Estruturas Algébricas

Paulo J. Almeida

Enide Martins

Departamento de Matemática da Universidade de Aveiro

Conteúdo

Capítulo 1

Preliminares

1.1 Conjuntos e subconjuntos

Chama-se *conjunto* a qualquer colecção bem definida de objectos, que serão chamados *elementos* do conjunto. A expressão 'bem definida' é necessária, porque nem toda a colecção de objectos pode ser considerada um conjunto, devido ao famoso paradoxo de Bertrand Russell:

Paradoxo: Seja A a colecção de todos os conjuntos que não são elementos de si próprios. Suponhamos que A é um conjunto. Se A for elemento de A então por definição do conjunto A, obtém-se que A não é elemento de si próprio. Se A não é elemento de si próprio, então por definição do conjunto A tem-se que A é elemento de si próprio. Portanto, A não pode ser um conjunto. □

Os conjuntos serão representados por letras grandes e os seus elementos por letras pequenas. A notação

$$a \in A$$

significa que a é elemento de A (ou a *pertence* a A), A negação de $a \in A$ é denotada por $a \notin A$. Conjuntos podem ser definidos escrevendo os seus elementos entre chavetas, como por exemplo, $\{1, 7, 11\}$ ou através de uma descrição formal dos seus elementos, da forma

$$A = \{a \,|\, a \text{ tem a propriedade } P\},$$

i. e., o conjunto A é formado pelos elementos que verificam uma certa propriedade P.

Chama-se *cardinal* de A ao número de elementos do conjunto A e este número é denotado por $|A|$.

Dados dois conjuntos A e B, se qualquer elemento de A pertencer a B, escrevemos $A \subseteq B$ e dizemos que A é um *subconjunto* de B ou que A está contido em B. Se $A \subseteq B$ e $B \subseteq A$ então dizemos que A é igual a B e escrevemos $A = B$.

A um conjunto com zero elementos chamamos *conjunto vazio*. Claramente, um conjunto vazio é subconjunto de qualquer outro conjunto, e portanto, atendendo à definição de igualdade de conjuntos, há um único conjunto vazio, que denotamos por $\emptyset$ (ou por $\{\}$).

Alguns outros conjuntos também têm uma notação fixa, como por exemplo

$$\mathbb{N},\ \mathbb{Z},\ \mathbb{Q},\ \mathbb{R},\ \mathbb{C} \text{ e } \mathbb{H},$$

que representam, respectivamente, os conjuntos formados por números naturais $1, 2, 3, \ldots$, por inteiros, por racionais, por reais, por complexos e por quaterniões.

Podemos obter novos conjuntos a partir de conjuntos dados utilizando operações em conjuntos. Vejamos algumas destas operações. Sejam A e B conjuntos, então

- a *união* de A e B é o conjunto formado pelos elementos que pertencem a A ou a B (podendo pertencer a ambos). Denotamos este conjunto por $A \cup B$. Assim,

$$A \cup B = \{x \,|\, x \in A \,\text{ou}\, x \in B\};$$

- a *intersecção* de A e B é o conjunto formado pelos elementos que pertencem a A e a B, simultaneamente. Denotamos este conjunto por $A \cap B$. Assim,

$$A \cap B = \{x \,|\, x \in A \,\text{e}\, x \in B\};$$

- a *diferença* entre A e B (ou *complemento relativo* de B em A) é o conjunto formado pelos elementos que pertencem a A e não pertencem a B. Denotamos este conjunto por $A \setminus B$. Assim,

$$A \setminus B = \{x \,|\, x \in A \,\text{e}\, x \notin B\};$$

- a *união disjunta* entre A e B é o conjunto formado pelos elementos que estão em um e um só dos conjuntos A ou B. Denotamos este conjunto por $A \oplus B$. Note-se que

$$A \oplus B = A \cup B \setminus A \cap B.$$

Dois conjuntos A e B tais que $A \cap B = \emptyset$ dizem-se *disjuntos*.

Define-se também união e intersecção de colecção arbitrária de conjuntos $\{A_i \,|\, i \in I\}$, indexados num conjunto I, que denotamos por

$$\bigcup_{i\in I} A_i = \{x \,|\, x \in A_i, \text{ para algum } i \in I\} \quad \text{e} \quad \bigcap_{i\in I} A_i = \{x \,|\, x \in A_i, \text{ para qualquer } i \in I\}.$$

Em seguida, vamos listar as propriedades fundamentais da união, intersecção e diferença de conjuntos, cuja demonstração fica como exercício.

Proposição 1.1.1. *Sejam A, B e C conjuntos e considere-se a colecção $\{B_i \,|\, i \in I\}$. São válidas as seguintes afirmações:*

(i) $A \cup B = B \cup A$ *e* $A \cap B = B \cap A$;

(ii) $(A \cup B) \cup C = A \cup (B \cup C)$;

(iii) $(A \cap B) \cap C = A \cap (B \cap C)$;

(iv) $A \cup A = A = A \cap A$;

(v) $A \cup \emptyset = A$ *e* $A \cap \emptyset = \emptyset$;

(vi)

$$A \setminus \left(\bigcup_{i\in I} B_i \right) = \bigcap_{i\in I} (A \setminus B_i)$$

e

$$A \setminus \left(\bigcap_{i\in I} B_i \right) = \bigcup_{i\in I} (A \setminus B_i)\,.$$

Dada uma colecção finita de conjuntos $A_1, A_2, \ldots, A_n$, chamamos n-uplo a uma sequência de elementos $a_1, a_2, \ldots, a_n$ tais que $a_i \in A_i$, para cada $i \in \{1, 2, \ldots, n\}$ e denota-mo-lo por $(a_1, a_2, \ldots, a_n)$. O conjunto de todos os n-uplos é denotado por

$$A_1 \times A_2 \times \cdots \times A_n$$

e é denominado por *produto cartesiano* dos conjuntos $A_1, A_2, \ldots, A_n$.

Dado um conjunto A, chama-se *partes* de A ao conjunto formado por todos os subconjuntos de A, incluindo o conjunto vazio e o próprio conjunto A. Denota-se este conjunto por $P(A)$.

1.2 Relações

No que se segue E e F são dois conjuntos não vazios.

Definição 1.2.1. *Chama-se relação de E para F a todo o subconjunto do produto cartesiano $E \times F$.*

Definição 1.2.2. *Chama-se relação binária (ou simplesmente relação) definida em E a todo o subconjunto do produto cartesiano de $E \times E$.*

Usualmente E^2 significa $E \times E$, E^3 significa $E \times E \times E$ (conjunto dos ternos ordenados de elementos de E). Mais geralmente E^n significa o conjunto dos $n-$uplos ordenados de E. Assim, chama-se relação $n-$ária sobre E a qualquer subconjunto de E^n, onde n é um inteiro positivo.

Se R é uma relação binária definida em E, em termos de notação escreve-se

$$(a, b) \in R \text{ ou } a\, R\, b,$$

para designar que (x, y) é um elemento de R. Se (x, y) não é um elemento de R escreve-se

$$(a, b) \notin R \text{ ou } a \not R\, b.$$

Exemplo 1.2.3. *Considere-se o conjunto $X = \{1, 2, 3\}$. O conjunto $R = \{(1, 1), (2, 3), (3, 2)\}$ é uma relação binária definida em X pois é um subconjunto de $X \times X$.*

Mais, $(1, 1) \in R$ mas o par $(2, 2) \notin R$.

Exemplo 1.2.4. *Sejam $X = \{1, 2, 3, 4\}$ e $R = \{(x, y) \in X \times X : x + y \leq 5\}$. Tem-se*

$$R = \{(1, 1), (1, 2), (1, 3), (1, 4), (2, 1), (2, 2), (2, 3), (3, 1), (3, 2), (4, 1)\} \subseteq X \times X.$$

Então R é uma relação binária definida em X.

1.2.1 Classificação da Relações Binárias:

Seja E um conjunto e R uma relação binária definida em E. Diz-se que R é uma relação:

1. **Reflexiva** se para todo $x \in E$, tem-se $x\, R\, x$;
2. **Simétrica** se para quaisquer $x, y \in E$ que verifiquem $x\, R\, y$ tem-se $y\, R\, x$;
3. **Transitiva** se para quaisquer $x, y, z \in E$ que verifiquem $x\, R\, y$ e $y\, R\, z$ tem-se $x\, R\, z$;

4. **Anti-simétrica** se para quaisquer $x, y \in E$, que verifiquem $x\,R\,y$ e $y\,R\,x$, tem-se $x = y$;

5. **Tricotómica** se para quaisquer $x, y \in E$, tem-se $x\,R\,y$ ou $y\,R\,x$, ou $x = y$.

Definição 1.2.5 (Relação de equivalência)**.** *Diz-se que R é uma* relação de equivalência *se R é reflexiva, simétrica e transitiva.*

Definição 1.2.6 (Relação de ordem)**.** *Diz-se que R é uma* relação de ordem *se R é reflexiva, anti-simétrica e transitiva.*

1.2.2 Relações de equivalência

Exemplo 1.2.7. *Seja $B = \{a, b, c, d\}$ e*

$$R = \{(a,a), (b,b), (c,c), (d,d), (a,b), (b,a), (c,d), (d,c)\}.$$

A relação R é uma relação de equivalência.

Exemplo 1.2.8. *Sejam P o conjunto de todas as pessoas e D a relação "ter o mesmo pai que". A relação D é uma relação de equivalência.*

Exemplo 1.2.9. *Seja $\mathbb{Z}$ o conjunto dos inteiros. Defina-se $\sim$ em $\mathbb{Z}$ por $x \sim y$ se e só se $x - y$ é par. A relação $\sim$ é uma relação de equivalência.*

Exemplo 1.2.10. *(Congruência módulo p) Sejam $h, k \in \mathbb{Z}$ e $n \in \mathbb{Z}^+$. Diz-se que h é congruente com k módulo n se e só se $h - k$ é divisível por n, ou seja, $h - k = sn$, para algum $s \in \mathbb{Z}$, e escreve-se $h \equiv k \mod n$ (ou $h \equiv k(\mod n)$). De forma equivalente também se escreve $h \equiv k \mod n$, se e só se os restos das divisões de h e k por n são iguais. A relação anterior é uma relação de equivalência.*

De facto, $h - h = 0 = 0 \times n$, então $h \equiv h \mod n$ para qualquer $h \in \mathbb{Z}$; Assim a relação anterior é reflexiva.

Sejam $h, k \in \mathbb{Z}$ tais que $h \equiv k \mod n$. Então, existe $\alpha \in \mathbb{Z}$ tal que $h - k = \alpha n$. Mas então,

$$k - h = (-\alpha)n.$$

Como $-\alpha \in \mathbb{Z}$ então $k \equiv h \mod n$ e a relação anterior é simétrica.

Sejam agora $h, k, w \in \mathbb{Z}$ tais que

$$h \equiv k \mod n \text{ e } k \equiv w \mod n.$$

Então, existem $\alpha_1 \in \mathbb{Z}, \alpha_2 \in \mathbb{Z}$ tais que

$$h - k = \alpha_1 n \text{ e } k - w = \alpha_2 n.$$

Consequentemente,

$$(h - k) + (k - w) = \alpha_1 n + \alpha_2 n.$$

Donde,

$$h - w = (\alpha_1 + \alpha_2)n.$$

Como $\alpha_1 + \alpha_2 \in \mathbb{Z}$, então a relação anterior é transitiva.

Exemplo 1.2.11. *Pretende-se mostrar que se* $x \equiv x' \mod n$ *e* $y \equiv y' \mod n$ *então*

$$x + y \equiv x' + y' \mod n.$$

Por hipótese $x \equiv x' \mod n$ *e* $y \equiv y' \mod n$ *ou seja*

$$\begin{aligned} x - x' &= \theta_1 n, \text{ com } \theta_1 \in \mathbb{Z}, \\ y - y' &= \theta_2 n, \text{ com } \theta_2 \in \mathbb{Z}. \end{aligned}$$

Pretendemos provar que então $(x + y) - (x' + y') = \theta_3 n$, *com* $\theta_3 \in \mathbb{Z}$. *Ora*

$$(x + y) - (x' + y') = x - x' + y - y' = \theta_1 n + \theta_2 n = (\theta_1 + \theta_2)n = \theta_3 n,$$

com $\theta_3 = \theta_1 + \theta_2 \in \mathbb{Z}$.

Apresenta-se de seguida um exemplo duma relação binária que não é relação de equivalência.

Exemplo 1.2.12. *Em* $\mathbb{Z}$ *a relação binária definida por*

$$n \, R \, m \text{ se e só se } nm \geq 0,$$

não é uma relação de equivalência. De facto R *é reflexiva, pois para todo* $a \in \mathbb{Z}$, *tem-se* $a \, R \, a$ *uma vez que* $a^2 \geq 0$. *Também é simétrica: Se* $a \, R \, b$, *então* $ab \geq 0$, *e, portanto,* $ba \geq 0$, *pois em* $\mathbb{Z}$ *a multiplicação é comutativa. Assim* $b \, R \, a$. *No entanto,* R *não é transitiva, por exemplo,* $-3 \, R \, 0$ *e* $0 \, R \, 5$ *mas* -3 *não está relacionado com* 5.

Exercício 1.2.13. *Mostre que, em* $\mathbb{Z} \setminus \{0\}$ *a relação binária definida por*

$$n \, R \, m \text{ se e só se } nm > 0,$$

é uma relação de equivalência.

Exercício 1.2.14. *Seja E um conjunto não vazio. Prove que, se R é uma relação binária definida em E tal que*

1. $a\,R\,a$, $\forall a \in E$;

2. *para quaisquer $a, b, c \in E$ que verifiquem $a\,R\,b$ e $b\,R\,c$ tem-se $c\,R\,a$.*

então R é uma relação de equivalência.

Solução: De **1.** resulta que R é reflexiva. Prove-se que R é simétrica, ou seja,

$$\forall a, b \in E,\ a\,R\,b \Rightarrow b\,R\,a.$$

Sejam então $a, b \in E$ tais que $a\,R\,b$. Por **1.** tem-se que $b\,R\,b$.

Assim, de $a\,R\,b$ e $b\,R\,b$ resulta $b\,R\,a$, por **2.**.

Prove-se agora a transitividade: Sejam $a, b, c \in E$ tais que $a\,R\,b$ e $b\,R\,c$. Por **2.** temos $c\,R\,a$. Como se provou que R é simétrica resulta que $a\,R\,c$.

Portanto, R é uma relação de equivalência. □

1.2.3 Partições

Uma partição dum conjunto E é uma decomposição de E em subconjuntos não vazios tais que todo o elemento de E pertence a um e um só desses subconjuntos. A cada um desses subconjuntos chamamos elementos da partição. Apresenta-se a definição formal.

Definição 1.2.15 (Partição de um conjunto)**.** *Uma* partição *de E é uma colecção P de subconjuntos de E, $P = (P_i)_{i \in I}$, indiciados num conjunto I não vazio, tais que*

1. *Para qualquer $i \in I$, tem-se $P_i \neq \emptyset$;*

2. *Todo o elemento de E pertence a um e um só P_i, com $i \in I$.*

Note-se que os elementos duma partição de um conjunto E são disjuntos dois a dois.

Exemplo 1.2.16. *Seja $E = \{1, 2, 3, 4, 5, 6\}$. Uma partição de E é formada pelos subconjuntos $\{1, 6\}, \{3\}$ e $\{2, 4, 5\}$. Os subconjuntos $\{1, 2, 3, 4\}$ e $\{4, 5, 6\}$ não constituem uma partição de E uma vez que o elemento 4 pertence aos dois subconjuntos. Os subconjuntos $\{1, 2, 3\}$ e $\{5, 6\}$ não constituem uma partição de E uma vez que o elemento 4 não pertence a nenhum subconjunto.*

Proposição 1.2.17. *Sejam E e I conjuntos não vazios e $(P_i)_{i\in I}$ subconjuntos de E. Então $(P_i)_{i\in I}$ formam um partição de E se e só se as seguintes condições forem válidas*

1. *Para qualquer $i \in I$, $P_i \neq \emptyset$;*
2. $E = \bigcup_{i\in I} P_i$;
3. $P_i \cap P_j = \emptyset$ *para quaisquer $i, j \in I$, com $i \neq j$.*

Demonstração. Exercício. □

Exemplo 1.2.18. *Sejam $r \in \mathbb{R}$ e $T_r = \{x \in \mathbb{R} : x^2 = r\}$. Então o conjunto:*

$$\mathcal{T} = \{T_r : r \in \mathbb{R} \text{ e } r \geq 0\}$$

é uma partição de $\mathbb{R}$.

1.2.4 Classes de Equivalência

Seja agora R uma relação de equivalência definida em E. A relação R determina uma partição natural em E, onde os elementos da partição são dados por

$$\overline{a} = \{x \in E \,|\, x\, R\, a\}. \tag{1.1}$$

Note-se que a simetria de R permite escrever $\overline{a} = \{x \in E \,|\, a\, R\, x\}$. Em termos de notação também se usa $[a]_R$ ou simplesmente $[a]$.

Definição 1.2.19. *Ao conjunto (1.1) chama-se* classe de equivalência *relativa a a.*

Exemplo 1.2.20. *No exemplo 1.2.7 tem-se*

$$\overline{a} = \{a, b\}, \overline{b} = \{a, b\}, \overline{c} = \{c, d\}, \overline{d} = \{c, d\}.$$

Então a relação R referida particiona o conjunto B em duas classes:

$$\overline{a} = \overline{b} = \{a, b\}, \overline{c} = \overline{d} = \{c, d\}.$$

Exemplo 1.2.21. *Considere-se R a relação* paralelismo *no conjunto das rectas do plano. Esta relação binária é uma relação de equivalência. As classes de equivalência são os conjuntos das rectas paralelas entre si. A cada uma destas classes chama-se* direcção *do plano.*

Exemplo 1.2.22. *Seja $n \in \mathbb{Z}^+$. A relação de congruência módulo n, determina em $\mathbb{Z}$ uma partição em classes de equivalência denotadas por $\overline{0}, \overline{1}, \ldots, \overline{n-1}$, onde cada $\overline{i}, i \in \{0, 1, \ldots, n-1\}$ é o conjunto dos inteiros da forma $kn + i, i \in \{0, 1, \ldots, n-1\}$, ou seja, o conjunto dos inteiros cujo resto na divisão por n dá i. Por vezes usa-se a notação $0, 1, \ldots, n-1$, para representar as classes $\overline{0}, \overline{1}, \ldots, \overline{n-1}$, respectivamente. Cada classe de equivalência para a relação de congruência módulo n chama-se* classe residual módulo n.

De facto, para todo $i \in \mathbb{Z}$, denote-se por $i + n\mathbb{Z}$ o conjunto

$$i + n\mathbb{Z} = \{i + kn : k \in \mathbb{Z}\}.$$

é fácil ver que, dados $i, i^\star \in \mathbb{Z}$

$$i \equiv i^\star \mod n \Leftrightarrow i^\star \in i + n\mathbb{Z},$$

pelo que

$$\overline{i} = i + n\mathbb{Z} = \{\ldots, -2n + i, -n + i, i, i + n, 2n + i, \ldots\}.$$

1.2.5 Conjunto cociente

Definição 1.2.23 (Conjunto cociente)**.** *Ao conjunto de todas as classes de equivalência determinadas em E pela relação de equivalência R chama-se* conjunto cociente *e denota-se por E/R, ou seja,*

$$E/R = \{\overline{a}, a \in E\}.$$

O conjunto de todas as classes de equivalência determinadas em $\mathbb{Z}$ pela relação de congruência módulo n é $\{\overline{0}, \overline{1}, \ldots, \overline{n-1}\}$.

Exemplo 1.2.24. *O conjunto cociente determinado no conjunto das rectas do plano para a relação paralelismo é o conjunto de todas as direcções.*

Proposição 1.2.25. *Sejam $x, y \in E$, então $\overline{x} = \overline{y}$ se e só se $x\,R\,y$.*

Demonstração. Exercício. □

Proposição 1.2.26. *Sejam $x, y \in E$, então $\overline{x} = \overline{y}$ ou $\overline{x} \cap \overline{y} = \emptyset$.*

Demonstração. Exercício. □

Provar-se-á na proposição enunciada em seguida que o conjunto cociente é de facto, a partição determinada em E por R.

Proposição 1.2.27. *Seja R uma relação de equivalência definida em E. O conjunto cociente E/R é a partição determinada em E por R.*

Demonstração. Note-se que $x \in \overline{x}$ pois R é reflexiva pelo que $\overline{x} \neq \emptyset$. Seguidamente mostre-se que $\overline{x} \cap \overline{y} = \emptyset$ se $\overline{x} \neq \overline{y}$. Por redução ao absurdo suponha-se que existe $z \in \overline{x} \cap \overline{y}$. Então, por definição de intersecção de conjuntos tem-se

$$z \in \overline{x} \text{ e } z \in \overline{y}.$$

Por definição de $\overline{x}$ e $\overline{y}$, vem

$$z\,R\,x \text{ e } z\,R\,y,$$

mas, R é simétrica logo,

$$x\,R\,z \text{ e } z\,R\,y.$$

Donde, pela transitividade de R,

$$x\,R\,y.$$

Pela Proposição 1.2.25, tem-se

$$\overline{x} = \overline{y},$$

o que é absurdo. Assim,

$$\overline{x} \cap \overline{y} = \emptyset.$$

Prove-se agora que $\bigcup_{x \in E} \overline{x} = E$.

Claramente $\bigcup_{x \in E} \overline{x} \subseteq E$. De facto, se $y \in \bigcup_{x \in E} \overline{x}$ então existe $z \in E$ tal que $y \in \overline{z}$. Mas por definição de $\overline{z}$, tem-se $y \in E$.

Prove-se agora a inclusão contrária, ou seja $E \subseteq \bigcup_{x \in E} \overline{x}$.

Seja $y \in E$. Como R é reflexiva, $y\,R\,y$, ou seja $y \in \overline{y}$. Assim, $y \in \bigcup_{x \in E} \overline{x}$, donde se conclui que $E \subseteq \bigcup_{x \in E} \overline{x}$.

Das duas inclusões resulta que

$$\bigcup_{x \in E} \overline{x} = E.$$

□

Reciprocamente, dada uma partição $\mathcal{P} = \{P_i\ , i \in I\}$ de E podemos associar-lhe uma relação de equivalência R, tal que as classes de equivalência da relação sejam exactamente os elementos P_i de $\mathcal{P}$, a saber:

Para todos $a, b \in E$, diz-se que $a\,R\,b$ se e só se existe $i \in I$ tal que $a, b\ \in\ P_i$.

Proposição 1.2.28. *A relação R definida atrás é uma relação de equivalência sobre E. Mais, $\mathcal{P} = E/R$.*

Demonstração. Seja $a \in E$. Como $\bigcup_{i \in I} P_i = E$, então existe $i \in I$ tal que $a \in P_i$, donde $a\,R\,a$. Portanto R é reflexiva. A simetria é imediata.

Sejam agora $x, y, z \in E$ tais que $x\,R\,y$ e $y\,R\,z$. Então existem $i \in I$ e $j \in I$ tais que $x, y \in P_i$ e $y, z \in P_j$. Como $y \in P_i \cap P_j$, então $P_i \cap P_j \neq \emptyset$ pelo que $i = j$. Logo $x, z \in P_i$ e consequentemente $x\,R\,z$. Portanto R é transitiva. Logo R é relação de equivalência.

Prove-se agora que $\mathcal{P} = E/R$. Seja $[a]_R \in E/R$. Como $a \in E$, então existe $i \in I$ tal que $a \in P_i$. Mostre-se que $[a]_R = P_i$. Se $b \in [a]_R$ então $a\,R\,b$. Como $\{P_j\ , j \in I\}$ é uma partição de E e $a \in P_i$, então $b \in P_i$. Logo $[a]_R \subseteq P_i$.

Reciprocamente, se $c \in P_i$, então $c\,R\,a$ e consequentemente, $c \in [a]_R$. Portanto, $[a]_R = P_i$ e $[a]_R \in \mathcal{P}$. Donde $E/R \subseteq \mathcal{P}$.

Mostre-se agora que $\mathcal{P} \subseteq E/R$. Seja $P_i \in \mathcal{P}$. Porque $P_i \neq \emptyset$, seja $a \in P_i$. Como já se viu, $[a]_R = P_i$, donde $P_i \in E/R$. Logo $\mathcal{P} \subseteq E/R$ e consequentemente, $\mathcal{P} = E/R$. □

Definição 1.2.29. *A função*

$$\begin{array}{ccc} \pi : E & \to & E/R \\ x & \to & \overline{x} \end{array}, \tag{1.2}$$

é chamada projecção canónica *de E sobre E/R (ou* projecção canónica associada à relação *R).*

Exemplo 1.2.30. *Seja R a relação de paralelismo definido no conjunto das rectas do plano. Observou-se anteriormente que R é uma relação de equivalência neste conjunto. A projecção canónica associa a cada recta do plano a sua direcção, ou seja, a classe das rectas que lhe são paralelas.*

é fácil provar que a função definida anteriormente é sobrejectiva.

1.2.6 Exercícios

1. Em cada uma das alíneas seguintes averigue se a relação binária indicada é uma relação de equivalência. Em caso afirmativo determine o conjunto cociente.

   1.1. $R = \{(1,2),(2,3),(3,2)\}$, no conjunto $\{1,2,3\}$.

   1.2. fRg se e só se $f(0) = g(0)$, $\forall f, g \in \mathcal{F}(\mathbb{R})$, onde $\mathcal{F}(\mathbb{R})$ designa o conjunto das funções reais de variável real.

1.3. $(x,y)R(z,t)$ se e só se $xt = yz$, $\forall (x,y),(z,t) \in \mathbb{Z} \times \mathbb{Z} \setminus \{0\}$.

1.4. aRb se e só se $a+b$ é par, $\forall a,b \in \mathbb{N}$.

1.5. aRb se e só se $\frac{a}{b} \in \mathbb{Q}$, $\forall a,b \in \mathbb{R} \setminus \{0\}$.

1.6. $(a,b)R(c,d)$ se e só se $a^2+b^2 = c^2+d^2$, $\forall (a,b),(c,d) \in \mathbb{R}^2$.

1.7. nRm se e só se $nm \geq 0$, $\forall n,m \in \mathbb{Z}$.

1.8. nRm se e só se $nm > 0$, $\forall n,m \in \mathbb{Z}$.

1.9. xRy se e só se $x \geq y$, $\forall x,y \in \mathbb{R}$.

1.10. xRy se e só se $|x| = |y|$, $\forall x,y \in \mathbb{R}$.

1.11. xRy se e só se $|x-y| \leq 3$, $\forall x,y \in \mathbb{R}$.

2. Seja $E = \{\alpha, \beta, \gamma\}$.

2.1. Indique todos os conjuntos cociente distintos que podem definir-se em E.

2.2. Dê um exemplo duma relação binária definida em E que seja:

i. anti-simétrica e simétrica;

ii. reflexiva, transitiva e anti-simétrica;

iii. relação de equivalência.

3. Seja $\mathcal{A} = \{A_r \mid r \in \mathbb{R}\}$ onde $A_r = \{(x,y) \in \mathbb{R}^2 \mid y = 2x + r\}$, uma família de subconjuntos de $\mathbb{R}^2$. Prove que $\mathcal{A}$ é uma partição de $\mathbb{R}^2$ e descreva-a geometricamente. Indique também a relação de equivalência correspondente.

4. Sejam R uma relação de equivalência sobre E e S uma relação de equivalência sobre F, onde E e F são dois conjuntos não vazios. Em $E \times F$ define-se uma relação binária π do modo seguinte:

$$(x,y)\pi(x',y') \text{ se e só se } xRx' \text{ e } ySy'.$$

4.1. Prove que π é uma relação de equivalência em $E \times F$.

4.2. Determine $(E \times F)/\pi$ e prove que existe uma bijecção entre este conjunto e o conjunto $(E/R) \times (F/S)$.

5. Seja p um número inteiro maior ou igual a 1. Considere a relação R definida em $\mathbb{Z}$ por

$$xRy \text{ sse } p \text{ divide } x-y, \ \forall x,y \in \mathbb{Z}.$$

A R chama-se **congruência módulo** p e escreve-se $x \equiv y \pmod{p}$ em vez de xRy.

5.1. Mostre que p divide $x - y$ se e só se a divisão de x e y por p dá o mesmo resto.

5.2. Verifique que R é uma relação de equivalência sobre $\mathbb{Z}$.

5.3. Determine o conjunto cociente de $\mathbb{Z}$ sobre R, onde:

5.3.1. R é a relação de congruência módulo 3;

5.3.2. R é a relação de congruência módulo 5.

6. Sejam R_1 e R_2 relações binárias definidas num conjunto não vazio E. Em E define-se a relação binária U (designada por **reunião** de R_1 com R_2) do modo seguinte:

$$xUy \text{ se e só se } xR_1y \text{ ou } xR_2y, \text{ para todos } x, y \in E.$$

Indique, justificando, se as afirmações seguintes são verdadeiras ou falsas:

6.1. Se R_1 e R_2 são reflexivas, então U é reflexiva.

6.2. Se R_1 e R_2 são simétricas, então U é simétrica.

6.3. Se R_1 e R_2 são relações de equivalência, então U é relação de equivalência.

7. Sejam R_1 e R_2 relações binárias definidas num conjunto não vazio E. Chamamos **intersecção** de R_1 com R_2 e denota-se por $R_1 \cap R_2$ à relação binária definida em E do modo seguinte:

$$x(R_1 \cap R_2)y \text{ se e só se } xR_1y \text{ e } xR_2y, \text{ para todos } x, y \in E.$$

Chamamos **recíproca** de R_1 e representa-se por R_1^{-1} à relação binária definida em E por:

$$xR_1^{-1}y \text{ se e só se } yR_1x, \text{ para todos } x, y \in E.$$

Chamamos relação **identidade** em E e denota-se por I à relação definida por:

$$xIy \text{ se e só se } x = y, \text{ para todos } x, y \in E.$$

Mostre que R_1 é anti-simétrica se e só se $R_1 \cap R_1^{-1} \subseteq I$.

1.3 Funções

Definição 1.3.1. *Sejam A e B conjuntos. Uma* função *(ou* aplicação*) de A para B, simbolicamente*

$$f : A \longrightarrow B,$$

é uma regra que atribui a cada elemento a de A um único elemento $f(a)$ de B, a que se chama imagem de *a por f. Os elementos de A são chamados* objectos. *Os conjuntos A e B são o* domínio *e* conjunto de chegada *respectivamente.*

Definição 1.3.2. *Sejam $f : A \to B$ uma função e $E \subseteq A$ e $F \subseteq B$. Ao conjunto,*

$$f(E) = \{f(x), x \in E\},$$

chama-se conjunto imagem *de E em B por f ou apenas* imagem *de E. Quando $A = E$, o conjunto $f(A)$ também se denota por $\Im f$. Ao conjunto*

$$f^{-1}(F) = \{x \in A : f(x) \in F\}$$

chama-se imagem recíproca *de F em A.*

Definição 1.3.3. *Seja $f : A \longrightarrow B$ uma função.*

Diz-se que f é injectiva *se $f(a) = f(b)$ implicar $a = b$, i. e. objectos distintos têm imagens distintas.*

Diz-se que f é sobrejectiva *se qualquer elemento de B for imagem de algum elemento de A através de f, i. e. $\Im f = B$.*

Diz-se que f é bijectiva *se f for injectiva e sobrejectiva.*

1.3.1 Relação de Equivalência Associada a uma Função

Seja f uma função de domínio E. Pode associar-se a f uma relação binária, denotada por R_f do seguinte modo:

$$x \, R_f \, y \text{ se e só se } f(x) = f(y), \forall x, y \in E.$$

A relação anterior é usualmente conhecida por *relação de equivalência associada à função f.*

Proposição 1.3.4. *A relação binária R_f é uma relação de equivalência.*

Demonstração. Exercício. □

Dada uma relação de equivalência R definida em E pode associar-se uma função f de domínio E tal que a relação de equivalência associada à função f, R_f, coincide com R. De facto, a projecção canónica π associada a R preenche os requisitos anteriores.

Proposição 1.3.5. *Seja R uma relação de equivalência definida em E. A projecção canónica $\pi : E \to E/R$ é uma função definida em E tal que a relação de equivalência associada a π coincide com R.*

Demonstração. Considere-se a função π definida como em (1.2). Sejam $x, y \in E$. Tem-se,

$$\begin{aligned} xR_\pi y &\iff \pi(x) = \pi(y) \text{ por definição de } R_\pi; \\ &\iff \overline{x} = \overline{y}, \text{ por definição de } \pi; \\ &\iff x\,R\,y, \text{ pela Proposição 1.2.25.} \end{aligned}$$

Assim,

$$\forall x, y \in E, x\,R_\pi\,y \iff x\,R\,y$$

ou seja, $R_\pi = R$. □

Ver-se-á em seguida de que forma o conjunto cociente intervém na factorização duma qualquer função.

1.3.2 Decomposição Canónica de uma Função

Proposição 1.3.6. *Sejam $f : E \to F$ uma função e R_f a relação de equivalência associada a f. Então existe uma função*

$$\widetilde{f} : E/R_f \to F$$

tal que $f = \widetilde{f} \circ \pi$.

Demonstração. Considere-se o diagrama:

$$\begin{array}{ccc} E & \xrightarrow{f} & F \\ \pi\downarrow & \nearrow_{\widetilde{f}} & \\ E/R_f & & \end{array}$$

Defina-se $\widetilde{f}$ da seguinte forma:

$$\begin{array}{rcl} \widetilde{f} : E/R_f & \to & F \\ \overline{x} & \to & \widetilde{f}(\overline{x}) = f(x). \end{array}$$

Prova-se simultaneamente que $\widetilde{f}$ está bem definida e é injectiva. Sejam $\overline{x}, \overline{y} \in E/R_f$ tais que

$$\begin{aligned} \widetilde{f}(\overline{x}) = \widetilde{f}(\overline{y}) &\iff f(x) = f(y), \text{ por definição de } \widetilde{f}; \\ &\iff xR_f y, \text{ por definição de } R_f; \\ &\iff \overline{x} = \overline{y}, \text{ pela Proposição 1.2.25.} \end{aligned}$$

Finalmente, prova-se que $\widetilde{f}$ permite factorizar f como se pretende. Tem-se então, para todo $x \in E$,

$$\begin{aligned} \widetilde{f} \circ \pi(x) &= \widetilde{f}(\pi(x)), \text{ por definição de composição de funções;} \\ &= \widetilde{f}(\overline{x}), \text{ por definição de } \pi; \\ &= f(x), \text{ por definição de } \widetilde{f}. \end{aligned}$$

Provou-se assim que

$$\forall x \in E, \widetilde{f} \circ \pi(x) = f(x),$$

o que equivale a dizer que

$$\widetilde{f} \circ \pi = f.$$

□

Note-se que

$$\begin{aligned} \widetilde{f}(E/R_f) &= \{\widetilde{f}(\overline{x}), \overline{x} \in E/R_f\}, \text{ por definição de conjunto imagem;} \\ &= \{f(x), x \in E\} = f(E), \text{ porque } E/R_f \text{ é uma partição de } E; \\ &= f(E). \end{aligned}$$

Corolário 1.3.7. *Nas condições da proposição anterior existe uma bijecção entre E/R_f e $f(E)$.*

Demonstração. Claramente a função

$$\begin{aligned} \widetilde{f} : E/R_f &\to f(E) \\ \overline{x} &\to \widetilde{f}(\overline{x}) = f(x) \end{aligned}$$

é injectiva e sobrejectiva. □

Corolário 1.3.8. *Suponha-se que $f : E \to F$ é uma função sobrejectiva. Então existe uma bijecção $\widetilde{f}$ tal que*

$$f = \widetilde{f} \circ \pi.$$

Demonstração. Resulta imediatamente da proposição e corolário anterior. □

Considere-se $\iota : F \to F$ a função identidade em F. Claramente a restrição de ι a $f(E)$, denotada por i, é uma função injectiva. A essa função chama-se *imersão canónica*.

Corolário 1.3.9. *Existe uma bijecção g de E/R_f em $f(E)$ tal que $f = i \circ g \circ \pi$.*

Demonstração. Considere-se o diagrama:

$$\begin{array}{lll} E & \stackrel{f}{\to} & F \\ \pi \downarrow & & \uparrow i \\ E/R_f & \stackrel{\overline{g}}{\to} & f(E) \end{array}$$

Do Corolário 1.3.7, a função

$$\begin{array}{rcl} g : E/R_f & \to & f(E) \\ \overline{x} & \to & g(\overline{x}) = f(x) \end{array}$$

é uma bijecção. Resta provar que

$$\forall x \in E, i \circ g \circ \pi(x) = f(x).$$

De facto,

$$\begin{array}{rcl} i \circ g \circ \pi(x) & = & i \circ g(\pi(x)), \text{ por definição de composição de funções;} \\ & = & i \circ g(\overline{x}), \text{ por definição de } \pi; \\ & = & i(f(x)), \text{ por definição de } g \text{ e de composição de funções;} \\ & = & f(x), \text{ por definição de } i. \end{array}$$

□

1.3.3 Exercícios

1. Sejam $\mathcal{F}(\mathbb{R})$ o conjunto das funções reais de variável real e $\mathcal{D}(\mathbb{R})$ o conjunto das funções reais de variável real que são deriváveis. Considere a função $d : \mathcal{D}(\mathbb{R}) \to \mathcal{F}(\mathbb{R})$, que a cada $f \in \mathcal{D}(\mathbb{R})$ faz corresponder a sua derivada f'.

1.1. Defina a relação de equivalência associada a d, R_d, e determine o conjunto cociente $\mathcal{D}(\mathbb{R})/R_d$.

1.2. Obtenha a decomposição canónica de d. Prove directamente as propriedades que enunciar, para cada uma das funções intervenientes na decomposição.

2. Seja $f : \mathbb{R} \to \mathbb{R}$ a função que a cada $x \in \mathbb{R}$ faz corresponder $f(x) = \text{sen } x$.

2.1. Defina a relação de equivalência associada a f, R_f, e determine o conjunto cociente $\mathbb{R}/R_f$.

2.2. Indique justificando, um subconjunto de $\mathbb{R}$ que está em bijecção com $\mathbb{R}/R_f$.

3. Sejam E e F dois conjuntos não vazios e $f : E \to F$ uma função.

3.1. Defina relação de equivalência associada a f, R_f, e verifique que R_f é, de facto, uma relação de equivalência. Defina conjunto cociente E/R_f.

3.2. Prove que E/R_f está em bijecção com $f(E)$.

3.3. Diga o que entende por decomposição canónica de f.

3.4. Suponha que $E = \mathbb{R}$, $F = \mathbb{R}_0^+$ e $f(x) = |x|$, para todo $x \in \mathbb{R}$. Obtenha a decomposição canónica de f. Justifique sucintamente.

1.4 Conceitos Básicos de Estruturas Algébricas

1.4.1 Operações Internas

Definição 1.4.1. *Chama-se operação binária em E, ou apenas operação em E a toda a função*

$$\begin{array}{rcl} \star : E \times E & \to & E \\ (u, v) & \to & u \star v \end{array}.$$

A uma operação binária também se chama lei de composição interna ou operação interna.

Note-se que dizer que $\star$ é uma operação interna em E significa dizer que para todo $(x, y) \in E \times E$ existe um e um só $z \in E$ tal que

$$z = x \star y.$$

Diz-se também que E é **fechado** para a operação.

Exemplo 1.4.2. *Em $\mathbb{R}, \mathbb{C}$, $\mathbb{Z}, \mathbb{R}^+, \mathbb{Z}^+$, a adição e multiplicação usuais são operações internas.*

Exemplo 1.4.3. *Em $\mathbb{R}\backslash\{0\}$ a adição não uma operação interna. Note-se que $2 + (-2) = 0 \notin \mathbb{R}\backslash\{0\}$.*

Exemplo 1.4.4. *No conjunto $\mathcal{M}_4(\mathbb{C})$ das matrizes de tipo 4×4 com entradas em $\mathbb{C}$, a multiplicação de matrizes é uma operação interna.*

Exemplo 1.4.5. *Seja $\mathcal{F}$ o conjunto das funções reais de variável real. A adição de funções é uma operação interna em $\mathcal{F}$.*

Note-se que a adição de funções é uma aplicação definida da seguinte forma:

$$\begin{array}{rcl} + : \mathcal{F} \times \mathcal{F} & \to & \mathcal{F} \\ (f, g) & \to & f + g \end{array}$$

onde, para todo $x \in \mathbb{R}$, $(f + g)(x) = f(x) + g(x)$. Note-se que aqui o símbolo "+" tem aqui dois significados diferentes.

Exemplo 1.4.6. *Em $\mathbb{Z}^+$, $\star$, definida por $a \star b = \min\{a, b\}$ é uma operação interna.*

Exemplo 1.4.7. *Em $\mathbb{Z}^+$, $\star$, definida por $a \star' b = a$ é uma operação interna.*

Exemplo 1.4.8. *Em $\mathbb{Z}^+$, $\star''$, definida por $a \star'' b = (a \star b) + 2$, onde $\star$ está definida no Exemplo 1.4.6 é uma operação interna.*

Exercício 1.4.9. *Em $\mathbb{R}$ considere definida a operação interna θ do seguinte modo:*

$$x\theta y = xy - x - y + 2,$$

para todos os $x, y \in \mathbb{R}$. Prove que θ é ainda interna em $\mathbb{R}\backslash\{1\}$. **Resposta:** Sejam $x, y \in \mathbb{R}\backslash\{1\}$ quaisquer. Vamos provar que

$$x\theta y \neq 1.$$

Suponhamos que $x\theta y = 1$, isto é, $x\theta y = xy - x - y + 2 = 1$. Do anterior tem-se

$$(x - 1)y = x - 1.$$

Note-se que $x \neq 1$ e portanto do anterior resulta que $y = 1$ o que não pode acontecer. Assim,

$$x\theta y \neq 1.$$

Definição 1.4.10. *(Operação comutativa) Uma operação binária $\star$ definida em E diz-se comutativa se e só se*

$$\forall a, b \in E, a \star b = b \star a.$$

Definição 1.4.11. *(Operação associativa) Uma operação binária $\star$ definida em E diz-se associativa se e só se*

$$\forall a, b, c \in E, (a \star b) \star c = a \star (b \star c).$$

Exemplo 1.4.12. *A adição e multiplicação são operações associativas e comutativas em* $\mathbb{Z}$ *mas a subtracção não é comutativa nem associativa nesse conjunto.*

Exemplo 1.4.13. *A composição de funções reais de variável real é associativa mas não é comutativa.*

1.4.2 Operações Externas

Introduz-se agora o conceito de Operação Externa. De facto, já foi definido este conceito na disciplina de álgebra Linear e Geometria Analítica e apresentam-se alguns exemplos que nos são familiares.

Definição 1.4.14 (Operação externa com domínio de operadores K)**.** *Seja* $K \neq \varnothing$*. Chama-se lei de composição externa com domínio de operadores* K *ou simplesmente operação externa com domínio de operadores* K *a toda a função "*$\bullet$*" definida da seguinte forma,*

$$\begin{array}{rcl} \bullet : K \times E & \to & E \\ (k, x) & \to & k \bullet x \end{array}.$$

Neste caso, diz-se também que E é fechado para a operação externa com domínio de operadores K.

Exemplo 1.4.15. *Se* $\mathcal{V}$ *for o conjunto dos vectores livres do espaço, a multiplicação por um escalar real é uma função de* $\mathbb{R} \times \mathcal{V}$ *em* $\mathcal{V}$ *e portanto é uma lei de composição externa com domínio de operadores* $\mathbb{R}$*.*

Definição 1.4.16. *(Operação externa definida em E) Seja* $K \neq \varnothing$*. Chama-se lei de composição externa definida em* E *ou simplesmente operação externa definida em* E *a toda a função "*$\bullet$*" definida da seguinte forma,*

$$\begin{array}{rcl} \bullet : E \times E & \to & K \\ (x, y) & \to & x \bullet y \end{array}.$$

Exemplo 1.4.17. *O produto interno é uma função de* $\mathcal{V} \times \mathcal{V}$ *em* $\mathbb{R}$ *e portanto é uma lei de composição externa definida em* $\mathcal{V}$*.*

1.4.3 Estruturas e Subestruturas Algébricas

Definição 1.4.18. *A todo o conjunto munido de uma ou mais operações internas e/ou externas chama-se estrutura algébrica.*

Suponha-se que o conjunto E está munido duma operação interna, $\star$ e uma operação externa $\bullet$ relativamente a um conjunto $K \neq \varnothing$ de operadores. Denote-se esta estrutura algébrica por $(E, \star, \bullet)$.

Definição 1.4.19. *Uma subestrutura algébrica de $(E, \star, \bullet)$ é um subconjunto $S \neq \varnothing$ de E que é fechado para as operações $\star$ e $\bullet$ de E, isto é:*

$$\forall x, y \in S, x \star y \in S$$

$$\forall \alpha \in K, \forall x \in S, \alpha \bullet x \in S.$$

Duma forma geral, se $(E, \star_1, \star_2, \ldots, \star_n, \bullet_1, \bullet_2, \ldots, \bullet_m)$ é uma estrutura algébrica onde $\star_1, \star_2, \ldots, \star_n$ são n operações internas e $\bullet_1, \bullet_2, \ldots, \bullet_m$ são m operações externas, onde $n, m \in \mathbb{N}$, define-se subestrutura algébrica da estrutura anterior da seguinte forma:

Definição 1.4.20. *Uma subestrutura algébrica de $(E, \star_1, \star_2, \ldots, \star_n, \bullet_1, \bullet_2, \ldots, \bullet_m)$ é um subconjunto $S \neq \varnothing$ de E que é fechado para as operações $\star_1, \star_2, \ldots, \star_n$ e $\bullet_1, \bullet_2, \ldots, \bullet_m$ de E, isto é, se para todos $i \in \{1, \ldots, n\}, j \in \{1, \ldots, m\}$, se tem*

$$\forall x, y \in S, x \star_i y \in S,$$

$$\forall \alpha \in K, \forall x \in S, \alpha \bullet_j x \in S.$$

Sejam $P_1, P_2, \ldots, P_l, l \in \mathbb{N}$, propriedades estruturais (propriedades caracterizadoras da estrutura) de $(E, \star_1, \star_2, \ldots, \star_n, \bullet_1, \bullet_2, \ldots, \bullet_m)$. Para que $S \subseteq E$, e munido com as operações induzidas pelas operações de E seja uma subestrutura (do mesmo tipo) de E tem que satisfazer igualmente as propriedades estruturais de E.

Exemplo 1.4.21. *Seja $(\mathcal{V}, +, \bullet)$ um espaço vectorial sobre $\mathbb{R}$. O subconjunto não vazio S de $\mathcal{V}$ é um subespaço vectorial de $\mathcal{V}$ se, para as operações induzidas pelas operações de $\mathcal{V}$ satisfizer as propriedades estruturais de $\mathcal{V}$, ou seja os axiomas de espaço vectorial.*

Se S é uma subestrutura algébrica de E denota-se por $S \prec E$. Se além disso S satisfizer as mesmas propriedades estruturais de E diz-se que S é um subestrutura do mesmo tipo de E e denota-se por $S \leq E$.

Definição 1.4.22. *Chamam-se propriedades hereditárias a todas as propriedades de uma estrutura algébrica válidas em todos os seus subconjuntos não vazios.*

Exemplo 1.4.23. *A comutatividade e associatividade da adição de números reais.*

Definição 1.4.24. *Chamam-se propriedades não hereditárias a todas as propriedades de uma estrutura algébrica que não são válidas em todos os seus subconjuntos não vazios.*

1.4.4 Grupóides, Semigrupos e Monóides

Definição 1.4.25. *Chama-se* grupóide *a todo o par* $(E, \star)$ *onde* $\star$ *é uma operação interna definida em* E*. Se a operação é comutativa diz-se que o grupóide é comutativo.*

No que se segue $(E, \star)$ é um grupóide.

Definição 1.4.26. *(Elemento neutro à direita) Um elemento* $\theta \in E$ *diz-se elemento neutro à direita para* $\star$ *em* E *(ou em relação a* $\star$ *em* E*), se* $x \star \theta = x$*, para todo* $x \in E$*.*

Definição 1.4.27. *(Elemento neutro à esquerda) Um elemento* $\mu \in E$ *diz-se elemento neutro à esquerda para* $\star$ *em* E *(ou em relação a* $\star$ *em* E*), se* $\mu \star x = x$*, para todo* $x \in E$*.*

Definição 1.4.28. *(Elemento neutro) Um elemento* $e \in E$ *diz-se elemento neutro para* $\star$ *em* E *(ou em relação a* $\star$ *em* E*), se* $e \star x = x \star e = x$*, para todo* $x \in E$*.*

Note-se que e é simultaneamente elemento neutro à direita e à esquerda.

Exemplo 1.4.29. *O elemento* 0 *é elemento neutro à direita em relação à operação subtracção em* $\mathbb{R}$ *mas não é elemento neutro à esquerda. O elemento* 1 *é o elemento neutro em relação à multiplicação em* $\mathbb{Z}$*.*

Definição 1.4.30. *(Elemento invertível à direita) Um elemento* $x \in E$ *diz-se invertível à direita se e só se existe um elemento* $d \in E$ *tal que* $x \star d = e$*.*

Definição 1.4.31. *(Elemento invertível à esquerda) Um elemento* $x \in E$ *diz-se invertível à esquerda se e só se existe um elemento* $l \in E$ *tal que* $l \star x = e$*.*

Definição 1.4.32. *(Inverso de um elemento) Um elemento* $x' \in E$*, chama-se inverso de* $x \in E$ *se* $x \star x' = x' \star x = e$*.*

Definição 1.4.33. *Um elemento diz-se invertível se possui inverso único.*

Teorema 1.4.34. *Dado um grupóide* $(E, \star)$*, se existir elemento neutro este será único.*

Demonstração. Suponhamos que e e e_1 são dois elementos de E tais que, para todo $x \in E$,

$$e \star x = x \star e = x$$

e,

$$e_1 \star x = x \star e_1 = x.$$

Considere-se $e \star e_1$. Se e é o elemento neutro de E tem-se $e \star e_1 = e_1$. Mas, se e_1 é o elemento neutro de E, $e \star e_1 = e$. Assim,

$$e_1 = e \star e_1 = e.$$

□

Definição 1.4.35. *Chama-se* semigrupo *a todo o grupóide associativo, isto é, a operação do grupóide é associativa.*

Definição 1.4.36. *Chama-se* monóide *a um semigrupo com elemento neutro.*

Exemplo 1.4.37. $(\mathbb{N}, .)$ *é um monóide.*

Teorema 1.4.38. *Seja $(E, \star)$ um monóide com elemento neutro e. Se $a \in E$ é invertível à direita e à esquerda, então esses inversos coincidem e a é invertível sendo o seu inverso um desses elementos.*

Demonstração. Sejam a' e a'' os inversos de a à esquerda e à direita respectivamente.

$$\begin{aligned} a' = a' \star e &= a' \star (a \star a''), \text{ definição de } e \text{ e } a''; \\ &= (a' \star a) \star a'', \text{ pela associatividade de } \star \text{ em } E; \\ &= e \star a'' = a'', \text{ por definição de } e. \end{aligned}$$

□

Teorema 1.4.39. *Sejam $(E, \star)$ um monóide e a, $b \in E$. Suponha-se que a é invertível. Então as equações lineares $a \star x = b$ e $y \star a = b$ têm solução única.*

Demonstração. Primeiro mostrar-se-á que $a' \star b$ é uma solução de $a \star x = b$, onde a' é o inverso de a. Note-se que

$$\begin{aligned} a \star (a' \star b) &= (a \star a') \star b, \text{ pela associatividade de } \star \text{ em } E; \\ &= e \star b, \text{ definição de } a'; \\ &= b, \text{ por definição de } e. \end{aligned}$$

Analogamente se mostra que $y = b \star a$ é uma solução de $y \star a = b$. Para mostrar a unicidade da solução suponha-se que temos duas soluções y_1, y_2 tais que

$$y_1 \star a = b \text{ e } y_2 \star a = b.$$

Então

$$y_1 \star a = \ y_2 \star a.$$

Uma vez que $\star$ é uma operação, a' é o inverso de a e $\star$ é associativa, a igualdade anterior é equivalente a

$$(y_1 \star a) \star a' = (y_2 \star a) \star a'.$$

Que, tendo em atenção que a é invertível e, por definição de elemento neutro, o anterior é equivalente a

$$y_1 = y_2.$$

□

Definição 1.4.40. *(Cancelamento à direita) Seja $(E, \star)$ um grupóide. Se,*

$$\forall x, y, z \in E, x \star z = y \star z \Rightarrow x = y,$$

diz-se que z é cancelável (simplificável ou regular) à direita *para a operação $\star$.*

Definição 1.4.41. *(Cancelamento à esquerda) Seja $(E, \star)$ um grupóide. Se,*

$$\forall x, y, z \in E, z \star x = z \star y \Longrightarrow x = y,$$

diz-se que z é cancelável (simplificável ou regular) à esquerda *para a operação $\star$.*

Definição 1.4.42. *(Elemento cancelável) Um elemento diz-se* cancelável *(simplificável ou regular) para a operação $\star$ se for cancelável (simplificável ou regular) à direita e à esquerda.*

Definição 1.4.43. *(Lei do Cancelamento) Um grupóide $(E, \star)$ goza da* lei do cancelamento *ou* lei do corte *se todos os seus elementos forem canceláveis.*

Exemplo 1.4.44. *Em $(\mathbb{N}, +)$ é válida a lei do corte.*

Exemplo 1.4.45. *Em $(\mathbb{R}, .)$ não é válida a lei do corte pois por exemplo, $0 \times 2 = 0 \times 5$ e $2 \neq 5$.*

1.4.5 Homomorfismo de Grupóides

Definição 1.4.46. *Sejam $(E, \star)$ e $(F, \bullet)$ dois grupóides. Chama-se* homomorfismo *de $(E, \star)$ para $(F, \bullet)$ a toda a função $f : E \to F$ tal que*

$$\forall x, y \in E, f(x \star y) = f(x) \bullet f(y).$$

Exemplo 1.4.47. *Sejam $(\mathbb{N}, +)$ e $(2\mathbb{N}, +)$ dois grupóides. A função $f : \mathbb{N} \to 2\mathbb{N}$ tal que para todo $n \in \mathbb{N}, f(n) = 2n$, é um homomorfismo de grupóides.*

Teorema 1.4.48. *Sejam $(E,\star)$, $(F,\circ)$ dois grupóides. Se $f : E \to F$ é um homomorfismo entre os dois grupóides então $f(E)$ é fechado para a operação $\circ$.*

Demonstração. Sejam $a, b \in f(E)$. Por definição de $f(E)$, existem $u, v \in E$ tais que $a = f(u)$, $b = f(v)$. Assim,

$$a \circ b = f(u) \circ f(v) = f(u \star v),$$

porque f é um homomorfismo de grupóides. Note-se que como $(E,\star)$ é um grupóide $u \star v \in E$.

Provou-se assim que

$$\forall a, b \in f(E), a \circ b \in f(E).$$

□

No que se segue E e F são conjuntos não vazios.

Teorema 1.4.49. *Sejam $(E,\star)$, $(F,\circ)$ dois grupóides. Se $f : E \to F$ é um homomorfismo entre os dois grupóides então:*

(a) Se $\star$ é associativa em E, então $\star$ é associativa em $f(E)$;
(b) Se $\star$ é comutativa em E, então $\star$ é comutativa em $f(E)$;
(c) Se e é elemento neutro de $(E,\star)$ então $f(e)$ é elemento neutro de $(f(E),\circ)$;
(d) Se em $(E,\star)$, x' é o inverso de x, então $f(x)$ é o inverso de $f(x')$ em $(f(E),\circ)$.

Demonstração. Demonstrar-se-á apenas a alínea (c). As demonstrações das alíneas de $(a), (b)$ e (d) serão deixadas como exercício.

Seja $a \in f(E)$ um elemento arbitrário. Por definição de $f(E)$, existe um elemento $u \in E$ tal que $a = f(u)$. Vai-se provar que

$$a \circ f(e) = f(e) \circ a = a.$$

Tem-se então,

$$a \circ f(e) = f(u) \circ f(e) = f(u \star e) = f(u) = a,$$

uma vez que f é um homomorfismo de grupóides e e é o elemento neutro de $(E,\star)$. Analogamente se prova que $f(e) \circ a = a$, para todo $a \in f(E)$. □

A $(f(E),\circ)$ chama-se *imagem homomorfa* de E por f.

Teorema 1.4.50. *A composição de homomorfismos de grupóides ainda é um homomorfismo de grupóides.*

Demonstração. Exercício. □

Definição 1.4.51. *Sejam $(E,\star)$, $(F,\circ)$ dois grupóides e $f : E \to F$ um homomorfismo entre os dois grupóides. Diz-se que f é:*

1. *um monomorfismo se f é injectiva;*
2. *um epimorfismo se f é sobrejectiva;*
3. *um isomorfismo se f é bijectiva;*
4. *um endomorfismo se $E = F$;*
5. *um automorfismo se f endomorfismo e isomorfismo.*

Quando existe um isomorfismo entre os dois grupóides, escreve-se $E \simeq F$ e diz-se que os grupóides são isomorfos.

Suponha-se agora que em E, F estão definidas duas operações externas $\bullet$ e $\odot$ (relativamente a um mesmo conjunto de operadores $K \neq \varnothing$ respectivamente).

Definição 1.4.52. *Chama-se* homomorfismo *de E para F (ou de $(E,\bullet)$ para $(F,\odot)$) a toda a função $f : E \to F$ tal que*

$$\forall \alpha \in K, \forall x \in E, f(\alpha \bullet x) = \alpha \odot f(x).$$

1.4.6 Exercícios

1. Para cada uma das regras seguintes indique as que são operações internas e as que não são.

1.1. $a \star b = \sqrt{|ab|}$ em $\mathbb{Q}$;

1.2. $a \star b = \frac{a}{b}$ em $\mathbb{Z}$;

1.3. $(a,b) \star (c,d) = (a+c, cb+d)$ em $\mathbb{R}^2$;

1.4. $a \star b =$ raiz da equação $x^2 - a^2b^2 = 0$ em $\mathbb{R}$;

1.5. $a \star b = a \log b$ no conjunto $\{x \in \mathbb{R} \mid x > 0\}$;

1.6. $a \star b = a + b$ em $\mathbb{N}$;

1.7. $\star =$ subtracção no conjunto $\{x \in \mathbb{Z} \mid x \geq 0\}$.

2. Para as operações $\star$ em $\mathbb{R}^2$ das alíneas (a) e (b) definidas abaixo, indique se $\star$ verifica (ou não) as propriedades seguintes:

2.1. $\star$ é comutativa;

2.2. $\star$ é associativa;

2.3. $\mathbb{R}^2$ possui um elemento neutro relativamente a $\star$;

2.4. Todo o elemento $(a, b) \in \mathbb{R}^2$ tem inverso relativamente a $\star$;

(a) $(a, b) \star (c, d) = (ac, bd)$, $\forall (a, b), (c, d) \in \mathbb{R}^2$;

(b) $(a, b) \star (c, d) = (a + c, cb + d)$, $\forall (a, b), (c, d) \in \mathbb{R}^2$.

3. Sejam G um conjunto não vazio e $\star$ uma operação interna em G. Defina elemento neutro de $(G, \star)$.

4. Suponha $G = \mathbb{R}$ e $\star$ tal que $a \star b = \sqrt{a^2 + b^2}$. Indique, justificando, o valor lógico da seguinte proposição:

$(G, \star)$ tem elemento neutro.

5. Seja $G = \{\sigma : \mathbb{Z} \to \mathbb{Z}\}$. Para $\sigma, \tau \in G$ define-se $\sigma \star \tau$ como sendo a aplicação tal que para todo $n \in \mathbb{Z}$, $(\sigma \star \tau)(n) = \sigma(n) \cdot \tau(n)$, onde $\cdot$ designa o produto usual.

5.1. Verifique que $\star$ é uma operação interna.

5.2. Encontre, caso exista, o elemento neutro de $(G, \star)$.

5.3. Indique os elementos de $(G, \star)$ que possuem inverso.

Capítulo 2

Tópicos sobre Teoria de Grupos

2.1 Propriedades Elementares

Definição 2.1.1. *(Grupo) Um grupo $(G, \star)$ é um conjunto fechado para a operação binária $\star$ e que satisfaz os seguintes axiomas:*

$\mathcal{G}_1$: *A operação $\star$ é associativa;*
$\mathcal{G}_2$: *Existe um elemento $e \in G$ tal que $e \star x = x \star e = x$, para todo $x \in G$.*
$\mathcal{G}_3$: *Para todo $a \in G$, existe um elemento $a' \in G$, tal que $a \star a' = a' \star a = e$.*

Como já se viu, a e chama-se elemento neutro (ou identidade) de G e a a' chama-se o inverso de a. Para não sobrecarregar a notação por vezes denotar-se-á o grupo $(G, \star)$ apenas por G.

Definição 2.1.2. *(Grupo abeliano) Um grupo G diz-se abeliano se a operação binária $\star$ é comutativa.*

Apresentam-se agora alguns exemplos de estruturas que são grupos e outras que não estão nas condições do teorema anterior.

Exemplo 2.1.3. *A estrutura $(\mathbb{Z}^+, +)$ não é um grupo pois não existe elemento identidade.*

Exemplo 2.1.4. *O conjunto dos números inteiros não negativos (incluindo o zero) com a operação adição não é um grupo. Apesar de existir elemento identidade, não existe inverso para o elemento 2.*

Exemplo 2.1.5. *As estruturas $(\mathbb{R}, +), (\mathbb{Z}, +), (\mathbb{Q}, +)$ e $(\mathbb{C}, +)$ são grupos.*

Exemplo 2.1.6. *A estrutura* $(\mathbb{Z}^+, \times)$ *não é um grupo. Apesar de existir elemento identidade, o elemento* 3 *não possui inverso.*

Exemplo 2.1.7. $(\mathbb{R}^+, \times), (\mathbb{Q}^+, \times)$, $(\mathbb{Q}\backslash\{0\}, \times), (\mathbb{R}\backslash\{0\}, \times)$ *e* $(\mathbb{C}\ \backslash\{0\}, \times)$ *são grupos.*

Exemplo 2.1.8. *O conjunto das funções reais de variável real com a adição de funções é um grupo. Este grupo é abeliano.*

Exemplo 2.1.9. *O conjunto das matrizes de tipo* $m \times n, m, n \in \mathbb{N}$*, com entradas em* $\mathbb{R}$ *denotado por* $M_{m\times n}\ (\mathbb{R})$ *é um grupo para a adição de matrizes. A sua identidade é a matriz cujas entradas são todas nulas.*

Exemplo 2.1.10. *O conjunto* $M_n\ (\mathbb{R})$ *de todas as matrizes de tipo* $n \times n$ *com a operação multiplicação de matrizes não é um grupo. A matriz de tipo* $n \times n$ *cujas entradas são todas nulas não tem inverso.*

Exemplo 2.1.11. *O subconjunto* S *de* $M_n\ (\mathbb{R})$ *de todas as matrizes* $n \times n$ *invertíveis com a operação multiplicação de matrizes é um grupo. Este grupo não é abeliano.*

Nos exemplos anteriores apresentaram-se estruturas em que as operações eram bastante familiares. Apresenta-se agora um exemplo duma estrutura em que a sua operação binária não é tão familiar.

Exemplo 2.1.12. *Considere-se a estrutura* $(\mathbb{Q}^+, \star)$ *onde* $\star$ *está definida da forma seguinte:*

$$a \star b = \frac{ab}{2}.$$

Então,

$$(a \star b) \star c = \frac{ab}{2} \star c = \frac{abc}{4},$$

e, da mesma forma

$$a \star (b \star c) = a \star \frac{bc}{2} = \frac{abc}{4}.$$

Assim, $\star$ *é associativa. é fácil verificar que*

$$2 \star a = a \star 2 = a, \forall a \in \mathbb{Q}^+,$$

e portanto, 2 *é o elemento identidade para* $\star$*. Finalmente,*

$$a \star \frac{4}{a} = \frac{4}{a} \star a = 2,$$

e portanto $a' = \frac{4}{a}$ *é o inverso de* a *em* $\mathbb{Q}^+$*. Assim,* $\mathbb{Q}^+$ *com a operação* $\star$ *é um grupo.*

Proposição 2.1.13. *Num grupo a identidade é única e cada elemento possui inverso único.*

Demonstração. Resulta das proposições já apresentadas. □

Proposição 2.1.14. *Num grupo é válida a lei do corte.*

Demonstração. Exercício. □

Teorema 2.1.15. *Seja $(E, \star)$ um semigrupo com identidade à esquerda, e, (respectivamente, direita) e em que todos os elementos têm inverso à esquerda (respectivamente direita) então $(E, \star)$ é um grupo.*

Demonstração. Seja $a \in E$ e seja a^{-1} o inverso à esquerda de a. Então

$$\begin{aligned}(aa^{-1})^2 &= (aa^{-1})(aa^{-1}) \\ &= a(a^{-1}a)a^{-1} \\ &= a(ea^{-1}) \\ &= aa^{-1}\end{aligned}$$

Seja r o inverso à esquerda de aa^{-1}, então

$$\begin{aligned}aa^{-1} &= eaa^{-1} \\ &= (raa^{-1})aa^{-1} \\ &= r(aa^{-1})^2 \\ &= raa^{-1} \\ &= e.\end{aligned}$$

Portanto, a^{-1} é o inverso à direita de a. Agora, como

$$\begin{aligned}ae &= a(a^{-1}a) \\ &= (aa^{-1})a \\ &= ea \\ &= a,\end{aligned}$$

podemos concluir que e é elemento neutro de E. Provámos que todo o elemento tem inverso bilateral e que E tem elemento neutro, logo E é um grupo.

De forma análoga, conclui-se que um semigrupo com identidade à direita e em que todos os seus elementos têm inverso à direita é um grupo. □

2.1.1 Grupos Finitos e Tabelas de Entradas

Definição 2.1.16. *Um grupo G diz-se finito se tiver um número finito de elementos.*

Em termos de notação usa-se:

$$|G| < \infty$$

ou

$$\text{card}(G) < \infty.$$

Se G for um grupo infinito escreve-se $|G| = \infty$.

Definição 2.1.17. *Chama-se ordem de G ao número de elementos de G.*

Em termos de notação usa-se:

$$|G| \text{ ou } O(G).$$

Um grupo finito, $(G, \star)$ onde $G = \{x_1, x_2, \ldots, x_n\}$ pode ser representado por uma tabela $n \times n$ a duas entradas onde cada elemento (ou entrada) (i, j) é o produto $x_i \star x_j$. Um vez que um grupo tem pelo menos um elemento, a sua identidade, um conjunto minimal que poderá ter a estrutura de grupo é o conjunto $\{e\}$. A única operação binária $\star$ possível em $\{e\}$ está definida por

$$e \star e = e.$$

Claramente todos os axiomas de grupo são verificados.

Ir-se-á agora, num conjunto com dois elementos, introduzir uma estrutura de grupo. Como um desses elementos desempenhará o papel de identidade do grupo e considere-se esse conjunto igual a $\{e, a\}$. Para escrever a sua tabela de grupo ir-se-á listar os elementos na mesma ordem, em linha e coluna considerando o elemento identidade em primeiro lugar como se apresenta na tabela:

$\star$	e	a
e		
a		

,

Como e é o elemento identidade dever-se-á ter

$$e \star x = x \star e = x, \forall x \in \{e, a\}.$$

Assim, pode preencher-se a primeira linha e coluna da tabela da seguinte forma:

$\star$	e	a
e	e	a
a	a	

.

O elemento a deverá ter um inverso a' tal que

$$a \star a' = a' \star a = e.$$

Observe-se que $a' \in \{e, a\}$. O caso em que $a' = e$ não funciona pois nesse caso $a = e$, assim considere-se $a' = a$. A tabela final terá a forma:

$\star$	e	a
e	e	a
a	a	e

. (2.1)

Os axiomas $\mathcal{G}_2$ e $\mathcal{G}_3$ são verificados. O axioma $\mathcal{G}_1$ terá que ser verificado caso a caso.

Ir-se-á agora listar algumas condições necessárias e suficientes para que uma tabela onde está definida uma operação binária num conjunto finito deverá satisfazer para que o conjunto com essa operação estabeleça um estrutura de grupo nesse conjunto.

1. Deverá existir um elemento desse conjunto, denotado por e, que desempenhará o papel da identidade do grupo.

2. A condição $e \star x = x$ significa que na linha correspondente ao elemento e, os elementos do conjunto aparecem na mesma ordem de disposição em que se encontram na linha de topo.

3. A condição $x \star e = x$ significa que na coluna correspondente ao elemento e, os elementos do conjunto aparecem na mesma ordem de disposição em que se encontram na coluna colocada mais à esquerda da tabela.

4. O facto de que todo o elemento a tem inverso à direita significa que na linha correspondente a a o elemento identidade deverá aparecer na entrada de cruzamento dessa linha com a coluna onde se encontra esse inverso à direita.

5. O facto de que todo o elemento a tem inverso à esquerda significa que na coluna correspondente ao elemento a aparece o elemento identidade na entrada de cruzamento dessa coluna com a linha onde se encontra esse inverso à esquerda.

6. Pelo Teorema 1.4.39 as equações $a \star x = e$ e $y \star a = e$ têm soluções únicas. De forma análoga se prova que as equações $x \star a = e$ e $a \star y = e$ têm soluções únicas. Ora isso significa que cada elemento b do grupo deverá aparecer uma e uma só vez em cada linha e coluna.

7. A comutatividade é traduzida pela simetria relativamente à diagonal principal da tabela.

Note-se que a associatividade, a menos que seja definida alguma propriedade caracterizadora da operação, terá que ser verificada caso a caso.

Suponha-se agora temos um conjunto com três elementos. Considere-se como anteriormente, o conjunto $\{e, a, b\}$, onde e denota a identidade do grupo. Uma operação binária definida neste conjunto deverá ter associada uma tabela da seguinte forma:

$\star$	e	a	b
e	e	a	b
a	a		
b	b		

.

Esta tabela deverá ser preenchida da forma apresentada abaixo onde cada elemento aparece uma e uma só vez em cada linha e em cada coluna.

$\star$	e	a	b
e	e	a	b
a	a	b	e
b	b	e	a

. (2.2)

Ir-se-á ver uma forma fácil de verificar a associatividade que será apresentada no Exemplo 2.1.18 de tal forma que podemos obter a propriedade associativa para $\star$ em $\{e, a, b\}$. Suponha-se agora que temos outro grupo G' com três elementos em que a identidade é o elemento que aparece primeiro. Uma vez que o preenchimento da tabela para $G = \{ e, a, b\}$ foi feita apenas de uma única forma, poderá observar-se que se tomarmos a tabela de G' e considerarmos o seu elemento identidade com sendo e, o primeiro elemento como sendo a e o último elemento como sendo b, a tabela resultante para G' é precisamente a mesma que foi considerada para G. Observe-se então que a estrutura das duas tabelas é precisamente a mesma para os dois grupos e, um grupo poderá ser encarado como o outro grupo bastando para isso fazer uma correspondência entre os elementos.

Assim, quaisquer dois grupos com três elementos têm exactamente a mesma estrutura. Esta é a primeira referência que se fará ao conceito de isomorfismo entre grupos. Esta referência é feita duma forma informal. Dar-se-á mais tarde uma definição formal de isomorfismo entre grupos.

Exemplo 2.1.18. *é fácil verificar que para $n \in \mathbb{Z}^+$, as n soluções em $\mathbb{C}$ da equação $x^n = 1$ formam um grupo multiplicativo U_n. Assim,*

$$U_1 = \{1\}, U_2 = \{-1, 1\} \text{ e } U_3 = \{1, -\frac{1}{2} + \frac{\sqrt{3}}{2}i, -\frac{1}{2} - \frac{\sqrt{3}}{2}i\}$$

e,

$$U_4 = \{1, i, -1, -i\}$$

são grupos abelianos para a operação multiplicação de complexos. Ao grupo U_n , $n \in \mathbb{N}$ chama-se grupo multiplicativo das n-ésimas raízes da identidade.

Como se viu anteriormente, o grupo U_2 deverá ter a mesma estrutura (isomorfo a) que o grupo $\{e, a\}$ apresentado na tabela 2.1. Como se sabe que a operação definida em U_2 é associativa conclui-se imediatamente que a operação definida em $\{e, a\}$ é associativa. De forma semelhante a operação definida em U_3 é associativa. Pelas observações anteriores conclui-se que a operação definida na tabela 2.2 também é associativa. O grupo U_1 é isomorfo ao grupo $\{e\}$. O próximo exercício mostrará que a tabela para U_4 é uma das duas possibilidades que será apresentada para um conjunto com 4 elementos.

Exercício 2.1.19. *Considere o conjunto $\{e, a, b, c\}$. Construa as tabelas de possíveis candidatos a grupos.*

2.1.2 Propriedade Associativa Generalizada

Sejam $x_1, x_2, \ldots, x_n$ elementos do grupo G. Define-se o produto $x_1 x_2 \cdots x_n$ da seguinte forma:

$$\begin{aligned}
x_1x_2x_3 &= (x_1x_2)x_3 \\
x_1x_2x_3x_4 &= (x_1x_2x_3)x_4 = ((x_1x_2)x_3)x_4 \\
x_1x_2x_3x_4x_5 &= (x_1x_2x_3x_4)x_5 = (((x_1x_2)x_3)x_4)x_5 \\
&\vdots \\
x_1x_2x_3\cdots x_n &= (x_1x_2x_3\cdots x_{n-1})x_n = (\cdots((x_1x_2))x_3)\cdots x_{n-1})x_n.
\end{aligned}$$

Assim, se $p_j = x_1 x_2 \cdots x_j$, para $j \in \{1, \ldots, n\}$, então, $p_j = p_{j-1} x_j$ para qualquer $j > 1$. A propriedade associativa generalizada válida num semigrupo, diz-nos que o produto de elementos $x_1, \ldots, x_n$, por uma certa ordem não depende do modo de associação dos factores.

Exemplo 2.1.20. *Dados quatro elementos x_1, x_2, x_3 e x_4 dum grupo, os produtos*

$$((x_1x_2)x_3)x_4, (x_1x_2)(x_3x_4), (x_1(x_2x_3))x_4, x_1((x_2x_3)x_4), x_1(x_2(x_3x_4))$$

representam todos o mesmo valor, (note-se que $x_1x_2x_3x_4$ é por definição o valor da primeira destas expressões).

A propriedade associativa generalizada para produtos de quatro ou mais elementos dum grupo pode ser verificada pelo princípio de indução matemática no número de elementos envolvidos nesses produtos.

Considere-se um produto de n elementos do grupo G, quando $n > 3$. Sejam esses elementos, $x_1, x_2, \ldots, x_n$ ordenados pela ordem em que aparecem na expressão do seu produto. Suponha-se que a propriedade associativa generalizada é verificada para todos os produtos de elementos envolvendo um número inferior a n (isto é, quaisquer dois produtos envolvendo um número inferior a n elementos tomam o mesmo valor sempre que os elementos de G ocorrem nos dois produtos pela mesma ordem). Pretende-se provar que o valor do produto $x_1x_2\cdots x_n$ é

$$x_1x_2x_3\cdots x_n = (\cdots((x_1x_2))x_3)\cdots x_{n-1})x_n.$$

O primeiro passo é considerar o produto dum elemento $x_r \in G$ com o seu sucessor x_{r+1}. Os passos seguintes permitem calcular um produto de $n-1$ elementos, nomeadamente considerando os elementos x_i para $1 \leq i < r$, os elementos x_rx_{r+1}, e os elementos x_i para $r+1 < i \leq n$. A validade da propriedade associativa generalizada para produtos de elementos de G com um número inferior a n permite-nos concluir que o valor p do produto é dado por:

$$p = \begin{cases} (x_1x_2)x_3\cdots x_n & \text{se} \quad r = 1; \\ x_1(x_2x_3)\cdots x_n & \text{se} \quad r = 2; \\ x_1x_2(x_3x_4)x_5\cdots x_n & \text{se} \quad r = 3(\text{ e } n > 4) \\ \vdots & \vdots \\ x_1x_2\cdots x_{n-2}(x_{n-1}x_n) & \text{se} \quad r = n-1. \end{cases}$$

Da mesma forma, a propriedade associativa generalizada para produtos de elementos de G com um número inferior a n assegura que se $r < n-1$ então

$$x_1x_2\cdots x_{r-1}(x_rx_{r+1}) = x_1x_2\cdots x_{r+1}$$

e assim $p = x_1x_2\cdots x_n$. Assim, para verificar a propriedade associativa generalizada para produtos com n elementos basta verificar que

$$x_1x_2\cdots x_{n-2}(x_{n-1}x_n) = x_1x_2\cdots x_n.$$

O caso $n = 3$ é a propriedade associativa para produtos com três elementos. Para $n > 3$ seja y o produto $x_1x_2\cdots x_{n-2}$ dos elementos $x_1, x_2, \ldots, x_{n-2}$ (com $y = x_1x_2$ no caso em que $n = 4$). Então

$$\begin{aligned} x_1x_2\cdots x_{n-2}(x_{n-1}x_n) &= y(x_{n-1}x_n) = (yx_{n-1})x_n = (x_1x_2\cdots x_{n-1})x \\ &= x_1x_2\cdots x_n. \end{aligned}$$

Provou-se então que se a propriedade associativa generalizada se verifica para um produto de elementos de G com um número inferior a n então também se verifica para um produto de elementos de G com n elementos. A validade da referida propriedade segue-se por indução no número de elementos que está envolvido nesse produto.

Note-se que o único axioma de grupo que foi usado foi a propriedade associativa para três elementos. Assim, a propriedade associativa generalizada é válida em qualquer grupóide onde se verifica a associatividade para três elementos, ou seja num semigrupo. Assim, a referida propriedade é válida em qualquer semigrupo.

2.1.3 Potências num Grupo

A propriedade associativa generalizada válida num semigrupo, diz-nos que o produto de elementos $x_1, \ldots, x_n$, por uma certa ordem não depende do modo de associação dos factores, isto é:

$$(x_1\cdots x_r)(x_{r+1}\cdots x_n) = (x_1\cdots x_s)(x_{s+1}\cdots x_n)\forall r, s, 1 \leq r < s < n.$$

Claramente esta propriedade é válida num grupo.

Se $x_1 = \cdots = x_n = x$, define-se, para $n \in \mathbb{N}$, potência multiplicativa de x, como sendo o produto de x

$$x^n = x\cdots x. \tag{2.3}$$

Proposição 2.1.21. *Nas condições do que foi dito anteriormente, para $n, m \in N$, tem-se*

$$x^m x^n = x^{m+n} \tag{2.4}$$

e,

$$(x^m)^n = x^{mn}. \tag{2.5}$$

Demonstração. Prove-se em primeiro lugar (2.4). Para qualquer $m \in \mathbb{N}$, a demonstração é feita por indução em n. Se $n = 1$, tem-se $x^m x^1 = x^m x = x^{m+1}$, atendendo à associatividade.

Para qualquer $m \in \mathbb{N}$, $x^m x^{n+1} = x^m(x^n x) = (x^m x^n)x = x^{m+n}x = x^{(m+n)+1} = x^{m+(n+1)}$. Prove-se agora (2.5). Ir-se-á fazer a demonstração por indução em m. Para qualquer $n \in \mathbb{N}$, se $m = 1$, tem-se $(x^n)^1 = x^n = x^{n1}$. Admita-se que para todo $n \in \mathbb{N}$, se tem $(x^n)^m = x^{nm}$. Então, para qualquer $n \in \mathbb{N}$, utilizando (2.4) e a hipótese de indução:

$(x^n)^{m+1} = (x^n)^m x^n = x^{nm}x^n = x^{nm+n} = x^{n(m+1)}$. □

Convenciona-se que

$$x^0 = e, \text{ (ou } x^0 = 1).$$

Se no grupo G está definida uma notação aditiva, escreve-se $(G, +)$, e, em vez de (2.3), (2.4) e (2.5) tem-se

$$nx = x + \cdots + x.$$

$$mx + nx = (m + n)x$$

e,

$$(\ n \text{ parcelas }\ ) \ mx + \cdots + mx = n(mx) = (nm)x, \text{ para } n, m \in \mathbb{N}.$$

Num grupo multiplicativo, além das potências de expoente inteiro não negativo define-se também potências de expoente negativo do seguinte modo:

$$x^{-n} = (x^{-1})^n, n \in \mathbb{N}.$$

2.1.4 Conjugado e Comutador

Seja G um grupo (considere-se um grupo multiplicativo).

Definição 2.1.22. *Chama-se conjugado de x por y, denota-se por x^y, ao elemento de G,*

$$x^y = y^{-1}xy.$$

Definição 2.1.23. *Chama-se comutador de x e y, denota-se por $[x, y]$, ao elemento de G,*

$$[x, y] = xyx^{-1}y^{-1}.$$

Exercício 2.1.24. *Sejam G um grupo multiplicativo com elemento neutro e e $x, y, z \in G$. Mostre que:*

1. $(x^y)^{-1} = (x^{-1})^y$.

Demonstração. Mostre-se apenas que $x^y(x^{-1})^y = e$. é deixado como exercício que $(x^{-1})^y x^y = e$. Tem-se então, por definição de conjugado,

$$x^y(x^{-1})^y = (y^{-1}xy)(y^{-1}x^{-1}y).$$

Tem-se então,

$$\begin{aligned}
(y^{-1}xy)(y^{-1}x^{-1}y) &= (y^{-1}x)(yy^{-1})(x^{-1}y), \text{pela associatividade,} \\
&= (y^{-1}x)e(x^{-1}y), \text{pela definição de elemento inverso} \\
&= (y^{-1}x)(x^{-1}y), \text{ pela definição de elemento neutro} \\
&= y^{-1}(xx^{-1})y, \text{pela associatividade} \\
&= e \text{ pela definição de elemento inverso e elemento neutro.}
\end{aligned}$$

□

2. $(xy)^z = x^z y^z$.

3. $x^z = y \iff x = y^{z^{-1}}$

4. $[x,y]^{-1} = [y,x]$.

5. Sejam G um grupo e $x_1, \ldots, x_n, y$ elementos de G, $n \in \mathbb{N}$. Mostre que

$$(x_1 x_2 \cdots x_n)^y = x_1^y \cdots x_n^y.$$

Exercício 2.1.25. *Sejam G um conjunto não vazio e $\star$ uma operação interna em G.*

1. Defina elemento neutro de $(G, \star)$.

Resposta: Diz-se que $e \in G$ é elemento neutro de G se e só se $e \star a = a \star e = a$, para todo $a \in G$.

2. Suponha $G = \mathbb{R}$ e $\star$ tal que $a \star b = \sqrt{a^2 + b^2}$. Indique, justificando, o valor lógico da seguinte proposição:

$$(G, \star) \text{ tem elemento neutro.}$$

Resposta: Seja então $e \in G$. Para que e seja o elemento neutro de $(G, \star)$, tem que verificar-se

$$a \star e = \sqrt{a^2 + e^2} = a \text{ e } e \star a = \sqrt{e^2 + a^2} = a.$$

Considere-se apenas uma das igualdades. O estudo da outra é análogo.

Tem-se $\sqrt{a^2+e^2}=a$ o que **implica** que $a^2+e^2=a^2$ donde resulta que $e=0$. Ora, para que se verifique a implicação contrária, $e=0$ terá que verificar $\sqrt{a^2+e^2}=a$. Mas isso não acontece para todo $a\in\mathbb{R}$, pois $\sqrt{a^2}=|a|$. Basta tomar $a=-1$. Assim, o valor lógico é falso.

2.1.5 Exercícios

1. Averigue se os conjuntos seguintes têm estrutura de grupo para as operações indicadas:

1.1. $(\mathbb{Q}\setminus\{0\},\times)$;

1.2. $(\mathbb{R},\star)$, com $x\star y=x+y-xy$, $\forall x,y\in\mathbb{R}$;

1.3. O conjunto das soluções complexas da equação $x^n-1=0$, $n\in\mathbb{N}$, para a multiplicação;

1.4. O conjunto das soluções reais da equação da alínea anterior para a mesma operação;

1.5. O conjunto das aplicações $\alpha_{a,b}:\mathbb{R}\to\mathbb{R}$, $a\in\mathbb{R}\setminus\{0\}$, $b\in\mathbb{R}$ definidas por $\alpha_{a,b}(x)=ax+b$, $\forall x\in\mathbb{R}$, para a composição de aplicações;

1.6. $(A,\times)$ onde $A=\{\cos\theta+i\,\mathrm{sen}\,\theta\in\mathbb{C}\mid\theta\in\mathbb{R}\}$;

1.7. $(G^S,\otimes)$, onde $(G,\times)$ é um grupo, G^S designa o conjunto das aplicações de um conjunto $S\neq\varnothing$ em G e

$$(f\otimes g)(s)=f(s)\times g(s),\ \forall f,g\in G,\ \forall s\in S;$$

2. Os inteiros pares constituirão um grupo para a adição? E os ímpares? E os números reais para a multiplicação?

3. Prove que:

3.1. Se a e b são elementos de um grupo tais que $ab=a$, então $b=e$, sendo e o elemento neutro do grupo.

3.2. O único elemento idempotente de um grupo é o elemento neutro.

4. Considere definidas no conjunto $A=\{a,b,c,d\}$ as seguintes operações:

$+$	a	b	c	d
a	a	b	c	d
b	b	a	d	c
c	c	d	a	b
d	d	b	c	a

$\times$	a	b	c	d
a	d	c	b	a
b	c	a	d	b
c	b	d	a	c
d	a	b	c	d

Diga, justificando, se algumas das operações confere ao conjunto uma estrutura de grupo.

5. Sejam a, b, c e x elementos dum grupo G. Resolva em ordem a x as equações seguintes em G:

5.1. $axb = c$.

5.2. $x^2a = bxc^{-1}$ e $acx = xac$.

5.3. $x^2 = a^2$ e $x^5 = 1$.

5.4. $(xax)^3 = bx$ e $x^2a = (xa)^{-1}$.

5.5. $x^2b = xa^{-1}c$.

6. Em cada uma das alíneas seguintes prove que a proposição é verdadeira para qualquer grupo G ou, caso contrário, dê um contra-exemplo mostrando que é falsa em pelo menos um grupo.

6.1. Se $x^2 = 1$, então $x = 1$;

6.2. $(ab)^2 = a^2b^2$;

6.3. Para todo $x \in G$ existe $y \in G$ tal que $x = y^2$ (isto é equivalente a dizer que todo o elemento de G tem uma "raiz quadrada");

6.4. Se $x^2 = a^2$, então $x = a$;

6.5. Se $x^2 = x$, então $x = 1$.

7. Mostre que, num grupo, $(x^{-1}yx)^k = x^{-1}yx \iff y^k = y$, $\forall k > 0$.

8. Seja G um grupo. Prove que as condições seguintes são equivalentes:

8.1. G é abeliano.

8.2. $\forall a, b \in G,\ aba^{-1}b^{-1} = e$, onde e é o elemento neutro de G.

8.3. $\forall a, b \in G,\ (ab)^2 = a^2b^2$.

9. Sejam a e b elementos de um grupo tais que $a^2 = e$ e $aba = b^3$. Prove que $b^8 = e$.

10. Mostre que

10.1. $a \leftrightharpoons b \iff aba^{-1}b^{-1} = 1$; (onde $a \leftrightharpoons b$ significa que a comuta com b)

10.2. $a \leftrightharpoons b \iff a^{-1} \leftrightharpoons b^{-1}$.

11. Seja G um grupo. Sejam a, x e y elementos de G. Mostre que, se $xay = a^{-1}$, então $yax = a^{-1}$.

12. Seja G um grupo. Mostre que:

12.1. Se $a, b \in G$ são tais que $a = a^{-1}$ e $b = b^{-1}$, então $ba = (ab)^{-1}$.

12.2. Se para todo $a \in G$, $a^2 = 1$, então G é comutativo.

13. Sejam G um grupo, a e x elementos de G. Prove as seguintes proposições:

13.1. Se $x^2ax = a^{-1}$, então a tem uma raiz cúbica.
(sugestão: Mostre que xax é uma raiz cúbica de a^{-1}.)

13.2. Se $a^3 = 1$, então a tem uma raiz quadrada.

2.2 Subgrupos

Definição 2.2.1. *(Subgrupo) Seja H um subconjunto não vazio dum grupo G. Diz-se que H é um subgrupo de G se H é um grupo relativamente à operação que confere a G a estrutura de grupo.*

Em termos gerais, H é uma subestrutura do mesmo tipo de G e por isso denota-se por $H \leq G$.

Exemplo 2.2.2. *Considere-se $\mathbb{R}^n$ o grupo aditivo de todos os vectores com entradas reais. O subconjunto constituído pelos vectores em que a primeira componente é nula é um subgrupo de $\mathbb{R}^n$.*

Definição 2.2.3. *(Subgrupos próprios ou triviais) Chamam-se subgrupos impróprios ou triviais a G ou $\{e\}$. Todos os outros subgrupos são chamados próprios ou não triviais.*

Exemplo 2.2.4. *$\mathbb{Q}^+$ com a operação multiplicação é um subgrupo próprio de $\mathbb{R}^+$ com a operação multiplicação.*

Exemplo 2.2.5. *O conjunto das n-ésimas raízes da identidade U_n, $n \in \mathbb{N}$, é um subgrupo do grupo $\mathbb{C}\backslash\{0\}$, conjunto dos números complexos não nulos.*

Proposição 2.2.6. *Seja H um subgrupo de G e $a \in H$. Então a identidade de H coincide com a identidade de G e o inverso de a em H coincide com o inverso de a em G.*

Demonstração. Considere-se e_H e e_G a identidade de H e G respectivamente.

Seja $a \in H$ e sejam a_G^{-1} o inverso de a em G. Como e_H é a identidade de H tem-se

$$e_H a = a.$$

Como $H \subseteq G$, da igualdade anterior em G obtém-se

$$e_H(aa_G^{-1}) = (e_H a)a_G^{-1} = aa_G^{-1} = e_G.$$

Mas como e_G é a identidade de G e $e_H \in G$ temos

$$e_H = e_H e_G = e_H(aa_G^{-1}) = e_G.$$

Seja a_H^{-1} o inverso de a em H. Então

$$a_H^{-1} = a_H^{-1}e_G = a_H^{-1}(aa_G^{-1}) = (a_H^{-1}a)a_G^{-1} = e_H a_G^{-1} = e_G a_G^{-1} = a_G^{-1}.$$

□

A partir de agora denotar-se-á apenas por a^{-1} o inverso de um elemento a.

Proposição 2.2.7. *Sejam G um grupo e $a, b \in G$. Então $(ab)^{-1} = b^{-1}a^{-1}$ e $(a^{-1})^{-1} = a$.*

Demonstração. Dos axiomas de grupo segue-se

$$(ab)(b^{-1}a^{-1}) = a(b(b^{-1}a^{-1})) = a((bb^{-1})a^{-1}) = a(ea^{-1}) = aa^{-1} = e.$$

De forma análoga prova-se que $(b^{-1}a^{-1})(ab) = e$, e assim $b^{-1}a^{-1}$ é o inverso de ab. A segunda igualdade prova-se de forma análoga. □

2.2.1 Caracterização de Subgrupos

Apresentam-se de seguida condições necessárias e suficientes para que um subconjunto não vazio de um grupo seja um subgrupo.

Teorema 2.2.8. *(Caracterização de um subgrupo) Sejam G um grupo e H um subconjunto não vazio de G. Diz-se que H é um subgrupo de G se e só se*

$$1.\ \forall x, y \in H, xy \in H$$
$$2.\ \forall x \in H, x^{-1} \in H.$$

Demonstração. Condição Necessária. A condição 1. resulta imediatamente da Definição 2.2.1. Como o inverso em G de um elemento $x \in H$ coincide com o inverso em H obtém-se 2. Condição Suficiente. Suponha-se agora que H é um subconjunto não vazio de G tais que as condições 1. e 2. se verificam.

A condição 1. e o facto de que H é um subconjunto não vazio de G garante que H é um grupóide.

Verifique-se que existe elemento identidade em H. Seja $x \in H$. Observe-se que como $H \neq \varnothing$, existe pelo menos um elemento em H. A condição 2. garante que $x^{-1} \in H$. Como H é grupóide vem $xx^{-1} \in H$ e $x^{-1}x \in H$. Mas, em G, $xx^{-1} = x^{-1}x = e$. Logo $e \in H$. A existência de inverso para cada $x \in H$ é garantida pela condição 2. Resta verificar que

$$\forall a, b, c \in H, (ab)c = a(bc).$$

Ora esta igualdade pode ser encarada em G e em G é válida a associatividade. Assim, essa propriedade é também válida em H. □

Exemplo 2.2.9. *Se $\mathcal{F}$ o conjunto das funções reais de variável real. O subconjunto de $\mathcal{F}$ cujas funções são diferenciáveis é um subgrupo de $\mathcal{F}$. De facto, a soma de duas funções diferenciáveis é uma função diferenciável e, o simétrico duma função diferenciável é uma função diferenciável.*

Exemplo 2.2.10. *Recorde-se da disciplina de Álgebra Linear que a toda a matriz quadrada A podemos associar o seu determinante $\det(A)$ e, uma matriz é invertível se e só se $\det(A) \neq 0$. Se A e B são matrizes quadradas do mesmo tipo então $\det(AB) = \det(A)\det(B)$. Seja G o grupo multiplicativo de todas as matrizes invertíveis de ordem n, com $n \in \mathbb{N}$, com entradas em $\mathbb{C}$ e seja T o subconjunto de G constituído pelas matrizes invertíveis com determinante igual a 1. A igualdade $\det(AB) = \det(A)\det(B)$ mostra que T é fechado para a multiplicação de*

matrizes. Note-se que $\det(I_n) = 1$. *Da igualdade* $\det(A)\det(A^{-1}) = \det(AA^{-1}) = \det(I_n) = 1$, *verifica-se que, se* $\det(A) = 1$, *então* $\det(A^{-1}) = 1$. *Assim, pelo Teorema 2.2.8, T é um subgrupo de G.*

Teorema 2.2.11 (Caracterização de um subgrupo)**.** *Sejam G um grupo e H um subconjunto não vazio de G. Então H é um subgrupo de G se e só se*

$$1'.\forall x, y \in H, xy^{-1} \in H.$$

Demonstração. Pretende-se provar que nas condições do teorema as condições 1. e 2. do teorema anterior equivalem a $1'$. Condição Necessária. Exercício.

Condição Suficiente. Seja $x \in H$ (a existência deste elemento está garantida porque $H \neq \varnothing$). Pela condição $1'$. tem-se

$$xx^{-1} \in H.$$

Encarando o produto anterior em G tem-se

$$e \in H.$$

Seja $x \in H$. Como $e \in H$, pela condição $1'$. tem-se

$$x^{-1} = ex^{-1} \in H,$$

e portanto a condição 2. é verificada.

Sejam agora $x, y \in H$. Pelo anterior, $y^{-1} \in H$. Pela condição $1'$.

$$x(y^{-1})^{-1} \in H,$$

o que é equivalente a

$$xy \in H,$$

donde resulta a condição 1. □

O próximo teorema caracteriza todos os subgrupos de um grupo finito.

Teorema 2.2.12. *[Caracterização dum subgrupo de um grupo finito] Seja G um grupo finito e H um subconjunto não vazio de G. Diz-se que H é um subgrupo de G se e só se*

$$1''.\forall x, y \in H, xy \in H.$$

Demonstração. Condição Necessária. Imediata.

Condição Suficiente.

O facto de que H é um subconjunto não vazio de G e a condição $1''$. garante que H é um grupóide. Como a associatividade é válida em G e $H \subseteq G$ então, por hereditariedade a associatividade é válida em H. Como G é finito e $H \subseteq G$ então H também é finito. Considere-se então $|H| = n$ e

$$H = \{x_1, \ldots, x_n\}.$$

Mostre-se em primeiro lugar que existe elemento neutro em H. Fixe-se $i \in \{1, \ldots, n\}$ e formem-se todos os produtos

$$x_i x_j, \forall j \in \{1, \ldots, n\}. \tag{2.6}$$

Pela condição $1''$. ,

$$x_i x_j \in H, \forall j \in \{1, \ldots, n\}.$$

Seja

$$B = \{x_i x_1, x_i x_2, \ldots, x_i x_n\}.$$

Se B tiver n elementos então tem-se $B = H$.

Mas, isso só é verdadeiro se todos os produtos (2.6) forem distintos, isto é

$$x_i x_t \neq x_i x_l, \text{ para } t \neq l, t, l \in \{1, \ldots, n\}.$$

De facto, se se tivesse

$$x_i x_t = x_i x_l, \text{ para } t \neq l,$$

a lei do corte em G permitiria concluir que

$$x_t = x_l, \text{ para } t \neq l,$$

o que não poderá acontecer pois $|H| = n$. Logo $B = H$, isto é, para i fixo

$$\{x_i x_1, x_i x_2, \ldots, x_i x_n\} = \{x_1, \ldots, x_n\}.$$

Existe assim $x_k \in H$ tal que

$$x_i x_k = x_i. \tag{2.7}$$

Considerando a igualdade 2.7 em G e aplicando a lei do corte tem-se

$$x_k = e_G,$$

onde e_G é o elemento neutro de G. Observe-se que, para $j \neq i$, e da igualdade entre os conjuntos

$$\{x_j x_1, x_j x_2, \ldots, x_j x_n\} = \{x_1, \ldots, x_n\},$$

existe $x_l \in H$ tal que $x_j x_l = x_j$. Do anterior resulta

$$x_l = e_G.$$

Assim, existe $e = e_G \in H$ tal que para todo $x_i \in H$, $e_G\ x_i = x_i e_G = x_i$. A existência de elemento inverso para cada elemento $x_j \in H$, $j \in \{1, \ldots, n\}$, prova-se com argumentos semelhantes. De facto, para qualquer $j \in \{1, \ldots, n\}$, tem-se

$$\{x_j x_1, x_j x_2, \ldots, x_j x_n\} = \{x_1, \ldots, x_n\}.$$

Assim, existe $t \in \{1, \ldots, n\}$ tal que $x_j x_t = e$. Encarando novamente esta igualdade em G tem-se que $(x_j)^{-1} = x_t \in H$. As conclusões seguem de imediato. □

Teorema 2.2.13. *Seja G um grupo finito e H um subconjunto não vazio de G. Então H é um subgrupo de G se e só se*

$$H^2 = H.$$

Demonstração. Condição necessária. Suponha-se que H é subgrupo de G. Prove-se que $H^2 = H$. De facto, $H^2 \subseteq H$ uma vez que o produto de dois elementos dum subgrupo H ainda é um elemento de H. Por outro lado, $H \subseteq H^2$ pois, $h = eh$, para qualquer $h \in H$, onde e, o elemento identidade de G, pertence a H. Condição suficiente. Suponha-se que $H^2 = H$. Sejam $a, b \in H$, $ab \in H^2 \subseteq H$. Logo $ab \in H$. Pelo Teorema 2.2.12, o resultado segue de imediato. □

2.2.2 Intersecção e União de Subgrupos

Teorema 2.2.14. *Seja G um grupo. A intersecção de subgrupos H_i de G para $i \in I$, denotada por $\bigcap_{i \in I} H_i$, ainda é um subgrupo de G.*

Demonstração. De facto, $\bigcap_{i \in I} H_i \subseteq G$ porque $H_i \subseteq G, \forall i \in I$. Por outro lado $e \in H_i, \forall i \in I$, logo $\bigcap_{i \in I} H_i \neq \varnothing$. Sejam

$$a \in \bigcap_{i \in I} H_i \text{ e } b \in \bigcap_{i \in I} H_i.$$

Por definição de intersecção de conjuntos,

$$a \in H_i \text{ e } b \in H_i \forall i \in I\ .$$

Como $H_i \leq G$, vem

$$ab \in H_i$$

para todo $i \in I$, ou seja,

$$ab \in \bigcap_{i \in I} H_i.$$

Provou-se então que

$$\forall a, b \in \bigcap_{i \in I} H_i \ , ab \in \bigcap_{i \in I} H_i.$$

Seja agora $a \in \bigcap_{i \in I} H_i$. Tem-se então,

$$a \in H_i \ , \forall i \in I \ .$$

Como $H_i \leq G$, vem

$$a^{-1} \in H_i \ , \forall i \in I \ ,$$

ou seja,

$$a^{-1} \in \bigcap_{i \in I} H_i.$$

Provou-se então,

$$\forall a \in \bigcap_{i \in I} H_i \ , a^{-1} \in \bigcap_{i \in I} H_i.$$

Pelo Teorema 2.2.8 $\bigcap_{i \in I} H_i$ é um subgrupo de G. □

Sejam G um grupo e $a_i \in G$, para qualquer $i \in I$. Existe pelo menos um subgrupo de G que contém todos os elementos a_i, para todo $i \in I$, nomeadamente o próprio G. O Teorema 2.2.14 garante que se tomarmos a intersecção de todos os subgrupos de G que contém todos os $a_i, \forall i \in I$, obtém-se ainda um subgrupo de G. Este subgrupo é o menor (no sentido da inclusão) subgrupo de G que contém todos os $a_i, \forall i \in I$. Observe-se que a reunião de dois subgrupos de um grupo G poderá não ser um subgrupo de G. De facto, se se considerar os subconjuntos $2\mathbb{Z}, 3\mathbb{Z}$ de $\mathbb{Z}$, estes são subgrupos de $\mathbb{Z}$, no entanto, $2\mathbb{Z} \cup 3\mathbb{Z}$ não é um subgrupo de $\mathbb{Z}$. De facto, $2 \in 2\mathbb{Z}$ e $3 \in 3\mathbb{Z}$ mas $5 \notin 2\mathbb{Z}$ e $5 \notin 3\mathbb{Z}$.

Proposição 2.2.15. *Sejam A, B subgrupos dum grupo G então $A \cup B$ é um subgrupo de G se e só se $A \subseteq B$ ou $B \subseteq A$.*

Demonstração. Suponha-se que $A \cup B$ é um subgrupo de G e que $A \subsetneq B$. Então existe $a \in A$ tal que $a \notin B$. Se $b \in B$ um elemento qualquer. Tem-se $a, b \in A \cup B$ e, por este ser um subgrupo de G, $ab^{-1} \in A \cup B$. Se $ab^{-1} \in B$, $a = (ab^{-1})b \in B$, o que seria contraditório; logo

$ab^{-1} \in A$ e como $a^{-1} \in A$, $b^{-1} = a^{-1}(ab^{-1}) \in A$. Por A ser um subgrupo, $b = (b^{-1})^{-1} \in A$. Portanto $B \subseteq A$. Reciprocamente, se $A \subseteq B$ ou $B \subseteq A$ tem-se $A \cup B = B$ ou $A \cup B = A$, respectivamente. Logo $A \cup B$ é um subgrupo de G. □

Definição 2.2.16. *Chama-se produto dos subconjuntos não vazios de G indicados, e denota-se por $H_1H_2 \cdots H_n$, ao subconjunto de G dado por*

$$H_1H_2 \cdots H_n = \{h_1h_2 \cdots h_n, h_1 \in H_1, h_2 \in H_2, \ldots, h_n \in H_n\}.$$

A multiplicação definida na Definição 2.2.16 é distributiva em relação à adição. Em geral, para dois subconjuntos não vazios de G, H, W, não se tem $HW = WH$. Em particular, se $a \in G$, e $H \subseteq G, H \neq \varnothing$, o produto $\{a\}H$ representa-se por aH. De forma análoga, o produto $H\{a\}$ representa-se por Ha.

Teorema 2.2.17. *Seja G um grupo e H um subconjunto não vazio de G. Então*

$$HG = G \text{ e } GH = G.$$

Demonstração. Prove-se a inclusão nos dois sentidos. Como a operação é interna em G e $H \subseteq G$ tem-se $HG \subseteq G$. Prove-se agora que $G \subseteq HG$. Seja $g \in G$. Então, dado $a \in H$ tem-se $g = (aa^{-1})g = a(a^{-1}g)$. Como G é grupo e $a, g \in G$ tem-se $a^{-1}g \in G$. Como $a \in H$, vem $g = a(a^{-1}g) \in HG$. Analogamente se prova que $GH = G$. □

2.2.3 Subgrupo Gerado

Definição 2.2.18 (Subgrupo de um grupo gerado por um subconjunto)**.** *Seja G um grupo e $a_i \in G$ para $i \in I$. O menor subgrupo de G que contém $K = \{a_i, i \in I\}$ é chamado subgrupo de G* gerado *por K.*

O menor subgrupo de G que contém K é a intersecção de todos os subgrupos H_i de G, para $i \in I$ que contém K. Denota-se por $< K >$, ou seja,

$$< K >= \bigcap_{i \in I} H_i.$$

Provou-se atrás que $< K >$ ainda é um subgrupo de G. é imediato que $K \subseteq < K >$ e, de facto, se H for um subgrupo de G que contém K, então $< K > \subseteq H$ o que garante que $< K >$ é o menor subgrupo de G que contém K.

Definição 2.2.19. *Se $< K >= G$ então diz-se que K gera G e todos os elementos a_i são chamados geradores de G. Se $I = \{1, \ldots, n\}$ ou seja K for um conjunto finito que gera G diz-se que G é finitamente gerado e escreve-se $G =< a_1, \ldots, a_n >$.*

Teorema 2.2.20. *Seja G um grupo e $K \subseteq G$, $K \neq \varnothing$. Seja $W = \{x_1^{\epsilon_1} x_2^{\epsilon_2} \cdots x_n^{\epsilon_n} : x_i \in K, i \in \{1, 2, \ldots, n\}, \epsilon_i \in \{-1, +1\}, n \in \mathbb{N}\}$. O conjunto anterior é um subgrupo de G. Mais, $W =< K >$.*

Demonstração. Exercício. □

Exercício 2.2.21. *Prove que em $\mathbb{Z}$ se tem $\mathbb{Z} =< 2, 3 >=< 1 >$.*

2.2.4 Exercícios

1. Seja G um grupo. Prove que o conjunto

$$\{x \in G \mid xg = gx, \forall g \in G\}$$

chamado centro de G, é um subgrupo abeliano de G.

2. Sejam G um grupo e S um subgrupo de G. Prove que o conjunto

$$\{g \in G \mid gS = Sg\},$$

chamado normalizador de S, é um subgrupo de G.

3. Seja $(M, \cdot)$ o grupo multiplicativo constituído pelas matrizes não singulares de ordem n sobre um corpo K. Verifique se cada um dos conjuntos seguintes é ou não um subgrupo de M:

3.1. $H = \{A \in M \mid AA^T = I\}$; onde A^T representa a transposta da matriz A;

3.2. $W = \{B \in M \mid B$ é anti-simétrica$\}$, observe-se que B é anti-simétrica se e só se $B = -B^T$.

4. Sejam A e B subgrupos de um grupo G. Mostre que $A \cup B$, não é, em geral, um subgrupo de G. Mostre que $A \cup B$ é subgrupo de G se e só se $A \subseteq B$ ou $B \subseteq A$.

5. Prove que o conjunto de matrizes seguinte é um subgrupo de $GL(2, \mathbb{R})$:

$$\left\{ \begin{bmatrix} a & c \\ b & d \end{bmatrix} \in M(2, \mathbb{R}) \mid ad - bc = 1 \right\}.$$

6. Sejam G um grupo abeliano e n um inteiro fixo, $n > 1$. Sejam

$$G_n = \{x \in G \mid x^n = 1\} \text{ e } G^n = \{x^n \mid x \in G\}.$$

Prove que G_n e G^n são subgrupos de G.

7. Sejam G um grupo abeliano e

$$H = \{x \in G \mid x = y^2 \text{ para algum } y \in G\},$$

ou seja, H é o conjunto de todos os elementos de G que possuem raiz quadrada. Prove que H é um subgrupo de G.

8. Sejam G um grupo, H um subgrupo de G e $K = \{x \in G \mid xax^{-1} \in H \text{ se e só se } a \in H,\ \forall a \in G\}$. Prove que K é um subgrupo de G.

9. Sejam G um grupo e H e K subgrupos de G. Prove que se $H \subseteq K$, então H é um subgrupo de K.

10. Sejam G e H dois grupos.

10.1. Mostre que o conjunto

$$G \times H = \{(g, h) \mid g \in G, h \in H\}$$

é um grupo para a operação:

$$(g, h) \cdot (g', h') = (gg', hh'),\ \forall (g, h), (g', h') \in G \times H.$$

10.2. Seja $G \times H$ o conjunto definido anteriormente. Prove que

$$\{(x, e_H) \mid x \in G\}$$

é um subgrupo de $G \times H$, onde e_H denota o elemento neutro de H.

11. Prove que se G é um grupo abeliano e H um subgrupo de G, então

$$S(H) = \{x \in G \mid x \cdot x \in H\} \text{ é um subgrupo de } G.$$

12. Sejam A_1 e A_2 subgrupos de um grupo G. Mostre que $A_1 \cap A_2$ é subgrupo de G. Generalize.

13. Considere as seguintes matrizes

$$A = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}, B = \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}$$

Determine os subgrupos de $GL(2, R)$ gerados por $\{A\}, \{B\}$, e $\{A, B\}$.

2.3 Classes Laterais e Teorema de Lagrange

Definição 2.3.1 (classe lateral à esquerda e à direita)**.** *Seja H um subgrupo dum grupo G. Ao subconjunto de G*

$$aH = \{ah, h \in H\}$$

chama-se classe lateral à esquerda *de H que contém a, e a*

$$Ha = \{ha, h \in H\}$$

chama-se classe lateral à direita *de H que contém a.*

A aH e Ha chamam-se também, respectivamente, classe lateral à esquerda módulo H e, classe lateral à direita módulo H. Ir-se-á provar que, para G um grupo multiplicativo e H um seu subgrupo, o conjunto das classe laterais esquerdas de H contendo $a \in G$ constitui uma partição de G. Far-se-á recurso à definição de partição. Um resultado análogo poderá ser enunciado para as classe laterais à direita.

Proposição 2.3.2. *Sejam H um subgrupo dum grupo G e $a, b \in G$, $aH = bH$ então $b^{-1}aH = H$.*

Demonstração. Sejam $a, b \in G$, tais que $aH = bH$. Prove-se que $b^{-1}aH \subseteq H$ e $H \subseteq b^{-1}aH$. Prove-se em primeiro lugar que $b^{-1}aH \subseteq H$. Seja $y \in b^{-1}aH$. Então $y = b^{-1}ah$, para algum $h \in H$. Mas, como $aH = bH$, $ah = bh_1$, para algum $h_1 \in H$. Assim,

$$y = b^{-1}ah = b^{-1}(ah) = b^{-1}(bh_1) = (b^{-1}b)h_1 = h_1 \in H.$$

Prove-se agora que $H \subseteq b^{-1}aH$. Seja $y \in H$. Então,

$$y = (b^{-1}a)(b^{-1}a)^{-1}y.$$

Mas,

$$(b^{-1}a)^{-1}y = a^{-1}by = a^{-1}(ah_2),$$

para algum $h_2 \in H$, pois por hipótese $by \in bH = aH$. Assim, $(b^{-1}a)^{-1}y = h_2 \in H$. Logo, $y \in b^{-1}aH$. □

Teorema 2.3.3. *Sejam H um subgrupo dum grupo G e $a, b \in G$. Então:*

1. *Os subconjuntos aH e bH coincidem se e só se $b^{-1}a \in H$;*
2. *Se $b^{-1}a \notin H$ então $aH \cap bH = \varnothing$;*
3. $\bigcup_{a \in G} aH = G$.

Demonstração. 1. Ir-se-á provar que $aH = bH$ se e só se $b^{-1}a \in H$. Condição Necessária: Pela proposição 2.3.2 tem-se $b^{-1}aH = H$. Claramente $b^{-1}a \in H$ pois

$$b^{-1}a \in b^{-1}aH \subseteq H.$$

Condição Suficiente: Prove-se agora que se $b^{-1}a \in H$ então $aH = bH$, ou seja $aH \subseteq bH$ e $bH \subseteq aH$. Prove-se em primeiro lugar que $aH \subseteq bH$. Seja $y \in aH$. Tem-se

$$y = ah,$$

para algum $h \in H$. Mas, por definição de elemento neutro,

$$y = eah,$$

para algum $h \in H$. Novamente por definição de elemento inverso e pela associatividade,

$$y = b(b^{-1}a)h,$$

para algum $h \in H$. Mas por hipótese, $b^{-1}a \in H$. Como $H \leq G$ então $(b^{-1}a)h \in H$. Assim,

$$y = bh',$$

para algum $h' \in H$. Prove-se agora que $bH \subseteq aH$. Seja $y \in bH$. Tem-se

$$y = bh,$$

para algum $h \in H$. Pelos argumentos usados anteriormente,

$$y = (aa^{-1})bh,$$

para algum $h \in H$. Pela proposição 2.2.7 e pela associatividade,

$$y = a(b^{-1}a)^{-1}h,$$

para algum $h \in H$. Por hipótese, $b^{-1}a \in H$. Como $H \leq G$ então $(b^{-1}a)^{-1} \in H$ e também $(b^{-1}a)^{-1}h \in H$. Assim,

$$y = bh^{\star},$$

para algum $h^{\star} \in H$. 2. Pretende-se mostrar que se $b^{-1}a \notin H$ então $aH \cap bH = \varnothing$. Por redução ao absurdo, suponha-se que se tem

$$b^{-1}a \notin H \text{ e } aH \cap bH \neq \varnothing.$$

Assim, existe $c \in aH \cap bH$. Por definição de intersecção de conjuntos tem-se,

$$c \in aH \text{ e } c \in bH.$$

Logo, existem $h_1, h_2 \in H$ tais que

$$c = ah_1 = bh_2,$$

ou seja,

$$b^{-1}ah_1 = h_2,$$

ou ainda porque $H \leq G$,

$$b^{-1}ah_1h_1^{-1} = h_2h_1^{-1},$$

ou seja

$$b^{-1}a = h_2h_1^{-1},$$

o que significa que

$$b^{-1}a \in H,$$

o que é absurdo. Provou-se então que se,

$$b^{-1}a \notin H \text{ então } aH \cap bH = \varnothing.$$

3. Pretende-se provar que $\underset{a\in G}{\cup} aH = G$. A inclusão $\underset{a\in G}{\cup} aH \subseteq G$ é óbvia, por definição de aH. Prove-se a inclusão recíproca,

$$G \subseteq \underset{a\in G}{\cup} aH.$$

Ora, para todo $a \in G$,

$$a \in aH,$$

pois

$$a = ae, e \in H.$$

Daqui sai o resultado. □

Teorema 2.3.4. *Seja H um subgrupo dum grupo G. Considere-se a relação $\sim_e$ definida em G por*

$$a \sim_e b \text{ se e só se } b^{-1}a \in H.$$

Considere-se a relação $\sim_d$ definida em G por

$$a \sim_d b \text{ se e só se } ab^{-1} \in H.$$

As relações anteriores são relações de equivalência em G. Mais, para a relação de equivalência $\sim_e$ (análogo para $\sim_d$)

$$\overline{a} = aH, \forall a \in G.$$

Demonstração. Provar-se-á apenas o resultado para a relação $\sim_e$.

Relação reflexiva: Seja $a \in G$. Então $a^{-1}a = e$ e $e \in H$ pois $H \leq G$. Assim, $a \sim_e a$.

Relação simétrica: Suponha-se que $a \sim_e b$. Então $b^{-1}a \in H$. Como $H \leq G, (b^{-1}a)^{-1} \in H$ e $(b^{-1}a)^{-1} = a^{-1}b$. Assim, $a^{-1}b \in H$ e $b \sim_e a$.

Relação transitiva: Sejam $a \sim_e b$ e $b \sim_e c$. Então $b^{-1}a \in H$ e $c^{-1}b \in H$. Como $H \leq G, (c^{-1}b)(b^{-1}a) = c^{-1}a \in H$ e $a \sim_e c$. Prove-se agora a segunda parte do teorema. Seja $a \in G$,

$$\begin{aligned} \overline{a} &= \{x \in G : x \sim_e a\} \text{ , por definição de classe de equivalência,} \\ &= \{x \in G : a^{-1}x \in H\}, \text{ por definição de } \sim_e. \end{aligned}$$

Mas, $a^{-1}x \in H$ se e só se $a^{-1}x = h$, para algum $h \in H$, ou de forma equivalente se e só se $x = ah$, para algum $h \in H$.

Assim, a classe de equivalência que contém $a \in G$ é dada pelo conjunto

$$\{ah : h \in H\} = aH.$$

□

Observe-se que a relação de equivalência $\sim_e$ determina em G uma partição e que os elementos dessa partição são precisamente as classes laterais à esquerda de H. Mais, tendo em atenção o anterior escreve-se $G = a_1H \oplus a_2H \oplus \cdots$ onde $a_iH, i \in I$, representam as classes laterais à esquerda relativamente a H. Analogamente pode usar-se a mesma notação considerando classes laterais à direita.

Exemplo 2.3.5. *Escreva as classes laterais à esquerda e direita do subgrupo $3\mathbb{Z}$ em relação a $\mathbb{Z}$. Note-se que neste exemplo a notação considerada é a aditiva. Assim, a classe lateral à esquerda de $3\mathbb{Z}$ que contém um inteiro m é dada por*

$$m + 3\mathbb{Z}.$$

Tomando $m = 0$, pode observar-se que

$$3\mathbb{Z} = \{\ldots, -9, -6, -3, 0, 3, 6, 9, \ldots\}$$

é uma classe lateral à esquerda de $3\mathbb{Z}$ *que contém o elemento* 0*. Para obter outra classe lateral à esquerda de* $3\mathbb{Z}$*, selecciona-se outro elemento de* $\mathbb{Z}$ *(que não esteja em* $3\mathbb{Z}$*), por exemplo* 1 *e considere-se a classe lateral à esquerda de* $3\mathbb{Z}$ *que contém* 1*,*

$$1 + 3\mathbb{Z} = \{\dots, -8, -5, -2, 1, 4, 7, 10, \dots\}.$$

Observe-se que a reunião destes dois conjuntos $3\mathbb{Z}$ *e* $1 + 3\mathbb{Z}$ *ainda não é o conjunto* $\mathbb{Z}$*, por exemplo o inteiro* 2 *não está em qualquer um destes conjuntos. A classe lateral à esquerda de* $3\mathbb{Z}$ *que contém* 2 *é dada por*

$$2 + 3\mathbb{Z} = \{\dots, -7, -4, -1, 2, 5, 8, 11, \dots\}.$$

Claramente a reunião destes três conjuntos é $\mathbb{Z}$ *e assim pode dizer-se que* $\mathbb{Z}$ *está particionado nestas três classes à esquerda de* $3\mathbb{Z}$*. Como* $\mathbb{Z}$ *é abeliano, as classes laterais à esquerda* $m+3\mathbb{Z}$ *e à direita* $3\mathbb{Z}+m$ *coincidem e portanto a partição de em classes laterais à direita é a mesma.*

Para um subgrupo H dum grupo abeliano G, a partição de G em classes laterais à esquerda de H e a partição de G em classes laterais à direita referida anteriormente é precisamente a mesma.

Tendo em atenção a definição de relação de congruência módulo p, onde $p \in \mathbb{N}$, pode observar-se que a relação de equivalência $\sim_d$ para o subgrupo $p\mathbb{Z}$ de $\mathbb{Z}$ é precisamente a relação de congruência módulo p. De facto, sejam $h, k \in \mathbb{Z}$, tais que $h \equiv k(mod\ p)$. Tem-se $h - k$ é divisível por p. Mas isso é equivalente a que $h + (-k) \in p\mathbb{Z}$, ou seja $h \sim_d k$. Assim, a partição de $\mathbb{Z}$ em subconjuntos de $p\mathbb{Z}$ é a partição de $\mathbb{Z}$ em classes residuais módulo p. Por vezes, na literatura chamam-se aos subconjuntos destas partição subconjuntos módulo p.

Exemplo 2.3.6. *O grupo* $\mathbb{Z}_6$ *é abeliano. Encontre a partição de* $\mathbb{Z}_6$ *em subconjuntos do subgrupo* $H = \{\overline{0}, \overline{3}\}$*. Claramente um subconjunto é o próprio* H*. O subconjunto que contém o* $\overline{1}$ *é* $\overline{1} + \{\overline{0}, \overline{3}\} = \{\overline{1}, \overline{4}\}$*. O subconjunto que contém o* $\overline{2}$ *é* $\overline{2} + \{\overline{0}, \overline{3}\} = \{\overline{2}, \overline{5}\}$*. Uma vez que a reunião dos conjuntos* $\{\overline{0}, \overline{3}\}, \{\overline{1}, \overline{4}\}$ *e* $\{\overline{2}, \overline{5}\}$ *é todo o conjunto* $\mathbb{Z}_6$ *então estes são todos os subconjuntos pretendidos.*

Proposição 2.3.7. *Sejam* H *um subgrupo dum grupo* G *e* $g \in G$*. Então a aplicação*

$$\begin{array}{rcl} \phi : H & \to & gH \\ h & \to & gh \end{array},$$

é bijectiva.

Demonstração. Sejam $h_1, h_2 \in H$ tais que,

$$\phi(h_1) = \phi(h_2).$$

Então, por definição de ϕ,

$$gh_1 = gh_2.$$

Como em G é válida a lei do corte, tem-se

$$h_1 = h_2.$$

A sobrejectividade ficará como exercício □

é óbvio que se pode definir uma aplicação injectiva de H em Hg, de forma análoga.

O resultado anterior permite concluir que as classes laterais à direita ou à esquerda de H têm o mesmo número de elementos que H.

Teorema 2.3.8 (Teorema de Lagrange)**.** *Seja H um subgrupo dum grupo finito. Então a ordem de H é um divisor da ordem de G.*

Demonstração. Sejam n e m as ordens de G e H respectivamente. Pela Proposição 2.3.7 toda a classe lateral de H tem o mesmo número de elementos que H. Seja r o número de subconjuntos na partição de G em classes laterais à esquerda de H. Então $n = rm$ e portanto m é um divisor de n. □

Corolário 2.3.9. *Todo o grupo G de ordem prima é gerado apenas por um elemento.*

Demonstração. Seja p a ordem prima de G. Seja $a \in G\backslash\{e\}$ e considere-se o subgrupo gerado por a, $< a >$. Este subgrupo tem pelo menos dois elementos, e e a. Pelo Teorema 2.3.8 , a ordem $m \geq 2$ de $< a >$ deverá dividir p. Mas p é primo então $m = p$ e $< a >= G$. □

Definição 2.3.10. *(índice de H em G) Seja H um subgrupo dum grupo G. O número de classes laterais à esquerda de H em G é chamado índice de H em G e denotado por $[G : H]$.*

O índice de H em G poderá ser finito ou infinito. Claramente se G for finito tem-se o seguinte corolário.

Corolário 2.3.11. *O índice de um subgrupo H dum grupo finito G, $[G : H]$, é dado por*

$$[G : H] = \frac{|G|}{|H|}$$

Demonstração. Exercício. □

2.3.1 Exercícios

1. Sejam $(G, .)$ um grupo abeliano e H e K subgrupos de G. Prove que $< H \cup K >= HK$.

2. Prove o seguinte teorema:

Teorema: Sejam H um subgrupo de G e a, b elementos quaisquer de G.

3. Mostre que

3.1. Os complexos aH e bH coincidem se e só se $b^{-1}a \in H$;

3.2. Se $b^{-1}a \notin H$ então $aH \cap bH = \phi$;

3.3. $\bigcup_{a \in G} aH = G$.

4. Ilustre o resultado anterior com $G = \mathbb{Z}$ e $H = 3\mathbb{Z}$.

5. Determine todas as classes laterais de $4\mathbb{Z}$ como subgrupo de

5.1. $\mathbb{Z}$

5.2. $2\mathbb{Z}$.

6. Para cada $r \in \mathbb{R}$, seja $A_r = \{(x, y) \in \mathbb{R} \times \mathbb{R} : y = 3x + r\}$.

6.1. Mostre que A_0 é um subgrupo (aditivo) de $\mathbb{R} \times \mathbb{R}$.

6.2. Mostre que $\{A_r : r \in \mathbb{R}\}$ é uma família de classes laterais de $\mathbb{R} \times \mathbb{R}$ relativamente a A_0.

6.3. Prove que $\{A_r\}_{r \in \mathbb{R}}$ é uma partição de $\mathbb{R} \times \mathbb{R}$ e descreva-a geometricamente. Indique também a correspondente relação de equivalência.

7. Sejam G um grupo, H um subgrupo de G e a, b elementos quaisquer de G. Prove que

7.1. Se $aH = Ha$ e $bH = Hb$ então $(ab)H = H(ab)$;

7.2. Se $aH = Ha$ então $a^{-1}H = Ha^{-1}$.

7.3. $(ab)H = H(ac)$ então $bH = cH$.

8. Seja H o subgrupo trivial do grupo G. Determine todas as classes laterais à direita de H em G.

9. Seja $G = \{a, b, c, d, e, f\}$ o grupo definido pela seguinte tabela

.	a	b	c	d	e	f
a	a	b	c	d	e	f
b	b	c	d	e	f	a
c	c	d	e	f	a	b
d	d	e	f	a	b	c
e	e	f	a	b	c	d
f	f	a	b	c	d	e

Averigue se cada um dos seguintes conjuntos é um subgrupo de G e, caso afirmativo, determine a decomposição em classes laterais.

9.1. $H = \{a, d, e\}$;

9.2. $H = \{b, c, d, e\}$;

9.3. $H = \{a, d\}$;

9.4. $H = \{a, b, c, d, f\}$;

9.5. $H = \{a, c, e\}$.

10. Sejam G, H e K grupos finitos tais que $H \subseteq G \subseteq K$. Prove que

$$[K : H] = [K : G].[G : H].$$

11. Sejam p um número primo e G um grupo de ordem p. Determine todos os subgrupos de G.

2.4 Subgrupos Normais. Definição e Caracterização

Definição 2.4.1. *Sejam G um grupo e $H \leq G$. Se, para todo $g \in G$ se tem*

$$gH = Hg,$$

diz-se que o subgrupo H de G é um subgrupo normal.

Se H for um subgrupo normal de G usa-se a notação $H \lhd G$.

Teorema 2.4.2. *Sejam G um grupo, $H \leq G$ e $g \in G$, o subconjunto,*

$$gHg^{-1} = \{ghg^{-1}, h \in H\},$$

é um subgrupo de G.

Demonstração. Seja $g \in G$. O conjunto $gHg^{-1} \neq \varnothing$ pois o elemento $geg^{-1} = e \in H$. Sejam $a, b \in gHg^{-1}$. Então, $a = gh_1g^{-1}$, para algum $h_1 \in H$ e $b = gh_2g^{-1}$, para algum $h_2 \in H$. Mas, porque G é grupo, $b^{-1} = gh_2^{-1}g^{-1}$. Assim, $ab^{-1} = (gh_1g^{-1})(gh_2^{-1}g^{-1}) = (gh_1)(g^{-1}g)(h_2^{-1}g^{-1})$. Por definição de elemento inverso e de elemento neutro em G tem-se $ab^{-1} = (gh_1)(h_2^{-1}g^{-1})$. Logo, pela associatividade tem-se $ab^{-1} = g(h_1h_2^{-1})g^{-1}$. Como $H \leq G, h_1h_2^{-1} \in H$. Assim, $ab^{-1} = gh_3g^{-1}$ para algum $h_3 \in H$. Provou-se então que $\forall a, b \in gHg^{-1}, ab^{-1} \in gHg^{-1}$. □

Apresenta-se de seguida algumas caracterizações para que um subgrupo H de um grupo G seja um subgrupo normal.

Teorema 2.4.3. *[Caracterizações de um subgrupo normal] Sejam G um grupo e $H \leq G$. O subgrupo H é um subgrupo normal de G se e só se*

1. *$ghg^{-1} \in H$ para todo $g \in G$ e $h \in H$;*
2. *$gHg^{-1} = H$, para todo $g \in G$;*
3. *$gH = Hg$, para todo $g \in G$.*

Demonstração. Prove-se que 1. $\Rightarrow$ 2. Suponha-se que H é um subgrupo de G tal que $ghg^{-1} \in H$ para todo $g \in G$ e $h \in H$. Então, $gHg^{-1} = \{ghg^{-1} : h \in H\} \subseteq H$, para todo $g \in G$. Pretende-se provar que $gHg^{-1} = H$. Dever-se-á provar que $H \subseteq gHg^{-1}$, para todo $g \in G$. Seja $h \in H$. Substituindo na relação $ghg^{-1} \in H$, o elemento g por g^{-1} obtém-se

$g^{-1}h(g^{-1})^{-1} = g^{-1}hg = h_1, h_1 \in H$. Consequentemente, $h = gh_1g^{-1} \in gHg^{-1}$ e obtém-se $H \subseteq gHg^{-1}$ completando a prova de 2.

Prove-se agora que 3. $\Rightarrow$ 1. Suponha-se que $gH = Hg$, para todo $g \in G$. Então $gh = h_1g$, para algum $h_1 \in H$ e assim, $ghg^{-1} \in H$ para todo $g \in G$ e todo $h \in H$.

Prove-se que 2. $\Rightarrow$ 3. Suponha-se que $gHg^{-1} = H$, para todo $g \in G$ então $ghg^{-1} = h_1$, para algum $h_1 \in H$, e portanto $gh = h_1g \in Hg$. Logo $gH \subseteq Hg$. Analogamente, se tem $g^{-1}hg = h_2$, para algum $h_2 \in H$ e portanto $hg = gh_2$ e assim, $Hg \subseteq gH$. □

Proposição 2.4.4. *Todo o subgrupo de um grupo abeliano é normal.*

Demonstração. Seja H um subgrupo dum grupo abeliano G. Então $ghg^{-1} = (gh)g^{-1} = (hg)g^{-1} = h(gg^{-1}) = he = h$ para todo $h \in H$ e $g \in G$. Pelo Teorema 2.4.3 $H \lhd G$. □

2.4.1 Exercícios

1. Seja G um grupo. Se H e K são subgrupos normais de G, prove que $H \cap K$ é um subgrupo normal de G.

2. Seja G um grupo. Prove que o conjunto

$$C = \{a \in G : ax = xa, \text{ para todo } x \in G\}$$

é um subgrupo normal de G. A C é usual chamar-se centro de G.

3. Sejam G um grupo, $H \leq G$ e $K \lhd G$. Mostre que $HK \leq G$ e $HK = KH$.

4. Sejam G um grupo, $H \lhd G$ e $K \lhd G$, tais que $H \cap K = \{e_G\}$. Prove que:

$$\forall x \in H, \forall y \in K, xy = yx.$$

5. Sejam G um grupo, A um subgrupo de G e H um subgrupo normal de G. Mostre que $A \cap H$ é um subgrupo normal de A.

6. Sejam G_1, G_1' subgrupos de G tais que G_1' é um subgrupo normal de G_1.

6.1. Prove que para qualquer subgrupo G_2 de G, $G_1' \cap G_2$ é um subgrupo normal de $G_1 \cap G_2$.

6.2. Para todo o subgrupo normal H de G se tem $G_1'H$ é um subgrupo normal de G_1H.

7. Seja G um grupo e H um seu subgrupo. Mostre que se $[G : H] = 2$ então H é normal.

2.5 Homomorfismo de Grupos

Definição 2.5.1 (Homomorfismos de grupos)**.** *Sejam G e G' dois grupos. Suponha-se que se está a usar notação multiplicativa. Diz-se que $\varphi : G \to G'$ é um* homomorfismo *(ou* morfismo*) de grupos se e só se*

$$\forall a, b \in G, \varphi(ab) = \varphi(a)\varphi(b).$$

Exemplo 2.5.2. *Seja q um inteiro. A função definida de $\mathbb{Z}$ em $\mathbb{Z}$ tal que a todo o inteiro n faz corresponder qn é um homomorfismo de grupos.*

Exemplo 2.5.3. *Seja x um elemento dum grupo. A função que faz corresponder a cada inteiro n o elemento de G, x^n , é um homomorfismo do grupo $\mathbb{Z}$ no grupo G pois $x^{n+m} = x^n x^m$, para quaisquer inteiros $m, n \in \mathbb{Z}$.*

Teorema 2.5.4. *Seja $\phi : G \to G'$ um homomorfismo de grupos.*

1. *Se e é a identidade de G, então $\phi(e)$ é a identidade de G';*
2. *Se $a \in G$, então $\phi(a^{-1}) = \phi(a)^{-1}$;*
3. *Se $H \leq G$, então $\phi(H) \leq G'$;*
4. *Se $K' \leq G'$, então $\phi^{-1}(K') \leq G$.*

Demonstração. A demonstração de 1. e 2. já foi feita na primeira secção. Prove-se 3. Sejam $H \leq G$, e $\phi(H) = \{\phi(h), h \in H\}$. Observe-se em primeiro lugar que $\phi(H) \neq \varnothing$. De facto, $e' = \phi(e) \in \phi(H)$. Sejam $a, b \in \phi(H)$. Então,

$$a = \phi(h_1),$$

para algum $h_1 \in H$,

$$b = \phi(h_2),$$

para algum $h_2 \in H$. Então $ab^{-1} = \phi(h_1)\phi(h_2)^{-1} = \phi(h_1)\phi(h_2^{-1}) = \phi(h_1 h_2^{-1})$, por 2. e porque ϕ é um homomorfismo. Como $H \leq G, h_1 h_2^{-1} \in H$ e assim, $ab^{-1} \in \phi(H)$. Provou-se então

$$\forall a, b \in \phi(H), ab^{-1} \in \phi(H).$$

Prove-se agora 4. Consideremos então

$$\phi^{-1}(K') = \{a \in G : \phi(a) \in K'\}.$$

Temos

$$e \in G : \phi(e) = e' \in K',$$

pois $K' \leq G'$. Assim $\phi^{-1}(K') \neq \varnothing$. Sejam agora $a, b \in \phi^{-1}(K')$, então

$$\phi(a), \phi(b) \in K'.$$

Então,

$$\phi(ab^{-1}) = \phi(a)\phi(b^{-1}) = \phi(a)\phi(b)^{-1} \in K'.$$

Assim, $ab^{-1} \in \phi^{-1}(K')$. □

Proposição 2.5.5. *Seja $\phi : G \to G'$ um homomorfismo de grupos. Com a notação introduzida na secção 1 prove que para $x, y \in G, \phi(x^y) = \phi(x)^{\phi(y)}$ e $\phi([x, y]) = [\phi(x), \phi(y)]$.*

Demonstração. Exercício. □

Definição 2.5.6 (Núcleo dum homomorfismo de grupos)**.** *Seja $\phi : G \to G'$ um homomorfismo de grupos. O subconjunto de G,*

$$\phi^{-1}(\{e'\}) = \{x \in G : \phi(x) = e'\}$$

é o núcleo *de ϕ, denotado por $Nuc(\phi)$ ou $Ker(\phi)$.*

Observe-se que $\mathrm{Nuc}(\phi) \neq \varnothing$ porque $e \in \mathrm{Nuc}(\phi)$.

Exemplo 2.5.7. *Considere-se o grupo $(\{1, -1\}, .)$ e a aplicação $\theta : \mathbb{Z} \to \{1, -1\}$ o homomorfismo entre os dois grupos tal que a cada $n \in \mathbb{Z}$ faz corresponder $(-1)^n$. O núcleo do homomorfismo θ é o subconjunto de $\mathbb{Z}$ formado por todos os inteiros pares.*

Exemplo 2.5.8. *Considere-se o grupo $(\mathbb{Q}\backslash\{0\}, .)$ e a aplicação $\Psi : \mathbb{Q}\backslash\{0\} \to \mathbb{Q}\backslash\{0\}$, o homomorfismo entre os dois grupos tal que $\Psi(x) = x^2$. Então $Nuc(\ \Psi) = \{x \in \mathbb{Q}\backslash\{0\} : x^2 = 1\} = \{1, -1\}$.*

Teorema 2.5.9. *Sejam $\phi : G \to G'$ um homomorfismo de grupos e $H = Nuc(\phi)$. Seja $a \in G$. Então o subconjunto*

$$\phi^{-1}(\{\phi(a)\}) = \{x \in G : \phi(x) = \phi(a)\}$$

coincide com a classe lateral à esquerda de H, aH,e também coincide com a classe lateral à direita de H, Ha. Consequentemente, as duas partições de G em classes laterais à esquerda de H e em classes laterais à direita de H respectivamente, coincidem.

Demonstração. Pretende-se provar que

$$\phi^{-1}(\{\phi(a)\}) = \{x \in G : \phi(x) = \phi(a)\} = aH.$$

Prove-se a inclusão nos dois sentidos dos conjuntos anteriores.

Suponha-se que $\phi(x) = \phi(a)$. Então

$$\phi(a)^{-1}\phi(x) = e',$$

onde e' é a identidade de G'. Pelo Teorema 2.5.4, sabe-se que $\phi(a)^{-1} = \phi(a^{-1})$, e assim tem-se

$$\phi(a^{-1})\phi(x) = e'.$$

Como ϕ é um homomorfismo,

$$\phi(a^{-1})\phi(x) = \phi(a^{-1}x)$$

e portanto

$$\phi(a^{-1}x) = e'.$$

Mas o anterior mostra que que $a^{-1}x \in H = \text{Nuc}(\phi)$, e assim, $a^{-1}x = h$, para algum $h \in H$ e $x = ah \in aH$. Isto mostra que

$$\{x \in G : \phi(x) = \phi(a)\} \subseteq aH.$$

Para mostrar que

$$aH \subseteq \{x \in G : \phi(x) = \phi(a)\},$$

seja $y \in aH$, ou seja $y = ah$, para algum $h \in H$. Então $\phi(y) = \phi(ah) = \phi(a)\phi(h) = \phi(a)e' = \phi(a)$, e portanto $y \in \{x \in G : \phi(x) = \phi(a)\}$. De forma análoga se prova que

$$\{x \in G : \phi(x) = \phi(a)\} = Ha.$$

□

Exemplo 2.5.10. *Seja $\mathcal{F}$ o conjunto de todas as funções reais de variável real e seja $\mathcal{D}$ o grupo aditivo das funções reais de variável real que são diferenciáveis. A função $\phi : \mathcal{D} \to \mathcal{F}$, tal que $\phi(f) = f'$, onde f'representa a derivada de f, para todo $f \in \mathcal{D}$. é fácil provar que ϕ é um homomorfismo de grupos já que para quaisquer $f, g \in \mathcal{D}, \phi(f+g) = (f+g)' = f+g' = \phi(f) + \phi(g)$. Ora, Nuc$(\phi) = \{f \in \mathcal{D} : \phi(f) = 0\} = \{f \in \mathcal{D} : f' = 0\}$, onde 0 representa a função constante nula. Assim, Nuc(ϕ) é formado por todas as funções constantes que constituem um subgrupo $\mathcal{C}$ de $\mathcal{F}$. Encontre-se agora todas as funções que estão em D cuja*

imagem por ϕ é x^2, ou seja, todas as funções diferenciáveis cuja derivada é x^2. Sabe-se que $\frac{x^3}{3}$ é uma dessas funções. Pelo Teorema 2.5.9, o conjunto formado por todas essas funções é o conjunto $\frac{x^3}{3}+\mathcal{C}$, o que parece familiar.

Corolário 2.5.11. *Um homomorfismo de grupos $: G \to G'$ é uma aplicação injectiva se e só se $Nuc(\phi) = \{e\}$.*

Demonstração. Prove-se em primeiro lugar que para quaisquer $x, a \in G$, tais que $\phi(x) = \phi(a)$, então $x = a$. Observe-se que para todo $a \in G$, o conjunto

$$\{x \in G : \phi(x) = \phi(a)\} = a\{e\} = \{a\},$$

pelo teorema anterior. Claramente obtém-se o resultado.

Suponha-se agora que ϕ é injectiva, pelos resultados provados na primeira secção, sabe-se que $\phi(e) = e'$, onde e' é a identidade de G'. Como ϕ é injectiva, e é o único elemento que é transformado em e' por ϕ. Assim, $\mathrm{Nuc}(\phi) = \{e\}$. □

Observe-se que o Teorema 2.5.9 permite também concluir que o núcleo de um homomorfismo $\phi : G \to G'$ é um subgrupo normal.

Ir-se-á provar este resultado tendo em atenção as caracterizações de subgrupo e subgrupo normal.

Teorema 2.5.12. *Seja $\phi : G \to G'$ um homomorfismo de grupos. O subconjunto de G, $Nuc(\phi)$, é um subgrupo normal de G.*

Demonstração. Note-se em primeiro lugar que $\mathrm{Nuc}(\phi) \neq \varnothing$ pois $e \in \mathrm{Nuc}(\phi)$. Sejam agora $a, b \in \mathrm{Nuc}(\phi)$. Tem-se

$$\phi(a) = \phi(b) = e'.$$

Assim, $\phi(ab) = \phi(a)\phi(b) = e'e' = e'$, pois ϕ é um homomorfismo de grupos. Assim, $ab \in \mathrm{Nuc}(\phi)$. Por outro lado $\phi(a^{-1}) = \phi(a)^{-1} = e'^{-1} = e'$pelo que $a^{-1} \in \mathrm{Nuc}(\phi)$. Provou-se então que

$$\forall a, b \in \mathrm{Nuc}(\phi), ab \in \mathrm{Nuc}(\phi)$$

e,

$$\forall a \in \mathrm{Nuc}(\phi), a^{-1} \in \mathrm{Nuc}(\phi).$$

Por outro lado, $\mathrm{Nuc}(\phi)$ é um subgrupo normal de G, pois basta verificar que se $g \in G$ e $a \in \mathrm{Nuc}(\phi)$,

$$\phi(gag^{-1}) = \phi(g)\phi(a)\phi(g^{-1}) = \phi(g)\phi(a)\phi(g)^{-1} = \phi(g)\phi(g)^{-1} = e'.$$

□

Exercício 2.5.13. *Seja $\phi : G \to G'$ um homomorfismo de grupos. Prove que :*

a) Se $N' \lhd G'$, então $\phi^{-1}(H') \lhd G$. b) Se ϕ é um epimorfismo e $N \lhd G$, então $\phi(N) \lhd G'$.

2.5.1 Exercícios

1. Mostre que a composição

a) entre dois homomorfismos é um homomorfismo;

b) entre dois monomorfismos é um monomorfismo;

c) entre dois epimorfismos é um epimorfismo.

2. Mostre que se ϕ é um homomorfismo entre os grupos $(G, .)$ e $(G\prime, \star)$, sendo u, u', as identidades de G e G' respectivamente, se tem:

2.1. $\phi(u) = u'$;

2.2. $\phi(a^{-1}) = (\phi(a))^{-1}, \forall a \in G$.

2.3. Se A é um subgrupo de G então $\phi(A) = \{\phi(a), a \in A\}$ é um subgrupo de $G\prime$.

3. Se A' é um subgrupo de G', então $\phi^{-1}(A')$ é um subgrupo de G, onde

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

3.1. Se ϕ é um epimorfismo e $H \lhd G$, então $\phi(H) \lhd G'$.

3.2. Se $H' \lhd G'$ então $\phi^{-1}(H') \lhd G$.

3.3. Considere o grupo multiplicativo dos reais não nulos e o seu subgrupo dos reais positivos.

4. Prove que a aplicação

$$\begin{array}{rccc} f: & \mathbb{R}\backslash\{0\} & \to & \mathbb{R}^+ \\ & x & \longmapsto & x^2 \end{array}$$

é um homomorfismo entre os grupos considerados. Determine $\ker f$ e $\Im f$.

5. Seja f o homomorfismo de $(\mathbb{Z}, +)$ em $(\mathbb{Q}\backslash\{0\})$, tal que

$$f(x) = \begin{cases} 1 \text{ se } x \text{ é par} \\ -1 \text{ se } x \text{ é ímpar} \end{cases}$$

Determine $\ker f$.

2.6 Grupos Cociente

Sejam G um grupo e $H \leq G$. Quando H é um subgrupo normal de G, as relações de equivalência $\sim_d$ e $\sim_e$ coincidem, pelo que é usual representar abreviadamente o conjunto cociente da seguinte forma:

$$G/\sim_d = G/\sim_e = G/H$$

Define-se em G/H uma operação tal que, para quaisquer $a, b \in G$,

$$(aH)(bH) = abH.$$

Proposição 2.6.1. *A operação definida anteriormente é consistente com a estrutura de classe lateral ou seja, o resultado (produto) não depende dos representantes das classes escolhidos.*

Demonstração. Sejam então $aH = a'H$, $bH = b'H$. Tem-se então $a' \in aH$, e $b' \in bH$. Ora, o anterior é equivalente a

$$a' = ah_1, b' = bh_2 \text{ com } h_1, h_2 \in H.$$

Fazendo

$$a'b' = ah_1bh_2,$$

ora

$$h_1b \in Hb = bH,$$

pelo que,

$$h_1b = bh_1',$$

com $h_1' \in H$. Donde

$$a'b' = ah_1bh_2 = abh_1'h_2 \in (ab)H.$$

Assim,

$$(a'b')H = (ab)H.$$

□

Teorema 2.6.2. *(Grupo cociente) Sejam G um grupo e H um subgrupo normal de G. Com a operação definida acima, G/H é um grupo (grupo cociente de G por H) e a aplicação*

$$\begin{array}{ccc} \pi : G & \to & G/H \\ a & \to & aH \end{array}$$

é um epimorfismo (epimorfismo canónico associado a H).

Demonstração. De facto, para quaisquer $aH, bH \in G/H$, $(aH)(bH) = abH \in G/H$ o que mostra que a operação é interna.

Sejam agora $aH, bH, cH \in G/H$. Então $((aH)(bH))(cH) = ((ab)H)(cH) = ((ab)c)H = (a(bc))H = (aH)((bc)H) = (aH)((bH)(cH))$, o que mostra que a operação é associativa.

$H(aH) = (eH)(aH) = (ea)H = aH$

$(aH)H = (aH)(eH) = (ae)H = aH$. Assim, eH é o elemento neutro de G/H. Mais,

$(aH)(a^{-1}H) = (aa^{-1})H = H$

$(a^{-1}H)\ (aH) = (a^{-1}a)H = H$, para qualquer elemento $a \in G$. Assim G/H é um grupo. A afirmação seguinte é de verificação trivial. □

2.6.1 Exercícios

1. Seja G um grupo. Suponha que existe $n \in \mathbb{Z}$ tal que

$$\forall a, b \in G, (ab)^n = a^n b^n.$$

Considere os conjuntos,

$$G_n = \{x \in G : x^n = e\} \text{ e } G^n = \{x^n : x \in G\},$$

onde e denota o elemento neutro de G.

1.1. Mostre que os conjuntos indicados são subgrupos normais de G.

1.2. Mostre que se G é de ordem finita então a ordem de G^n coincide com $[G : G_n]$.

Observação: Recorde que $[G : G_n]$ denota a ordem do grupo G/G_n e que se dois grupos são isomorfos têm a mesma ordem.

2. Seja G o conjunto das transformações

$$\begin{array}{rccc} \psi_{a,b}: & \mathbb{R} & \to & \mathbb{R} \\ & x & \longmapsto & ax+b \end{array}$$

com $a, b \in \mathbb{R}$ e $a \neq 0$.

2.1. Mostre que G constitui um grupo para a composição usual de aplicações.

2.2. Seja $S = \{f \in G : f(x) = x + b, b \in \mathbb{R}\}$. Mostre que S é um subgrupo normal de G.

2.3. Determine as classes laterais de S em G.

2.4. Mostre que G/S é isomorfo a $\mathbb{R}\backslash\{0\}$.

3. Seja $\mathcal{F}(\mathbb{R})$ o grupo das funções reais de variável real para a adição usual de funções.

3.1. Sendo f a função definida por $f(x) = x + 1$, determine o subgrupo $< f >$ gerado por f.

3.2. Mostre que $H = \{h_n \in \mathcal{F}(\mathbb{R}) : h_n(x) = 3nx + 3n, n \in \mathbb{Z}\}$ é um subgrupo de $< f >$.

3.3. Determine a decomposição de $< f >$ em classes laterais esquerdas relativamente a H.

3.4. Verifique se H é subgrupo normal de $< f >$.

2.7 Teorema Fundamental do Homomorfismo de Grupos

Teorema 2.7.1. *Sejam G um grupo, H um subgrupo normal de G e $\pi : G \to G/H$ o epimorfismo canónico. Seja $\phi : G \to G'$ um homomorfismo de grupos tal que $H \subseteq Nuc(\phi)$. Então existe um único homomorfismo $\phi^\star : G/H \to G'$, tal que $\phi^\star(gH) = \phi(g)$ e $\phi^\star \circ \pi = \phi$. Mais, $\phi^\star$ é um epimorfismo se, e só se, ϕ é um epimorfismo e, $\phi^\star$ é um monomorfismo se, e só se, $H = Nuc(\phi)$.*

$$\begin{array}{ccc} G & \stackrel{\phi}{\to} & G' \\ \pi \downarrow & \nearrow_{\phi^\star} & \\ G/H & & \end{array}$$

Demonstração. A existência da aplicação $\phi^\star$ está garantida pelos resultados da secção 1 e de facto é única. Para tal basta verificar que, em face das condições que lhe são exigidas, se ter á, obrigatoriamente, para cada $x \in G$,

$$\phi^\star(xH) = \phi^\star(\pi(x)) = (\phi^\star \circ \pi) = \phi(x).$$

Prove-se agora $\phi^\star$ está bem definida. Sejam $xH, yH \in G/H$ tais que

$$xH = yH$$

Donde resulta

$$y^{-1}x \in H \subseteq \mathrm{Nuc}(\phi)$$

ou seja

$$y^{-1}x \in \mathrm{Nuc}(\phi)$$

o que é equivalente a

$$\phi(y^{-1}x) = e',$$

onde e' representa o elemento neutro de G'. O anterior é ainda equivalente a

$$\phi(y^{-1})\phi(x) = e',$$

ou seja

$$\phi(y)^{-1}\phi(x) = e'.$$

Mas a igualdade anterior é equivalente a

$$\phi(y) = \phi(x).$$

Assim, provou-se que para todos $xH, yH \in G/H$, se

$$xH = yH \text{ então } \phi^\star(y) = \phi^\star(x),$$

ou seja $\phi^\star$ está bem definida.

Prove-se agora que $\phi^\star$ é um homomorfismo de grupos.

Sejam $xH, yH \in G/H$,

$$\phi^\star(xHyH) = \phi^\star(xyH),$$

por definição de produto em G/H. Mas,

$$\phi^\star(xyH) = \phi(xy) = \phi(x)\phi(y),$$

por definição de $\phi^\star$ e porque ϕ é um homomorfismo de grupos. Assim,

$$\phi^\star(xHyH) = \phi(x)\phi(y) = \phi^\star(xH)\phi^\star(yH),$$

por definição de $\phi^\star$. Finalmente, resulta da própria construção que se tem

$$\phi^\star \circ \pi = \phi$$

De facto, para todo $x \in G$,

$$\phi^\star \circ \pi(x) = \phi^\star(\pi(x)),$$

por definição de composição de aplicações.

Mas,

$$\phi^\star(\pi(x)) = \phi^\star(xH) = \phi(x).$$

Provou-se então,

$$\forall x \in G, \phi^\star \circ \pi(x) = \phi(x),$$

o que é equivalente a

$$\phi^\star \circ \pi = \phi.$$

Prove-se a segunda parte do teorema.

Se $\phi^\star$ é um epimorfismo também ϕ o é, porque π é um epimorfismo e $\phi = \phi^\star \circ \pi$. Reciprocamente, se ϕ é um epimorfismo, dado um elemento qualquer $x' \in G'$ tem-se, para algum $x \in G$,

$$x' = \phi(x) = (\phi^\star \circ \pi)(x) = \phi^\star(\pi(x)),$$

pelo que $\phi^\star$ é sobrejectiva.

Por outro lado

$$\begin{aligned} \mathrm{Nuc}(\phi^\star) &= \{xH \in G/H : \phi^\star(xH) = e'\}, \text{ por definição de } \mathrm{Nuc}(\phi^\star); \\ &= \{xH \in G/H : \phi(x) = e'\}, \text{ por definição de } \phi^\star; \\ &= \{xH \in G/H : x \in \mathrm{Nuc}(\phi)\}, \text{ por definição de } \mathrm{Nuc}(\phi). \end{aligned}$$

Pelo Corolário 2.5.11, $\phi^\star$ é um monomorfismo se, e só se, $\mathrm{Nuc}(\phi^\star) = \{H\}$. Por outro lado, para $x \in \mathrm{Nuc}(\phi)$, tem-se $xH = H$ se, e só se, $x \in H$. Logo ter-se-á $\mathrm{Nuc}(\phi^\star) = \{H\}$ se, e só se, $x \in H$. Logo, será $\mathrm{Nuc}(\phi^\star) = \{H\}$ se, e só se, $\mathrm{Nuc}(\phi) \subseteq H$, o que, atendendo à hipótese do teorema equivale a $H = \mathrm{Nuc}(\phi)$. □

Corolário 2.7.2 (Teorema do Homomorfismo)**.** *Sejam G e G'grupos e $\phi : G \to G'$ um homomorfismo de grupos. Então $\phi(G) \simeq G/Nuc(\phi)$.*

Demonstração. Considere-se o diagrama

$$\begin{array}{lll} G & \stackrel{\phi}{\to} & \phi(G) \\ \pi \downarrow & & \\ G/\mathrm{Nuc}(\phi) & & \end{array}$$

Pelo Teorema 2.7.1 existe um homomorfismo

$$\phi^\star : G/\mathrm{Nuc}(\phi) \to \phi(G)$$

tal que $\phi^\star \circ \pi = \phi$. Assim, tendo em atenção o que se disse no teorema anterior conclui-se que $\phi^\star$ é uma bijecção, logo um isomorfismo. □

Proposição 2.7.3. *Para um grupo G, tem-se $G/\{e\} \simeq G$ e $G/G \simeq \{e\}$.*

Demonstração. Exercício. □

Corolário 2.7.4. *(Primeiro Teorema do Isomorfismo) Seja $\phi : G \to G'$ um epimorfismo de núcleo N. Se $N \subseteq H \lhd G$, então $H' = \phi(H) \lhd G'$ e tem-se*

$$G/H \simeq G'/H'.$$

Demonstração. Pelo Exercício 2.5.13 resulta que $H' = \phi(H) \lhd G'$. Para se estabelecer o isomorfismo pretendido considere-se a composição de homomorfismos

$$G \underset{\phi}{\to} G' \underset{\pi_{H'}}{\to} G'/H'.$$

Pelo Teorema 2.7.2, ter-se-á

$$G'/H' \simeq G/(\mathrm{Nuc}(\pi_{H'} \circ \phi)).$$

Mas

$$\begin{aligned}
\mathrm{Nuc}(\pi_{H'} \circ \phi) &= \{x \in G : (\pi_{H'} \circ \phi)(x) = H'\}, \text{ por definição de } \mathrm{Nuc}(\pi_{H'} \circ \phi); \\
&= \{x \in G : \pi_{H'}(\phi(x)) = H'\}, \text{ por definição de composição}; \\
&= \{x \in G : \phi(x)H' = H'\}, \text{ por definição de } \pi_{H'}; \\
&= \{x \in G : \phi(x) \in H'\}, \text{ por definição de igualdade de classes laterais} \\
&= \phi^{-1}(H'), \text{ por definição de } \phi^{-1}(H').
\end{aligned}$$

Tem-se $H \subseteq \phi^{-1}(H')$. Prove-se a inclusão contrária $\phi^{-1}(H') \subseteq H$. Seja $x \in \phi^{-1}(H')$. Então, $\phi(x) \in H'$. Como ϕ é sobrejectiva, existe $h \in H$ tal que $\phi(x) = \phi(h)$. Mas, $\phi(x) = \phi(h)$ é equivalente a $\phi(x)\phi(h)^{-1} = e'$, onde e'representa o elemento neutro de G'. Como ϕ é um homomorfismo, tem-se $\phi(xh^{-1}) = e'$, pelo que $xh^{-1} \in \mathrm{Nuc}(\phi) \subseteq H$. Assim, $xh^{-1} = h'$, para algum $h' \in H$, ou seja, $x = h'h \in H$. Assim, $\phi^{-1}(H') \subseteq H$. Daqui resulta que

$$\mathrm{Nuc}(\pi_{H'} \circ \phi) = \phi^{-1}(H') = H,$$

e portanto obtém-se o isomorfismo pretendido. □

Corolário 2.7.5 (Segundo Teorema do Isomorfismo)**.** *Sejam M e N subgrupos normais dum grupo G, onde $M \subseteq N$. Então $N/M \lhd G/M$ e tem-se*

$$G/N \simeq (G/M)/(N/M).$$

Demonstração. Existe uma aplicação bem definida que é um homomorfismo $\phi : G/M \to G/N$ tal que $\phi(gM) = gN$, para todo $g \in G$. Mais, esse homomorfismo é sobrejectivo e $\text{Nuc}(\phi) = N/M$. Mas, pelo corolário 2.7.2 $\phi(G/M) \simeq (G/M)/\text{Nuc}(\phi)$. Assim, G/N é isomorfo a $(G/M)/(N/M)$, como se pretende. □

Proposição 2.7.6. *Sejam G um grupo e H um subgrupo de G e seja K um subgrupo normal de G. Então o conjunto HK é um subgrupo de G, onde $HK = \{hn, h \in H \text{ e } n \in K\}$.*

Demonstração. O conjunto HK contém claramente a identidade de G. Sejam $x, y \in HK$. Dever-se-á provar que xy e x^{-1} são elementos de HK. Sejam então

$$x = hu, \text{ para algum } h \in H \text{ e algum } u \in K,$$

$$y = kv, \text{para algum } k \in H \text{ e algum } v \in K.$$

Então,

$$xy = (hk)(k^{-1}ukv).$$

Mas $k^{-1}uk \in K$, pois K é normal. Assim, $k^{-1}ukv \in K$, porque K é subgrupo de G. Da mesma forma $hk \in H$. Tem-se então que $xy \in HK$. Prove-se agora que $x^{-1} \in HK$. Ora

$$x^{-1} = (hu)^{-1} = u^{-1}h^{-1} = h^{-1}(hu^{-1}h^{-1}).$$

Mas, $h^{-1} \in H$ pois H é subgrupo de G e $hu^{-1}h^{-1} \in K$ pois K é subgrupo normal de G. Tem-se então que $x^{-1} \in HK$. Provou-se que

$$\forall x, y \in HK, xy \in HK.$$

e,

$$\forall x \in HK, x^{-1} \in HK.$$

o que garante que HK é um subgrupo de G. □

Corolário 2.7.7 (Terceiro Teorema do Isomorfismo)**.** *Seja G um grupo e H um subgrupo de G, e seja N um subgrupo normal de G. Então*

$$HN/N \simeq H/(N \cap H).$$

Demonstração. Tem-se que $N \lhd HN \leq G$ e $N \cap H \lhd H$ (prove!). Todo o elemento de HN/N é um subconjunto de N que é da forma hN para algum $h \in H$. Assim, se $\phi(h) = hN$,

para todo $h \in H$ então $\phi : H \to HN/N$ é um homomorfismo sobrejectivo. Na verdade, um elemento de HN/N será da forma $(hx)N$, onde $h \in H, x \in N$. Mas

$$(hx)N = (hN)(xN) = (hN)N = \phi(h).$$

Por outro lado,

$$\begin{aligned} \text{Nuc}(\phi) &= \{h \in H : \phi(h) = N\}, \text{ por definição de Nuc}(\phi); \\ &= \{h \in H : hN = N\}, \text{ por definição de } \phi; \\ &= \{h \in H : h \in N\}, \text{ por definição de igualdade de classes laterais;} \\ &= N \cap H, \text{ por definição de intersecção de conjuntos.} \end{aligned}$$

Mas, pelo corolário 2.7.2 $\phi(H) \simeq H/\text{Nuc}(\phi)$. Assim, HN/N é isomorfo a $H/(N \cap H)$ como se pretende. □

2.7.1 Exercícios

1. Seja G um grupo. Denote por $Aut(G)$ o conjunto dos automorfismos de G.

1.1. Prove que $Aut(G)$ é um grupo para a composição usual.

1.2. Seja ι^a a função definida da seguinte forma

$$\begin{array}{rccc} \iota^a : & G & \to & G \\ & g & \longmapsto & a^{-1}ga. \end{array}$$

Prove que $InG = \{ \iota^a : a \in G\}$ é um subgrupo normal de $Aut(G)$.

1.3. Considere a função

$$\begin{array}{rccc} h : & G & \to & InG \\ & a & \longmapsto & \iota^{a^{-1}} \end{array}$$

Prove que h é um epimorfismo de grupos.

1.4. Prove que InG é isomorfo a $G/Z(G)$ onde $Z(G)$ representa o centro de G.

2. Sejam G, H dois grupos, J um subgrupo normal de G e K um subgrupo normal de H.

a) Considere a função

$$\begin{array}{rccc} f : & G \times H & \to & G/J \times H/K \\ & (x, y) & \longmapsto & (xJ, yK) \end{array}$$

(i) Prove que f é um epimorfismo de grupos.

(ii) Determine $\ker f$.

b) Prove que $\frac{G\times H}{J\times K}$ é isomorfo a $G/J \times H/K$.

3. Considere a aplicação $f : G \to H$ um homomorfismo de grupos. prove que:

3.1. Se a imagem de f tem n elementos, então $x^n \in \ker f$ para todo $x \in G$.

3.2. Seja m um inteiro tal que m e $|H|$ são primos entre si. Para todo $x \in G$, se $x^m \in \ker f$ então $x \in \ker f$. Observe que $|H|$ representa a ordem de H.

4. Considere o conjunto $\mathbb{R}^2$, com a adição definida do modo usual.

4.1. Verifique que $\left(\mathbb{R}^2, +\right)$ é um grupo.

4.2. Seja $C = \left\{(x, y) \in \mathbb{R}^2 : y = \frac{x}{2}\right\}$. Prove que $C \lhd \mathbb{R}^2$ e descreva o respectivo grupo cociente $\mathbb{R}^2/C$.

4.3. Dê uma interpretação geométrica de $\mathbb{R}^2$ e de $\mathbb{R}^2/C$.

5. Sejam $(\mathbb{R}, +)$ o grupo aditivo dos números reais, U o grupo multiplicativo dos números complexos de módulo unitário e $< 2\pi >$ o grupo cíclico gerado por 2π.

Prove directamente que $\frac{\mathbb{R}}{<2\pi>}$ é isomorfo a U.

Sugestão: Tenha em atenção a aplicação $\begin{array}{rccc} f: & \mathbb{R} & \to & U \\ & \theta & \longmapsto & e^{i\theta} = cis\theta, \end{array}$ com $|cis\theta| = 1$.

6. Seja $(G, +)$ o grupo **aditivo** formado por todas as sucessões de números reais onde,

$$\forall\, (x_n)_{n\in\mathbb{N}}, (y_n)_{n\in\mathbb{N}} \in G, (x_n)_{n\in\mathbb{N}} + (y_n)_{n\in\mathbb{N}} = (x_n + y_n)_{n\in\mathbb{N}}.$$

Considere o seguinte conjunto

$$H = \left\{(x_n)_{n\in\mathbb{N}} \in G : x_1 + x_2 = 0\right\}.$$

6.1. Mostre que $H \lhd G$ (ou seja, H é subgrupo normal de G).

6.2. Dada a aplicação $f : G \to \mathbb{R}$, definida por

$$f((x_n)_{n\in\mathbb{N}}) = x_1 + x_2$$

mostre que f é um homomorfismo entre os grupos **aditivos** G e $\mathbb{R}$. Averigúe, usando a definição, se f é sobrejectiva.

6.3. Determine $\ker f$ e descreva o grupo cociente $\frac{G}{\ker f}$.

6.4. Sendo $\pi : G \to \frac{G}{\ker f}$ o epimorfismo canónico, mostre directamente que existe um homomorfismo $f^* : \frac{G}{\ker f} \to \mathbb{R}$, tal que $f^* \circ \pi = f$.

2.8 Grupos Cíclicos

Viu-se anteriormente que cada subconjunto não vazio de um grupo G gera um determinado subgrupo de G. Qualquer grupo pode ser definido pela indicação de um sistema de geradores, já que se tem sempre $G =< G >$. Nesta secção estudam-se os grupos que são gerados apenas por um elemento.

Seja então G um grupo e $a \in G$. Um subgrupo de G que contém a, deverá conter a^2. Então, também conterá a^2a que é denotado por a^3. Em geral, deverá conter a^n com n inteiro positivo (viu-se que em notação aditiva se tem $na, n \in \mathbb{N}$). O conjunto das potências de expoente inteiro positivo de a é fechado para a multiplicação. No entanto, é possível que o inverso de a não esteja neste conjunto. Mas claramente, se um subgrupo de G contém a então também conterá a^{-1} e portanto $a^{-1}a^{-1}$, que se denota por a^{-2} e, em geral, deverá conter a^{-m}, para $m \in \mathbb{Z}^+$. Mas, também contém a identidade $a^0 = e = aa^{-1}$. Resumindo, um subgrupo de G que contém a, deverá conter todos os elementos da forma a^n(ou na, se se usar a notação aditiva), para qualquer $n \in \mathbb{Z}$. Ou seja, um subgrupo que contém a deverá conter

$$\{a^n, n \in \mathbb{Z}\}.$$

Observe-se que estas potências de a não necessitam de ser distintas.

é fácil verificar-se que $a^m a^n = a^{m+n}$, para $m, n \in \mathbb{Z}$.

Teorema 2.8.1. *Seja G um grupo e $a \in G$. Então $H = \{a^n : n \in \mathbb{Z}\}$ é um subgrupo de G e é o menor subgrupo de G que contém a, ou seja, todo o subgrupo que contém a contém H.*

Demonstração. De facto, $e = a^0 \in H$ e portanto $H \neq \varnothing$. Como $a^r a^s = a^{r+s}$, para $r, s \in \mathbb{Z}$, tem-se que o produto de dois elementos de H ainda está em H. Assim H é fechado para a operação que confere a G a estrutura de grupo.

Por outro lado, para $a^r \in H$, $a^{-r} \in H$, pois $-r \in \mathbb{Z}$. Assim, usando o Teorema 2.2.8, tem-se que $H \leq G$. Usando a argumentação feita antes do enunciado do teorema mostra-se que qualquer subgrupo de G que contém a deverá conter H, e portanto H é o menor subgrupo de G que contém a. □

Definição 2.8.2 (Subgrupo cíclico)**.** *O grupo $H = \{a^n : n \in \mathbb{Z}\}$ do Teorema 2.8.1 é o* subgrupo cíclico *de G gerado por a e será denotado por $< a >$.*

Note-se que, se G for aditivo, $< a >= \{na : n \in \mathbb{Z}\}$.

Definição 2.8.3 (Gerador; grupo cíclico)**.** *Um elemento a dum grupo G* gera *G e é chamado* gerador *de G se $G =< a >$. Um grupo é* cíclico *se é gerado apenas por um elemento.*

Não é difícil verificar que todo o grupo cíclico é comutativo.

Exemplo 2.8.4. *Considere-se o grupo $\mathbb{Z}$. Este grupo é cíclico e é gerado pelo elemento* 1 *ou pelo elemento* -1.

Exemplo 2.8.5. *Seja $\mathbb{Z}_4 = \{\overline{0}, \overline{1}, \overline{3}, \overline{4}\}$. Então $\mathbb{Z}_4$ é cíclico e $\overline{1}$ e $\overline{3}$ são geradores de $\mathbb{Z}_4$, ou seja*

$$< \overline{1} >=< \overline{3} >= \mathbb{Z}_4.$$

Exemplo 2.8.6. *O grupo $\{1, i, -1, -i\}$ é cíclico, pode-se tomar como gerador i ou $-i$.*

Exemplo 2.8.7. *Considere-se o grupo $(\mathbb{Z}, +)$. Vamos determinar $< 3 >$. Neste grupo a notação é aditiva e $< 3 >$ deverá conter*

$$\begin{aligned} 3, 3+3 &= 6, 3+3+3 = 9, \text{ e assim sucessivamente...} \\ 0, -3, -3+(-3) &= -6, -3+(-3)+(-3) = -9, \text{ e assim sucessivamente...} \end{aligned}$$

Por outras palavras, o subgrupo cíclico gerado por 3 *é constituído por todos os múltiplos de* 3*, positivos, negativos e nulos. Assim, $< 3 >= 3\mathbb{Z}$. De forma semelhante mostra-se que $n\mathbb{Z}$ é o subgrupo cíclico $< n >$ de $\mathbb{Z}$. Note-se que $6\mathbb{Z} \leq 3\mathbb{Z}$.*

Definição 2.8.8. *Sejam G um grupo e $a \in G$. Diz-se que a tem* ordem finita *em G se existirem inteiros positivos e distintos r, s tais que $a^r = a^s$.*

Neste caso usa-se a notação $O(a) < \infty$.

Definição 2.8.9. *Sejam G um grupo e $a \in G$. Diz-se que a tem* ordem infinita *em G se os elementos $a^0, a, a^2, \ldots$ são todos distintos.*

Neste caso usa-se a notação $O(a) = \infty$.

Proposição 2.8.10. *Seja um grupo cíclico $G =< a >$ finito. Então a tem ordem finita.*

Demonstração. Suponha-se que $< a >$ é finito e consider-se a aplicação $f : \mathbb{N} \to < a >$ definida por $f(n) = a^n, \forall n \in \mathbb{N}$. Se f fosse injectiva, $\mathbb{N} \simeq f(\mathbb{N})$, com $f(\mathbb{N}) \subseteq < a >$; como $\mathbb{N}$ é infinito $< a >$ também o seria. Logo f não é injectiva. Portanto, existem inteiros positivos distintos r, s tais que $a^r = a^s$. □

Proposição 2.8.11. *Seja um grupo cíclico $G =< a >$ finito. Então $G = \{e, a, \ldots, a^{\gamma-1}\}$ onde γ é igual ao menor dos naturais n tais que $a^n = e$.*

Demonstração. Seja um grupo cíclico $G =< a >$ finito. Pela proposição anterior existem inteiros positivos distintos r, s tais que $a^r = a^s$. Ter-se-á $r < s$ ou $r > s$. Sem perda de generalidade admita-se que $r < s$. Tem-se $s - r > 0$. De $a^r = a^s$, conclui-se que $a^{s-r} = e$. Logo existe um natural n tal que $a^n = e$ e $A = \{n \in \mathbb{N} : a^n = e\} \neq \varnothing$. Por $\mathbb{N}$ ser parcialmente ordenado, o conjunto A tem primeiro elemento γ, e tem-se $a^\gamma = e$. Prove-se que $< a >= \{e, a, \ldots, a^{\gamma-1}\}$. é evidente que $\{e, a, \ldots, a^{\gamma-1}\} \subseteq < a >$. Tome-se $a^l \in < a >$. Tem-se então, $l = \gamma q + r$, onde $r \in \{0, \ldots, \gamma - 1\}$ e $q \in \mathbb{Z}$. Donde $a^l = a^{\gamma q + r} = (a^\gamma)^q a^r = ea^r = a^r \in \{e, a, \ldots, a^{\gamma-1}\}$. Logo $< a > \subseteq \{e, a, \ldots, a^{\gamma-1}\}$. Assim, $G = \{e, a, \ldots, a^{\gamma-1}\}$. □

Definição 2.8.12. *Chama-se* ordem *dum elemento $a \in G$ ao menor inteiro positivo n tal que $a^n = e$.*

Usa-se a notação $O(a)$. Da proposição anterior tem-se que se $< a >$ é finito, $O(< a >) = O(a)$. Se G é um grupo infinito e $a \in G$ tem ordem infinita então o grupo cíclico gerado por a, $< a >$, tem ordem infinita.

2.8.1 Propriedades da Ordem de um Elemento

1. $O(e) = 1$

Demonstração. Trivial. □

2. $O(a) = O(a^{-1})$

Demonstração. Suponha-se que $O(a) = n$. Então, $a^n = e$ e $a^j \neq e$, $j \in \{1, \ldots, n-1\}$. Demonstre-se que $(a^{-1})^n = e$ e $(a^{-1})^j \neq e$ para todo $j \in \{1, \ldots, n-1\}$. Claramente $(a^{-1})^n = (a^n)^{-1} = e$. Suponha-se que existe $j \in \{1, \ldots, n-1\}$ tal que $(a^{-1})^j = e$. Então $(a^j)^{-1} = e$. Assim, $a^j = e$ o que é absurdo. □

3. Se $a = cbc^{-1}$ então $O(a) = O(b)$.

Demonstração. Suponha-se que $O(a) = n$ e prove-se que $O(b) = n$. Tem-se

$$a^n = (cbc^{-1})^n = (cbc^{-1}) \cdots (cbc^{-1}) = cb^n c^{-1}.$$

Assim, de

$$cb^n c^{-1} = a^n = e,$$

vem

$$b^n = e.$$

Suponha-se agora que existe $j \in \{1, \ldots, n-1\}$ tal que $b^j = e$. De $a = cbc^{-1}$ resulta $b = c^{-1}ac$ donde

$$b^j = c^{-1}a^j c = e.$$

Assim, existe $j \in \{1, \ldots, n-1\}$ tal que $a^j = e$ o que é absurdo porque $o(a) = n$. □

4. $O(a^m) \leq O(a), \forall m \in \mathbb{Z}$.

Demonstração. Suponha-se que $O(a) = n$ e que $O(a^m) = k$. Ora, por definição de ordem de um elemento, k é o menor inteiro positivo tal que $(a^m)^k = e$. Mas $(a^m)^n = e$, então $n \geq k$. □

5. Seja $O(a) = n$. Se $\text{mdc}(m, n) = 1$ então $O(a^m) = O(a) = n$.

Demonstração. Por 4. tem-se que $O(a^m) \leq n$. Prove-se que $O(a) = n \leq O(a^m)$. Como $\text{mdc}(m, n) = 1$, pelo Teorema de Bezout, existem inteiros α, β tais que

$$1 = \alpha m + \beta n.$$

Então,

$$a = a^{\alpha m + \beta n} = (a^m)^\alpha (a^n)^\beta = (a^m)^\alpha.$$

De $a = (a^m)^\alpha$ podemos concluir que $O(a) \leq O(a^m)$. □

Proposição 2.8.13. *Se $O(a) = n$ e se $m \in \mathbb{Z}$, então $a^m = e$ se e só se $m = kn$, $k \in \mathbb{Z}$ ou seja m é múltiplo de n.*

Demonstração. Condição Necessária. Suponha-se que $O(a) = n$ e $a^m = e$, com $m \in \mathbb{Z}$. Prove-se que m é múltiplo de n.

Tem-se

$$m = nq + r, r \in \{0, 1, \ldots, n-1\}, q \in \mathbb{Z}.$$

Então

$$e = a^m = a^{nq+r} = a^{nq}a^r = (a^n)^q a^r = a^r.$$

Assim, $r = 0$ pois $r \in \{0, 1, \ldots, n-1\}$ e $O(a) = n$. Portanto, m é múltiplo de n.

Condição Suficiente. Suponha-se que $m = nk, k \in \mathbb{Z}$. Então $a^m = a^{nk} = (a^n)^k = e$, como se pretendia. □

Teorema 2.8.14. *Todo o subgrupo dum grupo cíclico é cíclico.*

Demonstração. Seja H um subgrupo do grupo cíclico $G =< a >$. Suponha-se que $H = \{e\}$, então $H =< e >$ é cíclico.

Se $H \neq \{e\}$, seja a^m um elemento de H, de expoente positivo mínimo (justifique a sua existência). Então dado arbitrariamente $a^n \in H$ e considerando

$$n = mq + r, \text{ com } 0 \leq r < m, q \in \mathbb{Z}$$

tem-se

$$a^r = a^{n-mq} = a^n.(a^m)^{-q} \in H,$$

pelo que $r = 0$. Donde $a^n = a^{mq} = (a^m)^q$. Assim, $H =< a^m >$. □

Resulta deste teorema que se $H \neq \{e\}$ é um subgrupo de $G =< a >$, então $H =< a^m >$, onde m é o menor inteiro positivo tal $a^m \in H$. Por outro lado, se $H \neq \{e\}$ é um subgrupo de um grupo cíclico G, H é finito ou infinito conforme G é finito ou infinito.

Exemplo 2.8.15. *Seja $G =< a >$ um grupo cíclico de ordem 6. Tem-se $H =< a^4 >= \{e, a^2, a^4\} =< a^2 >$, onde $O(H) = 3$.*

Teorema 2.8.16. *Seja G um grupo cíclico infinito e H um seu subgrupo. Então $[G : H]$ é finito.*

Demonstração. No teorema anterior provou-se que $H =< a^m >$ onde a^m é um elemento de H, de expoente positivo mínimo. Prove-se então que $G = H \oplus Ha \oplus \cdots \oplus Ha^{m-1}$, é uma decomposição de G em classes laterais e portanto $[G : H] = m$. Prove-se primeiro que $Ha^i \cap Ha^j = \varnothing$ para $i \neq j$ e $i, j \in \{0, \ldots, m-1\}$ e $G = H \cup Ha \cup \cdots \cup Ha^{m-1}$. Suponha-se então que existe $x \in Ha^i \cap Ha^j$, para alguns $i, j \in \{0, \ldots, m-1\}$ e $i \neq j$. Suponha-se, sem perda de generalidade que $i > j$. Então,

$$x = (a^m)^q a^i = (a^m)^t a^j$$

com $q, t \in \mathbb{Z}$. Assim,

$$a^{i-j} = (a^m)^{t-q}$$

e, portanto $a^{i-j} \in H$ o que contraria o facto de m ser o menor inteiro positivo tal que $a^m \in H$. Assim, $Ha^i \cap Ha^j = \varnothing$ para $i \neq j$ e $i, j \in \{0, \ldots, m-1\}$. Prove-se agora que $G = Ha^0 \cup Ha \cup \cdots \cup Ha^{m-1}$. Seja $a^t, t \in \mathbb{Z}$ um elemento de G. Pelo algoritmo da divisão, existem q e r inteiros, com $0 \leq r \leq m-1$ tais que $t = mq + r$. Assim,

$$a^t = a^{mq+r} = (a^m)^q a^r \in Ha^r.$$

Portanto, $G \subseteq Ha^0 \cup Ha \cup \cdots \cup Ha^{m-1}$. Claramente $H \cup Ha \cup \cdots \cup Ha^{m-1} \subseteq G$. Das duas inclusões provou-se a igualdade. □

Teorema 2.8.17. *Se G é um grupo cíclico infinito e $m \in Z^+$, então existe um único subgrupo H tal que $[G : H] = m$.*

Demonstração. A existência está garantida pelos dois resultados anteriores. Prove-se a unicidade. Seja K um subgrupo de G tal que $[G : K] = m$. Como K é um subgrupo de G, pelo Teorema 2.8.14, K é cíclico e é gerado por a^t, onde t é o menor inteiro positivo tal que $a^t \in K$. Pelo Teorema 2.8.16, $[G : K] = t$, pelo que $t = m$ e por conseguinte $H = K$. □

Apresentam-se de seguida alguns teoremas que caracterizam os subgrupos dos grupos cíclicos finitos.

2.8.2 Caracterização dos Subgrupos dos Grupos Cíclicos Finitos

Teorema 2.8.18. *Seja G um grupo cíclico finito de ordem n. Então todo o seu subgrupo $H \neq \{e\}$ é cíclico e $[G : H]$ é divisor de n.*

Demonstração. Pelo Teorema 2.8.14, H é cíclico. Pelo Teorema de Lagrange, $[G : H]$ é divisor de n. □

Teorema 2.8.19. *Seja G um grupo cíclico finito de ordem n. Então G contém um único subgrupo de cada ordem que divide n.*

Demonstração. Seja $G =< a >$, $a \neq e$. Seja $d > 0$ um qualquer divisor de n. Tem-se $n = kd, k \in \mathbb{Z}^+$. Prove-se que existe um subgrupo de G de ordem d e de seguida, prove-se que esse subgrupo é único. Veja-se que $H = \{e, a^k, a^{2k}, \ldots, a^{(d-1)k}\}$ é um subgrupo de G. Claramente H é um subconjunto não vazio de G. Como G é finito, para provar que H é um subgrupo de G basta provar que para quaisquer elementos $a^{ik}, a^{jk}, i, j \in \{0, \ldots, d-1\}$,

$$a^{ik}a^{jk} = a^{(i+j)k} \in H.$$

De facto,

1. se $i + j \leq d - 1$, então $a^{(i+j)k} \in H$, por definição.
2. se $i + j \geq d$ então dividindo $i + j$ por d tem-se

$$i + j = qd + r, 0 \leq r < d.$$

Consequentemente $a^{(i+j)k} = a^{(qd+r)k} = a^{qdk}a^{rk} = (a^{dk})^q a^{rk} = (a^n)^q a^{rk} = a^{rk}$, $r \in \{0, \ldots, d-1\}$. Assim, $a^{(i+j)k} \in H$. Viu-se então que H é um subgrupo de G de ordem d. Mais, pelo Teorema de Lagrange, a ordem do subgrupo H divide a ordem do grupo.

Resta provar a unicidade. Admita-se que H' é um subgrupo de G de ordem d. Como G é cíclico, então H' é cíclico e gerado por a^m um elemento de H, de expoente positivo mínimo. Então, $[G : H'] = m$ e pelo Teorema de Lagrange $n = md$. Como $n = kd$ tem-se $kd = md$. Assim, $k = m$ pelo que $H' =< a^k >$ e portanto $H' = H$. □

A demonstração do teorema anterior indica-nos um processo de determinação dos geradores de um subgrupo de um grupo cíclico finito.

Exemplo 2.8.20. *Seja G um grupo cíclico de ordem 6 gerado por a. O grupo G tem um único subgrupo de ordem 3, H. Como $6 = 2 \times 3$, tem-se que H é o subgrupo de G gerado por a^2, ou seja, $H = \{e, a^2, a^4\}$.*

Teorema 2.8.21. *Seja G um grupo finito de ordem n, não prima. Então G tem pelo menos um subgrupo próprio.*

Demonstração. Exercício. □

Teorema 2.8.22. *Se G é um grupo finito de ordem prima, então G é cíclico e qualquer dos elementos distintos da identidade lhe serve de gerador.*

Demonstração. Suponha-se que $O(G) = n$, com n primo. Se $G = \{e\}$ a demonstração é trivial. Seja $H =< a >$, com $a \neq e$. Note-se que a tem ordem finita porque G é finito. Vamos ver que $H = G$. Como $O(H)|O(G)$, então $O(H) = 1$ ou $O(H) = n$. Mas $H \neq \{e\}$. Logo $O(H) = n$. Assim, $H = G$. □

Mostrar-se-á agora que é possível identificar todos os grupos cíclicos (a menos de isomorfismo).

Teorema 2.8.23. *Seja G um grupo cíclico, então G é isomorfo a $\mathbb{Z}$ ou a $\mathbb{Z}_m$, para $m \in \mathbb{N}$.*

Demonstração. Seja $G =< a >$. Defina-se a aplicação:

$$\begin{array}{rcl} \theta : \mathbb{Z} & \to & G \\ n & \to & a^n \end{array}$$

A aplicação θ é um homomorfismo de grupos, de facto, para quaisquer $n, m \in \mathbb{Z}$,

$$\theta(n+m) = a^{n+m} = a^n a^m = \theta(n)\theta(m).$$

Claramente θ é um epimorfismo. Aplicando o Teorema do Homomorfismo, tem-se que

$$< a > \simeq \mathbb{Z}/\mathrm{Nuc}(\theta).$$

Se θ é injectiva, então $\mathrm{Nuc}(\theta) = \{0\}$, pelo que

$$\mathbb{Z}/\mathrm{Nuc}(\theta) \simeq \mathbb{Z}/\{0\} \simeq \mathbb{Z}$$

e portanto

$$< a > \simeq \mathbb{Z}.$$

Se θ não é injectiva, então $\mathrm{Nuc}(\theta) \neq \{0\}$ e porque $\mathrm{Nuc}(\theta) \leq \mathbb{Z}$, haverá em $\mathrm{Nuc}(\theta)$ números positivos (porquê?). Seja então m o menor positivo em $\mathrm{Nuc}(\theta)$. Tomando arbitrariamente $n \in \mathrm{Nuc}(\theta)$, divida-se n por m. Tem-se então:

$$n = mk + r, \text{ com } 0 \leq r < m.$$

Assim,

$$\theta(n) = a^n = a^{mk+r} = (a^m)^k a^r = a^r.$$

Como $n \in \mathrm{Nuc}(\theta)$, $a^r = e$ e portanto $r \in \mathrm{Nuc}(\theta)$. Mas então $r = 0$ uma vez que $r < m$ e m é o menor positivo em $\mathrm{Nuc}(\theta)$, pelo que

$$n = mk, k \in \mathbb{Z}.$$

Assim $n \in m\mathbb{Z}$. Reciprocamente, seja y um elemento de $m\mathbb{Z}$. Então $y = ms$, para algum $s \in \mathbb{Z}$. Tem-se

$$\theta(y) = \theta(ms) = a^{ms} = (a^m)^s = e,$$

pelo que $ms \in \mathrm{Nuc}(\theta)$. Assim,

$$\mathrm{Nuc}(\theta) = m\mathbb{Z}.$$

Pelo Teorema Fundamental do Homomorfismo,

$$< a > \simeq \mathbb{Z}/m\mathbb{Z} = \mathbb{Z}_m.$$

□

2.8.3 Exercícios

1. Seja $a \in G$ um elemento de ordem finita ($a \neq e$). Prove que:

1.1. $O(a^k)$ divide $O(a)$;

1.2. Se $a^p = e$ e p é um número primo então $O(a) = p$;

1.3. Se $O(a) = km$ então $O(a^k) = m$;

1.4. Se $O(a) = n$ e n é ímpar então $O(a^2) = n$;

1.5. Se $O(a) = n$ e $a^r = a^s$ então n é um divisor de $r - s$;

1.6. Se $O(a) = mk$ e $a^{rk} = e$ então r é múltiplo de m.

2. Seja $G = \langle a \rangle, a \neq e_G$, onde e_G denota o elemento neutro de G.

2.1. Se $a^{56} = a^{73}$, qual é a ordem de G?

2.2. Se $a^{58} = a^{73}$, que se pode dizer sobre a ordem de G? E qual seria, neste caso, a ordem do subgrupo gerado por a^7?

3. Mostre que num grupo finito G de ordem m,

$$\forall g \in G, g^m = e.$$

4. Considere definida num grupo G a seguinte relação,

$$aRb \text{ se e só se } \exists g \in G : b = gag^{-1}.$$

Se aRb diz-se que a e b são elementos conjugados.

4.1. Prove que R é uma relação de equivalência.

4.2. Prove que elementos conjugados têm a mesma ordem.

5. Seja G o grupo cíclico de ordem 6 gerado por a.

Considere os seguintes subgrupos de G,

$$H = \{e, a^2, a^4\}, K = \{e, a^3\}.$$

Indique os elementos e escreva a tabela dos grupos cociente G/H e G/K.

6. Considere o grupo cíclico, G, gerado por um elemento a de ordem 12.

6.1. Indique todos os subgrupos de G de ordem 6. Justifique.

6.2. Prove que $H = \{e, a^4, a^8\}$ é um subgrupo de G.

6.3. Decomponha G em classes laterais à direita segundo H. Justifique.

7. Escreva os subgrupos de $\mathbb{Z}_{12}$ gerado por 6 e 9.

8. Mostre que $\mathbb{Z}_2 \times \mathbb{Z}_3$ é um grupo cíclico.

9. Sejam H, H^*, K, K^* grupos.

9.1. Prove que se H é isomorfo a H^* e K é isomorfo a K^* então $H \times K$ é isomorfo a $H^* \times K^*$.

9.2. Prove que $C_3 \times C_2$ é isomorfo a C_6. Onde C_n é o grupo cíclico de ordem n.

9.3. Justifique que $\mathbb{Z}_3 \times \mathbb{Z}_2$ é isomorfo a $\mathbb{Z}_6$ usando as duas alíneas anteriores.

10. Seja G o grupo $\mathbb{Z}_{15}$ e $H =< 5 >$ um subgrupo de G. Indique todas as classes laterais de H. Para cada classe lateral indique os seus elementos.

11. Seja G um grupo e $a, b \in G$. Prove que:

11.1. Se a, b e ab têm ordem 2 então a e b comutam.

11.2. Se $O(a) = m, O(b) = n$, com m, n primos entre si, e se $k, r \in \mathbb{Z}$ são tais que $a^k \neq e$ ou $b^r \neq e$, então $a^k \neq b^r$.

11.3. Se a, b comutam, $O(a) = m, O(b) = n$, com m, n primos entre si, então $O(ab) = mn$.

12. Seja $H = \{a^t, t \in \mathbb{Z}\}$ um grupo cíclico infinito. Determine um subgrupo K de H tal que $[H : K] = 7$.

13. Seja $G =< a >$ um grupo cíclico. Sejam $m, n \in \mathbb{N}$.

Sejam $H =< a^m >$ e $K =< a^n >$. Prove que:

13.1. $< H \cup K >=< a^d >$, onde d é o máximo divisor comum entre m e n.

13.2. $< H \cap K >=< a^c >$, onde c é o minimo múltiplo comum entre m e n.

14. Sejam $(G, .)$ um grupo cíclico, $(G', \star)$ um grupóide e $\phi : G \to G'$ um epimorfismo de grupóides. mostre que:

14.1. G' é grupo cíclico.

14.2. Se G é grupo de ordem finita então a ordem de G' divide a ordem de G.

2.9 O Grupo Simétrico

Seja X um conjunto não vazio.

Definição 2.9.1. *Chama-se permutação de X a toda a aplicação bijectiva de X em X.*

Denota-se por S_X o conjunto de todas as permutações de X. Enunciam-se algums resultados:

1. A composta de duas bijecções é uma bijecção.
2. A composta de aplicações é associativa.
3. A aplicação $\epsilon : X \to X$ tal que $\forall x \in X$, $\epsilon(x) = x$ é o elemento neutro para a composição de funções definidas em X.
4. Se f é uma bijecção definida em X, existe uma bijecção $f^{-1} : X \to X$ tal que $f^{-1} \circ f = f \circ f^{-1} = \epsilon$, onde $f^{-1} : X \to X$ tal que $f^{-1}(y) = x$ se e só se $y = f(x)$.

Das observações anteriores resulta que $(S_X, \circ)$ é um grupo.

Suponha-se que $X = \{a_1, a_2, \ldots, a_n\}$ é um conjunto não vazio e finito. O elemento $\sigma \in S_X$ pode ser representado pela tabela:

$$\sigma = \begin{pmatrix} a_1 & a_2 & \cdots & a_n \\ \sigma(a_1) & \sigma(a_2) & \cdots & \sigma(a_n) \end{pmatrix}. \tag{2.8}$$

A natureza dos objectos $a_i, i \in \{1, \ldots, n\}$ não tem qualquer importância para o estudo das permutações. Interessa saber apenas o cardinal de X. Assim,. para facilitar a manipulação das permutações toma-se para $X = \{1, \ldots, n\}$, onde os símbolos $1, 2, \ldots, n$ dum modo geral não têm qualquer significado numérico. Representam n objectos distintos.

Denota-se também S_X por S_n. Chama-se por vezes a S_n grupo simétrico de grau n. O grupo S_n tem $n!$ elementos.

Assim, em vez da representação 2.8 usar-se- á para σ a representação:

$$\sigma = \begin{pmatrix} a_1 & a_2 & \cdots & a_n \\ x_1 & x_2 & \cdots & x_n \end{pmatrix}$$

onde $x_i = \sigma(a_i)$ para todo $i \in \{1, \ldots, n\}$.

2.9.1 Produto de Permutações

Sejam σ e η dois elementos de S_n, onde

$$\sigma : i \to \sigma(i) = x_i$$

e

$$\eta : j \to \eta(j) = y_j$$

onde $i, j \in \{1, \ldots, n\}$. Defina-se $\sigma\ \eta = \eta \circ \sigma$. Temos pois

$$\sigma\eta(i) = \eta \circ \sigma(i) = \eta(\sigma(i)) = \eta(x_i).$$

De modo análogo,

$$\eta\sigma(j) = \sigma \circ \eta(i) = \sigma(\eta(j)) = \sigma(y_j).$$

Em geral

$$\sigma\eta \neq \eta\sigma$$

Exemplo 2.9.2. *Sejam* $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \end{pmatrix}$ *e* $\eta = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 1 & 4 & 2 \end{pmatrix}$

De

$$\sigma\eta(i) = \eta[\sigma(i)] = \eta(x_i),$$

tem-se

$$\sigma\eta(1) = \eta[\sigma(1)] = \eta(2) = 1$$

$$\sigma\eta(2) = \eta[\sigma(2)] = \eta(3) = 4$$

$$\sigma\eta(3) = 2$$

$$\sigma\eta(4) = 3.$$

Então, na prática, o cálculo do produto de duas permutações poderá ser organizado da seguinte forma:

$$\sigma\eta = \eta \circ \sigma = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \end{pmatrix} \begin{pmatrix} 2 & 3 & 4 & 1 \\ 1 & 4 & 2 & 3 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 4 & 2 & 3 \end{pmatrix}$$

Observe-se que

$$\eta = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 1 & 4 & 2 \end{pmatrix} = \begin{pmatrix} 2 & 3 & 4 & 1 \\ 1 & 4 & 2 & 3 \end{pmatrix}$$

$$\eta\sigma = \sigma \circ \eta = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 1 & 4 & 2 \end{pmatrix} \begin{pmatrix} 3 & 1 & 4 & 2 \\ 4 & 2 & 1 & 3 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 2 & 1 & 3 \end{pmatrix}.$$

Tem-se

$$\sigma\eta \neq \eta\sigma.$$

O elemento neutro de S_n é a permutação

$$\epsilon = \begin{pmatrix} 1 & 2 & 3 & \cdots & n \\ 1 & 2 & 3 & \cdots & n \end{pmatrix}$$

e a inversa duma permutação

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & \cdots & n \\ x_1 & x_2 & x_3 & \cdots & x_n \end{pmatrix}$$

$$\sigma^{-1} = \begin{pmatrix} x_1 & x_2 & x_3 & \cdots & x_n \\ 1 & 2 & 3 & \cdots & n \end{pmatrix},$$

Exemplo 2.9.3. *A inversa de* $\sigma = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}$ *é* $\sigma^{-1} = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}$. *Repare-se que* $\sigma\sigma^{-1} = \sigma^{-1}\sigma = \epsilon$.

2.9.2 Classe de Permutações Comutáveis

Comece-se por ilustrar esta subsecção com um exemplo.

Considerem-se as permutações σ e η de S_6 definidas por:

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 3 & 1 & 4 & 5 & 6 \end{pmatrix}$$

e

$$\eta = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 1 & 2 & 3 & 5 & 6 & 4 \end{pmatrix}.$$

Verifique que $\sigma\eta = \eta\sigma$. Este facto será acidental ou ilustrará uma classe de permutações comutáveis?

Observe-se que σ e η deixam invariantes partes complementares do domínio, o conjunto $X = \{1, 2, 3, 4, 5, 6\}$. Os conjuntos $A = \{1, 2, 3\}$, $B = \{4, 5, 6\}$ constituem uma partição de X; σ deixou invariante o conjunto B e η deixou invariante o conjunto A. Assim, formalizando:

Seja $\{a_1, a_2, \ldots, a_u, b_1, b_2, \ldots, b_v\}$, $u + v = n$ uma partição de $\{1, 2, \ldots, n\}$.

- σ actua sobre $a_1, a_2, \ldots, a_u$ e deixa $b_1, b_2, \ldots, b_v$ invariantes.
- η actua sobre $b_1, b_2, \ldots, b_v$ e deixa $a_1, a_2, \ldots, a_u$ invariantes.

Então,

$$\sigma = \begin{pmatrix} a_1 & a_2 & \cdots & a_u & b_1 & b_2 & \cdots & b_v \\ \sigma(a_1) & \sigma(a_2) & \cdots & \sigma(a_u) & b_1 & b_2 & \cdots & b_v \end{pmatrix}$$

e

$$\eta = \begin{pmatrix} a_1 & a_2 & \cdots & a_u & b_1 & b_2 & \cdots & b_v \\ a_1 & a_2 & \cdots & a_u & \eta(b_1) & \eta(b_2) & \cdots & \eta(b_v) \end{pmatrix}.$$

Tem-se, $\sigma\eta = \eta \circ \sigma = \sigma \circ \eta = \eta\sigma$. De facto,

$$\sigma\eta = \eta \circ \sigma = \sigma \circ \eta = \eta\sigma = \begin{pmatrix} a_1 & a_2 & \cdots & a_u & b_1 & b_2 & \cdots & b_v \\ \sigma(a_1) & \sigma(a_2) & \cdots & \sigma(a_u) & \eta(b_1) & \eta(b_2) & \cdots & \eta(b_v) \end{pmatrix}$$

2.9.3 Decomposição de uma permutação num produto de ciclos

Seja $\{a_1, a_2, \ldots, a_u, b_1, b_2, \ldots, b_v\}$, $u + v = n$ uma partição de $\{1, 2, \ldots, n\}$.

Definição 2.9.4. *Chama-se ciclo de comprimento u à permutação $\theta \in S_n$ definida por*

$$\begin{cases} \theta(a_i) = a_{i+1}, i \in \{1, \ldots, u-1\} \\ \theta(a_u) = a_1 \\ \theta(b_j) = b_j, j \in \{1, \ldots, v\}. \end{cases}$$

Ou seja,

$$\theta = \begin{pmatrix} a_1 & a_2 & \cdots & a_u & b_1 & b_2 & \cdots & b_v \\ a_2 & a_3 & \cdots & a_1 & b_1 & b_2 & \cdots & b_v. \end{pmatrix}$$

Em geral, representa-se θ indicando apenas os elementos sobre os quais ela actua (ou seja, os elementos que move),

$$\theta = \begin{pmatrix} a_1 & a_2 & \cdots & a_u \end{pmatrix}.$$

Diz-se também que θ é um ciclo de comprimento u. Um ciclo de comprimento 1 é a permutação identidade. Dois ciclos que actuam sobre subconjuntos disjuntos dizem-se ciclos disjuntos. Assim, dois (ou mais) ciclos disjuntos comutam.

Exemplo 2.9.5. *Em S_6,*

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 3 & 2 & 4 & 5 & 6 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 3 & 4 & 5 & 6 \end{pmatrix}\begin{pmatrix} 2 \end{pmatrix} = \begin{pmatrix} 1 & 3 & 4 & 5 & 6 \end{pmatrix}.$$ O próximo teorema não será demonstrado. Apenas faremos uma ilustração deste teorema.

Teorema 2.9.6. *Toda a permutação de S_n pode decompor-se num produto de ciclos disjuntos dois a dois.*

Seja $\sigma \in S_6$, tal que $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 3 & 1 & 2 & 4 & 6 & 5 \end{pmatrix}$. Proceda-se à factorização de σ num produto de ciclos.

Seja

$$\theta_1 = \begin{pmatrix} 1 & 3 & 2 \\ 3 & 2 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 3 & 2 \end{pmatrix}.$$

Como σ actua sobre $X = \{1,2,3,4,5,6\}$ e θ_1 actua sobre $\{1,2,3\} \subset X$, continua-se o processo. Considere-se um dos elementos de X que não pertence a $\{1,2,3\}$. Seja $b_1 = 4$. Obtém-se

$$\theta_2 = \begin{pmatrix} 4 \\ 4 \end{pmatrix} = (4).$$

Como $\{1,2,3\} \cup \{4\} \subset X$, continua-se o procedimento como anteriormente. Seja $c_1 = 5$;vem

$$\theta_3 = \begin{pmatrix} 5 & 6 \\ 6 & 5 \end{pmatrix} = \begin{pmatrix} 5 & 6 \end{pmatrix}.$$

O ciclo θ_3 actua sobre o conjunto $\{5,6\}$. Como $\{1,2,3,4\} \cup \{5,6\} = X$, o processo terminou em 3 passos. Tem-se a factorização:

$$\sigma = \theta_1\theta_2\theta_3 = \begin{pmatrix} 1 & 3 & 2 \end{pmatrix}\begin{pmatrix} 4 \end{pmatrix}\begin{pmatrix} 5 & 6 \end{pmatrix}.$$

Atendendo às observações anteriores,

$$\sigma = \theta_1\theta_2\theta_3 = \begin{pmatrix} 1 & 3 & 2 \end{pmatrix}\begin{pmatrix} 5 & 6 \end{pmatrix}.$$

Seguem-se algumas observações:

1. A ordem dos factores é arbitrária pois os ciclos comutam dois a dois.

2. Dadas duas permutações, se na factorização de uma delas existir algum ciclo que não existe na factorização da outra então as permutações dadas são necessariamente distintas.

3. A decomposição de uma permutação num produto de ciclos é pois, única a menos da ordem.

Teorema 2.9.7. *Seja* $\theta = \begin{pmatrix} a_1 & a_2 & \cdots & a_m \end{pmatrix}$ *um ciclo de comprimento* m*. Então a ordem de* θ *é* m*.*

Teorema 2.9.8. *A ordem de uma permutação* $\sigma \in S_n$ *é igual ao mínimo múltiplo comum das ordens dos ciclos em que esta se decompõe.*

Demonstração. Seja $\sigma = \theta_1\theta_2\cdots\theta_k$ onde $\theta_1, \theta_2, \ldots, \theta_k$ são ciclos disjuntos 2 a 2. Suponha-se que $O(\theta_i) = \mu_i, i \in \{1, \ldots, k\}$. Vamos ver que

$$O(\sigma) = c = \text{mmc}(\mu_1, \ldots, \mu_k).$$

Como os ciclos comutam 2 a 2 tem-se:

$$\sigma^c = (\theta_1\theta_2\cdots\theta_k)^c = \theta_1^c\theta_2^c\cdots{\theta_k}^c.$$

Mas, sendo $c = \text{mmc}(\mu_1, \ldots, \mu_k), c = \alpha_i\mu_i, \alpha_i \in \mathbb{Z}^+$,

$$\theta_i^c = \theta^{\alpha_i\mu_i,} = (\theta_i^{\mu_i})^{\alpha_i} = \varepsilon^{\alpha_i} = \varepsilon.$$

Assim,

$$\sigma^c = \varepsilon.$$

Seja agora $m \in \mathbb{N}$ tal que

$$\sigma^m = \varepsilon.$$

Mostre-se que m é múltiplo de c o que garante que $O(\sigma) = c$. De $\sigma^m = \varepsilon$ resulta que

$$\theta_1^m\theta_2^m\cdots{\theta_k}^m = \varepsilon,$$

e, da igualdade anterior vem

$$\theta_1^m = (\theta_2^m\cdots{\theta_k}^m)^{-1}, \tag{2.9}$$

mas, tendo em atenção que uma permutação e a sua inversa actuam sobre o mesmo conjunto e, como os ciclos anteriores são disjuntos 2 a 2, de (2.9) tem-se,

$$\theta_1^m = \varepsilon.$$

Procedendo de modo análogo para todo i, conclui-se:

$$\theta_i^m = \varepsilon.$$

Mas,

$$\theta_i^m = \varepsilon \Leftrightarrow m = \beta_i \mu_i, i \in \{1, \ldots, k\}.$$

Atendendo a que $c = \text{mmc}(\mu_1, \ldots, \mu_k)$ tem-se então

$$m = \alpha c, \alpha \in \mathbb{N}.$$

□

Exemplo 2.9.9. *Seja* $\sigma \in S_8$, $\sigma = \begin{pmatrix} 1 & 2 \end{pmatrix}\begin{pmatrix} 3 & 4 & 5 \end{pmatrix}\begin{pmatrix} 6 & 7 & 8 \end{pmatrix}$, *então*

$$O(\sigma) = mmc(2, 3) = 6.$$

2.9.4 Permutações Conjugadas

Definição 2.9.10. *Duas permutações* $\sigma, \eta \in S_n$ *dizem-se conjugadas se existir uma permutação* $\xi \in S_n$ *tal que*

$$\sigma = \xi^{-1}\eta\xi.$$

Note-se que, se existe uma permutação ξ tal que $\sigma = \xi^{-1}\eta\xi$ equivale a dizer que existe uma permutação τ tal que $\eta = \tau^{-1}\sigma\tau$, com $\tau = \xi^{-1}$.

Suponhamos que

$$\eta = \theta_1\theta_2 \cdots \theta_k$$

onde θ_i são ciclos disjuntos dois a dois, $i \in \{1, \ldots, k\}$. Então,

$$\sigma = \xi^{-1}\eta\xi = (\xi^{-1}\theta_1\xi)(\xi^{-1}\theta_2\xi)\cdots(\xi^{-1}\theta_k\xi)$$

onde, para cada $i \in \{1, \ldots, k\}, \xi^{-1}\theta_i\xi$ é um ciclo de comprimento igual ao de θ_i e portanto, duas permutações conjugadas decompõem-se em ciclos do mesmo comprimento.

Mais, se $\theta = \begin{pmatrix} a_1 & a_2 & \cdots & a_m \end{pmatrix}$ é um ciclo arbitrário de comprimento m, $\xi^{-1}\theta\xi$ é um ciclo que actua sobre o conjunto $\{\xi(a_1), \ldots, \xi(a_m)\}$ isto é:

$$\xi^{-1}\theta\xi = \begin{pmatrix} \xi(a_1) & \xi(a_2) & \cdots & \xi(a_m) \end{pmatrix}.$$

2.9.5 Regra Prática para o Cálculo de uma Permutação Conjugada

A permutação $\xi^{-1}\theta\xi$ obtém-se de θ aplicando ξ aos objectos sobre os quais θ actua.

Exemplo 2.9.11. *Seja* $\sigma = \begin{pmatrix} 1 & 3 \end{pmatrix}\begin{pmatrix} 2 & 4 & 5 \end{pmatrix}$ *e* $\xi = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 4 & 5 & 1 & 3 \end{pmatrix}$. *Calcule a conjugada de* σ *usando* ξ. *Tem-se*

$$\xi^{-1}\sigma\xi = \begin{pmatrix} \xi(1) & \xi(3) \end{pmatrix}\begin{pmatrix} \xi(2) & \xi(4) & \xi(5) \end{pmatrix} = \begin{pmatrix} 2 & 5 \end{pmatrix}\begin{pmatrix} 4 & 1 & 3 \end{pmatrix}.$$

De seguida confirme-se usando o produto das respectivas permutações:

$$\begin{aligned}
\xi^{-1}\sigma\xi &= \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 4 & 1 & 5 & 2 & 3 \end{pmatrix}\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 4 & 1 & 5 & 2 \end{pmatrix}\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 4 & 5 & 1 & 3 \end{pmatrix} \\
&= \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 5 & 4 & 1 & 2 \end{pmatrix} \\
&= \begin{pmatrix} 1 & 3 & 4 \end{pmatrix}\begin{pmatrix} 2 & 5 \end{pmatrix} \\
&= \begin{pmatrix} 2 & 5 \end{pmatrix}\begin{pmatrix} 3 & 4 & 1 \end{pmatrix} \\
&= \begin{pmatrix} 2 & 5 \end{pmatrix}\begin{pmatrix} 4 & 1 & 3 \end{pmatrix}.
\end{aligned}$$

2.9.6 Transposições

Definição 2.9.12. *Chama-se transposição a um ciclo de comprimento* 2.

Uma transposição troca a ordem dos elementos sobre os quais actua (sentido estrito). Com efeito, a transposição

$$\zeta = \begin{pmatrix} a & b \end{pmatrix}$$

não é mais do que o ciclo $\begin{pmatrix} a & b \\ b & a \end{pmatrix}, \zeta(a) = b, \zeta(b) = a.$ é óbvio que $\zeta^2 = \begin{pmatrix} a & b \end{pmatrix}^2 = \begin{pmatrix} a & b \end{pmatrix}\begin{pmatrix} a & b \end{pmatrix} = \epsilon$ e que $\zeta^{-1} = \begin{pmatrix} a & b \end{pmatrix}^{-1} = \begin{pmatrix} b & a \end{pmatrix} = \zeta$. Uma transposição é a mais simples permutação não trivial ($\neq \epsilon$).

Diz-se que uma permutação $\sigma \in S_n$ se decompõe ou factoriza num produto de transposições se existir $s \in \mathbb{N}$ e transposições $\zeta_1, \ldots, \zeta_s$ tal que

$$\sigma = \zeta_1 \cdots \zeta_s.$$

é fácil ver que todo o ciclo ($\neq \epsilon$) se decompõe num produto de transposições. Com efeito, seja $\theta = \begin{pmatrix} a_1 & a_2 & \cdots & a_m \end{pmatrix}$. Tem-se

$$\theta = \begin{pmatrix} a_1 & a_2 \end{pmatrix}\begin{pmatrix} a_1 & a_3 \end{pmatrix}\cdots\begin{pmatrix} a_1 & a_m \end{pmatrix}.$$

Atenção!! Esta decomposição não é única. Com efeito, seja $\theta = \begin{pmatrix} 1 & 2 & 3 & 4 \end{pmatrix} \in S_6$. Tem-se $\theta = \begin{pmatrix} 1 & 2 \end{pmatrix}\begin{pmatrix} 1 & 3 \end{pmatrix}\begin{pmatrix} 1 & 4 \end{pmatrix}$. No entanto, $\theta = \begin{pmatrix} 2 & 3 & 4 & 1 \end{pmatrix} = \begin{pmatrix} 2 & 3 \end{pmatrix}\begin{pmatrix} 2 & 4 \end{pmatrix}\begin{pmatrix} 2 & 1 \end{pmatrix}$. Viu-se atrás que toda a permutação se pode compor num produto de ciclos disjuntos. Assim, pode-se escrever o seguinte teorema:

Teorema 2.9.13. *Toda a permutação de S_n ($n \geq 2$) diferente da identidade é um produto de transposições.*

De facto, basta ver que todo o ciclo se decompõe num produto de transposições.

Observações:

1. Viu-se que ciclos disjuntos são comutáveis.
2. é fácil verificar que, por exemplo em S_3, $\begin{pmatrix} 1 & 2 \end{pmatrix}\begin{pmatrix} 1 & 3 \end{pmatrix} \neq \begin{pmatrix} 1 & 3 \end{pmatrix}\begin{pmatrix} 1 & 2 \end{pmatrix}$. Isto mostra-nos que na factorização de uma permutação em transposições a ordem dos factores é importante.
3. Em tal decomposição o número de"factores" não é fixo. Por exemplo, em S_3

$$\begin{aligned}\begin{pmatrix} 1 & 2 \end{pmatrix}\begin{pmatrix} 1 & 3 \end{pmatrix} &= \begin{pmatrix} 1 & 2 \end{pmatrix}\begin{pmatrix} 2 & 3 \end{pmatrix}\begin{pmatrix} 2 & 3 \end{pmatrix}\begin{pmatrix} 1 & 3 \end{pmatrix} \\ &= \begin{pmatrix} 1 & 2 \end{pmatrix}\begin{pmatrix} 2 & 3 \end{pmatrix}\begin{pmatrix} 3 & 2 \end{pmatrix}\begin{pmatrix} 1 & 3 \end{pmatrix}.\end{aligned}$$

O próximo teorema permite concluir que o grupo simétrico é gerado por $n-1$ elementos.

Teorema 2.9.14. *O grupo simétrico S_n é gerado pelas $n-1$ transposições*

$$\begin{pmatrix} 1 & 2 \end{pmatrix}, \begin{pmatrix} 1 & 3 \end{pmatrix}, \ldots, \begin{pmatrix} 1 & n \end{pmatrix}.$$

Demonstração. Viu-se que todo o ciclo θ se decompõe num produto de transposições

$$\begin{pmatrix} a_i & a_j \end{pmatrix}, i \neq j,$$

consequentemente qualquer permutação se decompõe num produto de transposições da forma $\begin{pmatrix} a_i & a_j \end{pmatrix}, i \neq j, a_i, a_j, \in \{1, \ldots, n\}$. Mostre-se que cada transposição se pode decompor num produto de elementos do conjunto

$$\mathcal{G} = \{\begin{pmatrix} 1 & 2 \end{pmatrix}, \begin{pmatrix} 1 & 3 \end{pmatrix}, \ldots, \begin{pmatrix} 1 & n \end{pmatrix}\}.$$

é fácil verificar que

$$\tau = \begin{pmatrix} a_i & a_j \end{pmatrix} = \begin{pmatrix} 1 & a_j \end{pmatrix}\begin{pmatrix} 1 & a_i \end{pmatrix}\begin{pmatrix} 1 & a_j \end{pmatrix}.$$

Então qualquer permutação $\sigma \in S_n$ se pode decompor num produto de elementos de $\mathcal{G}$ o que prova que $\mathcal{G}$ gera S_n, como pretendido. □

Exemplo 2.9.15. *Em* S_3, $\begin{pmatrix} 2 & 3 \end{pmatrix} = \begin{pmatrix} 1 & 3 \end{pmatrix}\begin{pmatrix} 1 & 2 \end{pmatrix}\begin{pmatrix} 1 & 3 \end{pmatrix}$.

2.9.7 Paridade de uma Permutação

Considere-se a função $\triangle$ definida nas variáveis $x_1, x_2, \ldots, x_n$ do modo seguinte:

$$\triangle(x_1, x_2, \ldots, x_n) = \sum_{i,j=1, i<j}^{n} \prod (x_i - x_j)$$

ou seja,

$$\begin{array}{rcccccc} \triangle & = & (x_1 - x_2) & (x_1 - x_3) & \cdots & (x_1 - x_{n-1}) & (x_1 - x_n) \\ & & & (x_2 - x_3) & \cdots & (x_2 - x_{n-1}) & (x_2 - x_n) \\ & & & & \cdots & & \\ & & & & & (x_{n-2} - x_{n-1}) & (x_{n-2} - x_n) \\ & & & & & & (x_{n-1} - x_n). \end{array}$$

Sendo σ uma permutação de S_n que actua sobre as variáveis $x_1, x_2, \ldots, x_n$ represente-se por $\triangle_\sigma$a expressão que se obtém da expressão anterior substituindo x_i por $\sigma(x_i)$, ou seja:

$$\triangle_\sigma = \sum_{i,j=1, i<j}^{n} \prod (\sigma(x_i) - \sigma(x_j)).$$

é óbvio que

$$\triangle_\sigma = \pm\triangle = \xi(\sigma)\triangle,$$

onde $\xi(\sigma) = \pm 1$. Pode assim interpretar-se $\xi(\sigma)$ como o valor de uma função ξ definida em S_n do seguinte modo:

$$\begin{array}{rcl} \xi : S_n & \to & \{1, -1\} \\ \sigma & \to & \pm 1 \end{array}.$$

Se $\xi(\sigma) = 1$ diz-se que σ é uma permutação *par*.

Se $\xi(\sigma) = -1$ diz-se que σ é uma permutação *ímpar*.

à função ξ chama-se *carácter alternante* de S_n.

Teorema 2.9.16. *A função ξ é um homomorfismo.*

O teorema anterior traduz que, para todas as permutações σ e η de S_n se tem:

$$\xi(\sigma\eta) = \xi(\sigma)\xi(\eta).$$

A expressão anterior permite concluir que:

O produto de duas permutações da mesma paridade é uma permutação par e o produto de duas permutações de paridades distintas é uma permutação ímpar.

Exercício 2.9.17. *A identidade de S_n é uma permutação par.*

Exercício 2.9.18. *Duas permutações inversas têm a mesma paridade.*

Exercício 2.9.19. *Duas permutações conjugadas têm a mesma paridade.*

Teorema 2.9.20. *As transposições são permutações ímpares.*

Teorema 2.9.21. *A paridade de uma permutação $\sigma \in S_n$ coincide com a paridade do número de transposições em que se decompõe.*

Demonstração. De acordo com o Teorema 2.9.13, σ pode decompor-se num produto de transposições:

$$\sigma = \tau_1\tau_2\cdots\tau_s,$$

onde $\tau_j, j \in \{1,\ldots,s\}$ é uma transposição.

Então

$$\xi(\sigma) = \xi(\tau_1\tau_2\cdots\tau_s) = \xi(\tau_1)\xi(\tau_2)\cdots\xi(\tau_s) = (-1)^s.$$

Assim, $\xi(\sigma) = 1$ se e só se s é par e $\xi(\sigma) = -1$ se e só se s é ímpar.

Assim, o anterior significa que:

σ é par se e só se σ se decompõe num número par de transposições;

σ é ímpar se e só se σ se decompõe num número ímpar de transposições. □

Exemplo 2.9.22. *A permutação* $\sigma = \begin{pmatrix} 1 & 3 & 5 \end{pmatrix}\begin{pmatrix} 2 & 4 & 8 \end{pmatrix} \in S_8$ *é par. De facto,* $\sigma = \begin{pmatrix} 1 & 3 \end{pmatrix}\begin{pmatrix} 1 & 5 \end{pmatrix}\begin{pmatrix} 2 & 4 \end{pmatrix}\begin{pmatrix} 2 & 8 \end{pmatrix}, \xi(\sigma) = (-1)^4 = 1.$

2.9.8 Teorema de Cayley

Considere-se qualquer tabela de grupo. Note-se que cada linha fornece uma permutação dos elementos do grupo dispostos no topo da tabela. Analogamente, cada coluna da tabela fornece uma permutação do conjunto dos elementos do grupo que se encontram dispostos à esquerda da tabela. Então, não é surpreendente que todo o grupo finito G é isomorfo a um subgrupo do grupo S_G de todas as permutações de G. O mesmo é verdadeiro se o grupo for infinito. O teorema de Cayley diz que todo o grupo é isomorfo a algum a algum grupo de permutações com a operação de multiplicação de permutações já definida. Este é um resultado simples e intrigante e é um clássico da teoria de grupos.

A demonstração deste teorema será separada em 3 passos. Considere-se um grupo G qualquer.

passo 1 Encontrar um conjunto G' de permutações, candidato a formar um grupo com a operação usual de multiplicação de permutações e que seja isomorfo a G.

passo 2 Provar que G'é um grupo usando a multiplicação de permutações.

passo 3 Definir uma aplicação $\Phi : G \to G'$ e mostrar que Φ é um isomorfismo entre G e G'.

Teorema 2.9.23. *(Teorema de Cayley) Todo o grupo é isomorfo a um grupo de permutações.*

Demonstração. Considere-se um grupo G qualquer.

passo 1. Encontre-se um conjunto G' de permutações, candidato a formar um grupo com a operação usual de multiplicação de permutações e que seja isomorfo a G. Para $a \in G$, seja σ_a a aplicação de G em G definida por:

$$\sigma_a(x) = xa,$$

para $x \in G$. A aplicação anterior está bem definida. De facto sejam $x, y \in G$ tais que $x = y$. Então $xa = ya$ o que é equivalente a $\sigma_a(x) = \sigma_a(y)$. Note-se que a operação no grupo G está bem definida.

Mostre-se agora que σ_a é injectiva. Sejam $x, y \in G$ tais que $\sigma_a(x) = \sigma_a(y)$. Tem-se, por definição de σ_a que $xa = ya$. Mas, G é um grupo, é válida a lei do cancelamento. Logo $x = y$. Mais, se $y \in G$, então

$$\sigma_a(ya^{-1}) = (ya^{-1})a = y,$$

e portanto σ_a é sobrejectiva. Assim, σ_a é bijectiva e portanto é uma permutação de G, ou seja $\sigma_a \in S_G$. Seja

$$G' = \{\sigma_a | a \in G\}.$$

passo 2. Mostre-se que G' é um subgrupo de S_G. Dever-se-á mostrar que G' é fechado para o produto de permutações já definido, contém a permutação identidade e o inverso para cada um dos seus elementos. Primeiro prove-se que:

$$\sigma_a \sigma_b = \sigma_{ab}.$$

De facto, seja $x \in G$,

$$(\sigma_a \sigma_b)(x) = \sigma_b(\sigma_a(x)) = \sigma_b(xa) = xab = \sigma_{ab}(x).$$

Do anterior se conclui que G' é fechado para o produto de permutações. Claramente, para todo $x \in G$,

$$\sigma_e(x) = xe = x,$$

onde e representa a identidade do grupo G. Assim, σ_e é a permutação identidade em S_G e está em G'. Como $\sigma_a \sigma_b = \sigma_{ab}$, tem-se

$$\sigma_a \sigma_{a^{-1}} = \sigma_{aa^{-1}} = \sigma_e$$

e,

$$\sigma_{a^{-1}} \sigma_a = \sigma_e.$$

Assim,

$$(\sigma_a)^{-1} = \sigma_{a^{-1}},$$

e portanto, $(\sigma_a)^{-1} \in G'$. Assim G' é um subgrupo de S_G.

passo 3. Resta provar que G é isomorfo ao grupo apresentado no passo 2. Defina-se $\Phi : G \to G'$ por

$$\Phi(a) = \sigma_a,$$

para $a \in G$. A prova de que Φ está bem definida é deixada ao cuidado do leitor. Prove-se que Φ é injectiva. Sejam $a, b \in G$ tais que $\Phi(a) = \Phi(b)$. Então

$$\sigma_a = \sigma_b.$$

Em particular,

$$\sigma_a(e) = \sigma_b(e).$$

Assim, $ea = eb$ e, como em G é válida a lei do cancelamento, $a = b$. Pela própria definição de G' resulta que Φ é sobrejectiva. Finalmente, dados a, b elementos arbitrários de G, $\Phi(ab) = \sigma_{ab}$ e

$$\Phi(a)\Phi(b) = \sigma_a\sigma_b.$$

Então

$$\Phi(ab) = \Phi(a)\Phi(b).$$

□

2.9.9 Exercícios

1. Averigue quais dos seguintes conjuntos constituem grupos de permutações:

1.1. $M = \{\ f : \ \mathbb{R} \ \rightarrow \ \mathbb{R} \ : f(x) = ax + b, a \in \mathbb{R}\backslash\{0\}, b \in \mathbb{R}\}$;

1.2. $M = \{\ f : \ \mathbb{R}^2 \ \rightarrow \ \mathbb{R}^2 \ : f(x, y) = (x + a, 0), a \in \mathbb{R}\}$.

2. Seja S_n o grupo simétrico de grau n.

2.1. Diga o que é uma permutação de S_n.

2.2. Considere $G = S_5$, e seja

$$\alpha = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 5 & 4 & 1 & 2 \end{pmatrix}$$

um elemento de G.

i. Diga qual é a ordem de α.

ii. Descreva o grupo cíclico $< \alpha >$ gerado por α.

iii. Descreva os subgrupos próprios de α.

iv. Seja H o subgrupo próprio de maior ordem. Determine os índices $[< \alpha >: H]$ e $[G : H]$.

3. Considere as seguintes permutações f, g e h em S_6,

$$f = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 6 & 1 & 3 & 5 & 4 & 2 \end{pmatrix}$$

$$g = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 3 & 1 & 6 & 5 & 4 \end{pmatrix}$$

$$h = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 3 & 1 & 6 & 4 & 5 & 2 \end{pmatrix}$$

Calcule

3.1. hfg

3.2. $f^{-1}g^{-1}h$

3.3. $h^{-1}g$

3.4. g^3

4. Escreva cada uma das seguintes permutações de S_8 como produto de transposições

4.1. $(123)(456)(1574)$

4.2. $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 3 & 1 & 4 & 2 & 8 & 7 & 6 & 5 \end{pmatrix}$

5. Considere as permutações

$$\sigma = \begin{pmatrix} 5 & 4 & 3 & 2 & 1 & 8 & 7 & 6 \\ 3 & 1 & 4 & 8 & 2 & 5 & 6 & 7 \end{pmatrix}$$

$$\alpha = \begin{pmatrix} 5 & 4 & 3 & 2 & 1 & 8 & 7 & 6 \\ 4 & 2 & 3 & 8 & 1 & 5 & 6 & 7 \end{pmatrix}$$

$$\eta = \begin{pmatrix} 5 & 4 & 3 & 2 & 1 & 8 & 7 & 6 \\ 3 & 1 & 8 & 7 & 6 & 5 & 2 & 4 \end{pmatrix}$$

5.1. Decomponha estas permutações em ciclos disjuntos. Será esta decomposição única?

5.2. Decomponha estas permutações em transposições. Será a decomposição única? Se não, dê outra decomposição.

5.3. Qual é a ordem de σ, α e η? E a sua paridade?

5.4. Qual é o suporte destas permutações?

6. Justifique que as permutações seguintes são conjugadas e determine β tal que $\alpha = \beta\delta\beta^{-1}$ sendo

6.1. $\alpha = (1234)$ e $\delta = (2143), \alpha, \delta \in S_4$.

6.2. $\alpha = (1234)$ e $\delta = (1364)(257), , \alpha, \delta \in S_7$.

7. Sejam α e β ciclos disjuntos, $\alpha = (a_1 a_2 \cdots a_s), \beta = (b_1 b_2 \cdots b_r)$. Prove que

7.1. Para todo o inteiro positivo $n, (\ \alpha\beta)^n = \alpha^n \beta^n$;

7.2. Se $\alpha\beta = \epsilon$ então $\alpha = \epsilon$ e $\beta = \epsilon$;

7.3. Se $(\alpha\beta)^t = \epsilon$ então $\alpha^t = \epsilon$ e $\beta^t = \epsilon$, onde t é qualquer inteiro positivo.

(Obs. Use as alíneas a e b)

8. Considere um triângulo equilátero e o exemplo apresentado em anexo, o grupo diedral de ordem $3, D_3$, constituído pelas rotações relativamente ao centro e pelas simetrias relativas às bissectrizes dos ângulos munido da operação composição.

8.1. Construa o grupo diedral de ordem $4, D_4$, relativamente ao quadrado.

8.2. Determine um subgrupo de D_4 cuja ordem seja metade da ordem de D_4.

9. Averigue se pode aplicar o teorema de Cayley com

9.1. $G = \mathbb{Z}_4$;

9.2. G é o grupo aditivo dos números reais;

9.3. O grupo cíclico de ordem 3.

Capítulo 3

Tópicos sobre Teoria de Anéis

3.1 Anéis e Homomorfismos

3.1.1 Conceitos Elementares

No conjunto dos inteiros $\mathbb{Z}$, definem-se duas operações, que se designam por adição e multipicação, as quais gozam das seguintes propriedades: em relação à adição são válidas as propriedades associativa e comutativa, existe elemento neutro e todo o elemento tem simétrico, ou seja $(\mathbb{Z}, +)$ é um grupo abeliano.; em relação à multiplicação, é válida a propriedade associativa; são ainda válidas as propriedades distributivas à direita e à esquerda da multiplicação em relação à adição.

ás estruturas algébricas que, tal como $(\mathbb{Z}, +, .)$, gozam destas propriedades chamam-se anéis. Apresenta-se de seguida a definição formal.

Definição 3.1.1. *Um anel $(R, +, .)$ é uma estrutura algébrica constituída por um conjunto R com duas operações binárias, $+$ e $.$, normalmente designadas por adição e multiplicação, tal que são satisfeitos os seguinte axiomas:*

$\mathcal{R}_1 : (R, +)$ *é um grupo abeliano;*
$\mathcal{R}_2 : (R, .)$ *é um semigrupo, (isto é, $(R, .)$ é grupóide e, $\forall x, y, z \in R, x.(y.z) = (x.y).z$*
$\mathcal{R}_3$: *Para todos $a, b, c \in R$, a lei distributiva à esquerda $a.(b + c) = (a.b) + (a.c)$,*
e a lei distributiva à direita $(a + b).c = (a.c) + (b.c)$, é verificada.

Exemplo 3.1.2. *$(\mathbb{Z}, +, .)$, $(\mathbb{R}, +, .)$, $(\mathbb{Q}, +, .)$ e $(\mathbb{C}, +, .)$ são anéis.*

Um anel $(R, +, .)$ diz-se um anel comutativo se para todos $a, b \in R, a.b = b.a$. Um anel diz-se um anel com identidade, ou unitário, se existir um elemento $u \in R$ tal que para todo

$a \in R$, $u.a = a.u = a$. Denote-se a identidade do anel por 1. é usual denotar a multiplicação num anel por justaposição, usando a simbologia ab em vez de $a.b$. Tal como foi feito para o estudo dos grupos passará a ser referido " o anel R" em vez de " o anel $(R, +, .)$"", por exemplo, a partir de agora $\mathbb{Z}$ denotará o anel $(\mathbb{Z}, +, .)$.

Exemplo 3.1.3. *Seja R um anel e $\mathcal{M}_n(R)$ o conjunto das matrizes de tipo $n \times n$ que têm entradas em R. Este conjunto é um anel com a adição e multiplicação usuais de matrizes.*

Exemplo 3.1.4. *Seja $\mathcal{F}(\mathbb{R})$ o conjunto das funções reais de variável real. Sabemos que $(\mathcal{F}(\mathbb{R}), +)$ é um grupo com a adição de funções, onde para cada $x \in \mathbb{R}, (f+g)(x) = f(x)+g(x)$. Defina-se a operação*

$$\begin{array}{rcl} \bullet : \mathcal{F}(\mathbb{R}) \times \mathcal{F}(\mathbb{R}) & \to & \mathcal{F}(\mathbb{R}) \\ (f, g) & \to & fg \end{array}$$

onde, para todo $x \in \mathbb{R}, (fg)(x) = f(x)g(x)$. Assim, $\mathcal{F}(\mathbb{R})$ algebrizado com estas operações é um anel.

Exemplo 3.1.5. *Considere-se o conjunto $n\mathbb{Z} = \{n\alpha, \alpha \in \mathbb{Z}\}$. Já se viu que $n\mathbb{Z}$ é um subgrupo aditivo de $\mathbb{Z}$. Como $(nr)(ns) = n(nrs)$, para $r, s \in \mathbb{Z}$, pode observar-se que $n\mathbb{Z}$ é fechado para a multiplicação. As propriedades associativa e distributiva que se verificam em $\mathbb{Z}$, também se verificam em $n\mathbb{Z}$. Assim, $n\mathbb{Z}$ é um anel.*

Exemplo 3.1.6. *Se $R_1, R_2, \ldots, R_n$ são anéis, então*

$$R_1 \times R_2 \times \cdots \times R_n = \{(r_1, r_2, \ldots, r_n), r_i \in R_i, i \in \{1, \ldots, n\}\}.$$

Dados, $(r_1, r_2, \ldots, r_n), (r'_1, r'_2, \ldots, r'_n) \in R_1 \times R_2 \times \cdots \times R_n$, tem-se,

$$(r_1, r_2, \ldots, r_n) + (r'_1, r'_2, \ldots, r'_n) = (r_1 + r'_1, r_2 + r'_2, \ldots, r_n + r'_n),$$

$$(r_1, r_2, \ldots, r_n)(r'_1, r'_2, \ldots, r'_n) = (r_1 r'_1, r_2 r'_2, \ldots, r_n r'_n).$$

O conjunto anterior, algebrizado com as duas operações referidas é um anel. A este anel chama-se produto directo dos anéis $R_i, i \in \{1, \ldots, n\}$.

Ao elemento neutro dum anel $(R, +, .)$ relativamente à adição designa-se por zero do anel e representa-se pelo símbolo 0. O inverso de um elemento $a \in R$, relativamente à adição, designa-se por simétrico e representa-se por $-a$. Apresenta-se agora no próximo teorema, algumas propriedades elementares válidas num anel.

Teorema 3.1.7. *Se R é um anel e $a, b \in R$. Então*

1. $0a = a0 = 0$;
2. $a(-b) = (-a)b = -(ab)$;
3. $(-a)(-b) = ab$.

Demonstração. Para demonstrar 1. note-se que, pelos axiomas $\mathcal{R}_1$ e $\mathcal{R}_2$,

$$a0 + a0 = a(0 + 0) = a0 = 0 + a0.$$

Assim, usando a lei do cancelamento para o grupo aditivo $(R, +)$, tem-se $a0 = 0$. De forma análoga,

$$0a + 0a = (0 + 0)a = 0a = 0 + 0a,$$

o que implica que $0a = 0$. Para demonstrar a propriedade 2. recorde-se que $-(ab)$ representa o simétrico de ab, ou seja o elemento que adicionado a ab dá o elemento neutro do anel. Assim, para mostrar que $a(-b) = -ab$, dever-se-á precisamente mostrar que

$$a(-b) + ab = 0.$$

Usando a lei distributiva à esquerda

$$a(-b) + ab = a(-b + b) = a0 = 0,$$

uma vez que $a0 = 0$ pela propriedade 1. Analogamente,

$$(-a)b + ab = (-a + a)b = 0b = 0.$$

□

Definição 3.1.8. *(Unidade de um anel) Seja R um anel com identidade 1. Um elemento $a \in R$ diz-se um unidade do anel se existir $b \in R$ tal que $ab = ba = 1$.*

Observe-se que se $R \neq \{0\}$ é um anel com identidade 1, então $1 \neq 0$ e o elemento 0 não é invertível.

Se $a \in R$ é um elemento invertível, o elemento b referido na definição anterior é único. A esse elemento dá-se o nome de inverso de a e representa-se por a^{-1}. Estabelece-se então o seguinte resultado:

Proposição 3.1.9. *O conjunto das unidades de um anel R é um grupo multiplicativo.*

Demonstração. Seja $U_R = \{u \in R : u \text{ é uma unidade }\}$. Tem-se $U_R \neq \emptyset$ pois a identidade do anel é um elemento de U_R. E para qualquer $a \in U_R$, existe $a^{-1} \in A$ tal que $aa^{-1} = a^{-1}a = 1$. Então $a = (a^{-1})^{-1}$ e a^{-1} é invertível. Logo $a^{-1} \in U_R$. Tome-se agora $a, b \in U_R$. Então $a^{-1}, b^{-1} \in U_R$ e, se se considerar $b^{-1}a^{-1} \in R$, tem-se $(ab)(b^{-1}a^{-1}) = 1 = (b^{-1}a^{-1})(ab)$, logo $ab \in U_R$. Assim U_R é grupo. □

3.1.2 Divisores de Zero num Anel

Seja R um anel. Suponha-se $a \in R\backslash\{0\}$.

Definição 3.1.10. *Se existir $b \neq 0$ tal que $ab = 0$ diz-se que a é um divisor de zero à esquerda.*

Definição 3.1.11. *Se existir $b \neq 0$ tal que $ba = 0$ diz-se que a é um divisor de zero à direita.*

Definição 3.1.12. *Se existir $b \neq 0$ tal que $ab = 0$ ou $ba = 0$ diz-se que a é um divisor de zero.*

Observe-se que se R é comutativo um divisor de zero à esquerda coincide com um divisor de zero à direita.

Proposição 3.1.13. *Seja R um anel e a um elemento invertível em R. Então a não é um divisor de zero.*

Demonstração. Suponha-se que $a \in R\backslash\{0\}$ é um divisor de zero. Então existe $b \in R\backslash\{0\}$ tal que $ab = 0$ ou $ba = 0$. Suponha-se que $ab = 0$. Como a segunda operação no anel está bem definida, então $a^{-1}(ab) = a^{-1}0$. Da igualdade anterior resulta que $b = 0$ o que é absurdo. Se $ba = 0$ as conclusões seriam as mesmas. Assim a não é um divisor de zero. □

Proposição 3.1.14. *Seja R um anel. Então são equivalentes:*

1. *R admite a lei do corte;*
2. *R não tem divisores de zero.*

Demonstração. Suponha-se que R admite a lei do corte e que $ab = 0$ para alguns $a, b \in R$. Dever-se-á mostrar que $a = 0$ ou $b = 0$. Se $a \neq 0$, então $ab = a0$ implica que $b = 0$ pelas leis de cancelamento. Analogamente, $b \neq 0$ implica que $a = 0$. Assim, se em R é válida a lei do corte então não existem divisores de zero. Reciprocamente suponha-se que em R não existem divisores de zero e suponha-se que

$$ab - ac = a(b - c) = 0.$$

Como $a \neq 0$ e como em R não existem divisores de zero, tem-se $b - c = 0$ e portanto $b = c$. Um argumento semelhante mostra que se $ba = ca$ com $a \neq 0$ então $b = c$. □

Definição 3.1.15. *(Domínio de integridade) Chama-se domínio de integridade ou apenas domínio a um anel comutativo com identidade* $1 \neq 0$ *e sem divisores de zero.*

Exemplo 3.1.16. *Embora* $\mathbb{Z}_2$ *seja um domínio de integridade, no anel* $M_2(\mathbb{Z}_2)$ *existem divisores de zero. Repara-se por exemplo que* $\begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix}$ *é um divisor de zero pois*

$$\begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix} \begin{bmatrix} 0 & 0 \\ 1 & 0 \end{bmatrix} = \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}.$$

Definição 3.1.17. *Chama-se corpo a todo o domínio* $(R, +, .)$ *tal que todo o elemento de* $(R\backslash\{0\}, .)$ *é invertível.*

Teorema 3.1.18. *Todo o domínio de integridade finito é um corpo.*

Demonstração. Sejam $1, 0$, $a_1, \ldots, a_n$ todos os elementos dum domínio de integridade D. Ir-se-á mostrar que para $a \in D$ com $a \neq 0$, existe $b \in D$ tal que $ab = 1$. Considere-se

$$a1, aa_1, \ldots, aa_n.$$

Note-se que todos estes elementos são distintos, de facto se,

$$aa_i = aa_j,$$

com $i, j \in \{1, \ldots, n\}, i \neq j$, então, pelas leis de cancelamento, $a_i = a_j$ o que seria absurdo. Mais, como D é um domínio, não tem divisores de zero e portanto, nenhum dos elementos $a_1, \ldots, a_n$ é nulo. Assim, por contagem, observa-se que $a1, aa_1, \ldots, aa_n$ são os elementos $1, a_1, \ldots, a_n$ por alguma ordem e assim, tem-se que ou

$$a1 = 1, \text{ ou seja } a = 1,$$

ou

$$aa_i = 1, \text{ para algum } i.$$

Em qualquer situação, a tem um inverso multiplicativo. □

Corolário 3.1.19. *Se* p *é primo, então* Z_p *é um corpo.*

Demonstração. Este resultado segue do facto de que Z_p é um domínio de integridade e do teorema anterior. □

3.1.3 Subanéis

Definição 3.1.20. *(Subanel) Seja R um anel e $A \subseteq R$, $A \neq \emptyset$. Diz-se que A é um subanel de R se for um anel para as operações induzidas em A pelas operações de R.*

Definição 3.1.21. *Seja R um anel. Chamam-se subanéis triviais aos subanéis R e $\{0\}$. Ao segundo também se chama subanel nulo.*

Apresenta-se de seguida uma caracterização para que um subconjunto não vazio dum anel seja um subanel.

Proposição 3.1.22. *(Caracterização de subanel) Seja R um anel e $A \subseteq R$, $A \neq \emptyset$. Diz-se que A é um subanel de R se e só se para quaisquer $a, b \in A, a - b \in A$ e $ab \in A$.*

Demonstração. Basta ter em conta que A é subanel se e só se $(A, +)$ é subgrupo de $(R, +)$ e $(A, .)$ é subsemigrupo de $(R, .)$. □

Observação: Nas condições anteriores diz-se que $(A, .)$ é subsemigrupo de $(R, .)$ se $(A, .)$ for um grupóide associativo.

Como exemplo de aplicação do critério anterior tem-se o seguinte resultado.

Proposição 3.1.23. *Se $\{S_i\}_{i \in I}$ é uma família não vazia de subanéis de um anel R, $S = \bigcap_{i \in I} S_i$ é um subanel de R.*

Demonstração. Exercício. □

3.1.4 Homomorfismos de Anéis

Definição 3.1.24. *Sejam A, B dois anéis. Uma aplicação $f : A \to B$ diz-se um homomorfismo de anéis se para todos $a, b \in A$, $f(a + b) = f(a) + f(b)$ e $f(ab) = f(a)f(b)$.*

Um homomorfismo injectivo (respectivamente sobrejectivo, bijectivo) chama-se um monomorfismo (respectivamente epimorfismo, isomorfismo). No caso em que $B = A$ diz-se que se trata dum endomorfismo. Um endomorfismo que seja simultaneamente isomorfismo toma o nome de automorfismo.

Exemplo 3.1.25. *Se A e B são anéis, a aplicação $f : A \to B$ tal que a todo $x \in A$, faz corresponder $f(x) = 0$ é um homomorfismo a que se chama homomorfismo nulo.*

Exemplo 3.1.26. *A aplicação $f : \mathbb{Z} \to \mathbb{Z}_n$ tal que a cada $x \in \mathbb{Z}$, faz corresponder a classe de equivalência $[x]_R$, onde R é a relação de congruência módulo n, é um epimorfismo de anéis.*

Exemplo 3.1.27. *A aplicação $f : \mathbb{C} \to \mathbb{C}$ tal que a cada complexo $z \in \mathbb{C}$ faz corresponder o seu conjugado é um automorfismo de anéis.*

Os homomorfismos de anéis gozam de propriedades semelhantes às dos homomorfismos de grupos.

Proposição 3.1.28. *A composição de dois homomorfismos (respectivamente monomorfismos,epimorfismos, isomorfismos) de anéis é um homomorfismo (respectivamente monomorfismo,epimorfismo, isomorfismo) de anéis.*

Proposição 3.1.29. *Sejam A e B dois anéis, $B \neq \{0\}$ e $f : A \to B$ um homomorfismo de anéis. Denote-se por 0_A e 0_B os zeros de A e B respectivamente. Então*

1. $f(0_A) = 0_B$;
2. *Para todo $a \in A$, $f(-a) = f(a)$;*
3. *Se f é um epimorfismo e $1 \in A$ é a identidade de A, então $f(1) \neq 0_B$ é a identidade de B;*
4. *Se S é um subanel de A, então $f(S)$ é um subanel de B;*
5. *Se S' é um subanel de B então $f^{-1}(S')$ é um subanel de A.*

Demonstração. 1. e 2. resultam directamente do facto de que $(A, +)$ é grupo. As outras alíneas provam-se directamente a partir das definições. Prove-se então 3. Seja $b \in B$. Verifique-se que

$$f(1)b = bf(1) = b.$$

Como f é um epimorfismo e $b \in B$, existe $a \in A$ tal que $b = f(a)$. Assim,

$$f(1)b = f(1)f(a) = f(1a),$$

porque f é um epimorfismo. Mas $f(1a) = f(a)$ pois 1 é a identidade de A. Provou-se então que $f(1)b = f(a) = b$. Analogamente se prova que $bf(1) = b$ o que garante que $f(1) \neq 0_B$ é a identidade de B. Demonstre-se agora 4. Como S é um subanel de A, já se provou anteriormente que, considerando o grupo aditivo $(S, +)$, o conjunto $(f(S), +')$ é um subgrupo de $(B, +')$. Se $f(s_1)$ e $f(s_2)$ são elementos de $f(S)$, então, porque f é um homomorfismo,

$$f(s_1)f(s_2) = f(s_1s_2) \in f(S).$$

Assim, $f(s_1)f(s_2) \in f(S)$ e portanto $f(S)$ é fechado para a multiplicação. Consequentemente $f(S)$ é um subanel de B. Demonstre-se agora 5. Como S' é um subanel de B, então, $(f^{-1}(S'), +)$ é um subgrupo de $(A, +)$. Sejam $a, b \in f^{-1}(S')$. Tem-se $f(a), f(b) \in S'$. Então

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

Como, $f(a)f(b) \in S'$, então $ab \in f^{-1}(S')$ e portanto $f^{-1}(S')$ é fechado para a multiplicação e portanto é um subanel de A. □

3.1.5 Núcleo de um homomorfismo de anéis

Definição 3.1.30. *(Núcleo de um homomorfismo de anéis) Sejam A, B dois anéis e $f : A \to B$ um homomorfismo de anéis. Chama-se Núcleo de f ao conjunto*

$$Nuc(f) = \{x \in A : f(x) = 0\} = f^{-1}(\{0_B\})$$

Note-se que o núcleo do homomorfismo referido é o mesmo núcleo do homomorfismo entre os grupos $(A, +)$ e $(B, +')$ assim, os resultados obtidos nesta secção serão semelhante aos resultados obtidos na secção "Tópicos sobre Teoria de Grupos".

Teorema 3.1.31. *Sejam $f : A \to B$ um homomorfismo de anéis e $H = Nuc(f)$. Seja $a \in A$. Então $f^{-1}(\{(a)\}) = a + H = H + a$, onde $a + H = H + a$ é a classe lateral à esquerda de G que contém a do grupo aditivo abeliano $(H, +)$.*

Corolário 3.1.32. *Um homomorfismo de anéis $f : A \to B$ é uma aplicação injectiva se e só se $Nuc(f) = \{0\}$.*

O próximo teorema diz que a todo o anel sem identidade se pode associar um anel com identidade.

Teorema 3.1.33. *Seja R um anel sem identidade. Existe um anel com identidade R' que contém um subanel isomorfo a R.*

Demonstração. Passo1: Considere-se o produto cartesiano $R' = R \times \mathbb{Z}$. Defina-se em R' as operações

$\forall (a, m), (b, n) \in R'$,

$$(a, m) + (b, n) = (a + b, m + n)$$

$$(a, m)(b, n) = (ab + na + mb, mn).$$

O conjunto R' com estas operações é um anel com identidade.(Mostre!)

Passo 2. O conjunto $R \times \{0\}$é um subanel de R'. (Mostre!)

Passo 3. $R \times \{0\}$ é isomorfo a R. □

3.1.6 Anel Cociente

Teorema 3.1.34. *Seja $f : R \to R'$ um homomorfismo de anéis de núcleo H, ou seja $Nuc(f) = H$. Então R/H é um anel para as operações*

$$(a + H) + (b + H) = (a + b) + H,$$

$$(a + H)(b + H) = (ab) + H.$$

Mais, a função $\mu : R/H \to f(R)$ definida por $\mu(a + H) = f(a)$ é um isomorfismo.

Demonstração. A demonstração da parte aditiva já está feita. Vamos mostrar agora que o produto anterior não depende dos representantes escolhidos para as classes laterais. Sejam então $a' \in a + H$, $b' \in b + H$. Ir-se-á mostrar que $a'b' \in ab + H$. Tem-se então

$$a' = a + h_1, h_1 \in H,$$

$$b' = b + h_2, h_2 \in H.$$

Assim, $a'b' = ab + ah_2 + h_1b + h_1h_2$. Observe-se que $ah_2 \in H$ pois $f(ah_2) = f(a)f(h_2) = 0'$, onde $0'$ denota o elemento neutro de R'. Analogamente pode ser provado que $h_1b \in H$ e claramente $h_1h_2 \in H$. Assim, $a'b' \in ab + H$. Para mostrar que R/H é um anel resta provar que as propriedades associativa para a multiplicação e distributiva da multiplicação em relação à adição são verificadas (exercício).

Já se provou num teorema anterior que a aplicação μ está bem definida e é uma bijecção.

Resta provar que:

$$\mu[(a + H)(b + H)] = \mu(ab + H) = f(ab) = f(a)f(b) = \mu(a + H)\mu(b + H).$$

□

Observe-se que o teorema anterior está demonstrado para o caso em que $H = \mathrm{Nuc}(f)$.

Resta agora caracterizar os subanéis dum anel R para os quais a operação multiplicação definida no teorema anterior está bem definida.

Teorema 3.1.35. *Seja H um subanel dum anel R. A multiplicação de classes laterais de R em relação a H definida no teorema anterior está bem definida pela igualdade*

$$(a + H)(b + H) = (ab) + H,$$

se e só se $ah \in H$ e $hb \in H$ para quaisquer $a, b \in R$ e $h \in H$.

Demonstração. Suponha-se em primeiro lugar que $ah \in H$ e $hb \in H$ para quaisquer $a, b \in R$ e $h \in H$. Sejam $a' \in a+H$ e $b' \in b+H$. Tem-se $a'b' = ab+ah_2+h_1b+h_1h_2$. Ora por hipótese $ah_2, h_1b, h_1h_2 \in H$. Assim, $a'b' \in ab + H$. Reciprocamente, suponha-se que a multiplicação anterior está bem definida. Seja $a \in R$ e considere-se o produto das classes laterais

$$(a + H)H.$$

Seja $a \in a + H$ e $0 \in H$. Então

$$(a + H)H = a0 + H = 0 + H = H.$$

Por outro lado, para qualquer $h \in H$, $ah \in ah + H = (a + H)H = H$ e portanto $ah \in H$. Um argumento semelhante considerando o produto $H(b + H)$ mostra que $hb \in H$ para qualquer $h \in H$. □

3.1.7 Exercícios

1. Sejam A e B dois anéis.

1.1. Prove que o terno $(A \times B, +, .)$ é um anel com as operações definidas do seguinte modo, para todo o $(a, b), (a', b') \in A \times B$,

$$\begin{aligned} (a, b) + (a', b') &= (a + a', b + b') \\ (a, b).(a', b') &= (aa', bb'). \end{aligned}$$

Este anel designa-se por *anel produto*.

1.2. Estude em que condições o anel produto é comutativo e possui elemento identidade.

1.3. Se A e B são domínios de integridade, será que $A \times B$ é também um domínio de integridade?

1.4. Seja $A = \{0, 1\}$ um domínio de integridade com dois elementos e seja A^n o anel produto de n anéis A.

i. Determine todos os divisores de zero de A^n.

ii. Mostre que todo o elemento de A^n é idempotente.

2. Verifique se o conjunto indicado é um subanel do anel dado:

2.1. O conjunto dos reais da forma $a + b\sqrt{2}$, com $a, b \in \mathbb{N}$ em $(\mathbb{R}, +, .)$.

2.2. O conjunto dos complexos da forma $a + bi$, com $a, b \in \mathbb{Z}$ em $(\mathbb{C}, +, .)$.

3. Seja A um anel comutativo. Prove que:

3.1. Para cada elemento $a \in A$, a função

$$\begin{array}{rccc} \pi_a : & A & \to & A \\ & x & \longmapsto & \pi_a(x) = ax \end{array}$$

é um endomorfismo do grupo aditivo de A.

3.2. π_a é injectiva se e só se a não é um divisor de zero (suponha $a \neq 0$).

3.3. Se A tem elemento identidade então π_a é sobrejectiva se e só se a é invertível.

3.4. $B = \{\pi_a : a \in A\}$ munido com as operações

$$\begin{array}{rcl} (\pi_a + \pi_b)(x) & = & \pi_a(x) + \pi_b(x) \forall x \in A \\ \pi_a.\pi_b & = & \pi_a \circ \pi_b \end{array}$$

é um anel.

3.2 Ideais de um Anel

Na teoria de grupos mostrou-se que os subgrupos normais eram precisamente o tipo de subestrutura de grupos necessária para se obter um grupo cociente com uma operação bem definida. O último teorema da secção anterior mostra que em teoria de anéis uma subestrutura análoga deverá ser um subanel I dum anel R tal que $aI \subseteq I$ e $Ib \subseteq I$, para quaisquer $a, b \in R$. Observe-se que o anterior é equivalente a dizer que para todo $a \in R$ e $x \in I, ax \in I$ e $xa \in I$. Segue-se então a próxima definição.

Definição 3.2.1. *Seja R um anel e $I \subseteq R$, $I \neq \varnothing$. Diz-se que I é um ideal de R se e só se I é um subanel de R e, para todo $a \in R$ e $x \in I, ax \in I$ e $xa \in I$.*

Exemplo 3.2.2. *Se R é um anel, $\{0\}$ e R são ideais. A $\{0\}$ também se chama ideal nulo.*

Exemplo 3.2.3. *Para qualquer inteiro $n \in \mathbb{Z}$, o conjunto $n\mathbb{Z} = \{nz, z \in \mathbb{Z}\}$ é um ideal de $\mathbb{Z}$.*

Exemplo 3.2.4. *Seja $f : A \to B$ um homomorfismo de anéis. Então $Nuc(f)$ é um ideal de A.*

Demonstração. Prove-se apenas que para todo $a \in A$ e $x \in \text{Nuc}(f)$, $ax \in \text{Nuc}(f)$ e $xa \in \text{Nuc}(f)$. Para que $ax \in \text{Nuc}(f)$ dever-se-á ter $f(ax) = 0_B$. Mas $f(ax) = f(a)f(x)$, porque f é um homomorfismo de anéis. Mas $x \in \text{Nuc}(f)$. Então

$$f(ax) = f(a)f(x) = f(a)0_B = 0_B.$$

□

Exemplo 3.2.5. *No conjunto de todas as funções reais de variável real, $\mathcal{F}$, o subanel C formado todas as funções constantes não é um ideal de $\mathcal{F}$. De facto, o produto da função* $\sin x$ *pela função constante* 2 *é a função* $2\sin x$.

Teorema 3.2.6. *Seja I um ideal dum anel R. Então o conjunto $R/I = \{a + I, a \in R\}$ é um anel para as operações:*

$$(a + I) + (b + I) = (a + b) + I,$$

$$(a + I)(b + I) = (ab) + I.$$

Demonstração. Exercício. □

Definição 3.2.7. *Ao anel do teorema anterior chama-se anel cociente de R módulo I.*

Todo o anel R tem dois ideais $\{0\}$ e o próprio R. Esses ideais são chamados ideais impróprios ou triviais. O anel cociente R/R tem apenas um elemento e, $R/\{0\}$ é isomorfo a R. Os casos referidos não têm grande interesse para o nosso estudo assim, interessa-nos apenas os ideais I de R tal que $I \neq R$ e $I \neq \{0\}$.

Teorema 3.2.8. *Se R é um anel com identidade, e I é um ideal de R que contém a identidade, então $I = R$.*

Demonstração. Seja I um ideal de R e suponha-se que $1 \in I$. Claramente $I \subseteq R$. Seja $r \in R$. Então $r = r1$, mas $1 \in I$ logo $r \in I$. □

Teorema 3.2.9. *Nas condições do teorema anterior, se I contém uma unidade de R então $I = R$.*

Demonstração. Seja u uma unidade de R tal que $u \in I$. Então $1 = uu^{-1} \in I$. Pelo Teorema 3.2.8, $I = R$. □

Teorema 3.2.10. *Um corpo K não contém ideais próprios.*

Demonstração. Seja $I \neq \{0\}$ um ideal de K. Seja $x \in K$, tal que $x \neq 0$. Como K é um corpo, x é uma unidade de K. Pelo Teorema 3.2.9, $I = K$. □

Definição 3.2.11. *Um anel diz-se simples se não tem ideais próprios.*

Assim, o teorema anterior garante que um corpo é um anel simples.

3.2.1 Teorema Fundamental do Homomorfismo

Proposição 3.2.12. *Seja $f : R \to R'$ um homomorfismo de anéis e seja I um ideal de R. Então $f(R)$ é um ideal de $f(R)$. Mais, se I' é um ideal de R' ou de $f(R)$ então $f^{-1}(I')$ é um ideal de R.*

Demonstração. Exercício. □

Teorema 3.2.13. *Seja I um ideal dum anel R. Então $\gamma : R \to R/I$ dada por $\gamma(x) = x + I$ é um homomorfismo de anéis cujo núcleo é I.*

Demonstração. A parte aditiva já foi demonstrada anteriormente. Sejam então $x, y \in R$ tais que

$$\gamma(xy) = (xy) + I = (x + I)(y + I) = \gamma(x)\gamma(y).$$

□

Teorema 3.2.14. *(Teorema Fundamental do Homomorfismo) Seja $f : R \to R'$ um homomorfismo de anéis de núcleo I. Então R/I é isomorfo a $f(R)$*

Demonstração. Seja $f^\star : R/I \to f(R)$ dada por $f^\star(x + I) = f(x)$. A aplicação anterior é um isomorfismo de anéis. □

Exercício 3.2.15. *Seja A um anel comutativo com identidade e, para cada $a \in A$, seja o conjunto*

$$aA = \{ax : x \in A\}.$$

a. Defina ideal de A.

Resposta: Seja I um subconjunto não vazio de A. Diz-se que I é um ideal de A se I for um subanel de A e, se para qualquer $a \in A$ e $b \in I$ se tem $ab, ba \in I$. Note-se que, neste caso particular, como A é anel comutativo basta considerar $ab \in I$.

b. Mostre que aA é um ideal de A.

Resposta: Observe-se que $aA \neq \emptyset$, pois, $O_A = aO_A \in aA$, onde O_A representa o zero do anel A. $aA \subseteq A$. De facto, dado $y \in aA$, $y = ax$, $x \in A$. Mas, $a \in A$ e $x \in A$. Logo $y \in A$ porque $(A, .)$ é um grupóide.

Sejam agora $z, t \in aA$. Vamos ver que $z - t \in aA$ e $zt \in aA$. De facto,

$$z = ax, x \in A$$

e

$$t = ay, y \in A.$$

Tem-se então:

$$z - t = ax - ay = a(x - y),$$

pela distributividade válida no anel. Logo,

$$z - t = aw,$$

onde $w = x - y \in A$ porque $(A, +)$ é grupo.

Analogamente se mostra que $zt \in aA$. De facto,

$$zt = axay = a(xay) = ar,$$

onde $r = xay \in A$ porque $(A, .)$ é grupóide.

Provou-se que aA é um subanel de A, ou seja:

$$\forall z, t \in aA, z - t \in aA, zt \in aA.$$

Seja agora $k \in aA$ e $b \in A$. Tem-se

$$k = ax, x \in A.$$

Ora $bk = b(ax) = a(bx)$, uma vez que o anel A é comutativo. Note-se que também se usou a associatividade.

Assim, $bk = as$, onde $s = bx \in A$ pois $(A, .)$ é um grupóide e portanto $bk \in aA$. Observe-se que $bk = kb$ pois o anel A é comutativo. Assim, provou-se:

$$\forall b \in A, \forall k \in aA, bk \in aA \text{ e } kb \in aA.$$

c. $a \in aA$.

Resposta: Como A tem identidade $\mathbf{e}$, $a = a\mathbf{e}$. Logo $a \in aA$.

d. Se I é um ideal de A tal que $a \in I$, então $aA \subseteq I$.

Resposta: Seja $y \in aA$. Tem-se $y = ax, x \in A$. Mas $a \in I$ e, como I é ideal, $y = ax \in I$. Logo, provou-se a inclusão dos conjuntos.

Viu-se atrás que um anel sem identidade se pode estender a um anel com identidade. Coloca-se a seguinte questão:

Será que é possível fazer uma extensão de um domínio por forma a que nessa extensão todos os elementos não nulos tenham inverso?

Se o domínio for finito viu-se que este é corpo. Assim, no caso finito a resposta é afirmativa, o próprio domínio em consideração é um corpo. Ora, mesmo no caso infinito a resposta é afirmativa. Apresenta-se então o corpo dos cocientes.

Teorema 3.2.16. *Seja D um domíno de integridade. Então existe um corpo Q que contém um subdomínio Q' isomorfo a D.*

Demonstração. Considere-se o produto cartesiano $D \times D\backslash\{0\}$. e, defina-se nesse conjunto a seguinte relação de equivalência:

$\forall\ (a,b),(c,d) \in D \times D\backslash\{0\}$,

$$(a,b)R(c,d) \Leftrightarrow ad = bc.$$

Verifica-se facilmente que R é uma relação de equivalência.

Considere-se o conjunto cociente $(D \times D\backslash\{0\})/R$ e, designe-se para todo $(a,b) \in D \times D\backslash\{0\}$, $[(a,b)]_R$ por $\frac{a}{b}$, ou seja,

$$\frac{a}{b} = \{(x,y) \in D \times D\backslash\{0\} : (a,b)R(x,y)\},$$

$$\frac{a}{b} = \{(x,y) \in D \times D\backslash\{0\} : ay = bx\}.$$

Defina-se em $(D \times D\backslash\{0\})/R$ as operações:

$\forall \frac{a}{b}, \frac{c}{d} \in (D \times D\backslash\{0\})/R$,

$$\frac{a}{b} + \frac{c}{d} = \frac{ad+bc}{bd}$$

$$\frac{a}{b} \cdot \frac{c}{d} = \frac{ac}{bd}.$$

Prove-se apenas a consistência da operação $+$. De facto, sejam $\frac{a}{b}, \frac{c}{d} \in (D \times D\backslash\{0\})/R$ elementos arbitrários, se

$$\frac{a}{b}=\frac{a'}{b'}\wedge\frac{c}{d}=\frac{c'}{d'}\Longrightarrow\frac{a}{b}+\frac{c}{d}=\frac{a'}{b'}+\frac{c'}{d'},$$

ora, o anterior ainda é equivalente a:

$$\frac{a}{b}=\frac{a'}{b'}\wedge\frac{c}{d}=\frac{c'}{d'}\Longrightarrow\frac{ad+bc}{bd}=\frac{a'd'+b'c'}{b'd'},$$

que por sua vez ainda é equivalente a provar que:

$$(a,b)R(a',b')\wedge(c,d)R(c',d')\Longrightarrow(ad+bc,bd)R(a'd'+b'c',b'd').$$

Ora,

$$(ad+bc,bd)R(a'd'+b'c',b'd')\Longleftrightarrow(ad+bc)b'd'=bd(a'd'+b'c').$$

Assim,

$$\begin{aligned}(ad+bc)b'd' &= (ad)b'd'+(bc)b'd', \text{ pela distributividade}\\ &= (ab')dd'+(cd')bb', \text{ pela comutatividade e associtividade de } \cdot,\\ &= ba'dd'+dc'bb', \text{ por hipótese},\\ &= bd(a'd'+b'c'), \text{ pela distributividade.}\end{aligned}$$

Designe-se por $Q=(D\times D\backslash\{0\})/R$ munido das operações $+$ e $\cdot$ definidas anteriormente.

A estrutura $(Q,+,\cdot)$ é um corpo (Prove!) onde $\frac{0}{1}$, é o seu zero e identidade $1=\frac{1}{1}$. Note-se ainda que $-\frac{a}{b}=\frac{-a}{b}$, para qualquer $\frac{a}{b}\in Q$ e, para qualquer $\frac{a}{b}\in Q\backslash\{0\},(\frac{a}{b}\ )^{-1}=\frac{b}{a}$. Para terminar a demonstração considere-se agora que o conjunto

$$Q'=\{\frac{a}{1},a\in D\}.$$

O conjunto anterior é um domínio de integridade (justifique!). Por outro lado a aplicação

$$\begin{aligned}f:D &\rightarrow Q'\\ a &\rightarrow f(a)=\tfrac{a}{1}\end{aligned}$$

é um isomorfismo entre os anéis indicados.

Claramente é sobrejectiva, pois

$$\begin{aligned}f(D) &= \{f(x),x\in D\}, \text{ por definição de conjunto imagem},\\ &= \{\tfrac{a}{1},a\in D\}, \text{ por definição de } f.\end{aligned}$$

Mais, para quaisquer $a,a'\in D$,

$$f(a+a')=\frac{a+a'}{1}=\frac{a}{1}+\frac{a'}{1}=f(a)+f(a'),$$

$$f(aa') = \frac{aa'}{1} = \frac{a}{1}\frac{a'}{1} = f(a)f(a'),$$

por definição de soma e produto em Q' e por definição de f. □

O corpo Q acabado de construir é conhecido por corpo das fracções de D ou corpo dos cocientes de D.

Exemplo 3.2.17. *Se o domínio anterior for o domínio $\mathbb{Z}$, o corpo das fracções de $\mathbb{Z}$ é o corpo $\mathbb{Q}$ dos números racionais.*

Retome-se agora a definição de ideal.

3.2.2 Ideal Gerado por um Conjunto. Ideal Principal

Sejam R um anel e Mum subconjunto arbitrário de R.

Definição 3.2.18. *Chama-se ideal gerado por M à intersecção de todos os ideais que contêm M e denota-se por $< M >$.*

Note-se que existem sempre ideais que contêm M, por exemplo o próprio R. O ideal $< M >$ é o mais "pequeno" ideal que contém M, ou seja, se existir um ideal I de R tal que $M \subseteq I$ então $< M > \subseteq I$. Convenciona-se que $< \varnothing >= \{0\}$. Se $M = \{x_1, x_2, \ldots, x_n\}$, o ideal gerado por M representa-se por $< x_1, x_2, \ldots, x_n >$.

Definição 3.2.19. *Chama-se ideal principal de R a um ideal gerado por um só elemento e denota-se por $< x >$, onde $x \in R$.*

3.2.3 Estrutura de um Ideal Principal

Considere-se $< x >$, onde $x \in R$. Como $< x >$ é um ideal, da definição resulta que $< x >$ é um grupo aditivo e que $x \in < x >$. Assim, $nx \in < x >$, com $n \in \mathbb{Z}$. Recorde-se que $nx = x + \cdots + x$, com n parcelas, $0x = 0$ e $(-n)x = -(x + \cdots + x)$. Como $< x >$ é fechado para a multiplicação definida em R,

$$xx \cdots x = x^m \in < x >, \forall m \in \mathbb{Z}^+.$$

Pertencem ainda a $< x >$ todos os elementos da forma,

$$rx, xs \text{ e } pxq,$$

para quaisquer $r, s, q \in R$. A soma dos elementos referidos pertencem igualmente a $< x >$. Assim pode dizer-se que pertencem a $< x >$ todos os elementos da forma:

$$nx + x^m + rx + xs + pxq, \tag{3.1}$$

com $n \in \mathbb{Z}, m \in \mathbb{Z}^+$, $p, q \in R$. Analisando com um pouco mais de atenção 3.1 pode observar-se que a parcela x^m pode ser suprimida.

De facto,

$$\text{se } m = 1, nx + x = (n+1)x, \tag{ B}$$

$$\text{se } m \geq 2, x^m = x^{m-1}x,$$

$$rx + x^m = (r + x^{m-1})x = r'x \tag{C}$$

com $r' = r + x^{m-1} \in R$. A estrutura básica dos elementos de $< x >$ é pois,

$$nx + rx + xs + pxq, \tag{ D}$$

Claro que são igualmente elementos de $< x >$ os elementos da forma

$$nx + rx + xs + \sum_{i=1}^{t} p_i x q_i \tag{E}$$

com $n \in \mathbb{Z}, r, s, p_i, q_i \in R$, $t \geq 1$ e onde o somatório que aparece na expressão tem um número finito de termos.

Resolva agora os seguintes exercícios:

- Mostre que o conjunto $T = \{nx + rx + xs + \sum_{i=1}^{t} p_i x q_i,\ n \in \mathbb{Z}, r, s, p_i, q_i \in R,\ t \geq 1\}$, é um ideal e que é exactamente igual a $< x >$.
- Mostre que se R é comutativo então a estrutura dos elementos de $< x >$ reduz-se a $nx + r'x, n \in \mathbb{Z}, r' \in R$.
- Mostre que se R é comutativo com identidade então a estrutura dos elementos de $< x >$ reduz-se a $ax, a \in R$.

Se R é um anel comutativo com identidade denota-se $< x >$ por Rx. No entanto, se R é apenas comutativo $Rx = \{rx, r \in R\}$ é um ideal de R mas não podemos garantir que seja $< x >$, para tal, basta que não exista nenhum elemento $u \in R$, tal que $xu = x$.

Exemplo 3.2.20. *Seja $R = 2\mathbb{Z}$ munido com as operações usuais de adição e multiplicação de inteiros. O conjunto $2\mathbb{Z}$ é um anel comutativo sem identidade. Para $x = 4$,*

$$< 4 >= \{n4 + r4, n \in \mathbb{Z}, r \in R\}$$

e,

$$R4 = \{r4, r \in R\} = \{0, \pm 8, \pm 16, \dots\} = 8\mathbb{Z}.$$

Tem-se $< 4 > \neq R4$. Ir-se-á mostrar agora que todo o ideal de $\mathbb{Z}$ é principal.

é sabido que os múltiplos de um inteiro p constituem um ideal de $\mathbb{Z}$. Ir-se-á mostrar que todo o ideal de $\mathbb{Z}$ é gerado por algum inteiro p.

Teorema 3.2.21. *Todo o ideal de $\mathbb{Z}$ é principal.*

Demonstração. Seja J um ideal de $\mathbb{Z}$. Ir-se-á mostrar $J =< p >$, para algum $p \in \mathbb{Z}$. Se $J = \{0\}$, ou $J = \mathbb{Z}$, o resultado é imediato (tem-se respectivamente $p = 0$ e $p = 1$). Suponha-se que $J \neq \{0\}$ e $J \neq \mathbb{Z}$. Então existe $x \in J$, tal $x \neq 0$. Se $x \in J$ então, também $-x \in J$ e, ou $x \in \mathbb{Z}^+$ou $-x \in \mathbb{Z}^+$. Assim, pertence a J pelo menos um elemento de $\mathbb{Z}$ que é inteiro positivo. Seja

$$n = \min\{x \in \mathbb{Z}^+ : x \in J\}.$$

Prove-se que $J = n\mathbb{Z}$. Da definição de ideal resulta imediatamente que $n\mathbb{Z} \subseteq J$. Suponha-se que a inclusão contrária não é verificada. Isto é, existe $a \in J$ tal que a não é múltiplo de n. Então existem $q, r \in \mathbb{Z}$, com $0 < r < n$ tais que $a = nq + r$. Como $a, nq \in J$ e $r = a - nq$, então $r \in J$, o que é absurdo, uma vez que $0 < r < n$. □

3.2.4 Ideais Primos e Ideais Maximais

Seja R um anel. Então R contém dois ideais, o ideal impróprio R e o ideal trivial $\{0\}$. Para estes ideais, os aneis cociente são R/R e $R/\{0\}$, respectivamente. O primeiro tem apenas um elemento e $R/\{0\}$ é isomorfo a R.

Teorema 3.2.22. *Se R é um anel com identidade e N é um ideal de R tal que $1 \in N$, então $N = R$.*

Demonstração. Seja N um ideal de R, e suponha-se que $u \in N$ para alguma unidade $u \in R$. Então da condição $rN \subseteq N$, para todo $r \in R$ tem-se que $1 = u^{-1}u \in N$. Mas, então a condição $rN \subseteq N$, para todo $r \in R$ implica que $r1 = r \in N$, para todo $r \in R$ e portanto $N = R$. □

Corolário 3.2.23. *Um corpo F não contém ideais próprios não triviais.*

Demonstração. Como qualquer elemento não nulo de um corpo é uma unidade, pelo Teorema 3.2.22, um ideal dum corpo só poderá ser $\{0\}$ ou F. □

Averigue-se seguidamente quando é que um anel cociente é um corpo ou apenas um domínio de integridade.

Definição 3.2.24. *(Ideal Maximal) Um ideal maximal dum anel R é um ideal M diferente de R e não existe nenhum ideal próprio N de R que contenha M propriamente.*

Teorema 3.2.25. *Seja R um anel comutativo com identidade. Então M é um ideal maximal de R se e só se R/M é um corpo.*

Demonstração. Suponha-se que M é um ideal maximal de R. Observe-se que se R é um anel comutativo com identidade, então R/M é também um anel comutativo com identidade se $M \neq R$, o que resulta da definição de ideal maximal. Seja

$$(a + M) \in R/M,$$

com $a \notin M$. Ir-se-á mostrar que $a + M$ tem um inverso multiplicativo em R/M. Seja

$$N = \{ra + m | r \in R, m \in M\}.$$

Então, $(N, +)$ é um grupo para a operação

$$(r_1a + m_1) + (r_2a + m_2) = (r_1 + r_2)a + (m_1 + m_2).$$

De facto, o resultado da operação pertence a N,

$$0 = 0a + 0,$$

$$-(ra + m) = (-r)a + (-m).$$

Considere-se agora

$$r_1(ra + m) = (r_1r)a + r_1m.$$

Claramente

$$r_1(ra + m) \in N,$$

para $r_1 \in R$ e, como R é um anel comutativo,

$$(ra + m)r_1 \in N.$$

Assim, N é um ideal. Mas,

$$a = 1a + 0,$$

o que mostra que $a \in N$, e para $m \in M$,

$$m = 0a + 0,$$

e portanto $M \subseteq N$. Assim, N é um ideal de R que contém M propriamente, uma vez que $a \in N$ e $a \notin M$. Como M é maximal dever-se-á ter $N = R$. Em particular $1 \in N$. Então, por definição de N, existe $b \in R$ e $m \in M$ tal que $1 = ba + m$. Assim,

$$1 + M = ba + M = (b + M)(a + M),$$

e portanto, $b + M$ é o inverso multiplicativo de $a + M$. Reciprocamente, suponha-se que R/M é um corpo. Observe-se que se N é um ideal qualquer de R tal que $M \subset N \subset R$ e γ é o homomorfismo canónico de R em R/M, então $\gamma(N)$ é um ideal de R/M e $\{(0 + M)\} \subset \gamma(N) \subset R/M$. Mas, pelo Corolário 3.2.23, um corpo não contém ideais próprios não triviais. Assim, se R/M é um corpo, M é maximal. □

Corolário 3.2.26. *Um anel comutativo com identidade é um corpo se e só se não tem ideais próprios não triviais.*

Demonstração. Pelo Corolário 3.2.23 diz-nos que um corpo não contém ideais próprios não triviais. Reciprocamente, se um anel comutativo R com identidade não tem ideais próprios não triviais então $\{0\}$ é um ideal maximal e $R/\{0\}$, que é isomorfo a R, é um corpo pelo Teorema 3.2.25. □

Definição 3.2.27. *Seja R um anel comutativo. Um ideal $N \neq R$ de R é um ideal primo se para $a, b \in R$ sempre que $ab \in N$ então $a \in N$ ou $b \in N$.*

Exemplo 3.2.28. *Observe-se que $\mathbb{Z} \times \{0\}$ é um ideal primo de $\mathbb{Z} \times \mathbb{Z}$. De facto, para $(a, b), (c, d) \in \mathbb{Z} \times \mathbb{Z}$ tais que $(a, b)(c, d) \in \mathbb{Z} \times \{0\}$ então $bd \in \mathbb{Z}$. Assim, $b \in \mathbb{Z}$ e portanto $(a, b) \in \mathbb{Z} \times \{0\}$ ou $d \in \mathbb{Z}$ e $(c, d) \in \mathbb{Z} \times \{0\}$.*

Teorema 3.2.29. *Seja R um anel comutativo com identidade e seja $N \neq R$ um ideal de R. Então R/N é um domínio de integridade se e só se N é um ideal primo de R.*

Corolário 3.2.30. *Todo o ideal maximal num anel comutativo R com identidade é um ideal primo.*

Demonstração. Se M é maximal em R, então R/M é um corpo e portanto um domínio de integridade. Assim, pelo Teorema 3.2.29, M é um ideal primo. □

3.2.5 Exercícios

1. Seja A um anel comutativo e $a \in A$.

1.1. Mostre que o conjunto

$$I_a = \{x \in A : xa = 0\}$$

é um ideal de A. Diga em que condições se tem $I_a \neq \{0\}$.

1.2. Seja P uma parte de A. Mostre que $J(P) = \{x \in A : \forall a \in P, xa = 0\}$ é um ideal de A e que

$$J(P) = \bigcap_{a \in P} I_a.$$

Diga em que condições se tem $J(P) \neq \{0\}$.

2. Seja A o seguinte conjunto de matrizes:

$$A = \left\{ \begin{bmatrix} a & b \\ b & a \end{bmatrix} : a, b \in \mathbb{Z} \right\}.$$

2.1. Mostre que $(A, +, \times)$ é um anel para as operações de adição e multiplicação usuais de matrizes.

2.2. Averigue se o anel é comutativo e se tem elemento identidade.

2.3. Determine o conjunto das unidades de A e o conjunto dos divisores de zero.

2.4. Considere as aplicações

$$\begin{array}{rccc} \sigma: & A & \to & \mathbb{Z} \\ & \begin{bmatrix} a & b \\ b & a \end{bmatrix} & \longmapsto & a+b \end{array}$$

$$\begin{array}{rccc} \nu: & A & \to & \mathbb{Z} \\ & \begin{bmatrix} a & b \\ b & a \end{bmatrix} & \longmapsto & a-b \end{array}$$

i. Mostre que σ e ν são homomorfismos de anéis. Determine $\ker\sigma, \ker\nu$, $\sigma(A)$ e $\nu(A)$.

ii. Seja p um inteiro e J_p o conjunto das matrizes $M \in A$ tais que $\sigma(M)$ é divisível por p. Mostre que J_p é um ideal de A e que $J_p \supset \ker\sigma$.

3. Seja $f : A \to A'$ um homomorfismo de anéis. Prove que a imagem recíproca por f de um ideal de A' é um ideal de A.

4. Seja

$$\begin{array}{rccc} \phi: & \mathcal{F}(\mathbb{R}) & \to & \mathbb{R}\times\mathbb{R} \\ & f & \longmapsto & (f(0), f(1)) \end{array}$$

onde $\mathcal{F}(\mathbb{R})$ é o conjunto das funções reais de variável real.

4.1. Prove que ϕ é um epimorfismo de anéis.

4.2. Justifique que o conjunto das funções reais de variável real cujo gráfico passa pelos pontos $(0,0)$ e $(1,0)$ é um ideal de $\mathcal{F}(\mathbb{R})$.

5. Seja A um anel comutativo tal que, para todo $a \in A, 2a = 0$.

5.1. Mostre que, para todos $x, y \in A$, $(x+y)^2 = x^2 + y^2$.

5.2. Conclua que a função $h : A \longrightarrow A$, $x \longrightarrow x^2$, é um endomorfismo de A.

5.3. Sejam $J = \{x \in A | x^2 = 0\}$ e $B = \{x^2 | x \in A\}$. Mostre que:

i. J é um ideal de A.

ii. B é um subanel. de A.

6. Seja I um ideal de A. Chama-se radical de I ao conjunto $\sqrt{I} = \{a \in A | a^n \in I$, para algum $n \in \mathbb{N}\}$. Se A é comutativo, mostre que:

6.1. $\sqrt{I}$ é um ideal de A que contém I.

6.2. Se $I \subset J$, então $\sqrt{I} \subset \sqrt{J}$.

6.3. $\sqrt{\sqrt{I}} = \sqrt{I}$.

7. Sejam I, J ideais de A. Mostre que se $I \cap J = \{0\}$, então $ij = 0$ para todos $i \in I$ e $j \in J$.

8. Se já A um anel. Prove que:

8.1. Para todo $a \in A$, as funções $\epsilon_a : A \longrightarrow A, x \longrightarrow ax$, e $\delta_a : A \longrightarrow A, x \longrightarrow xa$, são endomorfismos do grupo aditivo de A.

8.2. Se $a \neq 0$, então ϵ_a é injectiva se e só se a não é um divisor de zero à esquerda.

8.3. Se $a \neq 0$, então δ_a é injectiva se e só se a não é um divisor de zero à direita.

8.4. Se A é anel comutativo com identidade, então $\epsilon_a = \delta_a$ é sobrejectiva se e só se a é invertível.

8.5. Sejam $E = \{\ \epsilon_a : a \in A\}$ e $D = \{\delta_a : a \in A\}$. Mostre que E e D são anéis para a adição $\phi + \psi$ definida por $(\phi + \psi)(x) = \phi(x) + \psi(x)$ e para a multiplicação $\phi.\psi = \psi \diamond \phi = \psi(\phi(x))$.

3.3 Anel de Polinómios sobre Anéis Comutativos com Identidade

Nesta secção far-se-á um estudo sobre anéis de polinómios numa indeterminada analisando conceitos e resultados tais como a divisibilidade e a factorização. Começar-se-á por apresentar uma definição formal de polinómio numa indeterminada.

Definição 3.3.1. *Seja R um anel. Uma sucessão $p = (a_i)_{i\in\mathbb{N}_0}$ de elementos de R tal que $a_i = 0$ a partir de certa ordem $m \in \mathbb{N}_0$, diz-se um polinómio.*

Se $p = (a_i)_{i\in\mathbb{N}_0}$ e $a_i = 0$, para todo $i \in \mathbb{N}_0$, escreve-se $p = 0$. Pode-se escrever $\left(\ a_1,\quad a_2,\quad a_3,\quad \ldots\ \right)$ em vez de $(a_i)_{i\in\mathbb{N}_0}$. Dois polinómios $(a_i)_{i\in\mathbb{N}_0}$ e $(b_i)_{i\in\mathbb{N}_0}$ dizem-se iguais se e só se, para todo $i \in \mathbb{N}_0$, $a_i = b_i$.

Definição 3.3.2. *Dado um polinómio $p \neq 0$, chama-se grau de p ao maior $m \in \mathbb{N}_0$ tal que $a_m \neq 0$.*

Se $p = 0$ define-se grau de p como sendo $-\infty$. Um polinómio $\left(\ a,\quad 0,\quad 0,\quad \ldots\ \right)$ diz-se uma constante e representa-se por a. No conjunto $P(R)$ de todos os polinómios em R, define-se as seguintes operações de adição e multiplicação:

para todos $p = (a_i)_{i\in\mathbb{N}_0}$ e $q = (b_i)_{i\in\mathbb{N}_0}$,

$$p + q = (a_i + b_i)_{i\in\mathbb{N}_0}$$

$$pq = (c_i)_{i\in\mathbb{N}_0}$$

onde

$$c_i = \sum_{j+k=i} a_j b_k.$$

Proposição 3.3.3. *Seja R um anel (comutativo com identidade). Então $P(R)$ é um anel (comutativo com identidade) e $\Phi : R \to P(R)$ definida por $\Phi(a) = \left(\begin{array}{cccc} a, & 0, & 0, & \dots \end{array} \right)$, para todo $a \in R$ é uma bijecção de anéis.*

Demonstração. Note-se que o simétrico do polinómio $\left(\begin{array}{cccc} a_1, & a_2, & a_3, & \dots \end{array} \right)$ é o polinómio $\left(\begin{array}{cccc} -a_1, & -a_2, & -a_3, & \dots \end{array} \right)$ e $p = 0$ é o zero do anel $P(R)$. O resto da demonstração fica ao cuidado do leitor. □

Seja A um anel com identidade. considere-se $x = \left(\begin{array}{ccccccc} 0, & 1, & 0, & \dots, & 0, & \dots \end{array} \right)$. Pode-se provar facilmente que, para todo $n \in \mathbb{N}$,

$$x^n = \left(\begin{array}{ccccccc} 0, & 0, & \dots, & 0, & 1, & 0, & \dots \end{array} \right).$$

Defina-se $1 = \left(\begin{array}{cccc} 1, & 0, & 0, & \dots \end{array} \right)$ a identidade de $P(R)$, pode-se verificar que dado $p = \left(\begin{array}{ccccccc} a_0, & a_1, & \dots, & a_n, & 0, & 0, & \dots \end{array} \right)$,

$$p = a_0 + a_1 x + a_2 x^2 + \cdots + a_n x^n = a_n x^n + \cdots + a_1 x + a_0.$$

O polinómio x (de grau 1) chama-se *indeterminada* sobre R. Com esta notação, o polinómio p poderá denotar-se por $p(x)$. Usar-se-á as duas notações sempre que isso for necessário.

Um elemento $p(x) = a_0 + a_1 x + a_2 x^2 + \cdots + a_n x^n$ de $P(R)$ diz-se um polinómio na indeterminada x com coeficientes em R. Se $p(x)$ tem grau $n \geq 0$, ao coeficiente a_n chama-se coeficiente director de $p(x)$. Um polinómio diz-se mónico se o seu coeficiente director é 1. Representa-se o anel $P(R)$, sendo R um anel comutativo com identidade, por $R[x]$.

Exemplo 3.3.4. *Seja $R = \mathbb{Z}$ e $p = \left(\begin{array}{cccccccc} 2, & -3, & 0, & 5, & 0, & 0, & \dots \end{array} \right)$. Então*

$$\begin{aligned} p &= \left(\begin{array}{cccc} 2, & 0, & 0, & \dots \end{array} \right) + \left(\begin{array}{cccc} 0, & -3, & 0, & 0, & \dots \end{array} \right) + \left(\begin{array}{cccccc} 0, & 0, & 0, & 5, & 0, & \dots \end{array} \right) \\ &= 2 - 3x + 5x^3. \end{aligned}$$

Note-se que $R[x]$ não é corpo, mesmo se R for corpo. De facto, neste caso, os únicos elementos invertíveis de $R[x]$ são os polinómios constantes $\left(\begin{array}{cccc} a, & 0, & 0, & \dots \end{array} \right)$, como $a \neq 0$. No que se segue R será sempre um anel comutativo com identidade.

Definição 3.3.5. *Sejam R um anel comutativo com identidade e $p(x) = a_0 + a_1x + a_2x^2 + \cdots + a_nx^n$ um polinómio com coeficientes em R. à aplicação f_p,*

$$\begin{array}{rccl} f_p: & R & \to & R \\ & c & \to & a_0 + a_1c + a_2c^2 + \cdots + a_nc^n \end{array}$$

chama-se função polinomial definida por p. Para $c \in R$ escreve-se $p(c)$ em vez de $f_p(c)$.

Note-se que se $p(x) = c$ é constante, então a função polinomial

$$\begin{array}{rccl} f_p: & R & \to & R \\ & a & \to & p(a) = c \end{array}$$

é constante. Em particular, se $p(x) = 1$, então $p(a) = 1$, para todo $a \in R$. Note-se ainda que dados um anel R e polinómios $p(x)$, $q(x) \in R[x]$, podemos ter $p(x) \neq q(x)$ e $f_p = f_q$. De facto, veja-se o exemplo:

Exemplo 3.3.6. *Sejam $A = \mathbb{Z}_2$, $p(x) = 1 + x$ e $q(x) = 1 + x^3$. Logo $p \neq q$, mas*

$$\begin{array}{rccl} f_p: & \mathbb{Z}_2 & \to & \mathbb{Z}_2 \\ & 0 & \to & 1 \\ & 1 & \to & 0 \end{array} \quad e \quad \begin{array}{rccl} f_q: & \mathbb{Z}_2 & \to & \mathbb{Z}_2 \\ & 0 & \to & 1 \\ & 1 & \to & 0 \end{array}$$

donde $f_p = f_q$.

é importante não confundir o conjunto $R[x]$ de todos os polinómios com coeficientes num anel R com o conjunto de todas as funções polinomiais. Note-se que a natureza dos seus elementos

é diferente.

Segue-se agora a definição de raíz de um polinómio.

Definição 3.3.7. *Sejam R um anel comutativo com identidade e $p(x) \in R[x]$. Um elemento $\alpha \in R$ diz-se raíz do polinómio p se $p(\alpha) = 0$, isto é, α é um zero da função polinomial* $f_p: \quad R \quad \to \quad R$.

Teorema 3.3.8. *Seja R um anel comutativo com identidade. Se $a \in R$, a aplicação de substituição*

$$\begin{array}{rccl} \epsilon_a: & R[x] & \to & R \\ & p(x) & \to & p(a) \end{array}$$

é um homomorfismo de anéis com identidade.

Demonstração. A demonstração é deixada ao cuidado do aluno. □

Mais, chama-se a atenção que é útil que o anel dos coeficientes seja comutativo com identidade. Viu-se que a identidade é necessária para definir o elemento x. Quanto ao papel da comutatividade, ela permite definir o homomorfismo de substituição para qualquer elemento de R. Como exemplo, suponha-se que R não era comutativo, e tomem-se dois elementos $a, b \in R$, e considere-se o polinómio

$$(x-a)(x-b) = x^2 - (a+b)x + ab.$$

Se agora substituirmos x por a, viria, na igualdade anterior, $0 = ab - ba$. é por causa deste tipo de problemas que, em anéis não comutativos, só se define homomorfismo de substituição para elementos do centro do anel, isto é, para elementos que comutem com todos os elementos de R.

Teorema 3.3.9. *Seja R um anel comutativo com identidade. Então $R[x]$ é um anel comutativo com identidade. Se R é domínio de integridade então $R[x]$ também o é.*

Demonstração. Demonstre-se apenas que se R não tem divisores de zero então $R[x]$ também não tem. Suponha-se então que R é um domínio de integridade. Sejam $p(x) = a_n x^n + \cdots + a_1 x + a_0 \neq 0$ e $q(x) = b_m x^m + b_{m-1} x^{m-1} + \cdots + b_1 x + b_0 \neq 0$, com *grau* $p(x) = n$ e *grau* $q(x) = m$. Então $a_n, b_m \neq 0$ e

$$p(x)q(x) = a_n b_m x^{n+m} + \cdots + (a_0 b_1 + a_1 b_0)x + a_0 b_0.$$

Como R não tem divisores de zero , obtém-se $a_n b_m \neq 0$ e, portanto, $p(x)q(x) \neq 0$. Logo $R[x]$ não tem divisores de zero. □

Corolário 3.3.10. *Se R é um domínio de integridade e $p(x), q(x) \in R[x]\backslash\{0\}$ têm grau n e m respectivamente, então $p(x)q(x)$ tem grau $n+m$.*

De um modo geral, se R é um anel arbitrário, dados $p(x)$, $q(x) \in R[x]$ tem-se

$$grau\ (p(x)+q(x)) \leq \max\{grau\ p(x), grau\ q(x)\},$$

$$grau\ (p(x)q(x)) \leq grau\ p(x) + grau\ q(x).$$

Recorde-se que o grau do polinómio nulo foi definido com sendo $-\infty$, assim, o corolário anterior faz sentido mesmo quando p ou q são polinómios nulos.

3.3.1 Divisibilidade

Nesta subsecção vamos demonstrar que no anel dos polinómios com coeficientes num corpo é válido um algoritmo de divisão muito semelhante ao que é válido nos inteiros.

Lema 3.3.11. *Sejam $f, g \in R[x], f, g \neq 0$. Se o coeficiente director de f, ou o de g, for uma unidade, então $fg \neq 0$ e $grau\ (fg) = grau\ (f) + grau(g)$.*

Teorema 3.3.12. *Sejam R um anel e $f, g \in R[x]$. Suponha-se que $f \neq 0$ e que o coeficiente director de f é uma unidade de R. Então existem $q, r \in R[x]$, univocamente definidos, tais que*

$$g = qf + r \text{ e } grau\ r < grau\ f.$$

Demonstração. Se $grau\ g < grau\ f$, então $g = 0f + g$ é uma decomposição nas condições pretendidas. Senão, tome-se $m = grau\ g \geq n = grauf$ e usa-se agora indução em m. Seja $f(x) = ux^n + ax^{n-1} + \cdots$, e $g(x) = bx^m + cx^{m-1} + \cdots$ onde u é uma unidade, por hipótese, e $b \neq 0$. Considere-se então o polinómio

$$bu^{-1}x^{m-n}f$$

o múltiplo de f que subtraído a g lhe fará diminuir o grau. Temos então,

$$\begin{aligned} g_1 &= g - bu^{-1}x^{m-n}f \\ &= (bx^m + cx^{m-1} + \cdots) - bu^{-1}x^{m-n}(ux^n + ax^{n-1} + \cdots) \\ &= 0x^m + (c - bu^{-1}a)x^{m-1} + \cdots \end{aligned}$$

Tem-se então que $grau\ g_1 < grau\ g$, portanto, por indução, existem q_1 e r tais que $g_1 = q_1 f + r$, com $grau\ r < grau\ f$. Assim,

$$g = g_1 + bu^{-1}x^{m-n}f = (q_1 + bu^{-1}x^{m-n})f + r.$$

Pondo $q = q_1 + bu^{-1}x^{m-n}$ tem-se a existência da decomposição nas condições pretendidas. Resta ver a unicidade. Suponha-se então que

$$g = q'f + r' \text{e } grau\ r' < grau\ f.$$

Então $r - r' = (q' - q)f$. Se $q' - q \neq 0$, então como o coeficiente director de f é uma unidade, $(q' - q)f \neq 0$ pelo lema anterior, e

$$grau\ (r - r') = grau\ [(q' - q)f] = grau\ (q' - q) + grau\ f,$$

donde $grau\ (r - r') \geq grau\ (q - q') + grau\ f$, o que é falso. Assim, $q = q'$ e portanto $r - r' = (q' - q)f = 0$ e $r = r'$. □

Apresenta-se ainda o Teorema do Resto:

Teorema 3.3.13. *Seja R um anel comutativo com identidade. Se $f(x) \in R[x]$ e $a \in R$, então o resto da divisão de $f(x)$ pelo polinómio $x - a$ é $f(a)$.*

Demonstração. Usa-se o algoritmo da divisão em $R[x]$ para dividir f por $x - a$. Repare-se que o coeficiente director de $x - a$ é uma unidade. Tem-se

$$f(x) = q(x)(x - a) + r(x),$$

com $grau\ r < 1 = grau\ (x - a)$, ou seja, r é uma constante. Substituindo a em ambos os polinómios, obtém-se $f(a) = r$, que era o pretendido. □

Como consequência tem-se:

Corolário 3.3.14. *Se R é um anel comutativo com identidade, $f(x) \in R[x]$ e $a \in R$, então $x - a$ divide $f(x)$ se e só se $f(a) = 0$.*

Corolário 3.3.15. *Sejam R um domínio de integridade e $f(x) \in R[x]\backslash\{0\}$ de grau n. Então $f(x)$ tem no máximo n raízes distintas.*

3.4 Domínios de Ideais Principais e Domínios de Factorização única

Nesta secção ir-se-á provar que todo o domínio de ideais principais é um domínio de factorização única.

Definição 3.4.1. *(Domínio de Integridade) Um domínio de integridade D é um anel comutativo com identidade $(1 \neq 0)$ e sem divisores de zero.*

Num domínio de integridade é válida a seguinte proposição:

Proposição 3.4.2. *Sejam D um domínio de integridade e $a, b, c \in D$, com $a \neq 0$. Então:*

(*i*) *Se $ab = ac$, então $b = c$.*

(*ii*) *Se $ba = ca$, então $b = c$.*

Seja então $D^\star = D\backslash\{0\}$, e U_D o conjunto das unidades de D. Se $a, b \in D$ e a é factor de b, isto é $b = ad$, para algum $d \in D$, escreve-se $a|b$. Se $a_1, \ldots, a_n \in D$, $(a_1, \ldots, a_n)$ representa o ideal gerado por $\{a_1, \ldots, a_n\}$.

Definição 3.4.3. *(elementos associados) Sejam D um domínio de integridade e $a, b \in D$. Diz-se que a e b são associados se e só se existe $u \in U_D$ tal que $a = ub$.*

Definição 3.4.4. *(Domínio de Ideais Principais) Um domínio D é um domínio de ideais principais se e só se todos os ideais de D são principais.*

Definição 3.4.5. *(Cadeia Ascendente de Ideais) Sejam R um anel, $J \subseteq \mathbb{N}$ e $\{I_j : j \in J\}$ um conjunto de ideais de R. Diz-se que $\{I_j : j \in J\}$ é uma cadeia ascendente de ideais de R se e só se para todo $j \in J, I_j \subseteq I_{j+1}$.*

Proposição 3.4.6. *(Condição de Cadeia Ascendente) Seja R um anel em que todo o ideal de R é finitamente gerado. Seja $\{I_j : j \in J\}$ uma cadeia ascendente de ideais de A. Então existe $r \in J$ tal que para todo $s \in J$, se $r \geq r$, então $I_r = I_s$.*

Demonstração. Considere-se $I = \bigcup_{j \in J} I_j$. Bastará provar que $I \in \{I_j : j \in J\}$. Prove-se que I é um ideal de R. Sejam $a, b \in I$ elementos arbitrários. Pela definição de I, existem elementos $j_a, j_b \in J$ tais que $a \in I_{j_a}$ e $b \in I_{j_b}$. Como $\{I_j : j \in J\}$ é uma cadeia ascendente de ideais, então

$$I_{j_a} \subseteq I_{j_b} \text{ ou } I_{j_b} \subseteq I_{j_a}.$$

Suponha-se, sem perda de generalidade, que

$$I_{j_a} \subseteq I_{j_b}.$$

Então $a, b \in I_{j_b}$. Assim, como I_{j_b} é um ideal, $a-b, ab \in I_{j_b}$. Logo $a-b, ab \in I$, o que prova que I é um subanel de R. Seja agora $a \in R$ arbitrário. Prove-se que $aI \subseteq I$. Seja $b \in I$ arbitrário. Como $b \in I$, existe $j_b \in J$ tal que $b \in I_{j_b}$. Como I_{j_b} é um ideal de R, $ab \in I_{j_b}$, logo $ab \in I$. Então $aI \subseteq I$. Analogamente se prova que $Ia \subseteq I$ logo I é um ideal de R. Como R é um anel em que todos os ideais são finitamente gerados, existem $n \in \mathbb{N}$ e $a_1, a_2, \ldots, a_n \in I$ tais que $I = (a_1, a_2, \ldots, a_n)$. Para qualquer $i \in \{1, 2, \ldots, n\}, a_i \in I$, logo existe $\sigma \in S_n$, tal que $a_i \in I_{\sigma(i)}$. Seja $r = \max_{i \in \{1,\ldots,n\}} \sigma(i)$. Observe-se que qualquer que seja $i \in \{1, 2, \ldots, n\}, a_i \in I_r$. Então $(a_1, a_2, \ldots, a_n) \subseteq I_r \subseteq I = (a_1, a_2, \ldots, a_n)$, pelo que $I = I_r$. □

Proposição 3.4.7. *Seja D um domínio de integridade. Para quaisquer $a, b \in D$*

(*i*) $(a) \subseteq (b)$ *se e só se* $b|a$.

(*ii*) $(a) = (b)$ *se e só se* a *e* b *são associados.*

Demonstração. (*i*). $(a) \subseteq (b)$ se e só se $a \in (b)$, isto é, se e só se $a = db$, para algum $d \in D$, ou seja $b|a$. (*ii*) Suponha-se que $(a) = (b)$. Então por (*i*), $a|b$ e $b|a$. Portanto, existem $d_1, d_2 \in D$ tais que $a = d_1 b$ e $b = d_2 a$. Assim, $a = d_1 d_2 a$. Observe-se que se $a = 0$, então $b = 0$, logo a e b são associados.

Se $a \neq 0$, pela Proposição 3.4.2, $1 = d_1 d_2$. Então, $d_1, d_2 \in U_D$. Logo a e b são associados. Reciprocamente, suponha-se que a e b são associados. Então existe $u \in U_D$ tal que $a = ub$ e $b = u^{-1}a$. Assim, $a|b$ e $b|a$, por (*i*), $(a) = (b)$. □

Definição 3.4.8. *(elemento irredutível) Seja* D *um domínio de integridade e* $p \in D^\star \backslash U_D$. *Diz-se que* p *é um irredutível de* D *se e só se em qualquer factorização,* $p = ab$, $a \in U_D$ *ou* $b \in U_D$.

Proposição 3.4.9. *Seja* D *um domínio de ideais principais. Para qualquer* $p \in D$, (p) *é um ideal maximal se e só se* p *é irredutível em* D.

Demonstração. Seja $p \in D$ arbitrário. Suponha-se que (p) é um ideal maximal. Sejam $a, b \in D$ tais que $p = ab$. Então pela proposição 3.4.7, $(p) \subseteq (a)$. Como (p) é um ideal maximal então $(p) = (a)$ ou $(a) = (1) = D$. Se $(p) = (a)$, então, pela Proposição 3.4.7 a e p são associados, logo b é uma unidade de D. Se $(a) = (1)$, então, pela Proposição 3.4.7 1 e a são associados, logo a é uma unidade de D. Então, p é um elemento irredutível em D. Reciprocamente, suponha-se que p é um irredutível em D. Seja I um ideal de D tal que $(p) \subseteq I$. Como D é um domínio de ideais principais, então existe $a \in D$ tal que $I = (a)$. Como $(p) \subseteq (a)$, $p \in (a)$, logo existe $b \in D$ tal que $p = ab$. Por hipótese, p é um irredutível, logo $a \in U_D$ ou $b \in U_D$. Se $a \in U_D$, então $(a) = D$. Se $b \in U_D$, então existe $u \in U_D$ tal que $1 = ub$. Observe-se que $up \in (p)$. Mas

$$up = u(ab) = (ub)a = 1a = a,$$

logo $a \in (p)$ e portanto $(a) \subseteq (p)$. Provou-se então que $(a) = (p)$. □

Bibliografia

[1] Fraleigh, J- *A First Course in Abstract Algebra*, Addison Wesley, 5^a Edição, 1994.

[2] Chandler B. and Bumslag B., *Theory and Problems of Group Theory* , Shaum's Outline Series McGraw-Hill Book Company.

[3] Gomes, G., *Notas de curso álgebra II*, 2007/2008.

[4] Hollister, H., *Modern Algebra: A First Course*, Harper and Row Publishers.

[5] Lang S.- *Structures Algébriques*, InterEditions, Paris 1976.

[6] Monteiro, A. (et al)- *álgebra, Um Primeiro Curso*, Escolar Editora, 1995.

[7] Santos, V.M., *Apontamentos de álgebra*, 1988/89.