D.E. (Dominio Euclideano)

DIP (Dominio de Ideais Principais)

DFU (Dominio de Fatoração Única)

$\mathbb{Z}$
- Algoritmo da divisão
- $mdc(a,b) = ta + sb$ (o mdc se pode escrever como combinação linear de a e b)
- Teorema fundamental da aritmetica

## Dominios Euclideanos

$\mathbb{Z} \rightsquigarrow K[x]$ K corpo

K é corpo $(K,+,\cdot)$ tal que
- $(K,+)$ grupo abeliano
- $(K^*,\cdot)$ grupo abeliano
- $(K,+,\cdot)$ cumpre a propriedade distributiva

$(\mathbb{Q},+,\cdot)$ $(\mathbb{R},+,\cdot)$ $(A,+,\cdot)$ algebricos

$A = \{\alpha \in \mathbb{C} \mid \alpha$ é raiz de um polinomio com coeficientes racionais$\}$

A é corpo (Precisa de prova)

$\mathbb{Q}[\sqrt{2}] = \{a + \sqrt{2}\, b \mid a, b \in \mathbb{Q}\}$ é corpo

$$(a+\sqrt{2}\,b)^{-1} = \frac{1}{a+\sqrt{2}\,b}\cdot\frac{a-\sqrt{2}\,b}{a-\sqrt{2}\,b}$$

$$\Rightarrow$$

$$= \frac{a-\sqrt{2}\,b}{a^2-2b^2} = \frac{a}{a^2-2b^2} - \sqrt{2}\,\frac{b}{a^2-2b^2} \in \mathbb{Q}[\sqrt{2}]$$

$$\boxed{\begin{array}{l} a^2 = 2b^2 \Rightarrow \quad \frac{a^2}{b^2} = 2 \qquad a, b \in \mathbb{Z} \Rightarrow a = 2a_1 \\ (2a_1)^2 = 2b^2 \Rightarrow 2a_1^2 = b^2 \Rightarrow 2 \mid b \\ \text{Podemos supor } a, b \in \mathbb{Z} \text{ com } (a,b) = 1 \qquad \text{contraditório} \end{array}}$$

**Lema**: Se $\alpha$, $\beta$ são raízes de polinomios com coeficientes racionais então $\mathbb{Q}[\alpha, \beta]$ é corpo

**Prova**: $f(x) \in \mathbb{Q}[x]$ tq $f(\alpha) = 0$
$g(x) \in \mathbb{Q}[x]$ tq $g(\beta) = 0$

com graus $m$ e $n$ mínimos

$1, \alpha, \alpha^2, \dots, \alpha^{m-1}$ são $\mathbb{Q}$-linearmente independentes

Pois $a_0 + a_1\alpha + a_2\alpha^2 + \dots a_{m-1}\alpha^{m-1} = 0$

$\Rightarrow \alpha$ é raiz do polinomio

$a_0 + a_1 x + a_2 x^2 + \dots + a_{m-1} x^{m-1}$

Mesma coisa com $1 \; \beta \; \beta^2 \cdots \beta^{n-1}$ são $\mathbb{Q}$-LI.

$$\mathbb{Q}[\alpha] = \{ \underbrace{c_0 + c_1\alpha + c_2\alpha^2, \cdots + c_{m-1}\alpha^{m-1}} \mid c_j \in \mathbb{Q} \}$$

$$f(x) = x^m + \underbrace{f_{m-1}x^{m-1} + \cdots + f_1 x + f_0} \qquad f(\alpha) = 0$$

$$\underline{\underline{\alpha^m}} = \underbrace{-f_{m-1}\alpha^{m-1} \cdots - f_1\alpha - f_0}$$

$$g(x) = x^n + g_{n-1}x^{n-1} + \cdots + g_1 x + g_0 \qquad g(\beta) = 0$$

$$\underbrace{\mathbb{Q}[\alpha,\beta]} = \mathbb{Q}[\alpha][\beta]$$

$$= \left\{ \sum_{i=1}^{n} \sum_{j=1}^{m} a_{ij} \boxed{\beta^i \alpha^j} \;\middle|\; a_{ij} \in \mathbb{Q} \right\}$$

Pode ser visto como um $\mathbb{Q}$-espaço vetorial de dimensão $\underline{nm}$ com base

$$\{\alpha^j \beta^i\}_{\substack{i=0,\dots,n-1 \\ j=0,\dots,m-1}}$$

Seja $\gamma \in \mathbb{Q}[\alpha,\beta] \setminus \{0\}$

$\gamma$ tem inverso em $\mathbb{Q}[\alpha, \beta]$

$\underbrace{1, \gamma, \gamma^2, \gamma^3, \dots, \gamma^{mn}}_{mn+1 \text{ elementos}}$

visto como $\mathbb{Q}$ espaço vetorial tem dimensão $\leq mn$

Logo são $\mathbb{Q}$-linearmente dependentes

$$a_0 + a_1\gamma + a_2\gamma^2 + \dots a_{mn}\gamma^{mn} = 0$$

Com $a_j \in \mathbb{Q}$ (e não todos iguais a zero)

Se $a_0 = 0$ podemos dividir por $\gamma$ e o coeficiente independente nova e $a_1$

Podemos supor (aplicando essa processo) qe $a_0 \neq 0$

$$0 \neq a_0 = -(a_1\gamma + a_2\gamma^2 + \dots + a_{mn}\gamma^{mn})$$

$$1 = -\frac{a_1}{a_0}\gamma - \frac{a_2}{a_0}\gamma^2 + \dots - \frac{a_{mn}}{a_0}\gamma^{mn}$$

$$1 = \gamma\left(-\frac{a_1}{a_0} - \frac{a_2}{a_0}\gamma - \dots - \frac{a_{mn}}{a_0}\gamma^{mn-1}\right)$$

$$\gamma^{-1} = \underline{\left(-\frac{a_1}{a_0} - \frac{a_2}{a_0}\gamma - \cdots - \frac{a_{mn}}{a_0}\gamma^{mn-1}\right)} \in \mathbb{Q}[\alpha, \beta]$$

$\mathbb{Q}[\alpha, \beta]$ é corpo. $\left(\begin{array}{l}\text{pois ele é subanel de } \mathbb{C} \\ \text{assim faltava verificar que} \\ \text{os inversos estavam também}\end{array}\right)$

$\mathbb{Q}[\sqrt{2}, \sqrt[3]{5}, \sqrt[5]{2}+\sqrt{3}]$ é corpo

$$\boxed{\begin{array}{l}\text{Seja } U \text{ com } \mathbb{Q} \subseteq U \subseteq \mathbb{C} \text{ t.q.} \\ \bullet\ U \text{ é anel} \\ \bullet\ U \text{ é um } \mathbb{Q}\text{-espaço vetorial de dimensão finita} \\ \text{Então } U \text{ é corpo } \left(\begin{array}{c}\text{somente verificar} \\ \text{a propriedade dos} \\ \text{inversos}\end{array}\right)\end{array}}$$

Corpo $L \Rightarrow L[x]$ domínios euclideanos

$$\left.\begin{array}{l}\delta : L[x]^* \longrightarrow \mathbb{N} \\ \qquad f \longmapsto \delta(f) = \deg(f)\end{array}\right\}$$

Dados $f, g \in L[x]$ existem $q, r \in L[x]$

$f(x) = q(x)g(x) + r(x)$ com $\begin{array}{c} r \equiv 0 \\ \text{ou} \\ \deg(r) < \deg(g)\end{array}$

**Teorema:** $\mathbb{Z}[i] = \{a+bi \mid a, b \in \mathbb{Z}\}$ → Inteiros Gaussianos

é Domínio Euclideano

$\rho = ??$
tal que
Se $z_1 \mid z_2$ então
$\rho(z_1) \leq \rho(z_2)$

$$\mathbb{Z}[i]^* \xrightarrow{\rho} \mathbb{Z}$$
$$\underset{\parallel}{a+ib} \longmapsto a^2+b^2 =$$
$$z \longmapsto z\bar{z}$$

$z_2 = z_1 w \qquad w \in \mathbb{Z}[i]$

$$\rho(z_2) = \rho(z_1 w) = (z_1 w)(\overline{z_1 w}) = z_1 \bar{z}_1 w \bar{w}$$
$$= \rho(z_1)\,\rho(w) \geq \rho(z_1)$$

$w = a+bi \qquad \rho(w) = a^2+b^2 \geq 1$

---

$a+ib \qquad c+id$ dados, encontrar

$q = q_1 + i q_2 = ?? \quad r = r_1 + i r_2 = ? \in \mathbb{Z}[i]$

tal que

$\bullet\ a+ib = (q_1 + i q_2)(c+id) + (r_1 + i r_2)$ $(*)$

onde ou $r_1 + i r_2 \equiv 0$

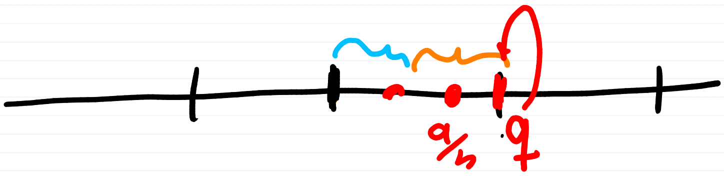
ou $\rho(r_1 + i r_2) < \rho(c+id)$

em $\mathbb{Z}$ $\quad a, b \quad \underbrace{a = qb + r \quad 0 \le r \le b-1}$

$$\underbrace{a = qb + r} \Rightarrow |r| \le \frac{b}{2}$$

$$\frac{a}{b} = q + \frac{r}{b} \rightarrow \left|\frac{r}{b}\right| \le \frac{1}{2}$$

$\frac{a}{b} \in \mathbb{Q}$




Escolhemos $q$ como o inteiro mais próximo de $\frac{a}{b}$ $\Rightarrow \left|\underbrace{\frac{a}{b} - q}_{= r/b}\right| \le \frac{1}{2}$

$$\Rightarrow \frac{a}{b} - q = \frac{r}{b} \Rightarrow \left|\frac{r}{b}\right| \le \frac{1}{2}$$

$$a = bq + r \quad \text{com } |r| \le \tfrac{1}{2} b$$

$$\frac{a+ib}{c+id} = \underline{q_1} + i\underline{q_2} + \frac{r_1 + ir_2}{c+id}$$

$$\frac{a+ib}{c+id} - (q_1 + iq_2) = \frac{r_1 + ir_2}{c+id}$$

$$\frac{(a+ib)(c-id)}{c^2+d^2} - (q_1 + iq_2) = \frac{r_1 + ir_2}{c+id}$$

$$\frac{ac+bd}{c^2+d^2}+i\left(\frac{bc-ad}{c^2+d^2}\right)-(q_1+iq_2)=\frac{r_1+ir_2}{c+id}$$

$$\Big(\overbrace{\frac{ac+bd}{c^2+d^2}-q_1}^{\varepsilon_1}\Big)+i\Big(\overbrace{\frac{bc-ad}{c^2+d^2}-q_2}^{\varepsilon_2}\Big)=\frac{r_1+ir_2}{c+id}$$

Precisamos $\left|\dfrac{r_1+ir_2}{c+id}\right|<1$

$q_1 =$ inteiro mais proximo a $\dfrac{ac+bd}{c^2+d^2}$

$q_2 =$ inteiro mais proximo a $\dfrac{bc-ad}{c^2+d^2}$

Logo $|\varepsilon_1|<\frac{1}{2}$ $\quad |\varepsilon_2|<\frac{1}{2}$

$$\left|\frac{r_1+ir_2}{c+id}\right|^2=|\varepsilon_1+i\varepsilon_2|^2=\varepsilon_1^2+\varepsilon_2^2\leq\frac{1}{4}+\frac{1}{4}=\frac{1}{2}$$

$$|r_1+ir_2|^2\leq\frac{1}{2}|c+id|^2$$

$$\rho(r_1+ir_2)\leq\frac{1}{2}\rho(c+id)<\rho(c+id).$$

$\mathbb{Z}[i]$ é um dominio euclideano

$\mathbb{Z}[\sqrt{2}]$ é dominio euclideano (Prova similar)

$\mathbb{Z}[\sqrt{-2}]$ ⋮

$\mathbb{Z}[\sqrt{3}]$

Existem outros dominios euclideanos da forma $\mathbb{Z}[\sqrt{n}]$ n inteiro na quadrado (mas é um número finito)

$\mathbb{Z}[\sqrt{-2}] = \{a+\sqrt{-2}\,b \mid a,b \in \mathbb{Z}\}$ é domino euclideano com função euclideana

$$\rho(a+\sqrt{-2}\,b) = a^2+2b^2$$

$$|\varepsilon_1| \leq \frac{1}{2} \qquad |\varepsilon_2| \leq \frac{1}{2}$$

$$\Downarrow$$

$$\rho(\varepsilon_1+\sqrt{-2}\,\varepsilon_2) = \varepsilon_1^2+2\varepsilon_2^2 \leq \frac{1}{4}+2\cdot\frac{1}{4} = \frac{3}{4} < 1$$

Teoria algebrica dos Números

$\Downarrow$

Teoria dos números em extensoes finitas de $\mathbb{Z}$

$$\begin{array}{ccc} B \ni \beta & & \\ | & & A[\beta] \\ A & & \end{array}$$

$A \hookrightarrow A[x]$ anel de polinomios

$a \longmapsto a$

Teorema Todo dominio Euclideano (DE) é dominio de ideais principais (D.I.P.)

Prova: Seja $A$ dominio euclideano e seja $I \subset A$ ideal. $I \neq (0)$

Temos que mostrar que existe $\alpha \in A$ tal que $I = (\alpha)$

Seja $f: A^{*} \longrightarrow \mathbb{N}$ função euclideana

$\underbrace{f(I^{*})}$ $\subseteq \mathbb{N}$ mas $\mathbb{N}$ é bem ordenado

logo $f(I^{*})$ tem elemento mínimo $c \in \mathbb{N}$

assim existe $\alpha \in I^{*}$ tal que $f(\alpha) = c$

além disso temos $(\alpha) \subseteq I$

Afirmação: $(\alpha) = I$ $\Leftarrow$

Suponhamos por contradição $I \setminus (\alpha) \neq \emptyset$

e seja $\beta \in I \setminus (\alpha)$ ✓.

Como $\alpha, \beta \in A$ e $\alpha \neq 0$ então existem $q, r \in A$ tais que

- $\beta = q\alpha + r$
- ① $r = 0$ ✓ ou ② $\rho(r) < \rho(\alpha)$ ✓

Se ① é verdadeiro $\Rightarrow$ $\beta \in (\alpha)$ contradição

Se ② $\rho(r) < \rho(\alpha) = \min(\rho(I^*))$ $\Rightarrow$ $r \notin I^*$

mas $r = \underset{\substack{\cap \\ I}}{\beta} - \underset{\substack{\cap \\ I}}{q\alpha} \in I$ contradição

$$\boxed{\text{D.E.} \Rightarrow \text{D.I.P.}} \Rightarrow \text{D.F.U}$$

$\not\Leftarrow$ $\qquad$ $\not\Downarrow$

Contraexemplo

$\mathbb{Z}[\sqrt{19}]$ $\Leftarrow$ Precisa de Prova