domínios de fatorização única

Definição. Um *domínio de fatorização única* ou *domínio de Gauss* é um domínio de integridade D no qual todo o elemento $x \in D\backslash(\mathcal{U}_D \cup \{0_D\})$ se escreve como produto de elementos irredutíveis, sendo essa decomposição única, a menos do produto por unidades, ou seja,

$$\forall x \in D\backslash(\mathcal{U}_D \cup \{0_D\}) \exists p_1, p_2, ..., p_n \text{ irredutíveis em } D : \quad x = p_1 p_2 \cdots p_n$$

e se existem $q_1, q_2, ..., q_t$ irredutíveis em D tais que

$$x = q_1 q_2 \cdots q_t,$$

então, $n = t$ e cada elemento p_i $(i = 1, 2, ..., n)$ é associado a um elemento q_j $(j = 1, 2, ..., n)$ e reciprocamente.

Ao número de fatores irredutíveis que aparecem na fatorização de um elemento x de D chamamos o *comprimento de* x.

Exemplo 7. O domínio de integridade $\mathbb{Z}$ é um domínio de Gauss. Pelo Teorema Fundamental da Aritmética, sabemos que todo o inteiro maior que do que 1 se escreve como produto de primos (que, como já vimos, são os elementos irredutíveis de $\mathbb{Z}^+$) de modo único, a menos da ordem dos fatores. Assim, concluímos que $x \in \mathbb{Z}\backslash\{-1, 0, 1\}$ se escreve como produto de elementos irredutíveis de $\mathbb{Z}$. Essa decomposição é única a menos do produto de ± 1. Por exemplo, as únicas fatorizações possíveis de 6 são, a menos da ordem dos fatores, $2 \cdot 3$ e $(-2)(-3)$.

Teorema. Seja D um domínio de Gauss e $a, b \in D$. Então, existe $\mathrm{m.d.c.}(a, b)$.

Demonstração. Se $a = 0_D$ ou $b = 0_D$, temos que $[a, b] = \{0_D\}$. Sejam, então, $a, b \in D\backslash\{0_D\}$. Suponhamos primeiro que $a \in \mathcal{U}_D$. Então, $a \mid b$ e, portanto, existe $\mathrm{m.d.c.}(a, b)$ e $[a, b] = a\mathcal{U}_D$. A situação é análoga se supormos que $b \in \mathcal{U}_D$.
Suponhamos, então, que $a, b \notin \mathcal{U}_D$. Então, existem $r \in \mathbb{N}$, $m_1, m_2, \ldots, m_r, n_1, n_2, \ldots, n_r \in \mathbb{N}_0$ e $p_1, p_2, \ldots, p_r, q_1, q_2, \ldots, q_r$ elementos irredutíveis em D tais que $a = p_1^{m_1} p_2^{m_2} \cdots p_r^{m_r}$ e $b == q_1^{n_1} q_2^{n_2} \cdots q_r^{n_r}$.

Observe-se que temos garantia que existe pelo menos um dos fatores. Se mais não houver, consideramos o expoente nulo, que transforma o fator em 1_D. Assim, nestas duas fatorizações, podemos considerar o mesmo número de fatores.

Seja $d = p_1^{s_1} p_2^{s_2} \cdots p_r^{s_r}$ onde $s_i = \min(m_i, n_i)$ para cada $i = 1, 2, \ldots, r$. Vamos provar que d é $\mathrm{m.d.c.}(a, b)$. Uma vez que $s_i \leq m_i$, podemos escrever

$$a =^{(} p_1^{s_1} p_2^{s_2} \cdots p_r^{s_r})(p_1^{m_1 - s_1} p_2^{m_2 - s_2} \cdots p_r^{m_r - s_r}) = d(p_1^{m_1 - s_1} p_2^{m_2 - s_2} \cdots p_r^{m_r - s_r}),$$

pelo que $d \mid a$. De modo análogo, concluímos que $d \mid b$.

Seja $k \in D$ tal que $k \mid a$ e $k \mid b$. Se $k \in \mathcal{U}_D$, temos obviamente que $k \mid d$. Se $k \notin \mathcal{U}_D$, existem $v_1, v_2, \ldots, v_r \in \mathbb{N}_0$ tais que $u = p_1^{v_1} p_2^{v_2} \cdots p_r^{v_r} u'$, com $u' \in \mathcal{U}_D$ e, como $k \mid a$ e $k \mid b$,

$$v_i \leq m_i \text{ e } v_i \leq n_i \qquad (i = 1, 2, \ldots, r).$$

Logo, para cada $i = 1, 2, \ldots, r$, $v_i \leq s_i$ e, portanto, $k \mid d$. Logo, d é $\mathrm{m.d.c.}(a, b)$. □

Observação. Este teorema permite-nos concluir que, num domínio de Gauss, são válidos todos os resultados que apresentámos que envolvem máximos divisores comuns, pois temos sempre a garantia que qualquer par de elementos admite pelo menos um $\mathrm{m.d.c.}$.

domínios de ideais principais

Definição. Um *domínio de ideais principais* é um domínio de integridade onde todos os ideais são principais.

Exemplo 8. O domínio de integridade dos inteiros é um domínio de ideais principais. De facto, sabemos que B é ideal de $\mathbb{Z}$ se e só se existe $n \in \mathbb{Z}$ tal que $B = (n)$.

Proposição. Se D é um domínio de ideais principais, $p \in D \backslash \{0_D\}$ é irredutível se e só se (p) é um ideal maximal de D. □

Teorema. Todos os domínios de ideais principais são domínios de fatorização única. □

Observação. O recíproco do teorema anterior não é verdadeiro:

Exemplo 9. Consideremos o conjunto dos polinómios em x com coeficientes em $\mathbb{Z}$, o qual representamos por $\mathbb{Z}[x]$. Prova-se que, quando algebrizado com a adição e a multiplicação usuais de polinómios, é um domínio de fatorização única. No entanto, não é um domínio de ideais principais. Para provarmos tal afirmação basta observar que o ideal gerado pelos polinómios $p(x) = 2$ e $q(x) = x$, i.e., o menor ideal que contém os dois polinómios, não é principal.

Observação. Num domínio de ideais principais, existe $\mathrm{m.d.c.}$ de qualquer par de elementos de D.

De facto, cada domínio de ideais principais é um domínio de Gauss e, em cada domínio de Gauss, existe $\mathrm{m.d.c.}$ de dois quaisquer elementos.

No entanto, é só num domínio de ideais principais que podemos escrever qualquer $\mathrm{m.d.c.}$ de dois elementos como combinação linear desses mesmos elementos.

Proposição. Sejam D um domínio de ideais principais e $a, b, d \in D$. Se d é $\mathrm{m.d.c.}(a, b)$, então, existem $\alpha, \beta \in D$ tais que $d = \alpha a + \beta b$.

Demonstração. Seja $I = \{xa + yb : x, y \in D\}$. Como

- $0_D = 0_D a + 0_D b \in I$;
- $(x_1 a + y_1 b) - (x_2 a + y_2 b) = (x_1 - x_2)a + (y_1 - y_2)b \in I$ para todos $x_1, x_2, y_1, y_2 \in D$;
- $t(xa + yb) = (tx)a + (ty)b \in I$, para todos $x, y, t \in D$,

concluímos que I é um ideal de D. Como D é um domínio de ideais principais, temos que existe $d \in D$ tal que $I = (d) = dD$.

Facilmente se vê que d é $\mathrm{m.d.c.}(a, b)$. Assim, de $d \in I$, concluímos que existem $\alpha, \beta \in D$ tais que $d = \alpha a + \beta b$. Mais ainda, se $d_1 \in [a, b]$, $d_1 = du$ para alguma unidade u de D. Logo, $d_1 = (\alpha u)a + (\beta u)b$. □

domínios euclidianos

Definição. Um domínio de integridade diz-se um *domínio euclidiano* se for possível definir uma aplicação $\delta : D \to \mathbb{N}_0$ tal que
(E1) $\forall a, b \in D \backslash \{0_D\} \qquad b \mid a \Rightarrow \delta(b) \leq \delta(a)$;
(E2) se $a, b \in D$ e $b \neq 0_D$, então, existem $q, r \in D$ tais que $a = bq + r$ e $\delta(r) < \delta(b)$.

À aplicação δ chama-se *valoração em* D.

Exemplo 10. O domínio de integridade $\mathbb{Z}$ é um domínio euclidiano. Basta pensar na aplicação que a cada inteiro faz corresponder o seu valor absoluto.

Proposição. Seja D um domínio euclidiano. Então,

$$\forall b \in D\backslash\{0_D\} \qquad \delta(0_D) < \delta(b).$$

Demonstração. Como $b \neq 0_D$ e $0_D \in D$, temos, por (E2) da definição de domínio euclidiano, que existem $q, r \in D$ tais que $0_D = bq + r$ e $\delta(r) < \delta(b)$. Assim, $r = -bq = b(-q)$ e, portanto, $b \mid r$. Se $r \neq 0_D$, temos, por (E1), que $\delta(b) \leq \delta(r)$. Logo, $\delta(r) < \delta(r)$, o que é um absurdo. O absurdo resulta do facto de supormos que $r \neq 0_D$. Concluímos, então, que $r = 0_D$ e, portanto, $\delta(0_D) < \delta(b)$. □

Teorema. Todo o domínio euclidiano é um domínio de ideais principais.

Demonstração. Sejam D um domínio euclidiano e I um ideal de D. Se $I = \{0_D\}$, então, $I = (0_D)$ e I é principal.

Suponhamos que $I \neq \{0_D\}$. Então, existe $b \neq 0_D$ e, portanto, pela proposição anterior, $\delta(b) \neq \delta(0_D)$. Seja $a \in I\backslash\{0_D\}$ tal que $\delta(a) \leq \delta(x)$ para todo $x \in I\backslash\{0_D\}$. Vamos provar que $I = (a)$. Seja $i \in I$. Como $a \neq 0_D$, por (E2) existem $q, r \in D$ tais que $i = aq + r$ e $\delta(r) < \delta(a)$. Então, $r = i - aq \in I$.

Como a é o elemento não nulo de D de menor valoração, concluímos que $r = 0_D$ e, portanto,

$i = aq \in aD = (a)$. Assim, $I \subseteq (a)$. Como a outra inclusão é trivial, concluímos que I é principal.

□

Corolário. Todo o domínio euclidiano é domínio de fatorização única.

Exemplo 11. O anel $\mathbb{Z}\left[\frac{1+\sqrt{-19}}{2}\right]$ é um domínio de ideais principais que não é euclidiano.

Observação. A importância do estudo dos domínios euclidianos prende-se com a generalização do conhecido Algoritmo de Euclides, enunciado para os inteiros (aliás, é deste facto que resulta a escolha do nome para esta classe de domínios de integridade).

Teorema. **(Algoritmo de Euclides)** Sejam D um domínio euclidiano e $a, b \in D\backslash\{0_D\}$. Sejam $r_1, q_1 \in D$ tais que

$$a = bq_1 + r_1 \qquad \text{onde ou } r_1 = 0_D \text{ } ou \text{ } \delta(r_1) < \delta(b).$$

Se $r_1 \neq 0_D$, sejam $r_2, q_2 \in D$ tais que

$$b = r_1 q_2 + r_2 \qquad \text{onde ou } r_2 = 0_D \text{ } ou \text{ } \delta(r_2) < \delta(r_1).$$

Em geral, sejam $r_{i+1}, q_{i+1} \in D$ tais que

$$r_{i-1} = r_i q_{i+1} + r_{i+1} \qquad \text{onde ou } r_{i+1} = 0_D \text{ } ou \text{ } \delta(r_{i+1}) < \delta(r_i).$$

Então, a sequência $r_1, r_2, \ldots$ tem de terminar para algum $r_s = 0_D$. Se

- $r_1 = 0_D$ então $b \in [a, b]$;
- $r_1 \neq 0_D$ e r_s é o primeiro dos r_i nulo, então $r_{s-1} \in [a, b]$.

Demonstração. Como $\delta(r_i) < \delta(r_{i-1})$ e $\delta(r_i) \in \mathbb{N}_0$, é óbvio que, após um número finito de passos, temos algum $r_s = 0_D$.

Se $r_1 = 0_D$, então $a = bq_1$ e, portanto, $b \mid a$. Logo, $b \in [a, b]$.

Suponhamos que $r_1 \neq 0_D$. Se $d \in D$ é tal que $d \mid a$ e $d \mid b$, então, $d \mid (a - bq_1)$, ou seja, $d \mid r_1$. No entanto, se $d_1 \in D$ é tal que $d_1 \mid r_1$ e $d_1 \mid b$, então, $d_1 \mid (bq_1 + r_1)$, i.e., $d_1 \mid a$. Assim, $[a, b] = [b, r_1]$. Com um raciocínio análogo, se $r_2 = 0_D$, provamos que $[b, r_1] = [r_1, r_2]$. Continuando o processo, concluímos que $[a, b] = [r_{s-2}, r_{s-1}]$, onde r_s é o primeiro dos r_i nulo. Mas, como

$$r_{s-2} = r_{s-1}q_s + r_s = r_{s-1}q_s,$$

$r_{s-1} \mid r_{s-2}$. Logo,

$$[a, b] = r_{s-1}\mathcal{U}.$$

□