Recordar: si K cpo de números, $\mathcal{O}_K$ anillo de enteros, todo ideal $\mathfrak{a} \subset \mathcal{O}_K$, tiene un representante $\mathfrak{b}$ con norma:

$$N(\mathfrak{b}) \leq \frac{n!}{n^n} \left(\frac{4}{\pi}\right)^s \sqrt{|\mathrm{disc}(\mathcal{O}_K)|}$$

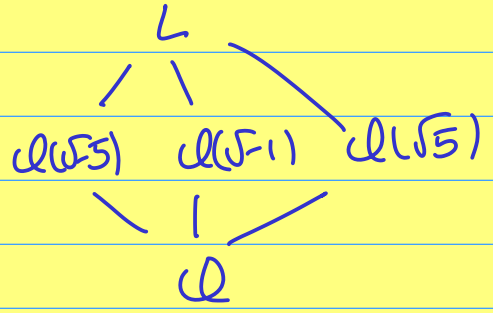
donde $\boxed{n = r + 2s}$, $r = \mathrm{Hom}_{\mathbb{Q}}(K, \mathbb{R})$, $2s = \mathrm{Hom}_{\mathbb{Q}}(K, \mathbb{C})$ cuya imagen no cae en $\mathbb{R}$.

Coro: toda extensión de $\mathbb{Q}$ ramifica en algún primo.

Ejemplo: $K = \mathbb{Q}(\sqrt{-5}) \rightsquigarrow h = 2$ $\mathcal{O}_K = \{\mathcal{O}_K, \langle 2, 1+\sqrt{-5}\rangle\}$

$L = K(\sqrt{-1})$, L/K cuadrática, $L/\mathbb{Q}$ es Galois,

$L = \mathbb{Q}(\sqrt{-5}, \sqrt{-1})$, $\mathrm{Gal}(L/\mathbb{Q}) \simeq \mathbb{Z}_2 \times \mathbb{Z}_2$.



Afirmo: L/K es no ramificada.

- Si $\mathfrak{P} \subset \mathcal{O}_K$ que ramifica en $L/K \Rightarrow \mathfrak{P} \cap \mathbb{Z} \in \{2, 5\}$

pues $p = \mathfrak{P} \cap \mathbb{Z}$, p debe ramificar en alguna de las tres

extensiones cuadráticas. Mirando las ramificaciones se sigue el resultado.

- $p = 5$, $\mathfrak{P} = (\sqrt{-5})$, $e(\mathfrak{P}|5) = 2$. Si $\tilde{\mathfrak{P}}_5$ denota un primo de L arriba de $\mathfrak{P}$, $e(\tilde{\mathfrak{P}}_5|5) = 2 = e(\tilde{\mathfrak{P}}_5|\mathfrak{P}_5)$.

$$e(\mathfrak{P}_5|5) \overset{\|}{2} \Rightarrow \boxed{e(\tilde{\mathfrak{P}}_5|\mathfrak{P}_5) = 1}$$

- $p = 2$ $\quad \mathfrak{P}_2 = \langle 2, 1+\sqrt{-5} \rangle$, $\quad e(\mathfrak{P}_2|2) = 2$

$$\begin{matrix} \mathbb{Q}(\sqrt{5}) \\ | \\ \mathbb{Q} \end{matrix} \quad 4 \nmid |\mathrm{disc}(\ )| = 5, \ 2 \text{ es inerte} \rightsquigarrow f = 2$$

Como antes, $\tilde{\mathfrak{P}}_2$ en L arriba de $\mathfrak{P}_2$, $e(\tilde{\mathfrak{P}}_2|2) = 2$

$\Rightarrow e(\tilde{\mathfrak{P}}_2|\mathfrak{P}_2) = 1$ ∎

Luego L/K es no ramificada en ningún primo.

<u>Versión 2</u>: $\mathrm{disc}(L/K) \overset{?}{=} \mathcal{O}_K = \langle \mathrm{disc}(\{\alpha, \beta\}) : \alpha, \beta \in \mathcal{O}_L \rangle_{\mathcal{O}_K}$

$\mathrm{disc}(\{1, i\}) = 4 \rightsquigarrow \mathrm{disc}(L/K) \mid 4 \cdot \mathcal{O}_K$.

$$\mathrm{disc}\left(\left\{1, \frac{1+\sqrt{5}}{2}\right\}\right) = \det\begin{pmatrix} 1 & \frac{1+\sqrt{5}}{2} \\ 1 & \frac{1-\sqrt{5}}{2} \end{pmatrix}^2 = 5$$

$\mathrm{disc}(L/K) \mid 5 \cdot \mathcal{O}_K \Rightarrow \mathrm{disc}(L/K) = \mathcal{O}_K$ ∎

Teo (Hilbert) Si K cuerpo de números, L/K la máxima extensión abeliana y no ramificada de K, entonces L/K es finita y $[L:K] = h_K = \#Gal(\mathcal{O}_K)$.

Más aún, $Gal(L/K) \simeq Cl(\mathcal{O}_K)$.

Al cuerpo L se lo llama el cuerpo de Hilbert de K.

Problema: ¿cómo construirlo? Abierto (muy difícil).

Para $\mathbb{Q}$: $L/\mathbb{Q}$ abeliana, $K \subset \mathbb{Q}(e^{2\pi i/N})$ algún N.

Si K cuadrático imaginario, algo similar ocurre, involucra curvas elípticas. $L = K(j(E))$

¿K cuadrático real? (Darmon y cía).

Problemas: • ¿Poder decir algo de h_K? Gauss: hay finitos cuerpos cuadráticos imaginarios con $h_K = 1$

(Heegner 1952). Mismo para $h_K = 2, 3, \ldots$

• ¿cuerpos cuadráticos reales? $\approx 75{,}446\,\%$ de cuerpos con $h_K = 1$ (heurística de Cohen-Lenstra).

El grupo de unidades

Dado K cpo de números, $\mathcal{O}_K$ anillo de enteros,

grupo de unidades.

¿$\mathcal{O}_K^\times$ = ? (elementos inversibles para el producto).

Ejemplos: ① si $K = \mathbb{Q}$, $\mathcal{O}_{\mathbb{Q}} = \mathbb{Z}$, $\mathbb{Z}^\times = \{\pm 1\}$.

② K cuadrático imaginario. $\mathcal{O}_K = \left\{ \frac{a + b\sqrt{-d}}{2} \right\}$ $d > 0$.

$$u \in \mathcal{O}_K^\times \Rightarrow Nm_{K/\mathbb{Q}}(u) \in \mathbb{Z}^\times = \{\pm 1\}$$

$$u \cdot u^{-1} = 1 \Rightarrow \underset{\in \mathbb{Z}}{Nm(u)} \cdot \underset{\in \mathbb{Z}}{Nm(u^{-1})} = 1$$

$$Nm\left(\frac{a + b\sqrt{-d}}{2}\right) = \frac{a^2 + b^2 d}{4} \geq 0 \rightsquigarrow Nm(u) = 1.$$

$$1 \qquad a^2 + b^2 d = 4 \text{ hay finitas.}$$

③ $K = \mathbb{Q}(\sqrt{5})$, $u = \frac{1+\sqrt{5}}{2}$, $Nm(\epsilon) = \frac{1-5}{4} = -1$.

$$u \cdot \frac{\bar{u}}{N(u)} = 1 \rightsquigarrow u \in \mathcal{O}_K^\times,\ u^k \in \mathcal{O}_K^\times,\ k \in \mathbb{Z}$$

$\rightsquigarrow$ ¡hay infinitas unidades!

Problema: ¿ $\mathcal{O}_K^\times$ es f.g.? ¿ rango? ¿ hallar generadores?

Teo (Dirichlet): $\mathcal{O}_K^\times$ es f.g., más aún, $\mathcal{O}_K^\times = U \times V$, U es finito (raíces de la unidad en K), V es libre de rango $r + s - 1$.

Obs: · K/ℚ cuad. imag., $r=0$, $s=1 \Rightarrow r+s-1=0$.

· K/ℚ cuad. real, $r=2$, $s=0 \Rightarrow r+s-1=1$.

$U = \langle \mu \rangle$ $\qquad U = \{\pm 1\}$.

↑ bien definido salvo $\{\pm\mu, \pm\mu^{-1}\}$

Problema: ¿cómo determinar la "unidad fundamental"?

(Ecuación de Pell ← algoritmo que involucra fracciones continuas)

· En general: → calcular U es fácil
↳ calcular V cuesta.

Dem: $[K:\mathbb{Q}] = n$, $n = r+2s$, $r = \#\mathrm{Hom}_{\mathbb{Q}}(K, \mathbb{R})$

$$\widetilde{Log}: K^\times \xrightarrow[\text{antes}]{} \left(\mathbb{R}^\times \Big|^r \times \left(\mathbb{R}^2 \setminus \{(0,0)\}\right)^s \longrightarrow \mathbb{R}^{r+s} \quad (\text{grupo con la suma})\right.$$

$$a \to (\sigma_1(a), \dots, \sigma_r(a), \mathrm{Re}(\tau_1(a)), \mathrm{Im}(\tau_1(a)), \dots)$$

$$\log(x_1, \dots, x_r, x_{r+1}, x_{r+2}, \dots, x_{n-1}, x_n) =$$

$$= (\log|x_1|, \dots, \log|x_r|, \log(x_{r+1}^2 + x_{r+2}^2), \dots$$
$$\dots, \log(x_{n-1}^2 + x_n^2))$$

Obs: $\Lambda(K^\times) \subset \left(\mathbb{R}^\times\right)^r \times \left(\mathbb{R}^2 \setminus \{(0,0)\}\right)^s$

$a \neq 0$, $\sigma_i(a) \neq 0 \Rightarrow \sigma_i(a) \in \mathbb{R}^\times$

$\tau_j(a) \neq 0 \Rightarrow \mathrm{Re}(\tau_j(a)) \neq 0$ ó $\mathrm{Im}(\tau_j(a)) \neq 0$.

Obs: $\widetilde{\log}(\alpha) = (\log(|\sigma_1(\alpha)|), \dots, \log(|\tau_1(\alpha)|^2), \dots, \log(|\tau_s(\alpha)|^2))$

Luego $\widetilde{\log}$ está bien definido. Su restricción a $\mathcal{O}_K^\times \subset K^\times$, satisface:

① $\widetilde{\log}(\alpha\beta) = \widetilde{\log}(\alpha) + \widetilde{\log}(\beta)$ ("morfismo")

② Si $\mu \in \mathcal{O}_K^\times$, $Nm_{K/\mathbb{Q}}(\mu) = \pm 1 = \prod_{i=1}^{r} \sigma_i(\alpha) \cdot \prod_{j=1}^{2s} \tau_j(\alpha)$

$\Rightarrow$ "$\log(|Nm(\mu)|) = \sum_{i=1}^{r} \log(|\sigma_i(\alpha)|) + \sum_{j=1}^{s} \log(|\tau_j(\alpha)|^2)$"

digamos $\overline{\tau}_1 = \tau_{s+1}$, $\overline{\tau}_2 = \tau_{s+2}, \dots$

$= \widetilde{\log}(\mu)$

$\Rightarrow \widetilde{\log}(\mathcal{O}_K^\times) \subset H = \{x_1 + \dots + x_{r+1} = 0\}$

↑ hiperplano en $\mathbb{R}^{r+1}$.

③ Si $U \subset \mathbb{R}^{r+1}$ acotado, $\log^{-1}(U) \subset \mathbb{R}^{r+1}$ es acotado (por la definición de log).

$\varphi : K \to \mathbb{R}^{r+1}$ ample $\varphi(\mathcal{O}_K)$ es discreto. Luego, $\varphi(\mathcal{O}_K) \cap \log^{-1}(U)$ es finito.

↑ discreto ↑ acotado

$\Rightarrow \widetilde{\log}^{-1}(U) \subset \mathcal{O}_K^\times$ está contenido en $\varphi^{-1}(\varphi(\mathcal{O}_K) \cap \log^{-1}(U))$

↑ restricción a $\mathcal{O}_K^\times$ es finito. ∎

Hicimos $U = \{\vec{0}\}$, $\widetilde{\log}^{-1}(\{\vec{0}\}) = N_\infty(\widetilde{\log})$

$$0 \to N_U(\widetilde{\log}) \to U_K^x \to \widetilde{\log}(U_K^x) \to 0$$

$\|$

U es finito.

Obs: $U \subset \{\text{raíces de 1 en } K\}$ por ser U finito.

si $u \in U$, $\exists N \mid u^N = 1$

2) si ξ es raíz de 1 en K, $\exists N \in \mathbb{N}$ t.q. $\xi^N = 1 \Rightarrow$

$\Rightarrow \widetilde{\log}(\xi^N) = 0$

$\|$

$N \cdot \widetilde{\log}(\xi) \in (\mathbb{R}^{r+1}, +)$ ← libre de torsión $\Rightarrow \widetilde{\log}(\xi) = 0$.

Ejercicio: U es cíclico.

① $\widetilde{\log}(U_K^x) \subset H$, es f.g.

Lema 1: si $L \subset \mathbb{R}^N$, L es un $\mathbb{Z}$-mod t.f. $L \cap U$ es finito $\forall U \subset \mathbb{R}^N$ acotado $\Rightarrow$ L es f.g. de (más adelante) rango $\leq N$.

Como $(\mathbb{R}^{r+1}, +)$ es sin torsión, $\widetilde{\log}(U_K^x) \simeq \mathbb{Z}^d$,

$d \leq r+1-1$. Resta ver $d = r+1-1$.

Lema 2: Fijado $1 \leq k \leq r+1$, dado $d \in \mathbb{Q}_K$, $\exists \beta \in \mathbb{Q}_K$ t.f. ① $|N_m(\beta)| \leq \left(\frac{2}{\pi}\right)^s \sqrt{|\text{disc}(\mathbb{Q}_K)|}$

② $\widetilde{\log}_i(\beta) < \widetilde{\log}_i(\alpha)$ i coordenada i de la imagen.

para $1 \le i \le r+1$, $i \neq k$

Lema 3: Fijado $1 \le k \le r+1$, $\exists\, u_k \in \mathcal{O}_K^\times$ t.q.

$$\widetilde{\log}_i(u_k) = \begin{cases} < 0 & \text{si } i \neq k \\ > 0 & \text{si } i = k \end{cases}$$

Así, construimos $r+1$ unidades que cumplen que sus coordenadas son todas < 0, salvo 1.

$$(A)_{ij} = \begin{pmatrix} \widetilde{\log}_1(u_1) & \cdots & \vdots \\ \vdots & & \vdots \\ \widetilde{\log}_{r+1}(u_1) & & \end{pmatrix} \begin{cases} A_{ij} < 0 \text{ si } i \neq j \\ A_{ii} > 0 \end{cases}$$

Lema 4: $\operatorname{rango}(A_{ij}) = r+1-1$.

$\Rightarrow \widetilde{\log}(\mathcal{O}_K^\times)$ tiene rango $r+1-1$.

"$\langle u_1, \dots, u_{r+1} \rangle$". $V = \langle \widetilde{\log}^{-1}(u_1), \dots, \widetilde{\log}^{-1}(u_{r+1-1}) \rangle$ alguno.