<u>Repaso:</u> definimos el anillo de enteros algebraicos (dado $K/\mathbb{Q}$ finita)

$$\mathcal{O}_K = \{ \alpha \in K : m_\alpha(x) \in \mathbb{Z}[x] \}$$

<u>vimos:</u> ① $\mathcal{O}_K$ es anillo
② $\mathcal{O}_K$ es un $\mathbb{Z}$-mód. de rango $d = [K:\mathbb{Q}]$
③ Algoritmo para calcular generadores.

¿Hay factorización única en $\mathcal{O}_K$? <u>NO</u> (en general)

<u>Ejemplo:</u> $K = \mathbb{Q}(\sqrt{-5})$, $\mathcal{O}_K = \mathbb{Z}[\sqrt{-5}]$

$$6 = 2.3 = (1+\sqrt{-5})(1-\sqrt{-5})$$

<u>Afirmo:</u> todos son irreducibles. (α es irreducible si cumple $\alpha = \beta.\gamma \Rightarrow \beta$ ó γ es una unidad)

<u>Demo:</u> Si $2 = \alpha.\beta$, $\underset{4}{N(2)} = N(\alpha).N(\beta)$ $N :=$ norma de $K \supset \mathbb{Q}$

$\alpha = a + b\sqrt{-5}$, $N(\alpha) = a^2 + 5b^2 \mid 4 \Rightarrow b = 0$ y

$a = \pm 1$ → α unidad

$a = \pm 2$ ⇒ $N(\beta) = 1$ ⇒ β unidad.

Si $3 = \alpha.\beta$, $N(3) = 9 = N(\alpha).N(\beta)$, $\alpha = a + b\sqrt{-5}$,

$N(\alpha) = a^2 + 5b^2 \mid 9 \Rightarrow b = 0, \pm 1$, $b = 0$, $a^2 \mid 9$ { $a = \pm 1$ ⇒ α unidad ; $a = \pm 3$ ⇒ $N(\alpha) = 9 \Rightarrow$ β unidad $\Leftarrow N(\beta) = 1$ }

Si $b = \pm 1$, $a^2 + 5 \mid 9$, $a = \pm 2$

si $\alpha = 2 \pm \sqrt{-5}$, $N(\alpha) = 9 \Rightarrow N(\beta) = 1 \Rightarrow \beta$ unidad.

Misma cuenta con $1 \pm \sqrt{-5}$.

Lo que sucede: $(2) = \langle 2, 1+\sqrt{-5} \rangle_{\mathbb{Z}}^2 = \langle 2, 1+\sqrt{-5} \rangle_{\mathbb{Z}} \cdot \langle 2, 1-\sqrt{-5} \rangle_{\mathbb{Z}}$

$$\langle 2, 1+\sqrt{-5} \rangle_{\mathbb{Z}}^2 = \langle 2, 1+\sqrt{-5} \rangle_{\mathbb{Z}} \cdot \langle 2, 1+\sqrt{-5} \rangle_{\mathbb{Z}} = \langle 4, 2+2\sqrt{-5}, -4+2\sqrt{-5} = 1+2\sqrt{-5}-5 \rangle = \langle 2\sqrt{-5}, 2 \rangle_{\mathbb{Z}} = (2)$$

$\mathfrak{a}, \mathfrak{b}$ ideales, $\mathfrak{a} \cdot \mathfrak{b} = \langle ab \mid a \in \mathfrak{a}, b \in \mathfrak{b} \rangle_{\mathbb{Z}}$

Ejercicio: ver que $\mathfrak{a} \cdot \mathfrak{b}$ es un ideal para $\mathcal{O}_K$.

Análogamente, $(3)_{\mathcal{O}_K} = \langle 3, 1+\sqrt{-5} \rangle_{\mathbb{Z}} \cdot \langle 3, 1-\sqrt{-5} \rangle_{\mathbb{Z}}$

$$(1+\sqrt{-5}) = \langle 2, 1+\sqrt{-5} \rangle_{\mathbb{Z}} \cdot \langle 3, 1+\sqrt{-5} \rangle_{\mathbb{Z}}$$

$$(1-\sqrt{-5}) = \langle 2, 1-\sqrt{-5} \rangle_{\mathbb{Z}} \cdot \langle 3, 1-\sqrt{-5} \rangle_{\mathbb{Z}}$$

$$(6) = \underbrace{\langle 2, 1+\sqrt{-5} \rangle_{\mathbb{Z}} \langle 2, 1-\sqrt{-5} \rangle_{\mathbb{Z}}}_{(2)} \underbrace{\langle 3, 1+\sqrt{-5} \rangle_{\mathbb{Z}} \langle 3, 1-\sqrt{-5} \rangle_{\mathbb{Z}}}_{(3)}$$

Veremos: $\mathcal{O}_K$ tiene factorización única $\Leftrightarrow$ todos los ideales son principales (D.I.P.)

Obs: los resultados valen en un contexto un poco más general que el que tenemos en extensiones finitas de $\mathbb{Q}$.

Def: un dominio de Dedekind es un dominio íntegro t.q.

1. Todo ideal de R es finitamente generado (Noetheriano) $\nwarrow$ si $\mathfrak{a}_1 \subset \mathfrak{a}_2 \subset \dots$ se estacionan $\mathfrak{a}_n = \mathfrak{a}_{n+j}$ $\forall j > 0$.

2. Todo ideal primo no nulo es maximal ($\Leftrightarrow \dim \operatorname{Krull} R = 1$).

3. R es integramente cerrado en su cuerpo de fracciones

$$K = \operatorname{Frac}(R) = \left\{ \frac{\alpha}{\beta} : \alpha, \beta \in R,\ \beta \neq 0 \right\} / \sim$$

$$\frac{\alpha}{\beta} \sim \frac{\gamma}{\delta} \Leftrightarrow \alpha\delta = \beta\gamma.$$

Si: $q \in K$ / $\exists p(x) \in R[x]$ mónico, $p(q) = 0 \Rightarrow q \in R$.

Ejemplo: $\mathbb{F}_p[t]$ es un dominio de Dedekind.

$\mathbb{P}^1(\mathbb{F}_p)$ recta proyectiva/afín.

① ✓

② $\mathfrak{Y} \subset \mathbb{F}_p[t]$ primo, $\mathbb{F}_p[t]/\mathfrak{Y}$ es íntegro
$(p(t))$ "
$\mathbb{F}_p[t]/(p(t))$ es finito.

Anillo íntegro finito $\Leftrightarrow$ cuerpo. ($q \in \mathbb{F}_p[t]/\mathfrak{Y}$, $q \neq 0$

$m_q: \mathbb{F}_p[t]/\mathfrak{Y} \to \mathbb{F}_p[t]/\mathfrak{Y}$ es inyectivo $\overset{\text{morfismo}}{\checkmark}$ entre dos cjtos finitos de igual cardinalidad $\Rightarrow$ sobre $\Rightarrow \exists \beta : q \cdot \beta = 1$)

Luego $\mathfrak{Y}$ es mxl.

③ Es el lema de Gauss.

Teo: el anillo de enteros de un cuerpo de números es un dominio de Dedekind.

Demo: ① Como $\mathcal{O}_K$ es un $\mathbb{Z}$-módulo libre, de rango $d = [K:\mathbb{Q}]$, si $\gamma \subset \mathcal{O}_K$ también es un $\mathbb{Z}$-módulo libre. (si $\gamma \neq 0$, $\beta \in \gamma$, si $\mathcal{O}_K = \langle \alpha_1, \dots \alpha_d \rangle_{\mathbb{Z}}$

$$\underbrace{\langle \beta\alpha_1, \dots, \beta\alpha_d \rangle_{\mathbb{Z}}}_{\text{libre de rango } d.} \subset \gamma \subset \langle \alpha_1, \dots \alpha_d \rangle_{\mathbb{Z}}$$

$\Rightarrow \gamma$ libre de rango d.)

② Primo $\Rightarrow$ mxl. $\gamma \subset \mathcal{O}_K$ no nulo, afirmo $\mathcal{O}_K/\gamma$ es finito. Luego, γ primo $\overset{\text{como antes}}{\Rightarrow}$ $\mathcal{O}_K/\gamma$ cpo $\Rightarrow \gamma$ mxl.

Afirmo: $\mathbb{Z} \subset \mathcal{O}_K$, $\gamma \cap \mathbb{Z} \neq \emptyset$.

Si $\alpha \in \gamma$, $\alpha \neq 0$, $N(\alpha) \neq 0$ $N(\alpha) \in \mathbb{Z}$. ($N(\alpha) = \prod_{\sigma: K \hookrightarrow \mathbb{C}} \sigma(\alpha)$)

entero. (entero: α; enteros: $\prod_{i=2}^{d} \sigma_i(\alpha)$)

$\alpha \Rightarrow N(\alpha) = \underbrace{\alpha}_{K} \cdot \underbrace{\prod_{i=2}^{d} \sigma_i(\alpha)}_{K}$ $\quad \{\sigma_1, \dots \sigma_d\} = \underset{\alpha}{\mathrm{Hom}}(K, \mathbb{C})$, $\sigma_1 = id$

$\frac{N(\alpha)}{\alpha} \in K$. Luego $\prod_{i=2}^{d} \sigma_i(\alpha) \in \mathcal{O}_K \Rightarrow \alpha \cdot (\underbrace{\prod_{i=2}^{d} \sigma_i(\alpha)}_{\in \mathcal{O}_K}) \in \gamma \Rightarrow N(\alpha) \in \gamma$.

$(N(\alpha)) \subset \gamma \Rightarrow |\mathcal{O}_K/\gamma| \leq |\mathcal{O}_K/N(\alpha)| = N(\alpha)^d$.

$m \in \mathbb{Z}$

$\mathcal{O}_K = \langle \alpha_1, \dots \alpha_d \rangle_{\mathbb{Z}}$, $(m) = \langle m\alpha_1, \dots m\alpha_d \rangle_{\mathbb{Z}}$

$\Rightarrow \mathcal{O}_K/(m) \simeq (\mathbb{Z}/m)^d$ ✓

③ Si $\alpha, \beta \in \mathcal{O}_K$, y $\frac{\alpha}{\beta}$ es raíz de un polinomio con coeficientes en $\mathcal{O}_K \Rightarrow \frac{\alpha}{\beta}$ es entero algebraico.

$\cdot \frac{\alpha}{\beta}$ lo deja fijo.

$\mathcal{O}_K = \langle \alpha_1, \dots, \alpha_d \rangle_{\mathbb{Z}}$ $\quad \mathcal{O}_K\left[\frac{\alpha}{\beta}\right]$ es $\mathbb{Z}$-mód. f.g.

α/β es entero algebraico y en $K \Rightarrow \alpha/\beta \in \mathcal{O}_K$. ✓

Teorema: Si R es Dedekind, todo ideal no nulo $\neq R$ se escribe de forma única como producto de ideales primos distintos a potencias.

Def: dados $\mathfrak{a}, \mathfrak{b} \subset R$, decimos que $\mathfrak{a} \mid \mathfrak{b}$ si $\exists\, \mathfrak{c} \subset R$ ideal tal que $\mathfrak{b} = \mathfrak{a}\cdot\mathfrak{c}$.

Idea: **Existencia:** $\rightsquigarrow$ Por ser Noetheriano.

↳ $\mathfrak{a} \subsetneq R$, $\exists\, \mathfrak{P}$ mxl $\mathfrak{a} \subset \mathfrak{P} \iff \mathfrak{P} \mid \mathfrak{a}$

$\Rightarrow \mathfrak{a} = \mathfrak{P}\cdot\mathfrak{a}'$ $\begin{cases} \mathfrak{a}' = R \checkmark \\ \text{↳ sigo. termina} \end{cases}$ ↳ Noetheriano ↳ norma de ideales.

Unicidad: Ley cancelativa: $\mathfrak{a}\cdot\mathfrak{b} = \mathfrak{a}\mathfrak{c}$, $\mathfrak{a} \neq 0$ $\Rightarrow \mathfrak{b} = \mathfrak{c}$.

Def: si $R = \mathcal{O}_K$, $K/\mathbb{Q}$ finita, $\mathfrak{a} \subset R$, su norma ($\mathfrak{a} \neq 0$) la definimos como $N(\mathfrak{a}) = |\mathcal{O}_K/\mathfrak{a}|$.

Antes de demostrar el Teo, veamos algunas operaciones de ideales: $\mathfrak{a}, \mathfrak{b} \subset R$ ideales,

- $\mathfrak{a}\cdot\mathfrak{b} = \langle a\cdot b : a \in \mathfrak{a},\ b \in \mathfrak{b} \rangle_R$, ideal de R
- $\mathfrak{a} \cap \mathfrak{b} \neq \emptyset$ ($0 \in \mathfrak{a} \cap \mathfrak{b}$) ideal de R.
  ideal más grande contenido en ambos ($= m.c.m(\mathfrak{a}, \mathfrak{b})$)

- $a+b = \langle a+b : a\in a,\ b\in b\rangle_R$ ideal, es el más chico que contiene a ambos ($= mcd(a,b)$)

Defi a, b son **coprimos** si $a+b = R$.

Teorema: si $a \subset R$, $\exists\ b \subset R$ t.q. $a.b$ es principal o sea $a.b = (d)_R$.

Idea: $d \in a$, no nulo, $b = \{b\in R : b.a \subset (d)\}$

$a.b \subset (d)$. **Difícil**: ver igualdad.

Lema: todo $a \subset R$ no nulo contiene un producto de ideales primos.

D/ Usar Zorn, R Noetheriano $\Rightarrow$ no hay nada que verificar.

$S = \{ a$ que no contiene un producto de ideales primos$\}$

Si $S \neq \emptyset$, por Zorn, S contiene un elemento maximal M.

M no es primo (si no contendría un producto de primos)

$\Rightarrow \exists\ x, y \in R\setminus M$ t.q. $x.y \in M$. ($M \subset R$)

$M \subsetneq M+(x)$ $\rightsquigarrow$ M max $\exists\ P_1 \dots P_r \subset M+(x)$

$M \subsetneq M+(y)$ $\exists\ Q_1 \dots Q_s \subset M+(y)$

$\Rightarrow P_1 \dots P_r . Q_1 \dots Q_s \subset (M+(x)).(M+(y))$

$= (\underbrace{M.M}_{\subset M}, \underbrace{My}_{\subset M}, \underbrace{Mx}_{\subset M}, \underbrace{x.y}_{\subset M}) \subset M$

Lo que es un absurdo $\Rightarrow S = \emptyset$ ☐

Lema 2: si $\mathfrak{a} \subsetneq R$, $K = \mathrm{Frac}(R)$, $\exists\, \gamma \in K \setminus R$ t.q. $\gamma \cdot \mathfrak{a} \subset R$.

D/ Sea $a \in \mathfrak{a}$ cualquiera (no nulo), el lema anterior dice que

$$\underline{P} \supset (a) \supset P_1 \dots P_r \quad \text{(número mínimo de tales ideales)}$$

Como $\mathfrak{a} \subsetneq R$, existe $\underline{P}$ t.q. $\mathfrak{a} \subset \underline{P}$. Como $a \in \mathfrak{a}$,

$$(a) \subset \mathfrak{a} \subset \underline{P}$$

Afirmo: $P \supset \underline{P}_i$ (alguno).

Sino, $\exists\, a_i \in \underline{P}_i \setminus P$, $a_1 \dots a_r \in (a) \subset \underline{P}$, ninguno de ellos está, Abs!.

Como primo = maximal, $\underline{P} = P_i$ (digamos $\underline{P} = P_1$)

Sea $b \in P_2 \dots P_r \setminus (a)$ (existe por ser r. mínimo) $\Rightarrow \frac{b}{a} \notin R$.

Afirmo: $\frac{b}{a} \cdot \mathfrak{a} \subset R$ ($\gamma = b/a$ sirve).

$$\mathfrak{a} \subset P_1, \quad (b) \subset P_2 \dots P_r \Rightarrow \mathfrak{a} \cdot (b) \subset P_1 \dots P_r \subset (a)$$

$$\Rightarrow \frac{\mathfrak{a} b}{a} \subset R. \qquad \blacksquare$$

Demo (Teo): $\mathfrak{b} = \{b \in R : b \cdot \mathfrak{a} \subset (a)\}$, queremos ver que $\mathfrak{a} \cdot \mathfrak{b} = (a)$. ($\mathfrak{a}\mathfrak{b} \subset (a)$).

Sea $\gamma = \frac{\mathfrak{a} \cdot \mathfrak{b}}{a} \subset R$, queremos ver la igualdad.

Si $\gamma \subsetneq R$, por el último lema, $\exists\, \gamma \in K \setminus R$ t.q. $\gamma \mathfrak{b} \subset R$ ①

$\alpha \in \mathcal{Q}$

Obs: $\boxed{b \subset \gamma} = \overline{\frac{a.b}{\alpha}} \subset R$

$\Rightarrow \gamma b \subset \gamma\gamma \subset R$, además, $\boxed{\gamma . b \subset b}$

$\gamma . \frac{a.b}{\alpha} \subset R \Rightarrow \gamma . a . b \subset (\alpha)$, si $b \in b$,

$\underline{\gamma . b . a} \subset (\alpha) \Rightarrow \gamma . b \in b$

Luego γ fija un $\mathcal{X}$-módulo finito $\Rightarrow$ es entero algebraico. Abs! $\Rightarrow$ $\gamma = R \Rightarrow ab = (\alpha)$ ∎

Corolario 1: (cancelación) si a, b, b ideales, $a \neq 0$

$$ab = a.b \Rightarrow b = b.$$

D/ Sea γ t.q. $a.\gamma = (\alpha) \Rightarrow ab\gamma = ab\gamma$

$$(a\gamma)b = (a\gamma)b$$

$$\alpha . b = (\alpha) b = (\alpha) b = \alpha . b$$ ∎

Corolario 2: si a, b ideales, $a \supset b \iff a \mid b$.

D/ ($\Leftarrow$) si $a \mid b$, $b = a.b$, $b \subset R$

$\hat{a} \Rightarrow b \subset a$ ✓

$\Rightarrow$) si $a \supset b$, sea γ / $a.\gamma = (\alpha)$

$a\gamma \supset b\gamma \Rightarrow \boxed{\frac{b\gamma}{\alpha} \subset R}$, $\alpha . b = a . \gamma . b \Rightarrow b = a \boxed{\frac{\gamma b}{\alpha}}$

(a)

$\hat{R}$ ∎