28/10) **Teorema** $d>1$ libre de cuadrados

$x^2 - dy^2 = 1$ tiene solución entera. distinta de $(\pm 1, 0)$

Dem. $K = \mathbb{Q}(\sqrt{d})$

$\alpha \in \mathbb{Z}[\sqrt{d}] \Rightarrow \alpha = x + y\sqrt{d} \qquad N(\alpha) = x^2 - dy^2$

$$\mathbb{Z}[\sqrt{d}] \hookrightarrow \mathbb{R}^2$$

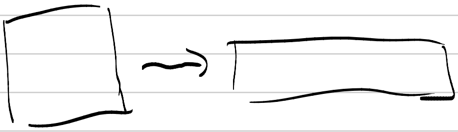
$$a + b\sqrt{d} \longmapsto (a + b\sqrt{d},\ a - b\sqrt{d}).$$

$\Lambda < \mathbb{R}^2 \qquad \Lambda \cap \{xy = 1\}$

$X \subset \mathbb{R}^2$ c.c.s., acotado, $\operatorname{vol} X > 4 \cdot \operatorname{covol} \Lambda$

$\underset{\text{Minkowski}}{\Rightarrow} \quad X \cap \Lambda \neq \{0\}$

$\lambda > 0 \qquad X_\lambda = (\lambda, \lambda^{-1}) \cdot X \qquad \operatorname{vol}(X_\lambda) = \operatorname{vol}(X).$



$X_\lambda \cap \Lambda \neq \{0\}$

$\forall \lambda > 0 \quad \exists\ \alpha_\lambda \in \mathbb{Z}[\sqrt{d}] \qquad X \cap \Lambda$

$|N_{K/\mathbb{Q}}(\alpha_\lambda)| \leq C \qquad$ hay # finito de (α_λ)

$\exists\ \lambda \neq \lambda'$ t.q. $(\alpha_\lambda) = (\alpha_{\lambda'})$ y $\alpha_\lambda \neq \pm \alpha_{\lambda'}$

$\Updownarrow$

$\alpha_\lambda = u \cdot \alpha_{\lambda'} \qquad u \in \mathbb{Z}[\sqrt{d}]^\times$, $u \neq \pm 1$

$u = x + y\sqrt{d}.$

$\pm 1 = N(u) = x^2 - dy^2$

Si $N(u) = -1 \Rightarrow N(u^2) = +1$. Ganamos $\square$

Corolario $\mathbb{Z}[\sqrt{d}]^\times$ es infinito.

Dem. $u \in \mathbb{Z}[\sqrt{d}]^\times$, $u \neq \pm 1 \Rightarrow u^n$, $n \in \mathbb{Z}$ son diferentes unidades $\square$

$\pm u^n \qquad \{\pm 1\} \times \langle u \rangle.$

§ Teorema de unidades de Dirichlet

Teorema $K/\mathbb{Q}$. $r_1 = \#$ de encajes reales
$2r_2 = \#$ de encajes complejos

$$\mathcal{O}_K^\times \simeq \mu_K \times \underbrace{\mathbb{Z}^{r_1+r_2-1}}$$

μ_K ← $(\mathcal{O}_K^\times)_{tors}$

$\mathbb{Z}^{r_1+r_2-1}$ ← libre de rango r_1+r_2-1

$\exists\ u_1, \dots, u_{r_1+r_2-1} \in \mathcal{O}_K^\times$ t.q. (unidades fundamentales)

$$\mathcal{O}_K^\times \simeq \mu_K \times \langle u_1 \rangle \times \dots \times \langle u_{r_1+r_2-1} \rangle$$

Ejemplos $K = \mathbb{Q}(\sqrt{d})$

- $d<0 \Rightarrow r_1 = 0,\ r_2 = 1 \quad r_1 + r_2 - 1 = 0.$

  $\mathcal{O}_K^\times$ es finito. $\mathcal{O}_K^\times = \mu_K.$

  $[\mathbb{Q}(\zeta_n) : \mathbb{Q}] = \varphi(n) \leq 2.$

  - $\mu_K = \mu_4(\mathbb{C}) = \{\pm 1, \pm i\}$ $\quad d = -1.$
  - $\mu_K = \mu_6(\mathbb{C})$ $\quad d = -3$
  - $\mu_K = \mu_2(\mathbb{C}) = \{\pm 1\}$ $\quad d \neq -1, -3.$

- $d > 0 \Rightarrow r_1 = 2,\ r_2 = 0, \quad r_1 + r_2 - 1 = 1$

  $\exists\ u \in \mathcal{O}_K^\times$ t.q. $\mathcal{O}_K^\times \simeq \{\pm 1\} \times \langle u \rangle$

Si u es una unidad fundamental $\Rightarrow \pm u^{\pm 1}$ también lo es.

Normalmente se toma $u > 1$. □

$$\left.\begin{array}{l} \Phi : K \hookrightarrow K_{\mathbb{R}} \\ \alpha \longmapsto (\tau(\alpha))_\tau \end{array}\right\} \rightsquigarrow \Phi : K^\times \hookrightarrow K_{\mathbb{R}}^\times$$

$|z_{\bar{\tau}}| = |\overline{z_\tau}| = |z_\tau|$

$\sigma, \bar{\sigma}$

$$\log|\cdot| : K_{\mathbb{R}}^\times \longrightarrow \mathbb{R}^{r_1+r_2}$$
$$(\dots, z_\tau, \dots) \longmapsto (\dots, \log|z_\tau|, \dots)$$

$$
\begin{array}{ccccccc}
\mathcal{O}_K^\times & \xrightarrow{\quad L \quad} & & & H & & \\
\downarrow & & & & \downarrow & & \\
K^\times & \xhookrightarrow{\ \Phi\ } & K^\times_{\mathbb{R}} & \xrightarrow{\log|\cdot|} & \mathbb{R}^{r_1+r_2} & \hookrightarrow & \mathbb{R}^n \\
{\scriptstyle N_{K/\mathbb{Q}}}\downarrow & & & & \downarrow{\scriptstyle \varphi} & & \downarrow{\scriptstyle \Sigma} \\
\mathbb{Q}^\times & & \xrightarrow{\quad \log|\cdot| \quad} & & \mathbb{R} & = & \mathbb{R}
\end{array}
$$

$\varphi : (x_\tau)_\tau \longmapsto \sum_\tau n_\tau x_\tau \qquad n_\tau = \begin{cases} 1, & \tau \text{ real} \\ 2, & \tau \text{ complejo} \end{cases}$

$H = \ker \varphi$.

$\text{codim } H = 1 \iff \dim_{\mathbb{R}} H = r_1 + r_2 - 1$

$\alpha \in \mathcal{O}_K^\times \Rightarrow N(\alpha) = \pm 1 \iff \prod_\tau \tau(\alpha) = \pm 1.$

$\Rightarrow \sum_\tau \log|\tau(\alpha)| = 0 \iff \log|\Phi(\alpha)| \in H$

$\ker L = \{\alpha \in \mathcal{O}_K^\times \mid |\tau(\alpha)| = 1 \ \forall\, \tau : K \hookrightarrow \mathbb{C}\}$

$\Phi(\mathcal{O}_K)$ es un retículo en $K_{\mathbb{R}}$.
(subgrupo discreto)

Hay un # finito de $\alpha \in \mathcal{O}_K$ t.q. $|\tau(\alpha)| = 1 \ \forall \tau$

$\ker L$ es finito. $\Rightarrow \alpha \in \ker L \Rightarrow \alpha \in \mu_\infty(\mathbb{C})$.

Viceversa, si $\alpha \in \mu_\infty(\mathbb{C}) \Rightarrow |\tau(\alpha)| = 1$

Conclusión: $\ker L = (\mathcal{O}_K^\times)_{tors}$

$= \mu_\infty(\mathbb{C}) \cap K = \mu_K.$

$\Lambda := L(\mathcal{O}_K^\times) \qquad \Lambda \subset H \qquad \Lambda$ es un gpo libre

$$1 \to \mu_K \xhookrightarrow{i} \mathcal{O}_K^\times \xrightarrow{L} \Lambda \to 0 \qquad \text{s.e.c.}$$

•) $L \circ s = id_\Lambda$

$\mathcal{O}_K^\times \simeq \mu_K \times \underline{\Lambda}$

•) $\Rightarrow \mathcal{O}_K^\times \simeq \mu_K \times \Lambda$

$(i(x), s(y)) \leftarrow (x, y)$

•) Λ es un retículo en H

($\Leftarrow$ subgrupo discreto)

$X \subset H$ acotado, $\omega \in \Lambda$, $\omega \in X$

$\longleftrightarrow$ cota sobre los $|\tau(\alpha)|$ para $\alpha \in \mathcal{O}_K^\times$

$\longleftrightarrow$ Cota sobre los coef. $f^{\alpha}_{K/\mathbb{Q}}(x) \in \mathbb{Z}[x]$.

$\Rightarrow$ # finito de α.

•) $rk\ \Lambda = r_1 + r_2 - 1 = \dim_{\mathbb{R}} H$

Λ es un retículo de rango completo.

$\Leftarrow \exists\ Y \subset H$ acotado t.q.

$$H = \bigcup_{\omega \in \Lambda} Y + \omega$$

$X_t = \{(x_\tau)_\tau \in K_{\mathbb{R}} \mid |x_\tau| < t \ \ \forall \tau\} \subset K_{\mathbb{R}}$

$$vol(X_t) = 2^{r_1} \cdot (2\pi)^{r_2} \cdot t^n.$$

$t >> 0$ t.q. $vol\ X_t > 2^n \cdot \underline{\sqrt{|\Delta_K|}}$

$\quad$ ↳ covol $\Phi(\mathcal{O}_K)$

$S = \{(x_\tau)_\tau \in K_{\mathbb{R}}^\times \mid |\prod_\tau x_\tau| = 1\} \subset K_{\mathbb{R}}^\times$

$\forall\ \underline{s} \in S \quad vol(\underline{s} \cdot X_t) = vol(X_t)$

$\exists\ \alpha_s \in \mathcal{O}_K$ t.q. $\Phi(\alpha_s) \in s \cdot X_t$.

$(x, x^{-1}) \cdot X$

$s \in \Phi(\alpha_s)^{-1} \cdot X_t.$

$$S = \bigcup_{s \in S'} \Phi(\alpha_s)^{-1} X_t.$$

$$\phi(\alpha_s) \in s X_t \Rightarrow |N(\alpha_s)| = \prod_{\tau} |\tau(\alpha_s)| < t^n.$$

los α_s tienen norma acotada $\Rightarrow$
Hay un # finito de ideales $(\alpha_s) \subset \mathcal{O}_K$

$$S = \bigcup_{s \in S_0} \Phi(\alpha_s)^{-1} \underbrace{\Phi(\mathcal{O}_K^\times) X_t}.$$

$S_0' \subseteq S'$ subconj. finito

$$\log |S| = H$$

$$H = \underbrace{\bigcup_{s \in S_0} \log |\Phi(\alpha_s)^{-1}|} + \Lambda + \log |X_t|.$$

$$H = \bigcup_{w \in \Lambda} Y + w$$

$$\Rightarrow \operatorname{rk} \Lambda = r_1 + r_2 - 1.$$

Ejemplo p primo impar, $K = \mathbb{Q}(\zeta_p) \hookrightarrow \mathbb{C}$

$r_1 + 2r_2 = p - 1$

$r_1 = 0$

$r_2 = \frac{p-1}{2}.$

$$\operatorname{rk} \mathcal{O}_K^\times = r_1 + r_2 - 1$$
$$= \frac{p-1}{2} - 1.$$

$$K = \mathbb{Q}(\zeta_p) \circlearrowleft \text{conjugación compleja.}$$

$$\Big|\, 2$$

$$K^+ = \mathbb{Q}(\zeta_p + \zeta_p^{-1})$$

$$\Big|\, \frac{p-1}{2}$$

$$\mathbb{Q}$$

Para K^+

$$r_1 = \frac{p-1}{2}$$

$$r_2 = 0.$$

$$\mathcal{O}_{K^+}^\times \subset \mathcal{O}_K^\times$$

$$[\mathcal{O}_K^\times : \mathcal{O}_{K^+}^\times] < \infty$$

$$\| \quad p.$$

Ejercicio:

$$\mathbb{Z}[\zeta_p]^\times = \langle \zeta_p \rangle \times \mathcal{O}_K^\times$$

$\boxed{p = 5}$

$$K = \mathbb{Q}(\zeta_5) \qquad \mathbb{Z}[\zeta_5].$$

$$\Big|\, 2$$

$$K^+ = \mathbb{Q}(\sqrt{5}) \qquad \mathbb{Z}\left[\frac{1+\sqrt{5}}{2}\right]$$

$$\Big|\, 2$$

$$\mathbb{Q}$$

Unidad fund. en $\mathbb{Z}\left[\frac{1+\sqrt{5}}{2}\right]$ es

$$\frac{1+\sqrt{5}}{2} = \zeta_5^2 + \zeta_5^3.$$

$$\mathbb{Z}[\zeta_5]^\times = \{\pm \zeta_5^a \cdot (\zeta_5^2 + \zeta_5^3)^n \mid n \in \mathbb{Z}\}$$

$$= \mu_{10}(\mathbb{C}) \times \langle 1 + \zeta_5 \rangle$$

parte libre rk = 1.