Repaso: R anillo de Dedekind:

(1) Noetheriano ($\mathfrak{a} \subset R \Leftrightarrow$ f.g.)

(2) $\dim R = 1 \Leftrightarrow$ primo $\neq 0 \Leftrightarrow$ maximal

(3) R íntegramente cerrado (K/ℓ ext. finita, $R = \mathcal{O}_K$)

Objetivo: si $\mathfrak{a} \subset R$ ideal no nulo, $\mathfrak{a} \neq R$, se factoriza de forma única como producto de primos a potencias.

Vimos: (1) si $\mathfrak{a} \subset R$, $\exists\, \mathfrak{b} \subset R$ t.f. $\mathfrak{a}\cdot\mathfrak{b} = (\alpha)$ principal, $\alpha \in \mathfrak{a}$

$\mathfrak{b} = \{ b \in R : b\cdot\mathfrak{a} \subset (a) \}$

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

Corolarios: • Vale la propiedad cancelativa: $\mathfrak{a}\cdot\mathfrak{b} = \mathfrak{a}\cdot\mathfrak{c}$ y $\mathfrak{a} \neq 0 \Rightarrow \mathfrak{b} = \mathfrak{c}$.

• si $\mathfrak{a}, \mathfrak{b} \subset R$ ideales, $\mathfrak{a} \mid \mathfrak{b} \Leftrightarrow \mathfrak{b} \subset \mathfrak{a}$.

$\Updownarrow$

$\exists\, \mathfrak{c} \subset R$ t.f. $\mathfrak{b} = \mathfrak{a}\cdot\mathfrak{c}$

Teo (Factorización única): como arriba.

Demo: Existencia: $S = \{ \mathfrak{a} \subsetneq R$ ideal no nulos que no tienen fact. en primos $\}$. ¿$S = \emptyset$?

Supongamos $S \neq \emptyset \Rightarrow$ (Zorn) $\exists\, M \in S$ mxl. $M \subsetneq R$

$\Rightarrow \exists\, P \subset R$ mxl t.f. $M \subset P \Leftrightarrow P \mid M \Leftrightarrow M = P\cdot\mathfrak{a}$

$\Rightarrow \mathfrak{a} \mid M \Rightarrow M \subsetneq \mathfrak{a} \Rightarrow \mathfrak{a}$ se factoriza $\Rightarrow M$ se factoriza

Abs!

Unicidad: Si $\mathfrak{P}_1 \dots \mathfrak{P}_r = \mathfrak{Q}_1 \dots \mathfrak{Q}_s \Rightarrow \mathfrak{P}_1 \mid \mathfrak{Q}_1 \dots \mathfrak{Q}_s \Rightarrow$

$\mathfrak{P}_1 \mid \mathfrak{Q}_1 \Rightarrow \mathfrak{Q}_1 \subset \mathfrak{P}_1$, ambos son m×l $\Rightarrow \mathfrak{Q}_1 = \mathfrak{P}_1$ cancelativa

$\rightsquigarrow$ terminar cómo en Algebra 1.

Ejercicio: Dados $\mathfrak{a}, \mathfrak{b} \subset R$ ideales,

1. $\mathfrak{a}+\mathfrak{b} = \text{m.c.d.}(\mathfrak{a},\mathfrak{b}) = \prod_{\mathfrak{P}} \mathfrak{P}^{\min\{v_{\mathfrak{P}}(\mathfrak{a}), v_{\mathfrak{P}}(\mathfrak{b})\}}$
2. $\mathfrak{a} \cap \mathfrak{b} = \text{m.c.m}(\mathfrak{a},\mathfrak{b})$.

donde $v_{\mathfrak{P}}(\mathfrak{a})$ = exponente de $\mathfrak{P}$ en la factorización de $\mathfrak{a}$.

Teo: R es Dedekind, R es DFU $\Leftrightarrow$ R es DIP.

D/ $\Leftarrow$) siempre (estructuras), $a \in R$, a no unidad, $a \neq 0$.

$(a) = \mathfrak{P}_1^{e_1} \dots \mathfrak{P}_r^{e_r}$, como R es DIP, $\mathfrak{P}_i = (\beta_i)$ (en R)

$(a) = (\beta_1^{e_1} \dots \beta_r^{e_r}) \Rightarrow a = u \cdot \beta_1^{e_1} \dots \beta_r^{e_r}$

Si $a = v \cdot \gamma_1^{t_1} \dots \gamma_s^{t_r} \rightsquigarrow (a) = (\gamma_1)^{t_1} \dots (\gamma_s)^{t_s} = \mathfrak{P}_1^{e_1} \dots \mathfrak{P}_r^{e_r}$

$\Rightarrow \boxed{r=1}$ $(\gamma_1) = \mathfrak{P}_1 = (\beta_1) \Rightarrow \gamma_1$ y β_1 son asociados.

$\Rightarrow$) Si $\mathfrak{a} \subsetneq R$ ideal, f.u.f. $\mathfrak{a}$ es principal. $\exists\, \mathfrak{b} \subset R$ t.q. $\mathfrak{a}\mathfrak{b} = (d)$;

d no cero ni unidad. Como R tiene F.U. $d = \beta_1^{e_1} \dots \beta_r^{e_r}$ (primos)

ideales primos.

$\Rightarrow a \cdot b = (\alpha) = (\beta_1)^{e_1} \cdots (\beta_r)^{e_r}$, en la factorización de a, aparecen algunos de estos primos a algunas potencias. Como todos son principales, a es principal. ∎

Obs: si R no es Dedekind, no vale. $\mathbb{R}[x,y]$ es DFU pero no es DIP $\langle x, y \rangle$

Teo (Chino del Resto): si $\mathfrak{I}_1, \dots, \mathfrak{I}_n \subset R$ ideales coprimos dos a dos,

$$\varphi : R/\bigcap_{i=1}^{n} \mathfrak{I}_i \xrightarrow{\sim} R/\mathfrak{I}_1 \times \cdots \times R/\mathfrak{I}_n$$
$$\bar{x} \longrightarrow (x, \dots, x)$$

$\bigcap_{i=1}^{n} \mathfrak{I}_i = \prod_{i=1}^{n} \mathfrak{I}_i$

Demo: basta ver el caso $n=2$. (Inducción). Claramente φ morfismo de anillos.

- $\ker(\varphi) = \{ \bar{a} : \bar{a} \text{ en } R/\mathfrak{I}_1 = 0, \ \bar{a} \text{ en } R/\mathfrak{I}_2 = 0 \} = \{0\}$
  $\bar{a} = 0 \Leftrightarrow a \in \mathfrak{I}_1$, $\bar{a} = 0 \Leftrightarrow a \in \mathfrak{I}_2 \Rightarrow a \in \mathfrak{I}_1 \cap \mathfrak{I}_2$
  $\Rightarrow \bar{a} = 0$ en $R/\mathfrak{I}_1 \cap \mathfrak{I}_2$

- Sobreyectiva: dados a_1, a_2 en R, $\exists\, \beta \in R$ tal que:

$$\begin{cases} \beta \equiv a_1 \ (\mathfrak{I}_1) \\ \beta = a_2 \ (\mathfrak{I}_2) \end{cases} \qquad \beta \longrightarrow (\bar{a}_1, \bar{a}_2) \text{ en } R/\mathfrak{I}_1 \times R/\mathfrak{I}_2$$

Como $\mathfrak{I}_1$ e $\mathfrak{I}_2$ son coprimos, $\mathrm{mcd}(\mathfrak{I}_1, \mathfrak{I}_2) = R$
$= \mathfrak{I}_1 + \mathfrak{I}_2$

Como $1 \in R$, $\exists\, a \in \mathfrak{I}_1,\ b \in \mathfrak{I}_2$ t.q. $a+b=1$ $\Rightarrow b \equiv 1 \ (\mathfrak{I}_1)$, $a \equiv 1 \ (\mathfrak{I}_2)$

$\beta = \alpha_2 a + \alpha_1 b$. $\begin{cases} \beta \equiv \alpha_1 b \equiv \alpha_1 & (\mathfrak{I}_1) \\ \beta \equiv \alpha_2 a \equiv \alpha_2 & (\mathfrak{I}_2) \end{cases}$ ✓ ∎

Cor: Si $\mathfrak{a} \subset R$ (Dedekind), $\alpha \in \mathfrak{a}$, $\alpha \neq 0$, $\exists \beta \in \mathfrak{a}$ t.q. $\mathfrak{a} = \langle \alpha, \beta \rangle_R$

D/ $\langle \alpha, \beta \rangle_R = (\alpha) + (\beta) = mcd((\alpha), (\beta))$

$\alpha \in \mathfrak{a} \Rightarrow (\alpha) \subset \mathfrak{a} \Rightarrow \mathfrak{a} \mid (\alpha)$

$$(\alpha) = \mathfrak{P}_1^{e_1} \cdots \mathfrak{P}_r^{e_r}, \quad \mathfrak{a} = \mathfrak{P}_1^{t_1} \cdots \mathfrak{P}_r^{t_r}$$

con $0 \leq t_i \leq e_i$. Si $e_i > t_i$, $\beta_i \in \mathfrak{P}_i^{t_i} \setminus \mathfrak{P}_i^{t_i+1}$ ($\mathfrak{P}_i^0 = R$)

Si $e_i = t_i$, $\beta_i \in \mathfrak{P}^{t_i} \setminus \mathfrak{P}^{t_i+1}$

Por T.C.R., $\exists\, \beta \in R$ t.q. $\beta \equiv \beta_i \ (\mathfrak{P}_i^{t_i+1})$

Luego, si $e_i > t_i$, $\beta \notin \mathfrak{P}_i^{t_i+1}$ ($\overline{\beta_i} \not\equiv 0 \ (\mathfrak{P}_i^{t_i+1})$)

$\beta \equiv \beta_i \ (\mathfrak{P}_i^{t_i+1}) \Rightarrow \beta \equiv \overline{0}$ (no) $\beta_i \ (\mathfrak{P}_i^{t_i}) \Rightarrow \beta \in \mathfrak{P}_i^{t_i}$

En definitiva, $(\beta) = \mathfrak{P}_1^{t_1} \cdots \mathfrak{P}_r^{t_r} \cdot \mathfrak{Q}_1^{a_1} \cdots \mathfrak{Q}_n^{a_n}$ (no aparecen en la factorización de (α))

$mcd((\alpha), (\beta)) = \mathfrak{P}_1^{t_1} \cdots \mathfrak{P}_r^{t_r} = \mathfrak{a}$. ∎

Norma de ideales

$R = \mathcal{O}_K$, K/ℓ ext. finita. ($R = \mathbb{F}_p[t]$)

Si $\mathfrak{a} \subset \mathcal{O}_K$ ideal no nulo, su norma es $N(\mathfrak{a}) = |\mathcal{O}_K/\mathfrak{a}|$

Teo: Si $\mathfrak{a}, \mathfrak{b} \subset \mathcal{O}_K$ ideales no nulos, $N(\mathfrak{a}\mathfrak{b}) = N(\mathfrak{a}) \cdot N(\mathfrak{b})$

Demo: (1º) Si $\mathfrak{a}, \mathfrak{b}$ coprimos ($\mathfrak{a} + \mathfrak{b} = R$)

T.C.R. $|\mathcal{O}_K/\mathfrak{a}\mathfrak{b}| \simeq |\mathcal{O}_K/\mathfrak{a}| \times |\mathcal{O}_K/\mathfrak{b}|$

$N(\mathfrak{a}\mathfrak{b}) = N(\mathfrak{a}) \cdot N(\mathfrak{b})$ ✓

(2º) Como $\mathcal{O}_K$ tiene F.U. en ideales, basta probarlo para potencias de un primo, o sea $N(\mathfrak{p}^r) = N(\mathfrak{p})^r$

$$\mathcal{O}_K \supsetneq \mathfrak{p} \supsetneq \mathfrak{p}^2 \supsetneq \dots \supsetneq \mathfrak{p}^r$$

$$N(\mathfrak{p}^r) = |\mathcal{O}_K/\mathfrak{p}^r| = |\mathcal{O}_K/\mathfrak{p}| \cdot |\mathfrak{p}/\mathfrak{p}^r| = |\mathcal{O}_K/\mathfrak{p}| \cdot \underbrace{|\mathfrak{p}/\mathfrak{p}^2|}_{N(\mathfrak{p})} \cdot \dots$$

$$N(\mathfrak{p})^r = \underbrace{|\mathfrak{p}^{r-1}/\mathfrak{p}^r|}_{N(\mathfrak{p})}$$

Basta ver que $|\mathfrak{p}^i/\mathfrak{p}^{i+1}| = |\mathcal{O}_K/\mathfrak{p}| \quad \forall i \geq 1$.

Sea $\alpha \in \mathfrak{p}^i \setminus \mathfrak{p}^{i+1}$, $\phi : \mathcal{O}_K \longrightarrow \mathfrak{p}^i/\mathfrak{p}^{i+1}$ (morfismo aditivo)

$x \longrightarrow \overline{\alpha \cdot x}$

$N_u(\phi) = \{x \in \mathcal{O}_K : x\alpha \in \mathfrak{p}^{i+1}\} \supseteq \mathfrak{p}^{i+1} \mid x\alpha$, $\mathfrak{p}^i \nmid \alpha$, $\mathfrak{p}^{i+1} \mid x\alpha$

$\mathfrak{p}$ ''

$\Rightarrow \mathfrak{p} \mid x$

$\rightsquigarrow \quad \phi : \mathcal{O}_K/\mathfrak{P} \longrightarrow \mathfrak{P}^i/\mathfrak{P}^{i+1}$

Suryectiva: dado $\beta \in \mathfrak{P}^i$, p.u.p. $\exists\, x \in \mathcal{O}_K$ t.p.

$$\overline{x.\alpha} \equiv \overline{\beta} \ (\mathfrak{P}^{i+1})$$

$\phi(x)$

$\alpha \in \mathfrak{P}^i \setminus \mathfrak{P}^{i+1} \Rightarrow \quad mcd\,((\alpha), \mathfrak{P}^{i+1}) = \mathfrak{P}^i$

$$(\alpha) + \mathfrak{P}^{i+1} = \mathfrak{P}^i$$

$$\alpha.x + \gamma = \beta \Rightarrow \alpha.x \equiv \beta\,(\mathfrak{P}^{i+1}) \quad \square$$

Si $\mathfrak{a} = (\alpha) \rightsquigarrow N(\mathfrak{a}) = N((\alpha)) \overset{?}{=} N_{K/\mathbb{Q}}(\alpha)$

Prop: $\Omega = \mathcal{O}_K$, $N((\alpha)) = |N_{K/\mathbb{Q}}(\alpha)|$

Demo: Si $\alpha \in \mathbb{Z}\ (< \mathcal{O}_K)$, $N((\alpha)) = |\mathcal{O}_K/(\alpha)| = |\alpha|^d$

$d = [K:\mathbb{Q}]$ $\qquad \mathcal{O}_K = \langle \alpha_1, \dots, \alpha_d \rangle_{\mathbb{Z}}$

$\rightsquigarrow \mathcal{O}_K/(\alpha) \simeq \mathbb{Z}/\alpha \times \dots \times \mathbb{Z}/\alpha$

$(\alpha) = \langle \alpha\alpha_1, \dots, \alpha\alpha_d \rangle_{\mathbb{Z}}$ (d factores)

$N_{K/\mathbb{Q}}(\alpha) = \alpha^d \Rightarrow N((\alpha)) = |N_{K/\mathbb{Q}}(\alpha)|$

Sea $\alpha \in \mathcal{O}_K$ cualquiera. Supongamos $K/\mathbb{Q}$ Galois.

$\{\sigma_1, \dots, \sigma_d\} = Gal(K/\mathbb{Q})$, $\sigma_i : K \longrightarrow K$

$\mathcal{O}_K \longrightarrow \mathcal{O}_K$

En particular, $\sigma_i : \mathcal{O}_K/\alpha \xrightarrow{\sim} \mathcal{O}_K/\sigma_i(\alpha)$

$\Rightarrow$ $N(\alpha) = N(\sigma_i(\alpha))$. $|\mathcal{O}_K/(\alpha)|$

$N(\alpha)^d = |\mathcal{O}_K/(\alpha)|^d = \prod_{i=1}^{d} |\mathcal{O}_K/(\sigma_i(\alpha))| = \prod_{i=1}^{d} N(\sigma_i(\alpha))$

$= N\left(\prod_{i=1}^{d}(\sigma_i(\alpha))\right) = N\left(\left(\prod_{i=1}^{d}\sigma_i(\alpha)\right)\right) = N(N_{K/\mathbb{Q}}(\alpha))$

$= |N_{K/\mathbb{Q}}(\alpha)|^d \Rightarrow N(\alpha) = |N_{K/\mathbb{Q}}(\alpha)|$.

Si $K/\mathbb{Q}$ no es Galois:

Galois $\begin{cases} L & \leftarrow \text{cpo de desc. de } m_\alpha(X). \\ | & t \\ K = \mathbb{Q}[\alpha] & \\ | & d \\ \mathbb{Q} & \end{cases}$ lo veremos la próxima

$|N_{L/\mathbb{Q}}(\alpha)| = N((\alpha)\mathcal{O}_L) = N((\alpha))^t$

$|N_{K/\mathbb{Q}}(N_{L/K}(\alpha))| = |N_{K/\mathbb{Q}}(\alpha^t)| = |N_{K/\mathbb{Q}}(\alpha)|^t$ ∎

Ejercicio: Dado $\alpha \in \mathcal{O}_K$, $m_\alpha : \mathcal{O}_K \to \mathcal{O}_K$, $x \to \alpha \cdot x$

(1°) $(\alpha) = \gamma_m(m_\alpha)$

(2°) $\mathcal{B}$ base de $\mathcal{O}_K$, $[m_\alpha]_{\mathcal{B}}$, $\det [m_\alpha]_{\mathcal{B}} =$ índice de $\mathcal{O}_K/(\alpha)$ (sup. Forma Normal de Smith).

$\mathcal{B}_1 \subset L_1 \subset L_2 \supset \mathcal{B}_2$ $\quad A \in G_{\mathcal{B}_1,\mathcal{B}_2}$ $\mathcal{B} = \begin{pmatrix} d_1 & & \\ & \ddots & \\ & & d_r \end{pmatrix}$ $d_i | d_{i+1}$

$\Rightarrow |\det(G_{\mathcal{B}_1,\mathcal{B}_2})| = |d_1 \cdots d_r|$

en las bases $A\mathcal{B}_1$, $\mathcal{B}^{-1}\mathcal{B}_2$, $G_{A\mathcal{B}_1, \mathcal{B}^{-1}\mathcal{B}_2} = \begin{pmatrix} d_1 & & \\ & \ddots & \\ & & d_r \end{pmatrix}$

$A\mathcal{B}_1 = \langle v_1, \dots, v_n \rangle$, $B^{-1}\mathcal{B}_2 = \langle \frac{v_1}{d_1}, \dots, \frac{v_n}{d_n} \rangle$

$\Rightarrow \boxed{|L_1/L_2| = |\mathbb{Z}/d_1| \times \cdots \times |\mathbb{Z}/d_n| = |d_1 \cdots d_n| = |\det(C_{\mathcal{B}_1,\mathcal{B}_2})|}$

Luego $|\det(m_\alpha)| = |N_{K/\mathbb{Q}}(\alpha)| = |\mathcal{O}_K/(\alpha)| = N((\alpha))$

$\mathcal{B}$ base de $\mathcal{O}_K$ como $\mathbb{Z}$-módulo es base de K como $\mathbb{Q}$-e.v. ∎