Capítulo 1

Grupos

1.1 Grupóides, semigrupos e monóides

Definição 1.1.1. Seja X um conjunto. Uma *operação binária (interna)* em X é uma função $*\colon X \times X \to X$, $(x, y) \mapsto x * y$. Uma operação binária $*$ em X diz-se *associativa* se para cada três elementos $x, y, z \in X$, $(x * y) * z = x * (y * z)$. Uma operação binária $*$ em X diz-se *comutativa* se para cada dois elementos $x, y \in X$, $x * y = y * x$.

Exemplos 1.1.2. (i) A adição $+$ e a multiplicação $\cdot$ são operações associativas e comutativas em $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$ e $\mathbb{R}$. Salienta-se que, nestes apontamentos, $\mathbb{N}$ designa o conjuntos dos inteiros não negativos: $\mathbb{N} = \{0, 1, 2, \dots\}$.

(ii) A subtração $-$ é uma operação binária em $\mathbb{Z}$, $\mathbb{Q}$ e $\mathbb{R}$, mas não em $\mathbb{N}$. A subtração não é associativa nem comutativa.

(iii) Uma operação em $\mathbb{N}$ que é comutativa mas não associativa é dada por $a*b = |a-b|$.

(iv) Uma operação associativa no conjunto $\mathcal{M}_{n\times n}(\mathbb{R})$ das matrizes reais $n \times n$ é dada pela multiplicação das matrizes. Se $n \geq 2$, então a multiplicação de matrizes não é comutativa.

(v) A composição de funções é uma operação associativa no conjunto $\mathcal{F}(X)$ das funções no conjunto X. Se X tiver pelo menos dois elementos, a composição não é comutativa.

(vi) A reunião e a intersecção são operações associativas e comutativas no conjunto potência $\mathcal{P}(X)$ de um conjunto X.

Nota 1.1.3. Uma operação binária $*$ num conjunto finito $X = \{x_1, \dots, x_n\}$ pode ser dada através de uma tabela da forma:

	x_1	x_2	$\cdots$	x_j	$\cdots$	x_n
x_1	$x_1 * x_1$	$x_1 * x_2$	$\cdots$	$x_1 * x_j$	$\cdots$	$x_1 * x_n$
x_2	$x_2 * x_1$	$x_2 * x_2$	$\cdots$	$x_2 * x_j$	$\cdots$	$x_2 * x_n$
$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$
x_i	$x_i * x_1$	$x_i * x_2$	$\cdots$	$x_i * x_j$	$\cdots$	$x_i * x_n$
$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$
x_n	$x_n * x_1$	$x_n * x_2$	$\cdots$	$x_n * x_j$	$\cdots$	$x_n * x_n$

Esta tabela é às vezes chamada a *tabela de Cayley* da operação $*$. Por exemplo, a tabela de Cayley da reunião no conjunto potência de um conjunto X com um elemento é dada por:

	$\emptyset$	X
$\emptyset$	$\emptyset$	X
X	X	X

Definição 1.1.4. Um *grupóide* é um par $(X, *)$ em que X é um conjunto não vazio e $*$ é uma operação binária em X. Um *semigrupo* é um grupóide associativo, isto é, um grupóide cuja operação é associativa.

Exemplos 1.1.5. Cada uma das operações binárias nos exemplos 1.1.2 (i),(iv),(v),(vi) é a operação de um semigrupo. O grupóide $(\mathbb{Z}, -)$ não é um semigrupo.

Convenção 1.1.6. No desenvolvimento da teoria, denotaremos as operações de grupóides em geral pelos símbolos $\cdot$ e $+$, sendo o uso do símbolo $+$ restrito a operações comutativas. No caso de uma operação denotada por $\cdot$ falaremos da *multiplicação* do grupóide e do *produto* $a \cdot b$ de dois elementos a e b. Em vez de $a \cdot b$ escrevemos também simplesmente ab. No caso de uma operação denotada por $+$ falaremos da *adição* do grupóide e da *soma* $a + b$ de a e b. Muitas vezes indicaremos um grupóide pelo símbolo do conjunto subjacente. Assim, faleremos simplesmente do grupóide X em vez do grupóide $(X, \cdot)$. Estas convenções serão aplicadas a quaisquer grupóides e, em particular, a grupóides especiais como, por exemplo, semigrupos. Em exemplos e exercícios continuaremos a usar símbolos como $*$ e $\bullet$ para designar operações de grupóides.

Definição 1.1.7. Definimos os *produtos* dos elementos $a_1, \ldots, a_n$ de um grupóide X (nesta ordem) recursivamente como se segue: O único produto de um elemento a é a. Para $n \geq 2$, um elemento $x \in X$ é um produto dos elementos $a_1, \ldots, a_n$ se existem $i \in \{1, \ldots, n-1\}$ e $y, z \in X$ tais que y é um produto dos elementos $a_1, \ldots, a_i$, z é um produto dos elementos $a_{i+1}, \ldots, a_n$ e $x = y \cdot z$.

Assim, o único produto de dois elementos a e b de um grupóide é $a \cdot b$. Para três elementos a, b e c temos os dois produtos $a \cdot (b \cdot c)$ e $(a \cdot b) \cdot c$, que são, em geral, diferentes.

Por isso devemos, em geral, fazer atenção aos parênteses. No entanto, em semigrupos podemos omitir os parênteses:

Proposição 1.1.8. *Sejam S um semigrupo e $a_1, \dots, a_n \in S$. Então existe um único produto dos elementos $a_1, \dots, a_n$.*

Demonstração: Procedemos por indução. Para $n = 1$ o resultado verifica-se por definição. Seja $n \geq 2$ tal que o resultado se verifica para qualquer $i \in \{1, \dots, n-1\}$. Por hipótese de indução, existe um único produto dos elementos $a_2, \dots, a_n$. Seja b este produto. Então $a_1 \cdot b$ é produto dos elementos $a_1, \dots, a_n$. A fim de mostrar a unicidade deste produto consideramos um produto x dos elementos $a_1, \dots, a_n$ e mostramos que $x = a_1 \cdot b$. Sejam $i \in \{1, \dots, n-1\}$ e $y, z \in S$ tais que y é um produto dos elementos $a_1, \dots, a_i$, z é um produto dos elementos $a_{i+1}, \dots, a_n$ e $x = y \cdot z$. Se $i = 1$, então $y = a_1$, $z = b$ e $x = a_1 \cdot b$. Suponhamos que $i > 1$. Pela hipótese de indução existe um produto c dos elementos $a_2, \dots, a_i$. Então $a_1 \cdot c$ é um produto dos elementos $a_1, \dots, a_i$. Pela hipótese de indução, $y = a_1 \cdot c$. Como a operação $\cdot$ de S é associativa, temos $x = y \cdot z = (a_1 \cdot c) \cdot z = a_1 \cdot (c \cdot z)$. Como $c \cdot z$ é um produto dos elementos $a_2, \dots, a_n$, temos $c \cdot z = b$ e então $x = a_1 \cdot b$. □

Notação 1.1.9. Sejam S um semigrupo e $a_1, \dots, a_n \in S$. O único produto dos elementos $a_1, \dots, a_n$ é denotado por $a_1 \cdots a_n$ ou por $\prod_{i=1}^{n} a_i$ no caso da escrita multiplicativa da operação e por $a_1 + \cdots + a_n$ ou por $\sum_{i=1}^{n} a_i$ no caso da escrita aditiva da operação.

Definição 1.1.10. Sejam S um semigrupo, $a \in S$ e $n \geq 1$ um inteiro. O único produto de n cópias de a é chamado *potência de ordem* n de a e é denotado por a^n. Se a operação de S for denotada por $+$, fala-se antes do *múltiplo de ordem* n de a e escreve-se $n \cdot a$ ou na em vez de a^n.

As seguintes regras de cálculo com potências seguem imediatamente de 1.1.8:

Proposição 1.1.11. *Sejam S um semigrupo, $a \in S$ um elemento e $m, n \geq 1$ números inteiros. Então $(a^n)^m = a^{nm}$ e $a^{n+m} = a^n a^m$.*

Definição 1.1.12. Seja X um grupóide. Um *elemento neutro à esquerda* de X é um elemento $e \in X$ tal que $e \cdot x = x$ para todo o $x \in X$. Um *elemento neutro à direita* de X é um elemento $e \in X$ tal que $x \cdot e = x$ para todo o $x \in X$. Um elemento de X que é ao mesmo tempo um elemento neutro à esquerda e à direita de X diz-se um *elemento neutro* de X.

Proposição 1.1.13. *Sejam e um elemento neutro à esquerda e e' um elemento neutro à direita de um grupóide X. Então $e = e'$. Em particular, um grupóide admite, no máximo, um elemento neutro.*

Demonstração: Como e' é um elemento neutro à direita, $e \cdot e' = e$. Como e é um elemento neutro à esquerda, $e \cdot e' = e'$. Logo $e = e'$. □

Definição 1.1.14. Chama-se *monóide* a um semigrupo com elemento neutro.

Exemplos 1.1.15. (i) Os semigrupos $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$ e $\mathbb{R}$ com a multiplicação como operação são monóides com elemento neutro 1.

(ii) Os semigrupos $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$ e $\mathbb{R}$ com a adição como operação são monóides com elemento neutro 0.

(iii) O semigrupo $\mathcal{M}_{n\times n}(\mathbb{R})$ das matrizes reais $n\times n$ é um monóide. A matriz identidade é o elemento neutro.

(iv) O semigrupo $\mathcal{F}(X)$ das funções no conjunto X é um monóide. A função identica id_X é o elemento neutro.

(v) O conjunto potência de um conjunto X é um monóide com a reunião ou a intersecção como multiplicação. O conjunto vazio é o elemento neutro para a reunião e X é o elemento neutro para a intersecção.

(vi) O semigrupo das matrizes reais $n \times n$ com determinante zero não é um monóide.

(vii) O semigrupo das funções constantes num conjunto com mais do que um elemento não é um monóide. Neste semigrupo, todos os elementos são elementos neutros à direita.

(viii) O grupóide $\mathbb{N}$ com a operação dada por $a \cdot b = |a - b|$ admite um elemento neutro, mas não é um monóide.

Notas 1.1.16. (i) Sejam M um monóide com elemento neutro e e $n \geq 1$ um inteiro. Uma indução simples mostra que $e^n = e$.

(ii) Na tabela de Cayley da multiplicação de um grupóide finito com elemento neutro costuma-se ordenar os elementos do grupóide de modo que o elemento neutro é o primeiro.

Notação 1.1.17. Se nada for especificado, o elemento neutro de um monóide será denotado por e. Na escrita multiplicativa da operação também é habitual usar o símbolo 1 para o elemento neutro. Na escrita aditiva também se usa o símbolo 0 para indicar o elemento neutro.

Elementos invertíveis

Definição 1.1.18. Seja X um grupóide com elemento neutro e. Um elemento $y \in X$ diz-se *inverso à esquerda* de um elemento $x \in X$ se $yx = e$. Um elemento $y \in X$ diz-se *inverso à direita* de um elemento $x \in X$ se $xy = e$. Um elemento $y \in X$ diz-se *inverso* de um elemento $x \in X$ se é ao mesmo tempo um inverso à esquerda e à direita de x. Um elemento $x \in X$ diz-se *invertível (à esquerda, à direita)* se admite um inverso (à esquerda, à direita).

Nota 1.1.19. Um elemento de um grupóide finito com elemento neutro é invertível à esquerda (direita) se e só se a coluna (linha) do elemento na tabela de Cayley da multiplicação contém o elemento neutro.

Proposição 1.1.20. *Sejam M um monóide e $x \in M$. Sejam y um inverso à esquerda de x e z um inverso à direita de x. Então $y = z$.*

Demonstração: Usando a associatividade, tem-se $y = ye = y(xz) = (yx)z = ez = z$. □

Notação. Pela proposição anterior, um elemento invertível x de um monóide admite um único inverso. Se a operação do monóide é denotada por $\cdot$, escrevemos x^{-1} para indicar o inverso de x. Se a operação é denotada por $+$, escrevemos $-x$ para indicar o inverso de x.

Observação 1.1.21. O elemento neutro de um monóide é sempre invertível e tem-se $e^{-1} = e$.

Exemplos 1.1.22. (i) Nos monóides $\mathbb{Q}$ e $\mathbb{R}$ com a multiplicação como operação, todos os elementos a menos do 0 são invertíveis. O inverso de um elemento x é o elemento $\frac{1}{x}$.

(ii) Nos monóides $\mathbb{N}$ e $\mathbb{Z}$ com a multiplicação como operação, nenhum elemento a menos dos de módulo 1 admite um inverso à esquerda ou à direita.

(iii) Nos monóides $\mathbb{Z}$, $\mathbb{Q}$ e $\mathbb{R}$ com a adição como operação, todos os elementos são invertíveis.

(iv) No monóide $\mathbb{N}$ com a adição como operação, nenhum elemento a menos do 0 admite um inverso à esquerda ou à direita.

(v) No monóide $\mathcal{M}_{n\times n}(\mathbb{R})$ das matrizes reais $n \times n$, os elementos invertíveis são as matrizes com determinante diferente de zero. Neste monóide, um elemento é invertível à esquerda se e só se é invertível à direita.

(vi) No monóide $\mathcal{F}(X)$ das funções no conjunto X, os elementos invertíveis são as funções bijectivas. Os elementos invertíveis à esquerda são as funções injectivas e os elementos invertíveis à direita são as funções sobrejectivas.

(vii) Num conjunto potência com a reunião ou a intersecção como multiplicação, o único elemento invertível à esquerda ou à direita é o elemento neutro.

Proposição 1.1.23. *Sejam a e b elementos invertíveis de um monóide M. Então a^{-1} e ab são invertíveis e $(a^{-1})^{-1} = a$ e $(ab)^{-1} = b^{-1}a^{-1}$.*

Demonstração: Tem-se $aa^{-1} = e$ e $a^{-1}a = e$. Logo a^{-1} é invertível e $(a^{-1})^{-1} = a$. Tem-se

$$(ab)(b^{-1}a^{-1}) = abb^{-1}a^{-1} = aea^{-1} = aa^{-1} = e$$

e

$$(b^{-1}a^{-1})(ab) = b^{-1}a^{-1}ab = b^{-1}eb = b^{-1}b = e.$$

Logo ab é invertível e $(ab)^{-1} = b^{-1}a^{-1}$. □

Corolário 1.1.24. *Sejam $a_1, \ldots, a_n$ elementos invertíveis de um monóide M. Então $a_1 \cdots a_n$ é invertível e $(a_1 \cdots a_n)^{-1} = a_n^{-1} \cdots a_1^{-1}$.*

Demonstração: Para $n = 1$, o resultado é trivial. Para $n = 2$, o resultado é a proposição 1.1.23. Seja $n \geq 3$ tal que o resultado se verifica para $m < n$. Então $a_1 \cdots a_{n-1}$ é invertível e $(a_1 \cdots a_{n-1})^{-1} = a_{n-1}^{-1} \cdots a_1^{-1}$. Logo $a_1 \cdots a_n = (a_1 \cdots a_{n-1}) \cdot a_n$ é invertível e $(a_1 \cdots a_n)^{-1} = ((a_1 \cdots a_{n-1}) \cdot a_n)^{-1} = a_n^{-1} \cdot (a_{n-1}^{-1} \cdots a_1^{-1}) = a_n^{-1} \cdots a_1^{-1}$. □

Corolário 1.1.25. *Sejam a um elemento invertível de um monóide M e $n \geq 1$ um inteiro. Então a^n é invertível e $(a^n)^{-1} = (a^{-1})^n$.*

Notação 1.1.26. Seja a um elemento invertível de um monóide M. Se a operação de M é denotada por $\cdot$, pomos $a^0 = e$ e $a^{-n} = (a^n)^{-1}$ para todo o inteiro $n \geq 1$. Se a operação de M é denotada por $+$, pomos $0 \cdot a = e$ e $(-n) \cdot a = -(n \cdot a)$ para todo o inteiro $n \geq 1$. Em vez de $m \cdot a$ escrevemos também simplesmente ma ($m \in \mathbb{Z}$).

Observação 1.1.27. Seja a um elemento invertível de um monóide M. Então para todo o $n \in \mathbb{Z}$, $a^{-n} = (a^n)^{-1} = (a^{-1})^n$. Isto segue de 1.1.25 para $n > 0$ e é claro para $n = 0$. Para $n < 0$, tem-se $-n > 0$ e logo $a^{-n} = ((a^{-n})^{-1})^{-1} = (a^{-(-n)})^{-1} = (a^n)^{-1}$ e $a^{-n} = ((a^{-n})^{-1})^{-1} = (a^{-(-n)})^{-1} = ((a^{-1})^{-n})^{-1} = (a^{-1})^{-(-n)} = (a^{-1})^n$. Na escrita aditiva da operação temos $(-n)a = -(na) = n(-a)$ para todo o $n \in \mathbb{Z}$.

Proposição 1.1.28. *Sejam a um elemento invertível de um monóide M e $m, n \in \mathbb{Z}$. Então $(a^n)^m = a^{nm}$ e $a^{n+m} = a^n a^m$.*

Demonstração: Mostramos primeiramente que $(a^n)^m = a^{nm}$. Se $m, n \geq 1$, isto segue de 1.1.11. Se $m = 0$ ou $n = 0$, $(a^n)^m = e = a^{nm}$. Suponhamos que $m \geq 1$ e $n < 0$. Seja $k = -n$. Então $k \geq 1$ e temos $(a^n)^m = (a^{-k})^m = ((a^k)^{-1})^m = ((a^k)^m)^{-1} = (a^{km})^{-1} = a^{-km} = a^{nm}$. Suponhamos que $m < 0$ e $n \geq 1$. Seja $l = -m$. Então $l \geq 1$ e temos $(a^n)^m = (a^n)^{-l} = ((a^n)^l)^{-1} = (a^{nl})^{-1} = a^{-nl} = a^{nm}$. Suponhamos finalmente que $m, n < 0$. Sejam $k = -n$ e $l = -m$. Então $k, l \geq 1$ e $(a^n)^m = (a^n)^{-l} = ((a^n)^{-1})^l = (a^{-n})^l = (a^k)^l = a^{kl} = a^{nm}$.

Mostramos agora que $a^{n+m} = a^n a^m$. Começamos com o caso $m > 0$. Se $n \geq 1$, o resultado segue de 1.1.11. Se $n = 0$, $a^{n+m} = a^m = ea^m = a^0 a^m = a^n a^m$. Se $n < 0$ e $n + m = 0$, então $n = -m$ e $a^{n+m} = e = a^{-m} a^m = a^n a^m$. Se $n < 0$ e $n + m > 0$, então $a^{-n} a^{n+m} = a^{-n+n+m} = a^m$, pelo que $a^{n+m} = a^n a^{-n} a^{n+m} = a^n a^m$. Se $n < 0$ e $n + m < 0$, então $a^{n+m}(a^m)^{-1} = a^{-(-(n+m))}(a^m)^{-1} = (a^{-(n+m)})^{-1}(a^m)^{-1} = (a^m a^{-(n+m)})^{-1} = (a^{m-(n+m)})^{-1} = (a^{-n})^{-1} = a^n$, pelo que $a^{n+m} = a^{n+m}(a^m)^{-1} a^m = a^n a^m$. No caso $m = 0$ temos $a^{n+m} = a^n = a^n e = a^n a^0 = a^n a^m$. Consideremos finalmente o caso $m < 0$. Então $-m > 0$. Segue-se que $a^{n+m} = a^{-(-n-m)} = (a^{-1})^{-n-m} = (a^{-1})^{-n}(a^{-1})^{-m} = a^n a^m$. □

1.2 Grupos

Definição 1.2.1. Um *grupo* é um monóide em que todos os elementos são invertíveis. Se a operação for comutativa, o grupo é dito commutativo ou *abeliano*.

Observação 1.2.2. Sejam M um monóide e G o conjunto dos elementos invertíveis de M. Segue-se de 1.1.21 e 1.1.23 que G é um grupo relativamente à multiplicação de M.

Exemplos 1.2.3. (i) Os conjuntos $\mathbb{Z}$, $\mathbb{Q}$ e $\mathbb{R}$ são grupos (comutativos/abelianos) relativamente à adição.

(ii) Os conjuntos $\mathbb{Q} \setminus \{0\}$ e $\mathbb{R} \setminus \{0\}$ são grupos (comutativos/abelianos) relativamente à multiplicação.

(iii) O conjunto das matrizes reais $n \times n$ com determinante diferente de zero é um grupo relativamente à multiplicação das matrizes. Este grupo é denotado por $GL_n(\mathbb{R})$.

(iv) O conjunto $S(X)$ das funções bijectivas num conjunto X é um grupo com a composição de funções como multiplicação. Chama-se *grupo simétrico* de X a este grupo e *permutações de* X aos seus elementos. Usa-se a abreviação $S_n = S(\{1, \ldots, n\})$.

(v) O conjunto $G = \{e\}$ é um grupo relativamente à única operação que existe em G.

(vi) O conjunto potência de um conjunto não vazio com a reunião ou a intersecção como multiplicação nunca é um grupo.

Definição 1.2.4. Se X é um grupóide e se $a \in X$, definimos as funções $\lambda_a : X \to X$ e $\rho_a : X \to X$ por $\lambda_a(x) = ax$ e $\rho_a(x) = xa$.

Proposição 1.2.5. *Se G for um grupo então, para todo o $a \in G$, as funções $\lambda_a : G \to G$ e $\rho_a : G \to G$ são bijetivas.*

Demonstração: Seja $a \in G$. Sejam $x, y \in G$ tais que $\lambda_a(x) = \lambda_a(y)$, isto é, $ax = ay$. Como a é invertível, multiplicando à esquerda por a^{-1}, obtemos $a^{-1}ax = a^{-1}ay$. Disto vem $ex = ey$ ou seja $x = y$, o que mostra a injetividade de λ_a. Seja agora $y \in G$. Temos $y = aa^{-1}y = \lambda_a(x)$ onde $x = a^{-1}y$. Como $x \in G$, podemos concluir que λ_a é sobrejetiva e, finalmente, bijetiva. De forma analoga, provamos que ρ_a é bijetiva. □

Nota 1.2.6. Segue-se da Proposição 1.2.5 que cada linha e cada coluna da tabela de Cayley de um grupo finito contém cada elemento do grupo exactamente uma vez. Assim, existe no máximo uma estrutura de grupo no conjunto $G = \{e, a, b\}$ na qual e é o elemento neutro. Com efeito, a única tabela de Cayley possível é:

	e	a	b
e	e	a	b
a	a	b	e
b	b	e	a

Verifica-se que a operação assim definida é associativa e então que G é de facto um grupo relativamente a esta operação.

Definição 1.2.7. Dizemos que um grupóide X satisfaz as *leis do corte* se para quaisquer três elementos $a, b, c \in X$, tem-se

(i) $ac = bc \Rightarrow a = b$

(ii) $ca = cb \Rightarrow a = b$

ou seja, se para todo o $a \in X$, as funções λ_a e ρ_a são injetivas.

Em consequência da Proposição 1.2.5 temos:

Proposição 1.2.8. *Qualquer grupo satisfaz as leis do corte.*

Proposição 1.2.9. *Seja G um semi-grupo. Se, para todo o $a \in G$, as funções $\lambda_a : G \to G$ e $\rho_a : G \to G$ são sobrejetivas então G é um grupo.*

Demonstração: Como G é um semi-grupo, falta ver que G admite um elemento neutro e que todo o elemento de G é invertível.

Como $G \neq \emptyset$, existe $a \in G$. Como λ_a é sobrejetiva, existe $e \in G$ tal que $a = ae$. Seja $x \in G$. Vamos ver que $xe = x$. Como ρ_a é sobrejetiva, existe $y \in G$ tal que $x = ya$. Logo $xe = yae = ya = x$. Provámos assim que e é elemento neutro à direita. Da mesma forma (começando com a sobrejetividade de ρ_a) podemos ver que existe $e' \in G$ tal que, para todo o $x \in G$, $e'x = x$. Segue-se da Proposição 1.1.13 que $e = e'$. Podemos concluir que este elemento é elemento neutro de G.

Seja $x \in G$. Como λ_x é sobrejetiva, existe $z \in G$ tal que $xz = e$. Como ρ_x é sobrejetiva, existe $y \in G$ tal que $yx = e$. Como G é um semi-grupo, deduzimos da Proposição 1.1.20 que $y = z$. Este elemento é o inverso de x pelo que x é invertível.

Podemos concluir que G é um grupo. □

Proposição 1.2.10. *Um semigrupo finito G é um grupo se e só se satisfaz as leis do corte.*

Demonstração: Basta mostrar que G é um grupo se satisfaz as leis do corte. Seja $a \in G$. Se G satisfaz as leis do corte, então as funções $\lambda_a \colon G \to G$ e $\rho_a \colon G \to G$ são injetivas. Como G é finito e é simultanemente o conjunto de partida e de chegada, podemos concluir que λ_a e ρ_a também são sobrejetivas. Pela Proposição 1.2.9, isto implica que G é um grupo. □

Nota 1.2.11. O resultado anterior não se estende aos semigrupos infinitos como mostra o exemplo do monóide $(\mathbb{N}, +)$.

1.3 Homomorfismos de grupos

Definição 1.3.1. Sejam G e H dois grupos. Um *homomorfismo de grupos* $f\colon G \to H$ é uma função $f\colon G \to H$ tal que $f(a \cdot b) = f(a) \cdot f(b)$ para quaisquer dois elementos $a, b \in G$. Um homomorfismo de grupos $f\colon G \to H$ diz-se

- *endomorfismo* se o grupo de chegada $(H, \cdot)$ é igual ao grupo de partida $(G, \cdot)$;
- *monomorfismo* se f é injectivo;
- *epimorfismo* se f é sobrejectivo;
- *isomorfismo* se f é bijectivo;
- *automorfismo* se f é um endomorfismo bijectivo.

Dois grupos G e H dizem-se *isomorfos*, $G \cong H$, se existe um isomorfismo entre eles.

Proposição 1.3.2. *Sejam G e H dois grupos e $f\colon G \to H$ um homomorfismo. Então*

(i) $f(e) = e$;

(ii) para todo o $x \in G$, $f(x^{-1}) = f(x)^{-1}$.

Demonstração: (i) Temos $f(e)^2 = f(e^2) = f(e) = f(e) \cdot e$. Pelas leis do corte, isto implica que $f(e) = e$.

(ii) Seja $x \in G$. Temos $f(x^{-1})f(x) = f(x^{-1}x) = f(e) = e = f(x)^{-1}f(x)$ e então $f(x^{-1}) = f(x)^{-1}$. □

Nota 1.3.3. Sejam G e H dois grupos e $f\colon G \to H$ um homomorfismo. Segue-se da proposição anterior que para qualquer $x \in G$ e qualquer $n \in \mathbb{Z}$, $f(x^n) = f(x)^n$ (exercício).

Exemplos 1.3.4. (i) Sejam G e H dois grupos. Então a função constante $g \mapsto e$ é um homomorfismo de G para H.

(ii) Seja $n \in \mathbb{Z}$. Um endomorfismo $f\colon (\mathbb{Z}, +) \to (\mathbb{Z}, +)$ é dado por $f(m) = nm$. O endomorfismo f é um monomorfismo se e só se $n \neq 0$ e um automorfismo se e só se $n \in \{1, -1\}$.

(iii) Um monomorfismo $f\colon (\mathbb{R}, +) \to (\mathbb{R} \setminus \{0\}, \cdot)$ é dado por $f(x) = 2^x$.

(iv) O determinante é um epimorfismo do grupo $GL_n(\mathbb{R})$ para o grupo $(\mathbb{R} \setminus \{0\}, \cdot)$.

(v) A função identidade de um grupo é um automorfismo.

Proposição 1.3.5. *Sejam $f\colon G \to H$ e $g\colon H \to K$ dois homomorfismos de grupos. Então $g \circ f$ é um homomorfismo de grupos de G para K.*

Demonstração: Sejam $x, y \in G$. Então $g \circ f(xy) = g(f(xy)) = g(f(x)f(y)) = g(f(x))g(f(y)) = g \circ f(x) \cdot g \circ f(y)$. $\square$

Definição 1.3.6. Seja $f \colon G \to H$ um homomorfismo de grupos. A *imagem* de f é o conjunto $\mathrm{Im}(f) = \{f(x) \mid x \in G\}$. O *núcleo* de f é o conjunto $\mathrm{Ker}(f) = \{x \in G \mid f(x) = e\}$. Às vezes escreve-se $\mathrm{Nuc}(f)$ em vez de $\mathrm{Ker}(f)$.

Proposição 1.3.7. *Um homomorfismo de grupos $f \colon G \to H$ é injectivo se e só se* $\mathrm{Ker}(f) = \{e\}$.

Demonstração: Basta demonstrar que f é injectivo se $\mathrm{Ker}(f) = \{e\}$. Sejam $x, y \in G$ tais que $f(x) = f(y)$. Então

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

Portanto $xy^{-1} \in \mathrm{Ker}(f)$, pelo que $xy^{-1} = e$. Logo $x = y$. Segue-se que f é injetivo. $\square$

Proposição 1.3.8. *Seja $f \colon G \to H$ um isomorfismo de grupos. Então a função inversa f^{-1} é também um isomorfismo de grupos.*

Demonstração: Como f^{-1} é bijectiva, basta demonstrar que f^{-1} é um homomorfismo de grupos. Sejam $x, y \in H$. Tem-se

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

Como f é injectiva, obtém-se $f^{-1}(xy) = f^{-1}(x)f^{-1}(y)$. $\square$

1.4 Subgrupos

Definição 1.4.1. Um subconjunto H de um grupo G diz-se *subgrupo* de G se é um grupo relativamente à multiplicação de G. Usa-se a notação $H \leq G$ para indicar que H é um subgrupo de G. Se se quiser indicar que H é um *subgrupo próprio* de G, isto é $H \leq G$ mas $H \neq G$, então escreve-se $H < G$.

Exemplos 1.4.2. (i) $\{-1, +1\}$ é um subgrupo do grupo multiplicativo $\mathbb{R} \setminus \{0\}$ e temos de facto $\{-1, +1\} < \mathbb{R} \setminus \{0\}$.

(ii) Em qualquer grupo G, o conjunto $\{e\}$ é um subgrupo, chamado o *subgrupo trivial* de G.

(iii) Para qualquer grupo G, $G \leq G$.

Observação 1.4.3. Sejam G um grupo, $K \leq G$ e $H \subseteq K$. Então $H \leq G \Leftrightarrow H \leq K$.

Proposição 1.4.4. *Seja G um grupo. Um subconjunto $H \subseteq G$ é um subgrupo de G se e só se satisfaz as seguintes condições:*

(i) $e \in H$;

(ii) *para quaisquer* $x, y \in H$, $xy \in H$;

(iii) *para qualquer* $x \in H$, $x^{-1} \in H$.

Demonstração: Basta mostrar que um subgrupo de G satisfaz estas três condições. Seja $H \leq G$. Por definição, H satisfaz a condição (ii). Como H é um grupo, existe um elemento neutro $\bar{e} \in H$. Tem-se $e\bar{e} = \bar{e} = \bar{e}^2$ e então $e = \bar{e} \in H$. Seja $x \in H$ e seja $\bar{x}$ o inverso de x no grupo H. Então $x^{-1}x = e = \bar{x}x$, pelo que $x^{-1} = \bar{x} \in H$. □

Exemplos 1.4.5. (i) $]0, +\infty[$ é um subgrupo do grupo multiplicativo $\mathbb{R} \setminus \{0\}$.

(ii) O conjunto das matrizes da forma $\begin{pmatrix} a & 0 \\ 0 & b \end{pmatrix}$ com $a, b \in \mathbb{R} \setminus \{0\}$ é um subgrupo de $GL_2(\mathbb{R})$.

Exemplo 1.4.6. Sendo G um grupo, o conjunto $Z(G) = \{g \in G \,|\, \forall x \in G \quad gx = xg\}$ é um subgrupo de G. É chamado *centro* de G.

Proposição 1.4.7. *Seja G um grupo. Um subconjunto não vazio $H \subseteq G$ é um subgrupo de G se e só se para quaisquer $x, y \in H$, $xy^{-1} \in H$.*

Demonstração: Suponhamos primeiramente que H é um subgrupo de G. Sejam $x, y \in H$. Então $y^{-1} \in H$. Logo $xy^{-1} \in H$.

Suponhamos agora que para quaisquer $x, y \in H$, $xy^{-1} \in H$. Como $H \neq \emptyset$, existe $a \in H$. Segue-se que $e = aa^{-1} \in H$. Seja $x \in H$. Então $x^{-1} = ex^{-1} \in H$. Sejam $x, y \in H$. Então $x, y^{-1} \in H$ e portanto $xy = x(y^{-1})^{-1} \in H$. Por 1.4.4, H é um subgrupo de G. □

Proposição 1.4.8. *Sejam $f\colon G \to H$ um homomorfismo de grupos, $U \subseteq G$ e $V \subseteq H$ subgrupos. Então $f^{-1}(V)$ é um subgrupo de G e $f(U)$ é um subgrupo de H.*

Demonstração: Como $f(e) = e \in V$, $e \in f^{-1}(V)$ e $f^{-1}(V) \neq \emptyset$. Sejam $x, y \in f^{-1}(V)$. Então $f(xy^{-1}) = f(x)f(y^{-1}) = f(x)f(y)^{-1} \in V$, pelo que $xy^{-1} \in f^{-1}(V)$. Por 1.4.7, $f^{-1}(V)$ é um subgrupo de G.

Como $U \neq \emptyset$, $f(U) \neq \emptyset$. Para quaisquer $a, b \in U$, $ab^{-1} \in U$ e $f(a)f(b)^{-1} = f(a)f(b^{-1}) = f(ab^{-1}) \in f(U)$. Por 1.4.7, $f(U)$ é um subgrupo de H. □

Corolário 1.4.9. *Seja $f\colon G \to H$ um homomorfismo de grupos. Então* $\mathrm{Ker}(f)$ *é um subgrupo de G e* $\mathrm{Im}(f)$ *é um subgrupo de H.*

Exemplo 1.4.10. O conjunto $\mathrm{SL}_n(\mathbb{R}) = \{A \in \mathrm{GL}_n(\mathbb{R}) \,|\, \det(A) = 1\}$ é o núcleo do homomorfismo $\det\colon \mathrm{GL}_n(\mathbb{R}) \to \mathbb{R} \setminus \{0\}$ e é portanto um subgrupo de $\mathrm{GL}_n(\mathbb{R})$. Este grupo é chama *grupo especial linear*.

Proposição 1.4.11. *Sejam G um grupo e $(H_i)_{i\in I}$ uma família não vazia de subgrupos de G. Então $\bigcap_{i\in I} H_i$ é um subgrupo de G.*

Demonstração: Como $e \in H_i$ para todo o $i \in I$, $\bigcap_{i\in I} H_i \neq \emptyset$. Sejam $x, y \in \bigcap_{i\in I} H_i$. Então $x, y \in H_i$ para todo o $i \in I$. Por 1.4.7, $xy^{-1} \in H_i$ para todo o $i \in I$, pelo que $xy^{-1} \in \bigcap_{i\in I} H_i$. Por 1.4.7, $\bigcap_{i\in I} H_i$ é um subgrupo de G. □

Definição 1.4.12. Sejam G um grupo e $X \subseteq G$ um subconjunto. O *subgrupo gerado por X*, $\langle X \rangle$, é a intersecção dos subgrupos de G que contêm X. Se $X = \{x_1, \ldots, x_n\}$, escrevemos também $\langle x_1, \ldots, x_n \rangle$ em vez de $\langle X \rangle$ e falamos do *subgrupo de G gerado pelos elementos $x_1, \ldots, x_n$*. O conjunto X diz-se um *conjunto gerador* de G se $G = \langle X \rangle$. Se G admite um conjunto gerador finito, G diz-se *finitamente gerado*.

Proposição 1.4.13. *Sejam G um grupo e $X \subseteq G$ um subconjunto. Então os elementos de $\langle X \rangle$ são o elemento neutro e os produtos finitos formados a partir dos elementos de X e dos seus inversos.*

Demonstração: Seja H o subconjunto de G cujos elementos são o elemento neutro e os produtos finitos formados a partir dos elementos de X e dos seus inversos. Então H é um subgrupo de G e $X \subseteq H$. Logo $\langle X \rangle \subseteq H$. Por outro lado, qualquer elemento de H pertence necessariamente a qualquer subgrupo de G que contém X. Logo $H \subseteq \langle X \rangle$. □

Exemplos 1.4.14. (i) Sendo G um grupo, o subgrupo de G gerado pelo elemento neutro e é $\{e\}$. Se $a \in G$, o subgrupo de G gerado por a é $\langle a \rangle = \{a^n \mid n \in \mathbb{Z}\}$.

(ii) O subgrupo de $(\mathbb{Z}, +)$ gerado por $m \in \mathbb{Z}$ é o conjunto $m\mathbb{Z} = \{mk \,|\, k \in \mathbb{Z}\}$. Em particular, o conjunto $\{1\}$ é um conjunto gerador de $(\mathbb{Z}, +)$. O subgrupo de $(\mathbb{Z}, +)$ gerado pelo conjunto $\{2, 3\}$ é o conjunto $\{2m + 3n \,|\, m, n \in \mathbb{Z}\}$.

Observação 1.4.15. Segue-se imediatamente da definição que para quaisquer dois subconjuntos X e Y de um grupo G, $X \subseteq Y \Rightarrow \langle X \rangle \leq \langle Y \rangle$.

Proposição 1.4.16. *Sejam $f, g\colon G \to H$ dois homomorfismos de grupos que coincidem num conjunto gerador X de G. Então $f = g$.*

Demonstração: Como f e g coincidem em X, também coincidem em qualquer produto finito formado a partir dos elementos de X e dos seus inversos. Como f e g são homomorfismos de grupos, $f(e) = g(e) = e$. Logo f e g coincidem em $\langle X \rangle = G$. $\square$

Exemplo 1.4.17. Seja G um grupo e $g \in G$. Como $\{1\}$ é um conjunto gerador de $(\mathbb{Z}, +)$, existe um único homomorfismo de grupos $f\colon (\mathbb{Z}, +) \to G$ com $f(1) = g$. Este homomorfismo é dado por $f(m) = g^m$ (na escrita multiplicativa da operação de G).

1.5 Teorema de Lagrange

Notação 1.5.1. Sejam G um grupo, $A, B \subseteq G$ dois subconjuntos não vazios e $x \in G$. Usamos as notações $AB = \{ab \,|\, a \in A, b \in B\}$, $Ax = \{ax \,|\, a \in A\}$ e $xA = \{xa \,|\, a \in A\}$. Em notação aditiva escreve-se $A + B$, $A + x$ e $x + A$ em vez de AB, Ax e xA.

Definição 1.5.2. Sejam G um grupo, H um subgrupo de G. Os conjuntos Hx (xH), $x \in G$, são as *classes laterais direitas (esquerdas) de* H.

Proposição 1.5.3. *Sejam G um grupo e H um subgrupo de G. Então uma relação de equivalencia em G é dada por $x \sim_H y \Leftrightarrow xy^{-1} \in H$. A classe de equivalência de um elemento $x \in G$ é a classe lateral direita Hx.*

Demonstração: Como $e \in H$, a relação $\sim_H$ é reflexiva. Sejam $x, y \in G$ tais que $x \sim_H y$. Então $xy^{-1} \in H$. Logo $yx^{-1} = (xy^{-1})^{-1} \in H$ e portanto $y \sim_H x$. Segue-se que $\sim_H$ é simétrica. Sejam $x, y, z \in G$ tais que $x \sim_H y$ e $y \sim_H z$. Então $xy^{-1} \in H$ e $yz^{-1} \in H$ Logo $xz^{-1} = xy^{-1}yz^{-1} \in H$ e $x \sim_H z$. Portanto $\sim_H$ é reflexiva. Segue-se que $\sim_H$ é uma relação de equivalência.

Seja $x \in G$ e $[x]$ a classe de equivalência de x. Seja $y \in [x]$. Então $y \sim_H x$, pelo que $yx^{-1} \in H$. Logo $y = yx^{-1}x \in Hx$ e $[x] \subseteq Hx$. Seja $y \in Hx$. Então $yx^{-1} \in Hxx^{-1} = H$, pelo que $y \sim_H x$. Portanto $y \in [x]$ e $Hx \subseteq [x]$. $\square$

Proposição 1.5.4. *Sejam G um grupo, H um subgrupo de G e $x \in G$. Então a função $f\colon H \to Hx$, $y \mapsto yx$ é bijectiva.*

Demonstração: Pelas leis do corte, f é injectiva. Seja $z \in Hx$. Então existe $y \in H$ tal que $z = yx = f(y)$. Isto mostra que f é sobrejectiva. $\square$

Definição 1.5.5. A *ordem* de um grupo finito G é o número de elementos de G. A *ordem* de um grupo infinito é ∞. A ordem de um grupo G é indicada por $|G|$. A *ordem* de um elemento a de um grupo G, indicada por $|a|$, é a ordem do subgrupo de G gerado por a.

Definição 1.5.6. Sejam G um grupo e H um subgrupo de G. O *índice* de H em G, denotado por $|G : H|$, é o número de classes laterais direitas de H (que pode ser finito ou ∞).

Teorema 1.5.7. *(Teorema de Lagrange) Sejam G um grupo finito e H um subgrupo de G. Então $|G| = |G : H||H|$.*

Demonstração: Por 1.5.4, cada classe lateral direita de H tem $|H|$ elementos. Por 1.5.3, as classes laterais direitas de H formam uma partição de G. Logo $|G| = |G : H||H|$. $\square$

Corolário 1.5.8. *A ordem de um subgrupo de um grupo finito é um divisor da ordem do grupo. Em particular, a ordem de um elemento de um grupo finito é um divisor da ordem do grupo.*

Exemplo 1.5.9. Seja G um grupo de ordem prima e $a \in G \setminus \{e\}$. Como $|a| > 1$ e $|a|$ divide $|G|$, tem-se $|a| = |G|$ e então $G = \langle a \rangle$.

1.6 Subgrupos normais e grupos quociente

Definição 1.6.1. Um subgrupo H de um grupo G diz-se *normal* ou *invariante* se para cada $a \in G$, $aHa^{-1} \subseteq H$. Usa-se a notação $H \trianglelefteq G$ ($H \triangleleft G$) para indicar que H é um subgrupo normal (próprio) de G.

Proposição 1.6.2. *Sejam G um grupo e H um subgrupo normal de G. Então, para todo o $a \in G$, $aH = Ha$.*

Demonstração: Seja $a \in G$. Seja $ah \in aH$ com $h \in H$. Como $aha^{-1} \in H$, existe $h' \in H$ tal que $aha^{-1} = h'$. Logo $ah = h'a$ e $ah \in Ha$. Isto mostra que $aH \subseteq Ha$. Por outro lado, para $h \in H$, $a^{-1}h(a^{-1})^{-1} \in H$ o que permite concluir que $ha \in aH$. $\square$

Exemplos 1.6.3. (i) Para qualquer grupo G, $\{e\}$ e G são subgrupos normais de G.
(ii) Num grupo comutativo todos os subgrupos são normais.
(iii) Para qualquer grupo G, o centro $Z(G)$ é um grupo normal de G.

Proposição 1.6.4. *Sejam G um grupo e $(H_i)_{i \in I}$ uma família não vazia de subgrupos normais de G. Então $\bigcap_{i \in I} H_i$ é um subgrupo normal de G.*

Demonstração: Por 1.4.11, $\bigcap_{i \in I} H_i$ é um subgrupo de G. Sejam $a \in G$ e $x \in \bigcap_{i \in I} H_i$. Então $x \in H_i$ para todo o $i \in I$. Portanto $axa^{-1} \in H_i$ para todo o $i \in I$. Logo $axa^{-1} \in \bigcap_{i \in I} H_i$. $\square$

Proposição 1.6.5. *Sejam $f\colon G \to G'$ um homomorfismo de grupos e $H \subseteq G$ e $H' \subseteq G'$ subgrupos normais. Então $f^{-1}(H')$ é um subgrupo normal de G e $f(H)$ é um subgrupo normal de* $\mathrm{Im}(f)$.

Demonstração: Por 1.4.8, $f^{-1}(H')$ é um subgrupo de G. Sejam $x \in f^{-1}(H')$ e $a \in G$. Como H' é um subgrupo normal de G', tem-se $f(axa^{-1}) = f(a)f(x)f(a^{-1}) = f(a)f(x)f(a)^{-1} \in H'$. Logo $axa^{-1} \in f^{-1}(H')$. Segue-se que $f^{-1}(H')$ é um subgrupo normal de G.

Por 1.4.8, $\mathrm{Im}(f)$ e $f(H)$ são subgrupos de G'. Logo $f(H)$ é um subgrupo de $\mathrm{Im}(f)$. Sejam $x \in f(H)$ e $a \in \mathrm{Im}(f)$. Então existem $h \in H$ e $g \in G$ tais que $x = f(h)$ e $a = f(g)$. Temos $axa^{-1} = f(g)f(h)f(g)^{-1} = f(g)f(h)f(g^{-1}) = f(ghg^{-1})$. Como H é um subgrupo normal de G, $ghg^{-1} \in H$. Segue-se que $axa^{-1} = f(ghg^{-1}) \in f(H)$ e então que $f(H)$ é um subgrupo normal de $\mathrm{Im}(f)$. □

Corolário 1.6.6. *O núcleo de um homomorfismo de grupos $f\colon G \to G'$ é um subgrupo normal de G.*

Exemplo 1.6.7. O conjunto $SL_n(\mathbb{R}) = \{A \in GL_n(\mathbb{R}) \mid \det A = 1\} = \mathrm{Ker}(\det\colon GL_n(\mathbb{R}) \to \mathbb{R} \setminus \{0\})$ é um subgrupo normal de $GL_n(\mathbb{R})$.

Proposição 1.6.8. *Sejam G um grupo e $H \subseteq G$ um subgrupo. Considere a relação de equivalência $\sim_H$ em G definida por $x \sim_H y \Leftrightarrow xy^{-1} \in H$. Então*

1. *Para quaisquer $x, y, a \in G$, tem-se $x \sim_H y \Rightarrow xa \sim_H ya$.*

2. *H é um subgrupo normal de G se e só se $x \sim_H y \Rightarrow ax \sim_H ay$ para quaisquer $x, y, a \in G$.*

Demonstração: Por 1.5.3, a classe de equivalência de um elemento $x \in G$ é a classe lateral direita Hx. Assim, $x \sim_H y \Leftrightarrow Hx = Hy$. Sejam $x, y, a \in G$ tais que $x \sim_H y$. Então $[x] = [y]$, ou seja, $Hx = Hy$. Então $Hxa = Hya$, ou seja, $[xa] = [ya]$. Logo $xa \sim_H ya$ o que prova (1). Suponhamos agora que H é um subgrupo normal de G. Temos

$$x \sim_H y \Rightarrow Hx = Hy \Rightarrow xH = yH \Rightarrow axH = ayH \Rightarrow Hax = Hay \Rightarrow ax \sim_H ay.$$

Reciprocamente, suponhamos que $x \sim_H y \Rightarrow ax \sim_H ay$ para quaisquer $x, y, a \in G$. Sejam $x \in H$ e $a \in G$. Então $x \sim_H e$ e portanto $ax \sim_H ae = a$. Segue-se que $axa^{-1} \in H$ e então que H é um subgrupo normal de G. □

Corolário 1.6.9. *Seja H um subgrupo normal de um grupo G. Então para quaisquer $x, y, x', y' \in G$, se $x \sim_H x'$ e $y \sim_H y'$, então $xy \sim_H x'y'$.*

Definição 1.6.10. Sejam G um grupo e $H \subseteq G$ um subgrupo normal. O *grupo quociente de G por H* é o conjunto das classes laterais

$$G/H = \{Hx \,|\, x \in G\}$$

munido da operação dada por

$$Hx \cdot Hy = Hxy.$$

Por 1.6.9, esta operação está bem definida. É óbvio que G/H é de facto um grupo. O elemento neutro é H e tem-se $(Hx)^{-1} = Hx^{-1}$ $(x \in G)$. Chama-se *epimorfismo canónico* ao homomorfismo de grupos sobrejectivo $\pi\colon G \to G/H$ definido por $\pi(x) = Hx$.

Exemplos 1.6.11. (i) Para qualquer grupo G, $G/G = \{G\}$.

(ii) Seja $n \geq 1$ um inteiro. Tem-se $\mathbb{Z}/n\mathbb{Z} = \{r + n\mathbb{Z} \,|\, 0 \leq r < n\}$. Este grupo quociente é denotado por $\mathbb{Z}_n$. Muitas vezes usa-se a notação $[r]_n = r + n\mathbb{Z}$. Nota-se que $k \in [r]_n$ se e só se $k \equiv r \mod n$. A operação de $\mathbb{Z}_n$ é denotada por $+$ e é dada por $(r + n\mathbb{Z}) + (s + n\mathbb{Z}) = r + s + n\mathbb{Z}$.

Observações 1.6.12. (i) Sejam G um grupo e $H \subseteq G$ um subgrupo normal. Então o núcleo do epimorfismo canónico $\pi\colon G \to G/H$ é H. Com efeito, tem-se $x \in \mathrm{Ker}(\pi) \Leftrightarrow \pi(x) = H \Leftrightarrow Hx = H \Leftrightarrow x \in H$.

(ii) Para qualquer grupo G, o epimorfismo canónico $G \to G/\{e\}$ é um isomorfismo.

(iii) Para um grupo G e um subgrupo normal $H \trianglelefteq G$, $|G/H| = |G : H|$. Em particular, se G é finito, tem-se, pelo Teorema de Lagrange, $|G/H| = |G|/|H|$.

Teorema 1.6.13. *(Propriedade universal) Sejam $f\colon G \to G'$ um homomorfismo de grupos, $H \subseteq G$ um subgrupo normal tal que $H \subseteq \mathrm{Ker}(f)$ e $\pi\colon G \to G/H$ o epimorfismo canónico. Então existe um único homomorfismo de grupos $\bar{f}\colon G/H \to G'$ tal que $\bar{f} \circ \pi = f$. O homomorfismo $\bar{f}$ é dado por $\bar{f}(Hx) = f(x)$ e é um monomorfismo se e só se $H = \mathrm{Ker}(f)$.*

Demonstração: Sejam $x, y \in G$ tais que $Hx = Hy$. Então $xy^{-1} \in H \subseteq \mathrm{Ker}(f)$. Logo $f(x)f(y)^{-1} = f(x)f(y^{-1}) = f(xy^{-1}) = e$, pelo que $f(x) = f(y)$. Segue-se que a função $\bar{f}\colon G/H \to G'$, $\bar{f}(Hx) = f(x)$ está bem definida. Tem-se $\bar{f}(HxHy) = \bar{f}(Hxy) = f(xy) = f(x)f(y) = \bar{f}(Hx)\bar{f}(Hy)$, pelo que $\bar{f}$ é um homomorfismo de grupos. Por definição, $\bar{f} \circ \pi = f$. Seja $g\colon G/H \to G'$ um homomorfismo tal que $g \circ \pi = f$. Então para qualquer $x \in G$, $g(Hx) = g \circ \pi(x) = f(x) = \bar{f} \circ \pi(x) = \bar{f}(Hx)$, pelo que $g = \bar{f}$.

Suponhamos que $H = \mathrm{Ker}(f)$. Seja $x \in G$ tal que $\bar{f}(Hx) = e$. Então $f(x) = e$ e $x \in \mathrm{Ker}(f) = H$. Segue-se que $Hx = H$ e então que $\bar{f}$ é um monomorfismo. Suponhamos inversamente que $\bar{f}$ é um monomorfismo. Seja $x \in \mathrm{Ker}(f)$. Então $\bar{f}(Hx) = f(x) = e = \bar{f}(H)$. Logo $Hx = H$ e portanto $x \in H$. Segue-se que $H = \mathrm{Ker}(f)$. $\square$

Corolário 1.6.14. *(Teorema do homomorfismo) Seja* $f\colon G \to G'$ *um homomorfismo de grupos. Então um isomorfismo de grupos* $G/\mathrm{Ker}(f) \to \mathrm{Im}(f)$ *é dado por* $\mathrm{Ker}(f)x \mapsto f(x)$.

Exemplo 1.6.15. Para qualquer inteiro $n \geq 1$, o grupo $GL_n(\mathbb{R})/SL_n(\mathbb{R})$ é isomorfo ao grupo multiplicativo $\mathbb{R} \setminus \{0\}$.

Proposição 1.6.16. *Sejam* G *um grupo,* $H \subseteq G$ *um subgrupo e* $N \trianglelefteq G$ *um subgrupo normal. Então* HN *é um subgrupo de* G *e* $H \cap N$ *é um subgrupo normal de* H.

Demonstração: Mostramos primeiramente que HN é um subgrupo de G. Tem-se $e = ee \in HN$, pelo que $HN \neq \emptyset$. Sejam $h, k \in H$ e $n, m \in N$. Então $hk^{-1} \in H$, $nm^{-1} \in N$ e $Nk^{-1} = k^{-1}N$. Portanto $(hn)(km)^{-1} = hnm^{-1}k^{-1} \in hNk^{-1} = hk^{-1}N \subseteq HN$. Segue-se que HN é um subgrupo de G.

Mostramos agora que $H \cap N$ é um subgrupo normal de H. Por 1.4.11, $H \cap N$ é um subgrupo de G e então de H. Sejam $h \in H$ e $x \in H \cap N$. Então $hxh^{-1} \in H$ e $hxh^{-1} \in N$, pelo que $hxh^{-1} \in H \cap N$. Segue-se que $H \cap N$ é um subgrupo normal de H. □

Terminamos esta secção com dois teoremas conhecidos como *teoremas do isomorfismo.*

Teorema 1.6.17. *Sejam* G *um grupo,* $H \subseteq G$ *um subgrupo e* $N \trianglelefteq G$ *um subgrupo normal. Então um isomorfismo* $H/(H \cap N) \to HN/N$ *é dado por* $(H \cap N)x \mapsto Nx$.

Demonstração: Consideremos a inclusão $i\colon H \to HN$, $h \mapsto h$ e o epimorfismo canónico $\pi\colon HN \to HN/N$. Então i e π são homomorfismos de grupos. A composta $\pi \circ i\colon H \to HN/N$ é um epimorfismo. Com efeito, para $h \in H$ e $n \in N$, $hnN = hN = \pi \circ i(h)$. Seja $h \in H$. Tem-se $\pi \circ i(h) = N \Leftrightarrow Nh = N \Leftrightarrow h \in H \cap N$ e então $\mathrm{Ker}(\pi \circ i) = H \cap N$. O resultado segue do Teorema do homomorfismo. □

Teorema 1.6.18. *Sejam* G *um grupo e* N *e* H *subgrupos normais de* G *tais que* $H \subseteq N$. *Então* N/H *é um subgrupo normal de* G/H *e um isomorfismo* $(G/H)/(N/H) \to G/N$ *é dado por* $(N/H)Hx \mapsto Nx$.

Demonstração: Consideremos os epimorfismos canónicos $\pi_N\colon G \to G/N$ e $\pi_H\colon G \to G/H$. Como $H \subseteq N = \mathrm{Ker}(\pi_N)$, existe, por 1.6.13, um único homomorfismo $\bar{\pi}_N\colon G/H \to G/N$ com $\bar{\pi}_N \circ \pi_H = \pi_N$. Seja $x \in G$. Então $Hx \in \mathrm{Ker}(\bar{\pi}_N) \Leftrightarrow \bar{\pi}_N(Hx) = N \Leftrightarrow \bar{\pi}_N \circ \pi_H(x) = N \Leftrightarrow \pi_N(x) = N \Leftrightarrow Nx = N \Leftrightarrow x \in N$. Assim, enquanto conjuntos, $\mathrm{Ker}(\bar{\pi}_N) = \{Hx \mid x \in N\} = N/H$. Como as operações em $\mathrm{Ker}(\bar{\pi}_N) \subseteq G/H$ e N/H coincidem, temos $\mathrm{Ker}(\bar{\pi}_N) = N/H$ enquanto grupos e, em particular, que N/H é um subgrupo normal de G/H. O resultado segue do Teorema do homomorfismo. □

Exemplo 1.6.19. Sejam $m, n \in \mathbb{N} \setminus \{0\}$. Tem-se que $m\mathbb{Z}$ é um subgrupo de $n\mathbb{Z}$ se e só se n divide m. Neste caso $n\mathbb{Z}/m\mathbb{Z}$ é um subgrupo normal de $\mathbb{Z}_m$ e $\mathbb{Z}_m/(n\mathbb{Z}/m\mathbb{Z}) \cong \mathbb{Z}_n$.

1.7 Grupos cíclicos

Definição 1.7.1. Um grupo gerado por um elemento diz-se *cíclico.*

Nota 1.7.2. Os elementos de um grupo cíclico $G = \langle g \rangle$ são as potências g^k, $k \in \mathbb{Z}$. Um grupo cíclico é comutativo.

Exemplos 1.7.3. (i) O grupo aditivo $\mathbb{Z}$ é cíclico. Tem-se $\mathbb{Z} = \langle 1 \rangle$.
(ii) Para cada numero natural $n > 0$, $\mathbb{Z}_n$ é cíclico, gerado por $[1]_n = 1 + n\mathbb{Z}$.
(iii) Por 1.5.9, qualquer grupo de ordem prima é cíclico.
(iv) O grupo simétrico S_3 não é cíclico.

Proposição 1.7.4. *Sejam $G = \langle g \rangle$ um grupo cíclico e $\{e\} \neq H \subseteq G$ um subgrupo. Seja m o menor número natural positivo tal que $g^m \in H \setminus \{e\}$. Então $H = \langle g^m \rangle$.*

Demonstração: É claro que $\langle g^m \rangle \subseteq H$. Seja $n \in \mathbb{Z}$ tal que $g^n \in H$. Então existem $k \in \mathbb{Z}$ e $0 \leq r < m$ tais que $n = km + r$. Portanto $g^n = g^{km} g^r$. Como $g^{km} \in \langle g^m \rangle \subseteq H$, temos $g^r = g^n g^{-km} \in H$. Então $g^r = e$ e portanto $g^n = g^{km} \in \langle g^m \rangle$. □

Corolário 1.7.5. *Qualquer subgrupo de um grupo cíclico é cíclico.*

Corolário 1.7.6. *Os subgrupos de $\mathbb{Z}$ são os conjuntos $m\mathbb{Z}$, $m \in \mathbb{N}$.*

Corolário 1.7.7. *(Lema de Bézout) Sejam $a, b \in \mathbb{Z}$, não ambos iguais a 0, e $d = \mathrm{mdc}(a, b)$. Então existem $u, v \in \mathbb{Z}$ tais que $au + bv = d$.*

Demonstração: Como $d = \mathrm{mdc}(a, b)$, existem números primos entre si $a', b' \in \mathbb{Z}$ tais que $a = da'$ e $b = db'$. Por 1.7.6, o subgrupo $\langle a', b' \rangle$ de $\mathbb{Z}$ é gerado por um elemento $m \in \mathbb{N}$, que então é um divisor comum de a' e b'. Como a' e b' são primos entre si, $m = 1$. Segue-se que $\langle a', b' \rangle = \mathbb{Z}$ e então que existem $u, v \in \mathbb{Z}$ tais que $a'u + b'v = 1$. Multiplicando por d obtém-se $au + bv = d$. □

Teorema 1.7.8. *Seja $G = \langle g \rangle$ um grupo cíclico. Se G é infinito, então um isomorfismo $\mathbb{Z} \to G$ é dado por $k \mapsto g^k$. Se G é finito, então um isomorfismo $\mathbb{Z}_{|g|} \to G$ é dado por $k + |g|\mathbb{Z} \mapsto g^k$.*

Demonstração: Consideremos o epimorfismo $\phi \colon \mathbb{Z} \to G$ dado por $\phi(k) = g^k$. Por 1.7.6, existe $n \in \mathbb{N}$ tal que $\mathrm{Ker}(\phi) = n\mathbb{Z}$. Pelo Teorema do homomorfismo, um isomorfismo $f \colon \mathbb{Z}/n\mathbb{Z} \to G$ é dado por $k + n\mathbb{Z} \mapsto g^k$. Se G é finito, f é o isomorfismo procurado pois, neste caso, $n = |\mathbb{Z}/n\mathbb{Z}| = |g|$ e $\mathbb{Z}/n\mathbb{Z} = \mathbb{Z}_{|g|}$. Se G é infinito, então $n = 0$ e $\mathrm{Ker}(\phi) = n\mathbb{Z} = \{0\}$, pelo que o epimorfismo ϕ é um isomorfismo. □

Corolário 1.7.9. *Seja $G = \langle g \rangle$ um grupo cíclico finito. Então*

(i) $G = \{e, g, \dots, g^{|g|-1}\}$;

(ii) para todo o $m \in \mathbb{Z}$, $g^m = e$ se e só se $m \in |g|\mathbb{Z}$;

(iii) a ordem de G é o menor inteiro positivo m tal que $g^m = e$.

Demonstração: Seja $f\colon \mathbb{Z}_{|g|} \to G$ o isomorfismo dado por $f(k + |g|\mathbb{Z}) = g^k$.

(i) Tem-se $G = Im(f) = \{f(\bar{0}), \dots, f(\overline{|g|-1})\} = \{e, g, \dots, g^{|g|-1}\}$.

(ii) Para todo o $m \in \mathbb{Z}$,

$$g^m = e \Leftrightarrow f(m + |g|\mathbb{Z}) = f(|g|\mathbb{Z}) \Leftrightarrow m + |g|\mathbb{Z} = |g|\mathbb{Z} \Leftrightarrow m \in |g|\mathbb{Z}.$$

(iii) segue imediatamente de (ii). □

Proposição 1.7.10. *Sejam $G = \langle g \rangle$ um grupo cíclico finito.*

(a) Para todo o $k \in \mathbb{Z} \setminus \{0\}$, $|g^k| = \dfrac{|g|}{\mathrm{mdc}(|g|, k)}$. Em particular, $G = \langle g^k \rangle$ se e só se a ordem de G e k são primos entre si.

(b) Para cada divisor $d \geq 1$ da ordem de G existe exactamente um subgrupo de G de ordem d. Este subgrupo é $\langle g^{\frac{|g|}{d}} \rangle$.

Demonstração: Seja $n = |g| = |G|$.

(a) Seja $d = \mathrm{mdc}(k, n)$. Escrevemos $n = n'd$ e $k = k'd$ onde $\mathrm{mdc}(n', k') = 1$. Por 1.7.9 (iii), $|g^k|$ é o menor inteiro positivo m tal que $g^{km} = e$. Por 1.7.9 (ii), isto implica que $|g^k|$ é o menor inteiro positivo m tal que $km \in n\mathbb{Z}$. Como $n' \geq 1$ e $g^{kn'} = g^{k'n} = e$ temos $|g^k| \leq n'$. Como $n = n'd$ divide $|g^k|k = |g^k|k'd$ obtemos que n' divide $|g^k|k'$. Como $\mathrm{mdc}(n', k') = 1$ podemos concluir que n' divide $|g^k|$ e portanto que $|g^k| = n' = \dfrac{n}{\mathrm{mdc}(n, k)}$.

(b) O único subgrupo de G de ordem 1 é o subgrupo trivial $\{e\} = \langle g^{|g|} \rangle$. Seja $d > 1$ um divisor de $|g|$. Seja $k = \dfrac{|g|}{d}$. Então $\langle g^k \rangle$ é um subgrupo de G e tem-se $|g^k| = \dfrac{|g|}{\mathrm{mdc}(|g|, k)} = \dfrac{|g|}{k} = d$. Seja $H \leq G$ com $|H| = d$. Seja m o menor número natural positivo tal que $g^m \in H \setminus \{e\}$. Por 1.7.4, $H = \langle g^m \rangle$. Por 1.7.9(i), $0 < m < |g|$. Tem-se $d = |g^m| = \dfrac{|g|}{\mathrm{mdc}(|g|, m)} = \dfrac{|g|}{m}$ e portanto $m = \dfrac{|g|}{d} = k$. Segue-se que $H = \langle g^k \rangle$. Logo existe exactamente um subgrupo de G de ordem d e este é $\langle g^k \rangle$. □

Corolário 1.7.11. *Os subgrupos de um grupo cíclico finito $G = \langle g \rangle$ são os grupos da forma $\langle g^{\frac{|g|}{d}} \rangle$, onde $d \geq 1$ é um divisor de $|g|$.*

Definição 1.7.12. O *produto directo* dos grupos $G_1, \ldots, G_n$ é o grupo cujo conjunto subjacente é o produto cartesiano $G_1 \times \cdots \times G_n$ e cuja operação é dada por

$$(g_1, \ldots, g_n) \cdot (h_1, \ldots, h_n) = (g_1 h_1, \ldots, g_n h_n).$$

Verifica-se facilmente que o produto directo dos grupos $G_1, \ldots, G_n$ é de facto um grupo. Este grupo é denotado por $\prod\limits_{i=1}^{n} G_i$ ou por $G_1 \times \cdots \times G_n$.

Exemplo 1.7.13. O exemplo $\mathbb{Z}_2 \times \mathbb{Z}_2$ mostra que o produto directo de dois grupos cíclicos não é, em geral, um gupo cíclico. Com efeito, $\mathbb{Z}_2 \times \mathbb{Z}_2$ tem dois subgrupos diferentes de ordem 2, nomeadamente $\mathbb{Z}_2 \times \{[0]_2\}$ e $\{[0]_2\} \times \mathbb{Z}_2$, e um grupo cíclico não pode ter mais do que um subgrupo de uma dada ordem.

Proposição 1.7.14. *Sejam $n_1, \ldots n_k \geq 1$ inteiros. Então o produto directo $\prod\limits_{i=1}^{k} \mathbb{Z}_{n_i}$ é cíclico se e só os inteiros $n_1, \ldots n_k$ são dois a dois primos entre si. Neste caso um isomorfismo $\mathbb{Z}_{n_1 \cdots n_k} \to \prod\limits_{i=1}^{k} \mathbb{Z}_{n_i}$ é dado por $m + n_1 \cdots n_k \mathbb{Z} \mapsto (m + n_1\mathbb{Z}, \ldots, m + n_k\mathbb{Z})$.*

Demonstração: Suponhamos primeiramente os inteiros $n_1, \ldots n_k$ são dois a dois primos entre si. Consideremos o homomorfismo $f \colon \mathbb{Z} \to \prod\limits_{i=1}^{k} \mathbb{Z}_{n_i}$ definido por

$$f(m) = (m + n_1\mathbb{Z}, \ldots, m + n_k\mathbb{Z}).$$

É claro que $n_1 \cdots n_k\mathbb{Z} \subseteq \mathrm{Ker}(f)$. Por outro lado, seja $m \in \mathrm{Ker}(f)$. Então existem $u_1, \ldots, u_k \in \mathbb{Z}$ tais que $m = n_1 u_1 = \cdots = n_k u_k$, ou seja, cada n_i divide m. Como os n_i são dois a dois primos entre si, o produto $n_1 \cdots n_k$ divide m. Logo $m \in n_1 \cdots n_k\mathbb{Z}$ e $\mathrm{Ker}(f) = n_1 \cdots n_k\mathbb{Z}$. Pelo teorema 1.6.13, $\bar{f} \colon \mathbb{Z}_{n_1 \cdots n_k} \to \prod\limits_{i=1}^{k} \mathbb{Z}_{n_i}$, $\bar{f}(m + n_1 \cdots n_k\mathbb{Z}) = (m + n_1\mathbb{Z}, \ldots, m + n_k\mathbb{Z})$ é um monomorfismo. Como $|\mathbb{Z}_{n_1 \cdots n_k}| = n_1 \cdots n_k = |\prod\limits_{i=1}^{k} \mathbb{Z}_{n_i}|$, $\bar{f}$ é de facto um isomorfismo e $\prod\limits_{i=1}^{k} \mathbb{Z}_{n_i}$ é cíclico.

Suponhamos agora que os inteiros $n_1, \ldots n_k$ não são dois a dois primos entre si. Então existem $i \neq j \in \{1, \ldots, k\}$ tais que n_i e n_j têm um divisor comum $d > 1$. Como $\mathbb{Z}_{n_i}$ e $\mathbb{Z}_{n_j}$ são cíclicos, existem subgrupos $U_i \leq \mathbb{Z}_{n_i}$ e $V_j \leq \mathbb{Z}_{n_j}$ de ordem d. Pomos $U_l = \{n_l\mathbb{Z}\}$ para $l \neq i$ e $V_l = \{n_l\mathbb{Z}\}$ para $l \neq j$. Então $\prod\limits_{l=1}^{n} U_l$ e $\prod\limits_{l=1}^{n} V_l$ são dois subgrupos diferentes de ordem d de $\prod\limits_{i=1}^{k} \mathbb{Z}_{n_i}$. Logo $\prod\limits_{i=1}^{k} \mathbb{Z}_{n_i}$ não é cíclico. $\square$

1.8 Grupos simétricos

Recorde que para um conjunto $X \neq \emptyset$, $S(X) = \{f : X \to X \ : \ f \text{ bijeção}\}$ é um grupo relativamente à composição, chamado grupo simétrico. Recorde ainda que S_n designa o grupo simétrico $S(\{1, 2, \dots, n\})$.

Teorema 1.8.1. *(Teorema de Cayley) Cada grupo G é isomorfo a um subgrupo do grupo simétrico $S(G)$.*

Demonstração: Para $g \in G$ seja $\lambda_g \colon G \to G$ a função definida por $\lambda_g(x) = gx$. Para quaisquer $g, h, x \in G$, $\lambda_{gh}(x) = ghx = g\lambda_h(x) = \lambda_g(\lambda_h(x)) = \lambda_g \circ \lambda_h(x)$. Segue-se que cada λ_g é bijectiva com função inversa $\lambda_{g^{-1}}$ e que a função $f \colon G \to S(G)$, $f(g) = \lambda_g$ é um homomorfismo. Seja $g \in Ker(f)$. Então $f(g) = \lambda_g = id_G$. Logo $g^2 = \lambda_g(g) = g = eg$. Pelas leis do corte, $g = e$ e temos $\mathrm{Ker}(f) = \{e\}$. Segue-se que f é um monomorfismo e portanto que $G \cong \mathrm{Im}(f)$. □

Corolário 1.8.2. *Cada grupo finito G de ordem n é isomorfo a um subgrupo de S_n.*

Demonstração: Seja $\alpha : G \to \{1, 2, \dots n\}$ uma bijeção. Verifica-se que $\Psi : S(G) \to S_n$ dada por $\Psi(f) = \alpha \circ f \circ \alpha^{-1}$ é um isomorfismo de grupos (nota: isto não utiliza a estrutura de grupo de G, tal isomorfismo existe para qualquer conjunto com n elementos). Como, pelo Teorema de Cayley, G é subgrupo de $S(G)$ e como Ψ é um isomorfismo de grupos, podemos concluir que G é isomormorfo a um subgrupo de S_n. □

Notação 1.8.3. Uma permutação $\sigma \in S_n$ é muitas vezes representada sob a forma

$$\begin{pmatrix} 1 & 2 & \cdots & n \\ \sigma(1) & \sigma(2) & \cdots & \sigma(n) \end{pmatrix}.$$

Observação 1.8.4. Um monomorfismo $S_n \to S_{n+1}$ é dado por

$$\sigma \mapsto \begin{pmatrix} 1 & \cdots & n & n+1 \\ \sigma(1) & \cdots & \sigma(n) & n+1 \end{pmatrix}.$$

Por conseguinte, S_n é isomorfo ao subgrupo de S_{n+1} das permutações α com $\alpha(n+1) = n+1$.

Proposição 1.8.5. $|S_n| = n!$

Definição 1.8.6. Uma permutação $\sigma \in S_n$ diz-se um *cíclo* se existem $k, i_1, \dots, i_k \in \{1, \dots, n\}$ tais que $\sigma(i_j) = i_{j+1}$ para $1 \leq j < k$, $\sigma(i_k) = i_1$ e $\sigma(i) = i$ para $i \notin \{i_1, \dots, i_k\}$. O cíclo assim definido é denotado por $(i_1, \dots, i_k)$. Aos cíclos da forma (i, j) com $i \neq j \in \{1, \dots, n\}$ chama-se também *transposições*. Dois cíclos $(i_1, \dots, i_k)$ e $(j_1, \dots, j_l)$ dizem-se *disjuntos* se $\{i_1, \dots, i_k\} \cap \{j_1, \dots, j_l\} = \emptyset$.

Observações 1.8.7. (i) A identidade de $\{1,\ldots,n\}$ é um cíclo. Para cada $i \in \{1,\ldots,n\}$, $id_{\{1,\ldots,,n\}} = (i)$.

(ii) Para quaisquer k números distintos $i_1,\ldots i_k \in \{1,\ldots,n\}$, $|(i_1,\ldots,i_k)| = k$.

(iii) Se $\alpha,\beta \in S_n$ são cíclos disjuntos, então $\alpha\beta = \beta\alpha$. Logo se $\alpha_1,\ldots\alpha_l \in S_n$ são cíclos dois a dois disjuntos, então $|\alpha_1\cdots\alpha_l| = \mathrm{mmc}(|\alpha_1|,\ldots,|\alpha_l|)$.

(iv) Para cada transposição $\tau \in S_n$, $\tau^2 = id$.

Proposição 1.8.8. *Cada permutação $\sigma \in S_n \setminus \{id\}$ pode ser factorizada em cíclos dois a dois disjuntos de $S_n \setminus \{id\}$.*

Demonstração: Seja $\sigma \in S_n \setminus \{id\}$. Para $i \in \{1,\ldots,n\}$, seja

$$k_i = \min\{k \in \{1,\ldots,n!\} \,|\, \sigma^k(i) = i\}.$$

Note-se que este mínimo existe pois $\sigma^{n!} = id$ pelo Exercício 33. Definimos os números $j_1,\ldots,j_m \in \{1,\ldots,n\}$ recursivamente como se segue: Enquanto tal i existe, j_l é o menor

$$i \in \{1,\ldots,n\} \setminus \{j_1,\sigma(j_1),\ldots,\sigma^{k_{j_1}-1}(j_1),\ldots,j_{l-1},\sigma(j_{l-1}),\ldots,\sigma^{k_{j_{l-1}}-1}(j_{l-1})\}$$

tal que $\sigma(i) \neq i$. Como $\sigma \neq id$, j_1 existe. Como $\{1,\ldots,n\}$ é finito, o processo pára depois de um número finito, m, de iterações. Para cada $l \in \{1,\ldots,m\}$, $(j_l,\sigma(j_l),\ldots,\sigma^{k_{j_l}-1}(j_l))$ é um cíclo em $S_n \setminus \{id\}$. Sejam $l,r \in \{1,\ldots,m\}$, $0 \leq k < k_{j_l}$ e $0 \leq s < k_{j_r}$ tais que $\sigma^k(j_l) = \sigma^s(j_r)$. Então $j_r = \sigma^{k_{j_r}}(j_r) \in \{j_l,\sigma(j_l),\ldots,\sigma^{k_{j_l}-1}(j_l)\}$, pelo que $r \leq l$. Do mesmo modo temos $l \leq r$ e então $r = l$. Segue-se que os cíclos $(j_l,\sigma(j_l),\ldots,\sigma^{k_{j_l}-1}(j_l))$ são dois a dois disjuntos. Seja

$$\psi = (j_1,\sigma(j_1),\ldots,\sigma^{k_{j_1}-1}(j_1))\cdots(j_m,\sigma(j_m),\ldots,\sigma^{k_{j_m}-1}(j_m)).$$

Temos $\psi(\sigma^k(j_l)) = \sigma^{k+1}(j_l)$ e $\sigma(i) = i = \psi(i)$ para

$$i \notin \{j_1,\sigma(j_1),\ldots,\sigma^{k_{j_1}-1}(j_1),\ldots,j_m,\sigma(j_m),\ldots,\sigma^{k_{j_m}-1}(j_m)\}.$$

Logo $\sigma = \psi$. □

Corolário 1.8.9. *S_n é gerado pelos cíclos.*

Exemplo 1.8.10. Consideremos a permutação $\sigma \in S_6$ dada por

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 1 & 5 & 2 & 6 & 3 & 4 \end{pmatrix}.$$

Tem-se $\sigma = (2,5,3)(4,6)$.

Nota 1.8.11. É possível mostrar que a factorização de uma permutação $\sigma \in S_n \setminus \{id\}$ em cíclos dois a dois disjuntos de $S_n \setminus \{id\}$ é única a menos da ordem dos factores (exercício).

Proposição 1.8.12. *Sejam $i_1, \ldots, i_k \in \{1, \ldots, n\}$ número distintos com $k \geq 3$. Então $(i_1, \ldots, i_k) = (i_1, i_k) \cdots (i_1, i_2)$.*

Demonstração: Tem-se

$$(i_1, i_k) \cdots (i_1, i_2)(i_1) = (i_1, i_k) \cdots (i_1, i_3)(i_2) = i_2,$$

$$(i_1, i_k) \cdots (i_1, i_2)(i_k) = (i_1, i_k)(i_k) = i_1,$$

$$\begin{aligned}(i_1, i_k) \cdots (i_1, i_2)(i_l) &= (i_1, i_k) \cdots (i_1, i_l)(i_l) \\ &= (i_1, i_k) \cdots (i_1, i_{l+1})(i_1) \\ &= (i_1, i_k) \cdots (i_1, i_{l+2})(i_{l+1}) \\ &= i_{l+1}\end{aligned}$$

para $1 < l < k$ e $(i_1, i_k) \cdots (i_1, i_2)(i) = i$ para $i \notin \{i_1, \ldots, i_k\}$. □

Corolário 1.8.13. *S_n é gerado pelas transposições.*

Definição 1.8.14. Seja $\sigma \in S_n$ uma permutação. Uma *inversão* em σ é um par $(i, j) \in \{1, \ldots, n\} \times \{1, \ldots, n\}$ tal que $i < j$ e $\sigma(i) > \sigma(j)$. O *sinal* de σ, $\operatorname{sgn}(\sigma)$, é 1 se existe um número par de inversões em σ e -1 caso contrário. Uma permutação diz-se *par (ímpar)* se tem sinal 1 (-1).

Observações 1.8.15. (i) Se m é o numéro de inversões em $\sigma \in S_n$, então $\operatorname{sgn}(\sigma) = (-1)^m$.
(ii) O sinal de qualquer transposição é -1.

Proposição 1.8.16. *O sinal é um homomorfismo de S_n para o grupo multiplicativo $\{1, -1\}$.*

Demonstração: Sejam $\alpha, \beta \in S_n$, k o número de inversões em α e l o número de inversões em β. Um par $(i, j) \in \{1, \ldots, n\} \times \{1, \ldots, n\}$ com $i < j$ é uma inversão em $\alpha\beta$ se e só se satisfaz uma das condições seguintes:

(a) (i, j) é uma inversão em β mas $(\beta(j), \beta(i))$ não é uma inversão em α;

(b) (i, j) não é uma inversão em β mas $(\beta(i), \beta(j))$ é uma inversão em α.

Seja r o número de pares (i, j) com $i < j$ que satisfazem a condição (a) e seja s o número de pares (i, j) com $i < j$ que satisfazem a condição (b). Então $\operatorname{sgn}(\alpha\beta) = (-1)^{r+s}$. Seja m o número de inversões (i, j) em β tais que $(\beta(j), \beta(i))$ é uma inversão em α. Então $l = r + m$. Também temos $k = s + m$. Com efeito, os pares (i, j) com $i < j$ que satisfazem a condição (b) estão em correspondência bijectiva com as inversões (x, y) em α com $\beta^{-1}(x) < \beta^{-1}(y)$, pelo que o número destas inversões em α é s. E as inversões (i, j) em

β tais que $(\beta(j), \beta(i))$ é uma inversão em α estão em correspondência bijectiva com as inversões (x, y) em α com $\beta^{-1}(y) < \beta^{-1}(x)$, pelo que o número destas inversões em α é m. Segue-se que $\mathrm{sgn}(\alpha\beta) = (-1)^{r+s} = (-1)^{l+k-2m} = (-1)^l(-1)^k(-1)^{-2m} = (-1)^l(-1)^k = (-1)^k(-1)^l = \mathrm{sgn}(\alpha)\mathrm{sgn}(\beta)$. □

Observação 1.8.17. Pela proposição precedente, um produto de um número par de transposições tem sinal 1 e um produto de um número ímpar de transposições tem sinal -1. Segue-se que uma permutação não pode ao mesmo tempo ser factorizada num número par e num número ímpar de transposições e que uma permutação é par se e só se ela pode ser factorizada num número par de transposições. Em particular, pela Proposição 1.8.12, um cíclo de ordem par é ímpar e um cíclo de ordem ímpar é par.

Proposição 1.8.18. *Sejam $i_1, \ldots, i_k \in \{1, \ldots, n\}$ k números distintos e seja σ o cíclo $(i_1, \ldots, i_k)$. Tem-se* $\mathrm{sgn}(\sigma) = (-1)^{k-1}$.

Observação 1.8.19. Em geral, para uma permutação qualquer $\sigma \in S_n$, não temos $\mathrm{sgn}(\sigma) = (-1)^{|\sigma|-1}$. Por exemplo, a permutação $\sigma = (1, 2)(3, 4, 5, 6, 7, 8)$ de S_8 têm ordem 6 mas $\mathrm{sgn}(\sigma) = 1 \neq (-1)^5$.

Capítulo 2

Anéis

2.1 Conceitos básicos

Definição 2.1.1. Um *anel* é um triplo $(A, +, \cdot)$ em que A é um conjunto e $+$ e $\cdot$ são operações binárias em A tais que

- $(A, +)$ é um grupo abeliano;
- $(A, \cdot)$ é um monóide;
- para quaisquer $a, b, c \in A$, $a \cdot (b + c) = (a \cdot b) + (a \cdot c)$ e $(a + b) \cdot c = (a \cdot c) + (b \cdot c)$ (*distributividade* de $\cdot$ em relação a $+$).

A operação $+$ diz-se a *adição* do anel e a operação $\cdot$ diz-se a *multiplicação* do anel. Muitas vezes indica-se um anel pelo símbolo do conjunto subjacente, isto é, escreve-se simplesmente A em vez de $(A, +, \cdot)$. O elemento neutro do *grupo aditivo* $(A, +)$ de um anel $A = (A, +, \cdot)$ é denotado por 0. O elemento neutro do *monóide multiplicativo* $(A, \cdot)$ de A é chamado *identidade* de A e é denotado por 1. O *simétrico* de um elemento a de um anel A é o inverso de a no grupo aditivo de A e é denotado por $-a$. Se a é invertível no monóide multiplicativo de A, o *inverso* de a é o inverso de a em $(A, \cdot)$ e é denotado por a^{-1}. Um elemento invertível no monóide multiplicativo de A diz-se uma *unidade* de A. Omitiremos muitas vezes o símbolo da multipicação e escreveremos ab em vez de $a \cdot b$. Usaremos as convenções habituais de omissão de parênteses e escreveremos, por exemplo, $ab + c$ em vez de $(ab) + c$ e $-ab$ em vez de $-(ab)$. Um anel diz-se *comutativo* se a sua multiplicação é comutativa.

Nota 2.1.2. Alguns autores não exigem a existência de um elemento neutro para a multiplicação na definição de um anel. Num tal contexto, a nossa definição de anel corresponde à noção de *anel unitário* ou *anel com identidade*.

Exemplos 2.1.3. (i) $\mathbb{Z}$, $\mathbb{Q}$ e $\mathbb{R}$ são anéis comutativos relativamente à adição e à multiplicação habituais.

(ii) Para qualquer inteiro $n \geq 1$, o grupo abeliano $\mathbb{Z}_n$ é um anel comutativo relativamente à multiplicação dada por $(k + n\mathbb{Z}) \cdot (l + n\mathbb{Z}) = kl + n\mathbb{Z}$.

(iii) Para cada natural $n \geq 1$, o conjunto $\mathcal{M}_{n\times n}(\mathbb{R})$ das matrizes reais $n \times n$ é um anel relativamente à adição e à multiplicação de matrizes.

(iv) O *produto directo* $A_1 \times \cdots \times A_n$ dos anéis $A_1, \ldots, A_n$ é o anel cujo conjunto subjacente é o produto cartesiano $A_1 \times \cdots \times A_n$ e cujas operações $+$ e $\cdot$ são definidas componente por componente.

(v) O conjunto $\{0\}$ admite uma única estrutura de anel. Note-se que neste anel, $1 = 0$.

Proposição 2.1.4. *Sejam A um anel e $x, y \in A$. Então*

(i) $0x = x0 = 0$*;*

(ii) $(-x)y = x(-y) = -xy$*;*

(iii) $(-x)(-y) = xy$.

Demonstração: (i) Tem-se $0x = (0 + 0)x = 0x + 0x$ e portanto $0 = 0x - 0x = 0x$. Do mesmo modo, $x0 = 0$.

(ii) Tem-se $xy + (-x)y = (x + (-x))y = 0y = 0$ e portanto $-xy = (-x)y$. Do mesmo modo, $-xy = x(-y)$.

(iii) Tem-se $(-x)(-y) = -x(-y) = -(-xy) = xy$. □

Observação 2.1.5. Pela propriedade (ii) da proposição precedente, $(-1)x = x(-1) = -x$ para qualquer elemento x de um anel.

Proposição 2.1.6. *Sejam A um anel, $n, m \geq 1$ inteiros e $x_1, \ldots, x_n, y_1, \ldots, y_m \in A$. Então*

$$\left(\sum_{i=1}^{n} x_i\right) \cdot \left(\sum_{j=1}^{m} y_j\right) = \sum_{1\leq i\leq n,\ 1\leq j\leq m} x_i y_j.$$

Demonstração: Exercício. □

Proposição 2.1.7. *Sejam A um anel, $n \in \mathbb{N}$ e $a, b \in A$ tais que $ab = ba$. Então*

$$(a + b)^n = \sum_{i=0}^{n} \binom{n}{i} a^{n-i} b^i.$$

Demonstração: Exercício. □

Definição 2.1.8. Um subconjunto B de um anel A diz-se um *subanel* de A se $1 \in B$ e para quaisquer $x, y \in B$, $x - y \in B$ e $xy \in B$.

Observação 2.1.9. Um subanel B de um anel A é um anel relativamente à adição e à multiplicação de A.

Exemplos 2.1.10. (i) Qualquer anel é sempre um subanel de si próprio.

(ii) O único subanel de $\mathbb{Z}$ é $\mathbb{Z}$.

(iii) O único subanel de $\mathbb{Z}_n$ é $\mathbb{Z}_n$.

(iv) $\mathbb{Q}$ é um subanel de $\mathbb{R}$.

(v) Os matrizes reais diagonais $n \times n$ formam um subanel de $\mathcal{M}_n(\mathbb{R})$.

Definição 2.1.11. Um aplicação entre dois anéis $f\colon A \to B$ diz-se um *homomorfismo de anéis* se $f(1) = 1$ e se para quaisquer dois elements $x, y \in A$, $f(x + y) = f(x) + f(y)$ e $f(xy) = f(x)f(y)$. Um homomorfismo de anéis diz-se um *monomorfismo* (*epimorfismo, isomorfismo*) se é injectivo (sobrejectivo, bijectivo). Um homomorfismo (isomorfismo) de anéis $f\colon A \to A$ diz-se um *endomorfismo* (*automorfismo*) de anéis. Dois anéis A e B dizem-se *isomorfos*, $A \cong B$, se existe um isomorfismo de anéis entre eles.

Observações 2.1.12. (i) Um homomorfismo de anéis é um homomorfismo dos grupos aditivos. Em particular $f(0) = 0$.

(ii) O núcleo $\mathrm{Ker} f$ de um homomorfismo de anéis $f\colon A \to B$ é o seu núcleo enquanto homomorfismo de grupos aditivos, isto é, $Ker(f) = \{a \in A \mid f(a) = 0\}$.

(ii) Um homomorfismo de anéis $f\colon A \to B$ é um monomorfismo de anéis se e só se é um monomorfismo de grupos aditivos e isto é caso se e só se $\mathrm{Ker}(f) = \{0\}$.

Exemplos 2.1.13. (i) Se B é um subanel do anel A, então a inclusão $B \to A$, $x \mapsto x$ é um monomorfismo de anéis.

(ii) Para qualquer anel A, id_A é um automorfismo de anéis.

(iv) O epimorfismo canónico $\mathbb{Z} \to \mathbb{Z}_n$, $k \mapsto k + n\mathbb{Z}$ é um epimorfismo de anéis.

Proposição 2.1.14. *A composta de dois homomorfismos de anéis $f\colon A \to B$ e $g\colon B \to C$ é um homomorfismo de anéis.*

Demonstração: A composta $g \circ f\colon A \to C$ é um homorfismo de grupos. Como $g \circ f(1) = g(f(1)) = g(1) = 1$ e $g \circ f(xy) = g(f(xy)) = g(f(x)f(y)) = g(f(x))g(f(y)) = g \circ f(x) g \circ f(y)$ para todos os $x, y \in A$, $g \circ f$ é um homomorfismo de anéis. □

Proposição 2.1.15. *A função inversa de um isomorfismo de anéis $f\colon A \to B$ é um isomorfismo de anéis.*

Demonstração: Por 1.3.8, f^{-1} é um isomorfismo de grupos. Como $f(1) = 1$, $1 = f^{-1}(f(1)) = f^{-1}(1)$. Para quaisquer $x, y \in B$, $f(f^{-1}(xy)) = xy = f(f^{-1}(x))f(f^{-1}(y)) = f(f^{-1}(x)f^{-1}(y))$. Como f é um monomorfismo, isto implica que $f^{-1}(xy) = f^{-1}(x)f^{-1}(y)$. Segue-se que f^{-1} é um homomorfismo de anéis e então um isomorfismo de anéis. □

Proposição 2.1.16. *Sejam $f\colon A \to B$ um homomorfismo de anéis, X um subanel de A e Y um subanel de B. Então $f(X)$ é um subanel de B e $f^{-1}(Y)$ é um subanel de A.*

Demonstração: Como $1 \in X$, $1 = f(1) \in f(X)$. Sejam $x, y \in X$. Então $x - y, xy \in X$. Logo $f(x) - f(y) = f(x - y) \in f(X)$ e $f(x)f(y) = f(xy) \in f(X)$. Segue-se que $f(X)$ é um subanel de B. Como $f(1) = 1 \in Y$, $1 \in f^{-1}(Y)$. Sejam $x, y \in f^{-1}(Y)$. Então $f(x-y) = f(x)-f(y) \in Y$ e $f(xy) = f(x)f(y) \in Y$. Logo $x-y \in f^{-1}(Y)$ e $xy \in f^{-1}(Y)$. Segue-se que $f^{-1}(Y)$ é um subanel de A. □

2.2 Ideais e anéis quociente

Definição 2.2.1. Um *ideal* de um anel A é um subgrupo I do grupo aditivo de A tal que para quaisquer $a \in A$ e $x \in I$, $ax \in I$ e $xa \in I$.

Observações 2.2.2. (i) Como o grupo aditivo de um anel é abeliano, qualquer ideal de um anel é um subgrupo normal do anel.

(ii) Se um ideal I de um anel A contém o elemento 1, então $I = A$. Com efeito, para qualquer $a \in A$, $a = 1a \in I$.

Exemplos 2.2.3. (i) Em qualquer anel A, $\{0\}$ e A são ideais.

(ii) Para $n \in \mathbb{Z}$, $n\mathbb{Z}$ é um ideal em $\mathbb{Z}$.

(iii) Sejam A e B dois anéis, I um ideal de A e J um ideal de B. Então $I \times J$ é um ideal em $A \times B$.

Proposição 2.2.4. *Sejam $f\colon A \to B$ um homomorfismo de anéis, I um ideal de A e J um ideal de B. Então $f(I)$ é um ideal de* $\mathrm{Im}(f)$ *e $f^{-1}(J)$ é um ideal de A. Em particular,* $\mathrm{Ker}(f) = f^{-1}(\{0\})$ *é um ideal de A.*

Demonstração: Por 1.6.5, $f(I)$ é um subgrupo do grupo aditivo de $\mathrm{Im}(f)$ e $f^{-1}(J)$ é um subgrupo do grupo aditivo de A. Sejam $a \in A$ e $x \in I$. Então $f(a)f(x) = f(ax) \in f(I)$ e $f(x)f(a) = f(xa) \in f(I)$. Segue-se que $f(I)$ é um ideal de $\mathrm{Im}(f)$. Sejam $a \in A$ e $x \in f^{-1}(J)$. Então $f(ax) = f(a)f(x) \in J$ e $f(xa) = f(x)f(a) \in J$, pelo que $ax \in f^{-1}(J)$ e $xa \in f^{-1}(J)$. Segue-se que $f^{-1}(J)$ é um ideal de A. □

Proposição 2.2.5. *Sejam A um anel e $(I_k)_{k\in K}$ uma familia não vazia de ideais de A. Então $\bigcap_{k\in K} I_k$ é um ideal de A.*

Demonstração: Por 1.4.11, $\bigcap_{k\in K} I_k$ é um subgrupo do grupo aditivo de A. Sejam $a \in A$ e $x \in \bigcap_{k\in K} I_k$. Então $x \in I_k$ para todo o $k \in K$. Logo $ax \in I_k$ e $xa \in I_k$ para todo o $k \in K$. Segue-se que ax, $xa \in \bigcap_{k\in K} I_k$ e que $\bigcap_{k\in K} I_k$ é um ideal de A. □

Definição 2.2.6. Sejam A um anel e $X \subseteq A$ um subconjunto. O *ideal gerado por* X, (X), é a intersecção dos ideais de A que contêm X. Se $X = \{x_1, \ldots, x_n\}$, escrevemos também $(x_1, \ldots, x_n)$ em vez de (X) e falamos do *ideal de A gerado pelos elementos* $x_1, \ldots, x_n$.

Proposição 2.2.7. *Sejam A um anel e $X \subseteq A$ um subconjunto. Então os elementos de (X) são o elemento 0 e as somas finitas formadas a partir dos elementos da forma axb, onde $a, b \in A$ e $x \in X$.*

Demonstração: Seja I o subconjunto de A cujos elementos são o elemento 0 e as somas finitas formadas a partir dos elementos de A da forma axb, onde $a, b \in A$ e $x \in X$. Então I é um ideal de A e $X \subseteq I$. Logo $(X) \subseteq I$. Por outro lado, qualquer elemento de I pertence necessariamente a qualquer ideal de A que contém X. Logo $I \subseteq (X)$. □

Exemplos 2.2.8. (i) Em qualquer anel A, $(\emptyset) = \{0\}$.

(ii) Num anel comutativo A, tem-se $(a) = aA = \{ax \,|\, x \in A\}$ para todo o $a \in A$. Em particular, em $\mathbb{Z}$, $(n) = n\mathbb{Z}$. Em $\mathbb{Z}_4$, $([2]) = [2]\mathbb{Z}_2 = \{[0], [2]\}$.

Nota 2.2.9. Sejam A um anel e I e J ideais de A. Então a soma $I + J = \{i + j \,|\, i \in I,\ j \in J\}$ também é um ideal de A e tem-se $(I \cup J) = I + J$.

Definição 2.2.10. Um ideal I de um anel A diz-se *principal* se existe um elemento $a \in A$ tal que $I = (a)$.

Exemplos 2.2.11. (i) Seja A um anel cujo grupo aditivo é cíclico. Então qualquer subgrupo de A é um ideal principal. Com efeito, seja $A = \langle a \rangle$ e consideremos um inteiro k e o subgrupo $I = \langle ka \rangle$. Então a^2 é um múltiplo de a e isto implica que I é um ideal de A. Como $(ka) \subseteq I = \langle ka \rangle \subseteq (ka)$, $I = (ka)$. Em particular, todos os subgrupos de $\mathbb{Z}$ e $\mathbb{Z}_n$ são ideais principais.

Lema 2.2.12. *Sejam A um anel, I um ideal de A e $a, a', b, b' \in A$ tais que $a - a', b - b' \in I$. Então $ab - a'b' \in I$.*

Demonstração: Tem-se $ab - a'b' = ab - a'b + a'b - a'b' = (a - a')b + a'(b - b') \in I$. □

Definição 2.2.13. Sejam A um anel e I um ideal. O *anel quociente* A/I é o grupo quociente A/I com a multiplicação definida por $(a+I)\cdot(b+I) = ab+I$. Pelo lema precedente, esta multiplicação está bem definida. Verifica-se facilmente que A/I é um anel e que o epimorfismo canónico $A \to A/I$, $a \mapsto a+I$ é um homomorfismo de anéis.

Exemplo 2.2.14. O anel $\mathbb{Z}_n$ é o anel quociente $\mathbb{Z}/n\mathbb{Z}$.

Teorema 2.2.15. *Sejam $f\colon A \to A'$ um homomorfismo de anéis, $I \subseteq A$ um ideal tal que $I \subseteq \mathrm{Ker}(f)$ e $\pi\colon A \to A/I$ o epimorfismo canónico. Então existe um único homomorfismo de anéis $\bar{f}\colon A/I \to A'$ tal que $\bar{f}\circ\pi = f$. O homomorfismo $\bar{f}$ é dado por $\bar{f}(a+I) = f(a)$ e é injetivo se e só se $I = \mathrm{Ker}(f)$.*

Demonstração: Por 1.6.13, existe um único homomorfismo de grupos $\bar{f}\colon A/I \to A'$ tal que $\bar{f}\circ\pi = f$. Como $\bar{f}(1+I) = \bar{f}\circ\pi(1) = f(1) = 1$ e $\bar{f}((a+I)(b+I)) = \bar{f}(ab+I) = \bar{f}\circ\pi(ab) = f(ab) = f(a)f(b) = \bar{f}\circ\pi(a)\bar{f}\circ\pi(b) = \bar{f}(a+I)\bar{f}(b+I)$ para todos os $a, b \in A$, $\bar{f}$ é de facto um homomorfismo de anéis. Por 1.6.13, $\bar{f}$ é injetivo se e só se $I = \mathrm{Ker}(f)$. $\square$

Corolário 2.2.16. *(Teorema do homomorfismo) Seja $f\colon A \to A'$ um homomorfismo de anéis. Então um isomorfismo de anéis $A/\mathrm{Ker}(f) \to \mathrm{Im}(f)$ é dado por $x+\mathrm{Ker}(f) \mapsto f(x)$.*

Teorema 2.2.17. *Sejam A um anel, $B \subseteq A$ um subanel e $I \subseteq A$ um ideal. Então $B+I$ é um subanel de A, I é um ideal de $B+I$, $B\cap I$ é um ideal de B e um isomorfismo de anéis $B/(B\cap I) \to (B+I)/I$ é dado por $x + B\cap I \mapsto x+I$.*

Demonstração: $B+I$ é um subgrupo do grupo aditivo de A que contém o elemento 1. Sejam $b, b' \in B$ e $x, x' \in I$. Então $(b+x)(b'+x') = bb' + bx' + xb' + xx' \in B+I$. Logo $B+I$ é um subanel de A. Como I é um ideal de A e $I \subseteq B+I$, I é um ideal de $B+I$. $B\cap I$ é um subgrupo de B e para $b \in B$ e $x \in B\cap I$, $bx \in B\cap I$ e $xb \in B\cap I$. Logo $B\cap I$ é um ideal de B. Por 1.6.17, um isomorfismo de grupos $f\colon B/(B\cap I) \to (B+I)/I$ é dado por $f(x+B\cap I) = x+I$. Como $f(1+B\cap I) = 1+I$ e $f((x+B\cap I)(y+B\cap I)) = f(xy+B\cap I) = xy+I = (x+I)(y+I) = f(x+B\cap I)f(y+B\cap I)$ para todos os $x, y \in B$, f é de facto um isomorfismo de anéis. $\square$

Teorema 2.2.18. *Sejam A um anel e I e J ideais de A tais que $J \subseteq I$. Então I/J é um ideal de A/J e um isomorfismo de anéis $(A/J)/(I/J) \to A/I$ é dado por $x+J+I/J \mapsto x+I$.*

Demonstração: Por 1.6.18, I/J é um subgrupo do grupo aditivo de A/J. Para $a \in A$ e $x \in I$, $(a+J)(x+J) = ax+J \in I/J$ e $(x+J)(a+J) = xa+J \in I/J$. Logo I/J é um ideal de A/J. Por 1.6.18, um isomorfismo de grupos $f\colon (A/J)/(I/J) \to A/I$ é dado por $f(x+J+I/J) = x+I$. Como $f(1+J+I/J) = 1+I$ e $f((x+J+I/J)(y+J+I/J)) = f((x+J)(y+J)+I/J) = f(xy+J+I/J) = xy+I = (x+I)(y+I) = f(x+J+I/J)f(y+J+I/J)$ para todos os $x, y \in A$, f é de facto um isomorfismo de anéis. $\square$

2.3 Domínios de integridade e corpos

Vamos supor que A é um anel não nulo, isto é $A \neq \{0\}$. Sendo assim, $1 \neq 0$ e A tem pelo menos dois elementos.

Definição 2.3.1. Seja A um anel não nulo. Um elemento $a \neq 0$ de A diz-se um *divisor de zero* se existe um elemento $b \neq 0$ em A tal que $ab = 0$ ou $ba = 0$.

Definição 2.3.2. Um *domínio de integridade* é um anel A comutativo não nulo que não admite divisores de zero, isto é, para quaisquer $a, b \in A$, $ab = 0$ implica $a = 0$ ou $b = 0$.

Exemplos 2.3.3. (i) $\mathbb{Z}$, $\mathbb{Q}$ e $\mathbb{R}$ são domínios de integridade.

(ii) $\mathbb{Z}_4$ não é um domínio de integridade. $[2]$ é um divisor de zero em $\mathbb{Z}_4$ pois $[2]\cdot[2] = [0]$.

(iii) Qualquer subanel de um domínio de integridade é um domínio de integridade.

Proposição 2.3.4. *Sejam A um domínio de integridade, $a \in A \setminus \{0\}$ e $b, c \in A$. Então $ab = ac \Rightarrow b = c$ e $ba = ca \Rightarrow b = c$.*

Demonstração: Como A é comutativo, basta mostrar a primeira implicação. Se $ab = ac$, então $a(b - c) = ab - ac = 0$. Como $a \neq 0$, $b - c = 0$. Logo $b = c$. □

Definição 2.3.5. Um ideal I de um anel A diz-se *primo* se $I \neq A$ e se para quaisquer dois elementos $a, b \in A$, $ab \in I$ implica $a \in I$ ou $b \in I$.

Exemplos 2.3.6. (i) Um anel comutativo não nulo é um domínio de integridade se e só se $\{0\}$ é um ideal primo.

(ii) Para $n \geq 1$, $n\mathbb{Z}$ é um ideal primo de $\mathbb{Z}$ se e só se n é primo.

Proposição 2.3.7. *Sejam A um anel comutativo e $I \neq A$ um ideal de A. Então I é primo se e só se A/I é um domínio de integridade.*

Demonstração: Suponhamos primeiramente que I é primo. Como A é comutativo, A/I é comutativo também. Como $I \neq A$, o anel A/I é não nulo. Sejam $a, b \in I$ tais que $(a + I)(b + I) = ab + I = I$. Então $ab \in I$ e portanto $a \in I$ ou $b \in I$. Logo $a + I = I$ ou $b + I = I$. Segue-se que A/I é um domínio de integridade.

Suponhamos inversamente que A/I é um domínio de integridade. Sejam $a, b \in A$ tais que $ab \in I$. Então $(a + I)(b + I) = ab + I = I$, pelo que $a + I = I$ ou $b + I = I$. Segue-se que $a \in I$ ou $b \in I$ e então que I é primo. □

Corolário 2.3.8. *$\mathbb{Z}_n$ é um domínio de integridade se e só se n é primo.*

Definição 2.3.9. Um anel comutativo A não nulo é um *corpo* se todo o elemento $a \in A$ não nulo é invertível (relativamente à multiplicação).

Exemplos 2.3.10. (i) $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ são corpos.
(ii) $\mathbb{Z}$ não é um corpo.

Proposição 2.3.11. *Qualquer corpo é um domínio de integridade.*

Demonstração: Sejam K um corpo e $a, b \in K$ tais que $ab = 0$ e $a \neq 0$. Então $b = a^{-1}ab = a^{-1}0 = 0$. Como K é comutativo e não nulo, podemos concluir que K é um domínio de integridade. □

Proposição 2.3.12. *$\mathbb{Z}_n$ é um corpo se e só se n é primo.*

Demonstração: Se n não é primo, $\mathbb{Z}_n$ não é um anel de integridade, pelo que não é um corpo. Se n é primo, $\mathbb{Z}_n$ é comutativo e não nulo e segue-se do Exercício que qualquer elemento não nulo de $\mathbb{Z}_n$ é invertível. Consequentemente, $\mathbb{Z}_n$ é um corpo. □

Observação 2.3.13. Num corpo K, os únicos ideais são os ideais principais $(0) = \{0\}$ e $(1) = K$. Com efeito, se $I \neq \{0\}$ é um ideal de K e $x \in I \setminus \{0\}$, então $1 = x^{-1}x \in I$, pelo que $I = K$.

Definição 2.3.14. Um ideal I de um anel A diz-se *maximal* se $I \neq A$ e se para qualquer ideal J de A, $I \subseteq J \neq A \Rightarrow J = I$.

Proposição 2.3.15. *Sejam A um anel comutativo e $I \neq A$ um ideal. Então I é maximal se e só se A/I é um corpo.*

Demonstração: Suponhamos primeiramente que I é maximal. Seja $a \in A \setminus I$. Então $(a) + I$ é um ideal de A que contém I como subconjunto próprio. Como I é maximal, $(a) + I = A$. Logo existem $b \in A$ e $x \in I$ tais que $1 = ab + x$. Tem-se $(a + I)(b + I) = ab + I = ab + x + I = 1 + I$, pelo que $a + I$ é uma unidade de A/I. Para qualquer $x \in A$, $(x + I)I = I \neq 1 + I$, pelo que I não é invertível em A/I. Segue-se que A/I é um corpo.

Suponhamos agora que A/I é um corpo. Seja J um ideal de A tal que $I \subseteq J \neq A$. Seja $a \in J$. Suponhamos, por absurdo, que $a \notin I$. Então $a + I$ é uma unidade de A/I e existe $b \in A$ tal que $ab + I = (a + I)(b + I) = 1 + I$. Logo $ab - 1 \in I \subseteq J$. Como $ab \in J$, obtém-se $1 \in J$ e então $J = A$. Contradição! Portanto $a \in I$ e I é maximal. □

Corolário 2.3.16. *Qualquer ideal maximal de um anel é primo.*

Proposição 2.3.17. *Seja A um domínio de integridade. Uma relação de equivalência em $A \times (A \setminus \{0\})$ é dada por $(a, b) \sim (x, y) \Leftrightarrow ay = xb$. Se $(a, b) \sim (x, y)$ e $(c, d) \sim (u, v)$, então $(ad + cb, bd) \sim (xv + uy, yv)$ e $(ac, bd) \sim (xu, yv)$.*

Demonstração: É óbvio que a relação $\sim$ é reflexiva e simétrica. Sejam $(a,b),(x,y),(u,v) \in A \times (A \setminus \{0\})$ tais que $(a,b) \sim (x,y)$ e $(x,y) \sim (u,v)$. Então $ay = xb$ e $xv = uy$. Logo $avy = ayv = xbv = bxv = buy$. Como $y \neq 0$, obtém-se $av = bu = ub$, ou seja, $(a,b) \sim (u,v)$. Logo $\sim$ é transitiva e então uma relação de equivalência.

Suponhamos agora que $(a,b) \sim (x,y)$ e $(c,d) \sim (u,v)$. Então $(ad+cb)yv = adyv + cbyv = aydv + cvby = xbdv + udby = xvbd + uybd = (xv+uy)bd$. Logo $(ad+cb, bd) \sim (xv+uy, yv)$. Tem-se $acyv = aycv = xbud = xubd$ e então $(ac,bd) \sim (xu,yv)$. $\square$

Definição 2.3.18. Seja A um domínio de integridade e $\sim$ a relação de equivalência em $A \times (A \setminus \{0\})$ dada por $(a,b) \sim (x,y) \Leftrightarrow ay = xb$. A classe de equivalência de um par $(a,b) \in A \times (A \setminus \{0\})$ é a *fracção* $\frac{a}{b}$. Pela proposição precedente podemos definir a adição e a multiplicação de fracções por

$$\frac{a}{b} + \frac{c}{d} = \frac{ad+cb}{bd} \qquad \text{e} \qquad \frac{a}{b} \cdot \frac{c}{d} = \frac{ac}{bd}.$$

O *corpo de fracções* de A, $Frac(A)$, é o conjunto das fracções $\frac{a}{b}$ $(a, b \in A,\ b \neq 0)$ munido da adição e da multiplicação de fracções.

Exemplo 2.3.19. $Frac(\mathbb{Z}) = \mathbb{Q}$.

Definição 2.3.20. Seja A um anel. A *característica* de A é definida por

$$\operatorname{car}(A) = \begin{cases} 0, & \text{se } |1| = \infty, \\ |1|, & \text{caso contrário.} \end{cases}$$

Exemplos 2.3.21. Tem-se $\operatorname{car}(\mathbb{Z}) = \operatorname{car}(\mathbb{Q}) = \operatorname{car}(\mathbb{R}) = 0$ e $\operatorname{car}(\mathbb{Z}_n) = n$.

Notas 2.3.22. (i) Num anel A de característica n tem-se $na = 0$ para todo o $a \in A$. Com efeito, para qualquer $a \in A$, $na = n(1a) = (n1)a = 0a = 0$.

(ii) Sejam A um anel e $f\colon \mathbb{Z} \to A$ o homomorfismo de anéis dado por $f(n) = n \cdot 1$. Note-se que f é o único homomorfismo de anéis de $\mathbb{Z}$ para A. Tem-se $\operatorname{car}(A) = n$ se e só se $\operatorname{Ker}(f) = n\mathbb{Z}$. Segue-se que a característica de A é o único número natural n tal que A contém um subanel isomorfo a $\mathbb{Z}/n\mathbb{Z}$.

Proposição 2.3.23. *A característica de um domínio de integridade é ou* 0 *ou um número primo.*

Demonstração: Seja A um domínio de integridade com $\operatorname{car}(A) \neq 0$. Então o elemento 1 de A tem ordem finita e $\operatorname{car}(A) = |1|$. Sejam $1 \leq k \leq l \leq |1|$ inteiros tais que $kl = |1|$. Então $k1 \cdot l1 = kl1 = |1|1 = 0$, pelo que $k1 = 0$ ou $l1 = 0$. Segue-se que $l = |1|$ e $k = 1$. Logo $\operatorname{car}(A) = |1|$ é um número primo. $\square$

Nota 2.3.24. Existe uma múltiplicação com a qual o grupo $\mathbb{Z}_2 \times \mathbb{Z}_2$ é um corpo. Este corpo tem característica 2 e 4 elementos. Note-se que para qualquer número primo p e qualquer número natural $n \geq 1$, existe um corpo $\mathbb{F}_{p^n}$ de característica p com p^n elementos e este corpo é único a menos de isomorfismo. Além disso, qualquer corpo finito é isomorfo a um dos corpos $\mathbb{F}_{p^n}$.

2.4 Divisibilidade num domínio de integridade

Definição 2.4.1. Seja A um domínio de integridade e sejam $a, b \in A$. Diz-se que *a divide b* (escreve-se $a|b$) se existir $q \in A$ tal que $a = bq$. Diz-se que a e b são *associados* se $a|b$ e $b|a$.

Notas 2.4.2. (i) Tem-se: $a|b \Leftrightarrow b \in (a) \Leftrightarrow (a) \subset (a)$.

(ii) Os elementos a e b são associados se e só se $(a) = (b)$. Mostra-se também que a e b são associados se e só se existir $u \in A$ invertível tal que $b = au$.

(iii) Qualquer elemento $a \in A$ divide 0 pois $0 = 0 \cdot a$ mas não é um divisor de zero no sentido da definição 2.3.1 pois, sendo A um domínio de integridade, não existe $q \neq 0$ tal que $0 = aq$.

Definição 2.4.3. Seja A um domínio de integridade e seja $p \in A$ um elemento não nulo, não invertível.

- p é dito *primo* se, para todos os $a, b \in A$, $p|ab \Rightarrow p|a$ ou $p|b$.
- p é dito *irredutível* se, para todos os $a, b \in A$, $p = ab \Rightarrow a$ é invertível ou b é invertível .

Nota 2.4.4. São duas noções que estendem a noção usual de primo nos inteiros. Em particular, $p \in \mathbb{Z}$ é primo/irredutível se e só se $|p|$ é um natural primo no sentido usual.

Proposição 2.4.5. Seja A um domínio de integridade e seja $p \in A$ um elemento não nulo, não invertível. Se p é primo então p é irredutível.

Demonstração: Sejam $a, b \in A$ tais que $p = ab$. Como $p \neq 0$, temos $a \neq 0$ e $b \neq 0$. Como $p = ab$, podemos dizer que $p|ab$ (pois $ab = 1 \cdot p$) e, como p é primo, temos $p|a$ ou $p|b$. Se $p|a$, então existe $q \in A$ tal que $a = pq$. Como $p = ab$, obtemos $a = abq$ e $a(1 - bq) = 0$. Como $a \neq 0$ e A é um domínio de integridade, obtemos $1 - bq = 0$. Logo $bq = 1$ e, sendo A comutativo, podemos concluir que b é invertível. Da mesma forma, se $b \neq 0$, obtemos que a é invertível. Em todos os casos, obtemos a invertível ou b invertível e podemos concluir que p é irredutível. □

Proposição 2.4.6. Seja A um domínio de integridade e seja $p \in A$ um elemento não nulo, não invertível. Considere o ideal (p) de A gerado por p. Tem-se

(i) p é primo se e só se (p) é primo.

(ii) Se (p) é maximal então p é irredutível.

Demonstração: Como p é não invertível tem-se $(p) \neq A$. A alínea (i) segue imediatamente das definições de elemento e ideal primo. Como um ideal maximal e sempre primo, a alínea (ii) segue da alínea (i) e da proposição anterior. $\square$

Não é verdade em geral que um elemento irredutível seja um elemento primo (ver Exercícios 56). No entanto, existem classes de anéis em que isto é verdade.

Definição 2.4.7. Seja A um domínio de integridade. Diz-se que A é um *domínio de fatorização única* se

(E) Para todo o $a \in A$ não nulo e não invertível, existem $p_1, \ldots, p_n$ elementos irredutíveis de A tais que $a = p_1 \cdots p_n$.

(U) Esta decomposição é única a menos da ordem e de fatores invertíveis. Isto é, se $p_1 \cdots p_n = q_1 \cdots q_m$ onde os p_i e q_j $(1 \leq i \leq n,\ 1 \leq j \leq m)$ são irredutíveis, então $n = m$ e existe uma permutação $\sigma \in S_n$ tal que, para todo o $i \in \{1, \cdots, n\}$, p_i e $q_{\sigma(i)}$ são associados.

Exemplos de domínios de fatorização única são $\mathbb{Z}$ (através da decomposição de um natural em naturais primos) e anéis de polinómios.

Proposição 2.4.8. Seja A um domínio de fatorização única e seja $p \in A$ um elemento não nulo não invertível. Se p é irredutível então p é primo.

Demonstração: Sejam $a, b \in A$ tais que $p|ab$. Queremos ver que $p|a$ ou $p|b$. Como $p|ab$ existe $q \in A$ tal que $ab = pq$. Em primeiro lugar, analisemos alguns casos particulares. Se $a = 0$ temos $a = 0 \cdot p$ pelo que $p|a$. Se a é invertível, temos $b = a^{-1}pq$ pelo que $p|b$. Da mesma forma, se $b = 0$, tem-se $p|b$ e, se b é invertível, tem-se $p|a$. Se $q = 0$ tem-se $a = 0$ ou $b = 0$ pelo que $p|a$ ou $p|b$. Se q é invertível, temos $p = abq^{-1}$. Como p é irredutível, temos a invertível ou bq^1 invertível. No primeiro caso, obtemos $b = pqa^{-1}$ pelo que $p|b$. No segundo caso, $a = pqb^{-1}$ pelo que $p|a$. Em todos os casos analisados, chegamos à conclusão que $p|a$ ou $p|b$. Podemos agora supor que a, b e q são não nulos, não invertíveis. Como A é um domínio de fatorização única, existem $p_1, \ldots, p_n, p'_1, \ldots, p'_m, p''_1, \ldots, p''_l$ elementos irredutíveis de A tais que $a = p_1 \cdots p_n$, $b = p'_1 \cdots p'_m$ e $q = p''_1 \cdots p''_l$. Como $ab = pq$ obtemos

$$p_1 \cdots p_n \cdot p'_1 \cdots p'_m = p \cdot p''_1 \cdots p''_l.$$

Pela unicidade da decomposição em irredutíveis, p é associado a um dos p_i (neste caso $p|a$) ou a um dos p'_j (neste caso $p|b$). Em todos os casos $p|a$ ou $p|b$ e podemos concluir que p é primo.

Definição 2.4.9. Um domínio de integridade A diz-se um *domínio de ideais principais* se todos os ideais de A são principais.

Exemplos 2.4.10. (i) Qualquer corpo é um domínio de ideais principais.
(ii) $\mathbb{Z}$ é um domínio de ideais principais.

Proposição 2.4.11. Seja A um domínio de ideais principais e seja $p \in A$ um elemento não nulo, não invertível. Se p é irredutível então (p) é maximal.

Demonstração: Como p não é invertível, $(p) \neq A$. Seja J um ideal de A tal que $(p) \subset J$. Queremos mostrar que $J = (p)$ ou $J = A$. Como A é um domínio de ideais principais, existe $a \in A$ tal que $J = (a)$. De $(p) \subset (a)$ deduzimos que $p \in (a)$ e que existe $b \in A$ tal que $p = ab$. Como p é irredutível, a é invertível ou b é invertível. Se a é invertível temos $J = (a) = A$. Se b é invertível, p e a são associados e consequentemente $J = (a) = (p)$. Podemos concluir que (p) é maximal. $\square$

Corolário 2.4.12. Sejam A um domínio de ideais principais e seja $p \in A$ um elemento não nulo, não invertível. São equivalentes:

(i) p é primo;

(ii) p é irredutível;

(iii) (p) é maximal;

(iv) (p) é primo.

Por fim, pode se estabelecer o seguinte resultado:

Teorema 2.4.13. Seja A um anel. Se A é um domínio de ideais principais então A é um domínio de fatorização única.