrak{q} \in \operatorname{Spec}(B)^*$, entonces los $B/\mathfrak{q}$ - esp. vectoriales
$V_0 := B/\mathfrak{q}^m \supseteq V_1 := \mathfrak{q}/\mathfrak{q}^m \supseteq V_2 := \mathfrak{q}^2/\mathfrak{q}^m \supseteq \dots \supseteq V_m = \mathfrak{q}^m/\mathfrak{q}^m = \{0\}$

Cumplen $V_i/V_{i+1} \cong \mathfrak{q}^i/\mathfrak{q}^{i+1} \cong B/\mathfrak{q}$ (por un Lema anterior) $\Rightarrow \dim_{B/\mathfrak{q}}(B/\mathfrak{q}^{e_\mathfrak{q}}) = e_\mathfrak{q}$ ✓

De lo anterior, calculamos $[B/\mathfrak{p}B : A/\mathfrak{p}] = \sum_{\mathfrak{q}|\mathfrak{p}} e_\mathfrak{q} [B/\mathfrak{q} : A/\mathfrak{p}] \overset{\text{dy}}{=} \sum_{\mathfrak{q}|\mathfrak{p}} e_\mathfrak{q} f_\mathfrak{q}$ ■

<u>Obs útil</u>: Sea π un parámetro local para $A_\mathfrak{p}$, i.e., $\mathfrak{p}A_\mathfrak{p} = \langle \pi \rangle \subseteq A_\mathfrak{p}$.
Sea $\mathfrak{q} \in \operatorname{Spec}(B)^*$ tal que $\mathfrak{q}|\mathfrak{p}$. Por un lado, $\mathfrak{p}B_\mathfrak{q} = \pi B_\mathfrak{q}$. Por otro lado,
$\mathfrak{p}B_\mathfrak{q} = (\mathfrak{p}B) \cdot B_\mathfrak{q} = (\prod_{\mathfrak{r}|\mathfrak{p}} \mathfrak{r}^{e_\mathfrak{r}}) \cdot B_\mathfrak{q} = \mathfrak{q}^{e_\mathfrak{q}} B_\mathfrak{q} = (\mathfrak{q}B_\mathfrak{q})^{e_\mathfrak{q}}$.
$\Rightarrow e_\mathfrak{q} = v_{B_\mathfrak{q}}(\pi)$ donde $v_{B_\mathfrak{q}}$ es la valuación discreta de $(B_\mathfrak{q}, m_\mathfrak{q} = \mathfrak{q}B_\mathfrak{q})$.

<u>Ejemplo</u> (detalles más adelante): Sea $\mathbb{K} = \mathbb{Q}$ y $\mathbb{L} = \mathbb{Q}(i)$, con $A = \mathbb{Z}$ y $B = \mathcal{O}_{\mathbb{Q}(i)} = \mathbb{Z}[i]$
En $\mathbb{Z}[i]$, $2 = (1+i)(1-i)$ y $i(1-i) = i+1 \Rightarrow \langle 2 \rangle = \langle 1+i \rangle^2$. Así, $\mathfrak{p} = \langle 2 \rangle \subseteq \mathbb{Z}$ cumple $\mathfrak{p}B = \mathfrak{q}^2$ con $\mathfrak{q} = \langle 1+i \rangle \subseteq \mathbb{Z}[i]$ ideal primo ($\boxed{\text{Ejercicio}}$), con $N_{\mathbb{Q}(i)/\mathbb{Q}}(1+i) = 2$.
Así, la fórmula de Ramificación implica $[\mathbb{Q}(i) : \mathbb{Q}] = 2 = e_\mathfrak{q} f_\mathfrak{q} = 2 f_\mathfrak{q} \Rightarrow f_\mathfrak{q} = 1$, i.e.,
$f_\mathfrak{q} = [\mathbb{Z}[i]/\langle 1+i \rangle^2 : \mathbb{Z}/2\mathbb{Z}] = 1$ y luego $\mathbb{Z}[i]/\langle 1+i \rangle^2 \cong \mathbb{F}_2$.

<u>Ejemplo geométrico</u>: Sea X una superficie de Riemann compacta conexa y sea $f \in \mathbb{C}(X)$ función meromorfa no-constante, i.e., $f : X \twoheadrightarrow \mathbb{P}^1(\mathbb{C})$ holomorfa sobreyectiva.
$\Rightarrow f^* : \mathbb{C}(T) \simeq \mathbb{C}(\mathbb{P}^1(\mathbb{C})) \hookrightarrow \mathbb{C}(X)$, $P \mapsto P \circ f$ extensión de grado $\deg(f) = [\mathbb{C}(X) : \mathbb{C}(T)]$
Sea $A := \mathbb{C}[T] \subseteq \mathbb{C}(T)$ y sea $B := \tilde{A} \subseteq \mathbb{C}(X)$ clausura integral (resp. a f^*),
donde $f^*(T) \overset{\text{dy}}{=} f \in B$ y donde $g \in B \overset{\text{dy}}{\Longleftrightarrow} g^d + \sum_{i=0}^{d-1} a_i(f) g^i = 0$ en $\mathbb{C}(X)$ ciertos $a_i \in \mathbb{C}[T]$.

⚠ Cada punto $x \in X$ define una valuación discreta no-trivial:
$$v_x : \mathbb{C}(X) \to \mathbb{Z} \cup \{+\infty\}, \quad g \mapsto \begin{cases} +\infty & \text{si } g = 0 \\ \max\{n \in \mathbb{Z}, \ g(x)/\varphi(x)^n \in \mathbb{C}\} \end{cases}$$
donde $\varphi : \mathcal{U}_x \to \mathbb{C}$ es una carta local tq $\varphi(x)$. Así, $g \underset{\text{loc}}{\simeq} (z \mapsto z^{v_x})$ cerca de $x \in X$.

$\boxed{\text{Ejercicio}}$ Probar que $B \subseteq \{g \in \mathbb{C}(X), v_x(g) \geq 0\} \Leftrightarrow f(x) \neq \infty$ en $\mathbb{P}^1(\mathbb{C})$.
(<u>Hint</u>: Notar que $f(x) = \infty \Leftrightarrow v_x(f) < 0$).

<u>Recuerdo</u> (cf. Hilbert Nullstellensatz débil): $\mathbb{C} \xrightarrow{\sim} \operatorname{Spec}(\mathbb{C}[T])^*$, $a \mapsto \langle T-a \rangle$ es <u>biyectiva</u>.
Así, si $a \in \mathbb{C} \overset{\text{dy}}{=} \mathbb{P}^1(\mathbb{C}) \setminus \{\infty\}$ (con $\mathfrak{p}_a = \langle T - a \rangle \in \operatorname{Spec}(A)^*$) entonces la fibra $f^{-1}(a) \subseteq X$ es un conjunto <u>finito</u> y cada $x \in f^{-1}(a)$ admite una carta local tal que $f \underset{\text{loc}}{\simeq} (z \mapsto z^{e_x})$ cerca de $x \in X$, con $e_x \in \mathbb{N}^{\geq 1}$. $\Rightarrow d = \deg(f) = \sum_{x \in f^{-1}(a)} e_x$.
Por otra parte, $[\mathbb{C}(X) : \mathbb{C}(T)] \overset{\text{Ram.}}{=} \sum_{\mathfrak{q}|\mathfrak{p}_a} e_\mathfrak{q} f_\mathfrak{q}$ donde $f_\mathfrak{q} \overset{\text{dy}}{=} [B/\mathfrak{q} : \underbrace{\mathbb{C}[T]/\langle T-a \rangle}_{\cong \mathbb{C} \text{ alg. cerrado!}}] = 1$

<u>Hecho</u>: Para todo $\mathfrak{q} \in \operatorname{Spec}(B)^*$ tal que $\mathfrak{q}|\mathfrak{p}_a$ existe $x \in f^{-1}(a)$ tal que $\mathfrak{q} = \{g \in B, v_x(g) > 0\}$
Más aún, $v_{B_\mathfrak{q}} = v_x$ y $e_\mathfrak{q} = e_x \Rightarrow [\mathbb{C}(X) : \mathbb{C}(T)] = \sum_{x \in f^{-1}(a)} e_x$ ✓

§14. Discriminante y Ramificación

En esta sección, $A \subseteq \mathbb{K} = \mathrm{Fr}(A)$ es un anillo de Dedekind, $\mathbb{L}/\mathbb{K}$ es una extensión finita y separable, y $B = \widetilde{A} \subseteq \mathbb{L}$ es la clausura integral de A.

Def: Sea $\mathfrak{p} \in \mathrm{Spec}(A)^*$ y sea $\mathfrak{q} \in \mathrm{Spec}(B)^*$ tal que $\mathfrak{q} | \mathfrak{p}$. Decimos que $\mathfrak{q}$ es no-ramificado en $\mathbb{L}/\mathbb{K}$ si $e_{\mathfrak{q}} = 1$ y $B/\mathfrak{q}$ es separable sobre $A/\mathfrak{p}$. En caso contrario, decimos que $\mathfrak{q}$ ramifica sobre $\mathbb{L}/\mathbb{K}$.

⚠ Si $\mathrm{char}(A/\mathfrak{p}) = 0$ o si $A/\mathfrak{p}$ es un cuerpo finito (eg. si $A = \mathcal{O}_{\mathbb{K}}$ anillo de enteros de un cuerpo de números $\mathbb{K}$) entonces $(B/\mathfrak{q})/(A/\mathfrak{p})$ es automáticamente separable.

El resultado principal de esta sección es el siguiente:

Teorema: Sea $\mathfrak{p} \in \mathrm{Spec}(A)^*$. Entonces, son equivalentes:

① Existe $\mathfrak{q} \in \mathrm{Spec}(B)^*$ con $\mathfrak{q} | \mathfrak{p}$ y tal que $\mathfrak{q}$ ramifica en $\mathbb{L}/\mathbb{K}$.

② $\mathfrak{p}$ divide a $d_{B/A} \subseteq A$.

En part, hay finitos $\mathfrak{q} \in \mathrm{Spec}(B)^*$ que ramifican en $\mathbb{L}/\mathbb{K}$.

Ejemplo (cf. P. Samuel §2.5): Sea $\mathbb{K} = \mathbb{Q}(\sqrt{d})$ con $d \in \mathbb{Z}$ libre de cuadrados. Entonces,

$$\mathcal{O}_{\mathbb{K}} = \begin{cases} \{a + b\sqrt{d} \,;\, a, b \in \mathbb{Z}\} & \text{si } d \equiv 2 \text{ o } 3 \pmod 4 \\ \{\frac{1}{2}(a + b\sqrt{d}) \,;\, a, b \in \mathbb{Z}\} & \text{si } d \equiv 1 \pmod 4 \end{cases} \quad \text{y} \quad d_{\mathbb{K}} = \begin{cases} 4d & \text{si } d \equiv 2 \text{ o } 3 \pmod 4 \\ d & \text{si } d \equiv 1 \pmod 4 \end{cases}$$

Por ejemplo, si $d = -1$ ($\equiv 3 \bmod 4$) y $\mathbb{K} = \mathbb{Q}(i)$ entonces $d_{\mathbb{K}} = -4 = -2^2$. Así, $\mathfrak{p} = \langle 2 \rangle \subseteq \mathbb{Z}$ y $\mathfrak{p}\mathcal{O}_{\mathbb{K}} = \mathfrak{q}^2$ con $\mathfrak{q} = \langle 1 + i \rangle \subseteq \mathcal{O}_{\mathbb{K}}$ ideal primo ramificado.

Recuerdo: Sea k un anillo conmutativo y $R \simeq k^d$ una k-álgebra que es un k-módulo libre de rango finito. Dado $\alpha \in R$, la aplicación $m_\alpha : R \to R$, $x \mapsto \alpha x$ es k-lineal y se definen $\chi_\alpha^k := \chi_{m_\alpha}$, $\mathrm{Tr}_{R/k}(\alpha) := \mathrm{Tr}(m_\alpha)$ y $N_{R/k}(\alpha) := \det(m_\alpha)$.

Lema 1: Sea $\mathfrak{p} \in \mathrm{Spec}(A)^*$, entonces el diagrama

$$\begin{tikzcd} B \arrow[r, two heads] \arrow[d, "\mathrm{Tr}_{\mathbb{L}/\mathbb{K}}"'] & B/\mathfrak{p}B \arrow[d, "\mathrm{Tr}_{(B/\mathfrak{p}B)/(A/\mathfrak{p})}"] \\ A \arrow[r, two heads] & A/\mathfrak{p} \end{tikzcd}$$

es conmutativo, ie, $[\mathrm{Tr}_{\mathbb{L}/\mathbb{K}}(\alpha)] = \mathrm{Tr}_{(B/\mathfrak{p}B)/(A/\mathfrak{p})}([\alpha])$ en $A/\mathfrak{p}$ para todo $\alpha \in B$.

Dem: Recordemos (cf. §13, pág 32) que si $A_{\mathfrak{p}} =: A' \subseteq \mathbb{K}$ entonces $B' := \widetilde{A_{\mathfrak{p}}} \subseteq \mathbb{L}$ coincide con la localización B_S, donde $S = A \setminus \mathfrak{p} \subseteq B$. Además, $A/\mathfrak{p} \xrightarrow{\sim} A'/\mathfrak{p}A'$ y $B/\mathfrak{p}B \xrightarrow{\sim} B'/\mathfrak{p}B'$, ie, basta probar el resultado para A' y B':

Dado que A' es principal, sabemos que $B' = \widetilde{A'} \simeq A'^d$ es libre con base $(e_1, \ldots, e_d)$.
$\Rightarrow ([e_1], \ldots, [e_d])$ es una $A/\mathfrak{p}$-base de $B'/\mathfrak{p}B'$. Luego, para todo $\alpha \in B$ tenemos que $[\mathrm{Mat}_{(e_1, \ldots, e_d)}(m_\alpha)] = \mathrm{Mat}_{([e_1], \ldots, [e_d])}(m_{[\alpha]})$ y concluimos tomando la traza ∎

Lema 2: Sea k un cuerpo y $R \simeq k^d$ una k-álgebra de dimensión finita. Sea $\alpha \in R$ nilpotente, entonces $\mathrm{Tr}_{R/k}(\alpha\beta) = 0$ para todo $\beta \in R$.

Dem: Sea $n \in \mathbb{N}^{\geq 1}$ tq $\alpha^n = 0 \Rightarrow (\alpha\beta)^n = 0$ y luego $(m_{\alpha\beta})^n = m_{(\alpha\beta)^n} = 0$, ie, $m_{\alpha\beta}$ es un endomorfismo nilpotente $\Rightarrow \mathrm{Tr}(m_{\alpha\beta}) = 0$ ✓ ∎

Lema 3: Sea k un cuerpo y sean R_1, R_2 k-álgebras de dimensión finita. Entonces, para todo $(x,y) \in R_1 \times R_2$ se tiene $Tr_{R_1\times R_2/k}((x,y)) = Tr_{R_1/k}(x) + Tr_{R_2/k}(y)$. Más aún, la forma bilineal asociada $tr_{R_1\times R_2/k}$ es degenerada $\Leftrightarrow$ $tr_{R_1/k}$ degenerada o $tr_{R_2/k}$ degenerada.

Obs: Aquí, $tr_{R/k} : R\times R \to k$, $(\alpha,\beta) \mapsto Tr_{R/k}(\alpha\beta)$.

Dem: Sea $\mathcal{B}$ base de R_1 y $\mathcal{C}$ base de R_2 como k-ev. Así, $(\mathcal{B},\mathcal{C})$ base de $R_1\times R_2$
$\Rightarrow Mat_{(\mathcal{B},\mathcal{C})}(m_{(x,y)}) = \begin{pmatrix} Mat_{\mathcal{B}}(m_x) & 0 \\ 0 & Mat_{\mathcal{C}}(m_y)\end{pmatrix}$ y $Mat_{(\mathcal{B},\mathcal{C})}(tr_{R_1\times R_2/k}) = \begin{pmatrix} Mat_{\mathcal{B}}(tr_{R_1/k}) & 0 \\ 0 & Mat_{\mathcal{C}}(tr_{R_2/k})\end{pmatrix}$ ∎

Dem del Teorema: Sea $k = A/\mathfrak{p}$ y sea $R = B/\mathfrak{p}B$. Probemos que $\exists\, \mathfrak{q} \in Spec(B)^*$ con $\mathfrak{q}|\mathfrak{p}$ y tal que $\mathfrak{q}$ ramifica en $\mathbb{L}/\mathbb{K}$ $\Leftrightarrow$ $tr_{R/k}: R\times R \to k$ es degenerada:
Dado que $R = \prod_{\mathfrak{q}|\mathfrak{p}} B/\mathfrak{q}^{e_\mathfrak{q}}$, el Lema 3 nos reduce a probar que $\exists\, \mathfrak{q}|\mathfrak{p}$ tal que la forma bilineal $tr_{(B/\mathfrak{q}^{e_\mathfrak{q}})/(A/\mathfrak{p})}$ es degenerada. Hay 3 casos:

(1°) Si $e_\mathfrak{q} \geq 2$: sea $x \in \mathfrak{q}/\mathfrak{q}^{e_\mathfrak{q}}$ no-nulo $\Rightarrow x^{e_\mathfrak{q}} = 0$ en $B/\mathfrak{q}^{e_\mathfrak{q}}$, i.e., x es un elemento nilpotente $\neq 0$ y luego $tr_{(B/\mathfrak{q}^{e_\mathfrak{q}})/(A/\mathfrak{p})}$ es degenerada por el Lema 2 ✓

(2°) Si $e_\mathfrak{q} = 1$ pero $(B/\mathfrak{q})/(A/\mathfrak{p})$ no es separable: $tr_{(B/\mathfrak{q})/(A/\mathfrak{p})} \equiv 0$ ✓ } visto antes!

(3°) Si $e_\mathfrak{q} = 1$ y $(B/\mathfrak{q})/(A/\mathfrak{p})$ separable: $tr_{(B/\mathfrak{q})/(A/\mathfrak{p})}$ no-degenerada ✓

Así, resta probar que $tr_{R/k}$ degenerada $\Leftrightarrow$ $\mathfrak{p}$ divide a $d_{B/A} \subseteq A$:
Si $tr_{R/k}$ es degenerada, entonces para todos $\lambda_1,\dots,\lambda_d \in R$ se verifica que $\det((Tr_{R/k}(\lambda_i\lambda_j)_{1\leq i,j\leq d})) = 0$. Así, por el Lema 1 se tiene que para $e_1,\dots,e_d \in B$ $[\det(Tr_{\mathbb{L}/\mathbb{K}}(e_ie_j)_{1\leq i,j\leq d})] = 0$ en $A/\mathfrak{p}$, i.e., $\det(Tr_{\mathbb{L}/\mathbb{K}}(e_ie_j)_{1\leq i,j\leq d}) \in \mathfrak{p}$
$\Rightarrow d_{B/A} \subseteq \mathfrak{p}$, i.e., $\mathfrak{p} | d_{B/A}$ ✓ Si $tr_{R/k}$ es no-degenerada, consideramos una base $(\lambda_1,\dots,\lambda_d)$ de R sobre k $\Rightarrow \det(Tr_{R/k}(\lambda_i\lambda_j)_{1\leq i,j\leq d}) \neq 0$.
Luego, si $e_i \in B$ se proyecta a $\lambda_i \in R$ $\overset{\text{Lema 1}}{\Longrightarrow}$ $\det(Tr_{\mathbb{L}/\mathbb{K}}(e_ie_j)_{1\leq i,j\leq d}) \notin \mathfrak{p} \Rightarrow d_{B/A} \not\subseteq \mathfrak{p}$ ∎

§15. Ramificación en extensiones de Galois

En esta sección, $A \subseteq \mathbb{K} = Fr(A)$ es un anillo de Dedekind, $\mathbb{L}/\mathbb{K}$ es una extensión finita y de Galois, y $B = \tilde{A} \subseteq \mathbb{L}$ la clausura integral de A.

⚠ Sea $G := Gal(\mathbb{L}/\mathbb{K})$. Entonces, $\sigma(B) = B$ para todo $\sigma \in G$. Además, si $\mathfrak{q} \subseteq B$ ideal primo no-nulo con $\mathfrak{p} = \mathfrak{q} \cap A$, entonces $\mathfrak{p} = \sigma(\mathfrak{q}) \cap A$ para todo $\sigma \in G$.
$\Rightarrow$ Para todo $\mathfrak{p} \in Spec(A)^*$, G actúa en $\{\mathfrak{q} \in Spec(B)^* \text{ tal que } \mathfrak{q}|\mathfrak{p}\}$.

Prop: $Gal(\mathbb{L}/\mathbb{K})$ actúa transitivamente en $\{\mathfrak{q} \in Spec(B)^* \text{ tal que } \mathfrak{q}|\mathfrak{p}\}$.

Dem: Sean $\mathfrak{q}, \mathfrak{q}' \in Spec(B)^*$ con $\mathfrak{q}|\mathfrak{p}$ y $\mathfrak{q}'|\mathfrak{p}$ y supongamos que $\sigma(\mathfrak{q}) \neq \mathfrak{q}'$ $\forall \sigma \in G$. Así, $\mathfrak{q}' + \sigma(\mathfrak{q}) = B$ (cf. §11, p.29) y luego $\exists\, b \in \mathfrak{q}'$ con $b \notin \sigma(\mathfrak{q})$ $\forall \sigma \in G$ (Teo. chino del Resto*), i.e., $\sigma(b) \notin \mathfrak{q}$ $\forall \sigma \in G$. Sea $a := \prod_{\sigma\in G} \sigma(b) \in \mathfrak{q}'$ con $a \notin \mathfrak{q}$ (ideal primo!).
Por definición, $a \in B^G = B \cap \mathbb{K} = A$ (de hecho, $a \overset{\text{def}}{=} N_{\mathbb{L}/\mathbb{K}}(b) \in A$) y así tenemos que $a \in \mathfrak{q}' \cap A = \mathfrak{p}$ pero $a \notin \mathfrak{q} \cap A = \mathfrak{p}$ ↯ ∎ (* Ver también "Prime avoidance").

Recuerdo: Si $\mathfrak{q}|\mathfrak{p}$ entonces el grado residual de $\mathfrak{q}$ es $f_\mathfrak{q} = f_{\mathfrak{q}|\mathfrak{p}} = [B/\mathfrak{q} : A/\mathfrak{p}]$ y el índice de ramificación de $\mathfrak{q}$ es $e_\mathfrak{q} = e_{\mathfrak{q}|\mathfrak{p}} = v_\mathfrak{q}(\mathfrak{p}B)$

Corolario: En el caso galoisiano, si $\mathfrak{p} \in \mathrm{Spec}(A)^*$ y $\mathfrak{q}, \mathfrak{q}' \in \mathrm{Spec}(B)^*$ son tales que $\mathfrak{q} | \mathfrak{p}$ y $\mathfrak{q}' | \mathfrak{p}$ entonces $e_{\mathfrak{q}|\mathfrak{p}} = e_{\mathfrak{q}'|\mathfrak{p}}$ y $f_{\mathfrak{q}|\mathfrak{p}} = f_{\mathfrak{q}'|\mathfrak{p}}$.

Dem: Sea $\sigma \in \mathrm{Gal}(\mathbb{L}/\mathbb{K})$, entonces $\sigma(\mathfrak{p}B) = \mathfrak{p}B$ y así $\sigma\left(\prod_{\mathfrak{q}|\mathfrak{p}} \mathfrak{q}^{e_\mathfrak{q}}\right) = \prod_{\mathfrak{q}|\mathfrak{p}} \mathfrak{q}^{e_\mathfrak{q}}$ donde $\sigma\left(\prod_{\mathfrak{q}|\mathfrak{p}} \mathfrak{q}^{e_\mathfrak{q}}\right) = \prod_{\mathfrak{q}|\mathfrak{p}} \sigma(\mathfrak{q})^{e_\mathfrak{q}}$. Por transitividad de la acción de $\mathrm{Gal}(\mathbb{L}/\mathbb{K})$ tenemos que $\prod_{\mathfrak{q}|\mathfrak{p}} \mathfrak{q}^{e_\mathfrak{q}} = \prod_{\mathfrak{q}|\mathfrak{p}} \sigma(\mathfrak{q})^{e_{\sigma(\mathfrak{q})}} \Rightarrow e_\mathfrak{q} = e_{\sigma(\mathfrak{q})}$ por unicidad ✓ Finalmente, notamos que $\sigma \in \mathrm{Gal}(\mathbb{L}/\mathbb{K})$ induce un isomorfismo de $A/\mathfrak{p}$-extensiones $\bar{\sigma} : B/\mathfrak{q} \xrightarrow{\sim} B/\sigma(\mathfrak{q})$ ■

⚠ (Abuso de) Notación: En el caso galoisiano, podemos escribir

$$e_\mathfrak{p} := e_{\mathfrak{q}|\mathfrak{p}} = v_\mathfrak{q}(\mathfrak{p}B) \quad \text{y} \quad f_\mathfrak{p} := f_{\mathfrak{q}|\mathfrak{p}} = [B/\mathfrak{q} : A/\mathfrak{p}] \quad \text{para } \underline{\text{todo}}\ \mathfrak{q}|\mathfrak{p}.$$

Así, en el caso galoisiano la Fórmula de Ramificación se reduce a lo siguiente:

Teorema ($d = efg$): Sea $A \subseteq \mathbb{K} = \mathrm{Fr}(A)$ anillo de Dedekind, $\mathbb{L}/\mathbb{K}$ extensión finita de Galois y $B := \tilde{A} \subseteq \mathbb{L}$ clausura integral de A. Si para todo $\mathfrak{p} \in \mathrm{Spec}(A)^*$ definimos

$$g_\mathfrak{p} := \#\{\mathfrak{q} \in \mathrm{Spec}(B)^* \text{ tal que } \mathfrak{q}|\mathfrak{p}\},$$

entonces $[\mathbb{L} : \mathbb{K}] = e_\mathfrak{p} f_\mathfrak{p} g_\mathfrak{p}$.

Terminología: En el caso galoisiano, el índice de ramificación de un primo se puede codificar usando Teoría de Grupos. Sea $\mathfrak{p} \in \mathrm{Spec}(A)^*$ y sea $\mathfrak{q} \in \mathrm{Spec}(B)^*$ tal que $\mathfrak{q}|\mathfrak{p}$. Se define el <u>grupo de descomposición</u> de $\mathfrak{q}$ como el subgrupo (estabilizador)

$$D_\mathfrak{q} := \{\sigma \in \mathrm{Gal}(\mathbb{L}/\mathbb{K}) \text{ tal que } \sigma(\mathfrak{q}) = \mathfrak{q}\}$$

y así $[\mathrm{Gal}(\mathbb{L}/\mathbb{K}) : D_\mathfrak{q}] = g_\mathfrak{p}$. Notar que todo $\sigma \in D_\mathfrak{q}$ induce un automorfismo de $A/\mathfrak{p}$-álgebras $\bar{\sigma} : B/\mathfrak{q} \xrightarrow{\sim} B/\mathfrak{q}$ y luego obtenemos un morfismo de grupos:

$$r_\mathfrak{q} : D_\mathfrak{q} \longrightarrow \mathrm{Aut}_{A/\mathfrak{p}\text{-alg}}(B/\mathfrak{q}), \quad \sigma \mapsto \bar{\sigma}.$$

Se define el <u>grupo de inercia</u> de $\mathfrak{q}$ como $I_\mathfrak{q} := \ker(r_\mathfrak{q}) \overset{\text{df}}{=} \{\sigma \in \mathrm{Gal}(\mathbb{L}/\mathbb{K}) \text{ tq } \bar{\sigma} = \mathrm{Id}_{B/\mathfrak{q}}\}$.

Para estudiar $r_\mathfrak{q}$ (probar que es sobreyectivo!) necesitamos lo siguiente:

Prop: La extensión $(B/\mathfrak{q})/(A/\mathfrak{p})$ es <u>normal</u> (pero no necesariamente separable).

Dem: Sea $a \in B/\mathfrak{q}$ y sea $b \in B$ tq $[b] = a$ en $B/\mathfrak{q}$. Entonces, el polinomio $P := \prod_{\sigma \in \mathrm{Gal}(\mathbb{L}/\mathbb{K})} (X - \sigma(b)) \in (B[X])^{\mathrm{Gal}(\mathbb{L}/\mathbb{K})} = A[X]$ tiene coef. en A. Además, la imagen de P en $B/\mathfrak{q}[X]$ es $\prod_{\sigma \in \mathrm{Gal}(\mathbb{L}/\mathbb{K})} (X - [\sigma(b)])$ y luego se anula en $a \in B/\mathfrak{q}$ y escinde! Si Q_a es la imagen de P en $A/\mathfrak{p}[X]$ entonces $B/\mathfrak{q}$ es el cuerpo de descomposición de $\{Q_a\}_{a \in B/\mathfrak{q}} \Rightarrow B/\mathfrak{q}$ es normal sobre $A/\mathfrak{p}$ ✓ ■

Lema técnico: Sea $\mathbb{L}/\mathbb{K}$ una extensión finita normal y sea $\mathbb{K} \subseteq \mathbb{L}' \subseteq \mathbb{L}$ la clausura separable de $\mathbb{K}$ relativa a $\mathbb{L}$. Entonces, $\mathbb{L}'/\mathbb{K}$ es de Galois y la restricción

$$\mathrm{Aut}_{\mathbb{K}\text{-alg}}(\mathbb{L}) \xrightarrow{\sim} \mathrm{Gal}(\mathbb{L}'/\mathbb{K}), \quad \sigma \mapsto \sigma|_{\mathbb{L}'}$$

es un isomorfismo.

Dem (Ejercicio*): ① Si $P \in \mathbb{K}[X]$ irred se anula en $\alpha \in \mathbb{L}'$ entonces escinde en $\mathbb{L}'[X]$.

② Sea $\sigma \in \mathrm{Gal}(\mathbb{L}'/\mathbb{K})$ y $\tau_0 \in \Sigma_{\mathbb{L}/\mathbb{K}}$. Probar que $\exists\, \tau \in \Sigma_{\mathbb{L}/\mathbb{K}}$ tq $\tau|_{\mathbb{L}'} = \tau_0 \circ \sigma$. Deducir que $\tilde{\sigma} := \tau_0^{-1} \circ \tau \in \mathrm{Aut}_\mathbb{K}(\mathbb{L})$ y que $\tilde{\sigma}|_{\mathbb{L}'} = \sigma$.

③ Probar que $\tau_1, \tau_2 \in \mathrm{Aut}_\mathbb{K}(\mathbb{L})$ con $\tau_1|_{\mathbb{L}'} = \tau_2|_{\mathbb{L}'} \Rightarrow \tau_1 = \tau_2$ [Hint: Si $a \in \mathbb{L} \Rightarrow a^{p^s} \in \mathbb{L}'$] ($p = $ exp. char$(\mathbb{K})$) ■

Teorema: El morfismo $r_{\mathfrak{q}} : D_{\mathfrak{q}} \twoheadrightarrow \mathrm{Aut}_{A/\mathfrak{p}\text{-alg}}(B/\mathfrak{q})$ es sobreyectivo.

Dem: Sea $A/\mathfrak{p} \subseteq (B/\mathfrak{q})' \subseteq B/\mathfrak{q}$ la clausura separable de $A/\mathfrak{p}$ relativa a $B/\mathfrak{q}$ y sea $\alpha \in (B/\mathfrak{q})'$ un elemento primitivo, i.e., $(B/\mathfrak{q})' = (A/\mathfrak{p})(\alpha)$. Podemos asumir $\alpha \neq 0$. Por el Teorema Chino del Resto (o por "Prime Avoidance"), $\exists\, b \in B$ tal que $[b] = \alpha$ en $B/\mathfrak{q}$ y $b \in \sigma(\mathfrak{q})$ $\forall \sigma \in \mathrm{Gal}(\mathbb{L}/\mathbb{K}) \setminus D_{\mathfrak{q}}$ ✓ Calculemos $\mu_\alpha^{A/\mathfrak{p}}$:

Sea $P := \mu_\alpha^{A/\mathfrak{p}} \in A/\mathfrak{p}[X]$ con $\deg(P) = [(A/\mathfrak{p})(\alpha) : A/\mathfrak{p}] = [(B/\mathfrak{q})' : A/\mathfrak{p}]$, y notar que $Q := \prod_{\tau \in \mathrm{Gal}((B/\mathfrak{q})'/(A/\mathfrak{p}))} (X - \tau(\alpha)) \in ((B/\mathfrak{q})'[X])^{\mathrm{Gal}((B/\mathfrak{q})'/(A/\mathfrak{p}))} = (A/\mathfrak{p})[X]$ verifica que $P \mid Q$. Como Q mónico y $\deg(P) = \deg(Q)$, tenemos que $P = Q$ ✓

Considerar $R := \prod_{\sigma \in \mathrm{Gal}(\mathbb{L}/\mathbb{K})} (X - \sigma(b)) \in (B[X])^{\mathrm{Gal}(\mathbb{L}/\mathbb{K})} = A[X]$ y sea $\overline{R} = [R] \in A/\mathfrak{p}[X]$.

Como $\overline{R}(\alpha) = 0 \Rightarrow P \mid \overline{R}$, i.e., $\prod_{\tau \in \mathrm{Gal}((B/\mathfrak{q})'/(A/\mathfrak{p}))} (X - \tau(\alpha)) \mid \prod_{\sigma \in \mathrm{Gal}(\mathbb{L}/\mathbb{K})} (X - \overline{\sigma(b)})$

y luego $\tau(\alpha) = \overline{\sigma_\tau(b)}$ para cierto $\sigma_\tau \in \mathrm{Gal}(\mathbb{L}/\mathbb{K})$. Veamos que $r_{\mathfrak{q}}$ es sobreyectivo:

Sea $\tau \in \mathrm{Aut}_{A/\mathfrak{p}\text{-alg}}(B/\mathfrak{q}) \underset{\text{Lema}}{\cong} \mathrm{Gal}((B/\mathfrak{q})'/(A/\mathfrak{p}))$ y sea $\sigma = \sigma_\tau \in \mathrm{Gal}(\mathbb{L}/\mathbb{K})$ tal que $\overline{\sigma(b)} = \tau(\alpha) \neq 0$ en $B/\mathfrak{q}$ $\Rightarrow \sigma(b) \notin \mathfrak{q}$, i.e., $b \in \sigma^{-1}(\mathfrak{q})$. Dado que $b \in \sigma(\mathfrak{q})$ para todo $\sigma \in \mathrm{Gal}(\mathbb{L}/\mathbb{K}) \setminus D_{\mathfrak{q}}$, se tiene $\sigma^{-1} \in D_{\mathfrak{q}}$, i.e., $\sigma = \sigma_\tau \in D_{\mathfrak{q}}$ ✓

Finalmente, $(r_{\mathfrak{q}}(\sigma))(\alpha) \overset{\text{def}}{=} \overline{\sigma(b)} = \tau(\alpha)$ y así, dado que $(B/\mathfrak{q})' = (A/\mathfrak{p})(\alpha)$, se deduce que $r_{\mathfrak{q}}(\sigma)|_{(B/\mathfrak{q})'} = \tau|_{(B/\mathfrak{q})'} \underset{\text{Lema técnico}}{\Longrightarrow} r_{\mathfrak{q}}(\sigma) = \tau$ ∎

Corolario: $r_{\mathfrak{q}}$ induce un isomorfismo $\hat{r}_{\mathfrak{q}} : D_{\mathfrak{q}}/I_{\mathfrak{q}} \xrightarrow{\cong} \mathrm{Gal}((B/\mathfrak{q})'/(A/\mathfrak{p}))$.

Notación: Sup. que la extensión $\mathbb{L}/\mathbb{K}$ es separable (no nec. de Galois). Se define $f'_{\mathfrak{q}|\mathfrak{p}} := [B/\mathfrak{q} : A/\mathfrak{p}]_s$ y $e'_{\mathfrak{q}|\mathfrak{p}} := [B/\mathfrak{q} : A/\mathfrak{p}]_i$. Así, $f_{\mathfrak{q}|\mathfrak{p}} = e'_{\mathfrak{q}|\mathfrak{p}} f'_{\mathfrak{q}|\mathfrak{p}}$.

Además: $\mathfrak{q}$ es no-ramificado $\overset{\text{def}}{\iff} e_{\mathfrak{q}|\mathfrak{p}} = 1$ y $(B/\mathfrak{q})/(A/\mathfrak{p})$ separable $\iff e_{\mathfrak{q}|\mathfrak{p}} e'_{\mathfrak{q}|\mathfrak{p}} = 1$.

Obs: En el caso en que $\mathbb{L}/\mathbb{K}$ es galoisiana, $e'_{\mathfrak{p}} := e'_{\mathfrak{q}|\mathfrak{p}}$ y $f'_{\mathfrak{p}} := f'_{\mathfrak{q}|\mathfrak{p}}$ sólo dependen de $\mathfrak{p} \in \mathrm{Spec}(A)^*$. En part, en tal caso

$$d = [\mathbb{L} : \mathbb{K}] = e_{\mathfrak{p}} f_{\mathfrak{p}} g_{\mathfrak{p}} = e_{\mathfrak{p}} e'_{\mathfrak{p}} f'_{\mathfrak{p}} g_{\mathfrak{p}} \quad \text{para todo } \mathfrak{p} \in \mathrm{Spec}(A)^*.$$

Ejercicio útil Supongamos que $\mathbb{L}/\mathbb{K}$ es galoisiana y sea $\mathfrak{q} | \mathfrak{p}$. Probar que:

1. $|D_{\mathfrak{q}}| = e_{\mathfrak{p}} e'_{\mathfrak{p}} f'_{\mathfrak{p}}$
2. $|I_{\mathfrak{q}}| = e_{\mathfrak{p}} e'_{\mathfrak{p}}$
3. $\mathfrak{q}$ es no-ramificado $\iff r_{\mathfrak{q}} : D_{\mathfrak{q}} \xrightarrow{\sim} \mathrm{Aut}_{A/\mathfrak{p}\text{-alg}}(B/\mathfrak{q})$ es un isomorfismo.

§16. Valores absolutos y lugares

Recordemos que hay una analogía entre Aritmética y Geometría

$$\begin{array}{ccc}
\mathrm{Spec}(\mathbb{Z})^* & \longleftrightarrow & \mathrm{Spec}(\mathbb{C}[T])^* \\
\updownarrow 1:1 & & \updownarrow 1:1 \\
\mathcal{P} := \{p \in \mathbb{Z} \text{ primo}\} & \longleftrightarrow & \mathbb{C} \\
\cap\! | & & \cap\! | \\
? & & \mathbb{P}^1(\mathbb{C}) \underset{(\S 13,\ p33)}{\overset{1:1}{\longleftrightarrow}} \{v : \mathbb{C}(T) \twoheadrightarrow \mathbb{Z} \cup \{\infty\} \text{ val. discreta sobreyectiva}\}
\end{array}$$

Grothendieck: En $\mathcal{P}$ "faltan puntos", ¡Es mejor $\mathrm{Spec}(\mathbb{Z})$!

Obs (Análisis Complejo): Si $X = \mathbb{P}^1(\mathbb{C})$ (o X sup. de Riemann compacta) y $f \in \mathbb{C}(X)^*$ entonces $\sum_{x \in \mathbb{C} \cup \{\infty\}} \operatorname{Res}(f, x) = 0 \iff \sum_{x \in X} v_x(f) = 0$. ¿Existe un análogo aritmético?

Def: Sea $\mathbb{K}$ un cuerpo. Un valor absoluto en $\mathbb{K}$ es una función $|\cdot| : \mathbb{K} \to \mathbb{R}^{\geq 0}$ tal que:
① $\forall x \in \mathbb{K}$, $|x| = 0 \iff x = 0$.
② $\forall x, y \in \mathbb{K}$, $|xy| = |x||y|$.
③ $\forall x, y \in \mathbb{K}$, $|x+y| \leq |x| + |y|$.
Decimos que $|\cdot|$ es no-arquimediano si se cumple además
③' $\forall x, y \in \mathbb{K}$, $|x+y| \leq \max\{|x|, |y|\}$. (**Obs**: ③' $\Rightarrow$ ③).

Ejemplos típicos:
① El valor absoluto trivial es $\mathbb{K} \to \mathbb{R}$, $x \mapsto |x| := \begin{cases} 0 & \text{si } x = 0 \\ 1 & \text{si } x \neq 1 \end{cases}$
② Sea $v : \mathbb{K} \to \mathbb{Z} \cup \{+\infty\}$ una valuación discreta y sea $\alpha \in \mathbb{R}^{>1}$ arbitrario. Entonces, $|x|_v := \alpha^{-v(x)}$ es un valor absoluto no-arquimediano en $\mathbb{K}$. ie, $\alpha > 1$ en $\mathbb{R}$
③ En $\mathbb{Q}$ hay los siguientes ejemplos importantes: $|x|_\infty := \max\{x, -x\}$ el valor absoluto usual y, para todo $p \geq 2$ número primo, el valor absoluto p-ádico $|x|_p := p^{-v_p(x)}$. Explícitamente, si $a, b \in \mathbb{Z}$ y $p \nmid a$, $p \nmid b$ y $n \in \mathbb{Z}$ entonces
$$\left|\frac{a}{b} p^n\right|_p \overset{\text{def}}{=} p^{-n}$$

Def: Sea $\mathbb{K}$ un cuerpo con un valor absoluto $|\cdot|$. Entonces, $d(x,y) := |x-y|$ define una métrica en $\mathbb{K}$ y luego una topología en $\mathbb{K}$, llamada la topología definida por $|\cdot|$. Decimos que dos valores absolutos $|\cdot|_1$ y $|\cdot|_2$ son dependientes si definen la misma topología.

Prop: Sean $|\cdot|_1, |\cdot|_2 : \mathbb{K} \to \mathbb{R}^{\geq 0}$ dos valores absolutos. Son equivalentes:
① $|\cdot|_1$ y $|\cdot|_2$ son dependientes.
② $\{x \in \mathbb{K}, |x|_1 < 1\} = \{x \in \mathbb{K}, |x|_2 < 1\}$.
③ Existe $\lambda \in \mathbb{R}^{>0}$ tal que $|x|_2 = |x|_1^\lambda$ para todo $x \in \mathbb{K}$.

Dem: ① $\Rightarrow$ ② pues $|x|_i < 1 \iff x^n \xrightarrow{n \to +\infty} 0$ resp. a la topología definida por $|\cdot|_i$, $i = 1, 2$ ✓
② $\Rightarrow$ ③: $|\cdot|_i$ trivial $\iff \{x \in \mathbb{K}, |x|_i < 1\} = \{0\}$. Así, $|\cdot|_1$ trivial $\iff |\cdot|_2$ trivial.
Sup. $|\cdot|_1$ no-trivial y sea $\alpha \in \mathbb{K}^*$ con $|\alpha|_1 \neq 1$. Reemplazando α por $1/\alpha$ si fuese necesario, podemos asumir $|\alpha|_1 > 1$. Dado que $\forall x \in \mathbb{K}^*$; $|x|_1 < 1 \iff |x^{-1}|_1 > 1$ tenemos $\{x \in \mathbb{K}, |x|_1 > 1\} = \{x \in \mathbb{K}, |x|_2 > 1\}$ y luego $|\alpha|_2 > 1$. Sea $a := |\alpha|_1$, $b := |\alpha|_2$ y sea $\lambda := \log(b)/\log(a) > 0$, ie, $|\alpha|_2 = |\alpha|_1^\lambda$ ✓
Sea $x \in \mathbb{K}^*$ arbitrario y sea $\beta = \beta(x) := \log(|x|_1)/\log(a)$, ie, $|x|_1 = |\alpha|_1^\beta$.
$\Rightarrow \forall m, n \in \mathbb{N}^{\geq 1}$ con $\frac{m}{n} > \beta$ se tiene $|\alpha|_1^{m/n} > |\alpha|_1^\beta = |x|_1$, ie, $|\alpha^m|_1 > |x^n|_1$,
ie, $\left|\frac{\alpha^m}{x^n}\right|_1 > 1 \overset{②}{\iff} \left|\frac{\alpha^m}{x^n}\right|_2 > 1$, ie, $|\alpha|_2^{m/n} > |x|_2$ $\forall m, n \in \mathbb{N}^{\geq 1}$ con $\frac{m}{n} > \beta$
$\Rightarrow |\alpha|_2^\beta \geq |x|_2$. Análogamente, $|x|_2 \geq |\alpha|_2^\beta \Rightarrow |x|_2 = |\alpha|_2^\beta = |\alpha|_1^{\lambda\beta} = |x|_1^\lambda$ ✓
③ $\Rightarrow$ ① Pues las bolas resp. a $|\cdot|_1$ y $|\cdot|_2$ son las mismas ∎

Def: Un lugar de un cuerpo $\mathbb{K}$ es una topología definida por un valor absoluto no-trivial. Denotamos por $\mathrm{Pl}(\mathbb{K})$ al conjunto de lugares de $\mathbb{K}$. Si $v \in \mathrm{Pl}(\mathbb{K})$ está definido por un valor absoluto $|\cdot| : \mathbb{K} \to \mathbb{R}^{\geq 0}$ entonces toda función de la forma $x \mapsto |x|^\lambda$ para algún $\lambda \in \mathbb{R}^{>0}$ es un representante de v.

⚠ Abuso de lenguaje: Un representante $|\cdot|^\lambda$ puede no ser un valor absoluto si $\lambda \gg 1$ (no cumple $|x+y|^\lambda \leq |x|^\lambda + |y|^\lambda$). Por ejemplo, $|\cdot|^2 : \mathbb{C} \to \mathbb{R}^{\geq 0}$, $z \mapsto N_{\mathbb{C}/\mathbb{R}}(z) = z\bar{z} = |z|^2$.

§17. Teorema de Ostrowski.

Teorema (Ostrowski, 1916): Sea $\mathcal{P} = \{p \in \mathbb{Z} \text{ número primo}\}$. Entonces, hay una biyección $\mathcal{P} \cup \{\infty\} \xrightarrow{\sim} \mathrm{Pl}(\mathbb{Q})$, $v \longmapsto$ Topología definida por $|\cdot|_v$.

Dem: Sea $p \in \mathcal{P}$ y sea $w \in \mathrm{Pl}(\mathbb{Q})$ definido por $v \in \mathcal{P} \cup \{\infty\}$. Entonces, $|p^n|_\infty = p^n$ y $|p^n|_v = p^{-n}$ (resp. $|p^n|_v = 1$) si $v = p$ (resp. si $v \in \mathcal{P} \setminus \{p\}$). Así, $p^n \xrightarrow{n \to +\infty} 0$ en w si y sólo si $v = p$, i.e., la función es inyectiva ✓ Para la sobreyectividad, consideremos $v \in \mathrm{Pl}(\mathbb{Q})$ definido por el valor absoluto $|\cdot| : \mathbb{Q} \to \mathbb{R}^{\geq 0}$. Notar que $|1|^2 = |1^2| = |1|$ y luego $|1| = 1$, y que $|-1|^2 = |1| = 1$ y así $|-1| = 1$. Hay 2 posibilidades:

Caso 1: Sup. que $\mathbb{Z} \subseteq \{x \in \mathbb{Q}, |x| \leq 1\}$. Como $|\cdot|$ es no-trivial, $\exists x \in \mathbb{Q}^*$ con $|x| \neq 1$. $\overset{x=a/b}{\Longrightarrow}$ $\exists a \in \mathbb{Z} \setminus \{0\}$ con $|a| \neq 1$, i.e., con $|a| < 1$. Escribiendo $a = \pm \prod_{i=1}^r p_i$ con p_i primo, tenemos que $\exists p \in \mathcal{P}$ tal que $|p| < 1$. Veamos que $|\cdot|$ y $|\cdot|_p$ son dependientes:
Sea $n \in \mathbb{Z}$ tal que $p \nmid n$. El lema de Bézout implica que $\forall m \in \mathbb{N}^{\geq 1}$ existen $a_m, b_m \in \mathbb{Z}$ con $a_m p^m + b_m n^m = 1 \implies 1 = |1| \leq \underbrace{|a_m|}_{\leq 1} \underbrace{|p|^m}_{\xrightarrow[m\to+\infty]{} 0} + \underbrace{|b_m|}_{\leq 1} |n|^m$ y luego $|n|^m \not\to 0$ cuando $m \to +\infty$, i.e., $|n| \geq 1 \implies |n| = 1$. Lo anterior implica que $|n| = |p|^{v_p(n)}$ $\forall n \in \mathbb{Z}$ $\implies |x| = |p|^{v_p(x)}$ $\forall x \in \mathbb{Q}$. Así, $|x| = |x|_p^\lambda$ con $\lambda = -\log(|p|)/\log(p) \in \mathbb{R}^{>0}$ ✓

Caso 2: Sup. que $\exists m \in \mathbb{Z}$ con $|m| > 1$. Podemos asumir $m \geq 0$ y luego $m > 1$.
Veamos que $|a| > 1$ para todo $a \in \mathbb{N}^{\geq 2}$: Sea $a > 1$ y sea $M_a := \max\{|1|, |2|, \ldots, |a-1|\}$. Escribamos m^n en base a, i.e., $m^n = \sum_{i=0}^r \mu_i a^i$ con $\mu_i \in \{0, \ldots, a-1\}$ donde $r = \lfloor n \frac{\log(m)}{\log(a)} \rfloor \leq n \frac{\log(m)}{\log(a)} \implies |m|^n \leq M_a \sum_{i=0}^r |a|^i = M_a \left(\frac{|a|^{r+1} - 1}{|a| - 1} \right)$ $(\star)$

Si $|a| \leq 1 \implies \{|m|^n\}_{n \in \mathbb{N}}$ sería acotada ↯ pues $|m| > 1$ ✓ Más aún, $(\star)$ implica que
$$n \log(|m|) \leq \log(M_a) - \log(|a|-1) + \log(|a|^{r+1} - 1) \leq \log(M_a) - \log(|a|-1) + (r+1)\log(|a|)$$
$$\leq \log(M_a) + \log\left(\frac{1}{1 - 1/|a|}\right) + r \log(|a|) \leq \text{constante} + n \frac{\log(m)}{\log(a)} \log(|a|)$$
$\implies \log(|m|) \leq \frac{\log(m)}{\log(a)} \log(|a|)$ al tomar $n \to +\infty$. Cambiando a por m deducimos que $\frac{\log(|m|)}{\log(m)} = \frac{\log(|a|)}{\log(a)} \equiv \lambda \in \mathbb{R}^{>0}$ constante. Así, todo $a \in \mathbb{N}^{\geq 2}$ cumple $|a| = |a|_\infty^\lambda$
$\implies$ Para todo $x \in \mathbb{Q}$ se verifica que $|x| = |x|_\infty^\lambda$ ■

Obs: En el caso arquimediano (i.e., Caso 2) se tiene que $\lambda \in]0, 1]$ pues para todo $n \in \mathbb{N}$ tenemos $|n| \leq n|1| = n = |n|_\infty \implies \lambda \leq 1$.

⚠ Convención: En todo lo que sigue, identificaremos $\mathcal{P} \cup \{\infty\} \simeq \mathrm{Pl}(\mathbb{Q})$.

Prop (Fórmula del Producto): Para todo $x \in \mathbb{Q}^*$ se tiene que
$$\prod_{v \in Pl(\mathbb{Q})} |x|_v = 1 .$$

Dem: Si escribimos $x = \pm \prod_{p \in \mathcal{P}} p^{v_p(x)}$ entonces $|x|_p = p^{-v_p(x)}$ y $|x|_\infty = \prod_{p\in\mathcal{P}} p^{v_p(x)}$ ■

Obs geométrica: Sea X sup. de Riemann compacta conexa. Para todo $x \in X$ se define $|\cdot|_x : \mathbb{C}(X) \to \mathbb{R}^{\geq 0}$, $f \mapsto |f|_x := e^{-v_x(f)}$. Así, la fórmula $\sum_{x \in X} v_x(f) = 0$ se reescribe como $\prod_{x\in X} |f|_x = 1 \ \forall f \in \mathbb{C}(X)^*$. Así, "$\infty$ es el punto faltante en $\mathcal{P}$".

§18. Completación

Def: Sea $\mathbb{K}$ un cuerpo y sea $|\cdot| : \mathbb{K} \to \mathbb{R}^{\geq 0}$ un valor absoluto. Una sucesión de Cauchy en $\mathbb{K}$ es una sucesión $(x_n)_{n\in\mathbb{N}} \subseteq \mathbb{K}$ tal que
$\forall \varepsilon \in \mathbb{R}^{>0}$, $\exists N = N(\varepsilon) \in \mathbb{N}$ tal que: $\forall p, q \in \mathbb{N}$, $(p \geq N$ y $q \geq N) \Rightarrow |x_p - x_q| < \varepsilon$.
(eg. toda sucesión convergente es de Cauchy). Decimos que $\mathbb{K}$ es completo resp. a $|\cdot|$ si toda sucesión de Cauchy en $\mathbb{K}$ converge.

Teorema: Sea $\mathbb{K}$ un cuerpo y sea $v \in Pl(\mathbb{K})$ un lugar definido por un valor absoluto (no-trivial) $|\cdot| : \mathbb{K} \to \mathbb{R}^{\geq 0}$. Entonces, existe un cuerpo $\mathbb{K}_v$ llamado la completación de $\mathbb{K}$ en v, un morfismo de cuerpos $i : \mathbb{K} \hookrightarrow \mathbb{K}_v$ y un valor absoluto $|\cdot|'$ en $\mathbb{K}_v$ verificando:
1. $\forall x \in \mathbb{K}$, $|i(x)|' = |x|$ (ie, $|\cdot|'$ extiende a $|\cdot|$).
2. $i(\mathbb{K})$ es denso en $\mathbb{K}_v$ respecto a $|\cdot|'$.
3. $\mathbb{K}_v$ es completo respecto a $|\cdot|'$.

Más aún, si $(\widetilde{\mathbb{K}}_v, \tilde{i} : \mathbb{K} \hookrightarrow \widetilde{\mathbb{K}}_v, |\cdot|'' : \widetilde{\mathbb{K}}_v \to \mathbb{R}^{\geq 0})$ cumplen 1, 2, 3 entonces existe un único isomorfismo de cuerpos $\varphi : \mathbb{K}_v \xrightarrow{\sim} \widetilde{\mathbb{K}}_v$ tal que $\tilde{i} = \varphi \circ i$ y $|\varphi(x)|'' = |x|' \ \forall x \in \mathbb{K}_v$.

Idea de Dem: Toda sucesión $(x_n)_{n\in\mathbb{N}}$ en $\mathbb{K}$ puede ser vista como elemento del anillo $\mathbb{K}^{\mathbb{N}}$. Sea A el subanillo de $\mathbb{K}^{\mathbb{N}}$ formado por sucesiones de Cauchy y sea $I \subseteq A$ el subconj. de sucesiones en $\mathbb{K}$ que convergen a 0 $\Rightarrow$ $I \subseteq A$ es un ideal (pues Cauchy $\Rightarrow$ acotado (!)).
Sea $\mathbb{K}_v := A/I$ anillo cociente, y sea $i : \mathbb{K} \hookrightarrow \mathbb{K}_v$, $x \mapsto \overline{(x)_{n\in\mathbb{N}}}$ suc. constante.
Veamos que $\mathbb{K}_v$ es un cuerpo: Sea $(x_n)_{n\in\mathbb{N}} \subseteq \mathbb{K}$ tal que $(x_n)_{n\in\mathbb{N}} \in A$ y $\overline{(x_n)_{n\in\mathbb{N}}} \neq 0$ en $\mathbb{K}_v$, ie, $x_n \not\to 0$ cuando $n \to +\infty$. Fijemos $\varepsilon \in \mathbb{R}^{>0}$ y notar que para todo $m_0 \in \mathbb{N}$ $\exists n \in \mathbb{N}$ tq $n \geq m_0$ y $|x_n| \geq \varepsilon$. Además, $\exists N \in \mathbb{N}$ tq $\forall p, q \geq N$ se tiene $|x_p - x_q| < \varepsilon/2$.
$\Rightarrow |x_n| - |x_p| < \varepsilon/2$ con $|x_n| \geq \varepsilon$, ie, $|x_p| > \varepsilon/2 \ \forall p \geq N$. Definamos $y_n := 1$ si $n < N$ y $y_n := 1/x_n$ si $n \geq N$. Podemos asumir $\frac{\varepsilon}{2} < 1$ y así $|y_n| > \frac{\varepsilon}{2} \ \forall n \in \mathbb{N}$, de donde se tiene $|y_p - y_q| = \left|\frac{1}{x_p} - \frac{1}{x_q}\right| = \frac{|x_p - x_q|}{|x_p||x_q|} \leq \frac{4}{\varepsilon^2} |x_p - x_q| \ \forall p, q \geq N \overset{\varepsilon \text{ fijo}}{\Longrightarrow} (y_n)_{n\in\mathbb{N}}$ es de Cauchy.
Como $x_n y_n = 1 \ \forall n \geq N$ se tiene $\overline{(x_n)_{n\in\mathbb{N}}} \cdot \overline{(y_n)_{n\in\mathbb{N}}} = 1$ y así $\overline{(x_n)_{n\in\mathbb{N}}} \in \mathbb{K}_v^*$ ✓
Si $(x_n)_{n\in\mathbb{N}}$ es de Cauchy en $\mathbb{K}$ $\Rightarrow$ $(|x_n|)_{n\in\mathbb{N}}$ es de Cauchy en $\mathbb{R}$ y luego converge (!).
Definimos $|\overline{(x_n)_{n\in\mathbb{N}}}|' := \lim_{n\to+\infty} |x_n|$ para todo $\overline{(x_n)_{n\in\mathbb{N}}} \in \mathbb{K}_v$. Por propiedades de los límites en $\mathbb{R}$: $|xy|' = |x|'|y|'$ & $|x+y|' \leq |x|' + |y|' \ \forall x, y \in \mathbb{K}_v$ y además $x = 0 \overset{\text{def de } I}{\Longleftrightarrow} |x|' = 0$

Además, $\forall x \in \mathbb{K}$ se tiene $|i(x)|' \overset{\text{def}}{=} \lim_{n\to+\infty} |x| = |x|$, i.e., ① ✓ Veamos que $i(\mathbb{K})$ es <u>denso</u> en $\mathbb{K}_v$: Sea $(x_m)_{m\in\mathbb{N}} \in A$ sucesión de Cauchy y $q \in \mathbb{N}$, entonces tenemos que $|\overline{(x_m)_{m\in\mathbb{N}}} - i(x_q)|' = \lim_{p\to+\infty} |x_p - x_q| < \varepsilon$ si $p, q \geq N = N(\varepsilon)$, i.e., $(i(x_q))_{q\in\mathbb{N}}$ converge a $\overline{(x_m)_{m\in\mathbb{N}}}$ i.e., ② ✓ Veamos que $\mathbb{K}_v$ es <u>completo</u>: sea $(u_m)_{m\in\mathbb{N}}$ una sucesión de Cauchy en $\mathbb{K}_v$ y notar que ② implica que $\forall n \in \mathbb{N}$ existe $x_m \in \mathbb{K}$ tq $|i(x_m) - u_m|' < \frac{1}{m+1}$ y así $|x_p - x_q| \overset{①}{=} |i(x_p) - i(x_q)|' \leq \frac{1}{p+1} + \frac{1}{q+1} + |u_p - u_q|' \Rightarrow (x_m)_{m\in\mathbb{N}}$ es de Cauchy en $\mathbb{K}$ y además $u_m \xrightarrow{n\to+\infty} \overline{(x_m)_{m\in\mathbb{N}}}$ en $\mathbb{K}_v$, i.e., ③ ✓ La unicidad de $\mathbb{K}_v$ se deja como $\boxed{\text{Ejercicio}}$ (Indicación: Si $x \in \mathbb{K}_v$ y $(x_m)_{m\in\mathbb{N}} \subseteq \mathbb{K}$ es tq $i(x_m) \xrightarrow{n\to+\infty} x$, definir $\varphi(x) := \lim_{n\to+\infty} \tilde{i}(x_m)$) ■

<u>Ejemplo importante</u>: Si $\mathbb{K} = \mathbb{Q}$ con $Pl(\mathbb{Q}) = \mathcal{P} \cup \{\infty\}$ entonces $\mathbb{R} := \mathbb{Q}_\infty$ y para todo $p \in \mathcal{P}$ primo $\mathbb{Q}_p$ es el cuerpo de los <u>números p-ádicos</u> (i.e., completación de $\mathbb{Q}$ resp. $|\cdot|_p$).

<u>Def</u>: Sea $\mathbb{K}$ un cuerpo y $|\cdot|: \mathbb{K} \to \mathbb{R}^{\geq 0}$ un valor absoluto. Sea E un $\mathbb{K}$-e.v. Una <u>norma</u> en E es una función $\|\cdot\|: E \to \mathbb{R}^{\geq 0}$ tal que:

① $\forall x \in E$, $\|x\| = 0 \Leftrightarrow x = 0$.

② $\forall \lambda \in \mathbb{K}$ y $\forall x \in \mathbb{K}$, $\|\lambda x\| = |\lambda| \|x\|$.

③ $\forall x, y \in E$, $\|x+y\| \leq \|x\| + \|y\|$.

Decimos que dos normas $\|\cdot\|_1$ y $\|\cdot\|_2$ en E son <u>equivalentes</u> si $\exists\, C_1, C_2 \in \mathbb{R}^{>0}$ tales que $C_1\|x\|_1 \leq \|x\|_2 \leq C_2\|x\|_1$ para todo $x \in E$.

Con la terminología anterior, se tiene el siguiente resultado clásico de Análisis:

<u>Teorema</u>: Sea $\mathbb{K}$ un cuerpo completo resp. a un valor absoluto no-trivial $|\cdot|: \mathbb{K} \to \mathbb{R}^{\geq 0}$. Sea E un $\mathbb{K}$-e.v. de dimensión finita, entonces <u>todas</u> las normas en E son equivalentes y E es completo.

§19. <u>Cuerpos completos arquimedeanos</u>

Un valor absoluto $|\cdot|: \mathbb{K} \to \mathbb{R}^{\geq 0}$ es arquimedeano si <u>no</u> es no-arquimedeano (i.e., si no se verifica $|x+y| \leq \max\{|x|, |y|\}$ $\forall x, y \in \mathbb{K}$).

<u>Teorema</u> (Ostrowski, 1918): Sea $\mathbb{K}$ un cuerpo <u>completo</u> resp. a un valor absoluto arquimedeano $|\cdot|: \mathbb{K} \to \mathbb{R}^{\geq 0}$. Entonces, existe un isomorfismo de cuerpos $\varphi: \mathbb{K} \xrightarrow{\sim} \mathbb{L}$ donde $\mathbb{L} = \mathbb{R}$ o $\mathbb{C}$, y existe $\lambda \in \mathbb{R}^{>0}$ tal que $|\varphi(x)|_\infty = |x|^\lambda$ $\forall x \in \mathbb{K}$.

Necesitaremos dos resultados previos:

<u>Lema 1</u>: Sea $\mathbb{K}/\mathbb{R}$ extensión con un valor absoluto $|\cdot|: \mathbb{K} \to \mathbb{R}^{\geq 0}$ tal que $|x| = |x|_\infty$ para todo $x \in \mathbb{R} \subseteq \mathbb{K}$. Entonces, $\mathbb{K}/\mathbb{R}$ es una extensión algebraica.

<u>Dem</u>: Sea $z \in \mathbb{K}$ y definamos $f: \mathbb{C} \to \mathbb{R}^{\geq 0}$, $\alpha \mapsto |z^2 - \overbrace{(\alpha+\bar{\alpha})}^{\in\mathbb{R}} z + \overbrace{\alpha\bar{\alpha}}^{\in\mathbb{R}}|$. Basta probar que $\exists\, \alpha \in \mathbb{C}$ tq $f(\alpha) = 0$. Notar que f es continua pues

$$|f(\alpha_1) - f(\alpha_2)| \leq |z^2 - (\alpha_1+\bar{\alpha}_1)z + \alpha_1\bar{\alpha}_1 - (z^2 - (\alpha_2+\bar{\alpha}_2)z + \alpha_2\bar{\alpha}_2)|$$
$$\leq |(\alpha_1+\bar{\alpha}_1) - (\alpha_2+\bar{\alpha}_2)|_\infty |z| + ||\alpha_1|^2_\infty - |\alpha_2|^2_\infty|_\infty \quad ✓$$

Además, $f(\alpha) \geq |\alpha|^2_\infty - |z|^2 - |\alpha+\bar{\alpha}|_\infty |z|$ y luego $f(\alpha) \longrightarrow +\infty$ si $|\alpha|_\infty \longrightarrow +\infty$.
$\Rightarrow \exists\, \alpha_0 \in \mathbb{C}$ tal que $\{\alpha \in \mathbb{C},\ f(\alpha) \leq f(\alpha_0)\}$ es compacto y <u>no-vacío</u>. Además,

$\exists \alpha_1 \in \mathbb{C}$ tq $f(\alpha_1) = \min\{f(\alpha), \alpha \in \mathbb{C}\}$. Sea $A := \{\alpha \in \mathbb{C}, f(\alpha) = f(\alpha_1)\}$ compacto no-vacío $\Rightarrow \exists \alpha_2 \in A$ tq $|\alpha_2|_\infty = \max\{|\alpha|_\infty, \alpha \in A\}$ y veamos que $f(\alpha_2) = 0$: Sup. que $f(\alpha_2) > 0$ y sea $\varepsilon \in \mathbb{R}^{>0}$ con $0 < \varepsilon < f(\alpha_2)$. Si $g := X^2 - (\alpha_2 + \overline{\alpha}_2)X + \alpha_2\overline{\alpha}_2 + \varepsilon \in \mathbb{R}[X]$ entonces $\Delta(g) = (\alpha_2 + \overline{\alpha}_2)^2 - 4\alpha_2\overline{\alpha}_2 - 4\varepsilon = -|\alpha_2 - \overline{\alpha}_2|_\infty^2 - 4\varepsilon < 0 \Rightarrow g$ posee $\alpha_3, \overline{\alpha}_3 \in \mathbb{C}$ raíces y $\alpha_3\overline{\alpha}_3 = \alpha_2\overline{\alpha}_2 + \varepsilon > \alpha_2\overline{\alpha}_2$, por lo que $\alpha_3 \notin A$. Sea $m \in \mathbb{N}^{\geq 1}$ y definamos $G_m \in \mathbb{R}[X]$ por

$$G_m(X) := (X^2 - (\alpha_2 + \overline{\alpha}_2)X + \alpha_2\overline{\alpha}_2)^m - (-\varepsilon)^m = \prod_{i=1}^{2m}(X - \beta_i) \overset{G_m \in \mathbb{R}[X]}{=} \prod_{i=1}^{2m}(X - \overline{\beta}_i) \quad \text{con } \beta_i \in \mathbb{C}.$$

Como $G_m(\alpha_3) = 0$, podemos asumir $\beta_1 = \alpha_3$. Por otra parte, calculamos

$$G_m(X)^2 = \prod_{i=1}^{2m}(X - \beta_i)(X - \overline{\beta}_i) = \prod_{i=1}^{2m}(X^2 - (\beta_i + \overline{\beta}_i)X + \beta_i\overline{\beta}_i) \Rightarrow |G_m(z)|^2 \underset{\text{def}}{=} \prod_{i=1}^{2m} f(\beta_i) \overset{\beta_1 = \alpha_3}{\geq} f(\alpha_3) f(\alpha_2)^{2m-1}$$

Por otra parte, $|G_m(z)| \leq f(\alpha_2)^m + \varepsilon^m$ y así $f(\alpha_3) f(\alpha_2)^{2m-1} \leq (f(\alpha_2)^m + \varepsilon^m)^2$, i.e.,

$\frac{f(\alpha_3)}{f(\alpha_2)} \leq \left(1 + \left(\frac{\varepsilon}{f(\alpha_2)}\right)^m\right)^2 \xrightarrow[m \to +\infty]{} 1$ pues $\frac{\varepsilon}{f(\alpha_2)} < 1 \Rightarrow f(\alpha_3) \leq f(\alpha_2) = f(\alpha_1)$ y así $\alpha_3 \in A$ $\lightning$

Luego, $f(\alpha_2) = 0$ y así $z \in \mathbb{K}$ es raíz de $X^2 - (\alpha_2 + \overline{\alpha}_2)X + \alpha_2\overline{\alpha}_2 \in \mathbb{R}[X]$ ■

<u>Lema 2</u>: Sea $\mathbb{K}$ un cuerpo con valor absoluto $|\cdot| : \mathbb{K} \to \mathbb{R}^{\geq 0}$. Entonces, $|\cdot|$ es no-arquimediano si y sólo si $\mathbb{Z} \subseteq \{x \in \mathbb{K}, |x| \leq 1\}$.

<u>Dem</u>: $(\Rightarrow)$ Si $n \in \mathbb{N}$ entonces $|n+1| \leq \max\{|n|, |1|\}$ y concluimos por inducción en n ✓

$(\Leftarrow)$ Sean $a, b \in \mathbb{K}$ y $m \in \mathbb{N}$, entonces $|(a+b)^m| \leq \sum_{k=0}^{m} \left|\binom{m}{k}\right| |a|^k |b|^{m-k} \leq \sum_{k=0}^{m} |a|^k |b|^{m-k}$.

Sup. (por ejemplo) $|a| \geq |b| \Rightarrow |a+b|^m \leq (m+1)|a|^m$, i.e., $|a+b| \leq (1+m)^{1/m}|a| \xrightarrow[m \to +\infty]{} |a|$ y así $|a+b| \leq |a| = \max\{|a|, |b|\}$ es no-arquimediano ■

<u>Dem del Teorema</u>: Por el Lema 2, $\exists n \in \mathbb{N}$ con $|n| > 1$ y luego $|n^k| \xrightarrow{k \to +\infty} +\infty$. Así, $\{n \cdot 1 = 1 + \overset{n}{\dots} + 1, n \in \mathbb{N}\}$ es infinito y luego $\mathrm{char}(\mathbb{K}) = 0$, i.e., $\mathbb{Q} \hookrightarrow \mathbb{K}$. El Teorema de Ostrowski para $\mathbb{Q}$ implica que $\exists \lambda \in \mathbb{R}^{>0}$ tq $|x| = |x|_\infty^\lambda$ $\forall x \in \mathbb{Q} \subseteq \mathbb{K}$. Sea $\widetilde{\mathbb{R}}$ la adherencia de $\mathbb{Q}$ en $\mathbb{K}$, que al ser cerrado en $\mathbb{K}$ se tiene que $\widetilde{\mathbb{R}}$ es un cuerpo completo y luego $\widetilde{\mathbb{R}} \cong \mathbb{R}$ por unicidad de $\mathbb{R} = \mathbb{Q}_\infty$. Así, $\mathbb{R} \hookrightarrow \mathbb{K}$ y por el Lema 1 se tiene que $\mathbb{K}/\mathbb{R}$ es una extensión algebraica. $(\Rightarrow \Sigma_{\mathbb{K}/\mathbb{R}} \neq \emptyset)$ y luego $\exists \sigma : \mathbb{K} \hookrightarrow \mathbb{C}$ morfismo de $\mathbb{R}$-álgebras. Como $[\mathbb{C} : \mathbb{R}] = 2$ entonces $\sigma(\mathbb{K}) = \mathbb{R}$ o $\mathbb{C}$. En el primer caso $\varphi : \mathbb{K} \xrightarrow{\sim} \sigma(\mathbb{K}) \xrightarrow{\sim} \mathbb{R}$ estamos OK, y en el caso $\varphi : \mathbb{K} \xrightarrow[\sigma]{\sim} \mathbb{C}$ se tiene que $\|z\| := |\varphi^{-1}(z)|$ es una norma en $\mathbb{C}$ que es por ende equivalente a $|z|_\infty = \sqrt{z\overline{z}}$ $\Rightarrow z \mapsto |\varphi^{-1}(z)|$ y $z \mapsto |z|_\infty$ definen la misma topología y luego son dependientes, i.e., $\exists \tilde{\lambda} \in \mathbb{R}^{>0}$ tq $|\varphi(x)|_\infty = |x|^{\tilde{\lambda}}$ $\forall x \in \mathbb{K}$ (de hecho, $\lambda = \tilde{\lambda}$ al restringirse a $\mathbb{Q}$) ■

<u>Corolario</u>: Sea $\mathbb{K}$ un cuerpo con un valor absoluto arquimediano $|\cdot| : \mathbb{K} \to \mathbb{R}^{\geq 0}$. Entonces, existe un morfismo de cuerpos $\sigma : \mathbb{K} \hookrightarrow \mathbb{C}$ y $\lambda \in]0, 1]$ tales que

$$|x| = |\sigma(x)|_\infty^\lambda \quad \text{para todo } x \in \mathbb{K}.$$

<u>Dem</u>: Tenemos que $\mathbb{K} \hookrightarrow \mathbb{K}_v$ donde $\mathbb{K}_v$ completo arquimediano. Luego $\exists \varphi : \mathbb{K}_v \xrightarrow{\sim} \mathbb{L}$ con $\mathbb{L} = \mathbb{R}$ o $\mathbb{C}$. En ambos casos $\mathbb{L} \hookrightarrow \mathbb{C}$ y así $\mathbb{K} \hookrightarrow \mathbb{K}_v \hookrightarrow \mathbb{L} \hookrightarrow \mathbb{C}$ nos da σ. Dado que $|n| = |1 + \overset{n}{\dots} + 1| \leq |1| + \dots + |1| = n$ se tiene que $\lambda \leq 1$ ■

§20. Extensiones algebraicas de cuerpos completos

Notar que si $a+ib \in \mathbb{C}$ entonces $|a+ib| \overset{\text{def}}{=} \sqrt{a^2+b^2} = |N_{\mathbb{C}/\mathbb{R}}(a+ib)|^{1/[\mathbb{C}:\mathbb{R}]}$. El resultado principal de esta sección es una vasta generalización de esta observación:

Teorema: Sea $\mathbb{K}$ un cuerpo completo respecto a un valor absoluto no-trivial $|\cdot| : \mathbb{K} \to \mathbb{R}^{\geq 0}$, y sea $\mathbb{L}/\mathbb{K}$ una extensión algebraica. Entonces, existe un único valor absoluto en $\mathbb{L}$ $|\cdot|' : \mathbb{L} \to \mathbb{R}^{\geq 0}$ tal que $|\cdot|' \circ \rho_{\mathbb{L}/\mathbb{K}} = |\cdot|$ (ie, $|x|' = |x|$ $\forall x \in \mathbb{K}$). Más aún, si la extensión $\mathbb{L}/\mathbb{K}$ es finita entonces $(\mathbb{L}, |\cdot|')$ es completo y

$$|x|' = |N_{\mathbb{L}/\mathbb{K}}(x)|^{1/[\mathbb{L}:\mathbb{K}]} \quad \text{para todo } x \in \mathbb{L}.$$

Los resultados de la sección anterior implican que si $\mathbb{K}$ es arquimedeano entonces $\mathbb{K} \simeq \mathbb{R}$ ó $\mathbb{K} \simeq \mathbb{C}$ y que $\mathbb{L} \simeq \mathbb{R}$ ó $\mathbb{C}$, de donde se obtiene el resultado.

⚠ En todo lo que sigue, asumiremos que $\mathbb{K}$ es no-arquimedeano.

Notación: Sea $v \in \mathrm{Pl}(\mathbb{K})$ el lugar definido por $|\cdot|$. Entonces,

$$\mathcal{O}_v := \{x \in \mathbb{K}, |x| \leq 1\}$$

es un subanillo de $\mathbb{K}$ y $\mathfrak{m}_v := \{x \in \mathbb{K}, |x| < 1\} \subseteq \mathcal{O}_v$ es un ideal propio de $\mathcal{O}_v$ (pues $1 \notin \mathfrak{m}_v$). Notar que $\mathbb{K} = \mathcal{O}_v \cup \mathcal{O}_v^{-1}$ donde $\mathcal{O}_v^{-1} := \{x^{-1}, x \in \mathcal{O}_v \setminus \{0\}\}$, y donde

$$\mathcal{O}_v^* \overset{\text{def}}{=} \mathcal{O}_v \cap \mathcal{O}_v^{-1} \overset{\text{def}}{=} \{x \in \mathbb{K}, |x| = 1\} \overset{\text{def}}{=} \mathcal{O}_v \setminus \mathfrak{m}_v \quad \text{unidades de } \mathcal{O}_v.$$

En particular, $\mathfrak{m}_v \subseteq \mathcal{O}_v$ es el único ideal maximal de $\mathcal{O}_v$ (si $I \subseteq \mathcal{O}_v$ ideal con $I \not\subseteq \mathfrak{m}_v$ entonces $\exists x \in I$ con $x \notin \mathfrak{m}_v$, ie, $x \in \mathcal{O}_v^*$ y luego $I = \mathcal{O}_v$).

Obs útil: Si $a, b \in \mathbb{K}$ cumplen $|a| \neq |b|$, entonces $|a+b| = \max\{|a|, |b|\}$. En efecto, si $|a| < |b|$ entonces $|a/b| < 1$ y luego $a/b \in \mathfrak{m}_v$, por lo que $1 + a/b \notin \mathfrak{m}_v$. $\Rightarrow 1 + a/b \in \mathcal{O}_v^*$ y así $|a+b| = |b| \underbrace{|1 + a/b|}_{=1} = |b|$ ✓

Def: Un anillo conmutativo A es un anillo local si posee un único ideal maximal

Ejemplos: ① Sea $v : \mathbb{K} \to \mathbb{Z} \cup \{+\infty\}$ una valuación discreta en un cuerpo $\mathbb{K}$. Entonces, el anillo de valuación discreta $A := \{x \in \mathbb{K}, v(x) \geq 0\}$ es un anillo local con ideal maximal $\mathfrak{m} = \{x \in \mathbb{K}, v(x) > 0\}$.

② Si A anillo conmutativo y $\mathfrak{p} \in \mathrm{Spec}(A)$, entonces $A_{\mathfrak{p}}$ es un anillo local con ideal maximal $\mathfrak{m}_{\mathfrak{p}} := \mathfrak{p} A_{\mathfrak{p}}$.

③ Si $\mathbb{K}$ es un cuerpo con valor absoluto no-arquimedeano no-trivial $|\cdot|$, entonces $\mathcal{O}_v = \{x \in \mathbb{K}, |x| \leq 1\}$ es un anillo local con ideal maximal $\mathfrak{m}_v = \{x \in \mathbb{K}, |x| < 1\}$.

Hecho (Lema de Nakayama): Sea A un anillo conmutativo y sea $I \subseteq A$ un ideal contenido en todos los ideales maximales de A. Entonces, para todo A-módulo finitamente generado M se tiene que si $M = IM$ entonces $M = 0$. En particular, si $(A, \mathfrak{m})$ es un anillo local entonces $M = \mathfrak{m} M$ implica $M = 0$.

Prop: Sea $A \subseteq \mathbb{K} = \mathrm{Fr}(A)$ dominio entero y $\mathbb{L}/\mathbb{K}$ extensión finita. Sea $\mathfrak{m} \subseteq A$ ideal maximal y sea $B := \tilde{A} \subseteq \mathbb{L}$ la clausura integral de A. Entonces, $\exists\, \mathfrak{n} \subseteq B$ ideal maximal tal que $\mathfrak{m} B \subseteq \mathfrak{n}$.

Dem: Sea $A' = A_{\mathfrak{m}}$ anillo local y $B' := \widetilde{A'} \subseteq \mathbb{L}$ su clausura integral. Entonces, tal como para anillos de Dedekind (cf. §13, pág 32) se tiene que $B' = B_S$ donde $S = A \setminus \mathfrak{m}$ $(= \rho_{\mathbb{L}/\mathbb{K}}(A\setminus \mathfrak{m}) \subseteq B)$. Además, si $\eta' \subseteq B'$ maximal con $\mathfrak{m}B' \subseteq \eta'$ entonces se tiene $\mathfrak{m}B \subseteq \eta' \cap B =: \eta$ maximal, y luego podemos asumir que A es un anillo local:
Si $\mathfrak{m}B = B$ entonces $1 = m_1 b_1 + \ldots + m_s b_s$ con $m_i \in \mathfrak{m}$ y $b_i \in B$ $(\star)$. Como los b_i son enteros sobre A, $B_0 := A[b_1, \ldots, b_s] \subseteq B$ es un A-módulo fin. gen y $B_0 = \mathfrak{m}B_0$ por $(\star)$ $\overset{\text{Nakayama}}{\Rightarrow}$ $B_0 = 0$ y luego $1 = 0$ en $\mathbb{L}$ ↯ Así, $\mathfrak{m}B \subsetneq B$ ideal propio y luego existe $\eta \subseteq B$ maximal tal que $\mathfrak{m}B \subseteq \eta$. ■

[Obs útil: $\mathfrak{m} \subseteq \rho^{-1}_{\mathbb{L}/\mathbb{K}}(\eta) \cap A$ "=" $\eta \cap A$ (ideal propio) y luego $\mathfrak{m} = \eta \cap A$.

La demostración del Teorema será dividida en varios pasos. Primero, para $\mathbb{L}/\mathbb{K}$ ext. finita:

Paso 1 Probaremos que $\exists B \subseteq \mathbb{L}$ subanillo tal que:
① $\mathcal{O}_v \subseteq B$ (ie, $\rho_{\mathbb{L}/\mathbb{K}}(\mathcal{O}_v) \subseteq B$).
② $\mathfrak{m}_v B \subsetneq B$ ideal propio.
③ $\forall x \in \mathbb{L}$, $x \in B$ o $x^{-1} \in B$.

Paso 2 Construiremos $|\cdot|' : \mathbb{L} \to \mathbb{R}^{\geq 0}$ valor absoluto tal que $B = \{x \in \mathbb{L}, |x|' \leq 1\}$ y tal que extienda $|\cdot| : \mathbb{K} \to \mathbb{R}^{\geq 0}$.

Paso 3 Probaremos que $|\cdot|'$ es único y que $\mathbb{L}$ es completo.

Luego, consideraremos el caso en que $\mathbb{L}/\mathbb{K}$ es una extensión algebraica arbitraria:

Paso 4 Construiremos $|\cdot|'$ en este caso.

Paso 5 usando el paso 4 para $\overline{\mathbb{K}}/\mathbb{K}$, probaremos la fórmula de $|\cdot|'$ para $\mathbb{L}/\mathbb{K}$ finita.

Comenzamos por suponer $\mathbb{L}/\mathbb{K}$ finita y construyamos $B \subseteq \mathbb{L}$ como en el Paso 1:

[Lema 1: Existe un subanillo $B \subseteq \mathbb{L}$ con $\mathcal{O}_v \subseteq B$ y tal que
① $\mathfrak{m}_v B \subsetneq B$.
② $\forall x \in \mathbb{L}$, $x \in B$ o $x^{-1} \in B$.

Dem: Sea X el conjunto de subanillos $B \subseteq \mathbb{L}$ que verifican ①. Por la Proposición anterior, $\widetilde{\mathcal{O}_v} \subseteq \mathbb{L}$ verifica ① y luego $X \neq \emptyset$. Notar que X es un conjunto con un orden parcial dado por la inclusión. Además, si $\mathcal{C} \subseteq X$ es una cadena no-vacía (ie, conj. totalmente ordenado) entonces $B' := \bigcup_{B \in \mathcal{C}} B$ es un subanillo de $\mathbb{L}$. Veamos que B' cumple ①: si $\mathfrak{m}_v B' = B'$ entonces $1 = m_1 b_1 + \ldots + m_s b_s$ con $m_i \in \mathfrak{m}_v$, $b_i \in B'$ $(\star)$ $\Rightarrow \exists B \in \mathcal{C}$ tq $b_1, \ldots, b_s \in B$ y luego $B = \mathfrak{m}_v B$ por $(\star)$ ↯ Así, $B' \in X$ cota superior de $\mathcal{C}$ $\Rightarrow \exists$ elemento maximal $B \in X$ (Lema de Zorn!). La maximalidad de B y la Proposición anterior implican $B = \widetilde{B} \subseteq \mathbb{L}$, ie, B es integralmente cerrado ✓
Sea $\eta \subseteq B$ ideal maximal tq $\mathfrak{m}_v B \subseteq \eta$ $\Rightarrow \mathfrak{m}_v B_\eta \subseteq \eta B_\eta \subsetneq B_\eta$ y luego $B = B_\eta$ por maximalidad (!). Así, B es un anillo local ✓ Veamos ②:
Sea $x \in \mathbb{L}$ con $x \notin B \overset{B \max}{\Rightarrow} B[x] \notin X$, ie, $\mathfrak{m}_v B[x] = B[x]$ y luego $\eta B[x] = B[x]$.
$\Rightarrow 1 = m_0 + m_1 x + \ldots + m_d x^d$ con $m_i \in \eta \Rightarrow 1 - m_0 \notin \eta$, ie, $(1 - m_0) \in B^*$ (pues B local).

Así, $1 = m_0 + m_1 x + \ldots + m_d x^d \iff (x^{-1})^d + \sum_{i=1}^{d} \frac{m_i}{1-m_0}(x^{-1})^{d-i} = 0$ y luego $x^{-1} \in \widetilde{B} = B$ ■

Para construir $|\cdot|' : \mathbb{L} \to \mathbb{R}^{\geq 0}$ como en el $\boxed{\text{Paso 2}}$ introducimos la siguiente

<u>Notación</u>: Definimos $V_{\mathbb{K}} := \mathbb{K}^*/\mathcal{O}_v^*$ y $V_{\mathbb{L}} := \mathbb{L}^*/B^*$, donde $B \subseteq \mathbb{L}$ es el anillo construido en el Lema 1. Dado que $\mathcal{O}_v^* = \{x \in \mathbb{K}, |x| = 1\}$, el valor absoluto $|\cdot|$ induce induce un morfismo de grupos (multiplicativos) <u>inyectivo</u>

$$\overline{v} : V_{\mathbb{K}} \hookrightarrow \mathbb{R}^{>0}, \ \overline{x} \mapsto |x|.$$

Así, $\overline{v}$ define un orden en $V_{\mathbb{K}}$: $|a| \leq |b| \overset{\text{def}}{\iff} \overline{a} \leq \overline{b} \iff a\mathcal{O}_v \subseteq b\mathcal{O}_v$.

De manera análoga, definimos un orden en $V_{\mathbb{L}}$ mediante:

$$\overline{a} \leq \overline{b} \text{ para } \overline{a}, \overline{b} \in V_{\mathbb{L}} \overset{\text{def}}{\iff} aB \subseteq bB.$$

Por último, notamos que $\rho_{\mathbb{L}/\mathbb{K}} : \mathbb{K}^* \hookrightarrow \mathbb{L}^*$ cumple $\rho_{\mathbb{L}/\mathbb{K}}(\mathcal{O}_v^*) \subseteq B^*$ pues $\mathcal{O}_v \subseteq B$.

Luego, $\rho_{\mathbb{L}/\mathbb{K}}$ induce $\overline{\rho} : V_{\mathbb{K}} \to V_{\mathbb{L}}$ morfismo de grupos <u>creciente</u>.

<u>Lema 2</u>: La relación $\leq$ en $V_{\mathbb{L}}$ es un <u>orden total</u> y es compatible con la ley de grupos.

<u>Dem</u>: La relación $\leq$ es reflexiva y transitiva por definición ✓ Sup. que $\overline{a} \leq \overline{b}$ y $\overline{b} \leq \overline{a}$, ie, $aB \subseteq bB \subseteq aB$, ie, $aB = bB$. Entonces, $\exists\, c, d \in B$ tq $a = bc$ y $b = ad$. $\Rightarrow a = cda$ y luego $cd = 1$, ie, $c \in B^*$ por lo que $\overline{a} = \overline{b}$ ✓ Sean $a, b \in \mathbb{L}^*$ y notar que $x = a/b \in B$ o $x^{-1} = b/a \in B$ (Lema 1), ie, $aB \subseteq bB$ o $bB \subseteq aB$, ie, $\overline{a} \leq \overline{b}$ o $\overline{b} \leq \overline{a}$ (ie, $\leq$ es un orden <u>total</u>) ✓ Por último, si $a, b, c \in \mathbb{L}^*$ entonces $aB \subseteq bB$ implica $acB \subseteq bcB$, ie, $\overline{a} \leq \overline{b}$ implica $\overline{a}\overline{c} \leq \overline{b}\overline{c}$ ✓ ■

<u>Lema 3</u>: $\rho_{\mathbb{L}/\mathbb{K}}^{-1}(B) = \mathcal{O}_v$ (ie, "$B \cap \mathbb{K} = \mathcal{O}_v$") y $\overline{\rho} : V_{\mathbb{K}} \hookrightarrow V_{\mathbb{L}}$ <u>inyectivo</u>.

<u>Dem</u>: Consideremos $x \in \mathbb{K}$ con $|x| > 1$, por lo que $x^{-1} \in \mathfrak{m}_v$ y luego $\rho_{\mathbb{L}/\mathbb{K}}(x^{-1}) \in \mathfrak{m}_v B \subseteq \eta$ con $\eta \subseteq B$ único ideal maximal $\Rightarrow \rho_{\mathbb{L}/\mathbb{K}}(x) \notin B$ (sino $\eta = B$ ↯). Así, $\rho_{\mathbb{L}/\mathbb{K}}(\mathbb{K} \setminus \mathcal{O}_v)$ está contenido en $\mathbb{L} \setminus B$ y luego $\mathcal{O}_v \subseteq \rho_{\mathbb{L}/\mathbb{K}}^{-1}(B) \subseteq \mathcal{O}_v$ ✓

Si $\overline{\rho}(\overline{a}) = \overline{\rho}(\overline{b})$ entonces $\rho_{\mathbb{L}/\mathbb{K}}(a) = \rho_{\mathbb{L}/\mathbb{K}}(b)x$ con $x \in B^*$ y luego $\rho_{\mathbb{L}/\mathbb{K}}(a/b) \in B$ y $\rho_{\mathbb{L}/\mathbb{K}}(b/a) \in B \Rightarrow a/b \in \mathcal{O}_v$ y $b/a \in \mathcal{O}_v$ y luego $\overline{a} = \overline{b}$ en $V_{\mathbb{K}}$ ■

<u>Lema 4</u>: $[V_{\mathbb{L}} : \overline{\rho}(V_{\mathbb{K}})] \leq [\mathbb{L} : \mathbb{K}]$.

<u>Dem</u>: Sean $e_1, \ldots, e_s \in \mathbb{L}^*$ tq sus imágenes en $V_{\mathbb{L}}/\overline{\rho}(V_{\mathbb{K}})$ sean todas diferentes, y veamos que $(e_1, \ldots, e_s)$ es un conjunto $\mathbb{K}$-l.i. Sup. por contradicción que $\sum_{i=1}^{s} a_i e_i = 0$ para ciertos $(a_1, \ldots, a_s) \in \mathbb{K}^s \setminus \{0\}$. Reordenando, podemos asumir $a_1 e_1 \neq 0, \ldots, a_r e_r \neq 0$ y $a_{r+1} e_{r+1} = 0, \ldots, a_s e_s = 0$ y que $\overline{a_1 e_1} \geq \overline{a_2 e_2} \geq \ldots \geq \overline{a_r e_r}$ (ie, $a_{i+1} e_{i+1} \in a_i e_i B$). $\Rightarrow a_1 e_1 = -\sum_{i=2}^{r} a_i e_i \in a_2 e_2 B$ y luego $\overline{a_1 e_1} \leq \overline{a_2 e_2} \leq \overline{a_1 e_1} \overset{\text{Lema 2}}{\Longrightarrow} \overline{a_1 e_1} = \overline{a_2 e_2}$, ie, $\overline{e_1} = \overline{e_2}$ en $V_{\mathbb{L}}/\overline{\rho}(V_{\mathbb{K}})$ ↯ Así, $s \leq [\mathbb{L} : \mathbb{K}]$ y luego $[V_{\mathbb{L}} : \overline{\rho}(V_{\mathbb{K}})] \leq [\mathbb{L} : \mathbb{K}]$ ■

<u>Construyamos $|\cdot|' : \mathbb{L} \to \mathbb{R}^{\geq 0}$</u>:

Dado que $V_{\mathbb{L}} \overset{\text{def}}{=} \mathbb{L}^*/B^*$ es totalmente ordenado, si $\overline{x} \in V_{\mathbb{L}}$ es tal que $\overline{x} > 1$ entonces $\overline{x}^n > 1$ para todo $n \in \mathbb{N}^{\geq 1}$ (por Lema 2). Similar si $\overline{x} < 1$. Sea $e := [V_{\mathbb{L}} : \overline{\rho}(V_{\mathbb{K}})] < +\infty$.

Luego, definimos $|\cdot|' : \mathbb{L} \to \mathbb{R}^{>0}$ como la siguiente composición:

$$\begin{tikzcd} \mathbb{L}^* \arrow[r] \arrow[d, "|\cdot|'"'] & V_{\mathbb{L}} \arrow[r, hook] & \overline{\rho}(V_{\mathbb{K}}) \arrow[d, "\overline{\rho}^{-1}", "\wr"'] \\ \mathbb{R}^{>0} & \mathbb{R}^{>0} \arrow[l] & V_{\mathbb{K}} \arrow[l, "\overline{v}"'] \end{tikzcd}$$

$\overline{x} \longmapsto \overline{x}^e$

$a^{1/e} \longleftarrow a$

y se define $|0|' := 0$.

Notar que si $x \in \mathbb{K}^* \subseteq \mathbb{L}^*$ entonces $\overline{v}(\overline{x}) \overset{\text{df}}{=} |x|$ y luego $|x|' \overset{\text{df}}{=} \left(\overline{v}\left(\overline{\rho}^{-1}\left(\overline{\rho}(\overline{x})^e\right)\right)\right)^{1/e} = |x|$ ✓

Además, $|ab|' = |a|'|b|'$ $\forall a, b \in \mathbb{L}$. Más aún, si suponemos que $|a|' \leq |b|'$, ie, $\overline{a} \leq \overline{b}$ en $V_{\mathbb{L}}$, ie, $aB \subseteq bB$, entonces $\frac{a}{b} \in B$ y luego $a+b = b\left(1+\frac{a}{b}\right) \in bB$ $\Rightarrow |a+b|' \leq |b|' = \max\{|a|', |b|'\}$, por lo que $|\cdot|'$ valor absoluto no-arquimedeano ✓

[Obs práctica: Si $w \in Pl(\mathbb{L})$ es el lugar definido por $|\cdot|'$, entonces $B = \mathcal{O}_w \subseteq \mathbb{L}$.

Veamos ahora la unicidad de $|\cdot|'$ y la completitud de $\mathbb{L}$ (ie, el $\boxed{\text{Paso 3}}$):

Notar que $\mathbb{L}$ es un $\mathbb{K}$-e.v. de dimensión finita y luego dos valores absolutos $|\cdot|'$ y $|\cdot|''$ en $\mathbb{L}$ extendiendo a $|\cdot|$ definen normas equivalentes y en particular definen la misma topología en $\mathbb{L}$ $\Rightarrow \exists \lambda \in \mathbb{R}^{>0}$ tq $|x|'' = (|x|')^{\lambda}$ $\forall x \in \mathbb{L}$. Dado que $|\cdot|$ es no-trivial y $|\cdot|', |\cdot|''$ extienden $|\cdot|$, se tiene que $\lambda = 1$. Por último, $\mathbb{L}$ es completo pues $[\mathbb{L}:\mathbb{K}] < +\infty$ ✓

Construyamos ahora $|\cdot|' : \mathbb{L} \to \mathbb{R}^{\geq 0}$ como en el $\boxed{\text{Paso 4}}$, ie, para $\mathbb{L}/\mathbb{K}$ extensión algebraica arbitraria (no necesariamente finita): Notar que

$$\mathbb{L} = \bigcup_{\substack{\mathbb{L}' \subseteq \mathbb{L} \\ \mathbb{L}'/\mathbb{K} \text{ ext finita}}} \mathbb{L}'$$

Por todo lo anterior, para cada $\mathbb{L}'/\mathbb{K}$ existe un único $|\cdot|' : \mathbb{L} \to \mathbb{R}^{\geq 0}$ extendiendo $|\cdot|$.

Notar que si $x \in \mathbb{L}' \cap \mathbb{L}''$ y $|\cdot|', |\cdot|''$ son los valores abs. en $\mathbb{L}', \mathbb{L}''$ respectivamente entonces $\mathbb{L}' \cap \mathbb{L}''/\mathbb{K}$ es finita y luego $|\cdot|' = |\cdot|''$. Así, construimos de manera única $|\cdot|' : \mathbb{L} \to \mathbb{R}^{>0}$ ✓

Para concluir, supongamos que $\mathbb{L}/\mathbb{K}$ es una extensión finita y probemos la fórmula

$$|x|' = |N_{\mathbb{L}/\mathbb{K}}(x)|^{1/[\mathbb{L}:\mathbb{K}]} \quad \forall x \in \mathbb{L}.$$

Sea $\overline{\mathbb{K}}$ una clausura algebraica de $\mathbb{K}$ y sea $|\cdot|'' : \overline{\mathbb{K}} \to \mathbb{R}^{>0}$ la única extensión de $|\cdot|$ a $\overline{\mathbb{K}}$. Notar que si $\sigma : \mathbb{L} \hookrightarrow \overline{\mathbb{K}}$ en $\Sigma_{\mathbb{L}/\mathbb{K}}$ entonces $x \mapsto |\sigma(x)|''$ es un valor absoluto en $\mathbb{L}$ que extiende $|\cdot|$ y luego es único. Así, $|\sigma'(x)|'' = |\sigma(x)|''$ $\forall \sigma, \sigma' \in \Sigma_{\mathbb{L}/\mathbb{K}}$.

Así, para todo $x \in \mathbb{L}$ se calcula:

$$\begin{aligned} (|x|')^{[\mathbb{L}:\mathbb{K}]} = (|x|')^{[\mathbb{L}:\mathbb{K}]_s [\mathbb{L}:\mathbb{K}]_i} &\overset{[\mathbb{L}:\mathbb{K}]_s = |\Sigma_{\mathbb{L}/\mathbb{K}}|}{=} \Big(\prod_{\sigma \in \Sigma_{\mathbb{L}/\mathbb{K}}} |x|'\Big)^{[\mathbb{L}:\mathbb{K}]_i} \\ &= \Big(\prod_{\sigma \in \Sigma_{\mathbb{L}/\mathbb{K}}} |\sigma(x)|''\Big)^{[\mathbb{L}:\mathbb{K}]_i} \\ &= \Big|\Big(\prod_{\sigma \in \Sigma_{\mathbb{L}/\mathbb{K}}} \sigma(x)^{[\mathbb{L}:\mathbb{K}]_i}\Big)\Big|'' \\ &\overset{\text{ver §10, Prop en pág 24}}{=} |N_{\mathbb{L}/\mathbb{K}}(x)|'' = |N_{\mathbb{L}/\mathbb{K}}(x)| \end{aligned}$$

Así, $|x|' = |N_{\mathbb{L}/\mathbb{K}}(x)|^{1/[\mathbb{L}:\mathbb{K}]}$ para todo $x \in \mathbb{L}$. Esto último demuestra el $\boxed{\text{Paso 5}}$ y con concluimos la prueba del Teorema principal de esta sección ■

§21. Completación para valuaciones discretas

Recordemos que si $v : \mathbb{K} \twoheadrightarrow \mathbb{Z}\cup\{+\infty\}$ es una valuación discreta y $\alpha \in \mathbb{R}^{>1}$, entonces $|\cdot|_v : \mathbb{K} \to \mathbb{R}^{\geq 0}$, $x \mapsto \alpha^{-v(x)}$ es un valor absoluto no-arquimedeano. El objetivo de esta sección es describir más detalladamente la completación $\mathbb{K}_v$ en este caso. Lo anterior es particularmente interesante para $\mathbb{Q}_p$.

<u>Def</u>: Sea $(I, \leq)$ un conjunto ordenado. Un <u>sistema proyectivo</u> (o sistema inverso) respecto a I es una colección $\{A_i\}_{i\in I}$ tal que para todo par de índices $i,j\in I$ con $i\leq j$ hay una función $f_{ij} : A_j \to A_i$ que cumplen:

① $\forall i \in I$, $f_{ii} = Id_{A_i}$.

② $\forall i,j,k \in I$ con $i\leq j \leq k$ se tiene $f_{ik} = f_{ij}\circ f_{jk}$.

Se define el <u>límite proyectivo</u> (o límite inverso) de $\{A_i\}_{i\in I}$ mediante

$$\varprojlim_{i\in I} A_i := \left\{ (x_i)_{i\in I} \in \prod_{i\in I} A_i \ , \ \forall i,j\in I \text{ con } i\leq j \text{ se tiene } x_i = f_{ij}(x_j) \right\}.$$

Denotamos por $f_j : \varprojlim_{i\in I} A_i \to A_j$, $(x_i)_{i\in I} \mapsto x_j$ la j-ésima proyección.

Así, por definición de límite proyectivo, se tiene que $f_i = f_{ij}\circ f_j$ para todo $i\leq j$.

<u>Obs importante</u>: Si los $\{A_i\}_{i\in I}$ son grupos (resp. anillos, módulos, esp. topológicos, etc) y los f_{ij} respetan la estructura, entonces $\varprojlim A_i$ es un subgrupo (resp. subanillo, etc) del producto $\prod_{i\in I} A_i$.

<u>Propiedad Universal del Límite Proyectivo</u>:

Sea $\{A_i\}_{i\in I}$ un sistema proyectivo. Sea B un conjunto tal que $\forall i \in I$ existe una función $g_i : B \to A_i$ tal que $f_{ij}\circ g_j = g_i$ $\forall i,j\in I$ con $i\leq j$.

$\Rightarrow \exists !\ g : B \to \varprojlim_{i\in I} A_i$ tal que $f_i \circ g = g_i$ $\forall i \in I$. Así, $g(x) = (g_i(x))_{i\in I}$ $\forall x\in B$.

<u>Notación</u>: Sea $v : \mathbb{K} \to \mathbb{Z}\cup\{+\infty\}$ valuación discreta sobreyectiva y sea $\alpha\in\mathbb{R}^{>1}$. Así, $x\mapsto |x|_v := \alpha^{-v(x)}$ es un valor absoluto en $\mathbb{K}$ y denotamos por $v \in Pl(\mathbb{K})$ el lugar correspondiente. Así,

$$\mathcal{O}_v \overset{\text{def}}{=} \{x\in\mathbb{K}, |x|_v \leq 1\} = \{x\in\mathbb{K}, v(x)\geq 0\} \quad \text{y} \quad \mathfrak{m}_v = \{x\in\mathbb{K}, v(x) > 0\}.$$

En lo que, para todo $n\in\mathbb{N}$ dotamos al anillo $\mathcal{O}_v/\mathfrak{m}_v^n$ de la topología discreta (ie, <u>todo</u> subconj. es abierto). Además, para todos $m,n\in\mathbb{N}$ con $m\leq n$ se define

$$\pi_{m,n} : \mathcal{O}_v/\mathfrak{m}_v^n \twoheadrightarrow \mathcal{O}_v/\mathfrak{m}_v^m$$

Luego, $\{\mathcal{O}_v/\mathfrak{m}_v^n\}_{n\in\mathbb{N}}$ es un sistema proyectivo de anillos topológicos.

Por último, denotemos por $\mathbb{K}_v$ la completación de $\mathbb{K}$ resp. a $|\cdot|_v : \mathbb{K}\to\mathbb{R}^{\geq 0}$ y sea $|\cdot|_w : \mathbb{K}_v \to \mathbb{R}^{\geq 0}$ la extensión de $|\cdot|_v$ a $\mathbb{K}_v$. Como $|\cdot|_w$ es no-arquimedeano se define $\mathcal{O}_w := \{x\in\mathbb{K}_v, |x|_w \leq 1\}$ y $\mathfrak{m}_v := \{x\in\mathbb{K}_v, |x|_w < 1\}$.

Denotamos por $\widehat{\pi}_m : \mathcal{O}_w \twoheadrightarrow \mathcal{O}_w/\mathfrak{m}_w^n$ la proyección al cociente, con $n\in\mathbb{N}$.

El siguiente resultado permite describir el anillo topológico $\mathcal{O}_w \subseteq \mathbb{K}_v$:

<u>Teorema</u>: Con la Notación anterior, tenemos que:

1. $\mathcal{O}_w$ es la adherencia de $\rho_{\mathbb{K}_v/\mathbb{K}}(\mathcal{O}_v)$ en $\mathbb{K}_v$, ie, $\mathcal{O}_w = \overline{\mathcal{O}_v}$ en $\mathbb{K}_v$.
2. Para todo $n \in \mathbb{N}$, el morfismo de $\mathcal{O}_v$-álgebras
$$\rho_n : \mathcal{O}_v/\mathfrak{m}_v^n \xrightarrow{\sim} \mathcal{O}_w/\mathfrak{m}_w^n \text{ es un isomorfismo.}$$
3. Las funciones $g_n := \rho_n^{-1} \circ \hat{\pi}_n : \mathcal{O}_w \twoheadrightarrow \mathcal{O}_v/\mathfrak{m}_v^n$ inducen un isomorfismo de anillos topológicos $g : \mathcal{O}_w \xrightarrow{\sim} \varprojlim_{n\in\mathbb{N}} \mathcal{O}_v/\mathfrak{m}_v^n$.

<u>Dem</u>: Para ①, consideramos $x \in \mathcal{O}_w \subseteq \mathbb{K}_v$ y $(x_n)_{n\in\mathbb{N}} \subseteq \mathbb{K}$ sucesión tq $x_n \xrightarrow{n\to+\infty} x$. Así, $(|x_n|_v)_{n\in\mathbb{N}} \subseteq \mathbb{R}$ converge a $|x|_w \leq 1$. Como $|x|_v \in \alpha^{\mathbb{Z}} \cup \{0\}$ para $\alpha \in \mathbb{R}^{>1}$, $\exists N \in \mathbb{N}$ tal que $|x_n|_v < \alpha$ $\forall n \geq N$ y en particular $|x_n|_v \leq \alpha^0 = 1$, ie, $x_n \in \mathcal{O}_v$ $\forall n \geq N$
$\Rightarrow \mathcal{O}_w \subseteq \overline{\mathcal{O}_v}$. Como $\mathcal{O}_v \subseteq \mathcal{O}_w$ y $\mathcal{O}_w$ cerrado, entonces $\overline{\mathcal{O}_v} \subseteq \mathcal{O}_w$ ✓

Para ②, consideramos $x \in \mathcal{O}_v$ tal que $\rho_{\mathbb{K}_v/\mathbb{K}}(x)$ "=" $x \in \mathfrak{m}_w^n$. Entonces, $|x|_w = |x|_v \leq \alpha^{-n}$ y luego $x \in \mathfrak{m}_v^n$. Así, ρ_n inyectivo. Veamos que ρ_n sobreyectivo: sea $x \in \mathcal{O}_w$ y sea $(x_n)_{n\in\mathbb{N}} \subseteq \mathcal{O}_v$ tal que $x_n \xrightarrow{n\to+\infty} x$. Sea $N \in \mathbb{N}$ tq $|x - \rho_{\mathbb{K}_v/\mathbb{K}}(x_m)|_w \leq \alpha^{-n}$ $\forall m \geq N$.
$\Rightarrow x - \rho_{\mathbb{K}_v/\mathbb{K}}(x_m) \in \mathfrak{m}_w^n$ y así $\overline{x} = \rho_n(x_m)$ en $\mathcal{O}_w/\mathfrak{m}_w^n$ ✓

Veamos ③: La Prop. Universal de límites proyectivos induce $g : \mathcal{O}_w \longrightarrow \varprojlim_{n\in\mathbb{N}} \mathcal{O}_v/\mathfrak{m}_v^n$ un morfismo de $\mathcal{O}_v$-álgebras. Para la inyectividad, consideramos $x \in \mathcal{O}_w$ tq $g(x) = 0$, ie, $g_n(x) \overset{\text{def}}{=} \rho_n^{-1}(\hat{\pi}_n(x)) = 0$ $\forall n \in \mathbb{N}$ y luego $x \in \bigcap_{n\in\mathbb{N}} \mathfrak{m}_w^n$, ie, $|x|_w \leq \alpha^{-n}$ $\forall n \in \mathbb{N}$
$\Rightarrow |x|_w = 0$ y así $x = 0$ ✓ Para la sobreyectividad, consideramos $(x_n)_{n\in\mathbb{N}} \in \varprojlim_{n\in\mathbb{N}} \mathcal{O}_v/\mathfrak{m}_v^n$ y para cada $n \in \mathbb{N}$ fijamos $y_n \in \mathcal{O}_v$ tal que $\overline{y_n} = x_n$ en $\mathcal{O}_v/\mathfrak{m}_v^n$. Dado que $\forall m, n \in \mathbb{N}$ con $m \leq n$ se tiene que $\pi_{m,n}(x_n) = x_m$, entonces la imagen de y_n en $\mathcal{O}_v/\mathfrak{m}_v^m$ es y_m, ie, $y_n - y_m \in \mathfrak{m}_v^m$. Luego, deducimos que: $|y_p - y_q|_v \leq \alpha^{-\min(p,q)}$ $\forall p, q \in \mathbb{N}$ (*).
$\Rightarrow (y_n)_{n\in\mathbb{N}} \subseteq \mathcal{O}_v \subseteq \mathbb{K}$ sucesión de Cauchy. Sea $y := \lim_{n\to+\infty} \rho_{\mathbb{K}_v/\mathbb{K}}(y_n) \in \mathbb{K}_v$ su límite. Dado que $|y_n|_v \leq 1$ $\forall n \in \mathbb{N}$, se tiene $|y|_w \leq 1$, ie, $y \in \mathcal{O}_w$. Por (*), $|y - \rho_{\mathbb{K}_v/\mathbb{K}}(y_q)|_w \leq \alpha^{-q}$ y luego $y - \rho_{\mathbb{K}_v/\mathbb{K}}(y_q) \in \mathfrak{m}_w^q \Rightarrow \hat{\pi}_n(y) = \rho_n(\overline{y_n}) = \rho_n(x_n)$ $\forall n \in \mathbb{N}$, de donde obtenemos que $g_n(y) = x_n$ $\forall n \in \mathbb{N}$ y luego $g(y) = (x_n)_{n\in\mathbb{N}} \in \varprojlim_{n\in\mathbb{N}} \mathcal{O}_v/\mathfrak{m}_v^n$ ✓

Veamos que g es un homeomorfismo: para la continuidad de g basta probar que cada $g_n : \mathcal{O}_w \to \mathcal{O}_v/\mathfrak{m}_v^n$ es continua. Sea $x \in \mathcal{O}_v/\mathfrak{m}_v^n$ y veamos que $g_n^{-1}(\{x\}) \subseteq \mathcal{O}_w$ abierto: Si $y = \rho_n(x) \in \mathcal{O}_w/\mathfrak{m}_w^n \Rightarrow g_n^{-1}(\{x\}) = \hat{\pi}^{-1}(\{y\}) \overset{\text{def}}{=} \{z \in \mathcal{O}_w, z - y \in \mathfrak{m}_w^n\}$
$$= \{z \in \mathcal{O}_w, |z - y|_w \leq \alpha^{-n}\} \overset{⚠}{=} \{z \in \mathcal{O}_w, |z - y|_w < \alpha^{-(n-1)}\}$$
⚠ En la topología v-ádica las bolas abiertas son cerradas ! $\Rightarrow g$ continua ✓

Resta probar que si $\emptyset \neq \mathcal{U} \subseteq \mathcal{O}_w$ abierto entonces $g(\mathcal{U})$ es abierto. Sea $y \in \mathcal{U}$ y $n \in \mathbb{N}$ tq $y + \mathfrak{m}_w^n = \{z \in \mathcal{O}_w, |z - y|_w \leq \alpha^{-n}\} \subseteq \mathcal{U}$. Como $\mathcal{O}_w = \overline{\mathcal{O}_v}$, podemos elegir $x \in \mathcal{O}_v$ tq $\rho_{\mathbb{K}_v/\mathbb{K}}(x) \in y + \mathfrak{m}_w^n$. Como $|\cdot|_w$ no-arq, $\rho_{\mathbb{K}_v/\mathbb{K}}(x) + \mathfrak{m}_w^n = y + \mathfrak{m}_w^n$ y luego basta probar que $g(\rho_{\mathbb{K}_v/\mathbb{K}}(x) + \mathfrak{m}_w^n)$ es <u>abierto</u>: Sea $z \in g(\rho_{\mathbb{K}_v/\mathbb{K}}(x) + \mathfrak{m}_w^n)$ donde $z = (\overline{z_n})_{n\in\mathbb{N}} \in \varprojlim \mathcal{O}_v/\mathfrak{m}_v^n$ y cada $z_n \in \mathcal{O}_v$ verifica $|z_p - z_q|_v \leq \alpha^{-\min(p,q)}$.

Así, $z \in g\left(\rho_{\mathbb{K}_v/\mathbb{K}}(x) + \mathfrak{m}_w^n\right) \iff z_m \in g_m\left(\rho_{\mathbb{K}_v/\mathbb{K}}(x) + \mathfrak{m}_w^n\right)\ \forall m \in \mathbb{N}$, ie, $\rho_m(z_m) \in \hat{\pi}_m\left(\rho_{\mathbb{K}_v/\mathbb{K}}(x) + \mathfrak{m}_w^n\right)\ \forall m \in \mathbb{N}$, ie, $\rho_m(z_m) - \rho_{\mathbb{K}_v/\mathbb{K}}(x) \in \mathfrak{m}_w^n + \mathfrak{m}_w^m \overset{\text{dy}}{=} \mathfrak{m}_w^{\min(n,m)}$ y así $|z_m - x|_v \leq \alpha^{-\min(n,m)}\ \forall m \in \mathbb{N} \overset{m=n}{\Longrightarrow} |z_m - x|_v \leq \alpha^{-m}$ y así $\bar{z}_m = \bar{x}$ en $\mathcal{O}_v/\mathfrak{m}_v^n$, ie, $pr_m(z) = \bar{x}$ en $\mathcal{O}_v/\mathfrak{m}_v^n$. Luego, $g\left(\rho_{\mathbb{K}_v/\mathbb{K}}(x) + \mathfrak{m}_w^n\right) = pr_m^{-1}(\{\bar{x}\})$ es <u>abierto</u> pues pr_m es continua y $\{\bar{x}\} \subseteq \mathcal{O}_v/\mathfrak{m}_v^n$ es abierto ✓ ■

<u>Obs útil</u>: En la prueba anterior se utilizó que si $\alpha \in \mathbb{R}^{>1}$ y $|x|_v = \alpha^{-v(x)}\ \forall x \in \mathbb{K}$, entonces $|\cdot|_w : \mathbb{K}_v \to \mathbb{R}^{\geq 0}$ <u>tiene</u> que ser de la forma $|x|_w = \alpha^{-w(x)}\ \forall x \in \mathbb{K}_v$ para cierta valuación discreta $w : \mathbb{K}_v \twoheadrightarrow \mathbb{Z} \cup \{+\infty\}$ extendiendo a v. En efecto, dado que $v : \mathbb{K}^* \to \mathbb{Z}$ es continua (dotando a $\mathbb{Z}$ de la top. discreta) $\exists!$ ext. continua $w : \mathbb{K}_v^* \to \mathbb{Z}$.

<u>Recuerdo</u>: Un esp. topológico X es <u>localmente compacto</u> si $\forall x \in X$ existe un abierto $\mathcal{U} \subseteq X$ y un compacto $K \subseteq X$ tal que $x \in \mathcal{U} \subseteq K$. (eg. $X = \mathbb{R}$ o $\mathbb{C}$ son loc. compactos).

<u>Corolario / Definición</u>: Las sgtes condiciones son equivalentes:

1. La completación $\mathbb{K}_v$ es <u>localmente compacta</u>.
2. El cuerpo cociente $\mathcal{O}_v/\mathfrak{m}_v$ es <u>finito</u>.

En tal caso, decimos que $\mathbb{K}_v$ es un <u>cuerpo local</u>. Más aún, $\mathcal{O}_w$ es compacto.

<u>Dem</u>: Recordar (ver §13) que $\mathcal{O}_v = \{x \in \mathbb{K},\ v(x) \geq 0\}$ es un anillo de valuación discreta (ie, Dedekind y local) y luego $\mathfrak{m}_v^n/\mathfrak{m}_v^{n+1} \simeq \mathcal{O}_v/\mathfrak{m}_v$ como $\mathcal{O}_v/\mathfrak{m}_v$ - e.v. Además, $\exists \pi \in \mathcal{O}_v$ "parametro local" tq $\mathfrak{m}_v^n = \langle \pi^n \rangle\ \forall n \in \mathbb{N}$. Veamos que ② ⇒ ①: Si $\mathcal{O}_v/\mathfrak{m}_v$ es finito entonces $\mathcal{O}_v/\mathfrak{m}_v^n$ también (pues $\dim_{\mathcal{O}_v/\mathfrak{m}_v}(\mathcal{O}_v/\mathfrak{m}_v^n) = n$) y luego es compacto para la topología discreta. Por el Teorema de Tychonoff, $\prod_{n \in \mathbb{N}} \mathcal{O}_v/\mathfrak{m}_v^n$ es <u>compacto</u> y así $\mathcal{O}_w \simeq \varprojlim_{n \in \mathbb{N}} \mathcal{O}_v/\mathfrak{m}_v^n \xhookrightarrow{\text{cerrado}} \prod_{n \in \mathbb{N}} \mathcal{O}_v/\mathfrak{m}_v^n$ también es compacto. Dado que la valuación discreta $w : \mathbb{K}_v \twoheadrightarrow \mathbb{Z} \cup \{+\infty\}$ extiende a v, tenemos que $w(\pi) = v(\pi) = 1$ y así $\mathfrak{m}_w = \langle \pi \rangle$, ie, $\pi\ (= \rho_{\mathbb{K}_v/\mathbb{K}}(\pi))$ es un parámetro local de $\mathcal{O}_w$ y además $\mathfrak{m}_w^n = \pi^n \mathcal{O}_w$ es <u>compacto</u> (pues $\mathcal{O}_w$ compacto) y <u>abierto</u>. Finalmente, notamos que si $V \subseteq \mathbb{K}_v$ es una vecindad abierta de $x \in \mathbb{K}_v$ entonces $\exists m \in \mathbb{N}$ tq $x + \pi^n \mathcal{O}_w = x + \mathfrak{m}_w^n \subseteq V \Rightarrow \mathbb{K}_v$ localmente compacto ✓ Veamos que ① ⇒ ②: Como $\mathbb{K}_v$ es localmente compacto, $\exists K$ vecindad compacta de $0 \in \mathbb{K}_v$ y $n \in \mathbb{N}$ tq $0 \in \mathfrak{m}_w^n \subseteq K$. Como $\mathfrak{m}_w^n$ también es cerrado, tenemos que es <u>compacto</u>. Así, considerando el homeomorfismo $\mathcal{O}_w \xrightarrow[\sim]{\cdot \pi^n} \pi^n \mathcal{O}_w = \mathfrak{m}_w^n$ se deduce que $\mathcal{O}_w$ es compacto y en part. $\mathcal{O}_w \overset{\mathcal{C}^0}{\twoheadrightarrow} \mathcal{O}_w/\mathfrak{m}_w \simeq \mathcal{O}_v/\mathfrak{m}_v$ también lo es. Dado que $\mathcal{O}_v/\mathfrak{m}_v$ es discreto y compacto, deducimos que es <u>finito</u> ✓ ■

<u>Ejemplo fundamental</u>: Sea p un número primo, y sea $|\cdot|_p : \mathbb{Q} \to \mathbb{R}^{\geq 0}$ el valor absoluto p-ádico. Denotamos por $|\cdot|_p$ su extensión a la completación $\mathbb{Q}_p$ (números p-ádicos). Definimos los <u>enteros p-ádicos</u> como $\mathbb{Z}_p := \{x \in \mathbb{Q}_p,\ |x|_p \leq 1\} \cong \varprojlim_{n \in \mathbb{N}} \mathbb{Z}/p^n\mathbb{Z}$ y donde $\mathbb{Q}_p = Fr(\mathbb{Z}_p)$. En part, $\mathbb{Q}_p$ es un <u>cuerpo local</u>.

⚠ $\mathrm{char}(\mathbb{Z}_p) = 0$. <u>No</u> confundir $\mathbb{Z}_p$ con $\mathbb{Z}/p\mathbb{Z}$ o con $\mathbb{Z}_{(p)}$ (localización).

Así, por definición de $\varprojlim_{n \in \mathbb{N}} \mathbb{Z}/p^n\mathbb{Z}$, tenemos que todo elemento en $\mathbb{Z}_p$ se escribe de manera única como $x = \sum_{n \in \mathbb{N}} \alpha_n p^n$, $\alpha_n \in \{0, 1, \ldots, p-1\}$, y donde $p^n \xrightarrow[n \to +\infty]{} 0$ en $\mathbb{Z}_p$.

Ejercicios ① Sea $\mathbb{K}$ un cuerpo completo resp. a un valor absoluto no-arquimedeano $|\cdot|$. Probar que la serie $\sum_{n\in\mathbb{N}} a_n$ converge en $\mathbb{K}$ $\Leftrightarrow$ $\lim_{n\to+\infty} a_n = 0$.

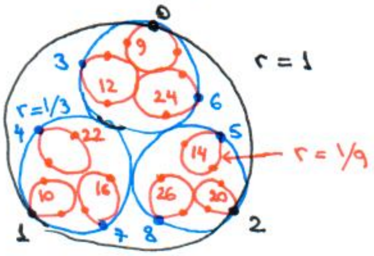
② Probar que $\mathbb{Z}_p$ es la adherencia de $\mathbb{Z}$ en $\mathbb{Q}_p$.

③ Sea $\mathcal{C} := \{ \alpha\in\mathbb{R},\ \exists (\alpha_n)_{n\in\mathbb{N}} \in \{0,2\}^{\mathbb{N}} \text{ tq } \alpha = \sum_{n\in\mathbb{N}} \alpha_n 3^{-(n+1)} \}$ conjunto de Cantor. Probar que $\mathbb{Z}_2 \xrightarrow{\sim} \mathcal{D}$, $\sum_{n\in\mathbb{N}} \alpha_n 2^n \mapsto \sum_{n\in\mathbb{N}} 2\alpha_n 3^{-(n+1)}$ es un homeomorfismo.

④ Probar que $\mathbb{Z}_p$ <u>no</u> es numerable.

<u>Obs</u>: Se recomienda leer J. Neukirch, Ch. II, §2 para más detalles.

Una representación gráfica de $\mathbb{Z}_3$:



$\mathbb{Z}_3 \xrightarrow{g_1} \mathbb{Z}/3\mathbb{Z}$

$\mathbb{Z}_3 \xrightarrow{g_2} \mathbb{Z}/9\mathbb{Z}$

$\mathbb{Z}_3 \xrightarrow{g_3} \mathbb{Z}/27\mathbb{Z}$

<u>Hecho</u> (Haar, 1933): Todo grupo abeliano localmente compacto admite una medida μ en la σ-álgebra generada por los subconj. compactos del grupo G tal que:

① $\mu(K) < +\infty$ para todo $K \subseteq G$ compacto.

② $\mu(E) = \inf\{\mu(\mathcal{U}),\ E\subseteq\mathcal{U} \text{ y } \mathcal{U} \text{ abierto}\}$ para todo $E\subseteq G$ de Borel.

③ $\mu(\mathcal{U}) = \sup\{\mu(K),\ K\subseteq\mathcal{U} \text{ y } K \text{ compacto}\}$ para todo $\mathcal{U}\subseteq G$ abierto.

④ $\mu(x+E) = \mu(E)$ $\forall x\in G$ y $\forall E\subseteq G$ de Borel.

Más aún, μ es única salvo mult. por escalares y se llama la <u>medida de Haar de G</u>

<u>Def</u>: Si $\mathbb{K}_v$ es un cuerpo local (i.e. $\mathcal{O}_v/\mathfrak{m}_v$ es finito) se define dx_v como la única medida de Haar de $\mathbb{K}_v$ tal que $\int_{\mathcal{O}_v} dx_v = 1$.

<u>Ejemplo</u>: En $\mathbb{Q}_p$ se tiene que $\int_{\mathbb{Z}_p} dx_p = 1$. Notar que $\mathbb{Z}_p/p\mathbb{Z}_p \cong \mathbb{F}_p$ y luego $\mathbb{Z}_p = p\mathbb{Z}_p \sqcup (p\mathbb{Z}_p+1) \sqcup \dots \sqcup (p\mathbb{Z}_p+p-1)$. Por la propiedad ④, $\int_{p\mathbb{Z}_p} dx_p = \frac{1}{p}$. Más generalmente, $\int_{p^n\mathbb{Z}_p} dx_p = \frac{1}{p^n}$ $\forall n\in\mathbb{N}^{\geq 1}$.

<u>Obs</u>: Si $\mathbb{K}_v \cong \mathbb{R}$ se define dx_v como la medida de Lebesgue.

§22. <u>Restricción y extensión de valores absolutos</u>

En esta sección consideramos extensiones $\mathbb{L}/\mathbb{K}$, dada por $\rho_{\mathbb{L}/\mathbb{K}} : \mathbb{K} \hookrightarrow \mathbb{L}$, y decimos:

① Si $|\cdot| : \mathbb{L} \to \mathbb{R}^{\geq 0}$ valor absoluto, entonces $|\cdot|_{|\mathbb{K}} := |\cdot| \circ \rho_{\mathbb{L}/\mathbb{K}}$ es la <u>restricción</u> a $\mathbb{K}$.

② Si $|\cdot| : \mathbb{K} \to \mathbb{R}^{\geq 0}$ valor absoluto, entonces una <u>extensión</u> a $\mathbb{L}$ es $|\cdot|' : \mathbb{L} \to \mathbb{R}^{\geq 0}$ valor absoluto tq $|\cdot|'_{|\mathbb{K}} = |\cdot|$.

<u>Prop</u>: Sea $\mathbb{L}/\mathbb{K}$ una extensión algebraica y sea $|\cdot| : \mathbb{L} \to \mathbb{R}^{\geq 0}$ valor absoluto. Entonces:

① $|\cdot|$ es trivial $\Longleftrightarrow$ $|\cdot|_{|\mathbb{K}}$ es trivial.

② $|\cdot|$ es no-arquimedeano $\Longleftrightarrow$ $|\cdot|_{|\mathbb{K}}$ es no-arquimedeano.

<u>Dem</u>: ($\Rightarrow$) es por definición en ① y ②. Para ($\Leftarrow$) en ② notar que $\mathbb{Z} \overset{|\cdot|_{|\mathbb{K}} \text{ no-arq.}}{\subseteq} \{x\in\mathbb{K},\ |x|_{|\mathbb{K}} \leq 1\} \subseteq \{x\in\mathbb{L},\ |x|\leq 1\}$ y luego $|\cdot|$ no-arquimedeano. Para ($\Leftarrow$) en ① consideramos $x\in\mathbb{L}$ y $\mu_x^{\mathbb{K}}(T) = T^d + \sum_{i=0}^{d-1} a_i T^i$ $\Rightarrow$ $x^d = -\sum_{i=0}^{d-1} a_i x^i$ y así, dado que $|\cdot|$ no-arquimedeano por

① (pues $|\cdot|_{\mathbb{K}}$ trivial), se tiene $|x|^d \leq \max\limits_{0\leq i\leq d-1} \{ \underbrace{|-a_i|_{\mathbb{K}}}_{\leq 1} |x|^i \} \leq \max\{1, |x|, \ldots, |x|^{d-1}\}$ $\Rightarrow |x| \leq 1$. Luego, si $x \in \mathbb{L}^*$ entonces $|x| \leq 1$ y también $|x^{-1}| \leq 1$ y así $|x| = 1$ ■

<u>Notación</u>: En todo lo que sigue, $\mathbb{L}/\mathbb{K}$ es una extensión <u>finita</u>. Dado $|\cdot|_{\mathbb{K}}$ un valor absoluto en $\mathbb{K}$ y $v \in Pl(\mathbb{K})$ el lugar asociado, denotamos por $|\cdot|_{\mathbb{K}_v}$ la única ext. continua de $|\cdot|_{\mathbb{K}}$ a $\mathbb{K}_v$. Además, fijaremos una clausura algebraica $\overline{\mathbb{K}_v}$ de $\mathbb{K}_v$, con $|\cdot|_{\overline{\mathbb{K}_v}} : \overline{\mathbb{K}_v} \to \mathbb{R}^{\geq 0}$ la única extensión de $|\cdot|_{\mathbb{K}_v}$, y denotamos por $\overline{\mathbb{K}} \subseteq \overline{\mathbb{K}_v}$ la clausura algebraica de $\mathbb{K}$ en $\overline{\mathbb{K}_v}$ (pensando $\mathbb{K} \subseteq \mathbb{K}_v$, como siempre). Así:

$$\begin{array}{ccc} & & \overline{\mathbb{K}_v} \\ & \mathbb{K}_v \diagup & | \\ \mathbb{L} & | & \overline{\mathbb{K}} \\ \text{finita}\diagdown & \mathbb{K} \diagup & \end{array}$$

Por último, recordemos que si $\mathbb{K} \subseteq \mathbb{L}_1 \subseteq \mathbb{M}$ y $\mathbb{K} \subseteq \mathbb{L}_2 \subseteq \mathbb{M}$ entonces $\mathbb{L}_1\mathbb{L}_2 \overset{\text{def}}{=} \mathbb{K}(\mathbb{L}_1 \cup \mathbb{L}_2) \subseteq \mathbb{M}$.

<u>Prop / Def</u>: Sea $|\cdot|_{\mathbb{L}}$ una extensión de $|\cdot|_{\mathbb{K}}$ a $\mathbb{L}$, y sea $w \in Pl(\mathbb{L})$ el lugar definido por $|\cdot|_{\mathbb{L}}$. En tal caso, escribimos $w | v$ (la topología de $\mathbb{K}$ está inducida por w). Sea $\mathbb{K}_v'$ la adherencia de $\mathbb{K}$ en $\mathbb{L}_w$, entonces:

① $\exists!$ $\mathbb{K}$-isomorfismo $\varphi : \mathbb{K}_v \xrightarrow{\sim} \mathbb{K}_v'$ tal que $|\cdot|_{\mathbb{L}_w} \circ \varphi = |\cdot|_{\mathbb{K}_v}$. En part, podemos ver a $\mathbb{L}_w$ como una $\mathbb{K}_v$-álgebra.

② $\mathbb{L}_w = \mathbb{L} \cdot \mathbb{K}_v$ y la extensión $\mathbb{L}_w / \mathbb{K}_v$ es <u>finita</u>.

Definimos el <u>grado local de $\mathbb{L}/\mathbb{K}$ en $w \in Pl(\mathbb{L})$</u> por $N_{w/v} = N_w := [\mathbb{L}_w : \mathbb{K}_v]$.

<u>Dem</u>: Para ① basta notar que $\mathbb{K}_v'$ es cerrado en $\mathbb{L}_w$ y luego completo, y luego φ se obtiene por unicidad de la completación ✓ Para ②, consideramos una base $(e_1, \ldots, e_d)$ de $\mathbb{L}$ como $\mathbb{K}$-ev. Así, $\mathbb{L}\mathbb{K}_v \overset{\text{def}}{=} \mathbb{L}\mathbb{K}_v' = \sum_{i=1}^{d} \mathbb{K}_v' e_i \subseteq \mathbb{L}_w$. Luego, $\mathbb{L}\mathbb{K}_v'$ es un $\mathbb{K}_v'$-ev de dim <u>finita</u> y por ende es completo, y en part. <u>cerrado</u>, en $\mathbb{L}_w$. Dado que $\mathbb{L} \subseteq \mathbb{L}\mathbb{K}_v'$ y $\mathbb{L}$ es denso en $\mathbb{L}_w$ concluimos que $\mathbb{L}_w = \mathbb{L}\mathbb{K}_v'$ y además se tiene que $[\mathbb{L}_w : \mathbb{K}_v] \leq d = [\mathbb{L} : \mathbb{K}] < +\infty$ ■

<u>Ejemplo</u>: Si $v \in Pl(\mathbb{K})$ es arquimedeano entonces $N_{w/v} \in \{1, 2\}$ pues $\mathbb{K}_v \simeq \mathbb{R}$ ó $\mathbb{C}$.

<u>Obs</u>: Para todo $\sigma : \mathbb{L} \hookrightarrow \overline{\mathbb{K}}$ en $\Sigma_{\mathbb{L}/\mathbb{K}} \neq \emptyset$, se tiene que $|\cdot|_{\overline{\mathbb{K}_v}} \circ \sigma$ es un valor absoluto en $\mathbb{L}$ que extiende $|\cdot|_{\mathbb{K}}$.

<u>Teorema</u>: ① <u>Toda</u> extensión de $|\cdot|_{\mathbb{K}}$ a $\mathbb{L}$ es de la forma $|\cdot|_{\overline{\mathbb{K}_v}} \circ \sigma$ para cierto $\sigma \in \Sigma_{\mathbb{L}/\mathbb{K}}$.
② Sean $\sigma, \sigma' \in \Sigma_{\mathbb{L}/\mathbb{K}}$. Entonces: $|\cdot|_{\overline{\mathbb{K}_v}} \circ \sigma = |\cdot|_{\overline{\mathbb{K}_v}} \circ \sigma' \Leftrightarrow \exists \tau \in Aut_{\mathbb{K}_v}(\overline{\mathbb{K}_v})$, $\sigma' = \tau \circ \sigma$.

<u>Dem</u>: Para ①, consideramos $|\cdot|_{\mathbb{L}}$ una extensión de $|\cdot|_{\mathbb{K}}$ a $\mathbb{L}$. Vimos que $\mathbb{L}_w / \mathbb{K}_v$ es una extensión finita y que $|\cdot|_{\mathbb{L}_w}$ extiende $|\cdot|_{\mathbb{K}_v}$. Por otro lado, si $\tilde{\sigma} : \mathbb{L}_w \hookrightarrow \overline{\mathbb{K}_v}$ en $\Sigma_{\mathbb{L}_w/\mathbb{K}_v} \neq \emptyset$ entonces $|\cdot|_{\overline{\mathbb{K}_v}} \circ \tilde{\sigma}$ extiende a $|\cdot|_{\mathbb{K}_v}$ también. Dado que para cuerpos completos las extensiones son <u>únicas</u>, tenemos que $|\cdot|_{\mathbb{L}_w} = |\cdot|_{\overline{\mathbb{K}_v}} \circ \tilde{\sigma}$. Así, si definimos $\sigma := \tilde{\sigma}|_{\mathbb{L}}$ entonces obtenemos $|\cdot|_{\mathbb{L}} = |\cdot|_{\overline{\mathbb{K}_v}} \circ \sigma$ ✓

Para ②: Notamos primero que $\sigma, \sigma' : \mathbb{L} \hookrightarrow \overline{\mathbb{K}}$ son continuas resp. a $|\cdot|_{\mathbb{L}} := |\cdot|_{\mathbb{K}_v} \circ \sigma$ $= |\cdot|_{\mathbb{K}_v} \circ \sigma'$. Por otro lado, si $\mathbb{L}^n \subseteq \overline{\mathbb{K}}$ es la clausura normal de $\mathbb{L}/\mathbb{K}$ en $\overline{\mathbb{K}}$

entonces $\mathbb{L}^n$ es la más pequeña ext. normal de $\mathbb{K}$ en $\overline{\mathbb{K}}$ que contiene $\sigma(\mathbb{L})$ $\forall \sigma \in \Sigma_{\mathbb{L}/\mathbb{K}}$. Explícitamente, si $\mathbb{L} = \mathbb{K}(\alpha_1, \dots, \alpha_r)$ entonces $\mathbb{L}^n = \mathbb{K}(\{\beta \in \overline{\mathbb{K}}, \exists i \in \{1,\dots,r\} \text{ tq } \mu_{\alpha_i}^{\mathbb{K}}(\beta) = 0\})$, y en part. $\mathbb{L}^n/\mathbb{K}$ es una extensión finita. Luego, $\mathbb{L}^n \mathbb{K}_v$ $(\subseteq \overline{\mathbb{K}_v})$ es una ext. finita de $\mathbb{K}_v$ y en part. es completa. Dado que $\sigma(\mathbb{L}) \subseteq \mathbb{L}^n \subseteq \mathbb{L}^n\mathbb{K}_v$ y $\sigma'(\mathbb{L}) \subseteq \mathbb{L}^n \mathbb{K}_v$, se puede extender σ y σ' continuamente a $\tilde{\sigma}, \tilde{\sigma}' : \mathbb{L}_w \hookrightarrow \mathbb{L}^n\mathbb{K}_v$ y así $\tilde{\sigma}, \tilde{\sigma}' \in \Sigma_{\mathbb{L}_w/\mathbb{K}_v}$. Usando la extensión de morfismos de cuerpos, $\exists \tau \in \mathrm{Aut}_{\mathbb{K}_v}(\overline{\mathbb{K}_v})$ tq $\tilde{\sigma}' = \tau \circ \tilde{\sigma}$ y luego, al restringirse a $\mathbb{L}$, obtenemos $\sigma' = \tau \circ \sigma$ ✓ Por último, basta notar que si $\tau \in \mathrm{Aut}_{\mathbb{K}_v}(\overline{\mathbb{K}_v})$ entonces $|\cdot|_{\overline{\mathbb{K}_v}} \circ \tau$ es un valor absoluto que extiende $|\cdot|_{\mathbb{K}_v}$ y luego $|\cdot|_{\overline{\mathbb{K}_v}} \circ \tau = |\cdot|_{\overline{\mathbb{K}_v}}$ (unicidad) ■

Corolario (Fórmula de Ramificación): Supongamos además que la extensión $\mathbb{L}/\mathbb{K}$ es finita y separable. Entonces:

1. $[\mathbb{L}:\mathbb{K}] = \sum_{w|v} N_w$
2. $N_{\mathbb{L}/\mathbb{K}}(\alpha) = \prod_{w|v} N_{\mathbb{L}_w/\mathbb{K}_v}(\alpha)$ para todo $\alpha \in \mathbb{L}$.
3. $\mathrm{Tr}_{\mathbb{L}/\mathbb{K}}(\alpha) = \sum_{w|v} \mathrm{Tr}_{\mathbb{L}_w/\mathbb{K}_v}(\alpha)$ para todo $\alpha \in \mathbb{L}$.

Dem: Si $w|v$, entonces $\mathbb{L}_w = \mathbb{L}\mathbb{K}_v$. Sea $\alpha \in \mathbb{L}$ elemento primitivo tq $\mathbb{L} = \mathbb{K}(\alpha)$. $\Rightarrow \mathbb{L}_w = \mathbb{K}_v(\alpha)$. Como $\mu_\alpha^{\mathbb{K}_v} \mid \mu_\alpha^{\mathbb{K}}$ y $\mu_\alpha^{\mathbb{K}}$ separable, tenemos que α separable sobre $\mathbb{K}_v$. Así, la extensión $\mathbb{L}_w/\mathbb{K}_v$ es separable. Veamos ①:
En este caso, $[\mathbb{L}:\mathbb{K}] = [\mathbb{L}:\mathbb{K}]_s \overset{\text{def}}{=} \#\Sigma_{\mathbb{L}/\mathbb{K}}$. Por la demostración del Teorema ②, hay una biyección $\Sigma_{\mathbb{L}/\mathbb{K}} \xrightarrow[1:1]{\sim} \coprod_{w|v} \Sigma_{\mathbb{L}_w/\mathbb{K}_v}$, $\sigma \mapsto \tilde{\sigma} : \mathbb{L}_w \to \overline{\mathbb{K}_v}$ (con inversa $\tilde{\sigma} \mapsto \tilde{\sigma}|_{\mathbb{L}}$).
Luego, $[\mathbb{L}:\mathbb{K}] = \sum_{w|v} \#\Sigma_{\mathbb{L}_w/\mathbb{K}_v} = \sum_{w|v} [\mathbb{L}_w : \mathbb{K}_v]$ pues $\mathbb{L}_w/\mathbb{K}_v$ separable ✓
Veamos ② y ③: La biyección anterior permite calcular tanto
$N_{\mathbb{L}/\mathbb{K}}(\alpha) = \prod_{\sigma \in \Sigma_{\mathbb{L}/\mathbb{K}}} \sigma(\alpha) = \prod_{w|v} \prod_{\tilde{\sigma} \in \Sigma_{\mathbb{L}_w/\mathbb{K}_v}} \tilde{\sigma}(\alpha) = \prod_{w|v} N_{\mathbb{L}_w/\mathbb{K}_v}(\alpha)$ como $\mathrm{Tr}_{\mathbb{L}/\mathbb{K}}(\alpha) = \sum_{w|v} \mathrm{Tr}_{\mathbb{L}_w/\mathbb{K}_v}(\alpha)$ ■

§23. Completación para anillos de Dedekind

El objetivo de esta sección es describir cómo los valores absolutos generalizan a los ideales primos en el caso de anillos de Dedekind.

Notación: En lo que sigue, $A \subseteq \mathbb{K} = \mathrm{Fr}(A)$ es un anillo de Dedekind, $\mathbb{L}/\mathbb{K}$ una extensión finita separable y $B = \tilde{A} \subseteq \mathbb{L}$ la clausura integral de A.
Sea $\mathfrak{p} \in \mathrm{Spec}(A)^*$ y $\mathfrak{q} \in \mathrm{Spec}(B)^*$ con $\mathfrak{q}|\mathfrak{p}$. Entonces podemos pensar $\mathfrak{p} \in \mathrm{Pl}(\mathbb{K})$ y $\mathfrak{q} \in \mathrm{Pl}(\mathbb{L})$ pues $v := v_{\mathfrak{p}} : \mathbb{K} \twoheadrightarrow \mathbb{Z} \cup \{+\infty\}$ y $w := v_{\mathfrak{q}} : \mathbb{L} \twoheadrightarrow \mathbb{Z} \cup \{+\infty\}$ son valuaciones discretas sobreyectivas, y luego definen lugares no-arquimedianos.

⚠ Obs importante: Dado que $\mathfrak{p}B \overset{\text{def}}{=} \prod_{\mathfrak{q}|\mathfrak{p}} \mathfrak{q}^{e_{\mathfrak{q}|\mathfrak{p}}}$ tenemos que para todo $x \in \mathbb{K}$:
$v_{\mathfrak{q}}(\rho_{\mathbb{L}/\mathbb{K}}(x)) = e_{\mathfrak{q}|\mathfrak{p}}\, v_{\mathfrak{p}}(x)$ y más generalmente $v_{\mathfrak{q}}(IB) = e_{\mathfrak{q}|\mathfrak{p}}\, v_{\mathfrak{p}}(I)$ $\forall I \in \mathcal{I}(A)$.
Así, el diagrama siguiente es conmutativo:

$$\begin{array}{ccc} \mathbb{K} & \xhookrightarrow{\rho_{\mathbb{L}/\mathbb{K}}} & \mathbb{L} \\ v\downarrow & & \downarrow w \\ \mathbb{Z}\cup\{+\infty\} & \xrightarrow{\cdot e_{\mathfrak{q}|\mathfrak{p}}} & \mathbb{Z}\cup\{+\infty\} \end{array}$$

Luego, si $\alpha \in \mathbb{R}^{>1}$ es tal que $|x|_v = \alpha^{-v(x)}$ y $|y|_w = \alpha^{-w(y)}$ entonces se tiene que $|\rho_{\mathbb{L}/\mathbb{K}}(x)|_w = |x|_v^{e_{\mathfrak{q}|\mathfrak{p}}}$ $\forall x \in \mathbb{K}$. En particular, $|\cdot|_w' := |\cdot|_w^{1/e_{\mathfrak{q}|\mathfrak{p}}}$ es una extensión de $|\cdot|_v : \mathbb{K} \to \mathbb{R}^{>0}$ a $\mathbb{L}$.

Teorema (Fórmula para el grado local): Para todos $\mathfrak{p} \in \mathrm{Spec}(A)^*$ y $\mathfrak{q} \in \mathrm{Spec}(B)^*$ con $\mathfrak{q}|\mathfrak{p}$ se tiene que $N_{w|v} = e_{\mathfrak{q}|\mathfrak{p}} f_{\mathfrak{q}|\mathfrak{p}}$ donde $v = v_\mathfrak{p}$ y $w = v_\mathfrak{q}$.

La estrategia será aprovecharnos de las siguientes inclusiones:

$$\begin{tikzcd}[column sep=small, row sep=small] & \mathbb{L}_w & \\ \mathbb{L} \arrow[ur, dash] & & \mathbb{K}_v \arrow[ul, dash] \\ & \mathbb{K} \arrow[ul, dash] \arrow[ur, dash] & \end{tikzcd} \qquad \begin{array}{ccccccc} \mathfrak{m}_v & \subseteq & \mathcal{O}_v & — & \mathcal{O}_w & \supseteq & \mathfrak{m}_w \\ & & \cup\!\shortmid & & \cup\!\shortmid & & \\ \mathfrak{p}A_\mathfrak{p} & \subseteq & A_\mathfrak{p} & — & B_\mathfrak{q} & \supseteq & \mathfrak{q}B_\mathfrak{q} \\ & & | & & & & \\ \mathfrak{p} & \subseteq & A & — & B & \supseteq & \mathfrak{q} \end{array}$$

Aquí: $\mathcal{O}_v = \{x \in \mathbb{K}_v, |x|_v \leq 1\}$

$\mathcal{O}_w = \{y \in \mathbb{L}_w, |y|_w \leq 1\}$

Lema: $A/\mathfrak{p} \xrightarrow{\sim} A_\mathfrak{p}/\mathfrak{p}A_\mathfrak{p} \xrightarrow{\sim} \mathcal{O}_v/\mathfrak{m}_v$ y $B/\mathfrak{q} \xrightarrow{\sim} B_\mathfrak{q}/\mathfrak{q}B_\mathfrak{q} \xrightarrow{\sim} \mathcal{O}_w/\mathfrak{m}_w$.

Dem: El primer isomorfismo fue discutido en §13. Dado que para $x \in \mathbb{K}$, $|x|_v = \alpha^{-v_\mathfrak{p}(x)}$ tenemos que $\{x \in \mathbb{K}, |x|_v \leq 1\} \overset{\text{dy}}{=} A_\mathfrak{p}$ y $\{x \in \mathbb{K}, |x|_v < 1\} \overset{\text{dy}}{=} \mathfrak{p}A_\mathfrak{p}$. Vimos en §21 que hay isomorfismos $\mathcal{O}_v/\mathfrak{m}_v^n \simeq A_\mathfrak{p}/(\mathfrak{p}A_\mathfrak{p})^n$ $\forall n \in \mathbb{N}$ y luego $A_\mathfrak{p}/\mathfrak{p}A_\mathfrak{p} \simeq \mathcal{O}_v/\mathfrak{m}_v$, donde $\mathfrak{m}_v \subseteq \mathcal{O}_v \subseteq \mathbb{K}_v$. Análogamente, $B_\mathfrak{q}/\mathfrak{q}B_\mathfrak{q} \simeq \mathcal{O}_w/\mathfrak{m}_w$ ■

Prop: $\mathcal{O}_w \subseteq \mathbb{L}_w$ es la clausura integral de $\mathcal{O}_v \subseteq \mathbb{K}_v$.

Dem: Sea $\overline{\mathbb{K}_v}$ una clausura algebraica de $\mathbb{K}_v$ y sean $|\cdot|_{\overline{\mathbb{K}_v}}$, $|\cdot|_{\mathbb{K}_v}$ las únicas ext. de $|\cdot|_v : \mathbb{K} \to \mathbb{R}^{\geq 0}$. Recordemos que si $\sigma : \mathbb{L}_w \hookrightarrow \overline{\mathbb{K}_v}$ en $\Sigma_{\mathbb{L}_w/\mathbb{K}_v}$ entonces $|\cdot|_{\mathbb{L}_w} = |\cdot|_{\overline{\mathbb{K}_v}} \circ \sigma$. Sea $\alpha \in \mathcal{O}_w$. Entonces, $\forall \sigma \in \Sigma_{\mathbb{L}_w/\mathbb{K}_v}$ se tiene $\sigma(\alpha) \in \{\beta \in \overline{\mathbb{K}_v}, |\beta|_{\overline{\mathbb{K}_v}} \leq 1\} \overset{\text{dy}}{=} \mathcal{O}_{\overline{\mathbb{K}_v}}$. Dado que $\mathbb{L}/\mathbb{K}$ es separable, entonces $\mathbb{L}_w/\mathbb{K}_v$ también y luego:

$$\chi_\alpha^{\mathbb{K}_v} = \prod_{\sigma \in \Sigma_{\mathbb{L}_w/\mathbb{K}_v}} (X - \sigma(\alpha)) \in \mathcal{O}_{\overline{\mathbb{K}_v}}[X] \cap \mathbb{K}_v[X] = \mathcal{O}_v[X] \Rightarrow \alpha \text{ entero sobre } \mathcal{O}_v.$$

Luego, $\mathcal{O}_w$ está contenido en la clausura integral de $\mathcal{O}_v$. Recíprocamente, dado que $|x|_{\mathbb{L}_w} = |N_{\mathbb{L}_w/\mathbb{K}_v}(x)|_{\mathbb{K}_v}^{1/[\mathbb{L}_w : \mathbb{K}_v]}$ tenemos que si $x \in \mathbb{L}_w$ es entero sobre $\mathcal{O}_v$ entonces $N_{\mathbb{L}_w/\mathbb{K}_v}(x) \in \mathcal{O}_v$ y luego $|x|_{\mathbb{L}_w} \leq 1$, ie, $x \in \mathcal{O}_w$ ■

Dem del Teorema: Dado que $\mathcal{O}_v \subseteq \mathbb{K}_v$ es un anillo de Dedekind (por ser anillo de valuación discreta), $\mathbb{L}_w/\mathbb{K}_v$ es una extensión finita separable, y $\mathcal{O}_w = \widetilde{\mathcal{O}_v} \subseteq \mathbb{L}_w$ es la clausura integral de $\mathcal{O}_v$ en $\mathbb{L}_w$, la fórmula de ramificación (ver §13) implica en este caso que $N_{w|v} \overset{\text{dy}}{=} [\mathbb{L}_w : \mathbb{K}_v] = \sum_{\eta | \mathfrak{m}_v} e_\eta f_\eta$. Como $(\mathcal{O}_v, \mathfrak{m}_v)$ y $(\mathcal{O}_w, \mathfrak{m}_w)$ anillos locales, $\eta = \mathfrak{m}_w$ es el único ideal primo tal que $\mathfrak{m}_w | \mathfrak{m}_v$ y así $N_{w|v} = e_{\mathfrak{m}_w|\mathfrak{m}_v} f_{\mathfrak{m}_w|\mathfrak{m}_v}$, donde $f_{\mathfrak{m}_w/\mathfrak{m}_v} \overset{\text{dy}}{=} [\mathcal{O}_w/\mathfrak{m}_w : \mathcal{O}_v/\mathfrak{m}_v] \overset{\text{Lema}}{=} [B/\mathfrak{q} : A/\mathfrak{p}] \overset{\text{dy}}{=} f_{\mathfrak{q}|\mathfrak{p}}$. Resta probar que $e_{\mathfrak{m}_w|\mathfrak{m}_v} = e_{\mathfrak{q}|\mathfrak{p}}$: La valuación $v = v_\mathfrak{p} : \mathbb{K}^* \twoheadrightarrow \mathbb{Z}$ (resp. $w = v_\mathfrak{q} : \mathbb{L}^* \twoheadrightarrow \mathbb{Z}$) se extiende continuamente a una única valuación $\hat{v} : \mathbb{K}_v^* \twoheadrightarrow \mathbb{Z}$ (resp. $\hat{w} : \mathbb{L}_w^* \twoheadrightarrow \mathbb{Z}$), de donde obtenemos el diagrama conmutativo

$$\begin{tikzcd} \mathbb{K} \arrow[rr, "v"] \arrow[dr, hook] \arrow[dd, hook] & & \mathbb{Z} \cup \{+\infty\} \arrow[dd, "\cdot\, e_{\mathfrak{q}|\mathfrak{p}} \ (\text{cf. Obs importante})"] \\ & \mathbb{K}_v \arrow[ur, "\hat{v}"] \arrow[dd, hook] & \\ \mathbb{L} \arrow[rr, dashed, "w"] \arrow[dr, hook] & & \mathbb{Z} \cup \{+\infty\} \\ & \mathbb{L}_w \arrow[ur, "\hat{w}"] & \end{tikzcd}$$

$\Rightarrow e_{\mathfrak{m}_w|\mathfrak{m}_v} = e_{\mathfrak{q}|\mathfrak{p}}$ por la Obs. importante. Así, $N_{w|v} = e_{\mathfrak{q}|\mathfrak{p}} f_{\mathfrak{q}|\mathfrak{p}}$ ■

§24. Fórmula del Producto y Norma de ideales

Recordemos (ver §17) que $Pl(\mathbb{Q}) \simeq \mathcal{P} \cup \{\infty\}$, con $\mathcal{P} = \{p \in \mathbb{N} \text{ número primo}\}$, de donde se deduce la fórmula del producto $\prod_{v \in Pl(\mathbb{Q})} |x|_v = 1$ para todo $x \in \mathbb{Q}^*$.

Def: Sea $\mathbb{K}$ un cuerpo de números y $w \in Pl(\mathbb{K})$. Sea $v \in Pl(\mathbb{Q})$ el lugar inducido por w (ie, $w | v$). El <u>valor absoluto normalizado</u> $|\cdot|_w$ está dado por

$$|\cdot|_w : \mathbb{K}_w \to \mathbb{R}^{\geq 0}, \quad x \mapsto |x|_w := |N_{\mathbb{K}_w/\mathbb{Q}_v}(x)|_v^{1/[\mathbb{K}:\mathbb{Q}]}$$

⚠ Por propiedades de la norma, $|x|_w = |x|_v^{[\mathbb{K}_w:\mathbb{Q}_v]/[\mathbb{K}:\mathbb{Q}]}$ $\forall x \in \mathbb{Q}_v$, ie, $|\cdot|_w$ <u>no</u> es una extensión de $|\cdot|_v$. Más precisamente, es una extensión de $|\cdot|_v^{[\mathbb{K}_w:\mathbb{Q}_v]/[\mathbb{K}:\mathbb{Q}]}$ y este último es un valor absoluto pues $\frac{[\mathbb{K}_w:\mathbb{Q}_v]}{[\mathbb{K}:\mathbb{Q}]} \leq 1$.

Teorema (Fórmula del Producto): Para todo $x \in \mathbb{K}^*$ se tiene que

$$\prod_{w \in Pl(\mathbb{K})} |x|_w = 1.$$

Dem: Calculamos $\prod_{w \in Pl(\mathbb{K})} |x|_w = \prod_{v \in Pl(\mathbb{Q})} \prod_{w|v} |x|_w \overset{\text{def}}{=} \prod_{v \in Pl(\mathbb{Q})} \prod_{w|v} |N_{\mathbb{K}_w/\mathbb{Q}_v}(x)|_v^{1/[\mathbb{K}:\mathbb{Q}]}$

$$= \prod_{v \in Pl(\mathbb{Q})} \Big| \prod_{w|v} N_{\mathbb{K}_w/\mathbb{Q}_v}(x) \Big|_v^{1/[\mathbb{K}:\mathbb{Q}]} \overset{§22}{=} \Big(\prod_{v \in Pl(\mathbb{Q})} \underbrace{|N_{\mathbb{K}/\mathbb{Q}}(x)|_v}_{\in \mathbb{Q}^*} \Big)^{1/[\mathbb{K}:\mathbb{Q}]} = 1^{1/[\mathbb{K}:\mathbb{Q}]} = 1 \quad ■$$

Def: Sea A un anillo conmutativo y sea $I \subseteq A$ un ideal tal que A/I es finito. Se define la <u>norma de I</u> como $N(I) := \mathrm{Card}(A/I)$.

Prop: Sea $\mathbb{K}$ un cuerpo de números y $\mathcal{O}_\mathbb{K} \subseteq \mathbb{K}$ su anillo de enteros. Entonces:

1. Para todo ideal no-nulo $I \subseteq \mathcal{O}_\mathbb{K}$ se tiene que $\mathcal{O}_\mathbb{K}/I$ es finito y además
$$N(I) = \prod_{\mathfrak{p} \in \mathrm{Spec}(\mathcal{O}_\mathbb{K})^*} N(\mathfrak{p})^{v_\mathfrak{p}(I)} = \prod_{p \in \mathcal{P}} \prod_{\mathfrak{p}|p} p^{v_\mathfrak{p}(I) f_{\mathfrak{p}|p}}$$

2. Para todo $x \in \mathcal{O}_\mathbb{K} \setminus \{0\}$, $N(\langle x \rangle) = |N_{\mathbb{K}/\mathbb{Q}}(x)|_\infty$.

Dem: Para ① notamos que $\mathcal{O}_\mathbb{K}/I \simeq \prod_{\mathfrak{p} \in \mathrm{Spec}(\mathcal{O}_\mathbb{K})^*} \mathcal{O}_\mathbb{K}/\mathfrak{p}^{v_\mathfrak{p}(I)}$ y que $\dim_{\mathbb{F}_p}(\mathcal{O}_\mathbb{K}/\mathfrak{p}) \overset{\text{def}}{=} f_{\mathfrak{p}|p}$ y luego $N(\mathfrak{p}) = \mathrm{Card}(\mathbb{F}_p^{f_{\mathfrak{p}|p}}) = p^{f_{\mathfrak{p}|p}}$ ✓ Para ②, notamos que $w := \mathfrak{p} \in Pl(\mathbb{K})$ es el lugar asociado a $v_\mathfrak{p}$ con $\mathfrak{p} \in \mathrm{Spec}(\mathcal{O}_\mathbb{K})^*$ tal que $\mathfrak{p} | p$, entonces para todo $x \in \mathbb{K}$:
$|x|_\mathfrak{p} \overset{\text{def}}{=} |N_{\mathbb{K}_\mathfrak{p}/\mathbb{Q}_p}(x)|_p^{1/[\mathbb{K}:\mathbb{Q}]} = p^{-v_p(N_{\mathbb{K}_\mathfrak{p}/\mathbb{Q}_p}(x))/[\mathbb{K}:\mathbb{Q}]}$. En particular, $x = p$ verifica $|p|_\mathfrak{p} = p^{-v_p(p^{[\mathbb{K}_\mathfrak{p}:\mathbb{Q}_p]})/[\mathbb{K}:\mathbb{Q}]} = p^{-[\mathbb{K}_\mathfrak{p}:\mathbb{Q}_p]/[\mathbb{K}:\mathbb{Q}]} \underset{\text{Ram.}}{\overset{§23}{=}} p^{-f_{\mathfrak{p}|p} e_{\mathfrak{p}|p}/[\mathbb{K}:\mathbb{Q}]}$
$\Rightarrow |p|_\mathfrak{p} = p^{-f_{\mathfrak{p}|p} v_\mathfrak{p}(p)/[\mathbb{K}:\mathbb{Q}]}$. Dado que $\forall x \in \mathbb{K}$ se tiene que $|x|_\mathfrak{p} = \alpha^{-v_\mathfrak{p}(x)}$ para cierto $\alpha \in \mathbb{R}^{>1}$, deducimos que $\alpha = p^{f_{\mathfrak{p}|p}/[\mathbb{K}:\mathbb{Q}]}$ y luego

$$|x|_\mathfrak{p} = p^{-f_{\mathfrak{p}|p} v_\mathfrak{p}(x)/[\mathbb{K}:\mathbb{Q}]} \quad \forall x \in \mathbb{K} \qquad (\star)$$

Así, para $x \in \mathcal{O}_\mathbb{K} \setminus \{0\}$ calculamos $N(\langle x \rangle) \overset{①}{=} \prod_{p \in \mathcal{P}} \prod_{\mathfrak{p}|p} p^{v_\mathfrak{p}(x) f_{\mathfrak{p}|p}} \overset{(\star)}{=} \prod_{p \in \mathcal{P}} \prod_{\mathfrak{p}|p} |x|_\mathfrak{p}^{-[\mathbb{K}:\mathbb{Q}]}$
$\overset{\text{def}}{=} \prod_{p \in \mathcal{P}} \prod_{\mathfrak{p}|p} |N_{\mathbb{K}_\mathfrak{p}/\mathbb{Q}_p}(x)|_p^{-1} = \prod_{p \in \mathcal{P}} \Big| \prod_{\mathfrak{p}|p} N_{\mathbb{K}_\mathfrak{p}/\mathbb{Q}_p}(x) \Big|_p^{-1} \overset{§22}{=} \prod_{p \in \mathcal{P}} |N_{\mathbb{K}/\mathbb{Q}}(x)|_p^{-1} = |N_{\mathbb{K}/\mathbb{Q}}(x)|_\infty$
donde la última igualdad es consecuencia de la Fórmula del Producto en $\mathbb{Q}$ ■

Ejercicio: Determinar el cardinal del anillo $\mathbb{Z}[i]/\langle a+ib \rangle$ para $(a,b) \in \mathbb{Z}^2 \setminus \{(0,0)\}$.

§25. Reticulados y Teorema de Minkowski

Recordemos que si $V \cong \mathbb{R}^d$, un reticulado (o retículo) es el grupo abeliano aditivo generado por una base de V (i.e., un $\mathbb{Z}$-módulo libre de rango d, i.e., $\simeq \mathbb{Z}^d$).
En V, la medida de Lebesgue "vol" es una medida de Haar y verifica que si $(e_1, \dots, e_d)$ es una base ortonormal de V entonces $\mathrm{vol}\left(\sum_{i=1}^{d} [0,1] e_i\right) = 1$.

Lema / Def: Sea $\Lambda = \sum_{i=1}^{d} \mathbb{Z} f_i \simeq \mathbb{Z}^d$ un reticulado en V generado por una base $(f_1, \dots, f_d)$. Entonces, el covolumen $\mathrm{covol}(\Lambda) := |\det_{(e_1,\dots,e_d)}(f_1, \dots, f_d)|$ no depende de la elección de la base de Λ ni de la base ortonormal de V.

Dem: Si $\mathcal{B} = (e_1, \dots, e_d)$ y $\mathcal{B}' = (e_1', \dots, e_d')$ (resp. $\mathcal{C} = (f_1, \dots, f_d)$ y $\mathcal{C}' = (f_1', \dots, f_d')$) son bases ortonormales de V (resp. bases de Λ) entonces $P = \mathrm{Mat}_{\mathcal{B}}(\mathcal{B}') \in O_d(\mathbb{R})$ y $Q = \mathrm{Mat}_{\mathcal{C}}(\mathcal{C}')$ en $GL_d(\mathbb{Z})$. Luego, $|\det(P)| = |\det(Q)| = 1$ ✓ ■

Obs (medida cociente): Dado que $\mathrm{vol}(x + B) = \mathrm{vol}(B)$ $\forall x \in V$ y todo $B \subseteq V$ Borel, podemos definir una medida μ en el cociente V/Λ: si $B \subseteq V$ es un Borel tal que $\pi|_B$ es inyectiva, donde $\pi : V \twoheadrightarrow V/\Lambda$, entonces definimos $\mu(\pi(B)) := \mathrm{vol}(B)$. Así, tenemos que $\mu(E/\Lambda) \overset{\text{dy}}{=} \mathrm{covol}(\Lambda)$.

Lema (Minkowski): Sea $\Lambda \subseteq V$ un reticulado, y sea $S \subseteq V$ medible tal que
$$\mathrm{vol}(S) > \mathrm{covol}(\Lambda).$$
Entonces, $\exists x, y \in S$ tal que $x - y \in \Lambda \setminus \{0\}$.

Dem: Como $\pi(S) \subseteq V/\Lambda$ se tiene $\mu(\pi(S)) \leq \mu(V/\Lambda) \overset{\text{dy}}{=} \mathrm{covol}(\Lambda) < \mathrm{vol}(S)$ y luego $\pi|_S$ no es inyectiva ■

Teorema del Reticulado de Minkowski (1889): Sea $\Lambda \simeq \mathbb{Z}^d$ un reticulado en $V \simeq \mathbb{R}^d$. Sea $C \subseteq V$ un conjunto medible y convexo tal que $C = -C$ (i.e., si $x \in C$ entonces $-x \in C$). Si alguna de las condiciones sgtes se cumple:
① $\mathrm{vol}(C) > 2^d \, \mathrm{covol}(\Lambda)$, o bien
② $\mathrm{vol}(C) \geq 2^d \, \mathrm{covol}(\Lambda)$ y C compacto.
Entonces, $C \cap \Lambda \neq \{0\}$.

Dem: Si se verifica ①, consideramos $S := \frac{1}{2} C$ y notamos que $\mathrm{vol}(S) = \frac{1}{2^d} \mathrm{vol}(C) > \mathrm{covol}(\Lambda)$ $\overset{\text{Lema}}{\Rightarrow}$ $\exists x, y \in S$ tq $x - y \in \Lambda \setminus \{0\}$. Dado que C convexo y $C = -C$, $2\left(\frac{x-y}{2}\right) = x - y \in C$ ✓
Si se verifica ②, consideramos $C_m := \left(1 + \frac{1}{m+1}\right) C$ para $m \in \mathbb{N}$. Dado que C_m verifica ①, $\exists x_m \in C_m \cap (\Lambda \setminus \{0\})$ $\forall m \in \mathbb{N}$ y en part $x_m \in 2C \cap (\Lambda \setminus \{0\})$ $\forall m \in \mathbb{N}$. Como el conjunto $2C \cap (\Lambda \setminus \{0\})$ es discreto y compacto, debe ser finito. Así, $\exists$ subsucesión $(x_{m_i})_{i \in \mathbb{N}}$ constante y cuyo límite $x = \lim_{i \to +\infty} x_{m_i} \in \bigcap_{m \in \mathbb{N}} C_m = C$. Así, $x \in C \cap (\Lambda \setminus \{0\})$ ■

Prop: Sean $\Lambda \simeq \mathbb{Z}^d$ y $\Lambda' \simeq \mathbb{Z}^d$ reticulados en $V \simeq \mathbb{R}^d$ tales que $\Lambda' \subseteq \Lambda$. Entonces, se tiene que $[\Lambda : \Lambda'] < +\infty$ y $\mathrm{covol}(\Lambda') = [\Lambda : \Lambda'] \, \mathrm{covol}(\Lambda)$.

Dem: Por el Teorema de la base adaptada, $\exists$ base $(e_1, \dots, e_d)$ de Λ y $\lambda_1, \dots, \lambda_d \in \mathbb{N}^{\geq 1}$ con $\lambda_1 | \lambda_2 | \cdots | \lambda_d$ tq $(\lambda_1 e_1, \dots, \lambda_d e_d)$ es una base de Λ'. Así, $\Lambda/\Lambda' \cong \prod_{i=1}^{d} \mathbb{Z}/\lambda_i \mathbb{Z}$.

De lo anterior, tenemos que $[\Lambda : \Lambda'] = \prod_{i=1}^{d} \lambda_i$. Por último, si $\mathcal{B}$ es una base ortonormal de $V \simeq \mathbb{R}^d$, entonces $\mathrm{covol}(\Lambda') \overset{\text{def}}{=} |\det_{\mathcal{B}}(\lambda_1 e_1, \ldots, \lambda_d e_d)| = \prod_{i=1}^{d} \lambda_i \cdot |\det_{\mathcal{B}}(e_1, \ldots, e_d)|$ y luego $\mathrm{covol}(\Lambda') = [\Lambda : \Lambda']\ \mathrm{covol}(\Lambda)$ ■

Terminemos la sección recordando la sgte caracterización de los reticulados de $\mathbb{R}^d$:

<u>Hecho</u>: Sea $V \simeq \mathbb{R}^d$ espacio vectorial real y $(\Lambda, +) \subseteq (V, +)$ subgrupo. Entonces, Λ es un <u>reticulado</u> si y sólo si:
① Λ es un conjunto discreto, y
② Λ genera de V como $\mathbb{R}$-espacio vectorial.

§26. <u>El anillo de enteros visto como reticulado</u>

Sea $\mathbb{K}$ un cuerpo de números. El objetivo de esta sección será considerar

$$\rho_\infty : \mathbb{K} \hookrightarrow \prod_{w|\infty} \mathbb{K}_w \ , \ x \longmapsto (\rho_{\mathbb{K}_w/\mathbb{K}}(x))_{w|\infty}$$

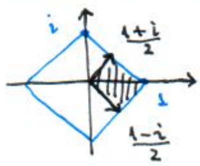
y probaremos que $\mathcal{O}_{\mathbb{K}} \simeq \mathbb{Z}^{[\mathbb{K}:\mathbb{Q}]}$ es un reticulado en el $\mathbb{R}$-e.v. $\prod_{w|\infty} \mathbb{K}_w$.

⚠ <u>Observación importante</u>: Si $\mathbb{K}$ es un cuerpo de números y $w \in \mathrm{Pl}(\mathbb{K})$ es un lugar arquimedeano (ie, $w|\infty$) tal que $[\mathbb{K}_w : \mathbb{R}] = 2$, entonces $\mathbb{K}_w \cong \mathbb{C}$ como $\mathbb{R}$-álgebras pero dicho isomorfismo <u>no</u> es canónico (hay dos $\sigma_1, \sigma_2 : \mathbb{K}_w \xrightarrow{\sim} \mathbb{C}$ en $\Sigma_{\mathbb{K}_w/\mathbb{R}}$).
Por otra parte, hay un morfismo natural de $\mathbb{R}$-álgebras

$$\varphi : \mathbb{K}_w \hookrightarrow \mathbb{C}^{\Sigma_{\mathbb{K}_w/\mathbb{R}}} \simeq \mathbb{C}^2 \ , \ x \longmapsto (\sigma(x))_{\sigma \in \Sigma_{\mathbb{K}_w/\mathbb{R}}}$$

Aquí, $\mathbb{C}^{\Sigma_{\mathbb{K}_w/\mathbb{R}}}$ es un espacio euclideano resp. a $\|(z, z')\|^2 := |z|^2 + |z'|^2$. Así, en <u>todo lo que sigue</u> dotamos a $\mathbb{K}_w \simeq \mathbb{C}$ de la estructura de espacio euclideano "<u>no tan inocente</u>" inducida por φ. Explícitamente, $\|\varphi(z)\| = \sqrt{2}\,|z|$ para todo $z \in \mathbb{K}_w$.

<u>Ejemplo</u>: Si $\mathbb{K}_w \simeq \mathbb{C}$ y $i \in \mathbb{K}_w$ es tal que $i^2 = -1$ entonces $\left(\frac{1+i}{2}, \frac{1-i}{2}\right)$ es una base ortonormal de $\mathbb{K}_w$, pues $\left\|\frac{1+i}{2}\right\| \overset{\text{def}}{=} \left\|\left(\frac{1+i}{2}, \frac{1-i}{2}\right)\right\|_{\mathbb{C}^2} = 1$.



Por convención, la medida de Haar en $\mathbb{K}_w \simeq \mathbb{C}$ será
$dx_w := 2\,dx\,dy$, para $z = x + iy$.

<u>Def</u>: El morfismo de anillos $\rho_\infty : \mathbb{K} \hookrightarrow \prod_{w|\infty} \mathbb{K}_w$, $x \longmapsto (\rho_{\mathbb{K}_w/\mathbb{K}}(x))_{w|\infty}$ se llama el <u>incrustamiento canónico</u> de $\mathbb{K}$.

<u>Notación clásica</u>: Sea $\mathbb{K}$ un cuerpo de números. Se definen:

$$r_1 := \#\{w \in \mathrm{Pl}(\mathbb{K}),\ w|\infty \text{ y } [\mathbb{K}_w : \mathbb{R}] = 1\}$$
$$r_2 := \#\{w \in \mathrm{Pl}(\mathbb{K}),\ w|\infty \text{ y } [\mathbb{K}_w : \mathbb{R}] = 2\}$$

Así, la Fórmula de Ramificación implica que:

$$[\mathbb{K} : \mathbb{Q}] = \sum_{w|\infty} N_w \overset{\text{def}}{=} r_1 + 2r_2 \overset{\text{def}}{=} \dim_{\mathbb{R}}\Big(\prod_{w|\infty} \mathbb{K}_w\Big)$$

En lo que sigue, $\prod_{w|\infty} \mathbb{K}_w \simeq \mathbb{R}^{r_1} \times \mathbb{C}^{r_2}$ está dotado de estr. euclideana "no tan inocente".

<u>Teorema</u>: Sea $I \in \mathcal{I}(\mathcal{O}_{\mathbb{K}})$ un ideal fraccionario. Entonces, $\rho_\infty(I)$ es un <u>reticulado</u> en $\prod_{w|\infty} \mathbb{K}_w$ y se tiene que $\mathrm{covol}(\rho_\infty(I)) = \sqrt{|d_{\mathbb{K}}|} \cdot N(I)$. En particular, se tiene que:

$$\mathrm{covol}(\rho_\infty(\mathcal{O}_{\mathbb{K}})) = \sqrt{|d_{\mathbb{K}}|}$$

Observaciones: 1. Usando la estructura euclideana "inocente" (cf. P. Samuel, Ch IV) se tiene $\mathrm{covol}(\rho_\infty(I)) = 2^{-r_2}\sqrt{|d_{\mathbb{K}}|}\, N(I)$.

2. Si $I \in \mathcal{I}(\mathcal{O}_{\mathbb{K}})$ y $c \in \mathcal{O}_{\mathbb{K}}\setminus\{0\}$ es tal que $cI \subseteq \mathcal{O}_{\mathbb{K}}$ es un ideal, entonces $N(I) := N(cI)/|N_{\mathbb{K}/\mathbb{Q}}(c)|$ y está bien definido ($\boxed{\text{Ejercicio}}$).

3. Vimos en §10 que si $I \in \mathcal{I}(\mathcal{O}_{\mathbb{K}})$ entonces $I \simeq \mathbb{Z}^d$ como $\mathbb{Z}$-módulo, con $d = [\mathbb{K}:\mathbb{Q}]$. Además, si $(e_1, \dots, e_d)$ base de I y si $\Sigma_{\mathbb{K}/\mathbb{Q}} = \{\sigma_1, \dots, \sigma_d\}$ entonces la Fórmula del Discriminante implica que $D_{\mathcal{O}_{\mathbb{K}}/\mathbb{Z}}(I) = \langle D_{\mathbb{K}/\mathbb{Q}}(I)\rangle_{\mathbb{Z}\text{-mód}} \subseteq \mathbb{K}$ con $D_{\mathbb{K}/\mathbb{Q}}(I) = \det\big((\sigma_i(e_j))_{i,j}\big)^2$.

Dem del Teorema: Recordemos que hay una biyección

$$\coprod_{w|\infty} \Sigma_{\mathbb{K}_w/\mathbb{R}} \xrightarrow{\sim} \Sigma_{\mathbb{K}/\mathbb{Q}}, \quad (\sigma : \mathbb{K}_w \hookrightarrow \mathbb{C}) \mapsto (\sigma \circ \rho_{\mathbb{K}_w/\mathbb{K}} : \mathbb{K} \hookrightarrow \overline{\mathbb{Q}})$$

Además, hay un diagrama conmutativo

"no tan 'inocente'"

$$\begin{tikzcd}
x \arrow[d, mapsto] & \mathbb{K} \arrow[r, hook, "\rho_\infty"] \arrow[d] \arrow[dr, bend left, "\varphi"] & \prod_{w|\infty} \mathbb{K}_w \arrow[d, "\psi"] & (x_w)_{w|\infty} \arrow[d, mapsto] \\
(\sigma(x))_{\sigma\in\Sigma_{\mathbb{K}/\mathbb{Q}}} & \overline{\mathbb{Q}}^{\Sigma_{\mathbb{K}/\mathbb{Q}}} \arrow[r, hook] & \prod_{w|\infty} \mathbb{C}^{\Sigma_{\mathbb{K}_w/\mathbb{R}}} \simeq \mathbb{C}^{\Sigma_{\mathbb{K}/\mathbb{Q}}} \simeq \mathbb{C}^d & (\sigma(x_w))_{w|\infty,\ \sigma\in\Sigma_{\mathbb{K}_w/\mathbb{R}}}
\end{tikzcd}$$

"inocente": $\|(z_\sigma)_{\sigma\in\Sigma_{\mathbb{K}/\mathbb{Q}}}\| = \sum_{\sigma\in\Sigma_{\mathbb{K}/\mathbb{Q}}} |z_\sigma|$

Sea $(e_1, \dots, e_d)$ una $\mathbb{Z}$-base de $\mathcal{O}_{\mathbb{K}}$ y sea $\Sigma_{\mathbb{K}/\mathbb{Q}} = \{\sigma_1, \dots, \sigma_d\}$, entonces tenemos $\sqrt{|d_{\mathbb{K}}|} = |\det(\sigma_i(e_j))_{1\le i,j\le d}| \neq 0$ y en particular $(\varphi(e_1), \dots, \varphi(e_d))$ es una base del $\mathbb{C}$-e.v. $\mathbb{C}^{\Sigma_{\mathbb{K}/\mathbb{Q}}}$ y en part $(\rho_\infty(e_1), \dots, \rho_\infty(e_d))$ es una base del $\mathbb{R}$-e.v. $\prod_{w|\infty}\mathbb{K}_w$. Así, $\rho_\infty(\mathcal{O}_{\mathbb{K}})$ es un reticulado en $\prod_{w|\infty}\mathbb{K}_w$.

Notar que si $\mathcal{B}$ es una base ortonormal de $\prod_{w|\infty}\mathbb{K}_w$ entonces $\psi(\mathcal{B})$ es una base ortonormal en el espacio hermitiano $\mathbb{C}^{\Sigma_{\mathbb{K}/\mathbb{Q}}}$ y luego:

$$\mathrm{covol}(\rho_\infty(\mathcal{O}_{\mathbb{K}})) \overset{\text{def}}{=} |\det_{\mathcal{B}}(\rho_\infty(e_1), \dots, \rho_\infty(e_d))| = |\det_{\psi(\mathcal{B})}(\varphi(e_1), \dots, \varphi(e_d))|$$
$$= |\det((\sigma_i(e_j))_{1\le i,j\le d})| = \sqrt{|d_{\mathbb{K}}|}.$$

Sea $\Lambda := \rho_\infty(\mathcal{O}_{\mathbb{K}})$ y sea $I \in \mathcal{I}(\mathcal{O}_{\mathbb{K}})$ con $c \in \mathcal{O}_{\mathbb{K}}\setminus\{0\}$ tal que $cI \subseteq \mathcal{O}_{\mathbb{K}}$ es un ideal. Sabemos (ver §3, pág 6) que $c^{-1} \in \mathbb{K}^*$ se escribe como $c^{-1} = a/m$ con $m \in \mathbb{N}^{\geq 1}$ y $a \in \mathcal{O}_{\mathbb{K}}\setminus\{0\}$. Luego, $\frac{m}{a} I \subseteq \mathcal{O}_{\mathbb{K}}$ implica que $mI \subseteq a\mathcal{O}_{\mathbb{K}} \subseteq \mathcal{O}_{\mathbb{K}}$ y luego $mI \subseteq \mathcal{O}_{\mathbb{K}}$ ideal para cierto $m \in \mathbb{N}^{\geq 1}$. Para concluir, calculamos:

$$\mathrm{covol}(\rho_\infty(mI)) = \mathrm{covol}(m\,\rho_\infty(I)) = m^d\,\mathrm{covol}(\rho_\infty(I)) \quad \text{y además}$$
$$\mathrm{covol}(\rho_\infty(mI)) = [\rho_\infty(\mathcal{O}_{\mathbb{K}}) : \rho_\infty(mI)]\,\mathrm{covol}(\Lambda) = [\mathcal{O}_{\mathbb{K}} : mI]\,\mathrm{covol}(\Lambda) \overset{\text{def}}{=} N(mI)\,\mathrm{covol}(\Lambda)$$
$$= N(m)\,N(I)\,\mathrm{covol}(\Lambda) \overset{\text{def}}{=} m^d\,N(I)\,\mathrm{covol}(\Lambda)$$

$$\Rightarrow \mathrm{covol}(\rho_\infty(I)) = N(I)\sqrt{|d_{\mathbb{K}}|} \quad \blacksquare$$

Obs: Al tensorizar por $\mathbb{C}$ se obtiene el siguiente isomorfismo canónico de $\mathbb{C}$-álgebras

$$\prod_{w|\infty} \mathbb{K}_w \otimes_{\mathbb{R}} \mathbb{C} \xrightarrow{\sim} \mathbb{C}^{\Sigma_{\mathbb{K}/\mathbb{Q}}}$$

$\boxed{\text{Ejercicio}}$ Sea $\mathbb{K} = \mathbb{Q}(\sqrt{d})$ extensión cuadrática, con $d \in \mathbb{Z}\setminus\{0\}$ libre de cuadrados. Usar el Teorema anterior, junto con la descripción explícita de $\mathcal{O}_{\mathbb{K}}$, para calcular el discriminante $d_{\mathbb{K}}$. [Indicación: Hay que tomar en cuenta si $d>0$ o $d<0$].

§27. Finitud del grupo de clases de ideales

El objetivo de esta sección es probar el siguiente resultado fundamental:

Teorema (Dirichlet): Sea $\mathbb{K}$ un cuerpo de números. Entonces, el grupo de clases de ideales
$$Cl(\mathcal{O}_\mathbb{K}) \overset{\text{def}}{=} \mathcal{I}(\mathcal{O}_\mathbb{K})/Pr(\mathcal{O}_\mathbb{K}) \text{ es finito.}$$
Su cardinal $h_\mathbb{K} := |Cl(\mathcal{O}_\mathbb{K})|$ es el número de clases de $\mathbb{K}$.

$\boxed{\text{Ejercicio}}$* Probar que $h_\mathbb{K} = 1 \iff \mathcal{O}_\mathbb{K}$ es un DIP $\iff \mathcal{O}_\mathbb{K}$ es un DFU.

Lema: Sea $I \in \mathcal{I}(\mathcal{O}_\mathbb{K})$. Entonces, $\exists\, x \in I\setminus\{0\}$ tal que $|N_{\mathbb{K}/\mathbb{Q}}(x)| \le \left(\frac{4}{\pi}\right)^{r_2} \frac{d!}{d^d} \sqrt{|d_\mathbb{K}|}\, N(I)$.

Dem: Para $t \in \mathbb{R}^{>0}$ consideramos $B_t := \{(x_w) \in \prod_{w|\infty} \mathbb{K}_w \,,\ \sum_{w|\infty} N_w |x_w| \le t\}$, el cual es un conj. compacto, convexo, y $-B_t = B_t$. Dado que si $N_w = [\mathbb{K}_w : \mathbb{R}] = 2$ entonces $dx_w = 2\,dx\,dy = 2r\,dr\,d\theta$, se calcula (cf. P. Samuel, Ch IV, Appendix):
$$\mathrm{vol}(B_t) = (2\cdot 2\pi)^{r_2} 2^{r_1} \int_{r_w\ge 0,\ \sum N_w r_w \le t} \prod_{w|\infty} r_w^{N_w - 1} \prod_{w|\infty} dr_w = (4\pi)^{r_2} 2^{r_1} \left(\tfrac{1}{4}\right)^{r_2} \int_{x_i \ge 0,\ \sum x_i \le t} dx_1 \cdots dx_d$$
$$= \pi^{r_2} 2^{r_1} \frac{t^d}{d!}$$
Así, para aplicar el Teorema de Minkowski se requiere $\mathrm{vol}(B_t) \ge 2^d\, \mathrm{covol}(\rho_\infty(I))$, i.e., que $\pi^{r_2} 2^{r_1} \frac{t^d}{d!} \ge 2^d \sqrt{|d_\mathbb{K}|}\, N(I)$, i.e., $t^d \ge 2^{d-r_1} \pi^{-r_2} d! \sqrt{|d_\mathbb{K}|}\, N(I)$ con $2^{d-r_1} \overset{\text{def}}{=} 2^{2r_2}$.

Para dicho t, se tiene $x \in I\setminus\{0\}$ tal que $\rho_\infty(x) \in B_t$. Dado que
$$|N_{\mathbb{K}/\mathbb{Q}}(x)| = \prod_{w|\infty} |N_{\mathbb{K}_w/\mathbb{R}}(\rho_{\mathbb{K}_w/\mathbb{K}}(x))| = \prod_{w|\infty} |\rho_{\mathbb{K}_w/\mathbb{K}}(x)|^{N_w},$$

$f\left(\frac{a+b}{2}\right) \ge \frac{f(a)+f(b)}{2}$

y dado que la función real $t \mapsto \log(t)$ es cóncava, tenemos que:
$$\frac{1}{d}\sum_{w|\infty} N_w \log|\rho_{\mathbb{K}_w/\mathbb{K}}(x)| \le \log\Big(\frac{1}{d}\sum_{w|\infty} N_w |\rho_{\mathbb{K}_w/\mathbb{K}}(x)|\Big) \le \log\left(\frac{t}{d}\right) \text{ pues } \rho_{\mathbb{K}_w/\mathbb{K}}(x) \in B_t$$
$\Rightarrow \prod_{w|\infty} |\rho_{\mathbb{K}_w/\mathbb{K}}(x)|^{N_w} \le \frac{t^d}{d^d}$. Para t minimal: $|N_{\mathbb{K}/\mathbb{Q}}(x)| \le \left(\frac{4}{\pi}\right)^{r_2} \frac{d!}{d^d} \sqrt{|d_\mathbb{K}|}\, N(I)$ ∎

Prop: Toda clase de ideales en $Cl(\mathcal{O}_\mathbb{K})$ posee un representante dado por un ideal $J \subseteq \mathcal{O}_\mathbb{K}$ tal que $N(J) \le \left(\frac{4}{\pi}\right)^{r_2} \frac{d!}{d^d} \sqrt{|d_\mathbb{K}|}$.

Dem: Sea $I \in \mathcal{I}(\mathcal{O}_\mathbb{K})$ y sea $x \in I^{-1}$ tal que $|N_{\mathbb{K}/\mathbb{Q}}(x)| \le \left(\frac{4}{\pi}\right)^{r_2} \frac{d!}{d^d} \sqrt{|d_\mathbb{K}|}\, N(I^{-1})$. El ideal $J := xI \subseteq I^{-1}I = \mathcal{O}_\mathbb{K}$ está en la misma clase de I en $Cl(\mathcal{O}_\mathbb{K})$ y se tiene $N(J) = |N_{\mathbb{K}/\mathbb{Q}}(x)|\, N(I^{-1}) \le \left(\frac{4}{\pi}\right)^{r_2} \frac{d!}{d^d} \sqrt{|d_\mathbb{K}|}\, N(\mathcal{O}_\mathbb{K})$, donde $N(\mathcal{O}_\mathbb{K}) \overset{\text{def}}{=} 1$ ∎

$\boxed{\text{Ejercicio}}$ Sea $\mathbb{K} = \mathbb{Q}(\sqrt{5})$. Usar la Prop. para probar que $h_\mathbb{K} = 1$ (Obs: $d_\mathbb{K} = 5$).

Dem del Teo. de Dirichlet: Por la Prop, basta probar que para todo $m \in \mathbb{N}^{\ge 1}$ el conjunto $\{I \subseteq \mathcal{O}_\mathbb{K}$ ideal tq $N(I) = m\}$ es finito. Para $I \subseteq \mathcal{O}_\mathbb{K}$ con $N(I) \overset{\text{def}}{=} \#(\mathcal{O}_\mathbb{K}/I) = m$ se tiene que $[m] = 0$ en $\mathcal{O}_\mathbb{K}/I$, i.e., $m \in I$. Así, basta probar que el conjunto de ideales $I \subseteq \mathcal{O}_\mathbb{K}$ tq $m \in I$ es finito. Por Teoría de Anillos, este último conj. está en biyección con el conjunto de ideales del cociente $\mathcal{O}_\mathbb{K}/m\mathcal{O}_\mathbb{K}$ y este es finito (escribir $m = \prod_p p^{v_p(m)}$) ∎

Corolario: Si $d = [\mathbb{K}:\mathbb{Q}] \ge 2$ entonces $|d_\mathbb{K}| \ge \frac{\pi}{3}\left(\frac{3\pi}{4}\right)^{d-1}$. En part, $\exists\, C \in \mathbb{R}$ tal que $[\mathbb{K}:\mathbb{Q}]/\log|d_\mathbb{K}| \le C$ para todo cuerpo de números $\mathbb{K}$.

Dem: Dado que $1 \le N(J) \le \left(\frac{4}{\pi}\right)^{r_2} \frac{d!}{d^d} \sqrt{|d_\mathbb{K}|}$ para cierto $J \subseteq \mathcal{O}_\mathbb{K}$, $|d_\mathbb{K}| \ge \left(\frac{\pi}{4}\right)^{2r_2} \frac{d^{2d}}{(d!)^2}$ donde $\frac{\pi}{4} < 1$ y $2r_2 \le d$. Así, $|d_\mathbb{K}| \ge a_d := \left(\frac{\pi}{4}\right)^d \frac{d^{2d}}{(d!)^2}$ y basta probar que $a_d \ge \frac{\pi}{3}\left(\frac{3\pi}{4}\right)^{d-1}$:

Para $d = 2$: $a_2 = \left(\frac{\pi}{4}\right)^2 \frac{2^4}{2^2} = \frac{\pi^2}{4} = \frac{\pi}{3}\left(\frac{3\pi}{4}\right)$ ✓ Para $d \geq 2$ basta usar inducción, puesto que $\frac{a_{d+1}}{a_d} \overset{\text{dy}}{=} \frac{\pi}{4}\left(1 + \frac{1}{d}\right)^{2d} \geq \frac{3\pi}{4}$ ■

Teorema de Hermite - Minkowski (1889): Todo cuerpo de números $\mathbb{K}$ con $[\mathbb{K}:\mathbb{Q}] \geq 2$ cumple que $|d_{\mathbb{K}}| \neq 1$.

Dem: Por el Corolario anterior, $|d_{\mathbb{K}}| \geq \frac{\pi}{3}\left(\frac{3\pi}{4}\right)^{d-1} > 1$. ■

⚠ En part, todo cuerpo de números $\mathbb{K}$ con $[\mathbb{K}:\mathbb{Q}] \geq 2$ es tal que el conjunto de ideales primos que ramifican en $\mathbb{K}/\mathbb{Q}$ es no-vacío! Sin embargo, existen extensiones $\mathbb{L}/\mathbb{K}$ con $[\mathbb{L}:\mathbb{K}] \geq 2$ que son no-ramificadas.

Teorema de Hermite ("1857"): Módulo isomorfismos, hay una cantidad finita de cuerpos de números $\mathbb{K}$ con discriminante $d_{\mathbb{K}}$ dado.

Dem: El Corolario anterior implica que $d = [\mathbb{K}:\mathbb{Q}]$ está acotado en términos de $|d_{\mathbb{K}}|$. Como $d = r_1 + 2r_2$, basta probar que hay finitos cuerpos de números en $\overline{\mathbb{Q}}$ con discriminante $d_{\mathbb{K}}$, grado d, y r_1 y r_2 dados. Sea $\mathbb{K}$ un tal cuerpo de números y sea $w_0 | \infty$ lugar de $\mathbb{K}$ con N_{w_0} minimal:

$\boxed{\text{Caso 1}}$ Si $N_{w_0} = 1$, definimos $\mathcal{B} := \{(z_w)_w \in \prod_{w|\infty} \mathbb{K}_w,\ |z_w| \leq \frac{1}{2}$ si $w \neq w_0$ y $|z_{w_0}| \leq 2^{d-1}\left(\frac{\pi}{2}\right)^{-r_2}\sqrt{|d_{\mathbb{K}}|}\}$

$\Rightarrow vol(\mathcal{B}) = \left(2 \cdot \frac{\pi}{4}\right)^{r_2} \cdot 1^{r_1 - 1} \cdot 2^d \left(\frac{\pi}{2}\right)^{-r_2}\sqrt{|d_{\mathbb{K}}|} = 2^d\sqrt{|d_{\mathbb{K}}|}$.

$\boxed{\text{Caso 2}}$ Si $N_{w_0} = 2$ (ie, $r_1 = 0$) definimos

"rectangulo en $\mathbb{K}_{w_0} \simeq \mathbb{C}$"

$\mathcal{B} = \{(z_w) \in \prod_{w|\infty} \mathbb{K}_w,\ |z_w| \leq \frac{1}{2}$ si $w \neq w_0$, y $|z_{w_0} + \overline{z}_{w_0}| \leq \frac{1}{2}$, $|z_{w_0} - \overline{z}_{w_0}| \leq 2^d \frac{\pi}{8}\left(\frac{\pi}{2}\right)^{-r_2}\sqrt{|d_{\mathbb{K}}|}\}$

$\Rightarrow vol(\mathcal{B}) = \left(2 \cdot \frac{\pi}{4}\right)^{r_2 - 1} \cdot 2 \cdot 1 \cdot 2 \cdot 2^d \frac{\pi}{8}\left(\frac{\pi}{2}\right)^{-r_2}\sqrt{|d_{\mathbb{K}}|} = 2^d\sqrt{|d_{\mathbb{K}}|}$.

En cada caso, $vol(\mathcal{B}) = 2^d\sqrt{|d_{\mathbb{K}}|} = 2^d\, covol(\rho_\infty(\mathcal{O}_{\mathbb{K}}))$ y luego (Minkowski) existe $x \in \mathcal{O}_{\mathbb{K}} \setminus \{0\}$ tal que $\rho_\infty(x) \in \mathcal{B}$. Veamos que $\mathbb{K} = \mathbb{Q}(x)$:

Recordemos que $\tau: \Sigma_{\mathbb{K}/\mathbb{Q}} \twoheadrightarrow \{w \in Pl(\mathbb{K}), w|\infty\}$, $\sigma \mapsto$ Top. def por $|\sigma(\cdot)|$ es sobreyectiva. Sea $\sigma_0: \mathbb{K} \hookrightarrow \overline{\mathbb{Q}}$ en $\Sigma_{\mathbb{K}/\mathbb{Q}}$ tq $|\sigma_0(\cdot)|$ induce w_0. Notar que como $x \in \mathcal{O}_{\mathbb{K}} \setminus \{0\}$,

$1 \leq |\overbrace{N_{\mathbb{K}/\mathbb{Q}}(x)}^{\in \mathbb{Z}}| = \prod_{w|\infty} |\rho_{\mathbb{K}_w/\mathbb{K}}(x)|^{N_w}$ $(\star)$. Como $\rho_\infty(x) \in \mathcal{B}$, si $\sigma \neq \sigma_0$ o $\overline{\sigma}_0$ entonces $|\sigma(x)| \leq 1/2$ y luego $(\star)$ implica que necesariamente $|\sigma_0(x)| > 1$. Así, en el Caso 2, la condición $|z_{w_0} + \overline{z}_{w_0}| \leq 1/2$ implica que $\sigma_0(x) \notin \mathbb{R}$, ie, $\sigma_0(x) \neq \overline{\sigma}_0(x)$. Luego, en ambos casos, toda $\sigma \in \Sigma_{\mathbb{K}/\mathbb{Q}}$ con $\sigma \neq \sigma_0$ cumple $\sigma_0(x) \neq \sigma(x)$!

Consideremos $\psi: \Sigma_{\mathbb{K}/\mathbb{Q}} \overset{\text{res}}{\twoheadrightarrow} \Sigma_{\mathbb{Q}(x)/\mathbb{Q}} \overset{\text{incl}}{\hookrightarrow} \overline{\mathbb{Q}}$, $\sigma \mapsto \sigma|_{\mathbb{Q}(x)} \mapsto \sigma(x)$, donde todas sus fibras tienen el mismo cardinal $[\mathbb{K}:\mathbb{Q}(x)]_s = [\mathbb{K}:\mathbb{Q}(x)]$. Como $\#\psi^{-1}(\sigma_0(x)) = 1$, se tiene que ψ es inyectiva y luego $[\mathbb{K}:\mathbb{Q}] = [\mathbb{Q}(x):\mathbb{Q}]$, ie, $\mathbb{K} = \mathbb{Q}(x)$ ✓

Por definición de $\mathcal{B}$, los valores $\{|\sigma(x)|\}_{\sigma \in \Sigma_{\mathbb{K}/\mathbb{Q}}}$ están acotados unif. por $C = C(d_{\mathbb{K}}, r_1, r_2)$. Dado que los coeficientes de $\mu_x^{\mathbb{Q}} = \chi_x^{\mathbb{Q}} = \prod_{\sigma \in \Sigma_{\mathbb{K}/\mathbb{Q}}}(X - \sigma(x)) \in \mathbb{Z}[X]$ son polinomios simétricos en $(\sigma(x))_{\sigma \in \Sigma_{\mathbb{K}/\mathbb{Q}}}$, tenemos que ellos forman un conjunto acotado de enteros. Así, los posibles $\mu_x^{\mathbb{Q}} \in \mathbb{Z}[X]$ (y luego los posibles $\mathbb{K} = \mathbb{Q}(x)$) son finitos ■

Cultura general: Recién en los años 1960s se probó (Baker - Heegner - Stark) que si $\mathbb{K} = \mathbb{Q}(\sqrt{-d})$ con $d \geq 1$ libre de cuadrados, entonces $h_{\mathbb{K}} = 1 \Leftrightarrow d \in \{1, 2, 3, 7, 11, 19, 43, 67, 163\}$. Esto había sido conjeturado por Gauss en 1798.

§28. Teorema de las unidades de Dirichlet

En esta sección estudiaremos el grupo de unidades $\mathcal{O}_{\mathbb{K}}^*$. El resultado principal que concebido por Dirichlet mientras escuchaba un concierto en la Capilla Sixtina.

Prop: Sea $\mathbb{K}$ un cuerpo de números y $x \in \mathcal{O}_{\mathbb{K}}$. Entonces, $x \in \mathcal{O}_{\mathbb{K}}^* \Leftrightarrow |N_{\mathbb{K}/\mathbb{Q}}(x)| = 1$.

Dem: $(\Rightarrow)$ Si $\exists\, y \in \mathcal{O}_{\mathbb{K}}$ tal que $xy = 1$ entonces $N_{\mathbb{K}/\mathbb{Q}}(x)\, N_{\mathbb{K}/\mathbb{Q}}(y) = 1$ y luego $N_{\mathbb{K}/\mathbb{Q}}(x)$ pertenece a $\mathbb{Z}^* = \{\pm 1\}$ ✓ $(\Leftarrow)$ Si $\chi_x^{\mathbb{Q}}(T) = T^n + a_{n-1}T^{n-1} + \ldots + a_1 T + a_0$, entonces $|a_0| = |N_{\mathbb{K}/\mathbb{Q}}(x)| = 1$, ie, $a_0 \in \mathbb{Z}^*$. Así, $\chi_x^{\mathbb{Q}}(x) = 0 \Leftrightarrow x \cdot (-a_0^{-1})(x^{n-1} + a_{n-1}x^{n-2} + \ldots + a_1) = 1$ ie, $xy = 1$ con $y = (-a_0^{-1})(x^{n-1} + \ldots + a_1) \in \mathcal{O}_{\mathbb{K}}$ y así $x \in \mathcal{O}_{\mathbb{K}}^*$ ■

Teorema de las unidades de Dirichlet (1846): Sea $\mathbb{K}$ un cuerpo de números de grado $d = r_1 + 2r_2$, y sea $\mu_\infty(\mathbb{K}) := \{x \in \mathbb{K},\ \exists\, n \in \mathbb{N}^{\geq 1} \text{ tal que } x^n = 1\}$ el grupo de raíces de la unidad de $\mathbb{K}$. Entonces, $\mu_\infty(\mathbb{K})$ es finito y $\mathcal{O}_{\mathbb{K}}^* \cong \mu_\infty(\mathbb{K}) \times \mathbb{Z}^{r_1 + r_2 - 1}$.

La demostración del Teorema será dividida en varios pasos:

$\boxed{\text{Paso 1}}$ Construir $\underline{\log}: \mathcal{O}_{\mathbb{K}}^* \to \prod_{w|\infty} \mathbb{R} \simeq \mathbb{R}^{r_1 + r_2}$.

$\boxed{\text{Paso 2}}$ Verificar que para todo $K \subseteq \prod_{w|\infty} \mathbb{R}$ compacto, $\mathrm{Im}(\underline{\log}) \cap K$ es finito.

$\boxed{\text{Paso 3}}$ Probar que $\ker(\underline{\log}) = \mu_\infty(\mathbb{K})$ es finito y $\mathrm{Im}(\underline{\log})$ discreto.

$\boxed{\text{Paso 4}}$ Probar que $\mathrm{Im}(\underline{\log}) \subseteq H := \{(x_w) \in \prod_{w|\infty} \mathbb{R},\ \sum_{w|\infty} N_w x_w = 0\} \cong \mathbb{R}^r$ con $r := r_1 + r_2 - 1$.

$\boxed{\text{Paso 5}}^*$ Probar que para todo funcional $f \in H^* \setminus \{0\}$, $\exists\, x \in \mathcal{O}_{\mathbb{K}}^*$ tal que $f(\underline{\log}(x)) \neq 0$.

Dem: Para el $\boxed{\text{Paso 1}}$ consideramos $\underline{\log}: \mathcal{O}_{\mathbb{K}}^* \to \prod_{w|\infty} \mathbb{R}$, $x \mapsto (\log|\rho_{\mathbb{K}_w/\mathbb{K}}(x)|)_{w|\infty}$, que es un morfismo de grupos ✓ Notar que para el $\boxed{\text{Paso 2}}$ basta probar que para todo $t \in \mathbb{R}^{>0}$ el conjunto $\{x \in \mathcal{O}_{\mathbb{K}}^*,\ \underline{\log}(x) \in \prod_{w|\infty} [-t, t]\}$ es finito. Lo anterior equivale a que $\forall\, \sigma \in \Sigma_{\mathbb{K}/\mathbb{Q}}$, $e^{-t} \leq |\sigma(x)| \leq e^t$. Así, los coef. de $\chi_x^{\mathbb{Q}} \in \mathbb{Z}[T]$ están acotados en términos de t. Dado que hay finitos $\chi_x^{\mathbb{Q}}$, existen finitos $x \in \mathbb{K}$ ✓

Por el Paso 2 (con $t \to 0$) tenemos que $\ker(\underline{\log})$ es finito de cardinal N. Así, para probar el $\boxed{\text{Paso 3}}$ basta notar que todo $x \in \ker(\underline{\log})$ cumple $x^N = 1$ (Lagrange) y luego $x \in \mu_\infty(\mathbb{K})$. Recíprocamente, $\mu_\infty(\mathbb{K}) \overset{\text{dy}}{\subseteq} \mathcal{O}_{\mathbb{K}}^*$ y $\mu_\infty(\mathbb{K}) \overset{\text{dy}}{\subseteq} \ker(\underline{\log})$. Así, tenemos que $\ker(\underline{\log}) = \mu_\infty(\mathbb{K})$ es finito y $\mathrm{Im}(\underline{\log})$ es discreto por el Paso 2 ✓

El $\boxed{\text{Paso 4}}$ se deduce al notar que si $x \in \mathcal{O}_{\mathbb{K}}^*$ entonces, por la Prop, $1 = |N_{\mathbb{K}/\mathbb{Q}}(x)| = \prod_{w|\infty} |\rho_{\mathbb{K}_w/\mathbb{K}}(x)|^{N_w}$ $\Leftrightarrow \sum_{w|\infty} N_w \log(|\rho_{\mathbb{K}_w/\mathbb{K}}(x)|) = 0$. Así, $\underline{\log}(x) \in H$ ✓

El $\boxed{\text{Paso 5}}$ ocupa la mayor parte de la demostración: sea $f \in H^* \setminus \{0\}$ y probemos que $\exists\, x \in \mathcal{O}_{\mathbb{K}}^*$ tal que $f(\underline{\log}(x)) \neq 0$. Comencemos por fijar un orden de $\{w \in \mathrm{Pl}(\mathbb{K}),\ w|\infty\} = \{w_1, \ldots, w_{r+1}\}$ de tal suerte que $i \mapsto N_{w_i}$ sea creciente, ie, $\mathbb{R}^{r+1} = \prod_{w|\infty} \mathbb{R} = \mathbb{R}^{r_1} \times \mathbb{R}^{r_2}$.

Consideremos el isomorfismo $\pi: H \xrightarrow{\sim} \mathbb{R}^r$, $(\lambda_1, \ldots, \lambda_{r+1}) \longmapsto (\lambda_1, \ldots, \lambda_r)$ y escribamos $f \in H^* \setminus \{0\}$ como $f(x_1, \ldots, x_{r+1}) = \sum_{i=1}^{r} c_i x_i$ para ciertos $(c_1, \ldots, c_r) \in \mathbb{R}^r$. Fijemos $\alpha \in \mathbb{R}^{>0}$ de tal suerte que $\alpha \geq 2^{d - r_1} \left(\frac{1}{2\pi}\right)^{r_2} \sqrt{|d_{\mathbb{K}}|}$ y para cada $\underline{\lambda} = (\lambda_1, \ldots, \lambda_r) \in \mathbb{R}^r_{>0}$ elegimos $\lambda_{r+1} \in \mathbb{R}^{>0}$ tal que $\prod_{i=1}^{r+1} \lambda_i^{N_{w_i}} = \alpha$. Con la notación anterior, definimos

$$B_\lambda := \{(x_w) \in \prod_{w|\infty} \mathbb{K}_w,\ |x_{w_i}| \leq \lambda_i \text{ para } i \in \{1, \ldots, r+1\}\}$$

$\Rightarrow \mathrm{vol}(B_\lambda) = 2^{r_1} \cdot (2\pi)^{r_2} \prod_{i=1}^{r+1} \lambda_i^{N_{w_i}} = 2^{r_1} \cdot (2\pi)^{r_2}\, \alpha \geq 2^d \sqrt{|d_{\mathbb{K}}|} = 2^d\, \mathrm{covol}(\rho_\infty(\mathcal{O}_{\mathbb{K}}))$.

Como B_λ es compacto, convexo, y $-B_\lambda = B_\lambda$, $\exists\, x_{\underline{\lambda}} \in \mathcal{O}_{\mathbb{K}} \setminus \{0\}$ tq $\rho_\infty(x_{\underline{\lambda}}) \in B_\lambda$ (Minkowski).

Cada w_i está dy. por $|\sigma(\cdot)|$ para cierto $\sigma : \mathbb{K} \hookrightarrow \overline{\mathbb{Q}}$ en $\Sigma_{\mathbb{K}/\mathbb{Q}}$, por lo que escribiremos $\lambda_\sigma := \lambda_i$ y así $|\sigma(x_{\underline{\lambda}})| \le \lambda_\sigma$ $\forall \sigma \in \Sigma_{\mathbb{K}/\mathbb{Q}}$. Como $1 \le |N_{\mathbb{K}/\mathbb{Q}}(x_{\underline{\lambda}})| = \prod_{\sigma \in \Sigma_{\mathbb{K}/\mathbb{Q}}} |\sigma(x_{\underline{\lambda}})| \le \alpha$, tenemos $|\sigma(x_{\underline{\lambda}})| \ge \prod_{\sigma' \ne \sigma} |\sigma'(x_{\underline{\lambda}})|^{-1} \ge \prod_{\sigma' \ne \sigma} \lambda_{\sigma'}^{-1} \overset{dy}{=} \alpha^{-1} \lambda_\sigma$, i.e., $\lambda_\sigma \ge |\sigma(x_{\underline{\lambda}})| \ge \alpha^{-1}\lambda_\sigma$
$\Rightarrow \log(\alpha) \ge |\log(\lambda_\sigma) - \log|\sigma(x_{\underline{\lambda}})|| \ge 0$ y así $|f(\log(x_{\underline{\lambda}})) - \sum_{i=1}^r c_i \lambda_i| \le \beta := \sum_{i=1}^r |c_i| \log(\alpha) \in \mathbb{R}^{>0}$.

$\log(\lambda_i)$

Para cada $h \in \mathbb{N}^{\ge 1}$ elegimos $\underline{\lambda}_h := (\lambda_1, \dots, \lambda_r)$ tq $\sum_{i=1}^r c_i \lambda_i = 3\beta h$, y sea $x_h := x_{\underline{\lambda}_h} \in \mathcal{O}_{\mathbb{K}}$.
$\Rightarrow |f(\log(x_h)) - 3\beta h| \le \beta$. En part, si $h_1 \ne h_2$ cumplen $f(\log(x_{h_1})) = f(\log(x_{h_2}))$ entonces $1 \le |h_1 - h_2|$ y luego $3\beta \le |3\beta h_1 - 3\beta h_2| \le \beta + \beta$ ↯, i.e., $h \mapsto f(\log(x_h))$ inyectiva, donde $\log$ es la extensión evidente a $\mathcal{O}_{\mathbb{K}}$. Estamos listos para concluir el Paso 5:

Para todo $h \in \mathbb{N}^{\ge 1}$ se tiene $N(\langle x_h \rangle) = |N_{\mathbb{K}/\mathbb{Q}}(x)| \le \alpha$ y (por factorización de ideales de $\mathcal{O}_{\mathbb{K}}$) el nº de ideales $I \subseteq \mathcal{O}_{\mathbb{K}}$ con $N(I) \le \alpha$ es finito $\Rightarrow \{\langle x_h \rangle\}_{h \in \mathbb{N}^{\ge 1}}$ es finito.
$\Rightarrow \exists\, h_1 \ne h_2$ tq $\langle x_{h_1} \rangle = \langle x_{h_2} \rangle$, i.e., $x_{h_2} = u x_{h_1}$ para cierto $u \in \mathcal{O}_{\mathbb{K}}^*$ y luego
$0 \ne f(\log(x_{h_2})) - f(\log(x_{h_1})) = f(\log(u))$ ✓

Así, $\mathrm{Im}(\log) \subseteq H$ es un subgrupo discreto que genera $H \simeq \mathbb{R}^r$, i.e., $\mathrm{Im}(\log) \simeq \mathbb{Z}^r$ reticulado.
$\Rightarrow \mathcal{O}_{\mathbb{K}}^* \simeq \mu_\infty(\mathbb{K}) \times \mathbb{Z}^r$ con $r = r_1 + r_2 - 1$ ■

Consecuencia: El grupo $\mathbb{K}^*$ puede entenderse mediante las sucesiones exactas

$$1 \longrightarrow \mathcal{O}_{\mathbb{K}}^* \longrightarrow \mathbb{K}^* \xrightarrow{(v_{\mathfrak{p}})_{\mathfrak{p} \in \mathrm{Spec}(\mathcal{O}_{\mathbb{K}})^*}} \mathcal{I}(\mathcal{O}_{\mathbb{K}}) \simeq \bigoplus_{\mathfrak{p} \in \mathrm{Spec}(\mathcal{O}_{\mathbb{K}})^*} \mathbb{Z} \twoheadrightarrow \underbrace{\mathcal{C}\ell(\mathcal{O}_{\mathbb{K}})}_{\text{finito}} \longrightarrow 1$$

y $1 \to \overbrace{\mu_\infty(\mathbb{K})}^{\text{finito}} \to \mathcal{O}_{\mathbb{K}}^* \xrightarrow{\log} \mathbb{Z}^{r_1 + r_2 - 1} \to 0$.

Notación: Es muy común denotar por $w_{\mathbb{K}} := |\mu_\infty(\mathbb{K})|$ al nº de raíces de la unidad en $\mathbb{K}$.

§29. El regulador

Motivados por la sección anterior, para cada cuerpo de números $\mathbb{K}$ fijamos un orden de $\{w \in \mathrm{Pl}(\mathbb{K}),\ w | \infty\} = \{w_1, \dots, w_m\}$, con $m \overset{dy}{=} r_1 + r_2$, tq $i \mapsto N_{w_i}$ sea creciente.

Definimos la función regulador por $\lambda : \mathcal{O}_{\mathbb{K}}^* \longrightarrow \mathbb{R}^m$, $x \longmapsto (N_{w_i} \log|\sigma_i(x)|)_{i = 1, \dots, m}$, donde w_i está dy por $|\sigma_i(\cdot)|$. Así, los cálculos de la sección anterior implican que:

$\lambda(\mathcal{O}_{\mathbb{K}}^*) \subseteq H(m)$ es un reticulado en el hiperplano $H(m) := \{v \in \mathbb{R}^m,\ v_1 + \dots + v_m = 0\}$.

Terminología: Un sistema de unidades fundamentales de $\mathcal{O}_{\mathbb{K}}$ son $u_1, \dots, u_{m-1} \in \mathcal{O}_{\mathbb{K}}^*$ tales que $(\lambda(u_1), \dots, \lambda(u_{m-1}))$ es una $\mathbb{Z}$-base del reticulado $\lambda(\mathcal{O}_{\mathbb{K}}^*) \simeq \mathbb{Z}^{m-1}$.

Def: Sea "vol" la medida de Lebesgue en $H(m) \simeq \mathbb{R}^{m-1}$ inducida por la restricción del producto punto usual de $\mathbb{R}^m$ a $H(m)$. Se define el regulador de $\mathbb{K}$ como

$$\mathrm{Reg}_{\mathbb{K}} = R_{\mathbb{K}} := \frac{\mathrm{vol}(H(m)/\lambda(\mathcal{O}_{\mathbb{K}}^*))}{\sqrt{r_1 + r_2}} \overset{dy}{=} \frac{\mathrm{covol}(\lambda(\mathcal{O}_{\mathbb{K}}^*))}{\sqrt{r_1 + r_2}}$$

donde $\mathrm{covol}(H(m)/\lambda(\mathcal{O}_{\mathbb{K}}^*)) := 1$ si $\dim_{\mathbb{R}}(H(m)) = 0$ (i.e., si $r_1 + r_2 = 1$) y luego $R_{\mathbb{K}} = 1$.

Obs: La condición $r_1 + r_2 = 1$ ocurre si $(r_1, r_2) = (1, 0)$, i.e., $d = 1$, i.e., $\mathbb{K} \cong \mathbb{Q}$; o bien si $(r_1, r_2) = (0, 1)$, i.e., $d = 2$ y $\mathbb{K} \cong \mathbb{Q}(\sqrt{-d})$ extensión cuadrática imaginaria. En este último caso, $\mathcal{O}_{\mathbb{K}}^*$ puede ser descrito explícitamente (ver P. Samuel §4.5).

Lema: Sup. que $m \ge 2$ y sea $\pi_i : H(m) \xrightarrow{\sim} \mathbb{R}^{m-1}$, $(v_1, \dots, v_m) \longmapsto (v_1, \dots, v_{i-1}, v_{i+1}, \dots, v_m)$ para $i \in \{1, \dots, m\}$. Entonces, $|\det(\pi_i)| = 1/\sqrt{m}$, i.e., π_i amplifica los volúmenes por $1/\sqrt{m}$.

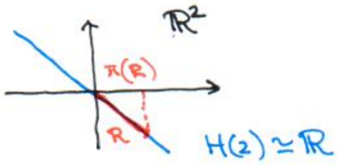
<u>Dem</u>: Basta probarlo para $\pi_m : H(m) \xrightarrow{\sim} \mathbb{R}^{m-1}$, $(v_1,\dots,v_m) \longmapsto (v_1,\dots,v_{m-1})$ cuya inversa está dada por $\nu : \mathbb{R}^{m-1} \xrightarrow{\sim} H(m)$, $(x_1,\dots,x_{m-1}) \longmapsto (x_1,\dots,x_{m-1}, -(x_1+\dots+x_{m-1}))$.
Sea $(e_1,\dots,e_{m-1})$ una base ortonormal de $\mathbb{R}^{m-1}$ y sea $n \in \mathbb{R}^m$ tal que $(\nu(e_1),\dots,\nu(e_{m-1}), n)$ es una base ortonormal de $\mathbb{R}^m$. Entonces, por def de $H(m)$, podemos considerar el vector $n = \frac{1}{\sqrt{m}}(1,\dots,1)$ que es normal al hiperplano $H(m)$ ✓
Así, si $R = \sum_{i=1}^{m-1}[0,1]e_i$ es el $(m-1)$-cubo de volumen 1, entonces el volumen de $\nu(R)$ es $|\det(M)|$ donde

$$M = \left[\begin{array}{ccccc} 1 & 0 & & 0 & 1/\sqrt{m} \\ 0 & 1 & & 0 & 1/\sqrt{m} \\ \vdots & \vdots & \cdots & \vdots & \vdots \\ 0 & 0 & & 1 & \vdots \\ -1 & -1 & \cdots & -1 & 1/\sqrt{m} \end{array}\right].$$

$\boxed{\text{Ejercicio}}$

ie, $\mathrm{vol}(\nu(R)) \overset{!}{=} 1/\sqrt{m} \cdot m = \sqrt{m} = |\det(\nu)|$ y así $|\det(\pi_m)| = 1/\sqrt{m}$ ■

<u>Ejemplo</u> $(m=2)$:



$|R| = \ell(R) = 1$
$\Rightarrow \ell(\pi(R)) = \cancel{1}/\sqrt{2}$

<u>Teorema</u>: Sea $\mathbb{K}$ un cuerpo de números y supongamos que $r = r_1 + r_2 - 1 \geq 1$ (ie, $r_1 + r_2 \geq 2$). Sea $u_1,\dots,u_r \in \mathcal{O}_{\mathbb{K}}^*$ un sistema de unidades fundamentales de $\mathcal{O}_{\mathbb{K}}$ y consideremos la matriz $\mathcal{U} \in M_{r \times (r_1+r_2)}(\mathbb{R})$ dada por $\mathcal{U} = (N_{v_j} \log|\sigma_j(u_i)|)_{\substack{i=1,\dots,r \\ j=1,\dots,r_1+r_2}}$. Entonces:
① Los elementos de cada fila de $\mathcal{U}$ suman 0.
② Si $\mathcal{U}_i$ es la matriz $r \times r$ obtenida al borrar la i-ésima columna de $\mathcal{U}$, entonces $|\det(\mathcal{U}_i)| = \mathrm{Reg}_{\mathbb{K}}$.

<u>Dem</u>: Para ①, notamos que los elementos de la i-ésima fila suman $\log|N_{\mathbb{K}/\mathbb{Q}}(u_i)| = 0$ ✓
Para ②, consideramos las proyecciones $\pi_i : \mathbb{R}^{r_1+r_2} \longrightarrow \mathbb{R}^r$ que en particular inducen <u>isom</u>. $H \xrightarrow{\sim} \mathbb{R}^r$ donde $H := \{v \in \mathbb{R}^{r_1+r_2},\ \sum_{j=1}^{r_1+r_2} v_j = 0\}$.
$\Rightarrow \pi_i(\lambda(\mathcal{O}_{\mathbb{K}}^*))$ es un reticulado en $\mathbb{R}^r$ con base $\pi_i(\lambda(u_1)),\dots,\pi_i(\lambda(u_r))$.
Por otra parte, por def, $\mathcal{U}_i^t$ es la matriz con $\pi_i(\lambda(u_1)),\dots,\pi_i(\lambda(u_r))$ como columnas!
$\Rightarrow |\det(\mathcal{U}_i)| \overset{\text{def}}{=} \mathrm{vol}(\mathbb{R}^r/\pi_i(\lambda(\mathcal{O}_{\mathbb{K}}^*))) \underset{\text{Lema}}{=} \frac{1}{\sqrt{r_1+r_2}}\ \mathrm{vol}(H/\lambda(\mathcal{O}_{\mathbb{K}}^*)) \overset{\text{def}}{=} \mathrm{Reg}_{\mathbb{K}}$ ■

<u>Ejemplo</u>: Si $d \in \mathbb{N}^{\geq 2}$ es un entero libre de cuadrados y $\mathbb{K} = \mathbb{Q}(\sqrt{d})$, entonces las unidades de $\mathcal{O}_{\mathbb{K}}$ pueden ser estudiadas mediante la <u>Ecuación de Pell</u> $x^2 - dy^2 = 1$, con $x, y \in \mathbb{Z}$. (Ver P. Samuel §4.6 para más detalles). Por ejemplo, si $\mathbb{K} = \mathbb{Q}(\sqrt{2})$ entonces $2 = r_1 + 2r_2$ y luego $r_1 = 2$ y $r_2 = 0$, por lo que $r = r_1 + r_2 - 1 = 1$ y luego $\mathcal{O}_{\mathbb{K}}^*/\mu_\infty(\mathbb{K}) \simeq \mathbb{Z}$.
Usando la ecuación de Pell, se puede verificar que $u = 1+\sqrt{2}$ es una unidad fundamental de $\mathcal{O}_{\mathbb{K}} = \mathbb{Z}[\sqrt{2}]$. Luego, $\mathcal{U} = [\log|1+\sqrt{2}|, \log|\underbrace{1-\sqrt{2}}_{\sigma(u)}|] \Rightarrow R_{\mathbb{K}} = |\log|1+\sqrt{2}|| \approx 0{,}88137$.

{Cultura general} Una importante generalización de la función zeta de Riemann es la <u>función zeta de Dedekind</u>, definida mediante

$$\zeta_{\mathbb{K}}(s) := \sum_{0 \neq I \subseteq \mathcal{O}_{\mathbb{K}}} \frac{1}{N(I)^s} = \prod_{\mathfrak{p} \in \mathrm{Spec}(\mathcal{O}_{\mathbb{K}})^*} \left(\frac{1}{1-N(\mathfrak{p})^{-s}}\right) \text{ para } \mathrm{Re}(s) > 1.$$

En 1917, E. Hecke prueba que $\zeta_{\mathbb{K}}$ se extiende a una función meromorfa en $\mathbb{C}$ con un único polo simple en $s = 1$. Más aún, prueba la fórmula analítica para el número de clases:

$$\lim_{s \to 1} (s-1)\zeta_{\mathbb{K}}(s) = \mathrm{Res}(\zeta_{\mathbb{K}}, 1) = \frac{2^{r_1}(2\pi)^{r_2} h_{\mathbb{K}} \mathrm{Reg}_{\mathbb{K}}}{w_{\mathbb{K}} \sqrt{|d_{\mathbb{K}}|}}$$

§30. El principio local-global

En Teoría de Números, decimos que un cuerpo global es una extensión finita de $\mathbb{Q}$ (ie, un cuerpo de números) o una extensión finita de $\mathbb{F}_p(T)$, con $p \geq 2$ un número primo. Además, decimos que un cuerpo local es la completación de un cuerpo global (eg. $\mathbb{R}$, $\mathbb{C}$, $\mathbb{Q}_p$).

En palabras simples, el "principio local-global" se pregunta cuándo podemos "pegar" soluciones locales de ecuaciones en una solución global.

Construcción (Grothendieck): Sea A un anillo conmutativo y sea B una A-álgebra. Decimos que $\mathrm{Spec}(B) \overset{dy}{=} \{\mathfrak{p} \subseteq B \text{ ideal primo}\}$ dotado de la topología de Zariski (ie, sus cerrados son $V(I) := \{\mathfrak{p} \in \mathrm{Spec}(B), \mathfrak{p} \supseteq I\}$ para $I \subseteq B$ ideal) es un esquema afín.

Sea $X := \mathrm{Spec}(C)$ con C una A-álgebra. Se define el conjunto de B-puntos de X como $X(B) := \mathrm{Hom}_{\mathrm{Spec}(A)}(\mathrm{Spec}\, B, X)$, donde $f \in X(B)$ si el diagrama

$$\begin{tikzcd} \mathrm{Spec}(B) \arrow[rr, "f"] \arrow[dr, "\rho^*_{B/A}"'] & \arrow[d, phantom, "\circlearrowleft"] & X = \mathrm{Spec}(C) \arrow[dl, "\rho^*_{C/A}"] \\ & \mathrm{Spec}(A) & \end{tikzcd}$$

es conmutativo.

Un Hecho importante de Geometría Algebraica es que $\mathrm{Hom}_{\mathrm{Spec}(A)}(\mathrm{Spec}\, B, \mathrm{Spec}\, C) \simeq \mathrm{Hom}_{A\text{-alg}}(C, B)$.

Así, si $C = A[X_1, \dots, X_n]/\langle f_1, \dots, f_r \rangle$ entonces hay una biyección

$$X(B) \simeq \{(b_1, \dots, b_n) \in B^n,\ f_i(b_1, \dots, b_n) = 0\ \forall i \in \{1, \dots, r\}\}.$$

Más aún, si $\varphi: B \to B'$ morfismo de A-álgebras, entonces $\varphi^*: \mathrm{Spec}(B') \longrightarrow \mathrm{Spec}(B)$ induce $\varphi: X(B) \longrightarrow X(B')$, $f \longmapsto f \circ \varphi^*$. Así, obtenemos un functor covariante

$$X: \underline{A\text{-alg}} \longrightarrow \underline{\mathrm{Conj}},\ B \longmapsto X(B)$$

Caso particular importante: Si $A = \mathbb{K}$ es un cuerpo y $\rho_{\mathbb{L}/\mathbb{K}}: \mathbb{K} \hookrightarrow \mathbb{L}$ es una extensión entonces $\rho_{\mathbb{L}/\mathbb{K}}: X(\mathbb{K}) \hookrightarrow X(\mathbb{L})$. Así, el encajamiento $\mathbb{K} \overset{\Delta}{\hookrightarrow} \prod_{v \in \mathrm{Pl}(\mathbb{K})} \mathbb{K}_v$ induce $X(\mathbb{K}) \overset{\Delta}{\hookrightarrow} \prod_{v \in \mathrm{Pl}(\mathbb{K})} X(\mathbb{K}_v)$ y en particular: $X(\mathbb{K}) \neq \emptyset \Rightarrow X(\mathbb{K}_v) \neq \emptyset\ \forall v \in \mathrm{Pl}(\mathbb{K})$.

Principio Local-Global: ¿Cuándo es válido el recíproco? ¿Cómo es la imagen de Δ?

Slogan: "$\prod_{v \in \mathrm{Pl}(\mathbb{K})} X(\mathbb{K}_v)$ es más fácil de calcular que $X(\mathbb{K})$". Por ejemplo, dados $f_1, \dots, f_r \in \mathbb{Q}[X_1, \dots, X_n]$ es un problema abierto demostrar si existe o no un algoritmo que permita decidir si $\{(x_1, \dots, x_n) \in \mathbb{Q}^n,\ f_i(x_1, \dots, x_n) = 0\ \forall i = 1, \dots, r\} \neq \emptyset$!

⚠ Teorema (Matiyasevich, 1970): Existe $f \in \mathbb{Z}[X_1, \dots, X_{27}]$ tal que no existe un algoritmo que permita decidir si para $n \in \mathbb{N}$ se tiene o no que $\{(x_1, \dots, x_{26}) \in \mathbb{Z}^{26},\ f(x_1, \dots, x_{26}, n) = 0\} \neq \emptyset$.

Def: Sea $\mathbb{K}$ un cuerpo de números y X un esquema definido sobre $\mathbb{K}$. Decimos que X verifica el principio de Hasse si $X(\mathbb{K}_v) \neq \emptyset\ \forall v \in \mathrm{Pl}(\mathbb{K})$ implica que $X(\mathbb{K}) \neq \emptyset$.

Teorema (Hasse, 1924): El principio de Hasse vale para soluciones no nulas de cuádricas $f = \sum_{i,j} a_{ij} x_i x_j$ de rango maximal.

Obs: Para leer más sobre el principio local-global se recomienda el libro "A Course in Arithmetic" por Jean-Pierre Serre y "Cubic forms" por Yuri Manin.

§31. Anillo de Adèles

Una herramienta importante para estudiar el Principio Local-Global es el "anillo de adèles", introducido por Claude Chevalley. La observación clave es que $\mathbb{Z} \hookrightarrow \hat{\mathbb{Z}} := \prod_{p\in\mathcal{P}} \mathbb{Z}_p$ donde $\hat{\mathbb{Z}}$ es compacto (por Tychonoff), pero $\mathbb{Q} \hookrightarrow \prod_{v\in Pl(\mathbb{Q})} \mathbb{Q}_v = \mathbb{R}\times\prod_{p\in\mathcal{P}}\mathbb{Q}_p$ y este último producto no es localmente compacto. La manera de arreglarlo es puramente topológica:

Def: Sea $\{X_i\}_{i\in I}$ una familia de esp. topológicos y sea $\{\mathcal{U}_i\subseteq X_i\}_{i\in I}$ una colección de abiertos. Se define el producto restringido $\coprod_{i\in I}(X_i,\mathcal{U}_i)$ como el esp. topológico
$$\coprod_{i\in I}(X_i,\mathcal{U}_i) := \left\{(x_i)_{i\in I}\in\prod_{i\in I}X_i,\ x_i\in\mathcal{U}_i \text{ salvo quizás finitos } i\in I\right\},$$
con una base de abiertos dada por los $\{\prod_{i\in I}V_i;\ V_i\subseteq X_i$ abierto $\forall i\in I$ y $V_i=\mathcal{U}_i$ salvo quizás finitos $i\in I\}$.

Sea $\mathbb{K}$ un cuerpo de números y note que todo $x\in\mathbb{K}^*$ verifica que
$$\{\mathfrak{p}\in\mathrm{Spec}(\mathcal{O}_\mathbb{K})^*,\ v_\mathfrak{p}(x)\neq 0\} \text{ es finito.}$$
Así, por la fórmula del producto, el conj. $\{v\in Pl(\mathbb{K}),\ |x|_v\neq 1\}$ es finito. Así, $\forall x\in\mathbb{K}$, el conj. $\{v\in Pl(\mathbb{K}),\ |x|_v>1\}$ es finito.

Def: El anillo de adèles del cuerpo de números $\mathbb{K}$ está dado por
$$\mathbb{A}_\mathbb{K} := \left\{(z_v)_v\in\prod_{v\in Pl(\mathbb{K})}\mathbb{K}_v,\ \text{el conj } \{v\in Pl(\mathbb{K}),\ |z_v|_v>1\} \text{ es finito}\right\} \overset{\text{df}}{=} \prod_{w|\infty}\mathbb{K}_w\times\coprod_{v\nmid\infty}(\mathbb{K}_v,\mathcal{O}_v)$$
y es una sub-$\mathbb{K}$-álgebra de $\prod_{v\in Pl(\mathbb{K})}\mathbb{K}_v$, donde $\rho_\mathbb{A}:\mathbb{K}\to\mathbb{A}_\mathbb{K},\ x\mapsto(\rho_{\mathbb{K}_v/\mathbb{K}}(x))_{v\in Pl(\mathbb{K})}$.

Si para todo $S\subseteq Pl(\mathbb{K})$ conjunto finito tal que $\{v|\infty\}\subseteq S$ definimos el anillo de S-adèles como $\mathbb{A}_{\mathbb{K},S} := \prod_{v\in S}\mathbb{K}_v\times\prod_{v\notin S}\mathcal{O}_v$, dotado de la topología producto. Así, $\mathbb{A}_\mathbb{K} \overset{\text{df}}{=} \bigcup_S \mathbb{A}_{\mathbb{K},S}$ y la topología de $\mathbb{A}_\mathbb{K}$ está generada por todos los abiertos en los $\mathbb{A}_{\mathbb{K},S}$.
$\Rightarrow \mathbb{A}_\mathbb{K}$ es un anillo localmente compacto, dotado de la medida de Haar $\prod_{v\in Pl(\mathbb{K})}dx_v$, donde por convención $dx_v(\mathcal{O}_v)=1$ si $v\nmid\infty$.

Lema: Sea $d=[\mathbb{K}:\mathbb{Q}]$ y sea $(e_1,\dots,e_d)$ una $\mathbb{Z}$-base de $\rho_\infty(\mathcal{O}_\mathbb{K})\subseteq\prod_{v|\infty}\mathbb{K}_v$. Entonces, $\mathfrak{D} := \left(\sum_{i=1}^d[0,1[\,e_i\right)\times\prod_{v\nmid\infty}\mathcal{O}_v$ es un dominio fundamental para $\mathbb{K}$ en $\mathbb{A}_\mathbb{K}$, i.e., se tiene:

1. $\mathbb{A}_\mathbb{K}=\bigcup_{x\in\mathbb{K}}(x+\mathfrak{D})$.
2. $(x+\mathfrak{D})\cap(x'+\mathfrak{D})\neq\emptyset \iff x+\mathfrak{D}=x'+\mathfrak{D}\iff x=x'$.

Así, todo $z\in\mathbb{A}_\mathbb{K}$ se escribe de manera única como $z=d+x$ con $d\in\mathfrak{D}$ y $x\in\mathbb{K}$ "=" $\rho_\mathbb{A}(\mathbb{K})$.

Dem: Sea $z=(z_v)_{v\in Pl(\mathbb{K})}\in\mathbb{A}_\mathbb{K}$ y veamos que $\exists!\, d\in\mathfrak{D},\ c\in\mathbb{K}$ tq $z=d+\rho_\mathbb{A}(c)$: Dado que $\mathrm{Spec}(\mathcal{O}_\mathbb{K})^*\xrightarrow{\sim}\{v\nmid\infty\}$, $\mathfrak{p}\mapsto v_\mathfrak{p}$ es una biyección y como $z_{v_\mathfrak{p}}\notin\mathcal{O}_{v_\mathfrak{p}} \overset{\text{df}}{\iff} v_\mathfrak{p}(z_{v_\mathfrak{p}})<0$ tenemos que $I:=\prod_{\substack{\mathfrak{p}\in\mathrm{Spec}(\mathcal{O}_\mathbb{K})^*\\ z_{v_\mathfrak{p}}\notin\mathcal{O}_{v_\mathfrak{p}}}}\mathfrak{p}^{-v_\mathfrak{p}(z_{v_\mathfrak{p}})}\subseteq\mathcal{O}_\mathbb{K}$ es un ideal de $\mathcal{O}_\mathbb{K}$.

Sea $x\in I\setminus\{0\}$. Entonces, $xz=(xz_v)_{v\in Pl(\mathbb{K})}$ verifica que $\forall\mathfrak{p}\in\mathrm{Spec}(\mathcal{O}_\mathbb{K})^*,\ v_\mathfrak{p}(xz_{v_\mathfrak{p}})\geq0$ i.e., $xz_{v_\mathfrak{p}}\in\mathcal{O}_{v_\mathfrak{p}}$. Por otro lado, el Teo. Chino del Resto y el lema en §23, pág 53 implican:
$$\mathcal{O}_\mathbb{K}/\langle x\rangle \xrightarrow{\sim}\prod_{\mathfrak{p}\in\mathrm{Spec}(\mathcal{O}_\mathbb{K})^*}\mathcal{O}_\mathbb{K}/\mathfrak{p}^{v_\mathfrak{p}(x)}\xrightarrow{\sim}\prod_{\mathfrak{p}\in\mathrm{Spec}(\mathcal{O}_\mathbb{K})^*}\mathcal{O}_{v_\mathfrak{p}}/\mathfrak{m}_{v_\mathfrak{p}}^{v_\mathfrak{p}(x)} \underset{\text{de } I}{\overset{\text{df}}{=}} \prod_{\substack{\mathfrak{p}\in\mathrm{Spec}(\mathcal{O}_\mathbb{K})^*\\ z_{v_\mathfrak{p}}\notin\mathcal{O}_{v_\mathfrak{p}}}}\mathcal{O}_{v_\mathfrak{p}}/\mathfrak{m}_{v_\mathfrak{p}}^{v_\mathfrak{p}(x)}$$

Así, $\exists\, y \in \mathcal{O}_{\mathbb{K}}$ tq $x z_{v_\mathfrak{p}} - y \in \mathfrak{m}_{v_\mathfrak{p}}^{v_\mathfrak{p}(x)}$ $\forall \mathfrak{p}$ con $v_\mathfrak{p}(z_{v_\mathfrak{p}}) < 0$. En part, para dichos $\mathfrak{p}$ se tiene $|x z_{v_\mathfrak{p}} - y|_\mathfrak{p} \le \alpha^{-v_\mathfrak{p}(x)} = |x|_\mathfrak{p}$, ie, $\left(z_{v_\mathfrak{p}} - \frac{y}{x}\right) \in \mathcal{O}_{v_\mathfrak{p}}$. Si $v_\mathfrak{p}(z_{v_\mathfrak{p}}) \geq 0$ entonces $v_\mathfrak{p}(x) \overset{\text{dy}}{=} 0$ y luego $|x z_{v_\mathfrak{p}} - y|_\mathfrak{p} \le \max\{|x z_{v_\mathfrak{p}}|, |y|_\mathfrak{p}\} \le 1 = |x|_\mathfrak{p}$ y así concluimos que $(z_{v_\mathfrak{p}} - y/x) \in \mathcal{O}_{v_\mathfrak{p}}$ para todo $\mathfrak{p} \in \operatorname{Spec}(\mathcal{O}_{\mathbb{K}})^*$. Así, $z - \rho_{\mathbb{A}}\left(\frac{y}{x}\right) \in \prod_{v|\infty} \mathbb{K}_v \times \prod_{v\nmid\infty} \mathcal{O}_v$.
Sea α la proyección de $z - \rho_{\mathbb{A}}(y/x)$ a $\prod_{v|\infty} \mathbb{K}_v$ y sean $(x_1, \dots, x_d) \in \mathbb{R}^d$ las coord. de α resp. a la base $(e_1, \dots, e_d)$. Entonces $\sum_{i=1}^d \lfloor x_i \rfloor e_i = \rho_\infty(u)$ para cierto $u \in \mathcal{O}_{\mathbb{K}}$ y por ende $z - \rho_{\mathbb{A}}\left(\frac{y}{x} - u\right)$ "$=$" $z - \frac{y}{x} - u \in \mathfrak{D}$, ie, $z = d + c$ con $d \in \mathfrak{D}$ y $c \in \mathbb{K}$ ✓

Para la unicidad, escribimos $d + c = d' + c'$ con $d, d' \in \mathfrak{D}$ y $c, c' \in \mathbb{K}$. Así, tenemos que $c - c' \in \prod_{v|\infty} \mathbb{K}_v \times \prod_{v\nmid\infty} \mathcal{O}_v$ y luego $v_\mathfrak{p}(c - c') \geq 0$ $\forall \mathfrak{p} \in \operatorname{Spec}(\mathcal{O}_{\mathbb{K}})^*$, ie, $c - c' \in \mathcal{O}_{\mathbb{K}}$. Proyectando en $\prod_{v|\infty} \mathbb{K}_v$, obtenemos que $\rho_\infty(c - c') \in \sum_{i=1}^d]-1,1[\, e_i$ por definición de $\mathfrak{D}$! Como $\rho_\infty(c - c') \in \rho_\infty(\mathcal{O}_{\mathbb{K}})$, deducimos que $\rho_\infty(c - c') = 0$, ie, $c = c'$ y $d = d'$ ■

<u>Teorema</u>: Sea $\mathbb{K}$ un cuerpo de números. Entonces:
1. La imagen de $\rho_{\mathbb{A}} : \mathbb{K} \hookrightarrow \mathbb{A}_{\mathbb{K}}$ es un subgrupo discreto.
2. El cociente $\mathbb{A}_{\mathbb{K}} / \rho_{\mathbb{A}}(\mathbb{K})$ es compacto.
3. $\operatorname{vol}(\mathbb{A}_{\mathbb{K}} / \rho_{\mathbb{A}}(\mathbb{K})) = \sqrt{|d_{\mathbb{K}}|}$.

<u>Dem</u>: Por definición, el conjunto $\mathcal{U} := \sum_{i=1}^d]-\frac{1}{2}, \frac{1}{2}[\, e_i \times \prod_{v\nmid\infty} \mathcal{O}_v$ es abierto en $\mathbb{A}_{\mathbb{K}}$. Si $x \in \mathbb{K}$ es tal que $\rho_{\mathbb{A}}(x) \in \mathcal{U}$ entonces $x = 0$ (cf. Lema anterior) y luego $\{\rho_{\mathbb{A}}(0)\}$ es abierto en $\mathbb{A}_{\mathbb{K}}$ y así $\{\rho_{\mathbb{A}}(x)\}$ abierto $\forall x \in \mathbb{K}$, ie, $\rho_{\mathbb{A}}(\mathbb{K})$ discreto. Así, ① OK ✓
Para ②, observamos que $\overline{\mathfrak{D}} = \sum_{i=1}^d [0,1]\, e_i \times \prod_{v\nmid\infty} \mathcal{O}_v$ es <u>compacto</u> y por el Lema anterior $\pi : \overline{\mathfrak{D}} \twoheadrightarrow \mathbb{A}_{\mathbb{K}} / \rho_\infty(\mathbb{K})$ es sobreyectiva y luego $\mathbb{A}_{\mathbb{K}} / \rho_\infty(\mathbb{K})$ compacto ✓ Por último, basta notar que
$$\operatorname{vol}(\mathbb{A}_{\mathbb{K}}/\mathbb{K}) \overset{\text{dy}}{=} \operatorname{vol}(\mathfrak{D}) = \underbrace{\operatorname{vol}\Big(\prod_{v|\infty} \mathbb{K}_v / \mathcal{O}_{\mathbb{K}}\Big)}_{= \sqrt{|d_{\mathbb{K}}|}} \times \underbrace{\prod_{v\nmid\infty} dx_v(\mathcal{O}_v)}_{\overset{\text{dy}}{=} 1} = \sqrt{|d_{\mathbb{K}}|}$$ ■

<u>Obs</u>: Varios resultados interesantes de Geometría Aritmética se obtienen mediante Análisis de Fourier usando Adèles (cf. A. Chambert-Loir & Yu. Tschinkel, 2000).

§32. <u>Grupo de Idèles</u>

La versión multiplicativa del anillo de adèles es conocida como el grupo de idèles. Más formalmente si consideramos el <u>grupo multiplicativo</u> como el esquema afín
$$\mathbb{G}_m := \operatorname{Spec}(\mathbb{Z}[T, T^{-1}]) \simeq \operatorname{Spec}(\mathbb{Z}[u,v] / \langle uv - 1 \rangle)$$
Entonces para toda álgebra conmutativa B tenemos $\mathbb{G}_m(B) \simeq \{(u,v) \in B^2,\ uv = 1\} \simeq B^\times$.

<u>Def</u>: El <u>grupo de idèles</u> está dado por $\mathbb{A}_{\mathbb{K}}^* = \mathbb{G}_m(\mathbb{A}_{\mathbb{K}})$. Explícitamente,
$$\mathbb{A}_{\mathbb{K}}^* = \{(z_v)_{v \in \mathrm{Pl}(\mathbb{K})} \in \mathbb{A}_{\mathbb{K}},\ z_v \neq 0 \text{ y el conj. } \{v \in \mathrm{Pl}(\mathbb{K}), |z_v|_v \neq 1\} \text{ es finito}\}.$$
Además, $\rho_{\mathbb{A}} : \mathbb{K} \hookrightarrow \mathbb{A}_{\mathbb{K}}$ induce un morfismo de grupos $\rho_{\mathbb{A}^*} : \mathbb{K}^* \hookrightarrow \mathbb{A}_{\mathbb{K}}^*$.

⚠ <u>Obs/Def</u>: La fórmula del producto implica que $\rho_{\mathbb{A}^*}(\mathbb{K}^*) \subseteq \mathbb{G}_m(\mathbb{A}_{\mathbb{K}})^1$, donde $\mathbb{G}_m(\mathbb{A}_{\mathbb{K}})^1 := \{(z_v)_{v \in \mathrm{Pl}(\mathbb{K})} \in \mathbb{A}_{\mathbb{K}}^*,\ \prod_{v \in \mathrm{Pl}(\mathbb{K})} |z_v|_v = 1\}$ es el <u>grupo de 1-idèles</u>.
Se puede probar que, a diferencia de $\mathbb{A}_{\mathbb{K}}^*$, $\mathbb{G}_m(\mathbb{A}_{\mathbb{K}})^1$ es un <u>grupo topológico</u> !

Para extender los resultados sobre adèles al caso de idèles necesitamos la sgte notación:
Sea $\log : \mathbb{A}_{\mathbb{K}}^* \longrightarrow \prod_{v|\infty} \mathbb{R} \simeq \mathbb{R}^{r_1+r_2}$, $(z_v)_{v\in Pl(\mathbb{K})} \longmapsto (\log |z_v|_v)_{v|\infty}$. Así, si consideramos $H := \{(x_w) \in \prod_{w|\infty} \mathbb{R},\ \sum_{w|\infty} N_w x_w = 0\} \simeq \mathbb{R}^r$ con $r = r_1+r_2-1$ y si identificamos $\mathcal{O}_{\mathbb{K}}^*$ con $\varrho_{\mathbb{A}^*}(\mathcal{O}_{\mathbb{K}}^*) \subseteq \mathbb{A}_{\mathbb{K}}^*$, entonces $\log(\mathcal{O}_{\mathbb{K}}^*)$ es un reticulado en H con $\mathbb{Z}$-base $(f_1, \dots, f_r)$.

Sea $\tau : \mathbb{A}_{\mathbb{K}}^* \twoheadrightarrow \mathcal{I}(\mathcal{O}_{\mathbb{K}})$, $(z_v)_{v\in Pl(\mathbb{K})} \longmapsto \prod_{\mathfrak{p}\in \operatorname{Spec}(\mathcal{O}_{\mathbb{K}})^*} \mathfrak{p}^{v_{\mathfrak{p}}(z_{v_{\mathfrak{p}}})}$ morfismo de grupos sobreyectivo, donde $\tau(\varrho_{\mathbb{A}^*}(\mathbb{K}^*)) \overset{\text{def}}{=} Pr(\mathcal{O}_{\mathbb{K}})$. Así, si $C(\mathbb{K}) := \mathbb{A}_{\mathbb{K}}^* / \varrho_{\mathbb{A}^*}(\mathbb{K}^*)$ es el grupo de clases de idèles entonces τ induce $C(\mathbb{K}) \twoheadrightarrow Cl(\mathcal{O}_{\mathbb{K}})$ morfismo sobreyectivo.

Ejercicio Probar que la restricción $\tau : \mathbb{G}_m(\mathbb{A}_{\mathbb{K}})^1 \twoheadrightarrow \mathcal{I}(\mathcal{O}_{\mathbb{K}})$ es sobreyectiva.

Así, si $h := h_{\mathbb{K}} \overset{\text{def}}{=} |Cl(\mathcal{O}_{\mathbb{K}})|$, existen $z_1, \dots, z_h \in \mathbb{G}_m(\mathbb{A}_{\mathbb{K}})^1$ tales que

$$Cl(\mathcal{O}_{\mathbb{K}}) = \{\overline{\tau(z_1)}, \dots, \overline{\tau(z_h)}\}.$$

Notamos que $\ker(\tau) \cap \mathbb{G}_m(\mathbb{A}_{\mathbb{K}})^1 \overset{\text{def}}{=} \{(z_v)_{v\in Pl(\mathbb{K})} \in \prod_{v|\infty} \mathbb{K}_v \times \prod_{v\nmid\infty} \mathcal{O}_v^*,\ \prod_{v|\infty} |z_v|^{N_v} = 1\}$, y luego $\log(\ker(\tau) \cap \mathbb{G}_m(\mathbb{A}_{\mathbb{K}})^1) \subseteq H$. Esto motiva a definir

$$\mathcal{D}_0 := \log^{-1}\Big(\sum_{i=1}^r [0,1[\, f_i\Big) \cap \ker(\tau) \cap \mathbb{G}_m(\mathbb{A}_{\mathbb{K}})^1 \quad \text{y como} \quad \mathcal{D} := \bigcup_{i=1}^h z_i \mathcal{D}_0.$$

Lema: $\mathcal{D}$ es un dominio fundamental para $\mathbb{K}^*$ en $\mathbb{G}_m(\mathbb{A}_{\mathbb{K}})^1$ módulo $\mu_\infty(\mathbb{K})$, i.e., se tiene:
① $\mathbb{G}_m(\mathbb{A}_{\mathbb{K}})^1 = \bigcup_{x\in\mathbb{K}^*} (x\mathcal{D})$.
② $x\mathcal{D} = x'\mathcal{D} \iff x\mathcal{D} \cap x'\mathcal{D} \neq \emptyset \iff x/x' \in \mu_\infty(\mathbb{K})$.

Dem: Para ①, consideramos $z \in \mathbb{G}_m(\mathbb{A}_{\mathbb{K}})^1$. Entonces, $\exists\, i \in \{1, \dots, h\}$ tal que $\overline{\tau(z)} = \overline{\tau(z_i)}$ en $Cl(\mathcal{O}_{\mathbb{K}})$, i.e., $\tau(z/z_i) = \langle x \rangle$ es un ideal fraccionario principal, con $x \in \mathbb{K}^*$. Así, $z/(xz_i) \in \mathbb{G}_m(\mathbb{A}_{\mathbb{K}})^1$ pertenece a $\ker(\tau) \subseteq \prod_{v|\infty} \mathbb{K}_v \times \prod_{v\nmid\infty} \mathcal{O}_v^*$ y cumple que $\log(z/(xz_i)) \in H$, i.e., $\log(z/(xz_i)) = \sum_{i=1}^r \lambda_i f_i$ para cierto $(\lambda_1, \dots, \lambda_r) \in \mathbb{R}^r$.
Sea $u \in \mathcal{O}_{\mathbb{K}}^*$ tal que $\log(u) = \sum_{i=1}^r \lfloor \lambda_i \rfloor f_i$. Entonces, $z/(z_i x u) \in \mathcal{D}_0$ y así $z/(xu) \in \mathcal{D}$.
La unicidad módulo $\mu_\infty(\mathbb{K})$ se deja como **Ejercicio** (Obs clave: $\log(x/x') = 0 \iff x/x' \in \mu_\infty(\mathbb{K})$) ■

Teorema (Lema de Fujisaki): Sea $\mathbb{K}$ un cuerpo de números. Entonces:
① La imagen de $\varrho_{\mathbb{A}^*} : \mathbb{K}^* \hookrightarrow \mathbb{G}_m(\mathbb{A}_{\mathbb{K}})^1$ es un subgrupo discreto.
② El cociente $\mathbb{G}_m(\mathbb{A}_{\mathbb{K}})^1 / \varrho_{\mathbb{A}^*}(\mathbb{K}^*)$ es compacto.

Dem: Por definición, el conjunto $\mathcal{U} := \log^{-1}\Big(\sum_{i=1}^r \left]-\tfrac{1}{2}, \tfrac{1}{2}\right[f_i\Big) \cap \overbrace{\prod_{v|\infty} \mathbb{K}_v \times \prod_{v\nmid\infty} \mathcal{O}_v^*}^{\ker(\tau)} \cap \mathbb{G}_m(\mathbb{A}_{\mathbb{K}})^1$ es abierto en $\mathbb{G}_m(\mathbb{A}_{\mathbb{K}})^1$ y $\mathcal{U} \cap \varrho_{\mathbb{A}^*}(\mathbb{K}^*) = \varrho_{\mathbb{A}^*}(\mu_\infty(\mathbb{K}))$ "=" $\mu_\infty(\mathbb{K})$ por el Lema anterior. Así, podemos elegir $v|\infty$ tal que $\mu_\infty(\mathbb{K}) \subseteq \mathbb{K}_v$ y, al ser $\mu_\infty(\mathbb{K})$ finito, podemos hallar una vecindad abierta de $\{1\}$ en $\mathbb{K}_v$. Así, $\{\varrho_{\mathbb{A}^*}(x)\}$ es abierto $\forall x \in \mathbb{K}^*$, i.e., ① ✓
Para ②, notamos que $\mathcal{O}_v^* = \mathcal{O}_v - \mathfrak{m}_v$ es compacto y luego $\overline{\mathcal{D}} \twoheadrightarrow \mathbb{G}_m(\mathbb{A}_{\mathbb{K}})^1 / \varrho_{\mathbb{A}^*}(\mathbb{K}^*)$ es sobreyectiva con $\overline{\mathcal{D}} = \bigcup_{i=1}^h z_i \cdot \Big(\log^{-1}\Big(\sum_{i=1}^r [0,1] f_i\Big) \times \prod_{v\nmid\infty} \mathcal{O}_v^*\Big)$ conjunto compacto ■

{Cultura general} Usando análisis de Fourier en el grupo de idèles, John Tate prueba en 1950 que $\operatorname{vol}\big(\mathbb{G}_m(\mathbb{A}_{\mathbb{K}})^1 / \varrho_{\mathbb{A}^*}(\mathbb{K}^*)\big) = \dfrac{2^{r_1} (2\pi)^{r_2} h_{\mathbb{K}} \operatorname{Reg}_{\mathbb{K}}}{w_{\mathbb{K}} \sqrt{|d_{\mathbb{K}}|}}$ ("Tate's thesis"), cf. § 29, pág 62 !

§33. Alturas y Teorema de Northcott

Recordemos que si $\mathbb{K}$ es cualquier cuerpo, entonces el espacio proyectivo n-dimensional es
$$\mathbb{P}^n(\mathbb{K}) := \{\text{subespacios vectoriales de dim } 1 \text{ de } \mathbb{K}^{n+1}\}.$$

Así, la aplicación $\pi : \mathbb{K}^{n+1}\setminus\{0\} \twoheadrightarrow \mathbb{P}^n(\mathbb{K})$, $(x_0,\dots,x_n) \mapsto [x_0,\dots,x_n] := \mathrm{Vect}_{\mathbb{K}}(x_0,\dots,x_n)$ es sobreyectiva y $[x_0,\dots,x_n] = [y_0,\dots,y_n] \overset{\text{def}}{\Longleftrightarrow} \exists \lambda \in \mathbb{K}^* \text{ tq } x_i = \lambda y_i \ \forall i \in \{0,\dots,n\}$.

Def: Sea $\mathbb{K}$ un cuerpo de números y $n \in \mathbb{N}^{\geq 1}$. La función de altura en $\mathbb{P}^n(\mathbb{K})$ está dada por $H_n : \mathbb{P}^n(\mathbb{K}) \to \mathbb{R}$, $[x_0,\dots,x_n] \mapsto \prod_{v\in Pl(\mathbb{K})} \max_{0\leq i\leq n} |x_i|_v$

Obs: Si $(y_0,\dots,y_n) = \lambda(x_0,\dots,x_n)$ para cierto $\lambda \in \mathbb{K}^*$ entonces:
$$\prod_{v\in Pl(\mathbb{K})} \max_{0\leq i\leq n} |y_i|_v = \prod_{v\in Pl(\mathbb{K})} \max_{0\leq i\leq n} |\lambda x_i|_v = \underbrace{\Big(\prod_{v\in Pl(\mathbb{K})} |\lambda|_v\Big)}_{=1 \text{ (Fórmula del Producto)}} \Big(\prod_{v\in Pl(\mathbb{K})} \max_{0\leq i\leq n} |x_i|_v\Big) = \prod_{v\in Pl(\mathbb{K})} \max_{0\leq i\leq n} |x_i|_v.$$

Ejemplo importante: Supongamos que $\mathbb{K} = \mathbb{Q}$. En este caso, decimos que $(x_0,\dots,x_n) \in \mathbb{Z}^{n+1}$ es primitivo si $\mathrm{mcd}(x_0,\dots,x_n) = 1$. Notemos que para todo $p \in \mathbb{P}^n(\mathbb{Q})$ existen dos vectores primitivos $\pm(x_0,\dots,x_n) \in \mathbb{Z}^{n+1}$ tal que $p = [x_0,\dots,x_n]$. En efecto:
Si $p = [y_0,\dots,y_n]$ con $(y_0,\dots,y_n) \in \mathbb{Q}^{n+1}\setminus\{0\}$ y N es el producto de los denominadores de los y_i, entonces $N(y_0,\dots,y_n) \in \mathbb{Z}^{n+1}\setminus\{0\}$. Entonces, $x_i := \frac{N y_i}{\mathrm{mcd}(Ny_0,\dots,Ny_n)}$ es tal que $(x_0,\dots,x_n) \in \mathbb{Z}^{n+1}\setminus\{0\}$ es primitivo y $p = [x_0,\dots,x_n]$ ✓ Por otra parte, si $\lambda = \frac{a}{b} \in \mathbb{Q}^*$ es tal que $(y_0,\dots,y_n) = \frac{a}{b}(x_0,\dots,x_n)$ y luego $a \mid \mathrm{mcd}(y_0,\dots,y_n) = 1$ y $b \mid \mathrm{mcd}(x_0,\dots,x_n) = 1$, ie, $\lambda = \pm 1$ ✓

Fórmula para la altura: Sea $p = [x_0,\dots,x_n] \in \mathbb{P}^n(\mathbb{Q})$ con $(x_0,\dots,x_n) \in \mathbb{Z}^{n+1}$ primitivo. Entonces: $H_n([x_0,\dots,x_n]) = \max_{0\leq i\leq n} |x_i|$ donde $|\cdot| = |\cdot|_\infty$.

Dem: La observación clave es que $\mathrm{mcd}(x_0,\dots,x_n) = 1 \Longleftrightarrow$ Para todo primo p se tiene que $\min_{0\leq i\leq n} v_p(x_i) = 0$, ie, $\max_{0\leq i\leq n} |x_i|_p = 1$. Así, $\prod_{v\in Pl(\mathbb{Q})} \max_{0\leq i\leq n} |x_i|_v = \max_{0\leq i\leq n} |x_i|_\infty$ ∎

Consecuencia: Para todo $B \in \mathbb{R}^{>0}$ el conjunto $\{p \in \mathbb{P}^n(\mathbb{Q}),\ H_n(p) \leq B\}$ es finito.
En efecto, $\#\{(x_0,\dots,x_n) \in \mathbb{Z}^{n+1},\ \max|x_i| \leq B\} = (2\lfloor B\rfloor + 1)^{n+1}$ es finito ✓

Notación: Sea $p = [x_0,\dots,x_n] \in \mathbb{P}^n(\overline{\mathbb{Q}})$ tal que $x_j \neq 0$. Definimos $\mathbb{K}(p) \subseteq \overline{\mathbb{Q}}$ como el cuerpo $\mathbb{Q}\left(\frac{x_0}{x_j},\dots,\frac{x_n}{x_j}\right)$, y es indep. de la elección de $j \in \{0,\dots,n\}$. Así, el grado del punto $p \in \mathbb{P}^n(\overline{\mathbb{Q}})$ se define por $\deg(p) := [\mathbb{K}(p):\mathbb{Q}]$.

Ejercicio útil: Sean $\mathbb{M}/\mathbb{L}/\mathbb{K}$ extensiones finitas de cuerpos, entonces $N_{\mathbb{M}/\mathbb{K}}(x) = N_{\mathbb{L}/\mathbb{K}}(N_{\mathbb{M}/\mathbb{L}}(x))$

Lema: Sea $\mathbb{L}/\mathbb{K}$ una extensión de cuerpos de números, y sea
$$\rho_{\mathbb{L}/\mathbb{K}} : \mathbb{P}^n(\mathbb{K}) \longrightarrow \mathbb{P}^n(\mathbb{L}),\ [x_0,\dots,x_n] \mapsto [\rho_{\mathbb{L}/\mathbb{K}}(x_0),\dots,\rho_{\mathbb{L}/\mathbb{K}}(x_n)]$$
Entonces, $H_n(\rho_{\mathbb{L}/\mathbb{K}}(p)) = H_n(p)$ para todo $p \in \mathbb{P}^n(\mathbb{K})$.

Dem: Sea $p = [x_0,\dots,x_n] \in \mathbb{P}^n(\mathbb{K})$ y escribamos $H_n(\rho_{\mathbb{L}/\mathbb{K}}(p)) = \prod_{w\in Pl(\mathbb{L})} \max_i |\rho_{\mathbb{L}/\mathbb{K}}(x_i)|_w$
$= \prod_{v\in Pl(\mathbb{K})} \prod_{w\mid v} \max_i |\rho_{\mathbb{L}/\mathbb{K}}(x_i)|_w$. Si $w \mid v \mid u$ con $w \in Pl(\mathbb{L})$, $v \in Pl(\mathbb{K})$, $u \in Pl(\mathbb{Q})$ entonces sabemos que $|y|_w = |N_{\mathbb{L}_w/\mathbb{Q}_u}(y)|_u^{1/[\mathbb{L}:\mathbb{Q}]}$ $\forall y \in \mathbb{L}_w$. Por el Ejercicio útil,

$N_{\mathbb{L}_w/\mathbb{Q}_u}(y) = N_{\mathbb{K}_v/\mathbb{Q}_u}(N_{\mathbb{L}_w/\mathbb{K}_v}(y))$ y así $|y|_w = |N_{\mathbb{K}_v/\mathbb{Q}_u}(N_{\mathbb{L}_w/\mathbb{K}_v}(y))|_u^{1/[\mathbb{L}:\mathbb{K}][\mathbb{K}:\mathbb{Q}]}$

$\Rightarrow |y|_w = |N_{\mathbb{L}_w/\mathbb{K}_v}(y)|^{1/[\mathbb{L}:\mathbb{K}]} \ \forall y \in \mathbb{L}_w$. Usando esto, calculamos $H_m(\rho_{\mathbb{L}/\mathbb{K}}(p))$ como:

$$\prod_{v \in P\ell(\mathbb{K})} \prod_{w|v} \max_i |N_{\mathbb{L}_w/\mathbb{K}_v}(\rho_{\mathbb{L}/\mathbb{K}}(x_i))|_v^{1/[\mathbb{L}:\mathbb{K}]} = \prod_{v \in P\ell(\mathbb{K})} \prod_{w|v} \max_i \left(|x_i|^{[\mathbb{L}_w:\mathbb{K}_v]}\right)^{1/[\mathbb{L}:\mathbb{K}]}$$

$$= \prod_{v \in P\ell(\mathbb{K})} \max_i \left(|x_i|_v^{\left(\sum_{w|v}[\mathbb{L}_w:\mathbb{K}_v]\right)/[\mathbb{L}:\mathbb{K}]}\right) = \prod_{v \in P\ell(\mathbb{K})} \max_i (|x_i|_v) = H_m(p) \quad \blacksquare$$

<u>Obs práctica</u>: El lema implica que $H_m : \mathbb{P}^m(\overline{\mathbb{Q}}) \to \mathbb{R}^{>0}$ está bien definida !

<u>Teorema</u> (Northcott, 1949): Para todos $d \in \mathbb{N}^{\geq 1}$ y $B \in \mathbb{R}^{>0}$ fijos, el conjunto

$\{p \in \mathbb{P}^m(\overline{\mathbb{Q}}),\ \deg(p) = d \ \text{y}\ H_m(p) \leq B\}$ es <u>finito</u>.

Em part, si $\mathbb{K}$ es un cuerpo de números $\#\{p \in \mathbb{P}^m(\mathbb{K}),\ H_m(p) \leq B\} < +\infty$.

<u>Dem</u> (J.P. Serre): Si $d = 1$ entonces $p \in \mathbb{P}^m(\mathbb{Q})$ y ya sabemos el resultado ✓ Sup. $d \geq 2$ y usemos Teoría de Galois para reducirnos al caso $d = 1$:

Sea $p \in \mathbb{P}^m(\overline{\mathbb{Q}})$ con $p = [x_0, \ldots, x_m]$ y $(x_0, \ldots, x_m) \in \mathbb{K}^{m+1} \setminus \{0\}$ tal que $[\mathbb{K}:\mathbb{Q}] = d$.

Para $\sigma_1, \ldots, \sigma_d : \mathbb{K} \hookrightarrow \overline{\mathbb{Q}}$ en $\Sigma_{\mathbb{K}/\mathbb{Q}}$ consideramos $p_i := [\sigma_i(x_0), \ldots, \sigma_i(x_m)] \in \mathbb{P}^m(\overline{\mathbb{Q}})$ y sea $q := (p_1, \ldots, p_d) \in \mathbb{P}^m(\overline{\mathbb{Q}})^d = \mathbb{P}^m(\overline{\mathbb{Q}}) \overset{d \text{ veces}}{\times \cdots \times} \mathbb{P}^m(\overline{\mathbb{Q}})$.

El grupo simétrico S_d actúa en $\mathbb{P}^m(\overline{\mathbb{Q}})^d$, por lo que definimos $\pi : \mathbb{P}^m(\overline{\mathbb{Q}})^d \twoheadrightarrow \Sigma_{m,d}(\overline{\mathbb{Q}})$ con $\Sigma_{m,d}(\overline{\mathbb{Q}}) := \mathbb{P}^m(\overline{\mathbb{Q}})^d / S_d$ y donde π tiene fibras de cardinal <u>finito</u> $\leq d!$.

Así, por construcción, $\pi(q)$ "=" $p_1 \cdots p_d$ es $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$-invariante y luego tenemos que $\pi(q) \in \Sigma_{m,d}(\mathbb{Q}) = \mathbb{P}^m(\mathbb{Q})^d / S_d$. Por otro lado, podemos construir explícitamente (cf. Mumford "Geometric Invariant Theory") $\chi : \Sigma_{m,d} \hookrightarrow \mathbb{P}^N$ como sigue (cf. "encajamiento de Segre"): En $\mathbb{K}[T_{i,j} \,;\, 0 \leq i \leq m,\ 1 \leq j \leq d]$ considere polinomios de la forma

$$\prod_{i=0}^m \sigma_{j_i}(T_{i,1}^{\alpha_i}, \ldots, T_{i,d}^{\alpha_i})$$

con $\alpha_0 + \ldots + \alpha_m = d$ y $0 \leq \alpha_i \leq d$, ie, consideramos una base de polinomios homogéneos de grado d en las variables $(T_{0,j}, \ldots, T_{m,j})$, con $1 \leq j \leq d$, y simétricos en las variables $(T_{i,1}, \ldots, T_{i,d})$ para $0 \leq i \leq m$. Sea $N+1$ el cardinal de esta base. Se verifica que si $(x_{0,j}, \ldots, x_{m,j}) \neq 0$, para cierto j entonces uno de estos polinomios es $\neq 0$. Así, obtenemos $(\mathbb{P}^m)^d \hookrightarrow \mathbb{P}^N$ que induce $\chi : \Sigma_{m,d} \hookrightarrow \mathbb{P}^N$ ✓

Si m es el máximo grado total de los polinomios usados entonces, acotando $\left|\prod_{i=0}^m \sigma_{j_i}(x_{i,1}^{\alpha_i}, \ldots, x_{i,d}^{\alpha_i})\right|_v$, deducimos que $\exists\, C \in \mathbb{R}^{>0}$ tal que $H_N(\chi(\pi(q))) \leq C\, H_m(p)^m \leq \widetilde{B}$ y luego deducimos que hay finitos $\chi(\pi(q)) \in \mathbb{P}^N(\mathbb{Q})$ y luego finitos $p \in \mathbb{P}^m(\mathbb{K})$ $\blacksquare$

Cultura general: Sea $\mathbb{K}$ un cuerpo de números. Para $B \in \mathbb{R}^{>0}$ se denota

$$N(\mathbb{P}^m(\mathbb{K}), B) := \#\{p \in \mathbb{P}^m(\mathbb{K}),\ H_m(p) \leq B\}.$$

En 1979, S. Schanuel prueba que para $m \geq 2$ se verifica que

$$N(\mathbb{P}^m(\mathbb{K}), B) = \frac{h_{\mathbb{K}}\, \mathrm{Reg}_{\mathbb{K}}\, (n+1)^{r_1+r_2-1}}{w_{\mathbb{K}}\, \zeta_{\mathbb{K}}(n+1)} \left(\frac{2^{r_1}(2\pi)^{r_2}}{\sqrt{|d_{\mathbb{K}}|}}\right)^{n+1} \cdot B^{n+1}(1 + o(1)).$$

Para más detalles se recomienda el libro "Lectures on the Mordell-Weil Theorem" por J.P. Serre.

⚠ Conjetura/Principio de Batyrev - Manin - Peyre: "$N(X, B)$ depende de la <u>geometría</u> de X"

Ver "Points de hauteur bornée et géométrie des variétés" por Emmanuel Peyre.