

Sebenta de exercícios
de
Álgebra I

Curso: Matemática

Ano Lectivo 2005/2006

23 de Setembro de 2005

(versão 1.1)

ÍNDICE

Notas Prévias	ii
Notações e terminologia	iii
1 Introdução	1
1.1 Noções elementares sobre conjuntos e relações	1
1.2 Noções elementares sobre aplicações	4
1.3 Noções elementares sobre números inteiros	7
2 Estruturas algébricas básicas	9
2.1 Grupóides, semigrupos e monóides	9
2.2 Grupos	12
2.3 Morfismos entre estruturas algébricas	16
2.4 Estruturas geradas e monogénicas	20
2.5 Relações de congruência. Coconjuntos	23
2.6 Estruturas normais. Estruturas quociente	25
2.7 Teoremas do isomorfismo	28
2.8 Estruturas actuando sobre conjuntos	30
2.9 Grupos- p e grupos de Sylow	32
3 Estruturas livres e apresentações	33
Bibliografia	34

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 neste caderno, 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. De salientar, 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, pode não estar isenta de - apesar de involuntárias - omissões e incorrecções¹.

¹apesar 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
$\mathbb{N} = \{0, 1, 2, 3, \dots\}$	o conjunto dos números naturais
$\mathbb{Z} = \{\dots, -2, -1, 0, 1, 2, \dots\}$	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:

$$\begin{aligned} X_{>0} &:= \{x \in X : x > 0\} \\ X_{\geq 0} &:= \{x \in X : x \geq 0\} \\ X_{\neq 0} &:= \{x \in X : x \neq 0\}. \end{aligned}$$

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 $\mathbb{C} \setminus \{0\}$.

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 $\text{card}(A)$ o cardinal do conjunto A . O símbolo ‘ \sqsubseteq ’ representa uma subestrutura de uma dada estrutura algébrica. Por exemplo, sendo M (resp., G) um monóide (resp., grupo) e A um subconjunto de M (resp., G), para abreviar a expressão ‘ A é um submonóide (resp., subgrupo) de M (resp., G)’, usamos o simbolismo $A \sqsubseteq M$ (resp., $A \sqsubseteq G$).

Tabela de Símbolos

Y^X	o conjunto de todas as aplicações de X em Y
$\text{Inj}(X, Y)$	o conjunto de todas as aplicações injectivas de X em Y
$\text{Surj}(X, Y)$	o conjunto de todas as aplicações sobrejectivas de X em Y
$\text{Bij}(X, Y)$	o conjunto de todas as aplicações bijectivas de X em Y
$\text{Mor}(G, H)$ (= $\text{Hom}(G, H)$)	o conjunto de todos os morfismos de G em H
$\text{End}(G)$	o conjunto de todos os endomorfismos em G
$\text{Mono}(G, H)$	o conjunto de todos os monomorfismos de G em H
$\text{Epi}(G, H)$	o conjunto de todos os epimorfismos de G em H
$\text{Bim}(G, H)$	o conjunto de todos os bimorfismos de G em H
$\text{Sect}(G, H)$	o conjunto de todas as secções de G em H
$\text{Retr}(G, H)$	o conjunto de todas as retracções de G em H
$\text{Iso}(G, H)$	o conjunto de todos os isomorfismos de G em H
$\text{Aut}(G)$	o conjunto de todos os automorfismos em G
$\text{Emb}(G, H)$	o conjunto de todos os mergulhos de G em H
$U_l(G)$ (resp., $U_G(G)$, $U(G)$)	o conjunto de todas as unidades (esq., direitas, bilaterais) de G
$N \trianglelefteq G$	N é subgrupo normal de G
$P(\mathbb{Z})$	o conjunto de todos os elementos primos de \mathbb{Z}
$\langle A \rangle$ (resp., $\langle A \rangle$)	o submonóide (resp., subgrupo) gerado por A
$\text{Idem}(M)$	o conjunto de todos os elementos idempotentes de M

1. INTRODUÇÃO

1.1. Noções elementares sobre conjuntos e relações

1.1.1) Sejam X e Y conjuntos quaisquer. Mostre que se tem as seguintes propriedades:

- a) $\emptyset \subseteq X$.
- b) $A \subseteq X \iff A \in \mathcal{P}(X)$.
- c) $X \subseteq Y \implies \mathcal{P}(X) \subseteq \mathcal{P}(Y)$.

1.1.2) Sejam X, Y e Z conjuntos quaisquer. Mostre que, a união de conjuntos tem as seguintes propriedades:

- a) $X \cup (Y \cap Z) = (X \cup Y) \cap Z$.
- b) $\emptyset \cup X = X \cup \emptyset = X$.
- c) $X \cup Y = Y \cup X$.
- d) $X \subseteq Y \iff X \cup Y = Y$.
- e) $X \cup X = X$.

1.1.3) Sejam X, Y e Z conjuntos quaisquer. Mostre que, a intersecção de conjuntos tem as seguintes propriedades:

- a) $X \cap (Y \cup Z) = (X \cap Y) \cup (X \cap Z)$.
- b) $\emptyset \cap X = X \cap \emptyset = \emptyset$.
- c) $X \cap Y = Y \cap X$.
- d) $X \subseteq Y \iff X \cap Y = X$.
- e) $X \cap X = X$.

1.1.4) Sejam X, Y e Z conjuntos quaisquer. Mostre que se tem as seguintes propriedades:

- a) $(X \cup Y) \cap Z = (X \cap Z) \cup (Y \cap Z)$.
- b) $(X \cap Y) \cup Z = (X \cup Z) \cap (Y \cup Z)$.
- c) $(X \cap Y) \cup Z = X \cap (Y \cup Z) \iff Z \subseteq X$.
- d) $\emptyset \times X = X \times \emptyset = \emptyset$.
- e) $A \subseteq X \wedge B \subseteq Y \iff A \times B \subseteq X \times Y$.
- f) $(X \cup Y) \times Z = (X \times Z) \cup (Y \times Z)$.
- g) $(X \cap Y) \times Z = (X \times Z) \cap (Y \times Z)$.

1.1.5) Seja ρ uma relação de equivalência definida num conjunto A . Mostre que:

- a) a definição de relação de equivalência é equivalente a ser formulada, pelas seguintes condições:

- i) $I_A \subseteq \rho$.
- ii) $\rho \subseteq \rho^{-1}$.
- iii) $\rho \circ \rho \subseteq \rho$.

b) $\rho = \rho^{-1}$, ou seja, i), ii) e iii) são equivalentes a ter i), ii) $\rho = \rho^{-1}$ e iii).

1.1.6) Sejam A um conjunto qualquer e ρ uma relação de equivalência definida em A .
Mostre que:

- a) $\forall a \in A \quad a \in [a]$.
- b) $\forall a, b \in A \quad a\rho b \Leftrightarrow [a] = [b]$.
- c) As classes de equivalência de elementos de A formam uma partição de A , ou seja,

- i) $\forall a \in A \quad [a] \neq \emptyset$.
- ii) $\forall a, b \in A \quad [a] \neq [b] \implies [a] \cap [b] = \emptyset$.
- iii) $\forall a \in A \quad \bigcup_{a \in A} [a] = A$.

1.1.7) Sejam A um conjunto qualquer e $\mathcal{C} := \{A_i \subseteq A : i \in I\} \subseteq \mathcal{P}(A)$ uma partição de A .
Então existe uma relação de equivalência em A tal que os elementos de \mathcal{C} são as classes de equivalência dos elementos de A .

Sugestão: Considere a seguinte relação, para todo o $a, b \in A$

$$a\rho b \iff \exists i \in I : (a \in A_i \wedge b \in A_i).$$

1.1.8) Seja $n \in \mathbb{Z}_{\neq 0}$. Mostre que a relação \equiv definida para todo o $a, b \in \mathbb{Z}$ por:

$$a \equiv b \pmod{n} \iff \exists k \in \mathbb{Z} : a - b = k \cdot n$$

é uma relação de equivalência. Esta relação é a relação usual de congruência dos números inteiros.

1.1.9) Sejam $A, B \subseteq X$. Mostre que a relação ρ definida para todo o $A, B \in \mathcal{P}(X)$ por:

$$A\rho B \iff A \subseteq B \vee B \subseteq A$$

é uma relação reflexiva, simétrica mas não transitiva.

1.1.10) Considere-se a relação \sim definida para todo o elemento de \mathbb{N}^2 por:

$$(a, b) \sim (c, d) \iff a + d = b + c.$$

Mostre que é uma relação de equivalência e diga o que é $[(a, b)]$. Com esta relação define-se $\mathbb{Z} := \frac{\mathbb{N}^2}{\sim}$ e à classe de equivalência $[(a, b)]$ chama-se número inteiro.

1.1.11) Seja $A := \{a, b, c, d, e\}$ e consideremos as relações ρ_i , $i = 1, \dots, 8$ definidas em A .

- a) Das relações seguintes, quais são reflexivas, simétricas, transitivas e equivalências:
 - 1) $\rho_1 := \{(a, b), (b, a), (c, d), (d, c)\}$.
 - 2) $\rho_2 := \{(a, b), (b, c), (a, c)\}$.
 - 3) $\rho_3 := \{(a, a), (b, b), (c, c), (d, d), (e, e), (a, b), (b, c)\}$.
 - 4) $\rho_4 := \{(a, a), (b, b), (c, c), (d, d), (e, e)\}$ (relação identidade).
 - 5) $\rho_5 := \{(a, b), (c, e), (d, a), (d, b)\}$.

6) $\rho_6 := \{(a, a), (b, b), (c, c), (d, d), (e, e), (c, d), (d, c)\}$.

7) $\rho_7 := \emptyset$ (relação vazia).

8) $\rho_8 := A \times A$ (relação universal).

b) Determine os seguintes conjuntos quociente A/ρ_4 , A/ρ_6 e A/ρ_8 .

1.1.12) Considere os conjuntos $A := \{a, b, c\}$, $B := \{d, e, f\}$ e $C := \{g, h\}$ e as relações:

$$R := \{(a, d), (b, e), (c, d)\} \quad \text{e} \quad S := \{(d, g), (e, h), (f, h)\}$$

definidas, respectivamente, em $A \times B$ e $B \times C$. Determine $S \circ R$.

1.1.13) Sejam $S := \mathbb{Z} \times \mathbb{Z}_{\neq 0}$ e $\rho := \{((r, s), (t, u)) \in S^2 : r \cdot u = s \cdot t\}$. Mostre que ρ é uma relação de equivalência em S .

1.2. Noções elementares sobre aplicações

1.2.1) Mostre que se $f : X \rightarrow Y$ é uma aplicação qualquer, então f induz as seguintes aplicações:

- a) $f^{\rightarrow} : \mathcal{P}(X) \rightarrow \mathcal{P}(Y)$.
- b) $f^{\leftarrow} : \mathcal{P}(Y) \rightarrow \mathcal{P}(X)$.

1.2.2) Sejam $f : X \rightarrow Y$ uma aplicação, $(A_i)_{i \in I}$ uma família de subconjuntos de X e $(B_i)_{i \in I}$ uma família de subconjuntos de Y . Mostre que:

- a) $f(\bigcup_{i \in I} A_i) = \bigcup_{i \in I} f(A_i)$.
- b) $f(\bigcap_{i \in I} A_i) \subseteq \bigcap_{i \in I} f(A_i)$.
- c) $f^{-1}(\bigcup_{i \in I} B_i) = \bigcup_{i \in I} f^{-1}(B_i)$.
- d) $f^{-1}(\bigcap_{i \in I} B_i) = \bigcap_{i \in I} f^{-1}(B_i)$.

1.2.3) Sejam $f : X \rightarrow Y$ e $g : Y \rightarrow Z$ aplicações quaisquer:

- a) Mostre que a composição de aplicações, $g \circ f$, é uma aplicação.
- b) Mostre que a composição de aplicações injetivas, $g \circ f$, é uma aplicação injetiva.
- c) Mostre que a composição de aplicações sobrejetivas, $g \circ f$, é uma aplicação sobrejetiva.
- d) Mostre que a composição de aplicações bijetivas, $g \circ f$, é uma aplicação bijetiva.
- e) Se $g \circ f$ é uma aplicação sobrejetiva, então g é uma aplicação sobrejetiva.
- f) Se $g \circ f$ é uma aplicação injetiva, então f é uma aplicação injetiva.

1.2.4) Seja $f : X \rightarrow Y$ uma aplicação qualquer.

- a) f é injetiva se, e só se, existe uma aplicação $g : Y \rightarrow X$ tal que $g \circ f = \text{id}_X$.
(A g chama-se a inversa esquerda de f e diz-se que f é uma secção).
- b) f é sobrejetiva se, e só se, existe $g : Y \rightarrow X$ tal que $f \circ g = \text{id}_Y$.
(A g chama-se a inversa direita de f e diz-se que f é uma retracção).
- c) f é bijetiva se, e só se, existe $g : Y \rightarrow X$ tal que $g \circ f = \text{id}_X \wedge f \circ g = \text{id}_Y$.
(A g chama-se função inversa de f e diz-se que f é um isomorfismo).
- d) Mostre que a aplicação inversa de f é única e, portanto, faz sentido representá-la por f^{-1} , i.e., $(f^{-1} : Y \rightarrow X)$.

1.2.5) Seja $f : X \rightarrow Y$ uma aplicação qualquer. Mostre que:

- a) f é injetiva se, e só se, para todo o conjunto Z e para todo o par de aplicações $g, g' : Z \rightarrow X$ as composições $f \circ g$ e $f \circ g'$ estão definidas, então tem-se que:

$$f \circ g = f \circ g' \implies g = g'.$$

(Uma aplicação que verifique esta condição diz-se um monomorfismo).

- b) f é sobrejectiva se, e só se, para todo o conjunto Z e para todo o par de aplicações $g, g' : Y \rightarrow Z$ as composições $g \circ f$ e $g' \circ f$ estão definidas, então tem-se que:

$$g \circ f = g' \circ f \implies g = g'.$$

(Uma aplicação que verifique esta condição diz-se um epimorfismo).

- 1.2.6) Considere X e Y dois conjuntos quaisquer. O conjunto X diz-se equivalente ou equipotente a Y e representa-se por $X \sim Y$ se, e só se, existe uma aplicação bijectiva de X em Y . Mostre que a seguinte relação:

$$X \sim Y \iff \exists f \in Y^X : f \in \text{Bij}(X, Y)$$

é uma relação de equivalência.

Diz-se que os conjuntos X, Y tem a mesma cardinalidade se

$$\text{card}(X) = \text{card}(Y) \iff X \sim Y.$$

- 1.2.7) Sejam X e Y conjuntos quaisquer. Mostre que a relação \leq definida por:

$$\text{card}(X) \leq \text{card}(Y) \iff \exists f \in Y^X : f \in \text{Inj}(X, Y)$$

é uma relação de ordem parcial.

(Sugestão: Use o teorema de Schröder-Bernstein para conjuntos infinitos. Se tivermos aplicações injectivas de X em Y e de Y em X , então $\text{card}(X) = \text{card}(Y)$).

- 1.2.8) Sejam X e Y conjuntos quaisquer e $f : X \rightarrow Y$ uma aplicação e considere a relação para todo $x, y \in X$

$$x \rho_f y \iff f(x) = f(y).$$

Mostre que ρ_f é uma relação de equivalência.

- 1.2.9) Considere uma relação de equivalência ρ definida em X .

- a) Mostre que existe uma aplicação $h : X \rightarrow X/\rho$ sobrejectiva.
 b) Considere uma aplicação $f : X \rightarrow Y$ qualquer, tal que f é compatível com ρ , i.e.,

$$\forall x, y \in X \quad x \rho y \implies f(x) = f(y).$$

Defina uma aplicação $g : \frac{X}{\rho} \rightarrow Y$, de modo que o diagrama

$$\begin{array}{ccc} X & \xrightarrow{h} & \frac{X}{\rho} \\ f \downarrow & & \nearrow g \\ Y & & \end{array}$$

seja comutativo, ou seja, $g \circ h = f$.

- c) Mostre ainda que, nestas condições, g é sobrejectiva se, e só se, f é sobrejectiva.
 d) Mostre também que, f é bicompatível com ρ se, e só se, g é injectiva.

1.2.10) Seja $f : X \rightarrow Y$ uma aplicação que preserva as relações, ou seja,

$$\forall a, b \in X \quad a \rho b \implies f(a) \rho' f(b).$$

Mostre que:

a) Existe uma única aplicação $f^* : X/\rho \rightarrow Y/\rho'$ tal que o seguinte diagrama

$$\begin{array}{ccc} X & \xrightarrow{\nu_X} & X/\rho \\ f \downarrow & & \downarrow f^* \\ Y & \xrightarrow{\nu_Y} & Y/\rho' \end{array}$$

é comutativo. Diz-se que f^* é a aplicação induzida por f . Reciprocamente, se para duas quaisquer aplicações f e f^* o diagrama é comutativo, então f é a aplicação que preserva a relação e, f^* é a aplicação induzida por f .

b) Se $f(a)\rho'f(b) \implies a\rho b$, então $f^* \in \text{Inj}(X/\rho, Y/\rho')$.

c) Se $f \in \text{Surj}(X, Y)$, então $f^* \in \text{Surj}(X/\rho, Y/\rho')$.

d) Sendo $X = Y := \mathbb{Z}$,

$$\rho := \{(a, a') \in \mathbb{Z}^2 : a \equiv a' \pmod{4}\}, \quad \rho' := \{(b, b') \in \mathbb{Z}^2 : a \equiv a' \pmod{2}\}$$

e $f : X \rightarrow Y$ uma aplicação que preserva a relação, definida por $f(n) = n$, então:

1) $f^*([0]_4) = f^*([2]_4) = [0]_2$.

2) $f^*([1]_4) = f^*([3]_4) = [1]_2$.

1.3. Noções elementares sobre números inteiros

1.3.1) Mostre que para qualquer $a, b, c \in \mathbb{Z}$ se tem o seguinte:

- a) $a \mid 0$.
- b) $\pm 1 \mid a$.
- c) $\pm a \mid a$.
- d) $a \mid b \Leftrightarrow a \mid (-b) \Leftrightarrow (-a) \mid b \Leftrightarrow (-a) \mid (-b)$.
- e) $a \mid b \wedge b \mid c \Rightarrow a \mid c$.
- f) $a \mid b \wedge a \mid c \Rightarrow \forall x, y \in \mathbb{Z} \ a \mid (bx + cy)$.

1.3.2) Considere $a, b, k \in \mathbb{Z}$ e $x \in \mathbb{Z}_{\neq 0}$. Mostre que se verifica o seguinte:

- a) $\gcd(a, b) = \gcd(a, b + ax)$.
- b) $\gcd(ka, kb) = k \gcd(a, b)$.

1.3.3) Determine o máximo divisor comum dos seguintes conjuntos e, exprima-o na forma $\gcd(a, b) = ax + by$:

- a) $\{167, 389\}$.
- b) $\{275, 726\}$.
- c) $\{242, 758\}$.

1.3.4) Determine o menor inteiro x não negativo tal que:

- a) $x \equiv 19 \pmod{5}$.
- b) $x \equiv 3312 \pmod{4}$.
- c) $x \equiv 26 \pmod{13}$.
- d) $x \equiv 177 \pmod{8}$.
- e) $x \equiv 111 \pmod{109}$.

1.3.5) Considere $a, b \in \mathbb{Z}$ e $n \in \mathbb{Z}_{\neq 0}$ um elemento fixo. Mostre que são equivalentes as seguintes alíneas:

- a) $a \equiv b \pmod{n}$;
- b) $n \mid a - b$;
- c) a e b dão o mesmo resto, na divisão por n .

1.3.6) Considere $a, b, a', b', k \in \mathbb{Z}$ e $n \in \mathbb{Z}_{\neq 0}$ um elemento fixo. Mostre que se verifica o seguinte:

- a) $a \equiv b \pmod{n} \Rightarrow ka \equiv kb \pmod{n}$.
- b) $a \equiv b \pmod{n} \wedge a' \equiv b' \pmod{n} \Rightarrow a + a' \equiv b + b' \pmod{n}$.
- c) $a \equiv b \pmod{n} \wedge a' \equiv b' \pmod{n} \Rightarrow aa' \equiv bb' \pmod{n}$.
- d) $a + k \equiv b + k \pmod{n} \Rightarrow a \equiv b \pmod{n}$.
- e) $ka \equiv kb \pmod{kn} \Rightarrow a \equiv b \pmod{n}$.

$$f) a \equiv b \pmod{n} \wedge a' \mid n \Rightarrow a \equiv b \pmod{a'}.$$

1.3.7) Indique, para as seguintes relações, quais são possíveis, e para essas, determine a respectiva solução:

a) $2x \equiv 3 \pmod{4}$.

b) $3x \equiv 2 \pmod{4}$.

c) $6x \equiv 2 \pmod{4}$.

d) $10x \equiv 14 \pmod{15}$.

e) $10x \equiv 14 \pmod{18}$.

f) $10x \equiv 14 \pmod{21}$.

2. ESTRUTURAS ALGÉBRICAS BÁSICAS

2.1. Grupóides, semigrupos e monóides

2.1.1) Diga se as relações a seguir indicadas são operações binárias de \mathbb{Z}^2 em \mathbb{Z} , onde o símbolo “+” (resp., “.”) representa a adição (resp., multiplicação) usuais em \mathbb{Z} .

a) $(x, y) \mapsto x + y$.

b) $(x, y) \mapsto x - y$.

c) $(x, y) \mapsto x \cdot y$.

d) $(x, y) \mapsto \sqrt{x \cdot y}$.

e) $(x, y) \mapsto x + 4y$.

f) $(x, y) \mapsto x^y$.

Em caso afirmativo, diga se a operação é associativa ou comutativa e verifique se existe elemento neutro (direito, esquerdo ou bilateral) e elementos invertíveis no respectivo grupóide.

2.1.2) Dê um exemplo de:

a) Grupóide que não seja associativo.

b) Semigrupo que não seja comutativo.

c) Grupóide que não seja associativo nem comutativo.

d) Semigrupo comutativo sem elemento neutro.

e) Monóide com elementos invertíveis.

f) Grupo.

g) Grupóide não associativo com elemento neutro e os elementos invertíveis.

2.1.3) Seja X um conjunto qualquer. Mostre que $(\mathcal{P}(X); \cup, \emptyset)$ e $(\mathcal{P}(X); \cap, X)$ são monóides.

2.1.4) Seja P o conjunto dos pontos do plano e considere a relação que a cada par de pontos de P associa o ponto médio do segmento por eles definido. Verifique que P com esta operação constitui um grupóide comutativo não associativo.

2.1.5) Estude os seguintes grupóides:

a) O conjunto $\{a, b, c, d\}$ com a operação definida pela seguinte tabela

*	a	b	c	d
a	d	b	b	d
b	c	d	b	a
c	a	c	a	a
d	b	a	d	c

- b) $(\mathbb{N}; *)$ com $a * b := a + 2b$, onde $+$ é a soma usual em \mathbb{N} .
- c) $(\mathbb{N}; *)$ com $a * b := a^b$.
- d) $(\mathbb{N}; *)$ com $a * b := |a - b|$.
- e) $(\mathbb{Q}_{\neq 0}; \theta)$ com $a\theta b := a \cdot b^{-1}$, onde \cdot é o produto usual em \mathbb{Q} .

2.1.6) Seja A um grupóide. Mostre que se 1_A é identidade esquerda e $1'_A$ é identidade direita (em A) então $1_A = 1'_A$, portanto 1_A é identidade única de A .

2.1.7) Construa um grupóide com duas identidades direitas. Verifique se é semigrupo.

2.1.8) Seja $(S; \cdot)$ um semigrupo. Mostre que:

- a) Se é válida a lei do corte à esquerda (resp., direita)

$$ab = ac \Rightarrow b = c \text{ (resp., } ba = bc \Rightarrow b = c)$$

e $a^2 = a$, então a é elemento neutro à esquerda (resp., direita) de S .

- b) Existe um e um só idempotente em S , concretamente o elemento neutro.

2.1.9) Mostre que se $(M; \cdot, 1_M)$ é um monóide e $a \in M$ tem um inverso direito e um inverso esquerdo, então estes coincidem.

2.1.10) Mostre que se $(M; \cdot, 1_M)$ é um monóide e $a \in U(M)$, então tem-se que:

- a) $\forall b, c \in M, ab = ac \Rightarrow b = c$.
- b) Qualquer das equações $ax = b$ e $ya = b$ com $b \in M$, admite uma e uma só solução.

2.1.11) Sejam M um monóide e $a, b \in U(M)$. Mostre que:

- a) $(ab)^{-1} = b^{-1}a^{-1}$.
- b) a e b comutam se, e só se, $(ab)^{-1} = a^{-1}b^{-1}$.

2.1.12) Seja A um grupóide. Mostre que se verifica sempre uma e uma só, das afirmações seguintes:

- a) A não tem identidade esquerda nem direita.
- b) A tem uma ou mais identidades direitas mas nenhuma identidade esquerda.
- c) A tem uma ou mais identidades esquerdas mas nenhuma identidade direita.
- d) A tem uma identidade e mais nenhuma (distinta) identidade esquerda ou direita.

2.1.13) Seja S um semigrupo finito. Mostre que S admite elemento neutro se, e só se, contém um elemento simplificável.

2.1.14) Sejam S um semigrupo e $a \in S$. Suponha que para esse elemento existe um elemento b de S tal que $ab = a$. Prove que quaisquer que sejam t e v , elementos de S , a equação $yt = v$ é solúvel, então b é elemento neutro direito de S .

2.1.15) Seja $M_{n \times n}(\mathbb{K})$ o conjunto das matrizes de ordem $n \times n$ sobre o corpo \mathbb{K} . Mostre que $(M_{n \times n}(\mathbb{K}); \cdot, I_n)$ é um monóide, onde \cdot é o produto usual de matrizes.

2.1.16) Mostre que se $(S; \cdot)$ é um semigrupo, então qualquer seu subgrupóide é um semigrupo. Conclua, analogamente para um semigrupo comutativo.

2.1.17) Seja $(S; \cdot)$ um semigrupo. Mostre que:

a) aS é um subsemigrupo de S .

b) se a um elemento idempotente de S tal que $\forall x \in S, x = xa$, então a é o elemento neutro de aS .

2.1.18) Mostre que um subconjunto $A \subseteq M$ é um submonóide de um monóide $(M; \cdot, 1_M)$ se, e só se, verifica:

i) $\forall x, y \in M : x, y \in A \implies x \cdot y \in A$;

ii) $1_M \in A$.

2.1.19) Sejam M um monóide e $A \subseteq M$. O centralizador de A em M é definido por:

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

Mostre que $C_M(A)$ é um submonóide de M . Quando $A := M$, chama-se o centro de do monóide M e representa-se por $Z(M)$.

2.2. Grupos

2.2.1) Suponha que $S := \{x, y, z, w\}$ é um grupo com elemento neutro x . Verifique que para cada uma das condições adicionais seguintes se tem uma única tabela de Cayley tal que S é um grupo:

- a) $y^2 = z$.
- b) $y^2 = w$.
- c) $y^2 = x$ e $z^2 = x$.
- d) $y^2 = x$ e $z^2 = y$.

2.2.2) Suponha que $S := \{a, b, c\}$ é um grupo. Só existe uma única maneira possível de

completar a seguinte tabela de Cayley $\begin{array}{c|ccc} * & a & b & c \\ \hline a & & b & \\ b & & & \\ c & & & \end{array}$. Encontre-a.

2.2.3) Mostre que num grupo é válida a lei do corte.

2.2.4) (Critério de Dickson) Mostre que um semigrupo S é um grupo se, e só se, verifica as seguintes condições:

- i) Existe um elemento neutro à direita de S , 1_r .
- ii) Qualquer que seja o elemento $a \in S$, existe um elemento $a' \in S$ tal que $aa' = 1_r$, ou seja, a' é o inverso direito relativamente a 1_r .

2.2.5) (Critério de Weber-Huntington) Mostre que um semigrupo S é um grupo se, e só se, as equações, para todo o $a, b \in S$, $ax = b$ e $ya = b$ são solúveis.

2.2.6) Mostre que um semigrupo S é um grupo se, e só se, qualquer que seja o elemento $a \in S$, $aS = Sa = S$.

2.2.7) Prove que para qualquer grupo G a equação $axb = c$ tem uma única solução, quaisquer que sejam os elementos $a, b, c \in G$.

2.2.8) Mostre que se G é um grupo e $a, b \in G$ são tais que $ab = b$, então a é o elemento neutro do grupo.

2.2.9) Sejam G um grupo e $a, b, c \in G$. Mostre que:

- a) qualquer uma das igualdades seguintes implica as outras duas:
 - 1) $ab = c$;
 - 2) $a = cb^{-1}$;
 - 3) $b = a^{-1}c$.
- b) $ab = c$ não implica $a = b^{-1}c$.

2.2.10) Mostre que todo o semigrupo finito em que é válida a lei do corte é um grupo (finito).

2.2.11) Sejam G um grupo e $A \subseteq G$. Mostre que, $A \sqsubseteq G$ se, e só se, verifica:

- i) $1_G \in A$;

ii) $\forall x, y \in G : x, y \in A \implies x \cdot y \in A$;

iii) $\forall x \in G : x \in A \implies x^{-1} \in A$.

2.2.12) Mostre que um semigrupo S com identidade 1_S em que $\forall x \in S, x^2 = 1_S$ é um grupo abeliano.

2.2.13) Mostre que num grupo se b é o inverso direito (resp., esquerdo) de a então b^k é o inverso direito (resp., esquerdo) de a^k .

2.2.14) Sejam G um grupo, $A, B, C \subseteq G$ e considerem-se os seguintes subconjuntos:

$$A^{-1} := \{a^{-1} \in G : a \in A\} \quad (\text{em notação aditiva } -A := \{-a \in G : a \in A\})$$

e

$$B^{-1} := \{b^{-1} \in G : b \in B\} \quad (\text{em notação aditiva } -B := \{-b \in G : b \in B\}).$$

Mostre que:

a) $(A \cdot B) \cdot C = A \cdot (B \cdot C)$ (em notação aditiva $(A + B) + C = A + (B + C)$).

b) $\{1_G\} \cdot A = A \cdot \{1_G\} = A$ (em notação aditiva $\{0_G\} + A = A + \{0_G\} = A$).

c) $(A \cdot B)^{-1} = B^{-1} \cdot A^{-1}$ (em notação aditiva $-(A + B) = (-B) + (-A)$).

d) $\forall x \in G, A \subseteq B \implies x \cdot A \subseteq x \cdot B$ (em notação aditiva $\forall x \in G, A \subseteq B \implies \{x\} + A \subseteq \{x\} + B$).

e) $\forall x \in G, \{x\} \cdot A = A \cdot \{x\} \iff \{x\} \cdot A \cdot \{x\}^{-1} = A$ (em notação aditiva $\{x\} + A = A + \{x\} \iff \{x\} + A + (-\{x\}) = A$).

f) $A \cdot G = G \cdot A = G$ (em notação aditiva $A + G = G + A = G$).

g) $A \subseteq B \implies A^{-1} \subseteq B^{-1}$ (em notação aditiva $A \subseteq B \implies -A \subseteq -B$).

Se $A \subseteq G$, então:

a) $A^{-1} = A$ (em notação aditiva $-A = A$).

b) $\forall x \in G, (\{x\} \cdot A)^{-1} = A \cdot \{x\}^{-1}$ (em notação aditiva $\forall x \in G, -(\{x\} + A) = A + (-\{x\})$).

c) $A \cdot A = A$ (em notação aditiva $A + A = A$), em particular, $\forall x \in A, \{x\} \cdot A = A$ (em notação aditiva $\forall x \in A, \{x\} + A = A$).

2.2.15) Considere-se o grupóide $(\mathbb{N}; \cdot)$, onde \cdot é a multiplicação usual e os seguintes subconjuntos de \mathbb{N} :

$$A := \{2\}, B := \{x \in \mathbb{N} : x \text{ é divisor de } 6\} \text{ e } C := \{x \in \mathbb{N} : x \text{ é múltiplo de } 6\}.$$

a) Determine $O \cdot B$ e $B \cdot A$, sendo $O := \{0\}$.

b) Dos conjuntos $A, B, O \cdot B$ e $B \cdot A$ quais são partes estáveis de \mathbb{N} para a mesma operação.

c) Mostre que $(C; \cdot)$ é subgrupóide de $(\mathbb{N}; \cdot)$ e escreva-o como produto de dois subgrupóides de $(\mathbb{N}; \cdot)$.

2.2.16) Sejam $(M; \cdot, 1_M)$ um monóide. Mostre que $U(M)$ é um subgrupo do monóide M .

2.2.17) Mostre que um grupo G é abeliano se, e só se, $\forall a, b \in G, (ab)^{-1} = a^{-1}b^{-1}$.

2.2.18) Sejam M_1 e M_2 monóides (resp., grupos), prove que:

- a) $(M_1 \times M_2; \cdot, (1_{M_1}, 1_{M_2}))$ é um monóide (resp., grupo).
- b) $(M_1 \times M_2; +, (0_{M_1}, 0_{M_2}))$ é um monóide (resp., grupo).
- c) Generalize para $M_1 \times M_2 \times \cdots \times M_n$.

2.2.19) Sejam A e B submonóides (resp., subgrupos) de um monóide M (resp., grupo). Mostre que:

- a) $A \times B$ é submonóide (resp., subgrupo) de $M \times M$.
- b) $A \cap B$ é submonóide (resp., subgrupo) de M .
- c) $A \cup B$ é submonóide (resp., subgrupo) de M se, e só se, $A \subseteq B \vee B \subseteq A$.
- d) AB (em notação aditiva $A + B$) é submonóide (resp., subgrupo) de M se, e só se, $AB = BA$ (em notação aditiva $A + B = B + A$).
No caso particular de M ser abeliano, então AB (em notação aditiva $A + B$) é submonóide (resp., subgrupo) de M .

2.2.20) Seja X um conjunto qualquer. Mostre que $(\mathcal{P}(X); \Delta, \emptyset)$ é um grupo abeliano, onde

$$A \Delta B := (A \setminus B) \cup (B \setminus A) = \{x \in X : x \in A \cup B \wedge x \notin A \cap B\}.$$

2.2.21) Sejam G um grupo, $A \in \mathcal{P}_{\neq \emptyset}(G)$ e o conjunto

$$gAg^{-1} := \{gag^{-1} \in G : a \in A\}$$

que se chama o conjugado direito de A em G . Mostre que $gAg^{-1} \sqsubseteq G$ se, e só se, $A \sqsubseteq G$.

2.2.22) Sejam G um grupo e $A \in \mathcal{P}(G)$. Chama-se normalizador de A em G ao conjunto

$$N_G(A) := \{x \in G : xAx^{-1} = A\}.$$

Mostre que $N_G(A)$ é um subgrupo de G .

2.2.23) Sejam $A \sqsubseteq K \sqsubseteq G$ e $x \in G$ (fixo). Mostre que:

- a) $N_K(A) = N_G(A) \cap K$.
- b) $N_G(xAx^{-1}) = xN_G(A)x^{-1}$.

2.2.24) Considere o grupo $GL_n(\mathbb{K}) := \{A \in M_{n \times n}(\mathbb{K}) : A \text{ é invertível}\}$.

- a) Mostre que $GL_n(\mathbb{K})$ é um grupo.
- b) Determine todos os subsemigrupos próprios de $GL_2(\mathbb{R})$.
- c) Verifique que o conjunto $\left\{ \begin{bmatrix} a & 0 \\ 0 & 0 \end{bmatrix} \in M_{2 \times 2}(\mathbb{R}) : a \in \mathbb{R} \right\}$ é um subsemigrupo de $GL_2(\mathbb{R})$. Será um submonóide de $GL_2(\mathbb{R})$? Justifique.
- d) Mostre que $SL_n(\mathbb{K}) \subseteq GL_n(\mathbb{K})$, onde $SL_n(\mathbb{K}) := \{A \in GL_n(\mathbb{K}) : \det(A) = 1\}$ é um subgrupo de $GL_n(\mathbb{K})$.
- e) Determine o centro do grupo $GL_n(\mathbb{K})$, i.e., $Z(GL_n(\mathbb{K}))$.

2.2.25) Determine os subgrupos de:

a) \mathbb{Z}_6 .

b) S_3 .

2.2.26) Simplifique cada uma das seguintes expressões em \mathbb{Z}_5 :

a) $[8] + [4]$.

b) $[2] + [7]$.

c) $[17] + [76]$.

d) $[3] \cdot [4]$.

e) $[2] \cdot [-7]$.

f) $[17] \cdot [76]$.

g) $([3] \cdot [2]) + ([3] \cdot [4])$.

h) $[3] \cdot ([2] + [4])$.

Resolva o mesmo exercício considerando as expressões em \mathbb{Z}_6 .

2.2.27) Construa as tabelas de Cayley de $(\mathbb{Z}_3; +)$, $(\mathbb{Z}_3; \cdot)$, $(\mathbb{Z}_4; +)$ e $(\mathbb{Z}_4; \cdot)$. Diga quais dos grupóides em questão são grupos.

2.2.28) Mostre que cada grupo \mathbb{Z}_n é abeliano.

2.2.29) Verifique se $(\mathbb{Z}_3 \setminus \{[0]\}; \cdot, [1])$ e $(\mathbb{Z}_4 \setminus \{[0]\}; \cdot, [1])$ são grupos.

2.2.30) Mostre que $(\mathbb{Z}_n \setminus \{[0]\}; \cdot, [1])$ é grupo se, e só se, n é primo.

2.2.31) Considerem-se o par $(a, b) \in \mathbb{R}_{\neq 0} \times \mathbb{R}$ e a aplicação $f_{(a,b)} : \mathbb{R} \rightarrow \mathbb{R}$ definida da seguinte forma $f_{(a,b)}(x) = ax + b$. Seja $A := \{f_{(a,b)} \in \mathbb{R}^{\mathbb{R}} : (a, b) \in \mathbb{R}_{\neq 0} \times \mathbb{R}\}$.

a) Mostre que $(A; \circ)$ é um grupóide e verifique se é comutativo.

b) Verifique se existe elemento neutro em $(A; \circ)$.

c) Determine $U(A)$.

d) Diga, justificando, se $(A; \circ, \text{id}_{\mathbb{R}})$ é um grupo.

2.3. Morfismos entre estruturas algébricas

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

- a) $f : (\mathbb{Z}; +) \rightarrow (\mathbb{R}; +)$ definida por $f(x) := 3x$.
- b) $f : (\mathbb{Z}; +) \rightarrow (\mathbb{R}; \cdot)$ definida por $f(x) := 3x$.
- c) $f : (\mathbb{R}; +) \rightarrow (\mathbb{Z}; +)$ definida por $f(x) := 3x$.
- d) $f : (\mathbb{Z}; \cdot) \rightarrow (\mathbb{Z}; \cdot)$ definida por $f(x) := 3x$.
- e) $f : (\mathbb{Z}; \cdot) \rightarrow (\mathbb{N}; \cdot)$ definida por $f(x) := x^2$.
- f) $f : (\mathbb{R}; \cdot) \rightarrow (\mathbb{R}_{\geq 0}; \cdot)$ definida por $f(x) := x^2$.
- g) $f : (\mathbb{R}_{> 0}; \cdot) \rightarrow (\mathbb{R}_{> 0}; \cdot)$ definida por $f(x) := x^2$.
- h) $f : (\mathbb{Z}; +) \rightarrow (\mathbb{Z}; +)$ definida por $f(x) := x^2$.
- i) $f : (\mathbb{Q}; +) \rightarrow (\mathbb{Q}; +)$ definida por $f(x) := x + 2$.
- j) $f : (\mathbb{R}_{\neq 0}; +) \rightarrow (\mathbb{R}_{\neq 0}; +)$ definida por $f(x) := |x|$.
- k) $f : (\mathbb{C}_{\neq 0}; +) \rightarrow (\mathbb{R}_{\neq 0}; \cdot)$ definida por $f(z) := |z|^2$.
- l) $f : (\mathbb{R}_{\neq 0}; +) \rightarrow (\mathbb{R}_{\neq 0}; +)$ definida por $f(x) := -x$.
- m) $f : (\mathbb{Z}; \cdot) \rightarrow (\mathbb{Z}; \cdot)$ definida por $f(x) := 2x + 1$.
- n) $f : (\mathbb{Z}; +) \rightarrow (\mathbb{Z}; *)$, onde $x * y := x + y - 1$ e f é definida por $f(x) := 2x + 1$.
- o) $f : (\mathbb{R}; \alpha) \rightarrow (\mathbb{R}; +)$, onde $x\alpha y := 2xy + x + y$ e f é definida por $f(x) := 2x + 1$.
- p) $f : \mathbb{Z}_8 \rightarrow \mathbb{Z}_2$ definida por $f(\bar{a}_8) = \bar{a}_2$.
- q) $f : \mathbb{Z}_{12} \rightarrow \mathbb{Z}_{12}$ definida por $f([a]_{12}) = [a + 1]_{12}$.
- r) $f : (\mathbb{R}; +) \rightarrow (\mathbb{R}_{\neq 0}; \cdot)$ definida por $f(x) := a^x$, sendo $a \in \mathbb{R}_{\neq 0}$ um elemento qualquer fixo.
- s) $f : (\mathbb{R}_{> 0}; \cdot) \rightarrow (\mathbb{R}; +)$ definida por $f(x) := \ln(x)$.
- t) $f : (\mathbb{R}_{\neq 0}; \cdot) \rightarrow (\{-1, 1\}; \cdot)$ definida por $f(x) := \begin{cases} 1 & \text{se } x > 0 \\ -1 & \text{se } x < 0 \end{cases}$.

2.3.2) Considere a relação $f : \mathbb{R} \rightarrow \mathbb{R}$ definida por $f(x) := x^2 - 1$.

- a) Mostre que é uma aplicação.
- b) Defina duas operações binárias α e β de modo que f seja um morfismo de $(\mathbb{R}; \alpha)$ para $(\mathbb{R}; \beta)$.
- c) Determine dois grupóides de modo que f seja um isomorfismo entre eles.

2.3.3) Considere a aplicação $f : \mathbb{C}_{\neq 0} \rightarrow \mathbb{R}_{\neq 0}$, definida por $f(z) = |z|$.

- a) Mostre que f é um morfismo do grupo $(\mathbb{C}_{\neq 0}; \cdot, 1)$ no grupo $(\mathbb{R}_{\neq 0}; \cdot, 1)$.
- b) Determine explicitamente os elementos de $\text{Ker}(f)$ e de $\text{Im}(f)$.
- c) Represente geometricamente os elementos de $f^{-1}(\{2\})$.

2.3.4) Sejam $(G; \cdot, 1_G)$ um grupo e a relação $f : G \rightarrow G$ definida nas seguintes alíneas por:

- a) $f(x) = x^{-1}$.
- b) $f(x) = x^2$.

- 1) Verifique que f não é, em geral, um morfismo de grupos.

- 2) Estabeleça uma condição necessária e suficiente para que f seja um morfismo de grupos.

2.3.5) Seja $S^1 := \{z \in \mathbb{C} : |z| = 1\}$.

- Mostre que S^1 é subgrupo de $(\mathbb{C}_{\neq 0}; \cdot, 1)$.
- Verifique se a aplicação $f : (\mathbb{R}; +, 0) \rightarrow (S^1; \cdot, 1)$, definida por $f(x) = \text{cis } x$ é um morfismo de grupos.
- Determine $f^{-1}(\{1\})$.

2.3.6) Considere o morfismo $f : (\mathbb{Z}_6; +, \bar{0}) \rightarrow (S_3; \circ, \text{id})$, tal que $f(\bar{1}_6) = \begin{pmatrix} 1 & 2 & 3 \end{pmatrix}$.

- Determine $\text{Ker}(f)$.
- Determine $\text{Im}(f)$.
- Será possível determinar um isomorfismo entre $(\mathbb{Z}_6; +, \bar{0})$ e $(S_3; \circ, \text{id})$?

2.3.7) Considere os conjuntos $A := \{1, 2, 3\}$ e $B := \{a, b, c\}$ e as operações θ e θ' dadas pelas tabelas seguintes:

θ	1	2	3
1	1	2	3
2	2	3	1
3	3	1	2

e

θ'	a	b	c
a	b	c	a
b	c	a	b
c	a	b	c

Mostre que existe um isomorfismo entre os grupóides $(A; \theta)$ e $(B; \theta')$.

2.3.8) Sejam $(G; *, 1_G)$, $(G'; \cdot, 1_{G'})$, $(G''; \theta, 1_{G''})$ grupos e, $f : G \rightarrow G'$ e $g : G' \rightarrow G''$ morfismos de grupos.

- Mostre que $g \circ f$ é um morfismo de grupos.
- Mostre que, se f e g são isomorfismos, então $g \circ f$ é um isomorfismo.

2.3.9) Sejam (M, d) e (M', d') dois espaços métricos. Uma isometria é uma aplicação bijectiva $f : M \rightarrow M'$ tal que

$$d'(f(x), f(y)) = d(x, y).$$

- Mostre que o conjunto de todas as isometrias em M , i.e.,

$$\text{Isom}(M) := \{f \in M^M : f \text{ é uma isometria}\}$$

é um grupo.

- Sejam agora $X \in \mathcal{P}_{\neq \emptyset}(M)$. Mostre que o conjunto de todas as isometrias que deixam o conjunto X fixo

$$S_M(X) := \{f \in \text{Isom}(M) : f(X) = X\}$$

é um subgrupo de $\text{Isom}(M)$. A este grupo, chama-se o grupo da simetria de X em relação ao espaço métrico M .

2.3.10) Sejam $X \neq \emptyset$ um conjunto qualquer e considere o conjunto X^X . Mostre que:

- $(X^X; \circ, \text{id}_X)$ é um monóide.
- $\text{Sym}(X)$ é um grupo.

2.3.11) Sejam X um conjunto qualquer e M (resp., G) um monóide (resp., um grupo). Mostre que:

- a) $(M^X; \cdot, c_{1_M})$ é um monóide.
- b) $(G^X; \cdot, c_{1_G})$ é um grupo.

2.3.12) Sejam M, N monóides (resp., grupos). Mostre que:

- a) $(N^M; \cdot, c_{1_N})$ é um monóide (resp., grupo).
- b) Se N é comutativo, então $(\text{Mor}(M, N); \cdot, c_{1_N})$ é um submonóide (resp., subgrupo) de N^M . Conclua que, $\text{Mor}(M, N)$ é comutativo.
- c) Sendo M comutativo, então $(\text{End}(M); \cdot, c_{1_M})$ (resp., $\text{Aut}(M)$) é um monóide (resp., grupo) comutativo.

2.3.13) Seja M um monóide (resp., grupo). Mostre que $(\text{End}(M); \circ, \text{id}_M)$ (resp., $(\text{Aut}(M); \circ, \text{id}_M)$) é um monóide (resp., grupo).

2.3.14) Considere a aplicação $f : \mathbb{N}_{\neq 0} \rightarrow \{0, 1\}$ definida por:

$$\left(\begin{array}{ccccccccc} 1 & 2 & 3 & 4 & \cdots & 2k-1 & 2k & \cdots \\ 1 & 0 & 1 & 0 & \cdots & 1 & 0 & \cdots \end{array} \right), \text{ onde } k \in \mathbb{N}_{\neq 0}.$$

- a) Mostre que $\forall a, b \in \mathbb{N}_{\neq 0}, f(ab) = f(a)f(b)$.
- b) Será f um isomorfismo entre os grupóides $(\mathbb{N}_{\neq 0}; \cdot)$ e $(\{0, 1\}; \cdot)$?

2.3.15) Sejam S e T grupóides (resp., semigrupos) e $f \in \text{Mor}(S, T)$. Mostre que:

- a) Se a é um idempotente em S , então $f(a)$ é um idempotente em T .
- b) Se A é um subgrupóide (resp., subsemigrupo) de S , então $f(A)$ é um subgrupóide (resp., subsemigrupo) de T .
- c) Se B é um subgrupóide (resp., subsemigrupo) de T , então $f^{-1}(B)$ é um subgrupóide (resp., subsemigrupo) de S .
- d) Se 1_S for o elemento neutro de S , indique condições para que $f(1_S)$ seja o elemento neutro de T .

2.3.16) Sejam $(G; \cdot, 1_G), (G'; \cdot', 1_{G'})$ grupos e $f : G \rightarrow G'$ um morfismo de grupos. Prove que:

- a) $f(1_G) = 1_{G'}$.
- b) $\forall a \in G, f(a^{-1}) = (f(a))^{-1}$.
- c) $\forall n \in \mathbb{Z} \forall a \in G, f(a^n) = (f(a))^n$. Em particular, $f(a^{-1}) = (f(a))^{-1}$.
- d) Se $A \subseteq G$, então $f(A) \subseteq G'$. Em particular, conclua que $\text{Im}(f) \subseteq G'$.
- e) Se $B \subseteq G'$, então $f^{-1}(B) \subseteq G$. Em particular, conclua que $\text{Ker}(f) \subseteq G$.

2.3.17) Sejam $(\mathbb{Z}; \cdot, 1)$ o monóide dos inteiros e $f : (\mathbb{Z}; \cdot, 1) \rightarrow (\mathbb{Z}; \cdot, 1)$ uma aplicação definida por $\forall x \in \mathbb{Z}, f(x) = 0$. Mostre que $\forall x, y \in \mathbb{Z}, f(xy) = f(x)f(y)$ mas que f não é um morfismo de monóides.

2.3.18) Dado um grupo G , considere a família de aplicações $(\sigma_g)_{g \in G}$, onde $\sigma_g : G \rightarrow G$ é definida por $\sigma_g(x) := gxg^{-1}$. Verifique se:

- a) Para todo o $g, \sigma_g \in \text{Aut}(G)$ (automorfismo interno direito de G).
 O conjunto de todos os automorfismos internos direitos representa-se por $\text{Inn}_r(G)$.
- b) $(\text{Inn}_r(G); \circ, \text{id}_G)$ é um subgrupo de $(\text{Aut}(G); \circ, \text{id}_G)$.
- c) Verifique que a aplicação $f : G \rightarrow \text{Aut}(G)$ definida por $f(g) := \sigma_g$ é um morfismo e tal que $\text{Ker}(f) = Z(G)$ e $\text{Im}(f) = \text{Inn}_r(G)$.

2.3.19) Sejam G, G', G'' grupo e f_0, f_1, f_2, f_3 morfismos tais que:

$$\{0\} \xrightarrow{f_0} G \xrightarrow{f_1} G' \xrightarrow{f_2} G'' \xrightarrow{f_3} \{0\}$$

e $\text{Im}(f_i) = \text{Ker}(f_{i+1}), i = 0, 1, 2$.

- a) Mostre que f_1 é um morfismo injectivo.
- b) Mostre que f_2 é um morfismo sobrejectivo.

2.3.20) Sejam G um grupo, $f \in \text{Aut}(G)$. Mostre que $f(Z(G)) \subseteq Z(G)$.

2.3.21) Sejam $f : G \rightarrow H$ um morfismo, $A \sqsubseteq G$ e $B \sqsubseteq H$. Mostre que:

- a) Se $f(A) = B$, então $f^{-1}(B) = A \text{Ker}(f)$.
- b) Se $f^{-1}(B) = A$, então $f(A) = B \cap \text{Im}(f)$.

2.3.22) (Teorema de Cayley) Seja $(M; \cdot, 1_M)$ um monóide (resp., grupo). Mostre que:

- a) todo o monóide é isomorfo a um submonóide de $(M^M; \circ, \text{id}_M)$.
- b) todo o grupo M é isomorfo a um subgrupo de $\text{Sym}(M)$.
- c) todo o grupo finito de ordem n é isomorfo a um subgrupo do grupo S_n .

2.3.23) Sejam G_1, G_2, G_3, G_4 grupos, $f \in \text{Mor}(G_1, G_2)$ e $g \in \text{Mor}(G_2, G_3)$ morfismos. Mostre que:

- a) $\text{Ker}(g \circ f) = f^{-1}(\text{Ker}(g))$ e $\text{Im}(g \circ f) = g(\text{Im}(f))$.
- b) se o diagrama

$$\begin{array}{ccc} G_1 & \xrightarrow{f} & G_2 \\ \downarrow h & & \downarrow g \\ G_4 & \xrightarrow{j} & G_3 \end{array}$$

é comutativo se $h \in \text{Surj}(G_1, G_4)$ e $g \in \text{Inj}(G_2, G_3)$, então $\text{Im}(f) = g^{-1}(\text{Im}(j))$ e $\text{Ker}(j) = h(\text{Ker}(f))$.

2.4. Estruturas geradas e monogénicas

2.4.1) Sejam G um grupo e $X \subseteq G$. Mostre que:

a) O conjunto gerado por X

$$\langle X \rangle = \{1_G, x_1^{\pm 1} x_2^{\pm 1} \cdots x_n^{\pm 1} \in G : x_i \in X, x_i^{-1} \in X^{-1}, i = 1, \dots, n, n \in \mathbb{N}_{\neq 0}\}$$

forma um subgrupo de G .

b) $X \subseteq \langle X \rangle$.

c) $\forall A \subseteq G : X \subseteq A \implies \langle X \rangle \subseteq A$.

2.4.2) Sejam G um grupo e $A, B \subseteq G$. Mostre que:

a) $A \subseteq B \implies \langle A \rangle \subseteq \langle B \rangle$.

b) $\langle \emptyset \rangle = \{1_G\}$.

c) Se $A \subseteq G$, $\langle A \rangle = A$. Em particular, $\langle \{1_G\} \rangle = \{1_G\}$ e $\langle G \rangle = G$.

d) Se $A \subseteq B \subseteq \langle A \rangle \implies \langle A \rangle = \langle B \rangle$.

2.4.3) Seja $C := \{1, 2, 3\} \subseteq \mathbb{N}$. Construa o grupo simétrico de C (escreva a tabela de Cayley). Determine todos os subgrupos de $\text{Sym}(C)$ e diga qual a cardinalidade mínima dos conjuntos de geradores dele.

2.4.4) Sejam G um grupo, $X \in \mathcal{P}_{\neq \emptyset}(G)$ e $(A_i)_{i \in I} \in \text{Sub}(G)^I$ tais que $\forall i \in I, A_i \subseteq X$. O interior de X em G é definido por

$$\text{Cor}_G(X) := \left\langle \bigcup_{\substack{i \in I \\ A_i \subseteq X}} A_i \right\rangle.$$

Mostre que:

a) $\text{Cor}_G(X)$ é um subgrupo de G .

b) Se $A \subseteq G$ tal que $\forall i \in I, A_i \subseteq A$, então

$$\text{Cor}_G(A) := \left\langle \bigcup_{\substack{i \in I \\ A_i \subseteq A}} A_i \right\rangle = \bigcap_{g \in G} g^{-1} A g.$$

2.4.5) Sejam $A, B \subseteq G$. Mostre que:

$$\langle A \cup B \rangle = \{a_1 b_1 a_2 b_2 \cdots a_n b_n \in G : a_i \in A, b_j \in B, i, j \in \mathbb{N}\}.$$

Se $A, B \subseteq G$ poder-se-ia dizer o mesmo? Justifique.

2.4.6) Sejam G um grupo e $A, B \subseteq G$ tais que $AB = BA$. Prove que $\langle A \cup B \rangle = AB$.

2.4.7) Sejam $f : G \rightarrow H$ um morfismo de grupos e $G = \langle X \rangle$. Mostre que:

a) $f(\langle X \rangle) = \langle f(X) \rangle$.

b) Se $f \in \text{Surj}(G, H)$, então $f(\langle X \rangle) = H$.

2.4.8) Sejam G um grupo e $a \in G$.

- a) Mostre que se existem $r, s \in \mathbb{Z}$ com $r \neq s$ tais que $a^r = a^s$, então existe o menor inteiro positivo n , tal que $a^n = 1$. A esse elemento (se existe) chama-se a ordem de a , e representa-se por $\text{ord}(a)$. Se tal elemento não existe então diz-se que a ordem de a é infinita.
- b) Sejam $t \in \mathbb{Z}$ e $\text{ord}(a) = n$, então tem-se que, $a^t = e \iff n \mid t$.

2.4.9) Determine a ordem de cada elemento no respectivo grupo:

- a) $(S_3; \circ, \text{id})$.
- b) $(S_4; \circ, \text{id})$.
- c) $(\mathbb{Z}_3; +, \bar{0})$.
- d) $(\mathbb{Z}_6; +, \bar{0})$.
- e) $(\mathbb{Z}_4; \cdot, \bar{1})$.

2.4.10) Seja G um grupo abeliano. Mostre que:

- a) Se $a, b \in G$ tais que $\text{ord}(a) = n$ e $\text{ord}(b) = m$, então $(ab)^{mn} = 1_G$.
- b) Se G não é abeliano o resultado anterior pode não se verificar.

Sugestão: Considere em S_3 , $a := \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}$ e $b := \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}$.

2.4.11) Seja G um grupo abeliano. Prove que o subconjunto F , dos seus elementos de ordem finita é um subgrupo de G . Se G não fosse abeliano F seria subgrupo de G ? Justifique.

2.4.12) Sejam G um grupo e a um seu elemento de ordem finita. Mostre que $\text{ord}(a) = \text{ord}(a^{-1})$.

2.4.13) Construa a tabela de Cayley para um grupo $G := \langle a \rangle$ com $a \neq 1_G$ e $a^5 = 1_G$.

2.4.14) Considere o subconjunto $A := \{1, -1, -i, i\} \subseteq \mathbb{C}$.

- a) Mostre que $(A; \cdot, 1)$ é um grupo abeliano.
- b) Verifique se $(A; \cdot, 1)$ é cíclico e, em caso afirmativo, indique os seus geradores.
- c) Indique os subgrupos de $(A; \cdot, 1)$.

2.4.15) Prove que um elemento diferente do elemento neutro de um grupo tem ordem 2 se, e só se, é igual ao inverso de si próprio.

2.4.16) Dado um grupo cíclico $G = \langle a \rangle$ de ordem 10, indique todos os subgrupos de G .

2.4.17) Seja $G := \langle a \rangle$ um grupo tal que $a^{56} = a^{73}$.

- a) Supondo $a \neq 1_G$, qual é a ordem de G .
- b) Se fosse $a^{76} = a^{72}$ qual seria a ordem de G .

2.4.18) Mostre que se G é um grupo finito de ordem n , qualquer que seja o elemento $a \in G$ tem-se que $a^n = 1_G$.

2.4.19) Verifique que \mathbb{Z}_{12} tem um subgrupo de ordem k para cada divisor k , de 12.

- 2.4.20) Seja G um grupo cíclico gerado por a tal que $a^{21} = a^6$.
- Que pode concluir quanto à ordem de G ?
 - Qual a ordem do subgrupo gerado por a^7 ?
- 2.4.21) Seja $n = p_1^{r_1} p_2^{r_2} \cdots p_s^{r_s}$ a ordem dum grupo cíclico, em que, $p_1, p_2, \dots, p_s \in P(\mathbb{Z})$ e são distintos. Verificar que a é sempre o produto de s elementos do grupo cíclico, cujas ordens são $p_1^{r_1}, p_2^{r_2}, \dots, p_s^{r_s}$, respectivamente.
- 2.4.22) Sejam M, M' monóides, X um conjunto de geradores de M e $f, g \in \text{Mor}(M, M')$. Mostre que se $\forall x \in X, f(x) = g(x)$, então $f = g$.
- 2.4.23) Mostre que um grupo cíclico infinito tem exactamente dois geradores.
- 2.4.24) Seja G um grupo cíclico finito de ordem n , gerado por x . Mostre que $\langle x^k \rangle = G$ se, e só se, k é primo com n .
- 2.4.25) Seja M um monóide gerado pelo subconjunto X e suponha-se que todo o elemento de X é invertível (em M). Mostre que:
- M é um grupo.
 - Se separarmos os elementos inversos num conjunto X' disjunto de X , então $M = \langle X \cup X' \rangle$.
- 2.4.26) Sejam G um grupo cíclico, S um grupóide e $f \in \text{Surj}(G, S)$. Mostre que:
- S também é um grupo cíclico.
 - Se G é finito a ordem de S divide a ordem de G .
- 2.4.27) Seja G um grupo cíclico de ordem n . Mostre que existe uma aplicação bijectiva entre os subgrupos de G e os divisores positivos de n .
- 2.4.28) Mostre que:
- Cada grupo cíclico de ordem finita n é isomorfo ao grupo multiplicativo das n raízes de 1, em \mathbb{C} .
 - Cada grupo cíclico infinito é isomorfo a \mathbb{Z} .
- 2.4.29) Sejam G um grupo cíclico, $A \subseteq G$ e $f \in \text{End}(G)$. Mostre que:
- $f(A) \subseteq A$.
 - Se $G = \langle a \rangle$, então $f \in \text{Aut}(G)$ se, e só se, $\langle f(a) \rangle = G$.
- 2.4.30) Dois grupos cíclicos são isomorfos se, e só se, tiverem a mesma ordem.
- 2.4.31) Seja G um grupo cíclico de ordem 15. Qual o número de geradores de G ? Quantos automorfismos há de G em G ?

2.5. Relações de congruência. Coconjuntos

2.5.1) Mostre que a relação binária ρ definida no conjunto de todos os subgrupóides do grupóide S , por

$$A\rho B \iff A \cong B$$

é uma relação de equivalência em $\text{Sub}(S)$.

2.5.2) Prove que se $A \sqsubseteq G$ as seguintes afirmações são equivalentes:

i) $x^{-1}y \in A$,

ii) $xA = yA$.

2.5.3) Sejam G um grupo e $A \sqsubseteq G$. Mostre que qualquer que seja $x \in G$,

$$\text{card}(A) = \text{card}(Ax) = \text{card}(xA).$$

2.5.4) Defina-se uma relação de equivalência em \mathbb{Z} do seguinte modo:

$$a \sim b \iff a, b \in \mathbb{Z}_{<0} \vee a, b \in \mathbb{Z}_{\geq 0}.$$

Verifique que ficam determinadas duas classes de equivalência $[-1]$ e $[0]$. Do conjunto $\{[-1], [0]\}^2$ para $\{[-1], [0]\}$ defina uma operação binária $+$ tal que

$$[a] + [b] := [a + b]$$

por analogia com a definição de $+$ em \mathbb{Z}_n . Mostre que $+$ assim definida não é uma operação binária em \mathbb{Z}/\sim .

2.5.5) Seja S um semigrupo em que é válida a lei do corte e com elemento neutro. Sejam $X \subseteq S$ e ρ uma relação binária em S definida por:

$$a\rho b \iff b \in aX.$$

Mostre que ρ é uma relação de congruência se, e só se, X for um subgrupo tal que

$$\forall a \in S, Xa \subseteq aX.$$

2.5.6) Sejam S um semigrupo e R uma relação de equivalência em S . Defina-se

$$R^c := \{(a, b) \in S \times S : \forall x, y \in S, (xay, xby) \in R\}.$$

Mostre que:

a) $R^c \subseteq R$.

b) R^c é uma relação de equivalência.

c) R^c é uma relação de congruência.

d) Se μ é uma relação de congruência tal que $\mu \subseteq R$, então $\mu \subseteq R^c$.

2.5.7) Determine as classes associadas direitas de:

a) $\langle [4] \rangle$ em \mathbb{Z}_8 .

b) $\langle [3] \rangle$ em \mathbb{Z}_{12} .

2.5.8) Sejam G um grupo, $A \subseteq G$ e a relação binária \sim definida em G por:

$$x \sim y \iff y^{-1}x \in A.$$

Mostre que é uma relação de equivalência em G .

2.5.9) Sejam $G := S_3$ e $A := \langle (1\ 3) \rangle$.

- Determine as classes associadas direitas de A em G .
- Determine as classes associadas esquerdas de A em G .
- Verifique que a coleção das classes associadas direitas é diferente da das esquerdas.

2.5.10) Em S_3 calcule:

- As classes associadas direitas e esquerdas de $\langle (1\ 2\ 3) \rangle$.
- Verifique que para cada elemento σ de S_3 a classe associada direita à qual σ pertence é a mesma que a classe associada esquerda à qual σ pertence.

2.5.11) Determine, nos respectivos grupos:

- $[\mathbb{Z}_{10} : \langle [2] \rangle]$.
- $[S_3 : \langle (1\ 2) \rangle]$.
- $[S_4 : \langle (1\ 2\ 3) \rangle]$.
- $[\mathbb{Z}_{40} : \langle [12], [20] \rangle]$.

2.5.12) Prove que se A é um subgrupo de G tal que $[G : A] = 2$ e x e y são elementos de G mas não de A , então $xy \in A$.

2.5.13) Prove que se A e B são subgrupos finitos de um grupo G e $\text{card}(A)$ e $\text{card}(B)$ não tem factores comuns além de um, então $A \cap B = \{1_G\}$.

2.5.14) Determine os elementos do subgrupo $A := \langle (1\ 2\ 3), (1\ 2)(3\ 4) \rangle$ de S_4 e verifique que $\text{card}(A) = 12$ e que A não tem subgrupos de ordem 6.

2.5.15) Sejam G um grupo finito e A um seu subgrupo. Mostre que a ordem de A divide a ordem de G .

2.6. Estruturas normais. Estruturas quociente

2.6.1) Mostre que para um subgrupo A de G são equivalentes as seguintes afirmações:

- $A \trianglelefteq G$.
- $\forall x \in G, xA = Ax$.
- $\forall x, y \in G, xAyA \subseteq xyA$.
- $\forall x, y \in G, xAyA = xyA$.
- $\forall x \in G, xAx^{-1} \subseteq A$.
- $\forall x \in G, xAx^{-1} = A$.

2.6.2) Sejam G, H grupos e $f \in \text{Mor}(G, H)$. Mostre que:

- $\text{Ker}(f) \trianglelefteq G$.
- Se $f \in \text{Surj}(G, H)$, então $\text{Im}(f) \trianglelefteq H$.
- Se $A \trianglelefteq G$ então $f(A) \trianglelefteq \text{Im}(f)$.
- Se $A \trianglelefteq G$ e $f \in \text{Surj}(G, H)$, então $f(A) \trianglelefteq H$.
- Se $B \trianglelefteq H$, então $f^{-1}(B) \trianglelefteq G$.

2.6.3) Sejam G um grupo e $Z(G)$ o seu centro. Mostre que $Z(G) \trianglelefteq G$.

2.6.4) Mostre que $SL_n(\mathbb{K}) \trianglelefteq GL_n(\mathbb{K})$. Como $Z(GL_n(\mathbb{K})) \trianglelefteq GL_n(\mathbb{K})$ e $Z(SL_n(\mathbb{K})) \trianglelefteq SL_n(\mathbb{K})$ define-se o grupo linear projectivo por:

$$PGL_n(\mathbb{K}) := \frac{GL_n(\mathbb{K})}{Z(GL_n(\mathbb{K}))},$$

e o grupo linear projectivo especial por:

$$PSL_n(\mathbb{K}) := \frac{SL_n(\mathbb{K})}{Z(SL_n(\mathbb{K}))}.$$

2.6.5) Dado um grupo G finito, mostre que todo o seu subgrupo A de G de índice 2, é um subgrupo normal de G .

2.6.6) Sejam G um grupo, $N, K \trianglelefteq G$, $X \subseteq G$, $(A_i)_{i \in I} \in \text{Nor}(G)^I$ e $g \in G$. Mostre que:

- $N \cap K \trianglelefteq G$. Generalize $(A_i)_{i \in I} \in \text{Nor}(G)^I$.
- $NK \trianglelefteq G$.
- $\langle N \cup K \rangle \trianglelefteq G$.
- $\langle gXg^{-1} \rangle \trianglelefteq G$, que é o fecho normal de X em G é um subgrupo normal que contém X .
- $\text{Cor}_G(X) := \left\langle \bigcup_{\substack{i \in I \\ A_i \trianglelefteq G \\ A_i \subseteq X}} A_i \right\rangle \trianglelefteq G$.

2.6.7) Sejam G um grupo e $X \subseteq G$. Mostre que:

- $\forall g \in G, gXg^{-1} \subseteq X$, então $X \subseteq \langle X \rangle \trianglelefteq G$.

$$\text{b) } \left\langle \bigcup_{g \in G} gXg^{-1} \right\rangle \trianglelefteq G.$$

$$\text{c) } \left\langle \bigcup_{g \in G} gXg^{-1} \right\rangle = \langle X \rangle.$$

2.6.8) Sejam G um grupo, $N, K \trianglelefteq G$ e o elemento neutro é o único elemento comum a estes dois subgrupos. Mostre que os elementos de cada um dos subgrupos N e K são permutáveis com os elementos do outro.

2.6.9) Sejam G um grupo, $A \trianglelefteq G$ e $N \trianglelefteq G$. Mostre que $A \cap N \trianglelefteq A$.

2.6.10) Sejam G um grupo e $N, K \trianglelefteq G$ tais que $K \trianglelefteq N \trianglelefteq G$. Mostre que $\forall g \in G, gKg^{-1} \trianglelefteq N$.

2.6.11) Sejam G um grupo e $A, N \trianglelefteq G$ tais que $N \trianglelefteq A$. Mostre que:

a) Para todo o $K \trianglelefteq G$, $N \cap K \trianglelefteq A \cap K$.

b) Para todo o $P \trianglelefteq G$, $NP \trianglelefteq AP$.

2.6.12) Sejam G um grupo e $a \in G$. Um elemento $b \in G$ diz-se o conjugado direito de a , se existe um elemento $x \in G$ tal que $b = xax^{-1}$. Verifique que:

a) A relação conjugado direito, é uma relação de equivalência em G .

b) Um subgrupo A de G é saturado para esta relação se, e só se, $A \trianglelefteq G$.

(Nota: Sejam C um conjunto, ρ uma relação de equivalência definida em C e C/ρ o respectivo conjunto quociente. Diz-se que uma parte A de C é saturada para a relação ρ se, e só se, sempre que $x \in A$, $[x] \subseteq A$.)

2.6.13) Sejam G um grupo e $A \trianglelefteq G$. Mostre que:

a) $A \trianglelefteq N_G(A)$.

b) $N_G(A)$ é o maior subgrupo de G no qual A é normal.

2.6.14) Sejam G um grupo e $A \trianglelefteq G$. Diz-se que A é normal maximal em G se $A \trianglelefteq G$, $A \neq G$ e não existe $A' \trianglelefteq G$, tal que $A \subsetneq A' \subsetneq G$. Mostre que:

a) A é normal maximal em G se, e só se, G/A é um grupo simples.

b) Se A_1 e A_2 são subgrupos normais maximais distintos, então $A_1A_2 = G$ e $A_1 \cap A_2$ é normal maximal em A_1 e em A_2 .

2.6.15) Prove que $V := \{\text{id}, (1\ 2)(3\ 4), (1\ 3)(2\ 4), (1\ 4)(2\ 3)\}$ é um subgrupo normal de S_4 . Indique um grupo isomorfo a S_4/V .

2.6.16) Mostre que dado um grupo quociente G/H os subgrupos de G/H são exactamente os grupos A/H em que A é subgrupo de G e contém H .

2.6.17) Mostre que para qualquer grupo quociente G/N os seus subgrupos normais são exactamente os grupos quociente K/N em que $K \trianglelefteq G$ e que contém N .

2.6.18) Sejam G um grupo e $N \trianglelefteq G$. Prove que G/N é abeliano se, e só se, $\forall a, b \in G$ $aba^{-1}b^{-1} \in N$.

- 2.6.19) Sejam G, H grupos, $B \trianglelefteq H$ e $f \in \text{Surj}(G, H)$. Prove que, se $A := \{g \in G : f(g) \in B\}$, então $A \trianglelefteq G$.
- 2.6.20) Sejam G um grupo e $\sigma_g \in \text{Inn}_r(G)$. Então, tem-se que:
- para todo o $f \in \text{Aut}(G)$, $f \circ \sigma_g \circ f^{-1} = \sigma_{f(g)}$.
 - $\text{Inn}_r(G) \trianglelefteq \text{Aut}(G)$.
- 2.6.21) Sejam M, M' grupos abelianos e $f \in \text{Mor}(M, M')$. Mostre que:
- $\text{Coker}(f) := M' / \text{Im}(f)$ é um grupo abeliano.
 - $\text{Coim}(f) := M / \text{Ker}(f)$ é um grupo abeliano.
- 2.6.22) Sejam M, M' grupos abelianos e $f \in \text{Mor}(M, M')$ e considere-se a relação $g : M \rightarrow \text{Coker}(f)$ definida por $g(x) := [x]$. Mostre que:
- $g \in \text{Mor}(M, M')$.
 - Se $f \in \text{Surj}(M, M')$, então $g \in \text{Surj}(M, M')$.
- 2.6.23) Sejam M, M' grupos abelianos e $f \in \text{Mor}(M, M')$ e considere-se a relação $k : \text{Ker}(f) \rightarrow M'$ definida por $k(x) := f(x)$. Mostre que:
- $k \in \text{Mor}(M, M')$.
 - Se $f \in \text{Inj}(M, M')$, então $k \in \text{Inj}(M, M')$.

2.7. Teoremas do isomorfismo

2.7.1) Sejam G, G' grupos e $g \in \text{Surj}(G, G')$. Suponhamos que $N \trianglelefteq G$ e $\text{Ker}(g) \subseteq N$.

a) Mostre que:

1) $g(N) := N' \trianglelefteq G'$.

2) $g^{-1}(N') = N$.

b) Considere a aplicação $f : G \rightarrow G'/N'$ tal que para cada $x \in G$, $f(x) := [g(x)]_{N'}$. Verifique que:

1) f é um morfismo sobrejectivo de G em G'/N' .

2) $G/N \cong G'/N'$ (1.º Teorema do isomorfismo).

2.7.2) Sejam G um grupo e A, N subgrupos invariantes de G tais que $A \subseteq N$.

a) Sendo ν_A e ν_N os morfismos sobrejectivos canónicos associados a A e a N , respectivamente. Mostre que existe um morfismo sobrejectivo de grupos $h : G/A \rightarrow G/N$ tal que $h \circ \nu_A = \nu_N$.

b) Verifique que $\text{Ker}(h) = N/A$ e conclua que $G/N \cong \frac{G/A}{N/A}$ (Corolário do 1.º Teorema do isomorfismo).

2.7.3) Sejam G um grupo, $A, K \trianglelefteq G$ e $K \trianglelefteq A$.

a) Mostre que $AK \trianglelefteq G$.

b) Mostre que $K \trianglelefteq AK$.

c) Considere a aplicação $f : A \rightarrow (AK)/K$ tal que para cada $a \in A$, $f(a) := [a]_K$. Verifique que:

1) f é um morfismo sobrejectivo de A em $\frac{AK}{K}$.

2) $\frac{A}{A \cap K} \cong \frac{AK}{K}$ (2.º teorema do isomorfismo).

2.7.4) Sejam G_1, G_2 grupos, $N_1 \trianglelefteq G_1$ e $N_2 \trianglelefteq G_2$.

a) Se $N_1 \cong N_2$, ter-se-á que $G_1/N_1 \cong G_2/N_2$? E nas mesmas condições, mas sendo $G = G_1 = G_2$, será que se tem $G/N_1 \cong G/N_2$?

b) Se $N_1 \trianglelefteq G_1$, $N_2 \trianglelefteq G_2$, $N_1 \cong N_2$ e $G_1/N_1 \cong G_2/N_2$ ter-se-á que $G_1 \cong G_2$?

c) Se $N_1 \trianglelefteq G_1$, $N_2 \trianglelefteq G_2$, $G_1 \cong G_2$ e $G_1/N_1 \cong G_2/N_2$ ter-se-á que $N_1 \cong N_2$? E nas mesmas condições, mas sendo $G = G_1 = G_2$, será que se tem $N_1 \cong N_2$?

2.7.5) Use o teorema do homomorfismo para mostrar que se G é um grupo qualquer com elemento neutro 1_G , então $G/\{1_G\} \cong G$.

2.7.6) Mostre que se G_1, G_2 são grupos e $G_1 \times \{1_{G_2}\} \trianglelefteq G_1 \times G_2$, então $\frac{G_1 \times G_2}{G_1 \times \{1_{G_2}\}} \cong G_2$.

2.7.7) Mostre que $\mathbb{Z}_{18}/\langle [3] \rangle \cong \mathbb{Z}_3$.

2.7.8) Sejam G um grupo, $A \trianglelefteq G$, $N \trianglelefteq G$, $A \cap N = \{1_G\}$ e $A \cup N = G$. Mostre que $G/N \cong A$.

2.7.9) Seja G um grupo. Mostre que $G/Z(G) \cong \text{Inn}_r(G)$.

2.7.10) Sejam G um grupo, $H_1, H_2, K_1, K_2 \trianglelefteq G$ tais que $K_1 \trianglelefteq H_1$ e $K_2 \trianglelefteq H_2$. Mostre que:

a) (Lema da borboleta) $(H_1 \cap K_2)K_1 \trianglelefteq (H_1 \cap H_2)K_1$.

b) $(K_1 \cap H_2)K_2 \trianglelefteq (H_1 \cap H_2)K_2$.

c) $(K_1 \cap H_2)(H_1 \cap K_2) \trianglelefteq H_1 \cap H_2$.

d) Conclua que, $\frac{(H_1 \cap H_2) \cdot K_1}{(H_1 \cap K_2)K_1} \cong \frac{(H_1 \cap H_2)K_2}{(K_1 \cap H_2)K_2}$.

Este resultado usa-se no teorema do refinamento de Otto Schreier (1901-1929)

2.8. Estruturas actuando sobre conjuntos

2.8.1) Sejam G um grupo, $X \neq \emptyset$ um conjunto qualquer e o morfismo $f : G \rightarrow \text{Sym}(X)$, definido por $f(a) := f_a$. Mostre que, $f_a \in \text{Bij}(X, X)$ se, e só se, se tem a condição $f(1_G) = \text{id}_X$.

2.8.2) Sejam G um grupo e considere $X := G$. Mostre que:

- G actua à esquerda sobre G , se definirmos para todo o $g \in G$, $x \in X$, $gx := g \cdot x$ (esta acção chama-se acção de G em si próprio por multiplicações esquerdas).
- G actua à direita em G , considerando $gx := xg^{-1}$.
- G actua à esquerda em G por conjugação direita, i.e., a acção esquerda de G em G é definida por, $gx := gxg^{-1}$.
- o núcleo da acção por conjugação direita é o centro do grupo.

2.8.3) Sejam G um grupo finito e $A \in \text{Sub}(G)$. Mostre que, com a acção esquerda $gA := gAg^{-1}$, G actua em $\text{Sub}(G)$.

2.8.4) Sejam ${}_G X$ um G -conjunto e $X \subseteq G$. Considere o conjunto

$$\text{Stab}(X) := \{g \in G : \forall x \in X \quad gx = x\}.$$

Mostre que:

- $\text{Stab}(X)$ é um subgrupo de G .
- se $X := G$ e, actua por conjugação direita, então $\text{Stab}(X) = C_G(X)$.

2.8.5) Sejam G um grupo finito actuando num conjunto X . Mostre que:

$$\text{card}(\text{Orb}(x)) = [G : \text{Stab}(x)] = \frac{\text{card}(G)}{\text{card}(\text{Stab}(x))}.$$

2.8.6) Sejam ${}_G X$ um G -conjunto e considere-se a seguinte relação para todo o elemento $x, x' \in X$:

$$x \sim_G x' \iff \exists g \in G : gx = x'.$$

Mostre que:

- \sim_G é uma relação de equivalência em X .
- a classe de equivalência de um elemento $x \in X$ é igual à $\text{Orb}(x)$.

2.8.7) Sejam G um grupo actuando em X e $A \subseteq G$. Mostre que:

- A actua em X .
- $x \sim_A y \implies x \sim_G y$.

2.8.8) Sejam G, H grupos, ${}_H X$ e $f \in \text{Surj}(G, H)$. Verifique se:

- G actua em X se definirmos a acção por $gx := f(g)x$.
- $x, y \in X$, então $x \sim_H y \iff x \sim_G y$.

2.8.9) Sejam G um grupo, $A \subseteq G$ e X o conjunto dos coconjuntos esquerdos de A em G .

a) Mostre que:

1) G actua em X , para a acção $a(xA) := (ax)A$.

2) $\text{Ker}(f) = \bigcap_{x \in G} xAx^{-1}$.

3) $\text{Ker}(f)$ é o maior subgrupo normal de G que está contido em A .

4) a acção de G sobre X é efectiva se, e só se, A só contém como subgrupo normal de G , $\{1_G\}$.

b) Resolva o exercício anterior para uma acção esquerda de G no conjunto $B := \{Ax \in \mathcal{P}(G) : x \in G\}$ definida por $g(Ax) := (Ax)g^{-1}$.

2.8.10) Sejam ${}_G X$ um G -conjunto, $x, y \in X$ e $\text{Orb}(x) = \text{Orb}(y)$. Mostre que:

$$\text{card}(\text{Stab}(x)) = \text{card}(\text{Stab}(y)).$$

2.8.11) Sejam ${}_G X$ e ${}_G Y$ dois G -conjuntos. Mostre que $X \times Y$ é um G -conjunto definindo a acção esquerda do seguinte modo: $\forall (x, y) \in X \times Y, g(x, y) := (gx, gy)$.

2.8.12) Sejam X, Y dois G -conjuntos e se definirmos a seguinte relação de equivalência para todo o elemento de $X \times Y$ por:

$$(x, y)\rho(x', y') \iff \exists g \in G : gx = x' \wedge gy = y'.$$

Mostre que $\frac{X \times Y}{\rho}$ é um G -conjunto.

2.8.13) Mostre que ${}_G X$ induz uma acção esquerda no conjunto potência $\mathcal{P}(X)$ definindo-se para um elemento $A \neq \emptyset$, a acção por

$$gA := \{gx \in X : x \in A\} \quad \text{e} \quad g\emptyset := \emptyset.$$

2.8.14) Sejam X, Y conjuntos e G um grupo finito actuando à esquerda em X . Mostre que G actua à esquerda em Y^X se definirmos para cada aplicação $f \in Y^X, g \in G, x \in X$ a acção por $gf := f(g^{-1}x)$.

2.8.15) Sejam G, H grupos, X, Y conjuntos disjuntos e ${}_G X, {}_H Y$. Mostre que $G \times H$ actua em $X \dot{\cup} Y$ se definirmos a acção por, para todo o $x \in X \dot{\cup} Y$

$$\begin{cases} (g, h)x := gx, & \text{se } x \in X \\ (g, h)x := hx, & \text{se } x \in Y \end{cases}.$$

2.8.16) Sejam $\mathbb{K}[x]$ um espaço vectorial sobre o corpo \mathbb{K} e G actua à esquerda em \mathbb{K} . Mostre que G actua à esquerda em $\mathbb{K}[x]$ se para todo o $g \in G$ e $p \in \mathbb{K}[x]$ definimos a acção por:

$$gp := ga_0 + (ga_1)x + \cdots + (ga_n)x^n.$$

2.9. Grupos- p e grupos de Sylow

3. ESTRUTURAS LIVRES E APRESENTAÇÕES

BIBLIOGRAFIA

- [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 (Coleção Schaum)*. McGraw-Hill, 1965.