Sebenta de exercícios de Álgebra II

Curso: Matemática

Ano Lectivo 2007/2008

6 de Junho de 2008

(versão 1.4)

Conteúdo

Notas Prévias

Esta sebenta de exercícios juntamente com a matéria leccionada nas aulas teóricas formam um todo, i.e., são uma parte integrante do programa da disciplina e não meramente um conjunto de exercícios soltos.

Em relação à resolução dos exercícios que constam nesta sebenta, chama-se a atenção de que, só tem sentido tentar resolvê-los, após um estudo, cuidadoso, da matéria leccionada nas aulas teóricas, tudo o resto, será uma mera tentativa de resolução mecânica dos exercícios, sem qualquer fundamentação.

O material contido nesta sebenta de exercícios, foi elaborado com base nas referências [1, 2, 3, 4, 5] e de um conjunto de exercícios elaborados pelo próprio. Saliente-se que, alguns destes exercícios, foram revistos por alguns dos meus colegas do Departamento de Matemática com quem tenho trabalhado ao longo dos anos. A todos eles, os meus sinceros e profundos agradecimentos.

N.B.: Na elaboração desta sebenta, e dentro do possível, houve o cuidado de se usar uma escrita matemática rigorosa e uma simbologia o mais actualizada possível, no entanto, esta sebenta pode não estar isenta de - apesar de involuntárias - omissões e incorrecções[1].

[1] apesar de se encontrar em permanente actualização, aceitam-se e agradecem-se sugestões, comentários e correcções, de preferência, enviados para psemiao@ualg.pt.

Notações e terminologia

Faremos uso dos seguintes símbolos para representar os conjuntos usuais:

$\emptyset$	o conjunto vazio
$\mathbb{N} = \{0, 1, 2, 3, \cdots\}$	o conjunto dos números naturais
$\mathbb{Z} = \{\cdots, -2, -1, 0, 1, 2, \cdots\}$	o conjunto dos números inteiros
$\mathbb{Q} = \left\{ \frac{x}{y} \in \mathbb{R} : x \in \mathbb{Z} \wedge y \in \mathbb{Z} \setminus \{0\} \right\}$	o conjunto dos números racionais
$\mathbb{R}$	o conjunto dos números reais
$\mathbb{C}$	o conjunto dos números complexos

Sendo $X \in \{\mathbb{N}, \mathbb{Z}, \mathbb{Q}, \mathbb{R}\}$, representaremos por $X_{>0}, X_{\geq 0}$ e $X_{\neq 0}$, respectivamente, os seguintes conjuntos:

$$X_{>0} := \{x \in X : x > 0\}$$
$$X_{\geq 0} := \{x \in X : x \geq 0\}$$
$$X_{\neq 0} := \{x \in X : x \neq 0\}.$$

Como exemplos, o conjunto

$$\mathbb{R}_{\geq 0} := \{x \in \mathbb{R} : x \geq 0\} = [0, +\infty[,$$

representa o conjunto dos números reais não negativos, enquanto que o conjunto

$$\mathbb{R}_{\neq 0} := \{x \in \mathbb{R} : x \neq 0\} = \mathbb{R} \setminus \{0\},$$

representa o conjunto de todos os números reais, excepto o zero.
Faremos também uso do símbolo $\mathbb{C}_{\neq 0}$, para representar o conjunto $\mathbb{C} \setminus \{0 + 0i\}$.

De um modo geral, o símbolo $\mathbb{K}$ representa um corpo qualquer e o símbolo ':=' quer designar a igualdade de duas entidades por definição.
Iremos representar por $\mathrm{card}(A)$ o cardinal do conjunto A. O símbolo '$\sqsubseteq$' representa uma subestrutura de uma dada estrutura algébrica. Por exemplo, sendo R um anel e A um subconjunto de R, para abreviar a expressão 'A é um subanel de R', usamos o simbolismo $A \sqsubseteq R$.

Tabela de Símbolos

Y^X	o conjunto de todas as aplicações de X em Y
$\mathrm{Inj}(X,Y)$	o conjunto de todas as aplicações injectivas de X em Y
$\mathrm{Surj}(X,Y)$	o conjunto de todas as aplicações sobrejectivas de X em Y
$\mathrm{Bij}(X,Y)$	o conjunto de todas as aplicações bijectivas de X em Y
$\mathrm{Mor}(R,S)$ $(= \mathrm{Hom}(R,S))$	o conjunto de todos os morfismos de R em S
$\mathrm{End}(R)$	o conjunto de todos os endomorfismos em R
$\mathrm{Mono}(R,S)$	o conjunto de todos os monomorfismos de R em S
$\mathrm{Epi}(R,S)$	o conjunto de todos os epimorfismos de R em S
$\mathrm{Bim}(R,S)$	o conjunto de todos os bimorfismos de R em S
$\mathrm{Sect}(R,S)$	o conjunto de todas as secções de R em S
$\mathrm{Retr}(R,S)$	o conjunto de todas as retracções de R em S
$\mathrm{Iso}(R,S)$	o conjunto de todos os isomorfismos de R em S
$\mathrm{Aut}(R)$	o conjunto de todos os automorfismos em R
$\mathrm{Emb}(R,S)$	o conjunto de todos os mergulhos de R em S
$U_R^l(A)$ (resp., $U_R^r(A)$, $U_R(A)$)	o conj. de todas as unidades esq. (resp., dir., bilat.) de A em R
$\mathcal{I}_R^l(A)$ (resp., $\mathcal{I}_R^r(A)$, $\mathcal{I}_R(A)$)	o conj. de todos os ideais esq. (resp., dir., bilat.) de A em R
${}_R(A)$ (resp., $(A)_R$, (A))	ideal esquerdo (resp., direito, bilateral) gerado por A
$P(R)$	o conjunto de todos os elementos primos de R
$\mathrm{Ann}_R(X)$	o anulador de X em R
$\langle A\rangle$ (resp., ${}_R\langle A\rangle$)	o subanel (resp., R-submódulo) gerado por A
$\mathrm{Idem}(R)$	o conjunto de todos os elementos idempotentes de R
$\mathbb{F}_k$	um corpo finito com k elementos
$\mathrm{Frac}_R(R,S)$	o anel das fracções (direito) de R com respeito a S

1. Anéis

1.1. Anéis e subanéis

1.1.1) Mostre que num anel $(R; +, \cdot, 0_R)$ com elemento identidade 1_R tem-se que $0_R = 1_R$ se, e só se, o conjunto suporte R tem um único elemento.

1.1.2) Mostre que se num conjunto singular definirmos duas operações binárias, então ele é um anel multiplicativo e comutativo.

1.1.3) Verifique se os seguintes conjuntos com as operações indicadas são anéis e, indique, os que são comutativos e os que tem identidade:

a) $(M_{n\times n}(R); +, \cdot, O_{n\times n})$, onde R é um anel.
Em particular, com $R := \mathbb{Z}$, obtemos o anel $M_{n\times n}(\mathbb{Z})$.

b) $\left(\mathbb{Z}_n; +, \cdot, \overline{0}_n, \overline{1}_n\right)$, onde $n \in \mathbb{N}_{\neq 0}$.

c) $\left(\mathbb{Q}\left[\sqrt{p}\right]; +, \cdot, 0\right)$, onde $\mathbb{Q}\left[\sqrt{p}\right] := \left\{x + y\sqrt{p} \in \mathbb{R} : x, y \in \mathbb{Q} \wedge p \in P(\mathbb{N}_{\geq 2})\right\}$ e as operações binárias são definidas por:

$$(a + b\sqrt{p}) + (c + d\sqrt{p}) := (a + c) + (b + d)\sqrt{p}$$
$$(a + b\sqrt{p}) \cdot (c + d\sqrt{p}) := (ac + pbd) + (ad + bc)\sqrt{p}.$$

Em particular, conclua que $\mathbb{Z}\left[\sqrt{p}\right]$ é um anel.

d) $2\mathbb{Z}$ com a soma usual e a operação binária $*$ definida por:

$$m * n := \frac{1}{2}mn.$$

e) $\mathbb{R}$ com as operações binárias θ e θ' definidas por:

$$x\theta y := x + y \quad \text{e} \quad x\theta' y := 2xy.$$

f) $A := \{(x, 1) \in \mathbb{R}^2 : x \in \mathbb{R}\}$ e as operações θ e θ' definidas por:

$$(x, 1)\theta(x', 1) := (x + y, 1) \quad \text{e} \quad (x, 1)\theta'(x', 1) := (xy, 1).$$

g) $\{a, b\}$ com as operações binárias "+" e "·" definidas através das seguintes tabelas:

$+$	a	b
a	a	b
b	b	a

e

$\cdot$	a	b
a	a	a
b	a	b

.

1.1.4) Seja $(R; +, 0_R)$ um grupo abeliano no qual se introduz a operação binária "·" definida para todo o $a, b \in R$ por $a \cdot b = 0_R$. Mostre que R é um anel e verifique se este anel tem identidade.

1.1.5) Sejam R um anel (resp., anel unitário) e X um conjunto qualquer.

a) Mostre que R^X é um anel (resp., anel unitário) para as operações usuais de adição e multiplicação de funções, ou seja, para todo o $x \in X$:

$$(f+g)(x) := f(x)+g(x) \quad \text{e} \quad (f \cdot g)(x) := f(x) \cdot g(x).$$

b) Indique condições para que R^X seja um anel comutativo.

c) Mostre que, se $X := R$, então R^R é um anel (resp., anel unitário).

d) Mostre que, em particular, o conjunto de todas as funções reais de variável real, i.e., $\mathbb{R}^{\mathbb{R}}$ é um anel unitário comutativo. Estude ainda como caso particular o conjunto $\mathbb{R}^{[a,b]}$, onde $[a,b] \subseteq \mathbb{R}$.

1.1.6) Sejam $(R; +_R, \cdot_R, 0_R)$ e $(S; +_S, \cdot_S, 0_S)$ (resp., $(R; +_R, \cdot_R, 0_R, 1_R)$ e $(S; +_S, \cdot_S, 0_S, 1_S)$ anéis unitários) e $R \times S$ o produto cartesiano de R e S.

a) Mostre que $R \times S$ é um anel (resp., anel unitário) se definirmos as seguintes operações binárias:
$\forall a_1, a_2 \in R$, $\forall b_1, b_2 \in S$,

$$(a_1, b_1) + (a_2, b_2) := (a_1 +_R a_2, b_1 +_S b_2) \quad \text{e} \quad (a_1, b_1) \cdot (a_2, b_2) := (a_1 \cdot_R a_2, b_1 \cdot_S b_2).$$

Este anel (resp., anel unitário) é o produto cartesiano dos anéis R e S e é também conhecido por produto directo (externo) dos anéis R e S.

b) Generalize para o produto cartesiano de n anéis (resp., anéis unitários) distintos.

Conclua que, em particular, $R^n := \overbrace{R \times R \times \cdots \times R}^{n}$ é um anel (resp., anel unitário).

1.1.7) Seja R um anel. Mostre que para todo o $a, a_1, ..., a_n, b_1, b_2, ..., b_n \in R$ tem-se que:

a) $a(b_1 + b_2 + \cdots + b_n) = ab_1 + ab_2 + \cdots + ab_n$.

b) $(b_1 + b_2 + \cdots + b_n)a = b_1 a + b_2 a + \cdots + b_n a$.

c) $\left(\sum\limits_{i=1}^{n} a_i\right)\left(\sum\limits_{j=1}^{m} b_j\right) = \sum\limits_{i=1}^{n}\sum\limits_{j=1}^{m} a_i b_j$.

1.1.8) Sejam R um anel e $a, b, c \in R$.

a) Mostre que para o grupo aditivo do anel tem-se que:

1) O elemento neutro aditivo do anel, 0_R, é único.
2) Cada elemento de R tem um único simétrico.
3) $-(-a) = a$.
4) $-(a+b) = (-a) + (-b)$.
5) Se $a + b = a + c$, então $b = c$ (analogamente, $b + a = c + a$, então $b = c$).
6) Cada uma das equações $a + x = b$ e $x + a = b$ tem uma única solução.

b) Mostre que para o semigrupo multiplicativo do anel tem-se que:

1) $0_R a = a 0_R = 0_R$.
2) Se o anel tem elemento unidade 1_R, então $(-1_R)a = -a$.
3) $a(-b) = (-a)b = -(ab)$.

4) $(-a)(-b) = ab$.
5) $a(b-c) = ab - ac$ e $(b-c)a = ba - ca$.

1.1.9) Prove que num anel R são válidas as seguintes regras usuais da aritmética, para todo o $m, n \in \mathbb{Z}$ e $a, b \in R$:

a) $(m+n)a = ma + na$.
b) $(mn)a = m(na)$.
c) $m(a+b) = ma + mb$.
d) $n(ab) = (na)b = a(nb)$.
e) $(ma)(nb) = (mn)ab$.

1.1.10) Prove que num anel R com elemento unidade são válidas as seguintes regras usuais da aritmética, para todo o $m, n \in \mathbb{N}$ e $a, b \in R$:

a) $a^n a^m = a^{n+m}$.
b) $(a^n)^m = a^{nm}$.
c) Se a e b comutam, então $(ab)^n = a^n b^n$.
d) Se a e b comutam, então $a^m b^n = b^n a^m$.

1.1.11) Sejam R um anel e $a, b \in R$ elementos permutáveis. Mostre que se tem:

a) $a(-b) = (-b)a$.
b) $(-a)(-b) = (-b)(-a)$.
c) $(a+b)^n = a^n + \binom{n}{1}a^{n-1}b + \binom{n}{2}a^{n-2}b^2 + \cdots + \binom{n}{n-1}ab^{n-1} + b^n$, onde $\binom{n}{k} := \frac{n!}{k!(n-k)!}$.

1.1.12) Sejam R um anel e $a, b \in R$. Mostre que:

a) $a^2 - b^2 = (a+b)(a-b)$ se, e só se, R é comutativo.
b) $a^2 - b^2 = (a-b)(a+b)$ se, e só se, R é comutativo.

1.1.13) Sejam R um anel (resp., anel unitário) e $A \subseteq R$. Mostre que A é um subanel (resp., subanel unitário) de R se, e só se, verifica o seguinte:

i) $0_R \in A$ (resp., $1_R \in A$);
ii) $\forall x, y \in R : x, y \in A \Rightarrow x + (-y) \in A$;
iii) $\forall x, y \in R : x, y \in A \Rightarrow xy \in A$.

1.1.14) Verifique nas alíneas seguintes se os subconjuntos são subanéis do respectivo anel e, indique, os que são comutativos e os que tem identidade:

a) Considere o anel $\mathbb{R}^{[a,b]}$ e o subconjunto $A := \left\{ f \in \mathbb{R}^{[a,b]} : f(b) = 0 \right\}$.
b) Considere o anel $\mathbb{R}^{\mathbb{R}}$ e o subconjunto $C(\mathbb{R}, \mathbb{R})$ de todas as funções contínuas reais de variável real.
c) Considere o anel $(M_{2\times 2}(\mathbb{Z}); +, \cdot, O_{2\times 2})$ e os seguintes subconjuntos dele:

1) $\left\{ \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in M_{2\times 2}(\mathbb{Z}) : c = d = 0 \right\}$.

2) $\left\{ \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in M_{2\times2}(\mathbb{Z}) : c = 0 \right\}$.

3) $\left\{ \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in M_{2\times2}(\mathbb{Z}) : b = c = 0 \right\}$.

4) $\left\{ \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in M_{2\times2}(\mathbb{Z}) : b = d = 0 \right\}$.

5) $\left\{ \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in M_{2\times2}(\mathbb{Z}) : b = c = 0 \wedge d = 1 \right\}$.

1.1.15) Seja R um anel unitário. Mostre que:

a) $a, b \in U(R) \Rightarrow ab \in U(R)$.

b) $a^n \in U(R) \Rightarrow a \in U(R)$.

c) Se $a, b \in U(R)$, então não necessariamente se tem que $a + b \in U(R)$.

1.1.16) Determine:

a) $U(\mathbb{Z}_8)$.

b) $U(M_{2\times2}(\mathbb{Z}))$ (anel definido no exercício 1.1.3 com $R := \mathbb{Z}$ e $n := 2$).

c) $U\left(\mathbb{Z}\left[\sqrt{2}\right]\right)$ (anel definido no exercício 1.1.3 com $p := 2$).

1.1.17) Mostre que no anel $\mathbb{Z}_n$, tem-se que para todo o $n \in \mathbb{N} \setminus \{0, 1\}$, $\overline{n-1} \in U(\mathbb{Z}_n)$.

1.1.18) Seja $\mathbb{K}$ um corpo. Mostre que:

a) O conjunto $U(M_{n\times n}(\mathbb{K}))$, que se representa por:

$$GL_n(\mathbb{K}) := \{A \in M_{n\times n}(\mathbb{K}) : A \text{ é invertível}\}$$

é um subgrupo do monóide multiplicativo do anel unitário $M_{n\times n}(\mathbb{K})$.

b) O conjunto de todas as matrizes diagonais invertíveis, $\mathrm{Diag}(GL_n(\mathbb{K}))$, é um subgrupo de $GL_n(\mathbb{K})$.

1.1.19) Sejam R um anel (resp., anel unitário) e $A, B \sqsubseteq R$. Mostre que:

a) $A \cap B \sqsubseteq R$, i.e, a intersecção de dois subanéis (resp., subanéis unitários) de R ainda é um subanel (resp., subanel unitário) de R.
Generalize para uma família infinita $(A_i)_{i\in I}$ de subanéis de R.

b) $A \cup B \sqsubseteq R \Leftrightarrow A \subseteq B \vee B \subseteq A$, i.e., a união de dois subanéis (resp., subanéis unitários) de R ainda é um subanel (resp., subanel unitário) de R se, e só se, um deles está contido no outro.

c) Se $A \cdot B \subseteq A \ \wedge \ B \cdot A \subseteq B \Rightarrow A + B \sqsubseteq R$, i.e., a soma de dois subanéis (resp., subanéis unitários) de R é um subanel (resp., subanel unitário) de R se o produto deles está contido em ambos os factores.

d) Se $B \cdot A \subseteq A \cdot B \Rightarrow A \cdot B \sqsubseteq R$, i.e., o produto de dois subanéis (resp., subanéis unitários) de R é um subanel (resp., subanel unitário) de R se o produto do segundo pelo primeiro está contido no produto do primeiro pelo segundo.
Mostre que se tem a recíproca no caso de R ser anel unitário.

1.1.20) Sejam R um anel e $X \subseteq R$. Mostre que $\langle X \rangle$ é um subanel de R.

1.1.21) Sejam R um anel e $A \subseteq R$. O centralizador de A em R é definido como sendo o conjunto

$$C_R(A) := \{x \in R : \forall a \in A, \, ax = xa\}.$$

a) Mostre que o centralizador é um subanel de R.
No caso particular de $A := R$, chama-se centro do anel R e representa-se por:

$$Z(R) := \{x \in R : \forall r \in R, \, xr = rx\}.$$

b) Indique qual é o centro se o anel for comutativo.

1.1.22) Sejam $(R; +, \cdot, 0_R, 1_R)$ um anel unitário e $R^{op} := (R; +, \cdot^{op}, 0_R, 1_R)$, onde para todo o $x, y \in R$,

$$x \cdot^{op} y := y \cdot x.$$

Mostre que R^{op} é um anel unitário.
Ao anel unitário R^{op} chama-se anel oposto do anel R.

1.1.23) Diga, justificando, se é verdadeira ou falsa cada uma das seguintes afirmações:

a) Se A é subanel de um anel R que contém uma unidade b, então A contém b^{-1}.

b) Num anel de característica 2, qualquer elemento é simétrico de si próprio.

c) Um anel finito pode ter característica zero.

d) A característica de um anel é sempre um número primo.

e) A característica de um corpo é sempre um número primo.

1.2. Morfismos de anéis

1.2.1) Indique, quais das seguintes aplicações são morfismos de anéis e, em cada caso afirmativo, determine o respectivo núcleo e classifique o respectivo morfismo:

a) $f : \mathbb{Z} \to \mathbb{Z}$ definida por $f(a) := 3a$.

b) $f : \mathbb{Z} \to \mathbb{Z}$ definida por $f(a) := a^2$.

c) $f : \mathbb{Z}_6 \to \mathbb{Z}_3$ definida por $f([a]_6) := [a]_3$.

d) $f : \mathbb{C} \to \mathbb{R}$ definida por $f(z) := |z|$.

e) $f : \mathbb{C} \to \mathbb{R}$ definida por $f(z) := \mathrm{Re}(z)$.

f) $f : \mathbb{C} \to \mathbb{C}$ definida por $f(z) := iz$.

g) $f : \mathbb{C} \to \mathbb{C}$ definida por $f(z) := \overline{z}$.

h) $f : M_{n\times n}(\mathbb{R}) \to M_{n\times n}(\mathbb{R})$ definida por $f(A) := A^t$.

i) $f : M_{n\times n}(\mathbb{R}) \to \mathbb{R}$ definida por $f(A) := \det(A)$.

1.2.2) Sejam R, S anéis (resp., anéis unitários) e $f : R \to S$ um morfismo de anéis (resp., morfismos unitários). Mostre que:

a) f é injectiva se, e só se, f é um monomorfismo.

b) f é sobrejectiva, então f é um epimorfismo. Será que a recíproca é verdadeira?

1.2.3) Sejam $(R; +_R, \cdot_R, 0_R)$, $(S; +_S, \cdot_S, 0_S)$ anéis e $f : R \to S$ um morfismo de anéis. Mostre que:

a) $f(0_R) = 0_S$.

b) $f(-a) = -f(a)$.

c) $\forall n \in \mathbb{Z}, \forall a \in R,\ f(na) = nf(a)$.

d) Se $A \sqsubseteq R$, então $f^{\to}(A) \sqsubseteq S$.

e) Se $B \sqsubseteq S$, então $f^{\leftarrow}(B) \sqsubseteq R$.

f) $f \in \mathrm{Inj}(R, S)$ se, e só se, $\mathrm{Ker}(f) = \{0_R\}$.

1.2.4) Sejam R e S anéis (resp., anéis unitários). Mostre que:

a) $\mathrm{Mor}(R, S)$ não é um subanel do anel S^R para as operações "+" e "·" de morfismos.

b) $\mathrm{End}(R)$ não é um anel para as operações "+" e "·" de morfismos.

c) $\mathrm{Mor}(R, S)$ é um subanel do anel S^R para as operações "+" e "·" de funções (não de morfismos) (resp., anel unitário).
Em particular, quando $S := R$, então $\mathrm{End}(R)$ é um anel (resp., anel unitário).

1.2.5) Sejam R e S anéis e S é comutativo. Indique, condições, para que se tenha o seguinte:

a) $f, g \in \mathrm{Mor}(R, S)$, então $f + g \in \mathrm{Mor}(R, S)$.

b) $f, g \in \mathrm{Mor}(R, S)$, então $f \cdot g \in \mathrm{Mor}(R, S)$.

c) Com a(s) condição(ões) que deduziu será que $\mathrm{Mor}(R, S)$ é um anel, para as operações de "+" e "·" de morfismos de anéis?
Em particular, quando $S := R$, então $\mathrm{End}(R)$ é um anel.

1.2.6) Seja R um anel. Mostre que:

a) $(R^R; +, \circ, c_{0_R})$ não é um anel.

b) $(\mathrm{End}(R); +, \circ, c_{0_R})$ não é um anel.

1.2.7) Considere o grupo comutativo $(M; +, 0_M)$. Mostre que:

a) $(\mathrm{End}(M); +, \circ, c_{0_M}, \mathrm{id}_M)$ é um anel unitário, a que se chama o anel dos endomorfismos de M.

b) Se R é um anel (resp., anel unitário) e temos uma acção esquerda de R em M, então a relação $\rho : R \to \mathrm{End}({}_R M)$ definida por $\rho(r) := \rho_r$, onde para todo o $a \in M$, $\rho_r(a) := ra$, é um morfismo (resp., unitário) de anéis.
(Se $A \sqsubseteq \mathrm{End}({}_R M)$, então diz-se que $\rho : R \to A$ é uma representação do anel R em A.)

1.2.8) Mostre que as seguintes aplicações são morfismos e classifique-os:

a) $f : \mathbb{Z}\left[\sqrt{2}\right] \to \mathbb{Z}\left[\sqrt{2}\right]$ definida por $a + b\sqrt{2} \mapsto a - b\sqrt{2}$.

b) $f_n : (\mathbb{Z}; +, \cdot, 0) \to (\mathbb{Z}_n; +_n, \cdot_n, [0]_n)$, onde $n \in \mathbb{N}_{\neq 0}$ um elemento arbitrário mas fixo e definida por $x \mapsto [x]_n$.

c) $f : \mathbb{C} \to M_{2\times 2}(\mathbb{R})$ definida por $f(a + bi) = \begin{bmatrix} a & b \\ -b & a \end{bmatrix}$.

d) $f : M_{n\times n}(\mathbb{R}) \to M_{n\times n}(\mathbb{R})$ definida por $f(A) = P^{-1}AP$, onde $P \in U(M_{n\times n}(\mathbb{R}))$.

1.2.9) Sejam R, S e T anéis. Mostre que:

a) $R \cong R$.

b) Se $R \cong S$, então $S \cong R$.

c) Se $R \cong S$ e $S \cong T$, então $R \cong T$.

1.2.10) Sejam R e S anéis. Mostre que se $R \cong S$, então $\mathrm{char}(R) = \mathrm{char}(S)$.

1.2.11) Sejam R e S anéis (resp., anéis unitários). Mostre que para qualquer morfismo de anéis (resp., morfismo unitário) $f \in \mathrm{Mor}(R, S)$ tem-se que:

a) Se $A \sqsubseteq R$, então

$$f^{\leftarrow}(f^{\rightarrow}(A)) = A + \mathrm{Ker}(f) \quad \text{e} \quad \mathrm{Ker}(f) \subseteq A + \mathrm{Ker}(f).$$

Em particular, se $b := f(a) \in \mathrm{Im}(f)$, então $f^{\leftarrow}(\{b\}) = \{a\} + \mathrm{Ker}(f)$.

b) Se $B \sqsubseteq S$, então

$$f^{\rightarrow}(f^{\leftarrow}(B)) = B \cap \mathrm{Im}(f).$$

c) Se $g \in \mathrm{Mor}(S, T)$, então

$$\mathrm{Ker}(g \circ f) = f^{\leftarrow}(\mathrm{Ker}(g)) \quad \text{e} \quad \mathrm{Im}(g \circ f) = g^{\rightarrow}(\mathrm{Im}(f)).$$

1.2.12) Sejam R, S anéis e $f : R \to S$ um isomorfismo de anéis. Prove que:

a) R é comutativo se, e só se, S é comutativo.

b) R tem identidade 1_R se, e só se, S tem identidade $f(1_R)$.

c) $a \in U(R)$ se, e só se, $f(a) \in U(S)$.

d) R é corpo se, e só se, S é corpo.

1.2.13) Mostre que não existe nenhum isomorfismo (de anéis) entre os anéis $(\mathbb{Z}; +, \cdot, 0)$ e $(2\mathbb{Z}; +, \cdot, 0)$.

1.3. Ideais

1.3.1) Sejam R um anel, $A \sqsubseteq R$ e $I \trianglelefteq R$. Mostre que:

a) $\{0_R\}$ e o próprio anel R são ideais de R.

b) Se $I \subseteq A$, então $I \trianglelefteq A$.

1.3.2) Sejam R um anel unitário e $I \trianglelefteq R$. Mostre que as seguintes condições são equivalentes:

i) $1_R \in I$. ii) I contém uma unidade. iii) $I = R$.

1.3.3) Sejam R um anel, $A \sqsubseteq R$ e $I, J \trianglelefteq R$. Mostre que:

a) $A + I \sqsubseteq R$.

b) $I \cap A \trianglelefteq A$.

c) Se $I \subseteq A$, então $I \trianglelefteq A$.

1) $A \cdot I \trianglelefteq_l R$ (resp., $I \cdot B \trianglelefteq_r R$).

2) Se R é um anel comutativo, então $I \cdot A \trianglelefteq R$ (resp., $A \cdot I \trianglelefteq R$).

d) Se $I, J \subseteq A$, então $I + J \trianglelefteq A$.

1.3.4) Sejam R um anel e $I, J \trianglelefteq R$. Mostre que:

a) $I + J \trianglelefteq R$.

b) $I \cdot J \trianglelefteq R$.

c) $I \cap J \trianglelefteq R$.
Generalize para uma família (finita ou infinita) de ideais de R.

1.3.5) Sejam R um anel e $I, J, K \trianglelefteq R$. Mostre que se tem:

a) $I + (0_R) = (0_R) + I = I$.

b) $I + (J + K) = (I + J) + K$.

c) $I \cdot (J \cdot K) = (I \cdot J) \cdot K$.

d) $I \cdot (J + K) = (I \cdot J) + (I \cdot K)$ e $(I + J) \cdot K = (I \cdot K) + (J \cdot K)$.

e) $I \cdot (J \cap K) \subseteq (I \cdot J) \cap (I \cdot K)$.

f) Se $J \subseteq I$, então $I \cap (J + K) = J + (I \cap K)$.

1.3.6) Sejam R um anel e $X, Y \subseteq R$. Mostre que:

a) $X \subseteq (X)$.

b) $X \subseteq Y \Longrightarrow (X) \subseteq (Y)$.

1.3.7) Seja R um anel unitário comutativo. Determine:

a) (1_R) e (0_R).

b) (u), onde $u \in U(R)$.

1.3.8) Sejam R um anel unitário e $a, b \in R$. Mostre que:

a) Se $a, b \in Z(R)$, então $(a \cdot b) = (a) \cdot (b)$.

b) $(\{a,b\}) = (a) + (b)$.

c) $(\{a\} \times \{b\}) \subseteq (a) \times (b)$.

1.3.9) Seja $\mathcal{I}(R)$ o conjunto de todos os ideais do anel $(R; +, \cdot, 0_R)$. Classifique $\mathcal{I}(R)$ como estrutura algébrica, relativamente às operações de soma e produto de ideais de R.

1.3.10) Sejam R um anel e $A \in \mathcal{P}(R)$. Os conjuntos

$$\mathrm{Ann}^l_R(A) := \{r \in R : \forall a \in A,\ ra = 0_R\} \text{ e } \mathrm{Ann}^r_R(A) := \{r \in R : \forall a \in A,\ ar = 0_R\}$$

chamam-se, respectivamente, anulador esquerdo e anulador direito de A em R. Mostre que:

a) $\mathrm{Ann}^l_R(A) \trianglelefteq R$.

b) $\mathrm{Ann}^r_R(A) \trianglelefteq R$.

c) Se $A \trianglelefteq R$, então $\mathrm{Ann}^l_R(A)$ e $\mathrm{Ann}^r_R(A)$ são ambos ideais (bilaterais) de R.

d) Se R é um anel unitário, então $\mathrm{Ann}^l_R(A) = \mathrm{Ann}^r_R(A) = \{0_R\}$.

1.3.11) Sejam R um anel e $a, b \in R$. Mostre que $(\{a,b\}) = (a) + (b)$.
Generalize para $\{x_1, x_2, \ldots, x_n\} \subseteq R$, i.e., $(\{x_1, x_2, \ldots, x_n\}) = (x_1) + (x_2) + \cdots + (x_n)$.

1.3.12) Sejam R um anel e $a \in R$.

a) Prove que $(a)_R \trianglelefteq_r R$ (resp., ${}_R(a) \trianglelefteq_l R$).

b) Mostre que é o menor (no sentido de contido) ideal direito (resp., esquerdo) que contém o elemento a.

c) Se a é um elemento idempotente, então $a \in (a)_R$.

d) Se R tem identidade, então $a \in (a)_R$.

e) Se $I \trianglelefteq R$ tal que $a \in I$, então ${}_R(a) \subseteq I$.

1.3.13) Seja R um anel. Mostre que para qualquer elemento $a \in R$ tem-se que:

a) $(a) = \left\{ na + at + pa + \sum_{i=1}^{k} r_i a s_i \in R : n \in \mathbb{Z},\ t, p, r_i, s_i \in R,\ k \in \mathbb{N}_{\neq 0} \right\}$.

b) Dê um aspecto mais simplificado no caso de R ser um anel unitário.

1.3.14) Mostre que para qualquer anel unitário R e $a \in R$ tem-se que:

$$(a) = \left\{ \sum_{i=1}^{k} r_i a s_i \in R : s_i, r_i \in R,\ k \in \mathbb{N}_{\neq 0} \right\} = RaR.$$

1.3.15) Seja R um anel comutativo. Mostre que:

a) $\forall a \in R,\ (a) = (a)_R = {}_R(a)$.

b) se $I, I' \trianglelefteq R$ tais que $I + I' = R$, então $I \cap I' = I \cdot I'$.

c) $Z(R) = R$. O que conclui quanto à recíproca, i.e., se $Z(R) = R$, então R é um anel comutativo?

1.3.16) Considere o anel unitário $(M_{2\times 2}(\mathbb{Z}); +, \cdot, O_{2\times 2}, I_{2\times 2})$.

a) Determine $Z\left(M_{2\times 2}\left(\mathbb{Z}\right)\right)$.

b) Será que $Z\left(M_{2\times 2}\left(\mathbb{Z}\right)\right) \trianglelefteq M_{2\times 2}\left(\mathbb{Z}\right)$?

1.3.17) Prove que no anel dos inteiros $(\mathbb{Z};+,\cdot,0,1)$ todo o ideal é principal.

1.3.18) Mostre que para todo o $n \in \mathbb{N}$, o conjunto $n\mathbb{Z} := \{nk \in \mathbb{Z} : k \in \mathbb{Z}\}$ é ideal de $(\mathbb{Z};+,\cdot,0,1)$.

1.3.19) Em $\mathbb{Z}$, determine os seguintes ideais indicando qual o seu gerador:

a) $(2)+(5)$. b) $(2)+(6)$. c) $(2)\cap((5)+(6))$.
d) $(2)\cdot((5)\cap(6))$. e) $(8)\cap(12)$. f) $(8)\cdot(12)$.

1.3.20) Determine todos os ideais do anel unitário $\left(\mathbb{Z}_n;+,\cdot,\overline{0}_n,\overline{1}_n\right)$ no seguintes casos:

a) $n=4$.

b) $n=11$.

c) $n=12$.

d) $n=6$, mas somente para $\left(\overline{4}_6\right)$ e $\left(\overline{3}_6\right)$.

1.3.21) Considere os seguintes subconjuntos de matrizes em $(M_{2\times 2}(\mathbb{Z});+,\cdot,O_{2\times 2},I_{2\times 2})$:

$$B := \left\{\begin{bmatrix} a & b \\ c & d \end{bmatrix} \in M_{2\times 2}(\mathbb{Z}) : a=b=0\right\}. \quad C := \left\{\begin{bmatrix} a & b \\ c & d \end{bmatrix} \in M_{2\times 2}(\mathbb{Z}) : c=d=0\right\}.$$

$$D := \left\{\begin{bmatrix} a & b \\ c & d \end{bmatrix} \in M_{2\times 2}(\mathbb{Z}) : a=c=0\right\}. \quad E := \left\{\begin{bmatrix} a & b \\ c & d \end{bmatrix} \in M_{2\times 2}(\mathbb{Z}) : b=d=0\right\}.$$

a) Mostre que D e E são ideais esquerdos mas não direitos de $M_{2\times 2}(\mathbb{Z})$.

b) Mostre que B e C são ideais direitos mas não esquerdos de $M_{2\times 2}(\mathbb{Z})$.

c) Dê exemplos de subconjuntos de matrizes que não sejam nem ideais esquerdos nem direitos de $M_{2\times 2}(\mathbb{Z})$.

d) Determine em $M_{2\times 2}(\mathbb{Z})$, os elementos do ideal esquerdo do exercício 1.3.10.a), considerando para tal $A := \left\{\begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix}\right\}$.

1.3.22) Sejam R um anel, $X \subseteq R$, $I \trianglelefteq R$ e

$$C_R(X) := \{a \in R : \forall x \in X,\, ax = xa\}.$$

Mostre que:

a) $C_R(X) \sqsubseteq R$.

b) $X \subseteq C_R(X) \Leftrightarrow$ os elementos de X comutam.
Em particular, $Z(R) = R \Leftrightarrow R$ é comutativo.

c) $I \subseteq C_R(I) \Rightarrow C_R(I) \trianglelefteq I$.
Em particular, $Z(R) = R \Rightarrow Z(R) \trianglelefteq R$.

d) $I \subseteq C_R(I) \Leftrightarrow I$ é comutativo.

1.3.23) Sejam R, S anéis, $I, I' \trianglelefteq R$, $J \trianglelefteq S$ e $f : R \to S$ um morfismo de anéis. Mostre que:

a) $\mathrm{Ker}(f) \trianglelefteq R$.

b) Se $f \in \mathrm{Surj}(R, S)$, então $\mathrm{Im}(f) \trianglelefteq S$.

c) $f^{\rightarrow}(I) \trianglelefteq \mathrm{Im}(f)$.

d) Se $f \in \mathrm{Surj}(R, S)$, então $f^{\rightarrow}(I) \trianglelefteq S$.

e) $f^{\leftarrow}(J) \trianglelefteq R$.

f) $f^{\rightarrow}((a)_R) = (f(a))_{\mathrm{Im}(f)}$.

g) $f^{\rightarrow}(I + I') = f^{\rightarrow}(I) + f^{\rightarrow}(I')$.

h) $f^{\rightarrow}(I \cdot I') = f^{\rightarrow}(I) \cdot f^{\rightarrow}(I')$.

i) $f^{\rightarrow}(I \cap I') \subseteq f^{\rightarrow}(I) \cap f^{\rightarrow}(I')$, tem-se a igualdade se $\mathrm{Ker}(f) \subseteq I \vee \mathrm{Ker}(f) \subseteq I'$.

1.4. Relações de congruência. Anéis quociente

1.4.1) Sejam R um anel e ρ uma relação de congruência definida em R. Sendo $[0_R]_\rho$ a classe do zero, mostre que $[0_R]_\rho \trianglelefteq R$.

1.4.2) Sejam R um anel, ρ uma relação de congruência definida em R, $I \trianglelefteq R$ e $X \subseteq R$. Mostre que:

a) Se $[0_R]_\rho = I$, então $X = X + I$.

b) Se $[0_R]_\rho = I$ e $A \sqsubseteq R$, então $A = A + I$.

c) Se $J \trianglelefteq R$, então $J/\rho \trianglelefteq R/\rho$.

d) Se $A \sqsubseteq R$, então $A = A + I$ se, e só se, $I \subseteq A$.

1.4.3) Sejam R um anel (resp., anel unitário) e $I \trianglelefteq R$. Mostre que R/I é um anel (resp., anel unitário).

1.4.4) Sejam R um anel e $I \trianglelefteq R$. Mostre que:

a) se R é comutativo, então R/I é comutativo.

b) se R tem identidade, então R/I tem identidade.

c) se R é domínio, então R/I não é necessariamente um domínio.

1.4.5) Sejam R um anel e $I \trianglelefteq R$. Mostre que R/I é comutativo se, e só se, para todo o $a, b \in R$, $ab - ba \in I$.

1.4.6) Sejam R, R' anéis (ou anéis unitários) e $I \trianglelefteq R$. Mostre que:

a) A relação $\nu : R \to R/I$ é um morfismo sobrejectivo.

b) Se $I \subseteq \mathrm{Ker}(f)$, então para todo o morfismo $f : R \to R'$, existe um morfismo $g : R/I \to R'$ tal que o seguinte diagrama

$$\begin{tikzcd} R \arrow[r, "\nu"] \arrow[d, "f"'] & R/I \arrow[dl, "g"] \\ R' & \end{tikzcd}$$

é comutativo.

Mostre ainda que, nestas condições:

1) $I = \mathrm{Ker}(f)$ se, e só se, $g \in \mathrm{Inj}(R/I, R')$.

2) $f \in \mathrm{Surj}(R, R')$ se, e só se, $g \in \mathrm{Surj}(R/I, R')$.

3) $\mathrm{Coim}(f) \cong \mathrm{Im}(f)$.

1.4.7) Sejam R um anel e $f \in \mathrm{Surj}\,(\mathbb{Z}, R)$. Mostre que, $\mathbb{Z}_n \cong R$.

1.4.8) Considere a relação $f : \mathbb{Z}_{12} \to \mathbb{Z}_4$, definida por $f\,(\overline{a}_{12}) := \overline{a}_4$.

a) Mostre que f assim definida é uma aplicação.

b) Verifique que f é um morfismo de anéis.

c) Verifique que $\mathbb{Z}_{12}/\left(\overline{4}_{12}\right) \cong \mathbb{Z}_4$.

d) Construa as tabelas de Cayley para o anel $\mathbb{Z}_{12}/\left(\overline{4}_{12}\right)$.

1.4.9) Sejam R um anel e $I, J \trianglelefteq R$ tais que $I \subseteq J$. Mostre que:

a) $I \trianglelefteq J$.

b) $J/I \trianglelefteq R/I$.

c) Será que todos os ideais de R/I são da forma J/I nas condições do enunciado?

1.4.10) (2.º teorema do isomorfismo) Sejam R um anel e $I, J \trianglelefteq R$ tais que $I \subseteq J$. Seja $f : R/I \longrightarrow R/J$ a relação definida por $f\left([a]_I\right) = [a]_J$. Mostre que:

a) f é uma aplicação.

b) f é um morfismo de anéis.

c) $\mathrm{Ker}(f) = J/I$.

d) f é sobrejectiva.

e) Conclua, usando o teorema do homomorfismo, que $\frac{R/I}{J/I} \cong R/J$.

1.5. Divisores de zero. Domínios

1.5.1) Considere o anel unitário $(M_{2\times 2}(\mathbb{Z}_3);+,\cdot,O_{2\times 2},I_{2\times 2})$, com a soma e o produto usuais de matrizes e, seja $A := \left\{ \begin{bmatrix} \overline{a}_3 & \overline{b}_3 \\ \overline{c}_3 & \overline{d}_3 \end{bmatrix} \in M_{2\times 2}(\mathbb{Z}_3) : \overline{c}_3 = \overline{0}_3 \right\}$.

a) Verifique se $M_{2\times 2}(\mathbb{Z}_3)$ é um domínio.

b) Mostre que A é um subanel de $M_{2\times 2}(\mathbb{Z}_3)$ e verifique se $A \trianglelefteq M_{2\times 2}(\mathbb{Z}_3)$.

c) Determine a característica de $M_{2\times 2}(\mathbb{Z}_3)$.

1.5.2) Verifique se as seguintes estruturas algébricas são domínios de integridade.

a) $\left(\mathbb{R}^{\mathbb{R}};+,\cdot,c_{0_{\mathbb{R}}}\right)$.
Será que o subanel $(C(\mathbb{R},\mathbb{R});+,\cdot,c_{0_{\mathbb{R}}})$ é um domínio de integridade?

b) $\mathbb{R}^{[a,b]}$.

c) $\left(\mathbb{Z}\left[\sqrt{2}\right];+,\cdot,0_{\mathbb{Z}\left[\sqrt{2}\right]}\right)$.

1.5.3) Considere o anel $\mathbb{R}^2$ onde estão definidas as operações binárias θ e θ' definidas por:

$$(x,y)\theta(z,t) := (x+z,y+t) \quad \text{e} \quad (x,y)\theta'(z,t) := (xz+4yt,xt+yz).$$

Averigúe se o anel tem divisores de zero.

1.5.4) Sejam R um anel sem elemento identidade esquerdo (resp., direito) e $b \in R_{\neq 0}$ um elemento idempotente. Mostre que b é um divisor de zero esquerdo (resp., direito).

1.5.5) Indique um anel R e elementos $a,b,c \in R_{\neq 0}$ para os quais se tem $ab = ac$ mas, não obrigatoriamente, $b = c$.

1.5.6) Determine os divisores de zero dos seguintes conjuntos:

a) $\mathbb{Z}_4$.

b) $\mathbb{Z}_{10}$.

c) $\mathbb{Z}\times\mathbb{Z}$.

1.5.7) Mostre que um anel unitário $R \neq \{0_R\}$ no qual se tem $\forall a \in R_{\neq 0},\ aR = R$ é um domínio.

1.5.8) Prove que um anel unitário $R \neq \{0_R\}$ é um domínio se, e só se, qualquer um dos seus elementos diferentes de zero é simplificável.

1.5.9) Seja R um anel. Mostre que R é um domínio se, e só se, $(R_{\neq 0};\cdot,1_R)$ é um monóide.

1.5.10) Prove que se R é um domínio, então é válida a lei do corte para o produto no monóide multiplicativo $(R_{\neq 0};\cdot,1_R)$.

1.5.11) Mostre que um anel R é um domínio se, e só se, a solução (admitindo que ela existe) de qualquer equação do tipo $ax = b$ (ou $xa = b$), com $a \neq 0_R$, é única.

1.5.12) Considere no anel $M_{2\times 2}(\mathbb{C})$, o subconjunto $H := \left\{ \begin{bmatrix} a-di & c+bi \\ -c+bi & a+di \end{bmatrix} \in M_{2\times 2}(\mathbb{C}) : a,b,c,d \in \mathbb{R} \right\}$ e as seguintes matrizes:

$$I := \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, \quad J := \begin{bmatrix} 0 & i \\ i & 0 \end{bmatrix}, \quad K := \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix}, \quad \text{e} \quad L := \begin{bmatrix} -i & 0 \\ 0 & i \end{bmatrix}.$$

Verifique que:

a) $\pm I, \pm J, \pm K, \pm L \in H$.

b) $J^2 = K^2 = L^2 = -I$.

c) $JK = L$.

d) $KL = J$.

e) $LJ = K$.

f) $KJ = -L$.

g) $LK = -J$.

h) $JL = -K$.

i) $H = \{aI + bJ + cK + dL \in M_{2\times 2}(\mathbb{C}) : a,b,c,d \in \mathbb{R}\}$.

j) H é fechado para a adição e multiplicação de matrizes.
Conclua que, $(H; +, \cdot, O_{2\times 2}, I_{2\times 2})$ é um anel unitário.

k) $\forall A \in H$, $\det(A) \neq 0 \iff A \neq O_{2\times 2}$.

l) H é um anel de divisão.

1.5.13) Sejam R um anel unitário, S um submonóide do monóide multiplicativo de R e todo o elemento de S não é divisor de zero em R, ou seja, para todo o $s \in S$ e para todo o $r \in R_{\neq 0}$, $rs \neq 0_R$ e $sr \neq 0_R$. Considere a seguinte relação $\sim$ em $R \times S$ definida por:

$$(a,s) \sim (b,s') \iff \exists t \in S : t(s'a - sb) = 0_R.$$

a) Mostre que $\sim$ é uma relação de equivalência em $R \times S$.

b) Defina-se em $\frac{R\times S}{\sim}$ as seguintes relações:

$$\frac{a}{s} + \frac{b}{s'} := \frac{(as' + sb)}{ss'} \qquad \text{e} \qquad \frac{a}{s} \cdot \frac{b}{s'} := \frac{ab}{ss'},$$

onde $\frac{a}{s} := [(a,s)]$. Mostre que:

1) As relações dadas são operações binárias em $\frac{R\times S}{\sim}$.

2) O conjunto $\mathrm{Frac}_R(R,S) := \frac{R\times S}{\sim}$ é um anel unitário. Ao anel unitário $\mathrm{Frac}_R(R,S)$, chama-se o anel das fracções direito de R com respeito a S.

3) Se R é um domínio, então a relação $\sim$ reduz-se a

$$(a,s) \sim (b,s') \iff s'a = sb.$$

Conclua que, se R for um domínio, então $\mathrm{Frac}_R(R,S)$ é um domínio.

4) Se R é um domínio de integridade, então $\mathrm{Frac}_R(R, R_{\neq 0})$ é um corpo. A este corpo chama-se o corpo das fracções clássico.
No caso particular do domínio de integridade $R := \mathbb{Z}$ e $S := \mathbb{Z}_{\neq 0}$ define-se $\mathbb{Q} := \frac{\mathbb{Z}\times\mathbb{Z}_{\neq 0}}{\sim}$.

5) A relação $v : R \to \mathrm{Frac}_R(R,S)$ definida por $v(a) := [(a, 1_R)]$ é um morfismo unitário injectivo tal que para todo o $s \in S$, $v(s)$ é invertível.

   i) $\mathrm{Im}(v) = \mathrm{Frac}_R(R, \{1_R\})$.

   ii) $R \cong \mathrm{Frac}_R(R, \{1_R\})$.

6) Se $f : R \to R'$ é um morfismo de anéis unitários tal que para todo $s \in S$, $f(s)$ é um elemento invertível, então existe um e um só morfismo $g : \mathrm{Frac}_R(R,S) \to R'$ tal que o seguinte diagrama

$$\begin{tikzcd} R \arrow[r, "v"] \arrow[d, "f"'] & \mathrm{Frac}_R(R,S) \arrow[dl, "g"] \\ R' & \end{tikzcd}$$

   é comutativo.

   Ao par $(\mathrm{Frac}_R(R,S), v)$ chama-se localização de R em S.

7) $\mathrm{Ker}(g) = \mathrm{Frac}_R(\mathrm{Ker}(f), S)$.

1.5.14) Seja R um anel unitário comutativo. Prove que:

a) Se $u \in U(R)$, então u não é divisor de zero.

b) O produto de um divisor de zero por qualquer outro elemento de R ou é nulo ou é um divisor de zero.

c) Se o produto de dois elementos de R é um divisor de zero, então algum dos factores o é.

1.5.15) No anel $\mathbb{Z}_n$, mostre o seguinte:

a) Se $[a]_n \neq [0]_n$, então $[a]_n \in U(\mathbb{Z}_n) \Leftrightarrow \gcd(a,n) = 1$.

b) $\mathrm{Zdiv}(\mathbb{Z}_n) = (\mathbb{Z}_n \setminus \{[0]_n\}) \setminus U(\mathbb{Z}_n)$, ou seja, os divisores de zero são precisamente os elementos não nulos de $\mathbb{Z}_n$ que não são invertíveis.

c) Se $\mathbb{Z}_n$ não é domínio de integridade, então $n \in \mathbb{N} \setminus \{0, 1\}$ não é primo.

1.6. Anéis de divisão. Corpos

1.6.1) Seja $R \neq \{0_R\}$ um anel unitário e comutativo. Mostre que:

a) Se os únicos ideais de R são (0_R) e o próprio R, então R é corpo.

b) Se R é um corpo, então os únicos ideais de R são (0_R) e R.

c) Conclua que, se R é um corpo, então os únicos corpos quociente são $\frac{R}{R}$ e $\frac{R}{(0_R)}$.

1.6.2) Mostre que um anel $R \neq \{0_R\}$ é um anel de divisão se, e só se, para todo o $a \in R_{\neq 0}$ e para todo o $b \in R$ as equações $ax = b$ e $ya = b$ são solúveis.

1.6.3) Mostre que todo o domínio finito (resp., domínio de integridade finito) é um anel de divisão finito (resp., corpo finito).

1.6.4) Seja $R \neq \{0_R\}$ um anel. Mostre que, se para todo o $a \in R_{\neq 0}$, $aR = Ra = R$ se, e só se, R é um anel de divisão.

1.6.5) Mostre que um subconjunto A de um anel de divisão R é um subanel de divisão se, e só se, tem-se que:

i) $0_R, 1_R \in A$;

ii) $\forall a, b \in R : a, b \in A \Rightarrow a + (-b) \in A$;

iii) $\forall a, b \in R_{\neq 0} : a, b \in A \Rightarrow ab^{-1} \in A$.

1.6.6) Sejam R um anel de divisão e $a \in U(R)$. Verifique se a relação $f : R \to R$ definida por $f(x) := axa^{-1}$ é um automorfismo de anéis de divisão.

1.6.7) Sejam $\mathbb{K}$ um corpo, R anel e $f : \mathbb{K} \to R$ é um morfismo de anéis. Mostre que:

a) ou f é injectiva ou $f = c_{0_R}$.

b) Se $R := \mathbb{K}$ e $f \in \mathrm{Surj}\,(\mathbb{K}, \mathbb{K})$, então $f \in \mathrm{Aut}\,(\mathbb{K})$.

c) Se $R := \mathbb{K}$ e $\mathrm{card}\,(\mathbb{K}) < \aleph_0$, então $f \in \mathrm{Aut}\,(\mathbb{K})$.

d) Se $R := \mathbb{K}'$ é corpo, então $f \in \mathrm{Inj}(\mathbb{K}, \mathbb{K}')$. Em particular, $f \in \mathrm{Iso}(\mathbb{K}, \mathrm{Im}(f))$.

1.6.8) Mostre que, p é primo se, e só se, $\mathbb{Z}_p$ é um corpo.

1.7. Divisibilidade

1.7.1) Considere um anel unitário $R \neq \{0_R\}$ comutativo e principal. Mostre que:

a) Se $a, b \in R_{\neq 0}$ e $\gcd(a, b) = 1_R$, então $(\{a, b\}) = R$ e é único.

b) No anel $\mathbb{Z}$, o único ideal que contém 2 e 3 é $\mathbb{Z}$.

c) No anel $\mathbb{Z}$, se $m, n \in \mathbb{Z}_{\neq 0}$ e $\gcd(m, n) = 1$, então o único ideal que contém m e n é $\mathbb{Z}$.

1.7.2) Considere o anel $\mathbb{Z}$ e $a, b \in \mathbb{Z}$.

a) Mostre que, $(a) + (b) = (\gcd(a, b))$.

b) Mostre que, $(a) \cap (b) = (\operatorname{lcm}(a, b))$.

c) Dê uma nova interpretação às alíneas do exercício 1.3.19 na página 10.

1.7.3) Sejam R um anel unitário comutativo e $a, b \in R$. Mostre que:

a) $(a) \subseteq (b)$ se, e só se, existe um elemento $r \in R$ tal que $a = rb$.

b) Se R é um domínio de integridade, então $(a) = (b)$ se, e só se, existe $u \in U(R)$ tal que $a = ub$.

1.7.4) Mostre que se $n \in \mathbb{N} \setminus \{0, 1\}$, então (n) é ideal primo de $\mathbb{Z}$ se, e só se, n é um número primo.

1.7.5) Sejam $R \neq \{0_R\}$ um anel unitário comutativo, $I \trianglelefteq R$ e $I \neq R$. Mostre que R/I é um domínio de integridade se, e só se, I é um ideal primo.

1.7.6) Sejam $R \neq \{0_R\}$ um anel, $I \trianglelefteq R$ e $I \neq R$. O ideal I diz-se um ideal maximal em R se $I \neq R$ e não existe nenhum ideal J, tal que $I \neq J$, $I \neq R$ e $I \subseteq J \subseteq R$. Mostre que se R é um anel unitário comutativo, R/I é um corpo se, e só se, I é um ideal maximal de R.

1.7.7) Sejam $R \neq \{0_R\}$ um anel unitário comutativo e I um ideal maximal de A. Mostre que I é um ideal primo.

1.7.8) Sejam $R \neq \{0_R\}$ um anel, D um domínio e $f : R \to D$ um morfismo de anéis não nulo. Prove que $\operatorname{Ker}(f)$ é um ideal primo de R.

2. Anéis de polinómios

2.1. Polinómios numa indeterminada

2.1.1) Mostre que os polinómios constantes em $\mathbb{Z}[x]$ formam um subanel dele que não é ideal.

2.1.2) Mostre que:

a) Se R é um anel (resp., anel unitário), então $R[x]$ é um anel (resp., anel unitário).
b) Se R é um anel (resp., anel unitário) comutativo, então $R[x]$ é um anel (resp., anel unitário) comutativo.

2.1.3) Simplifique cada uma das seguintes expressões (resp., das expressões correspondentes), no anel $\mathbb{Z}[x]$ (resp., no anel $\mathbb{Z}_2[x]$, $\mathbb{Z}_3[x]$ e $\mathbb{Z}_4[x]$):

a) $(1+2x)+(2-x+2x^2)$.
b) $(2x+x^3)+(x+2x^4)$.
c) $(1+2x)(2-x+2x^2)$.
d) $(2x+x^3)(x+2x^4)$.
e) $(2x+x^2)^3$.

2.1.4) Determine todos os polinómios de grau 2 nos seguintes anéis:

a) $\mathbb{Z}_2[x]$.
b) $\mathbb{Z}_3[x]$.

2.1.5) Em $\mathbb{Z}_n[x]$, e considerando $m \in \mathbb{N}$, determine:

a) Quantos polinómios existem de grau $\leq m$?
b) Quantos polinómios existem de grau m?
c) Quantos polinómios mónicos existem de grau m?

2.1.6) Sejam R e S anéis. Mostre que:

a) Se $I \trianglelefteq R$, então $I[x] \trianglelefteq R[x]$.
b) Se $R \cong S$, então $R[x] \cong S[x]$.
c) $\mathrm{char}(R[x]) = \mathrm{char}(R)$.
d) R é um domínio de integridade se, e só se, $R[x]$ é um domínio de integridade.

2.1.7) Seja R um anel unitário. Mostre que:

a) $a \in U(R) \Rightarrow p := a + 0_R x + \cdots \in U(R[x])$.
b) Se R é um domínio, então $a \in U(R) \Leftrightarrow p := a + 0_R x + \cdots \in U(R[x])$.
c) Se R não é um domínio, a equivalência anterior não necessariamente se verifica.
d) Se R é um domínio, então $U(R) = U(R[x])$.

2.2. Divisibilidade de polinómios

2.2.1) Sejam $a := -x^4 + 3x^2 + 2x + 1$ e $b := 2x^2 + 3x + 2$. Efectue, se possível, a divisão do polinómio (resp., polinómio correspondente) a por b nos anéis $\mathbb{Z}[x]$, $\mathbb{Q}[x]$ e $\mathbb{R}[x]$ (resp., no anel $\mathbb{Z}_2[x]$, $\mathbb{Z}_3[x]$ e $\mathbb{Z}_4[x]$).

2.2.2) Para cada um dos anéis $\mathbb{Z}[x]$, $\mathbb{R}[x]$ e $\mathbb{C}[x]$ (resp., no anel $\mathbb{Z}_2[x]$, $\mathbb{Z}_3[x]$ e $\mathbb{Z}_8[x]$), determine:

a) as raízes e respectivas multiplicidades dos polinómios (resp., polinómios correspondentes) a, b e c:

1) $a := x^4 - 1$.
2) $b := x^4 - 16$.
3) $c := x^8 - 256$.

b) (apenas no anel $\mathbb{Z}_8[x]$) as raízes dos polinómios a, b e b^2 sendo:

1) $a := x^2 + \overline{2}x$.
2) $b := x^2 + \overline{6}x + \overline{5}$.

2.2.3) No anel $\mathbb{Z}[x]$, mostre que é possível efectuar a divisão do polinómio $a := 4x^2 + 2x - 1$ pelo polinómio $b := 2x+1$. Este facto contradiz o teorema demonstrado sobre a divisão de polinómios?

2.2.4) No anel $\mathbb{Z}_9[x]$, considere os polinómios $p_1 := \overline{3}x + \overline{5}$ e $p_2 := \overline{6}x + \overline{3}$.

a) Determine, caso exista, um polinómio $q \in \mathbb{Z}_9[x]$, tal que $\deg(q) = 1$ e $p_1 q = 1$.
b) Determine, caso exista, um polinómio $q \in \mathbb{Z}_9[x]$, tal que $\deg(q) = 1$ e $p_2 q = 0$.

2.2.5) No anel $\mathbb{Z}_8[x]$, considere os polinómios $a := x^2 + \overline{2}x$ e $b := x^2 + \overline{6}x + \overline{5}$. Determine as raízes de a, b e b^2.

2.2.6) Mostre que, em $\mathbb{Z}_2[x]$, um polinómio a é divisível por $x - \overline{1}$ se, e só se, a tem um número par de coeficientes não nulos.

2.2.7) Determine qual a multiplicidade de -1, 1 e 0 como raízes do polinómio (resp., polinómio correspondente) $a := x^6 - x^2$ em $\mathbb{Z}[x]$, $\mathbb{R}[x]$ e $\mathbb{C}[x]$ (resp., no anel $\mathbb{Z}_2[x]$, $\mathbb{Z}_3[x]$ e $\mathbb{Z}_5[x]$):

a) $\mathbb{Z}_2[x]$. b) $\mathbb{Z}_3[x]$. c) $\mathbb{Z}_5[x]$.
d) $\mathbb{Z}[x]$. e) $\mathbb{R}[x]$. f) $\mathbb{C}[x]$.

2.2.8) No anel $\mathbb{R}[x]$, determine o número de raízes reais dos seguintes polinómios:

a) $x^3 - 3x + 5$.
b) $x^3 - 3x^2 + 2x - 1$.
c) $x^3 + 9x^2 - 1$.

2.2.9) No anel $\mathbb{Z}[x]$ determine, se existirem, as raízes racionais de:

a) $2x^3 - 3x + 4$.
b) $2x^4 - 4x + 3$.
c) $2x^3 + 4x^2 + 5x + 1$.
d) $\frac{3}{2}x^3 - 2x^2 + x + \frac{1}{2}$.

2.2.10) Determine para que elementos primos o polinómio $x^4 + x^3 + x^2 + x \in \mathbb{Z}_p[x]$, com p primo, admite a raiz $\overline{2}$.

2.2.11) Seja R um anel finito com k elementos. Determine, justificando, quantos polinómios de grau menor ou igual a n em $R[x]$ admitem a raiz zero.

2.2.12) Sejam R um domínio de integridade e $p := x^2 + bx + c \in R[x]$.

a) Mostre que, se p tem raízes x_1 e x_2, então $-(x_1 + x_2) = b$ e $x_1 x_2 = c$.

b) Encontre um resultado análogo ao da alínea anterior mas para um polinómio mónico de grau 3.

2.2.13) Seja $p := a_0 + a_1 x + \cdots + a_{n-1}x^{n-1} + a_n x^n \in \mathbb{Z}[x]$. Mostre que p admite a raiz $\frac{r}{s} \in \mathbb{Q}$, com $\gcd(r, s) = 1$ se, e só se, $sx - r$ divide p em $\mathbb{Z}[x]$.

2.2.14) Se R é um corpo e $a, b \in R[x]$, mostre que existe um único máximo divisor mónico entre a e b.

2.2.15) Em $\mathbb{R}[x]$, considere os seguintes polinómios:

$$p := x^4 - 2x^3 + 2x^2 - 2x + 1 \quad \text{e} \quad q := x^6 + 2x^5 - 2x^4 - 6x^3 - 7x^2 - 8x - 4.$$

Determine um máximo divisor comum de p e q e escreva-o na forma $ap + bq$, onde $a, b \in \mathbb{R}[x]$.

2.2.16) Em $\mathbb{Z}_2[x]$, considere os polinómios $p_1 := x^5 + \overline{1}$ e $p_2 := x^2 + \overline{1}$. Determine o máximo divisor comum de p_1 e p_2 e escreva-o na forma $ap_1 + bp_2$, onde $a, b \in \mathbb{Z}_2[x]$.

2.2.17) Em $\mathbb{Z}_3[x]$, considere os polinómios $p_1 := x^2 - x + \overline{1}$ e $p_2 := x^3 + \overline{2}x^2 + \overline{2}$. Determine todos os máximos divisores comuns de p_1 e p_2.

2.3. Irredutibilidade de polinómios

2.3.1) Sejam R e S anéis tais que $R \subseteq S$ e $p \in R[x]$. Diga, justificando, se é verdadeira ou falsa cada uma das afirmações:

a) Se $\deg(p) > 1$ e p admite uma raiz em R, então p é factorizável em R.

b) Se p é factorizável em R, então p admite uma raiz em R.

c) Se $\deg(p) = 1$, então p admite uma raiz em R.

d) Se R é um corpo e $\deg(p) = 1$, então p admite uma raiz em R.

e) Se p é irredutível em R também é irredutível em S.

f) Se p é factorizável em R também é factorizável em S.

g) Se p é factorizável em S também é factorizável em R.

2.3.2) Prove que se $\deg(p) > 1$ e p é irredutível em $\mathbb{Z}_2[x]$, então p tem termo independente 1 e um número ímpar de coeficientes não nulos.

2.3.3) Dê exemplos, se possível, de:

a) Um polinómio de grau 3, não factorizável, em $\mathbb{R}[x]$.

b) Um polinómio de grau 1, factorizável, em $\mathbb{Z}[x]$.

c) Um polinómio em $\mathbb{R}[x]$, não mónico, de grau 5, que admita como raízes reais apenas os números $\sqrt{5}$, -17 e $\dfrac{20}{3}$.

d) Um polinómio de grau 2, irredutível, em $\mathbb{R}[x]$.

e) Um polinómio de grau 2, irredutível, em $\mathbb{C}[x]$.

f) Um polinómio irredutível em $\mathbb{R}[x]$, mas redutível em $\mathbb{C}[x]$.

g) Um polinómio redutível em $\mathbb{R}[x]$, mas irredutível em $\mathbb{C}[x]$.

h) Um polinómio de grau 2 irredutível em $\mathbb{Q}[x]$, mas redutível em $\mathbb{R}[x]$.

2.3.4) Sejam R um corpo e $p \in R[x]$. Mostre que:

a) Se $\deg(p) = 2$, p é factorizável se, e só se, p tem uma raiz em R.

b) Se $\deg(p) = 3$, p é factorizável se, e só se, p tem uma raiz em R.

c) Verifique que se R não é corpo os resultados anteriores não são válidos.

2.3.5) Em $\mathbb{Z}_2[x]$, determine:

a) Todos os polinómios irredutíveis de grau 1.

b) Todos os polinómios irredutíveis de grau 2.

c) Todos os polinómios irredutíveis de grau 3.

d) Todos os polinómios irredutíveis de grau 4.

2.3.6) Em $\mathbb{Z}_3[x]$, determine:

a) Todos os polinómios irredutíveis de grau 1.

b) Todos os polinómios irredutíveis de grau 2.

2.3.7) Para p primo, quantos polinómios mónicos de grau 2, redutíveis, existem em $\mathbb{Z}_p[x]$?

2.3.8) Para p primo, quantos polinómios mónicos de grau 2, irredutíveis, existem em $\mathbb{Z}_p[x]$?

2.3.9) Determine em $\mathbb{R}[x]$ um polinómio p que satisfaça simultaneamente as seguintes condições e apresente-o, justificando, na forma do produto de factores irredutíveis em $\mathbb{R}[x]$:

a) O coeficiente director de p é 4.

b) $\deg(p) = 7$.

c) $2 - i\sqrt{3}$ é raiz de p.

d) A equação $p = 0$ admite as raízes 0 e $-\pi$.

e) p é divisível por $x^3 - 2x^2 + 3x - 6$.

2.3.10) Em $\mathbb{R}[x]$, considere o polinómio $p := x^7 + 2x^5 - 8x^3$. Decomponha-o em factores irredutíveis em $\mathbb{R}$, e indique as suas raízes reais e as respectivas multiplicidades.

2.3.11) Considere o polinómio $p := x^8 - 256$. Decomponha-o, justificando, em factores irredutíveis em:

a) $\mathbb{C}[x]$.

b) $\mathbb{R}[x]$.

2.3.12) Diga, justificando, se é verdadeira ou falsa cada uma das seguintes afirmações:

a) A divisão de polinómios é sempre possível em $\mathbb{Z}_{23}[x]$.

b) O polinómio $x^2 + x + 1$ divide $x^6 - 1$.

c) $(x^2 + 1)(x^2 + 2)$ é irredutível em $\mathbb{R}$.

d) O produto dos polinómios x^4 e x^6 em $\mathbb{Z}_7[x]$ é x^3.

e) $x^3 - 12x - 6$ tem apenas uma raiz real.

2.3.13) Se possível, dê exemplos de:

a) Um polinómio sem raízes em $\mathbb{R}$, factorizável em $\mathbb{Z}$.

b) Dois polinómios p e q em $\mathbb{R}[x]$ distintos, irredutíveis, tais que $p|q$.

c) Um elemento $m \in \mathbb{N}$ para o qual o polinómio $x^4 + x^3 + x^2 + x \in \mathbb{Z}_m[x]$ admita como divisores $x - \overline{2}$ e $x - \overline{1}$.

d) Um polinómio mónico associado de $\overline{2}x^5 - \overline{3}x^2 + \overline{1}$ em $\mathbb{Z}_7[x]$.

e) Dois polinómios distintos, associados em $\mathbb{Z}_8[x]$.

2.3.14) Diga quais dos seguintes polinómios são primitivos:

a) $p_1 := x^5 - 10x^4 + 40x^3 - 80x^2 + 80x - 32$.

b) $p_2 := 14x^{24} - 10x^{23} + 40x^{21} - 80x^{18} + 80x^{16} - 32x^{10} + 40x^8 - 80x^7 + 80x - 32$.

c) $p_3 := \frac{14}{23}x^{24} - \frac{10}{7}x^{23} + \frac{32}{5}x^{21} - 80x^{18} + 80x^{16} - 32x^{10} + 40x^8 - 80x^7 + 80x - 32$.

d) $p_4 := 48x^{10} - 45x^8 + 81x^6 - 63x^4 + 213x^2 - 51$.

2.3.15) Em $\mathbb{Z}[x]$, se possível dê exemplos de:

a) Um polinómio primitivo e redutível.

b) de um polinómio mónico, que admita como raízes os números 2, $-\dfrac{1}{3}$ e 0.

c) Um polinómio de grau 6 que admita a raiz -1 com multiplicidade 3, a raiz 4 com multiplicidade 2 e que seja múltiplo de $x^2 + 3x + 2$.

2.3.16) Em $\mathbb{Q}[x]$, se possível dê exemplos de:

a) Um polinómio de grau 2, irredutível e com coeficiente director 1.

b) Um polinómio de grau 5, irredutível e com coeficiente director 7.

2.3.17) Em $\mathbb{R}[x]$, se possível dê exemplos de:

a) Um polinómio de grau 3 redutível, que admita só duas raízes reais.

b) Um polinómio de grau 5 redutível, que admita só duas raízes reais.

2.3.18) Seja $p := \frac{7}{2}x^3 + \frac{7}{3}x^2 + \frac{14}{3}x + 7 \in \mathbb{Q}[x]$.

a) Determine um polinómio primitivo q em $\mathbb{Z}[x]$ associado a p.

b) Mostre que q é irredutível em $\mathbb{Z}[x]$ e em $\mathbb{Q}[x]$.

2.3.19) Considere o polinómio $p := 4x^3 + 4x - x - 2$.

a) Diga, justificando, se é verdadeira ou falsa cada uma das seguintes afirmações:

   1) p é primitivo.
   2) p é redutível em $\mathbb{Q}[x]$.
   3) p é irredutível em $\mathbb{Z}[x]$.

b) Decomponha p em factores irredutíveis em $\mathbb{R}[x]$.

2.3.20) Mostre que são irredutíveis em $\mathbb{Z}[x]$:

a) $x^4 + x + 1$.

b) $x^4 + 3x + 5$.

c) $3x^4 + 2x^3 + 4x^2 + 5x + 1$.

d) $x^5 + 5x^2 + 4x + 7$.

e) $15x^5 - 2x^4 + 15x^2 - 2x + 15$.

2.3.21) Diga, justificando, se é verdadeira ou falsa cada uma das afirmações:

a) Um polinómio primitivo em $\mathbb{Z}[x]$ é irredutível em $\mathbb{Q}[x]$.

b) Qualquer polinómio em $\mathbb{Z}[x]$ de grau positivo, que seja irredutível, é primitivo.

c) Um polinómio em $\mathbb{Z}[x]$ que não admita raízes racionais é irredutível em $\mathbb{Q}[x]$.

d) Um polinómio em $\mathbb{Z}[x]$ que admita raízes racionais é redutível em $\mathbb{Q}[x]$.

e) Um polinómio em $\mathbb{Z}[x]$ que admita raízes complexas é redutível em $\mathbb{Q}[x]$.

f) Um polinómio em $\mathbb{Z}[x]$ que admita uma raiz complexa $a + bi \in \mathbb{Q}[i]$ é redutível em $\mathbb{Q}[x]$.

2.3.22) Diga, justificando, se é verdadeira ou falsa cada uma das afirmações:

a) Seja R um anel unitário comutativo. Então:

1) Se p é um polinómio irredutível em $R[x]$, então para todo o $q \in R[x]$, pq também é irredutível em $R[x]$.
2) Se p é um polinómio redutível em $R[x]$, então para todo o $q \in R[x]$, pq também é redutível em $R[x]$.
3) Se p é um polinómio irredutível em $R[x]$, então existe um polinómio $q \in R[x]$ tal que pq ainda é irredutível em $R[x]$.

b) Sejam $q := a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0 \in \mathbb{Z}[x]$ e p um primo que não divide a_n. Então:

1) Se q é redutível em $\mathbb{Q}[x]$, então $f_{(p)}$ é redutível em $\mathbb{Z}_p[x]$.
2) Se $q_{(p)}$ é redutível em $\mathbb{Z}_p[x]$, então q é redutível em $\mathbb{Q}[x]$.
3) Se q é irredutível em $\mathbb{Q}[x]$, então $q_{(p)}$ é irredutível em $\mathbb{Z}_p[x]$.

c) Um polinómio $p \in \mathbb{Z}[x]$, no qual o coeficiente director é ímpar e para o qual, em $\mathbb{Z}_2[x]$, $p_{(2)} = x^2 + x + 1$, é irredutível em $\mathbb{Q}$.

2.3.23) Em $\mathbb{Q}[x]$, verifique se os seguintes polinómios são irredutíveis:

a) $3x^5 - 4x^4 + 2x^3 + x^2 + 18x + 31$.
b) $x^5 + 4x^4 + 2x^3 + 3x^2 - x + 5$.
c) $x^3 + 2x + 10$.
d) $x^3 - 2x^2 + x + 15$.
e) $x^5 - 21x^3 + 49x^2 + 7x - 14$.
f) $\frac{1}{6}x^3 - \frac{2}{3}x^2 + x + \frac{1}{2}$.
g) $\frac{4}{3}x^4 - 10x^3 + \frac{5}{9}x^2 + \frac{15}{2}x + \frac{1}{2}$.
h) $x^4 + 2x^3 - 6x + 2$.

2.3.24) No anel $\mathbb{Z}[x]$, considere o polinómio $p := x^7 + 2x^5 - 8x^3$.

a) Decomponha-o em factores irredutíveis como elemento de $\mathbb{R}[x]$ e, indique, as suas raízes reais e as respectivas multiplicidades.
b) Determine $\gcd(p, x^5 + 4x^3)$.

2.3.25) Se possível, dê exemplos de:

a) Um polinómio redutível, em $\mathbb{Z}_2[x]$, que seja máximo divisor comum de dois polinómios de graus 4 e 5.
b) Um polinómio p, de grau 5, mónico, irredutível em $\mathbb{Z}[x]$ e tal que $p_{(3)}$ que redutível em $\mathbb{Z}_3[x]$.
c) Um inteiro m para o qual o polinómio $x^4 + x^3 + x^2 + x \in \mathbb{Z}_m[x]$ admita como divisores $x - 2$ e $x - 1$.
d) Em $\mathbb{Z}[x]$, um polinómio mónico que admita como raízes os números -1, $\dfrac{1}{5}$ e 3.
e) Dois polinómios distintos, de grau 2 e irredutíveis em $\mathbb{Z}_2[x]$.

2.3.26) Seja $p := x^7 + 2x^6 - 2x^5 - 4x^4 + 6x^3 - 9x^2 + 9x - 3$.

a) Mostre que p é divisível por $x - 1$ em $\mathbb{Q}[x]$ e por $x - i$ em $\mathbb{C}[x]$.
b) Decomponha-o, justificando, em factores irredutíveis em $\mathbb{Q}[x]$ e diga se essa decomposição em factores irredutíveis é também válida em $\mathbb{R}[x]$.

2.3.27) Considere o polinómio $p := (x^8 - 9)(x^4 - 8x^2 + 16)$.

a) Decomponha-o, justificando, em factores irredutíveis em:

   1) $\mathbb{Z}[x]$.
   2) $\mathbb{R}[x]$.

b) Indique as suas raízes racionais, indicando as respectivas multiplicidades.

c) Em $\mathbb{Z}[x]$, determine $\gcd(p, x-7)$.

3. Módulos

3.1. Módulos e submódulos

3.1.1) Mostre que R é um anel unitário se, e só se, tem-se que:

a) ${}_RR$ é um R-módulo.

b) R_R é um módulo-R.

c) ${}_RR_R$ é um R-bimódulo-R.

3.1.2) Mostre que se R é um anel unitário comutativo, então todo o R-módulo (resp., módulo-R) é um módulo-R (resp., R-módulo).

3.1.3) Sejam R, S anéis unitários, $S \sqsubseteq R$ e ${}_RM$ um R-módulo. Mostre que ${}_SM$ é um S-módulo.

3.1.4) Sejam $\mathbb{K}$ um corpo (fixo) e V um espaço vectorial sobre $\mathbb{K}$. Mostre que:

a) Todo o espaço vectorial V sobre o corpo $\mathbb{K}$ é um $\mathbb{K}$-módulo.
Conclua que é um $\mathbb{K}$-bimódulo-$\mathbb{K}$.

b) Qualquer corpo $\mathbb{K}$ é um $\mathbb{K}$-módulo.
Conclua que, $\mathbb{Q}$ (resp., $\mathbb{R}$ e $\mathbb{C}$) é um módulo sobre $\mathbb{Q}$ (resp., $\mathbb{R}$ e $\mathbb{C}$).

3.1.5) Sejam ${}_RM$ um R-módulo e A um conjunto qualquer. Mostre que:

a) M^A é um R-módulo para a operação de adição de funções e operação binária externa definidas, para todo o $x \in A$ e $\alpha \in R$, por:

$$(f+g)(x) := f(x) + g(x) \quad \text{e} \quad (\alpha f)(x) := \alpha(f(x)).$$

b) Se $A := M$, então M^M é um R-módulo.

c) $\mathrm{End}(M)$ é um R-submódulo do módulo M^M.

d) Em particular, o conjunto de todas as funções reais de variável real, i.e., $\mathbb{R}^{\mathbb{R}}$ é um $\mathbb{R}$-módulo. Estude ainda como caso particular o conjunto $\mathbb{R}^{[a,b]}$.

3.1.6) Sejam $M_1, M_2, \ldots, M_n$, R-módulos. Considere o produto cartesiano $M_1 \times M_2 \times \cdots \times M_n$ munido das seguintes operações para todo o $(x_1, x_2, \ldots, x_n), (y_1, y_2, \ldots, y_n)$ elementos de $M_1 \times M_2 \times \cdots \times M_n$ e $\alpha \in R$:

$$\begin{aligned} (x_1, x_2, \ldots, x_n) + (y_1, y_2, \ldots, y_n) &:= (x_1 + y_1, x_2 + y_2, \ldots, x_n + y_n) \\ \alpha(x_1, x_2, \ldots, x_n) &:= (\alpha x_1, \alpha x_2, \ldots, \alpha x_n). \end{aligned}$$

a) Prove que estas operações conferem ao conjunto $M_1 \times M_2 \times \cdots \times M_n$ uma estrutura de R-módulo.

b) Utilize a alínea anterior, para provar que $M^n := \overbrace{M \times M \times \cdots \times M}^{n}$ é um R-módulo.

3.1.7) Verifique se cada um dos seguintes conjuntos de polinómios numa indeterminada e com coeficientes reais é um R-módulo em relação às operações ordinárias de adição de polinómios e multiplicação de um polinómio por um elemento de R:

a) Conjunto dos polinómios de grau menor ou igual a n, i.e., $R_n[x]$.

b) Conjunto dos polinómios de grau n (n fixo).

3.1.8) Seja R um anel unitário. Mostre que:

a) $M_{m\times n}(R)$ é um R-módulo, se considerarmos a soma e a operação binária externa definidas por:

$$[a_{ij}] + [b_{ij}] := [a_{ij} + b_{ij}] \quad \text{e} \quad \alpha\, [a_{ij}] := [\alpha a_{ij}]\,.$$

b) $M_{m\times n}(R)$ é um módulo-R, se considerarmos a soma e a operação binária externa definidas por:

$$[a_{ij}] + [b_{ij}] := [a_{ij} + b_{ij}] \quad \text{e} \quad [a_{ij}]\,\alpha := [a_{ij}\alpha]\,.$$

Conclua que, $M_{m\times n}(R)$ é um R-bimódulo-R, para as operações acima introduzidas.

c) $M_{m\times n}(R^{op})$ é um R-módulo, onde R^{op} é o anel oposto do anel R.

3.1.9) Em $\mathbb{R}^n$, defina-se as operações:

$$a + b := a - b \quad \text{e} \quad \alpha \cdot a := -\alpha a$$

com $a, b \in \mathbb{R}^n$ e $\alpha \in \mathbb{R}$.

Quais dos axiomas da definição de $\mathbb{R}$-módulo são satisfeitos por ${}_{\mathbb{R}}\mathbb{R}^n$ para a operação binária $+$ e a operação binária externa $\cdot$ sobre $\mathbb{R}^n$?

3.1.10) Considere o conjunto $\mathbb{R}_{>0}$ dos números reais positivos e as operações:

$$\boxplus : \mathbb{R}_{>0} \times \mathbb{R}_{>0} \to \mathbb{R}_{>0} \quad \text{e} \quad \boxdot : \mathbb{R} \times \mathbb{R}_{>0} \to \mathbb{R}_{>0}$$

definidas, respectivamente, por:

$$(a, b) \mapsto a \boxplus b := a \cdot b \text{ (produto usual) e } (\alpha, a) \mapsto \alpha \boxdot a := a^{\alpha} \text{ (potência usual).}$$

a) Mostre que $\mathbb{R}_{>0}$ para as operações $\boxplus$ e $\boxdot$ é um $\mathbb{R}$-módulo.

b) Verifique se $\mathbb{R}$ com as operações $\boxplus'$ e $\boxdot'$ (operações análogas às anteriores mas de domínio $\mathbb{R} \times \mathbb{R}$ e codomínio $\mathbb{R}$), é $\mathbb{R}$-módulo? Justifique.

3.1.11) Considere os R-módulos ${}_RM$, ${}_RM'$ e as operações binária e binária externa definidas em $M \times M'$ por:

$$(a, b) + (c, d) := (a + c, b + d) \quad \text{e} \quad \alpha\,(a, b) := (\alpha a, 0_{M'})\,.$$

Verifique quais dos axiomas da definição de R-módulo são satisfeitos.

3.1.12) Sejam ${}_RM$ um R-módulo, $x, y, z \in {}_RM$ e $\alpha, \beta \in R$. Prove que:

a) $0_R x = 0_M$.

b) $\alpha 0_M = 0_M$.

c) $(-\alpha)x = \alpha(-x) = -\alpha x$.

d) $(\alpha - \beta)x = \alpha x - \beta x$.

e) $\alpha(x - y) = \alpha x - \alpha y$.

f) $-(-x) = x$.

g) se $\alpha \in U(R)$ e $\alpha x = 0_M \Rightarrow x = 0_M$.

h) $x + y = z + y \Rightarrow x = z$.

3.1.13) Sejam ${}_RM$ um R-módulo e $A \subseteq M$. Mostre que ${}_RA$ é um R-submódulo se, e só se, verifica o seguinte:

i) $0_M \in A$;

ii) $\forall x, y \in M : x, y \in A \Rightarrow x + y \in A$;

iii) $\forall \alpha \in R \;\; \forall x \in M : x \in A \Rightarrow \alpha x \in A$.

3.1.14) Sejam ${}_RM$ um R-módulo e $A \subseteq M$. Mostre que ${}_RA$ é um R-submódulo se, e só se, verifica o seguinte:

i) $0_M \in A$;

ii) $\forall \alpha, \beta \in R \;\; \forall x, y \in M : x, y \in A \Rightarrow \alpha x + \beta y \in A$.

3.1.15) Dos seguintes subconjuntos, determine quais são submódulos do respectivo módulo:

a) $A := \{f \in \mathbb{R}^{[a,b]} : f(x) = c,\, c \in \mathbb{R} \text{ (fixo)}\}$.

b) $B := \{p \in \mathbb{R}^{[a,b]} : p(x) = a_0 + a_1 x + \cdots + a_n x^n, \text{ com } a_i \in \mathbb{R} \text{ (fixos)}\}$.

c) $C := \{f \in \mathbb{R}^{[0,1]} : f(x) = f(1 - x)\}$.

d) $D := \{f \in \mathbb{R}^{[0,1]} : f(0) = f(1) = 0\}$.

e) $E := \{f \in \mathbb{R}^{[0,1]} : f(0) + f(1) = 0\}$.

f) $F := \{f \in \mathbb{R}^{\mathbb{R}} : f(-x) = -f(x)\}$.

g) $G := \{f \in \mathbb{R}^{\mathbb{R}} : f(-x) = f(x)\}$.

h) $H := \{f \in \mathbb{R}^{\mathbb{R}} : f(x) \geq 0\}$.

i) $I := \{f \in \mathbb{R}^{\mathbb{R}} : f \text{ é limitada em } \mathbb{R}\}$.

j) $J := \{f \in \mathbb{R}^{[a,b]} : f \text{ é integrável à Riemann em } [a, b]\}$.

k) $K := \{f \in \mathbb{R}^{[a,b]} : f \text{ é contínua em } [a, b]\}$.

3.1.16) Sejam ${}_RM$ um R-módulo e $A, B, C \sqsubseteq M$. Se $C \subseteq A$, então tem-se que:

$$A \cap (B + C) = (A \cap B) + C.$$

Obteria o mesmo resultado se $C \nsubseteq A$?

3.2. Submódulo gerado por um conjunto. Módulos livres

3.2.1) Sejam ${}_RM$ um R-módulo, $A, B \subseteq {}_RM$, $F, G \sqsubseteq {}_RM$ e $\alpha \in Z(R)$. Então, tem-se que:

a) $F \cap G \sqsubseteq M$.

b) $F \cup G \sqsubseteq M \Leftrightarrow F \subseteq G \vee G \subseteq F$.

c) $F + G \sqsubseteq M$.

d) $\alpha F \sqsubseteq M$.

e) $\langle A \rangle + \langle B \rangle = \langle A \cup B \rangle$.

3.2.2) Sejam ${}_RM$ um R-módulo e $A \subseteq M$. Mostre que:

$$\langle A \rangle = \left\{ \sum_{i=1}^{n} \alpha_i x_i \in M : \alpha_i \in R \wedge x_i \in M \wedge n \in \mathbb{N}_{\neq 0} \right\}.$$

3.2.3) Sejam ${}_RM$ um R-módulo e $A, B \subseteq M$. Mostre que:

a) Se $A \subseteq B$, então $\langle A \rangle \subseteq \langle B \rangle$.

b) $\langle \langle A \rangle \rangle = \langle A \rangle$.

3.2.4) Seja M um R-módulo. Mostre que se $(x_i)_{i \in J}$ é uma subfamília de $(x_i)_{i \in I}$, então

$$\langle \{x_i \in M : i \in J\} \rangle \subseteq \langle \{x_i \in M : i \in I\} \rangle .$$

3.2.5) Mostre que todo o anel unitário R é um módulo ${}_RR$ com base.

3.2.6) Mostre que ${}^IR$ é um ${}^IR$-módulo com base.

3.2.7) Sejam R e R' anéis unitários. Mostre que:

a) $R \times R'$ é um ${}_{R \times R'}R \times R'$ módulo com base.

b) $R \times \{0_{R'}\}$ é um ${}_{R \times R'}R \times \{0_{R'}\}$ submódulo do módulo ${}_{R \times R'}R \times R'$.

c) o submódulo $R \times \{0_{R'}\}$ não tem base.

3.3. Morfismos de módulos

3.3.1) Sejam ${}_RM$ e ${}_RM'$ módulos.

a) Indique qual(is) dos axiomas da definição de R-módulo não é (são) satisfeito(s) de modo que $\mathrm{Mor}({}_RM, {}_RM')$ seja um R-módulo.

b) Indique condições que o anel unitário R deve satisfazer, para que $\mathrm{Mor}({}_RM, {}_RM')$ seja um R-módulo.

3.3.2) Sejam R, S e T anéis unitários (fixos). Mostre que:

a) $\mathrm{Mor}(M_S, {}_RN_S)_S$ é um R-módulo.

b) $\mathrm{Mor}({}_RM, {}_RN_S)$ é um módulo-S.

c) $\mathrm{Mor}({}_RM_S, {}_RN)$ é um S-módulo, se definirmos $(\beta f)(x) := f(x\beta)$.

d) $\mathrm{Mor}({}_RM_S, N_S)_S$ é um módulo-R, se definirmos $(f\alpha)(x) := f(\alpha x)$.

e) $\mathrm{Mor}({}_RM_S, {}_RN_T)$ é um S-bimódulo-T.

f) $\mathrm{Mor}({}_RM_S, {}_TN_S)_S$ é um T-bimódulo-R.

3.3.3) Sejam ${}_RM$, ${}_RN$ e ${}_RP$ módulos. Mostre que:

a) se $f \in \mathrm{Mor}(M, N)$ e $g \in \mathrm{Mor}(N, P)$, então $g \circ f \in \mathrm{Mor}(M, P)$.

b) para todo $f, g \in \mathrm{Mor}(M, N)$, todo o $h, k \in \mathrm{Mor}(N, P)$ e todo o $\alpha \in R$ tem-se que:

1) $h \circ (f + g) = (h \circ f) + (h \circ g)$.
2) $(h + k) \circ f = (h \circ f) + (k \circ f)$.
3) $\alpha(h \circ f) = (\alpha h) \circ f = h \circ (\alpha f)$.

3.3.4) Seja M_R é um módulo-R. Mostre que:

a) Se f é um anti-automorfismo, então M_R é um R-módulo, se para todo o $\alpha \in R$, $\alpha x := x f(\alpha)$.

b) Se $f \in \mathrm{Mor}(R)$ será que se pode concluir que M_R é um R-módulo? Indique condições que R deva satisfazer para que M_R seja um R-módulo.

3.3.5) Seja R um anel unitário (fixo). Mostre que:

a) o dual de um módulo-R, i.e., $M_R^* := \mathrm{Mor}(M_R, {}_RR_R)_R$ é um R-módulo.

b) o dual de um R-módulo, i.e., ${}_RM^* := \mathrm{Mor}({}_RM, {}_RR_R)$ é um módulo-R.

c) Conclua que, se R é um anel unitário comutativo, então M_R^* e ${}_RM^*$ são R-bimódulos-R.

3.3.6) Seja M_R um módulo-R, então mostre que ${}_{\mathrm{End}(M)}M$ é um $\mathrm{End}(M)$-módulo.

3.3.7) Sejam R um anel unitário e M um grupo comutativo. Mostre que o morfismo $\rho : R \to \mathrm{End}(M)$ define uma estrutura de R-módulo em M se definirmos $\alpha x := \rho_\alpha(x)$ e vice-versa, ou seja, se ${}_RM$ é um R-módulo, então $\rho : R \to \mathrm{End}({}_RM)$ é uma representação, i.e., um morfismo de anéis.

3.3.8) Seja ${}_RM$ um módulo, então mostre que $\mathrm{Mor}({}_RR, {}_RM) \cong_{\mathbb{Z}\text{-}\mathrm{Mod}} {}_RM$ através da aplicação $f : \mathrm{Mor}({}_RR, {}_RM) \to {}_RM$ definida por $f(g) := g(1_R)$.

3.3.9) Sejam R um anel unitário comutativo, ${}_RM$ um módulo e $A \subseteq \mathrm{End}({}_RM)$ um subanel unitário. Mostre que M é um A-módulo, se definirmos a operação binária externa por $(f, x) \mapsto f(x)$.

3.3.10) Sejam ${}_RM$ um módulo e $f \in \mathrm{End}(M)$. Mostre que:

a) $g : R[t] \to \mathrm{End}(M)$ é um morfismo de módulos, dado por $p_t \mapsto p_f$, onde $p_t := a_0 + a_1 t + \cdots + a_n t^n \in R[t]$ e $p_f := a_0 \,\mathrm{id}_M + a_1 f + \cdots + a_n f^n$.

b) $R[f]$ é um R-submódulo de $\mathrm{End}(M)$.

c) $g : R[t] \to R[f]$, definido por $p_t \mapsto p_f$ é um morfismo de módulos.

d) M é um $R[f]$-módulo, se definirmos a operação binária externa por:

$$(p_f, x) \mapsto p_f x := p_f(x).$$

e) M é um $R[t]$-módulo se definirmos a operação binária externa para todo o $x \in M$, por $p_t x \mapsto p_f x$.

3.4. Módulos quociente. Teoremas de isomorfismos

3.4.1) Sejam ${}_RM$ um módulo cíclico gerado por x (i.e., ${}_RM = {}_R\langle x\rangle = Rx$) e a relação $\rho_x : R \to Rx$ definida por $\rho_x(\alpha) := \alpha x$. Mostre que:

a) ρ_x é um morfismo sobrejectivo.

b) $s : R \to \frac{R}{\mathrm{Ker}(\rho_x)}$ é um morfismo sobrejectivo.

c) $\frac{R}{\mathrm{Ker}(\rho_x)} \cong Rx$.

d) Define-se o anulador do elemento x de ${}_RM$ por $\mathrm{Ann}(\{x\}) := \mathrm{Ker}(\rho_x)$ e tem-se o isomorfismo $Rx \cong \frac{R}{\mathrm{Ann}(\{x\})}$. Mais geralmente, sendo $A \subseteq M$ define-se

$$\mathrm{Ann}_M(A) := \mathrm{Ker}(\rho) = \{\alpha \in R : \alpha A = \{o_M\}\},$$

sendo $\rho : R \to {}_RM$ definido por $\rho(x) := \alpha x$.

e) Se $\mathbb{F}$ é um corpo e M um $\mathbb{F}$-módulo cíclico não-nulo, então ${}_{\mathbb{F}}M \cong \mathbb{F}$.

3.4.2) Sejam ${}_RM, {}_RM', {}_RN, {}_RN'$ módulos, $f : M \to M'$, $g : N \to N'$ e $f\times g : M\times N \to M'\times N'$ morfismos. Mostre que:

a) $f \times g$ é um morfismo.

b) $\mathrm{Ker}(f \times g) = \mathrm{Ker}(f) \times \mathrm{Ker}(g)$.

c) $\mathrm{Im}(f \times g) = \mathrm{Im}(f) \times \mathrm{Im}(g)$.

d) $f \times g$ é um morfismo injectivo se, e só se, f e g são morfismos injectivos.

e) $f \times g$ é um morfismo sobrejectivo se, e só se, f e g são morfismos sobrejectivos.

f) $f \times g$ é um bimorfismo se, e só se, f e g são bimorfismos.

g) $f \times g$ é um isomorfismos se, e só se, f e g são isomorfismos.

h) $\frac{M\times N}{\mathrm{Ker}(f\times g)} \cong \frac{M}{\mathrm{Ker}(f)} \times \frac{N}{\mathrm{Ker}(g)}$.

3.4.3) Sejam R um domínio e $x \in R_{\neq 0}$. Mostre que:

a) existe uma cadeia descendente

$$\cdots \subseteq Rx^{n+1} \subseteq Rx^n \subseteq \cdots \subseteq Rx^2 \subseteq Rx \subseteq R$$

de submódulos do módulo ${}_RR$.

b) para cada $n \in \mathbb{N}$ se tem

$$\frac{R}{Rx} \cong \frac{Rx^n}{Rx^{n+1}}.$$

Referências bibliográficas

[1] A. Monteiro e I. Matos. *Álgebra - Um primeiro curso.* Livraria Escolar Editora, 1995.

[2] J. Durbin. *Modern Algebra, An Introduction.* John Wiley, 1992.

[3] W. Adkins and S. Weintraub. *Algebra, An Approach via Module Theory.* Springer-Verlag, 1992.

[4] S. Lang. *Undergraduate Algebra.* Springer-Verlag, 1990.

[5] N. Jacobson. *Basic Algebra I.* W. H. Freeman, 1985.

[6] M. Sobral. *Álgebra.* Universidade Aberta, 1996.

[7] P. Cameron. *Introduction to Algebra.* Oxford University Press, 1998.

[8] T. Hungerford. *Algebra.* Springer-Verlag, 1974.

[9] C. Gardiner. *Algebraic Structures.* Ellis Horwood, 1986.

[10] A. Kostrikin. *Exercises in Algebra: A collection of exercises in Algebra, Linear Algebra and Geometry.* Gordon and Breach Publishers, 1996.

[11] F. Ayres. *Álgebra Moderna (Colecção Schaum).* McGraw-Hill, 1965.