Exercícios

1.1. Mostre que num domínio de integridade D:

(a) $\langle a\rangle \subseteq \langle b\rangle$ sse $b \mid a$.

(b) $\langle a\rangle = \langle b\rangle$ sse $a \sim b$.

(c) $\langle a\rangle = D$ sse $a \in D^*$.

(d) $D[x]^* = D^*$.

1.2. Mostre que num domínio de integridade D:

(a) $u \in D^*$ sse $u \mid d$ para todo o $d \in D$.

(b) Qualquer associado de uma unidade é uma unidade.

(c) Qualquer associado de um elemento irredutível é irredutível.

1.3. Demonstre a Proposição 1.2.

1.4. Verifique que um anel (comutativo com identidade) A é um domínio de integridade se e só $ab \in \langle 0\rangle \Rightarrow a \in \langle 0\rangle$ ou $b \in \langle 0\rangle$.

1.5. (a) Determine as unidades do *anel dos inteiros de Gauss* $\mathbb{Z}[i]$.

(b) Verifique que $1 \pm i$ são elementos irredutíveis de $\mathbb{Z}[i]$. Observe que $2 \in \mathbb{Z}[i]$ não é irredutível em $\mathbb{Z}[i]$ apesar de o ser em $\mathbb{Z}$.

1.6. Seja D um domínio de integridade onde é possível definir uma função $N\colon D \to \mathbb{N}_0$ (chamada *norma*) com as seguintes propriedades:

(1) $N(a) = 0$ sse $a = 0$.

(2) $N(a) = 1$ sse $a \in D^*$.

(3) $N(ab) = N(a)N(b)$ para quaisquer $a, b \in D \setminus \{0\}$.

Mostre que todo o elemento de $D \setminus D^*$ não nulo admite uma factorização como produto de elementos irredutíveis.

1.7. Considere o anel $\mathbb{Z}[\sqrt{d}] = \{a + b\sqrt{d} \mid a, b \in \mathbb{Z}\}$ onde $d \neq 0, 1$ é *livre de quadrados*, isto é, para qualquer primo $p \in \mathbb{Z}$, $p^2 \nmid d$.

(a) Mostre que $a + b\sqrt{d} = a' + b'\sqrt{d}$ se e só se $a = a'$ e $b = b'$.

(b) Prove que a aplicação $N\colon \mathbb{Z}[\sqrt{d}] \to \mathbb{N}_0$ definida por $N(a + b\sqrt{d}) = |a^2 - db^2|$ é uma norma (recorde o exercício anterior).

(c) Conclua que em $\mathbb{Z}[\sqrt{-5}] = \mathbb{Z}[i\sqrt{5}]$ os elementos 3 e $2 \pm \sqrt{-5}$ são irredutíveis.

(d) Mostre que em $\mathbb{Z}[\sqrt{-5}]$ todos os elementos admitem factorizações em irredutíveis, mas a decomposição não é, em geral, única.

1.8. Seja C um corpo. Verdadeiro ou falso?

(a) Se $a, b, c \in C^*$ então $a \in \text{mdc}(b, c)$.

(b) C é um DFU.

1.9. Seja D um DIP e $a, b \in D$. Prove que:

(a) $d \in \text{mdc}(a, b)$ se e só se $\langle d\rangle = \langle a, b\rangle = \langle a\rangle + \langle b\rangle$.

(b) $m \in \text{mmc}(a, b)$ se e só se $\langle m\rangle = \langle a\rangle \cap \langle b\rangle$.

(c) Se $d \in \text{mdc}(a, b)$ então existem $p, q \in D$ tais que $d = pa + qb$ (*Relação de Bézout*).

1.10. Seja D um domínio de integridade e $a_1, \ldots, a_n \in D$.

(a) Defina $\text{mdc}(a_1, \ldots, a_n)$ e $\text{mmc}(a_1, \ldots, a_n)$.

(b) Mostre que se $d' \in \text{mdc}(a_1, \ldots, a_{n-1})$ e $d \in \text{mdc}(d', a_n)$ então $d \in \text{mdc}(a_1, \ldots, a_n)$.

(c) Enuncie e demonstre o resultado análogo para mmc's.

1.11. Seja A um anel comutativo com identidade e seja $\mathcal{S}$ o conjunto das sequências infinitas $(a_n)_{n\in\mathbb{N}_0}$ de elementos de A. Defina $+$ e $\cdot$ em $\mathcal{S}$ por

$$(a_n)_{n\in\mathbb{N}_0} + (b_n)_{n\in\mathbb{N}_0} = (a_n + b_n)_{n\in\mathbb{N}_0} \quad \text{e} \quad (a_n)_{n\in\mathbb{N}_0} \cdot (b_n)_{n\in\mathbb{N}_0} = (c_n)_{n\in\mathbb{N}_0}$$

onde $c_n = a_0b_n + a_1b_{n-1} + \cdots + a_nb_0$ para $n = 0, 1, 2, \ldots$. Mostre que:

(a) $(\mathcal{S}, +, \cdot)$ é um anel comutativo com identidade.

(b) $(a_n)_{n\in\mathbb{N}_0} \in \mathcal{S}^*$ se e só se $a_0 \in A^*$.

(c) Se A é um corpo então $\mathcal{S}$ é um domínio de ideais principais.

1.12. Seja D um DFU e C o seu corpo de fracções. Mostre que é possível escrever qualquer elemento de C como a/b com $a, b \in D$ elementos *coprimos* (ou *primos entre si*, isto é, tais que $\text{mdc}(a, b) = D^*$).

1.13. Seja $A = \{p(x) \in \mathbb{R}[x] \colon p(x) \text{ não tem monómio de grau } 1\}$.

(a) Verifique que A é um anel (subanel de $\mathbb{R}[x]$).

(b) Verifique que todos os polinómios de grau 2 ou 3 são irredutíveis em A.

(c) Verifique que os polinómios $x^2(x^2 + x)^2$ e $x^3(x^2 + x)$ não têm mdc em A. Que pode dizer do mmc?

(d) Prove que todo o elemento de A se factoriza como produto de irredutíveis, mas esta factorização nem sempre é única.

(**Observação:** este exercício mostra que um subanel de um DFU não é necessariamente um DFU.)

1.14. Seja D um domínio de integridade.

(a) Verifique que se $p(x) \in D[x]$ é primitivo e $q(x) \mid p(x)$, com $\mathrm{gr}(q(x)) \geq 1$, então $q(x)$ é primitivo.

(b) Mostre que todo o polinómio primitivo de $D[x]$ admite factorizações em irredutíveis em $D[x]$.

1.15. Seja D um DFU, $a \in D$, com $a \neq 0$, e $p(x), q(x) \in D[x]$ tais que $q(x) \mid ap(x)$ e $q(x)$ é primitivo. Prove que $q(x) \mid p(x)$.

1.16. Seja D um DFU. Mostre que, para quaisquer $a, b, c \in D$, se $1 \in \mathrm{mdc}(a, b)$ e $a \mid bc$ então $a \mid c$.

1.17. Seja D um domínio euclidiano com função euclidiana δ.

(a) Prove que $a \in D$ é uma unidade se $\delta(a)$ for um mínimo do conjunto $\{\delta(x) \mid x \in D, x \neq 0\}$. Mostre que se $\delta(a) \leq \delta(ab)$ para quaisquer $a, b \in D \setminus \{0\}$, então a implicação recíproca também é verdadeira.

(b) Revisite o Exercício 1.5, resolvendo-o agora usando o facto de $\mathbb{Z}[i]$ ser um domínio euclidiano.

1.18. Calcule em $\mathbb{Z}[i]$:

(a) $\mathrm{mdc}(2, 3 + i)$.

(b) $\langle 2 \rangle + \langle 3 + i \rangle$.

(c) $\langle 2 \rangle \cap \langle 3 + i \rangle$.

(d) $\mathrm{mdc}(9 - 5i, -9 + 13i)$.

1.19. Seja D um domínio euclidiano com função euclidiana δ (satisfazendo $\delta(a) \leq \delta(ab)$ para quaisquer $a, b \in D \setminus \{0\}$). Seja $I \neq \{0\}$ um ideal de D. Prove que se existir $a \in I$ tal que $\delta(a) = \delta(1)$, então $I = D$.

1.20. Seja D um domínio euclidiano com função euclidiana δ (satisfazendo $\delta(a) \leq \delta(ab)$ para quaisquer $a, b \in D \setminus \{0\}$). Mostre que se n é um inteiro tal que $\delta(1) + n > 0$, então a função $\delta' \colon D \setminus \{0\} \to \mathbb{N}$ definida por $\delta'(a) = \delta(a) + n$ é também uma função euclidiana em D.

1.21. Seja D um domínio euclidiano. Mostre, usando o método das divisões sucessivas (Euclides), que dados $a, b \in D$ (não simultaneamente nulos), existem $p, q \in D$ tais que $pa + qb \in \text{mdc}(a, b)$.

1.22. Seja A um anel comutativo com 1. Mostre que as seguintes condições são equivalentes:

(i) A é um corpo.

(ii) $A[x]$ é um domínio euclidiano.

(iii) $A[x]$ é um DIP.

1.23. Seja $\phi\colon A \to B$ um homomorfismo de anéis. Mostre que:

(a) $\phi(0) = 0$ e $\phi(-a) = -\phi(a)$.

(b) $N(\phi)$ é um ideal de A.

(c) ϕ é injectiva sse $N(\phi) = \{0\}$.

(d) $\phi(A)$ é um subanel de B.

1.24. Seja A um anel. Sendo I um ideal de A e B um subanel de A, mostre que:

(a) $B + I$ é um subanel de A e I é um ideal de $B + I$.

(b) A correspondência $a \mapsto a + I$ define um homomorfismo sobrejectivo $\pi\colon A \to A/I$ com núcleo I.

(c) A correspondência $b \mapsto b + I$ define um homomorfismo $B \to A/I$ com núcleo $B \cap I$ e imagem $(B + I)/I$.

1.25. (a) Sejam A um DIP, B um domínio de integridade e $\phi\colon A \to B$ um homomorfismo sobrejectivo de anéis com $N(\phi) \neq \{0\}$.

(i) Prove que $N(\phi)$ é um ideal maximal de A.

(ii) Conclua que B é um corpo.

(b) Sendo D um domínio de integridade, mostre que $D[x]$ é um DIP se e só se D é um corpo.

1.26. Prove que os anéis $\mathbb{Z}_n \oplus \mathbb{Z}_m$ e $\mathbb{Z}_{nm}$ são isomorfos se $\text{mdc}(n, m) = 1$. Mais geralmente, mostre que $\mathbb{Z}_n \oplus \mathbb{Z}_m \cong \mathbb{Z}_d \oplus \mathbb{Z}_k$ para $d = \text{mdc}(n, m)$ e $k = \text{mmc}(n, m)$.

Soluções de exercícios seleccionados

1.11. (a) É fácil verificar que $\mathcal{S}$ é um anel comutativo com 1. A sequência $(1, 0, 0, \dots)$ é a identidade de $\mathcal{S}$.

(b) Consideremos $(a_n)_{n\in\mathbb{N}_0} \in \mathcal{S}$. Suponhamos que (a_n) é uma unidade. Então existe uma sequência $(b_n)_{n\in\mathbb{N}_0}$ tal que $(a_n)\cdot(b_n) = 1$. Logo, $a_0b_0 = 1$ e portanto a_0 é uma unidade de A.

Reciprocamente, suponhamos que $a_0 \in A^*$ e consideremos a sequência (b_n) definida por

$$b_0 = a_0^{-1}, \quad b_1 = -a_0^{-1}(a_1a_0^{-1}), \quad \dots, \quad b_k = -a_0^{-1}(a_1b_{k-1}+\cdots+a_kb_0), \quad k \geq 2.$$

É claro que $a_0b_0 = 1$, $a_0b_1 + a_1b_0 = a_0(-a_0^{-1}(a_1a_0^{-1})) + a_1a_0^{-1} = 0, \dots,$ $a_kb_0+a_{k-1}b_1+\cdots+a_0b_k = a_kb_0+a_{k-1}b_1+\cdots+a_0(-a_0^{-1}(a_1b_{k-1}+\cdots+a_kb_0)) =$ 0. Então $(a_n)\cdot(b_n) = 1$, o que prova que (a_n) é uma unidade de $\mathcal{S}$.

(c) Suponhamos que A é um corpo. Seja I um ideal de $\mathcal{S}$. Se $I = \{0\}$, então I é um ideal principal. Suponhamos então que $I \neq \{0\}$. Seja (a_n) um elemento não nulo de I. Definimos a *ordem* $\mathrm{o}(a_n)$ de uma sequência não nula (a_n) de $\mathcal{S}$ como sendo o primeiro inteiro não negativo tal que $a_n \neq 0$ e $a_i = 0$ para $i < n$. Existe uma sequência (a_n) tal que $\mathrm{o}(a_n) = \kappa \leq \mathrm{o}(b_n)$ para qualquer $(b_n) \in I$. Seja (c_n) a sequência tal que $c_i = a_{\kappa+i}$ para todo o $i \geq 0$. Então $(c_n)^{-1}$ existe e $(c_n)^{-1}\cdot(a_n) = (d_n) \in I$. Além disso, $d_\kappa = 1$ e $d_i = 0$ para todo o $i \neq \kappa$. Provemos que $I = \langle(d_n)\rangle$. Claramente $\langle(d_n)\rangle \subseteq I$. Seja $(u_n) \in I$ com ordem m. Então $m \geq \kappa$. Seja $(r_n) \in \mathcal{S}$ tal que $r_{m-\kappa+i} = u_{m+i}$ para qualquer $i \geq 0$ e $r_i = 0$ para qualquer $i \leq m - \kappa$. É fácil verificar que $(u_n) = (r_n)\cdot(d_n) \in \langle(d_n)\rangle$. Logo, $I = \langle(d_n)\rangle$.

1.14. (a) Seja $d \in D$ um divisor de $q(x)$ de grau zero. Como $d \mid p(x)$ então d é uma unidade.

(b) Seja $p(x)$ um polinómio primitivo de $D[x]$. Faremos a demonstração por indução sobre o grau $n \geq 1$ de $p(x)$:

Se $n = 1$ então $p(x)$ não admite factorizações próprias e, sendo primitivo, é irredutível e está provado.

Tomemos $p(x)$ de grau n e suponhamos, como hipótese de indução, que o resultado é válido para todos os polinómios de grau $< n$. Se $p(x)$ admitir uma factorização própria então $p(x) = q(x)r(x)$ com $\mathrm{gr}(q(x)), \mathrm{gr}(r(x)) < n$ e, pela hipótese de indução, ambos são factorizáveis em polinómios irredutíveis, o que nos dá uma factorização de $p(x)$ em irredutíveis. No caso em que $p(x)$

não admite factorizações próprias, como é primitivo, então é irredutível e está provado.

1.16. Seja $p_1p_2\cdots p_n$ a factorização de a em primos. Para cada $i = 1, 2, \ldots, n$, $p_i \mid bc$ logo $p_i \mid b$ ou $p_i \mid c$. Mas como a e b são primos entre si e $p_i \mid a$ (para qualquer i), se p_i dividisse b para algum i teríamos $p_i \mid 1$, isto é, $p_i \in D^*$, um absurdo. Logo nenhum p_i divide b pelo que $p_i \mid c$ para $i = 1, 2, \ldots, n$ e portanto $a \mid c$.

1.17. (b) $\mathbb{Z}[i]$ é um domínio euclidiano com função euclidiana

$$\delta(a + ib) = |a + ib|^2 = a^2 + b^2$$

que satisfaz a propriedade $\delta(xy) = \delta(x)\delta(y)$. As unidades de $\mathbb{Z}[i]$ são ± 1 e $\pm i$, pois $\delta(a + ib) = 1$ se e só se $a + ib \in \{\pm 1, \pm i\}$.

Se $1 \pm i = (a + ib)(c + id)$ então $\delta(1 \pm i) = \delta(a + ib)\delta(c + id)$, isto é, $2 = \delta(a + ib)\delta(c + id)$. Como 2 é primo em $\mathbb{Z}$, então $\delta(a + ib) = 1$ (ou seja, $a + ib$ é uma unidade) ou $\delta(c + id) = 1$ (ou seja, $c + id$ é uma unidade).

Claro que 2 é irredutível em $\mathbb{Z}$ porque é primo. Mas em $\mathbb{Z}[i]$, $2 = (1+i)(1-i)$, logo é redutível em $\mathbb{Z}[i]$.

1.18. (a) Pelo exercício anterior, $2 = (1 + i)(1 - i)$ é a factorização (única) de 2 em irredutíveis (primos). Como $3 + i = (1 + i)(2 - i)$ é a factorização de $3 + i$ em primos (de facto, $2 - i$ também é irredutível pois $\delta(2 + i) = 5$ é um inteiro primo), então $1 + i \in \text{mdc}(2, 3 + i)$. Logo,

$$\text{mdc}(2, 3 + i) = \{1 + i, -1 - i, -1 + i, 1 - i\}.$$

(b) Como em qualquer DIP, $\langle a\rangle + \langle b\rangle = \langle \text{mdc}(a, b)\rangle$, então $\langle 2\rangle + \langle 3 + i\rangle = \langle \text{mdc}(2, 3 + i)\rangle = \langle 1 + i\rangle = \{(a + ib)(1 + i) \mid a, b \in \mathbb{Z}\} = \{(a - b) + i(a + b) \mid a, b \in \mathbb{Z}\}$.

(c) Como em qualquer DIP, $\langle a\rangle \cap \langle b\rangle = \langle \text{mmc}(a, b)\rangle$, então $\langle 2\rangle \cap \langle 3 + i\rangle = \langle \text{mmc}(2, 3+i)\rangle = \langle (1+i)(1-i)(2-i)\rangle = \langle 4-2i\rangle = \{(4a+2b)+i(-2a+4b) \mid a, b \in \mathbb{Z}\}$.

1.22. (i)⇒(ii): Sendo A um corpo, dados $a(x), b(x) \in A[x]$ com $b(x) \neq 0$ sabemos que existem $q(x), r(x) \in A[x]$ tais que $a(x) = q(x)b(x) + r(x)$ com $r(x) = 0$ ou $gr(r(x)) < gr(b(x))$ (equivalentemente, $gr(r(x)) + 1 < gr(b(x)) + 1$). Portanto, fazendo $\delta(p(x)) = gr(p(x)) + 1$, temos claramente uma função euclidiana em $A[x]$.

(ii)⇒(iii): Basta aplicar a Proposição 4.2 que assegura que todo o domínio euclidiano é um DIP.

(iii)⇒(i): Seja $a \neq 0$ em A. Teremos que mostrar que a é invertível. Para isso consideremos o ideal $I = \langle a, x \rangle$ de $A[x]$, que é principal. Portanto, existe $p(x) \in A[x]$ tal que $I = \langle p(x) \rangle$. Como $a, x \in I$ então existem $a(x)$ e $b(x)$ em $A[x]$ tais que $a = a(x)p(x)$ e $x = b(x)p(x)$. Consequentemente, $gr(p(x)) = 0$ (observe que $A[x]$ sendo um domínio de integridade, implica necessariamente que A o seja), isto é, $p(x) = d \in A$. Então $x = b(x)d$, o que implica que $cd = 1$ para algum $c \in A$. Portanto d é uma unidade e $I = \langle d \rangle = A[x]$. Daqui podemos concluir que $1 \in I$, isto é, $1 = ap_1(x) + xp_2(x)$ para algum par $p_1(x), p_2(x)$ em $A[x]$. Isto implica $1 = ab$ para algum $b \in A$ e a é assim invertível.