31/08/20 K $\mathcal{O}_K = \{\alpha \in K \mid \alpha \text{ enteros} / \mathbb{Z}\} = \{\alpha \in K \mid f_{\mathbb{Q}}^{\alpha} \in \mathbb{Z}[x]\}$

$K \mid < \infty$ $\rightsquigarrow$ anillo de enteros

$\mathbb{Q}$

Lema $\forall\, \alpha \in K \;\; \exists N \in \mathbb{Z},\, N \neq 0$ t.q. $N \cdot \alpha \in \mathcal{O}_K$.

Dem $\alpha \in K \Rightarrow a_n \alpha^n + a_{n-1}\alpha^{n-1} + \cdots + a_1 \alpha + a_0 = 0.$

$a_n \neq 0,\; a_i \in \mathbb{Z}$,

multiplicar por a_n^{n-1}:

$$(a_n\alpha)^n + a_{n-1}\cdot (a_n\alpha)^{n-1} + \cdots + a_1 a_n^{n-2}(a_n\alpha) + a_1 a_n^{n-1} = 0$$

$\Rightarrow a_n \alpha \in \mathcal{O}_K$ $\square$

Proposición $\operatorname{Frac} \mathcal{O}_K = K$.

Dem $\mathcal{O}_K \subset K \Rightarrow \operatorname{Frac} \mathcal{O}_K \subseteq K$

Lema $\Rightarrow \exists N \neq 0$ t.q. $N\alpha \in \mathcal{O}_K \Rightarrow \alpha = \frac{1}{N}\cdot N\alpha \in \operatorname{Frac}\mathcal{O}_K$. $\square$

Proposición $\mathcal{O}_K$ es integralmente cerrado. $\Leftrightarrow$

Si $\alpha \in K$ es entero $/ \mathcal{O}_K \Rightarrow \alpha \in \mathcal{O}_K$.

Dem 1) $\alpha \in K$ es entero $/\mathcal{O}_K \Rightarrow$

$\alpha^n + a_{n-1}\alpha^{n-1} + \cdots + a_1\alpha + a_0 = 0$ $\quad a_i \in \mathcal{O}_K$.

$\Rightarrow R[\alpha]$ es un R-módulo f.g., donde $R = \mathbb{Z}[a_0, \dots, a_{n-1}]$

2) Los a_i son enteros $/\mathbb{Z} \Rightarrow R$ es un $\mathbb{Z}$-módulo f.g.

1) & 2) $\Rightarrow R[\alpha]$ es un $\mathbb{Z}$-módulo f.g.

$\Rightarrow \alpha$ entero$/\mathbb{Z} \Rightarrow \alpha \in \mathcal{O}_K$. $\square$

Ejemplo $K = \mathbb{Q} \Rightarrow \mathcal{O}_K = \mathbb{Z}$

Ejemplo $K = \mathbb{Q}(\sqrt{d})$ (d libre de cuadrados)

$\alpha \in K \setminus \mathbb{Q} \Rightarrow$ pol. mínimo es

$\alpha = a + b\sqrt{d}$ $\quad (x - (a+b\sqrt{d}))(x + (a + b\sqrt{d})) = x^2 - 2ax + a^2 - db^2$

$\alpha \in \mathcal{O}_K \Leftrightarrow \begin{cases} 2a \in \mathbb{Z} \\ a^2 - db^2 \in \mathbb{Z} \end{cases} \Rightarrow a = \frac{a'}{2},\; a' \in \mathbb{Z}$

$b = \frac{b'}{2},\; b' \in \mathbb{Z}$

$a^2 - db^2 \in \mathbb{Z} \Leftrightarrow a'^2 - db'^2 \equiv 0 \; (4)$

•) $d \equiv 1\ (4)$

$$\mathcal{O}_K = \left\{ \frac{a'}{2} + \frac{b'}{2}\sqrt{d} \;\middle|\; \begin{array}{c} a', b' \in \mathbb{Z} \\ a' \equiv b'\ (2) \end{array} \right\} = \mathbb{Z}\left[\frac{1+\sqrt{d}}{2}\right]$$

•) $d \equiv 2,3\ (4) \Rightarrow a' \equiv b' \equiv 0\ (2)$

$$\mathcal{O}_K = \{ a + b\sqrt{d} \mid a, b \in \mathbb{Z} \} = \mathbb{Z}[\sqrt{d}] \qquad \square$$

Si $K = \mathbb{Q}(\alpha)$, α - entero algebraico.

$\mathcal{O}_K$ puede ser más grande $\mathbb{Z}[\alpha]$

Ejemplo $K = \mathbb{Q}(\zeta_n) \Rightarrow \mathbb{Z}[\zeta_n] = \mathcal{O}_K$.

Para $n = p$ primo: mis apuntes.

En todos los ejemplos:

$$\mathcal{O}_K = \mathbb{Z}[\alpha] = \mathbb{Z} \oplus \alpha\mathbb{Z} \oplus \cdots \oplus \alpha^{n-1}\mathbb{Z}, \quad \text{para } \alpha \in \mathcal{O}_K.$$

Esto normalmente no sucede.

Ejemplo (Dedekind) Para $K = \mathbb{Q}[x] / (x^3 - x^2 - 2x - 8)$

$\mathcal{O}_K$ no es de la forma $\mathbb{Z}[\alpha]$

§ Dominios de Dedekind

$K \,|\, {<}\infty \,\mathbb{Q} \rightsquigarrow \mathcal{O}_K \subset K$

$\uparrow$ un dominio de Dedekind.

def R es un **dominio de Dedekind**:

a) R es noetheriano

b) $\dim R = 1$. (todo primo no nulo es maximal)

c) R es integralmente cerrado.

Objetivo: $I = \mathfrak{p}_1^{e_1} \cdots \mathfrak{p}_s^{e_s}$.

Hasta el final de clase: R - d. de Dedekind.

$K = \operatorname{Frac} R$.

Lema 1 Todo $I \subset R$, $I \neq 0$ contiene un producto de ideales primos.

Dem Supongamos que es falso. Sea I un ideal $\neq 0$ que es maximal respecto a la propiedad de no contener un producto de primos no nulos.

El mismo I no es primo $\Rightarrow \exists\, \alpha, \beta \in R$ t.q.

$\alpha\beta \in I$, $\alpha, \beta \notin I$.

$$I \subsetneq I + \alpha R \qquad I \subsetneq I + \beta R.$$

Por la maximalidad de I. $\Rightarrow$

$$\mathfrak{p}_1 \cdots \mathfrak{p}_s \subseteq I + \alpha R. \qquad \mathfrak{q}_1 \cdots \mathfrak{q}_t \subseteq I + \beta R.$$

$$\mathfrak{p}_1 \cdots \mathfrak{p}_s \mathfrak{q}_1 \cdots \mathfrak{q}_t \subseteq (I+\alpha R)(I+\beta R) = I^2 + \alpha I + \beta I + \alpha\beta R.$$
$$\subseteq I. \quad \text{Contradicción} \quad \square$$

<u>Lema 2</u> a) Para $I \subset K$, $I \neq 0$ se tiene

$$(I:I) \overset{\text{def}}{=} \{\alpha \in K \mid \alpha I \subseteq I\} = R.$$

b) Para $0 \neq I \subsetneq R$ se tiene $R \subsetneq I^{-1}$

<u>Dem</u> $R \subseteq (I:I)$. por la dfn.

si $\alpha \in K$ cumple $\alpha I \subseteq \underset{\uparrow\, R\text{-mód. f.g.}}{I} \Rightarrow \alpha$ es entero$/R$.

$\Rightarrow \alpha \in R$. (pq. R es integralmente cerrado).

b) Recordemos que $I^{-1} = \{\alpha \in K \mid \alpha I \subseteq R\}$.

Si $\alpha \in I$, $\alpha \neq 0$.

Lema anterior $\Rightarrow \mathfrak{p}_1 \cdots \mathfrak{p}_s \subseteq \alpha R \subseteq I \subsetneq R$.

Sea s el mínimo posible t.q. αR contiene un producto de s ideales primos no nulos.

Sea $\mathfrak{p}$ un ideal maximal t.q. $I \subseteq \mathfrak{p}$.

$$\underset{\text{maximal}}{\mathfrak{p}_1 \cdots \mathfrak{p}_s} \subseteq \underset{\uparrow\,\text{primo.}}{\mathfrak{p}} \Rightarrow \mathfrak{p} = \mathfrak{p}_i \text{ para algún } i$$

(s.p.d.g. $i = 1$)

$\boxed{s=1}$ $\underbrace{\mathfrak{p}_1 \subseteq \alpha R \subseteq I \subseteq \mathfrak{p}}_{=}$ $\qquad I^{-1} = \alpha^{-1} R \supsetneq R.$

$(\alpha^{-1} \notin R)$

$\boxed{s>1}$ Minimalidad de s:

$$\mathfrak{p}_2 \cdots \mathfrak{p}_s \not\subseteq \alpha R.$$

Tomemos $\beta \in \mathfrak{p}_2 \cdots \mathfrak{p}_s \setminus \alpha R$.

$$\alpha^{-1}\beta \notin R.$$

$$\alpha^{-1}\beta I \subseteq \alpha^{-1}\beta \mathfrak{p} \subseteq \alpha^{-1}\mathfrak{p}_1\mathfrak{p}_2\cdots\mathfrak{p}_s \subseteq \alpha^{-1}(\alpha R) = R$$

$$\Rightarrow \alpha^{-1}\beta \in I^{-1}. \qquad \square$$

Lema 3 Todo ideal $I \subset K$ no nulo es invertible.

Dem Hay que ver que $I I^{-1} = R$.

Por la def. de I^{-1}, $I I^{-1} \subseteq R$.

$$(I I^{-1})(I I^{-1})^{-1} \subseteq R \Rightarrow$$

$$I^{-1}(I I^{-1})^{-1} \subseteq I^{-1} \Rightarrow$$

$$(I I^{-1})^{-1} \subseteq (I^{-1} : I^{-1}) = R.$$

(parte a) del lema)

Por la parte 3) del lema

$$I I^{-1} \subsetneq R \Rightarrow R \subsetneq (I I^{-1})^{-1},$$ pero no es el caso

$$\Rightarrow I I^{-1} = R. \qquad \square$$

Teorema Todo $0 \neq I \subsetneq R$ puede ser escrito como un producto de ideales primos:

$$I = \mathfrak{p}_1 \cdots \mathfrak{p}_s,$$ y esta expr. es única.

Dem **Existencia**: Supongamos que existen ideales que no admiten factorización en ideales primos.

Sea I un ideal maximal resp. a esta propiedad.

I no es primo $\Rightarrow \exists$ ideal maximal $\mathfrak{p}$ t.q.

$$I \subsetneq \mathfrak{p}.$$

$I = \mathfrak{p} J$, donde $J = \mathfrak{p}^{-1} I$. (usando invertibilidad).

$J \subsetneq \mathfrak{p}^{-1}\mathfrak{p} \subseteq R. \Rightarrow J$ es integral

$$I \subsetneq J \Rightarrow J = \mathfrak{p}_1 \cdots \mathfrak{p}_s \Rightarrow I = \mathfrak{p}\mathfrak{p}_1 \cdots \mathfrak{p}_s.$$

Contradicción.

Unicidad Si $I = \mathfrak{p}_1 \cdots \mathfrak{p}_s = \mathfrak{q}_1 \cdots \mathfrak{q}_t$.

$\Longrightarrow$ usando la primalidad / maximalidad,

s.p.d.g. $\mathfrak{p}_s = \mathfrak{q}_t \Longrightarrow \mathfrak{p}_1 \cdots \mathfrak{p}_{s-1} = \mathfrak{q}_1 \cdots \mathfrak{q}_{t-1}$.

$\Longrightarrow$ el paso inductivo. $\square$

Entonces, $0 \neq I \subsetneq R$ $\quad I = \prod_{\mathfrak{p}} \mathfrak{p}^{v_{\mathfrak{p}}(I)}$, $\left(v_{\mathfrak{p}} = 0, \text{ salvo un \# finito} \right)$

donde el producto es sobre $0 \neq \mathfrak{p} \subset R$ primos y $v_{\mathfrak{p}}(I)$ está definido de modo único.

Generalizando a los ideales, $I \subset K$,

$\exists\ \alpha \in K^{\times}$ t.q. $\alpha I \subseteq R$

$$\alpha I = \prod \mathfrak{p}^{v_{\mathfrak{p}}(\alpha I)}$$

$$I = \prod_{\mathfrak{p}} \mathfrak{p}^{v_{\mathfrak{p}}(I)}, \quad \text{donde } v_{\mathfrak{p}}(I) \in \mathbb{Z}.$$

Proposición (usando factorización única).

En un Dominio de Dedekind R, para $I \subset R$, y $\alpha \in I$, $\alpha \neq 0$. existe $\beta \in I$ t.q. $I = (\alpha, \beta)$.

En particular, todo ideal puede ser generado por dos elementos.

Dem: en mis apuntes.

Teorema Para un dominio de Dedekind, las siguientes condiciones son equivalentes:

1) $\mathrm{Pic}(R) = 0$.

2) R es un DIP.

3) R es un DFU.

Dem $\mathrm{Pic}(R) = \dfrac{I(R)}{P(R)} = \dfrac{\text{ideales frac. } \cancel{\text{invertibles}}\ \neq 0}{\text{ideales frac. principales}}$

los ideales frac. son principales $\Longleftrightarrow$ los ideales enteros $I \subset R$ son principales.

1) $\Leftrightarrow$ 2)

2) $\Rightarrow$ 3) : lo vimos al inicio del curso.

3) $\Rightarrow$ 2) ocupando $\dim R = 1$.

$I = \mathfrak{p}_1 \cdots \mathfrak{p}_s$ $\Rightarrow$ basta probar que todo ideal primo es principal.

Para $\mathfrak{p} \neq 0$, tomemos $\alpha \in \mathfrak{p}$, $\alpha \neq 0$.

$\alpha = \pi_1 \cdots \pi_s$, donde π_i — elementos primos.

$\Rightarrow$ $\alpha R = \mathfrak{p}_1 \cdots \mathfrak{p}_s$, donde $\mathfrak{p}_i = \pi_i R$. ideales primos.

$\mathfrak{p}_1 \cdots \mathfrak{p}_s \subseteq \mathfrak{p}$ $\Rightarrow$ $\mathfrak{p} = \pi_i R$. es principal.

$\square$

Definición Para un campo de números $K/\mathbb{Q}$, el grupo de clases es

$$Cl(K) := \operatorname{Pic}(\mathcal{O}_K).$$

Más adelante: $Cl(K)$ es siempre finito. y veremos cómo calcularlo.