divisibilidade em domínios de integridade

lcc :: lmat :: 2.º ano

paula mendes martins

departamento de matemática :: uminho

definições básicas

observações

Ao longo deste capítulo:

- D é um domínio de integridade, i.e., um anel comutativo com identidade no qual 0_D é o único divisor de zero.

- $\mathcal{U}_D$ representa o conjunto das unidades de D, i.e., o conjunto dos elementos $u \in D$ para os quais existe $u^{-1} \in D$.

- Como $1_D \in D$, temos que $\mathcal{U}_D \neq \emptyset$.

Definição. Dados $x, y \in D$, diz-se que x *divide* y (ou que x *é fator de* y ou que y *é divisível por* x) se

$$\exists t \in D : \ y = tx.$$

Neste caso, diz-se também que tx é uma *fatorização* (ou *decomposição em fatores*) *de* y.

Exemplo 1. No domínio de integridade $\mathbb{Z}$, temos que $-2 \mid 4$, mas $2 \nmid 3$.

Proposição. Sejam $x, y \in D$. Então,

1. $x \mid 0_D$;
2. $1_D \mid x$;
3. $\forall u \in \mathcal{U}_D \quad u \mid x$;
4. $x \mid y$ e $y \mid x$ se e só se $y = ux$ para algum $u \in \mathcal{U}_D$ (e, consequentemente, $x = u^{-1}y$).

Demonstração.

1. Seja $x \in D$. Então, $0_D = 0_D x$, pelo que podemos afirmar que $x \mid 0_D$.

2. Seja $x \in D$. Como $x = 1_D x$, temos que $1_D \mid x$.
3. Sejam $x \in D$ e u uma unidade de D. Como $x = 1_D x = u(u^{-1}x)$, concluímos que $u \mid x$.
4. Sejam $x, y \in D$ tais que $y = ux$ e $x = u^{-1}y$ para algum $u \in \mathcal{U}_D$. Então, obviamente, temos que $x \mid y$ e $y \mid x$.

   Reciprocamente, suponhamos que $x \mid y$ e $y \mid x$. Então, existem $t, s \in D$ tais que

   $$y = tx \text{ e } x = sy. \qquad (*)$$

   Temos que considerar 2 casos:

   Caso 1: $x = 0_D$ ou $y = 0_D$. Neste caso, concluímos que $x = y = 0_D$ e, como $0_D = 1_D 0_D$, temos que $x = uy$ para $u = 1_D \in \mathcal{U}_D$;

   Caso 2: $x \neq 0_D$ e $y \neq 0_D$. Neste caso, por $(*)$, temos que

   $$1_D x = x = sy = stx.$$

   Aplicando a lei do corte (pois $x \neq 0_D$), temos que $st = 1_D$. Assim, $s = t^{-1}$ e $t = s^{-1}$, pelo que $s, t \in \mathcal{U}_D$. □

Exemplo 2. No anel dos inteiros relativos, se $x, y \in \mathbb{Z}$ são tais que $x \mid y$ e $y \mid x$, então, $x = \pm y$. De facto, sabemos que $\mathcal{U}_{\mathbb{Z}} = \{-1, 1\}$.

Definição. Dois elementos x e y de um domínio de integridade D dizem-se *associados* se $x \mid y$ e $y \mid x$.

Proposição. Sejam $x, y \in D$. Então, são equivalentes as seguintes afirmações:

1. x e y são associados;
2. $x \in y\mathcal{U}_D$;
3. $y \in x\mathcal{U}_D$.

Proposição. Sejam D um domínio de integridade e $a, b \in D$. Então,

1. $a \mid b \Leftrightarrow (b) \subseteq (a)$;
2. a e b são associados se e só se gerarem o mesmo ideal principal.

Demonstração. Começamos por observar que, como D é um anel comutativo com 1_D, $(x) = xD$, para todo $x \in D$.

1. Por um lado,se $a \mid b$, existe $x \in D$ tal que $b = ax$, pelo que
$$(b) = bD = (ax)D = a(xD) \subseteq aD = (a).$$
Por outro lado, se $(b) \subseteq (a)$, como $b \in (b)$, temos que $b \in aD$, pelo que existe $x \in D$ tal que $b = ax$. Assim, $a \mid b$.
2. O resultado resulta do ponto anterior e do facto de $a \mid b$ e $b \mid a$.

Definição. Um elemento $p \in D$ diz-se *irredutível em* D se

(i) $p \neq 0_D$ e $p \notin \mathcal{U}_D$;

(ii) $p = ab \Rightarrow a \in \mathcal{U}_D$ *ou* $b \in \mathcal{U}_D$.

O elemento p diz-se *redutível em* D se não for irredutível em D.

Exemplo 3. Em $\mathbb{Z}$, os elementos irredutíveis são os números primos e os seus simétricos.

Definição. Um elemento $p \in D$ diz-se *primo* se

(i) $p \neq 0_D$ e $p \notin \mathcal{U}_D$;

(ii) $p \mid ab \Rightarrow p \mid a$ *ou* $p \mid b$.

Proposição. Seja p um elemento não nulo de D. Então,

1. p é primo se e só se (p) é ideal primo de D;
2. p é irredutível se e só se (p) é ideal maximal na classe dos ideais principais de D.

Demonstração.

1. Como D é um anel comutativo com identidade, temos que $(p) = pD$.
   Suponhamos, então, que p é primo. Como $p \notin \mathcal{U}_D$, $1_D \notin pD$, pelo que $D\backslash(p) \neq \emptyset$. Sejam $a, b \in D$ tais que $ab \in pD$.
   Então, $p \mid ab$. Como p é primo, temos que $p \mid a$ ou $p \mid b$ e, portanto, $a \in pD$ ou $b \in pD$. Estamos em condições de concluir que pD é ideal primo de D.
   Reciprocamente, suponhamos que $(p) = pD$ é um ideal primo. Então, $pD \neq D$ pelo que $1_D \notin pD$ e, portanto, p não é unidade de D.
   Sejam $a, b \in D$ tais que $p \mid ab$. Então, $ab \in (p)$. Como (p) é ideal primo, concluímos que $a \in (p)$ ou $b \in (p)$. Assim, temos que $p \mid a$ ou $p \mid b$. Logo, p é primo. □

Proposição. Todo o elemento primo de D é um elemento irredutível.

Demonstração. Suponhamos que p é um elemento primo em D. Então p não é nulo nem é uma unidade. Sejam $a, b \in D$ tais que $p = ab$. Como p é primo, temos que $p \mid a$ ou $p \mid b$.
Suponhamos, sem perdas de generalidade, que $p \mid a$. Então, $a = px$, para algum $x \in D$. Logo,

$$p1_D = p = ab = pxb.$$

Como é um elemento não nulo num domínio de integridade, p é simplificável, e, portanto, temos que $1_D = xb$, ou seja, b é uma unidade. Logo, p é irredutível. □

Exemplo 4. Considere-se o conjunto $\mathbb{Z}[\sqrt{-5}] = \{a + b\sqrt{-5} : a, b \in \mathbb{Z}\}$, algebrizado com duas operações definidas por, para todos $a, b, c, d \in \mathbb{Z}$:

$$(a + b\sqrt{-5}) + (c + d\sqrt{-5}) = (a + c) + (b + d)\sqrt{-5},$$

$$(a + b\sqrt{-5})(c + d\sqrt{-5}) = (ac - 5bd) + (ad + bc)\sqrt{-5}.$$

Então, $\mathbb{Z}[\sqrt{-5}]$ é um domínio de integridade e $\mathcal{U}_{\mathbb{Z}[\sqrt{-5}]} = \{-1, 1\}$.

Neste domínio, o elemento $x = 1 + \sqrt{-5}$ é irredutível, mas não é primo.

Claramente, $1 + \sqrt{-5}$ não é o zero nem uma unidade do anel.

Sejam $a + b\sqrt{-5}, c + d\sqrt{-5} \in \mathbb{Z}[\sqrt{-5}]$ tais que

$$1 + \sqrt{-5} = (a + b\sqrt{-5})(c + d\sqrt{-5}).$$

Sendo estes dois complexos iguais, então, também o são os quadrados dos seus módulos. Logo, temos que

$$6 = (a^2 + 5b^2)(c^2 + 5d^2).$$

Tendo em conta que os fatores são não negativos, as únicas fatorizações possíveis são, a menos da ordem dos fatores, 2×3 e 1×6. Como a primeira é impossível (pois $a^2 + 5b^2 \neq 2$, para quaisquer inteiros a e b), concluímos que $a^2 + 5b^2 = 1$ ou $c^2 + 5d^2 = 1$. Como $a, b, c, d \in \mathbb{Z}$, concluímos que só podemos ter $a = \pm 1$ e $b = 0$ ou $c = \pm 1$ e $d = 0$, i.e., concluímos que $a + b\sqrt{-5}$ é uma unidade ou $c + d\sqrt{-5}$ é uma unidade. Logo $1 + \sqrt{-5}$ é irredutível.

Mas, $1+\sqrt{-5}$ não é primo pois divide $(1+\sqrt{-5})(1-\sqrt{-5}) = 6 = 2 \times 3$ e não divide nem 2 nem 3. De facto, se $1+\sqrt{-5} \mid 2$, existiria $a+b\sqrt{-5} \in \mathbb{Z}[\sqrt{-5}]$ tal que

$$2 = (1+\sqrt{-5})(a+b\sqrt{-5}) = (a-5b)+(b+a)\sqrt{-5},$$

ou seja, existiria $b \in \mathbb{Z}$ tal que $2 = -6b$, o que é impossível em $\mathbb{Z}$. Do mesmo modo, se $1+\sqrt{-5} \mid 3$, existiria $a+b\sqrt{-5} \in \mathbb{Z}[\sqrt{-5}]$ tal que

$$3 = (1+\sqrt{-5})(a+b\sqrt{-5}) = (a-5b)+(b+a)\sqrt{-5},$$

ou seja, existiria $b \in \mathbb{Z}$ tal que $3 = -6b$, o que também é impossível em $\mathbb{Z}$.

Definição. Dados $a, b \in D$, um elemento d de D diz-se um máximo divisor comum de a e b (abreviadamente, $\mathrm{m.d.c.}(a, b)$) se:

(i) $d \mid a$ e $d \mid b$;

(ii) $(\forall c \in D) \qquad c \mid a$ e $c \mid b \Longrightarrow c \mid d$.

Exemplo 5. No domínio de integridade dos inteiros relativos, 2 e -2 são $\mathrm{m.d.c.}(4, 6)$.

Exemplo 6. No domínio de integridade $\mathbb{Z}[\sqrt{-3}]$, não existe máximo divisor comum dos elementos $-2 + 2\sqrt{-3}$ e 8. Tirando as unidades, os divisores comuns dos dois elementos são 2, -2, $1 + \sqrt{-3}$ e $-1 - \sqrt{-3}$. No entanto, dentro desta lista não temos nenhum elemento que seja maior do que os outros, no sentido em não há nenhum elemento que seja divisível por todos os outros (basta verificarmos que $2 \nmid 1 + \sqrt{-3}$ e $1 + \sqrt{-3} \nmid 2$, todos os outros casos são iguais a este a menos de uma unidade).

Proposição. Sejam d um $\mathrm{m.d.c.}(a, b)$ e $d' \in D$. Então,

$$d' \text{ é } \mathrm{m.d.c.}(a, b) \iff d' \in d\,\mathcal{U}_D.$$

Demonstração. Suponhamos que d e d' são $\mathrm{m.d.c.}(a, b)$. Então,

(i_d) $d \mid a$ e $d \mid b$;

(ii_d) $c \mid a$ e $c \mid b \Longrightarrow c \mid d$;

$(i_{d'})$ $d' \mid a$ e $d' \mid b$;

$(ii_{d'})$ $c \mid a$ e $c \mid b \Longrightarrow c \mid d'$.

Logo, de (i_d) e de $(ii_{d'})$, concluímos que $d \mid d'$ e, de $(i_{d'})$ e de (ii_d), concluímos que $d' \mid d$. Assim, $d' \in d\,\mathcal{U}_D$.

Reciprocamente, suponhamos que $d' \in d\,\mathcal{U}_D$ e que d é $\mathrm{m.d.c.}(a, b)$. Então:

(i_d) $d \mid a$ e $d \mid b$;

(ii_d) $c \mid a$ e $c \mid b \Longrightarrow c \mid d$;

(iii) $\exists u_0 \in \mathcal{U}_D : \qquad d' = du_0$.

Assim,

- De (i_d), temos que existem $s, t \in D$ tais que $a = ds$ e $b = dt$. Então, $a = (du_0)(u_0^{-1}s)$ e $b = (du_0)(u_0^{-1})$. Logo, por (iii), temos que $d' \mid a$ e $d' \mid b$.

- Seja $c \in D$ tal que $c \mid a$ e $c \mid b$. Então, por (ii_d), temos que $c \mid d$, pelo que existe $r \in D$ tal que $d = cr$. Logo, $d' = du_0 = cru_0$ e, portanto, $c \mid d'$.

Estamos em condições de concluir que d' é $\mathrm{m.d.c.}(a, b)$. □

Observação. Esta proposição permite-nos afirmar que, se existe $\mathrm{m.d.c.}(a, b)$, ele é univocamente determinado a menos de uma unidade. Assim, representando por $[a, b]$ o conjunto dos $\mathrm{m.d.c.}(a, b)$ em D, se d é $\mathrm{m.d.c.}(a, b)$, temos que

$$[a, b] = d\,\mathcal{U}_D.$$

Mais ainda, como a relação "ser associado de" é uma relação de equivalência, o conjunto $[a, b]$ pode ser visto como uma classe de equivalência.

Corolário. Sejam $a, b, c, e, d, d' \in D$ tais que $d \in [a, b]$, $d' \in [c, e]$ e d e d' são associados. Então, $[a, b] = [c, e]$.

Proposição. Sejam $a, b, p \in D$. Então,

1. se $a \mid b$, $a \in [a, b]$ e, portanto, $[a, b] = a\mathcal{U}_D$;
2. se p é irredutível, existe $\mathrm{m.d.c.}(a, p)$ e

$$[a, p] = \mathcal{U}_D \qquad ou \qquad [a, p] = p\mathcal{U}_D.$$

Proposição. Em D, sempre que as expressões fizerem sentido, são válidas as seguintes igualdades:

1. $[ac, bc] = [a, b]c$;
2. $[[a, b], c] = [a, [b, c]]$.

Demonstração.

1. Seja $d' \in [ac, bc]$. Queremos provar que $d' = d_1 c$ para algum $d_1 \in [a, b]$. Começamos por observar que, por um lado,

$$\begin{aligned} d \in [a, b] \quad &\Rightarrow d \mid a \text{ e } d \mid b \\ &\Rightarrow dc \mid ac \text{ e } dc \mid bc \\ &\Rightarrow dc \mid d' \\ &\Rightarrow \exists t \in D : \ d' = tdc = dtc. \end{aligned}$$

Por outro lado,

$$\begin{aligned} d' \mid ac \quad &\Rightarrow \exists q \in D : \ ac = d'q \\ &\Rightarrow \exists q \in D : \ ac = dtcq \\ &\Rightarrow \exists q \in D : \ a = dtq \end{aligned}$$

e, de modo análogo,

$$d' \mid b \Rightarrow \exists s \in D : \ b = dts.$$

Logo, $dt \mid a$ e $dt \mid b$, pelo que $dt \mid d$ (pois $d \in [a, b]$). Assim,

$$\exists r \in D : \ d = dtr$$

e, portanto, $1_D = tr$. Concluímos então que $t \in \mathcal{U}_D$ e, assim, $dt \in [a, b]$. Logo, existe $d_1 = dt \in [a, b]$ tal que $d' = d_1 c$.

Reciprocamente, seja $d \in [a, b]$. Queremos provar que $dc \in [ac, bc]$. Seja $d' \in [ac, bc]$. Como $dc \mid ac$ e $dc \mid bc$, temos que $dc \mid d'$. Assim, existe $t \in D$ tal que $d' = dct$. Como já provamos que existe $d_1 \in [a, b]$ tal que $d' = d_1 c$, concluímos que $d_1 = dt$ e, portanto, $t \in \mathcal{U}_D$. Logo, $dc \in d' \mathcal{U}_D = [ac, bc]$.

2. Sejam $d \in [a, b]$, $d' \in [b, c]$, $d_1 \in [d, c]$ e $d_1' \in [a, d']$. Então,
   (a) de $d \mid a$, $d \mid b$ e $d_1 \mid d$, concluímos que $d_1 \mid a$ e $d_1 \mid b$;
   (b) de $d_1 \mid b$ e $d_1 \mid c$, concluímos que $d_1 \mid d'$;
   (c) de $d_1 \mid d'$ e $d_1 \mid a$, concluímos que $d_1 \mid d_1'$.

   De igual modo,
   (d) de $d' \mid b$, $d' \mid c$ e $d_1' \mid d'$, concluímos que $d_1' \mid b$ e $d_1' \mid c$;
   (e) de $d_1' \mid a$ e $d_1' \mid b$, concluímos que $d_1' \mid d$;
   (f) de $d_1' \mid d$ e $d_1' \mid c$, concluímos que $d_1' \mid d_1$.

   De (c) e (f), temos que d_1 e d_1' são associados e, portanto, $[d, c] = [a, d']$, i.e., $[[a, b], c] = [a, [b, c]]$.

□

Proposição. Sejam $a, b, c \in D$. Se existe $\mathrm{m.d.c.}$ de qualquer par de elementos em D, então,

$$[a, b] = \mathcal{U}_D, \;\; [a, c] = \mathcal{U}_D \Rightarrow [a, bc] = \mathcal{U}_D.$$

Demonstração. Seja $d \in [a, bc]$. Então, $d \mid a$ e $d \mid bc$, pelo que $d \mid ac$ e $d \mid bc$. Logo, $d \mid d_1$ para algum $d_1 \in [ac, bc]$. Então, pela Proposição anterior, existe $u \in [a, b] = \mathcal{U}_D$ tal que $d_1 = uc$. Logo, $d \mid uc$. Como $uc \mid c$, temos que $d \mid c$. Assim, de $d \mid a$ e $d \mid c$, concluímos que $d \mid u'$, para qualquer $u' \in \mathcal{U}_D = [a, c]$. Logo, $d \in \mathcal{U}_D$. Logo, $[a, bc] \subseteq \mathcal{U}_D$. Como $[a, bc]$ é uma classe de equivalência, temos que $[a, bc] = \mathcal{U}_D$. □

Observação. Vimos já que, num domínio de integridade, nem todo o elemento irredutível é primo. No entanto, se existir $\mathrm{m.d.c.}$ de dois quaisquer elementos do domínio, prova-se que todo o elemento irredutível é primo.

Proposição. Se $[a, b] \neq \emptyset$, para todos $a, b \in D$, então, qualquer elemento irredutível é primo.

Demonstração. Sejam $x \in D$ um elemento irredutível e $a, b \in D$ tais que $x \mid ab$. Se $x \nmid a$ e $x \nmid b$, teríamos $[x, a] = [x, b] = \mathcal{U}_D$ e, portanto, $[x, ab] = \mathcal{U}_D$. Mas, como $x \mid ab$, $[x, ab] = x\mathcal{U}_D$. No entanto, $x\mathcal{U}_D \neq \mathcal{U}_D$, já que $x \notin \mathcal{U}_D$. A contradição a que chegamos resultado do facto de supormos que $x \nmid a$ e $x \nmid b$. Logo, $x \mid a$ ou $x \mid b$. □