26/08/20 $\quad 0 \neq I \subset R \subset K \Rightarrow \#(R/I) < \infty$

$\qquad\qquad\qquad\qquad\quad\ |{<}\infty$

$\qquad\qquad\qquad\qquad\quad\ \mathbb{Q}$

Corolario 1 $\quad R$ es noetheriano.

Dem $\quad I \subsetneq J \rightsquigarrow R/I \twoheadrightarrow R/J \Rightarrow \#(R/J) < \#(R/I)$

No puede haber $\underset{\substack{\neq\\(0)}}{I_0} \subsetneq I_1 \subsetneq I_2 \subsetneq \cdots$ $\square$

Corolario 2 $\quad$ Todo primo no nulo $\mathfrak{p} \subset R$ es maximal

Dem $\quad R/\mathfrak{p}$ dominio finito $\Rightarrow$ campo. $\square$

Corolario 3 $\quad$ Para primos no nulos $\mathfrak{p} \subseteq \mathfrak{q} \Rightarrow \mathfrak{p} = \mathfrak{q}$ $\square$

def Dimensión de Krull

$\dim R = \sup\{ n \mid \exists$ cadena de ideales primos $\mathfrak{p}_0 \subsetneq \mathfrak{p}_1 \subsetneq \cdots \subsetneq \mathfrak{p}_n \subset R \}$

Ejemplos

- $\dim k = 0$.
- $\dim \mathbb{Z} = 1 \qquad (0) \subsetneq (p)$
- $\dim k[x_1,\dots,x_n] = n \qquad (0) \subsetneq (x_1) \subsetneq (x_1,x_2) \subsetneq \cdots \subsetneq (x_1,\dots,x_n)$
- $\dim \mathbb{Z}[x] = 2 \qquad (0) \subsetneq (x) \subsetneq (2,x)$
- Si R es un anillo de números $\qquad (0) \subsetneq \mathfrak{p}$

  $\dim R = 1$ (ó 0)

R anillo de números

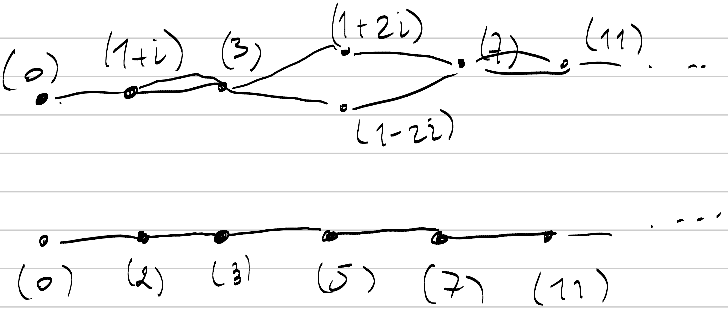
$$\begin{tikzcd} \mathfrak{p} \subset R \arrow[r, two heads] \arrow[d, dash] & R/\mathfrak{p} \simeq \mathbb{F}_{p^f} \arrow[d, dash] \\ (p) = \mathfrak{p} \cap \mathbb{Z} \subset \mathbb{Z} \arrow[r, two heads] & \mathbb{F}_p \end{tikzcd}$$

$\mathbb{F}_{p^f}$: campo residual de $\mathfrak{p}$

Ejemplo $\quad R = \mathbb{Z}[i]$.

- $2\mathbb{Z}[i] = \mathfrak{p}^2 \qquad \mathfrak{p} = (1+i). \qquad f = 1.$
- $p \equiv 1 \ (4) \Rightarrow p\mathbb{Z}[i] = \mathfrak{p}\,\overline{\mathfrak{p}} \qquad f_{\mathfrak{p}} = f_{\overline{\mathfrak{p}}} = 1$
- $p \equiv 3 \ (4) \Rightarrow p\mathbb{Z}[i]$ es primo $\qquad f = 2.$

$$\begin{array}{ccc} \mathfrak{p} & \in & \operatorname{Spec} \mathbb{Z}[i] \\ \downarrow & & \downarrow \\ \mathfrak{p} \cap \mathbb{Z} & \in & \operatorname{Spec} \mathbb{Z} \end{array}$$



§ Ideales fraccionarios Cómo invertir los ideales?

$I = 2\mathbb{Z}$ $I^{-1} = \frac{1}{2}\mathbb{Z}$

def R-dominio, $K = \operatorname{frac} R$.

$I \subseteq K$ es un ideal fraccionario si •) R-submódulo

•) $\exists\, \alpha \in K^\times$ tq $\alpha \cdot I \subseteq R$.

•) I es principal si αR, $\alpha \in K^\times$.

•) Si $I \subseteq R$, se dice que I es integral

Ejemplo $R = \mathbb{Z} \Rightarrow K = \mathbb{Q}$.

$\underset{\text{subgr.}}{\alpha I \subseteq \mathbb{Z}} \Rightarrow \alpha I = n\mathbb{Z} \Rightarrow I = \alpha^{-1} n \mathbb{Z}$.

Conclusión: Los ideales frac. para $\mathbb{Z}$ son $\frac{a}{b}\mathbb{Z}$ para $\frac{a}{b} \in \mathbb{Q}$.

(Similar para DIP).

$\mathbb{Z}[\frac{1}{2}] \subset \mathbb{Q}$ no es un ideal frac.

Ejercicio $I+J$, $I \cdot J$, $I \cap J$ se extienden a los ideales fraccionario.

def $I \subset K$ es invertible si $\exists\, J \subset K$ t.q $IJ = R$.

Note Si I es invertible, entonces

$I^{-1} = \{\alpha \in K \mid \alpha I \subseteq R\}$

I invertible $\Longleftrightarrow I \cdot I^{-1} = R$.

$I I^{-1} \subseteq R$.

Si $IJ = R \Rightarrow$

$J \subseteq I^{-1}$, además

$I^{-1} = I^{-1}(IJ) =$

$= (I^{-1} I) J \subseteq RJ \subseteq J$

Ejemplo $(\alpha R)^{-1} = \alpha^{-1}R$. todos los ideales (frac.) principales son invertibles.

Ejemplo $\mathfrak{p} = (2, 1+\sqrt{-3}) \subset \mathbb{Z}[\sqrt{-3}]$.

$\mathbb{Z}[\sqrt{-3}]/\mathfrak{p} \simeq \mathbb{F}_2$, el ideal es maximal.

$$\mathfrak{p}^{-1} = \left\{ \alpha \in \mathbb{Q}(\sqrt{-3}) \;\middle|\; \begin{array}{l} 2\alpha \in \mathbb{Z}[\sqrt{-3}] \\ (1+\sqrt{-3})\alpha \in \mathbb{Z}[\sqrt{-3}] \end{array} \right\} = \left\{ \frac{a}{2} + \frac{b}{2}\sqrt{-3} \;\middle|\; \begin{array}{l} a,b \in \mathbb{Z} \\ a \equiv b \ (2) \end{array} \right\}$$

$$= \mathbb{Z}\left[\frac{1+\sqrt{-3}}{2}\right]$$

$$2\alpha \in \mathbb{Z}[\sqrt{-3}] \iff \frac{a}{2} + \frac{b}{2}\sqrt{-3}, \quad a,b \in \mathbb{Z}$$

$$(1+\sqrt{-3})\left(\frac{a}{2} + \frac{b}{2}\sqrt{-3}\right) \in \mathbb{Z}[\sqrt{-3}]$$

$$\| $$

$$\frac{a-3b}{2} + \frac{a+b}{2}\sqrt{-3} \implies a \equiv b \ (2)$$

$$\mathfrak{p}\,\mathfrak{p}^{-1} = \mathfrak{p} \cdot \mathbb{Z}\left[\frac{1+\sqrt{-3}}{2}\right] = (2, 1+\sqrt{-3})\left(1, \frac{1+\sqrt{-3}}{2}\right)$$

$$= \Big(2, 1+\sqrt{-3}, \underbrace{\frac{(1+\sqrt{-3})^2}{2}}_{= -1+\sqrt{-3}}\Big) = \mathfrak{p} \neq R.$$

Conclusión: $\mathfrak{p}$ no es invertible en $\mathbb{Z}[\sqrt{-3}]$.

Sin embargo, en $\underbrace{\mathbb{Z}\left[\frac{1+\sqrt{-3}}{2}\right]}_{= \mathbb{Z}[\zeta_3]}$ $\quad \mathfrak{p} = (2, 1+\sqrt{-3})$
$= (2)$ es principal.
$\implies$ invertible $\square$

Def Para un dominio R, el **grupo de Picard**:

$$\mathrm{Pic}(R) = \frac{I(R)}{P(R)} = \frac{\text{ideales frac. invertibles}}{\text{ideales frac. principales}}.$$

Sucesión exacta.

$$1 \to R^\times \to K^\times \to I(R) \to \mathrm{Pic}(R) \to 0$$
$$\alpha \longmapsto \alpha R$$

Ejemplo Si R es un DIP $\Rightarrow$ $I(R) = P(R)$
$\Rightarrow$ $\mathrm{Pic}(R) = 0$.

Más adelante:

$$\begin{matrix} R & \subset & K \\ |{<\infty} & & |{<\infty} \\ \mathbb{Z} & \subset & \mathbb{Q} \end{matrix} \Rightarrow \# \mathrm{Pic}(R) < \infty$$
finitud, cálculos.

Ejemplo $R = \mathbb{Z}[\sqrt{-5}]$.

$\mathfrak{p} = (2, 1+\sqrt{-5})$ no principal. $R/\mathfrak{p} \simeq \mathbb{F}_2$.

$$\mathfrak{p}^2 = (2^2, 2\cdot(1+\sqrt{-5}), \underset{\substack{\| \\ -4+2\sqrt{-5}}}{(1+\sqrt{-5})^2}) = 2R\cdot\underbrace{(2, 1+\sqrt{-5}, -2+\sqrt{-5})}_{=R}$$
$$= 2R.$$

$$\mathfrak{p}^{-1} = \frac{1}{2}\mathfrak{p} = \left(1, \frac{1+\sqrt{-5}}{2}\right)$$

$\mathfrak{p}$ no es principal: si $\mathfrak{p} = (\alpha) \Rightarrow \alpha^2 \sim 2$
pero 2 es irreducible!

$[\mathfrak{p}] \in \mathrm{Pic}(\mathbb{Z}[\sqrt{-5}])$ – elemento no trivial

$[\mathfrak{p}]^2 = [R]$ – trivial

De hecho, $\mathrm{Pic}(\mathbb{Z}[\sqrt{-5}]) = \{[R], [\mathfrak{p}]\}$
$\simeq \mathbb{Z}/2\mathbb{Z}$.

Cómo funciona: $\mathfrak{q} = (3, 1+\sqrt{-5})$ – no principal.

$\mathfrak{q}\bar{\mathfrak{q}} = 3R$, $R/\mathfrak{q} \simeq \mathbb{F}_3$.

$[\mathfrak{q}] = [\mathfrak{p}]$ en $\mathrm{Pic}(R)$.

$$\left(\frac{-1-\sqrt{-5}}{3}\right)\cdot \mathfrak{q} = \mathfrak{p} \qquad \text{—} \quad \square$$

Ejemplo diofántico $y^2 = x^3 - 5$. $x, y \in \mathbb{Z}$

$x^3 = (y - \sqrt{-5})(y + \sqrt{-5})$ en $\mathbb{Z}[\sqrt{-5}]$ ← no es un DFU.

1) $y \neq 0$ y par. (reducir mód 4)

$\underset{\text{ejercicio}}{\Rightarrow}$ $(y - \sqrt{-5}) + (y + \sqrt{-5}) = \mathbb{Z}[\sqrt{-5}]$

2) $(y + \sqrt{-5}) = I^3$ $[I]^3 = [R]$ en $Pic(R) \cong \mathbb{Z}/2\mathbb{Z}$

$\Rightarrow [I] = [R]$
(I es principal)

$I = (a + b\sqrt{-5}) \Rightarrow$

$y + \sqrt{-5} = (a + b\sqrt{-5})^3 = a(a^2 - 15b^2) + b(3a^2 - 5b^2)\sqrt{-5}$

No tiene sol. $a, b \in \mathbb{Z} \Rightarrow y^2 = x^3 - 5$ no tiene sol. $x, y \in \mathbb{Z}$.

$\square$

§ Anillo de enteros $\mathcal{O}_K$

Idea: aritmética de $\alpha \in R$ $\rightsquigarrow$ aritmética de $I \subset R$

Nos gustaría tener el "teorema fundamental de la aritmética" para ideales.

$I = p_1^{e_1} \cdots p_s^{e_s}$ p_i primos.
($I \neq 0, I \neq R$)

Ejemplo $p = (2, 1 + \sqrt{-3}) \subset \mathbb{Z}[\sqrt{-3}]$.

$p^2 = (2^2, 2(1 + \sqrt{-3}), (1 + \sqrt{-3})^2) =$

$= 2R \cdot \underbrace{(2, 1 + \sqrt{-3}, -1 + \sqrt{-3})}_{= p} = 2R \cdot p$.

factorización única $\left.\right\}$ $\Rightarrow$ $\mathfrak{p} = 2R$
invertibilidad de $\mathfrak{p}$

$$R \supset \mathfrak{p} \supsetneq \underbrace{2R}_{} \supsetneq \mathfrak{p}^2 \supset \mathfrak{p}^3 \supset \mathfrak{p}^4 \supset \dots$$

Cómo factorizar $2R$ en ideales primos?

$2R = \mathfrak{p}_1^{e_1} \dots \mathfrak{p}_s^{e_s}$, $\quad \mathfrak{p}_i$ primos.

$\mathfrak{p}^2 \subseteq 2R \subseteq \mathfrak{p}_i$ $\quad \mathfrak{p}_i$ primo $\Rightarrow$ $\mathfrak{p} \subseteq \mathfrak{p}_i$

$\mathfrak{p}$ maximal $\Rightarrow$ $\mathfrak{p} = \mathfrak{p}_i$

$2R = \mathfrak{p}^n$ — imposible

$2R$ no admite factorización en ideales primos.

$\mathfrak{p}$ no es invertible en $\mathbb{Z}[\sqrt{-3}]$.

Prop Supongamos que en un anillo de números R todo $I \subset R$ (propio no nulo) es un producto de ideales primos. Entonces todo ideal frac. en R debe ser invertible.

Dem Bajo la hipótesis, bastaría ver que todos $\mathfrak{p} \subset R$ primos no nulos son invertibles.

$\alpha \in \mathfrak{p}$, $\alpha \neq 0$. $\quad \alpha R = \mathfrak{p}_1^{e_1} \cdots \mathfrak{p}_s^{e_s}$.

$\mathfrak{p}_i$ son invertibles. $\quad \mathfrak{p}_i^{-1} = \alpha^{-1} R \cdot \mathfrak{p}_1^{e_1} \cdots \mathfrak{p}_i^{e_i - 1} \cdots \mathfrak{p}_s^{e_s}$

$\underbrace{\mathfrak{p}_1^{e_1} \dots \mathfrak{p}_s^{e_s}}_{\text{maximales}} = \alpha R \subseteq \underbrace{\mathfrak{p}}_{\text{primo}}$ $\Rightarrow$ $\mathfrak{p} = \mathfrak{p}_i$.

invertible. $\square$

Ejemplo $\mathbb{Z}[\sqrt{-3}] \subset \mathbb{Q}(\sqrt{-3})$

$\alpha = \frac{1+\sqrt{-3}}{2}$ — entero algebraico $\quad \underline{\alpha^2 - \alpha + 1 = 0}$.

$I = (1, \alpha)$ — ideal frac.

$I^2 = (1, \alpha, \alpha^2) = I$. $\quad$ Si I invertible $\Rightarrow$

$I^2 = I \Rightarrow I = R$

Pero, $\alpha \in I \setminus R$. $\square$

Prop. Si en R todo ideal frac. es invertible $\Rightarrow$ para todo $\alpha \in \mathrm{Frac}(R)$ t.q.

$$\alpha^n + a_{n-1}\alpha^{n-1} + \dots + a_1\alpha + a_0 = 0$$

$(a_i \in R)$

tenemos $\alpha \in R$.

Dem. Tomamos $I = (1, \alpha, \alpha^2, \dots, \alpha^{n-1})$

$I^2 = I \Rightarrow I = R$, en particular, $\alpha \in R$. $\square$

Def R - dominio. $K = \mathrm{Frac}\, R$

$\alpha \in K$ es entero sobre R si

$$\alpha^n + a_{n-1}\alpha^{n-1} + \dots + a_1\alpha + a_0 = 0. \quad a_i \in R$$

Si $\forall\, \alpha \in K$ entero$/R$ $\alpha \in R \Rightarrow$ se dice que R es integralmente ~~enteramente~~ cerrado (integrally closed)

Ejempl $\frac{1+\sqrt{-3}}{2} \notin \mathbb{Z}[\sqrt{-3}]$

Lema Las siguientes condiciones son equivalentes:

1) $\alpha \in K$ es entero $/R$

2) $R[\alpha] \subset K$ es un R-mód f.g.

3) $\exists$ R-mód f.g. $M \subset K$ t.q. $\alpha M = M$.

Dem 1) $\Rightarrow$ 2) $\alpha^n + a_{n-1}\alpha^{n-1} + \dots + a_1\alpha + a_0 = 0$.

$\Rightarrow 1, \alpha, \dots, \alpha^{n-1}$ generan a $R[\alpha]$ como R-módulo.

2) $\Rightarrow$ 3) $M = R[\alpha]$.

3) $\Rightarrow$ 1) $\quad M = \alpha_1 R + \cdots + \alpha_n R.$

Multiplicación por α: $A: M \longrightarrow M$

$$x \longmapsto \alpha x.$$

$$\alpha \alpha_i = \sum_j a_{ij} \alpha_j \Rightarrow A = (a_{ij})$$

Teorema de Cayley-Hamilton:

$$\det(\alpha I_n - A) = 0.$$

pol. mónico con coef. en R. $\square$

Proposición - definición Dado un cuerpo de números $K/\mathbb{Q}$, el anillo de enteros:

$$\mathcal{O}_K = \{\alpha \in K \mid \alpha \text{ entero } / \mathbb{Z}\}$$

$$= \{\alpha \in K \mid f_{\mathbb{Q}}^{\alpha} \in \mathbb{Z}[x]\}$$

Dem. $\alpha, \beta \in \mathcal{O}_K \Rightarrow M = \mathbb{Z}[\alpha, \beta]$ f.g. como $\mathbb{Z}$-mó[dulo]

$$\left.\begin{matrix}\alpha \pm \beta \\ \alpha\beta\end{matrix}\right\} \in \mathbb{Z}[\alpha, \beta] \Rightarrow \alpha \pm \beta, \alpha\beta \in \mathcal{O}_K.$$

·) Si $g(\alpha) = 0$ para $g \in \mathbb{Z}[x]$ mónico.

$$\Rightarrow f_{\mathbb{Q}}^{\alpha} \mid g \xRightarrow[\text{lema de Gauss}]{} f_{\mathbb{Q}}^{\alpha} \in \mathbb{Z}[x]$$

$\square$

La próxima sesión ·) ejemplos de $\mathcal{O}_K$.

·) propiedades aritméticas.

$$\mathbb{Z}[\sqrt{-3}] \subset \underset{\mathcal{O}_K}{\underset{\|}{\mathbb{Z}\left[\frac{1+\sqrt{-3}}{2}\right]}} \subset \underset{K.}{\underset{\|}{\mathbb{Q}(\sqrt{-3})}}$$

(Comentario) Anillos con factorización de ideales en ideales primos

$\Longleftrightarrow$ anillos de Dedekind

$\Longleftrightarrow$ •) dominio noetheriano ✓

•) $\boxed{\dim R = 1}$ ✓

•) integralmente cerrado. — no siempre.

$R \subset K$
$|<\infty$
$\mathbb{Q}$

$\dim R = 1 \Longrightarrow$ R es "una especie de curva" (?!)

$$\mathrm{Pic}(C) = \frac{\text{divisores}}{\text{divisores principales}}$$

grupo de Picard de una curva. (similar a $\mathrm{Pic}(R)$)