Estruturas Algébricas

Licenciatura em Ciências da Computação
Apontamentos das aulas teóricas
Ano lectivo 2010-2011
Docente: Thomas Kahl

Conteúdo

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 $\mathbb{R}$.

(ii) A subtracção $-$ é uma operação binária em $\mathbb{Z}$, $\mathbb{Q}$ e $\mathbb{R}$, mas não em $\mathbb{N}$. A subtracção 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 $X = \{x_1, \ldots, x_n\}$ 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 $a_1, \ldots, a_n \in S$. Então existe um único produto dos elementos $a_1, \ldots, a_n$.*

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 $i \in \{1, \ldots, n-1\}$. Por hipótese de indução, existe um único produto dos elementos $a_2, \ldots, a_n$. Seja b este produto. Então $a_1 \cdot b$ é produto dos elementos $a_1, \ldots, a_n$. A fim de mostrar a unicidade deste produto consideramos um produto x dos elementos $a_1, \ldots, a_n$ e mostramos que $x = a_1 \cdot b$. Sejam $i \in \{1, \ldots, n-1\}$ e $y, z \in S$ 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 $x = y \cdot z$. 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 $a_2, \ldots, a_i$. Então $a_1 \cdot c$ é um produto dos elementos $a_1, \ldots, a_i$. 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 $a_2, \ldots, a_n$, temos $c \cdot z = b$ e então $x = a_1 \cdot b$. □

Notação 1.1.9. Sejam S um semigrupo e $a_1, \ldots, a_n \in S$. O único produto dos elementos $a_1, \ldots, a_n$ 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 determinate zero não é um monóide (porquê?).

(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 (qual?), 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.

1.2 Elementos invertíveis

Definição 1.2.1. 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 1.2.2. 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 1.2.3. *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: Tem-se $y = ye = yxz = ez = z$. □

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

Exemplos 1.2.5. (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 1.2.6. *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 1.2.7. *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 1.2.6. 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 1.2.8. *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 1.2.9. 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 1.2.10. 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 1.2.8 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 1.2.11. *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 $a^{n+m} = a^{-(-n-m)} = (a^{-1})^{-n-m} = (a^{-1})^{-n}(a^{-1})^{-m} = a^n a^m$. □

1.3 Grupos

Definição 1.3.1. Um *grupo* é um monóide em que todos os elementos são invertíveis.

Observação 1.3.2. Sejam M um monóide e M^* o conjunto dos elementos invertíveis de M. Segue-se de 1.2.4 e 1.2.6 que M^* é um grupo relativamente à multiplicação de M.

Exemplos 1.3.3. (i) Os conjuntos $\mathbb{Z}$, $\mathbb{Q}$ e $\mathbb{R}$ são grupos relativamente à adição.

(ii) Os conjuntos $\mathbb{Q}^* = \mathbb{Q}\backslash\{0\}$ e $\mathbb{R}^* = \mathbb{R}\backslash\{0\}$ são grupos 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.

Proposição 1.3.4. *Um grupóide G é um grupo se e só se*

(a) G é um semigrupo;

(b) G admite um elemento neutro à esquerda e;

(c) para todo o elemento $x \in G$ existe um elemento $y \in G$ tal que $yx = e$.

Demonstração: Basta demonstrar que um grupóide G que satisfaz as condições (a), (b) e (c) é um grupo. Seja $x \in G$. Por (c), existem $y, z \in G$ tais que $yx = e$ e $zy = e$. Tem-se

$$x = ex = (zy)x = z(yx) = ze$$

e então

$$xy = (ze)y = z(ey) = zy = e.$$

Logo

$$xe = x(yx) = (xy)x = ex = x.$$

Segue-se que e é um elemento neutro à direita e então que G é um monóide. Mostrámos que $xy = e$. Isto implica que todos os elementos de G são invertíveis. Portanto G é um grupo. □

Proposição 1.3.5. *Um semigrupo G é um grupo se e só se para cada dois elementos $a, b \in G$ existem $x, y \in G$ tais que $ax = b$ e $ya = b$.*

Demonstração: Suponhamos primeiramente que G é um grupo. Sejam $a, b \in G$. Então $a(a^{-1}b) = (aa^{-1})b = eb = b$ e $(ba^{-1})a = b(a^{-1}a) = be = b$.

Suponhamos agora que para cada dois elementos $a, b \in G$ existem $x, y \in G$ tais que $ax = b$ e $ya = b$. Como $G \neq \emptyset$, existe $a \in G$. Seja $e \in G$ tal que $ea = a$. Mostramos que e é um elemento neutro a esquerda de G. Seja $b \in G$. Seja $x \in G$ tal que $ax = b$. Tem-se $eb = eax = ax = b$. Logo e é um elemento neutro a esquerda e G satisfaz as condições (a) e (b) da proposição 1.3.4. Seja $b \in G$. Por hipótese, existe $y \in G$ tal que $yb = e$. Logo G satisfaz também a condição (c) de 1.3.4. Segue-se que G é um grupo. □

Definição 1.3.6. Dizemos que um grupóide G satisfaz as *leis do corte* se para quaisquer três elementos $a, b, c \in G$,

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

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

Proposição 1.3.7. *Qualquer grupo satisfaz as leis do corte.*

Demonstração: Sejam a, b, c três elementos de um grupo G. Se $ac = bc$, então

$$a = ae = acc^{-1} = bcc^{-1} = be = b.$$

Da mesma maneira mostra-se a condição (ii) de 1.3.6. □

Nota 1.3.8. Segue-se das proposições 1.3.5 e 1.3.7 que num grupo as equações $ax = b$ e $xa = b$ têm soluções únicas para quaisquer dois elementos a e b. Isto implica que cada linha e cada coluna da tabela de Cayley de um grupo finito contém cada elemento do grupo exactamente uma vez (no quadrante dos produtos). 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.

Proposição 1.3.9. *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. Para $a \in G$ sejam $\lambda_a \colon G \to G$ e $\rho_a \colon G \to G$ as funções dadas por $\lambda_a(x) = ax$ e $\rho_a(x) = xa$. Pelas leis do corte, λ_a e ρ_a são injectivas. Como G é finito, λ_a e ρ_a são sobrejectivas. Logo para cada dois elementos $a, b \in G$, existem elementos $x, y \in G$ tais que $ax = \lambda_a(x) = b$ e $ya = \rho_a(y) = b$. Pela proposição 1.3.5, isto implica que G é um grupo. □

Nota 1.3.10. O resultado precedente não se estende aos semigrupos infinitos como mostra o exemplo do monóide $(\mathbb{N}, +)$.

1.4 Homomorfismos de grupos

Definição 1.4.1. 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 $G = H$;
- *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 1.4.2. *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 1.4.3. Sejam G e H dois grupos e $f \colon G \to H$ um homomorfismo. Segue-se da proposição precedente que para qualquer $x \in G$ e qualquer $n \in \mathbb{Z}$, $f(x^n) = f(x)^n$ (exercício).

Exemplos 1.4.4. (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 identica de um grupo é um automorfismo.

(vi) Seja $f\colon X \to Y$ uma função bijectiva entre dois conjuntos. Um isomorfismo de grupos $S(f)\colon S(X) \to S(Y)$ é dado por $S(f)(\sigma) = f \circ \sigma \circ f^{-1}$. Tem-se $S(f)^{-1} = S(f^{-1})$. Em particular, o grupo simétrico de um conjunto com n elementos é isomorfo ao grupo simétrico S_n.

(vii) Sejam G um grupo e $g \in G$. Então um automorfismo $\phi_g\colon G \to G$ é dado por $\phi_g(x) = gxg^{-1}$. Um automorfismo desta forma diz-se um *automorfismo interno* de G. Nota-se que dois elementos $x, y \in G$ dizem-se *conjugados* se existe um elemento g tal que $y = gxg^{-1}$.

Proposição 1.4.5. *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 $g \circ f(xy) = g(f(xy)) = g(f(x)f(y)) = g(f(x))g(f(y)) = g \circ f(x) \cdot g \circ f(y)$. □

Definição 1.4.6. Seja $f\colon G \to H$ um homomorfismo de grupos. A *imagem* de f é o conjunto $\mathrm{Im}(f) = \{f(x) \,|\, x \in G\}$. O *núcleo* de f é o conjunto $\mathrm{Ker}(f) = \{x \in G \,|\, f(x) = e\}$. Às vezes escreve-se $\mathrm{Nuc}(f)$ em vez de $\mathrm{Ker}(f)$.

Proposição 1.4.7. *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 $x = xe = xy^{-1}y = ey = y$. Segue-se que f é injectivo. □

Proposição 1.4.8. *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 $f^{-1}(xy) = f^{-1}(x)f^{-1}(y)$. □

Observação 1.4.9. Seja G um grupo. Segue-se das proposições 1.4.5 e 1.4.8 que o conjunto $Aut(G)$ dos automorfismos de G é um grupo com a composição de funções como multiplicação. Um homomorfismo de grupos $\Phi\colon G \to Aut(G)$ é dado por $\Phi(g)(x) = \phi_g(x) = gxg^{-1}$.

1.5 Subgrupos

Definição 1.5.1. 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 1.5.2. (i) $\mathbb{Z}$ é um subgrupo do grupo aditivo $\mathbb{Q}$ e temos de facto $\mathbb{Z} < \mathbb{Q}$.

(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 1.5.3. Sejam G um grupo, $H \leq G$ e $K \subseteq H$. Então $K \leq G \Leftrightarrow K \leq H$.

Proposição 1.5.4. *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 1.5.5. (i) $]0, +\infty[$ é um subgrupo do grupo multiplicativo $\mathbb{R}^* = \mathbb{R} \setminus \{0\}$.

(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 $GL_2(\mathbb{R})$.

Proposição 1.5.6. *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 1.5.4, H é um subgrupo de G. □

Proposição 1.5.7. *Um subconjunto finito $H \neq \emptyset$ de um grupo G é um subgrupo se e só se para quaisquer $x, y \in H$, $xy \in H$.*

Demonstração: Basta demonstrar que H é um subgrupo se para quaisquer $x, y \in H$, $xy \in H$. Esta condição implica que H é um semigrupo que satisfaz as leis do corte. Por 1.3.9, H é um grupo. Logo H é um subgrupo de G. □

Proposição 1.5.8. *Sejam G um grupo e $(H_i)_{i \in I}$ uma familia 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 1.5.6, $xy^{-1} \in H_i$ para todo o $i \in I$, pelo que $xy^{-1} \in \bigcap_{i \in I} H_i$. Por 1.5.6, $\bigcap_{i \in I} H_i$ é um subgrupo de G. □

Definição 1.5.9. 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 1.5.10. *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 1.5.11. (i) O subgrupo de $(\mathbb{Z}, +)$ gerado por $m \in \mathbb{Z}$ é o conjunto $m\mathbb{Z} = \{mk \,|\, k \in \mathbb{Z}\}$.

(ii) O subgrupo de $(\mathbb{Z}, +)$ gerado pelo conjunto $\{2, 3\}$ é o conjunto $\{2m+3n \,|\, m, n \in \mathbb{Z}\}$.

(iii) O conjunto $\{1\}$ é um conjunto gerador de $(\mathbb{Z}, +)$.

(iv) O *grupo de Klein* é o subgrupo V de S_4 gerado pelas permutações a e b dadas por $a(1) = 2$, $a(2) = 1$, $a(3) = 4$, $a(4) = 3$, $b(1) = 3$, $b(2) = 4$, $b(3) = 1$ e $b(4) = 2$. Os elementos do grupo de Klein são $e = id_{\{1,2,3,4\}}$, a, b e $ab = ba$. Tem-se $a^2 = b^2 = e$. Nota-se que a única estrutura de grupo no conjunto V com esta propriedade (e em que e é o elemento neutro) é a do grupo de Klein.

(v) Em qualquer grupo G, $\langle\emptyset\rangle = \{e\}$.

Observação 1.5.12. 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 1.5.13. *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 $\langle X\rangle = G$. □

Exemplo 1.5.14. 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).

Proposição 1.5.15. *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 1.5.6, $f^{-1}(V)$ 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 1.5.6, $f(U)$ é um subgrupo de H. □

Corolário 1.5.16. *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 1.5.17. O *centro* de um grupo G é o conjunto

$$Z(G) = \{g \in G \,|\, \forall x \in G \quad gx = xg\}.$$

Como $Z(G)$ é o núcleo do homomorfismo $\Phi\colon G \to Aut(G)$, $\Phi(g)(x) = gxg^{-1}$, o centro de G é um subgrupo de G.

1.6 Teorema de Lagrange

Notação 1.6.1. 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 1.6.2. 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 1.6.3. *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. Para quaisquer $x, y, a \in G$, tem-se $x \sim_H y \Rightarrow xa \sim_H ya$.*

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 $Hx \subseteq [x]$.

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 $xa \sim_H ya$. □

Proposição 1.6.4. *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 $z = yx = f(x)$. Isto mostra que f é sobrejectiva. □

Definição 1.6.5. 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 1.6.6. 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 1.6.7. *(Teorema de Lagrange) Sejam G um grupo e H um subgrupo de G. Então $|G| = |G : H||H|$.*

Demonstração: Se $|H| = \infty$, obviamente também $|G| = \infty$. Suponhamos que $|H|$ é finito. Por 1.6.4, cada classe lateral direita de H tem $|H|$ elementos. Por 1.6.3, as classes laterais direitas de H formam uma partição de G. Logo $|G| = |G : H||H|$ (seja $|G : H|$ finito ou não). □

Corolário 1.6.8. *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 1.6.9. 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 $G = \langle a \rangle$.

1.7 Subgrupos normais e grupos quociente

Definição 1.7.1. 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 1.7.2. *Sejam G um grupo e H um subgrupo de G. Então as seguintes afirmações são equivalentes:*

(a) H é um subgrupo normal de G;

(b) para cada $a \in G$, $aHa^{-1} = H$;

(c) para cada $a \in G$, $aH = Ha$;

(d) para cada $a \in G$, $aH \subseteq Ha$.

Demonstração: (a) ⇒ (b): Sejam $x \in H$ e $a \in G$. Então $a^{-1}xa = a^{-1}x(a^{-1})^{-1} \in H$. Logo $x = aa^{-1}xaa^{-1} \in aHa^{-1}$.

As implicações (b) ⇒ (c) ⇒ (d) ⇒ (a) são triviais. □

Exemplos 1.7.3. (i) Para qualquer grupo G, $\{e\}$ e G são subgrupos normais de G.

(ii) Num grupo comutativo todos os subgrupos são normais.

Proposição 1.7.4. *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 1.5.8, $\bigcap_{i\in I} H_i$ 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 $axa^{-1} \in \bigcap_{i\in I} H_i$. □

Proposição 1.7.5. *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 1.5.15, $f^{-1}(H')$ 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 1.5.15, $\mathrm{Im}(f)$ 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 1.7.6. *O núcleo de um homomorfismo de grupos $f\colon G \to G'$ é um subgrupo normal de G.*

Exemplos 1.7.7. (i) O centro $Z(G)$ de um grupo G é um subgrupo normal de G.

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

Proposição 1.7.8. *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 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 1.6.3, a classe de equivalência de um elemento $x \in G$ é a classe lateral direita Hx. Assim, $x \sim_H y \Leftrightarrow Hx = Hy$.

Suponhamos primeiramente que H é um subgrupo normal de G. Sejam $x, y, a \in G$. Então $x \sim_H y \Rightarrow Hx = Hy \Rightarrow xH = yH \Rightarrow axH = ayH \Rightarrow Hax = Hay \Rightarrow ax \sim_H ay$.

Suponhamos agora 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 1.7.9. *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 1.7.10. Sejam G um grupo e $H \subseteq G$ um subgrupo normal. O *grupo quociente de G por H* é o conjunto das classes laterais

$$G/H = \{Hx \mid x \in G\}$$

munido da operação dada por

$$Hx \cdot Hy = Hxy.$$

Por 1.7.9, 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 1.7.11. (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 abreviação $\bar{r} = r + n\mathbb{Z}$. Nota-se que $k \in \bar{r}$ 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 1.7.12. (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 $H \subseteq G$, $|G/H| = |G : H|$.

Teorema 1.7.13. *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 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 $H = \mathrm{Ker}(f)$. □

Corolário 1.7.14. *(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 $\mathrm{Ker}(f)x \mapsto f(x)$.*

Exemplos 1.7.15. (i) Para qualquer grupo G, o grupo $G/Z(G)$ é isomorfo ao subgrupo de $Aut(G)$ dos automorfismos internos de G.

(ii) Para qualquer inteiro $n \geq 1$, o grupo $GL_n(\mathbb{R})/SL_n(\mathbb{R})$ é isomorfo ao grupo multiplicativo $\mathbb{R}^*$.

Proposição 1.7.16. *Sejam G um grupo, $H \subseteq G$ um subgrupo e $N \subseteq G$ 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 1.5.8, $H \cap N$ 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 1.7.17. *Sejam G um grupo, $H \subseteq G$ um subgrupo e $N \subseteq G$ 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. □

Exemplo 1.7.18. Considere o grupo de Klein $V = \{e, a, b, ab\}$ (cf. 1.5.11(iv)). Como V é comutativo, $\langle a\rangle = \{e, a\}$ e $\langle b\rangle = \{e, b\}$ são normais em V. Tem-se $\langle a\rangle\langle b\rangle = V$ e $\langle a\rangle \cap \langle b\rangle = \{e\}$. Com o teorema do isomorfismo 1.7.17 obtém-se $V/\langle b\rangle \cong \langle a\rangle/\{e\} \cong \langle a\rangle$. Como todos os grupos com dois elementos são isomorfos, tem-se $V/\langle b\rangle \cong \mathbb{Z}_2$. Este resultado obtém-se também contando os elementos de $V/\langle b\rangle$, por exemplo usando o Teorema de Lagrange: $|V/\langle b\rangle| = |V : \langle b\rangle| = \frac{|V|}{|b|} = \frac{4}{2} = 2$.

Teorema 1.7.19. *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 1.7.13, 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 1.7.20. 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 $\mathbb{Z}_m/(n\mathbb{Z}/m\mathbb{Z}) \cong \mathbb{Z}_n$.

1.8 Grupos cíclicos

Definição 1.8.1. Um grupo gerado por um elemento diz-se *cíclico*.

Nota 1.8.2. Os elementos de um grupo cíclico $G = \langle g \rangle$ são as potências g^k, $k \in \mathbb{Z}$.

Exemplos 1.8.3. (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 $\bar{1} = 1 + n\mathbb{Z}$.
(iii) Por 1.6.9, qualquer grupo de ordem prima é cíclico.
(iv) O grupo de Klein $V = \{e, a, b, ab\}$ (cf. 1.5.11(iv)) não é cíclico.

Proposição 1.8.4. *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 1.8.5. *Qualquer subgrupo de um grupo cíclico é cíclico.*

Corolário 1.8.6. *Os subgrupos de $\mathbb{Z}$ são os conjuntos $m\mathbb{Z}$, $m \in \mathbb{N}$.*

Corolário 1.8.7. *(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 1.8.6, 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 $au + bv = d$. □

Notas 1.8.8. (i) Seja $G = \langle g \rangle$ um grupo cíclico e $H \subseteq G$ um subgrupo. Então H é normal em G e G/H é cíclico, gerado por Hg.
(ii) Qualquer grupo isomorfo a um grupo cíclico é cíclico.

Teorema 1.8.9. *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 1.8.6, 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 1.8.10. *Seja $G = \langle g \rangle$ um grupo cíclico finito. Então*

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

(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 $G = Im(f) = \{f(\bar{0}\}, \ldots, f(\overline{|g|-1})\} = \{e, g, \ldots, g^{|g|-1}\}$.
(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). □

Corolário 1.8.11. *(Pequeno teorema de Fermat) Num grupo finito* G *tem-se* $a^{|G|} = e$ *para todo o* $a \in G$.

Demonstração: Seja $a \in G$. Pelo Teorema de Lagrange, $|G| = |G : \langle a \rangle||a|$. Como $a^{|a|} = e$, $a^{|G|} = (a^{|a|})^{|G:\langle a \rangle|} = e^{|G:\langle a \rangle|} = e$. □

Proposição 1.8.12. *Sejam* $G = \langle g \rangle$ *um grupo cíclico finito.*

(a) Para todo o $k \in \mathbb{Z}$, $|g^k| = \dfrac{|g|}{\mathrm{mdc}(|g|, k)}$. *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, *nomeadamente* $\langle g^{\frac{|g|}{d}} \rangle$.

Demonstração: Exercício. □

Corolário 1.8.13. *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* $|g|$.

Exemplo 1.8.14. Os subgrupos próprios do grupo cíclico $\mathbb{Z}_6 = \{\bar{0}, \bar{1}, \bar{2}, \bar{3}, \bar{4}, \bar{5}\} = \langle \bar{1} \rangle$ são $\{\bar{0}\}$, $\langle \bar{2} \rangle = 2\mathbb{Z}/6\mathbb{Z}$ e $\langle \bar{3} \rangle = 3\mathbb{Z}/6\mathbb{Z}$. Tem-se $|\bar{2}| = 3$ e $|\bar{3}| = 2$. Como $|\bar{4}| = \frac{6}{2} = 3$, $\langle \bar{4} \rangle = \langle \bar{2} \rangle$. Como 5 e 6 são primos entre si, $\langle \bar{5} \rangle = \mathbb{Z}_6$.

Definição 1.8.15. 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 $\prod_{i=1}^{n} G_i$ ou por $G_1 \times \cdots \times G_n$.

Nota 1.8.16. Sejam $G_1, \ldots, G_n$ grupos e $\sigma \in S_n$ uma permutação. Um isomorfismo $\prod_{i=1}^{n} G_i \to \prod_{i=1}^{n} G_{\sigma(i)}$ é dado por $(g_1, \ldots g_n) \mapsto (g_{\sigma(1)}, \ldots, g_{\sigma(n)})$.

Exemplo 1.8.17. 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 $\mathbb{Z}_2 \times \{\bar{0}\}$ e $\{\bar{0}\} \times \mathbb{Z}_2$, e um grupo cíclico não pode ter mais do que um subgrupo de uma dada ordem. Notamos que $\mathbb{Z}_2 \times \mathbb{Z}_2$ é isomorfo ao grupo de Klein $V = \{e, a, b, ab\}$ (cf. 1.5.11(iv)). Um isomorfismo $f\colon V \to \mathbb{Z}_2 \times \mathbb{Z}_2$ é dado por $f(e) = (\bar{0}, \bar{0})$, $f(a) = (\bar{1}, \bar{0})$, $f(b) = (\bar{0}, \bar{1})$ e $f(ab) = (\bar{1}, \bar{1})$.

Proposição 1.8.18. *Sejam $n_1, \ldots n_k \geq 1$ inteiros. Então o produto directo $\prod_{i=1}^{k} \mathbb{Z}_{n_i}$ é cíclico se e só os inteiros $n_1, \ldots n_k$ são dois a dois primos entre si. Neste caso um isomorfismo $\mathbb{Z}_{n_1 \cdots n_k} \to \prod_{i=1}^{k} \mathbb{Z}_{n_i}$ 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 $f\colon \mathbb{Z} \to \prod_{i=1}^{k} \mathbb{Z}_{n_i}$ 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 1.7.13, $\bar{f}\colon \mathbb{Z}_{n_1 \cdots n_k} \to \prod_{i=1}^{k} \mathbb{Z}_{n_i}$, $\bar{f}(m + n_1 \cdots n_k\mathbb{Z}) = (m + n_1\mathbb{Z}, \ldots, m + n_k\mathbb{Z})$ é um monomorfismo. Como $|\mathbb{Z}_{n_1 \cdots n_k}| = n_1 \cdots n_k = |\prod_{i=1}^{k} \mathbb{Z}_{n_i}|$, $\bar{f}$ é de facto um isomorfismo e $\prod_{i=1}^{k} \mathbb{Z}_{n_i}$ 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 $\prod_{l=1}^{n} U_l$ e $\prod_{l=1}^{n} V_l$ são dois subgrupos diferentes de ordem d de $\prod_{i=1}^{k} \mathbb{Z}_{n_i}$. Logo $\prod_{i=1}^{k} \mathbb{Z}_{n_i}$ não é cíclico. □

Corolário 1.8.19. *(Teorema Chinês dos Restos) Sejam $n_1, \ldots n_k \geq 1$ inteiros dois a dois primos entre si e sejam $a_1, \ldots a_n \in \mathbb{Z}$. Então existe um inteiro x, único $\mod n_1 \cdots n_k$, tal que $x \equiv a_i \mod n_i$ para todo o $i \in \{1, \ldots, k\}$.*

1.9 Grupos abelianos

Definição 1.9.1. Um grupo *abeliano* é um grupo comutativo, isto é, um grupo cuja operação é comutativa.

Exemplos 1.9.2. (i) Os grupos cíclicos são abelianos.
(ii) O grupo de Klein $V = \{e, a, b, ab\}$ (cf. 1.5.11(iv)) é abeliano.
(iii) Para $n \geq 3$, o grupo simétrico S_n não é abeliano.
(iv) Para $n \geq 2$, o grupo $GL_n(\mathbb{R})$ não é abeliano.

Observações 1.9.3. (i) Qualquer subgrupo de um grupo abeliano é abeliano e normal.
(ii) Para qualquer grupo G, o centro $Z(G)$ é um subgrupo abeliano. Um grupo G é abeliano se e só se $G = Z(G)$.
(iii) O único automorfismo interno de um grupo abeliano é a identidade.

Proposição 1.9.4. *Sejam G um grupo abeliano, $a_1, \ldots, a_n \in G$ e $\sigma \in S_n$ uma permutação. Então $a_1 \cdots a_n = a_{\sigma(1)} \cdots a_{\sigma(n)}$.*

Demonstração: Procedemos por indução. Para $n = 1$ e $n = 2$, a propriedade é óbvia. Seja $n \geq 3$ tal que a propriedade é válida para $n - 1$. Seja $k = \sigma^{-1}(n)$ e seja $\alpha \in S_{n-1}$ a permutação dada por

$$\alpha(i) = \begin{cases} \sigma(i), & 1 \leq i < k, \\ \sigma(i+1), & k \leq i \leq n-1. \end{cases}$$

Pela hipótese de indução, $a_{\alpha(1)} \cdots a_{\alpha(n-1)} = a_1 \cdots a_{n-1}$. Temos então

$$\begin{aligned} a_{\sigma(1)} \cdots a_{\sigma(n)} &= (a_{\sigma(1)} \cdots a_{\sigma(k-1)}) a_{\sigma(k)} (a_{\sigma(k+1)} \cdots a_{\sigma(n)}) \\ &= (a_{\sigma(1)} \cdots a_{\sigma(k-1)}) (a_{\sigma(k+1)} \cdots a_{\sigma(n)}) a_{\sigma(k)} \\ &= (a_{\alpha(1)} \cdots a_{\alpha(k-1)}) (a_{\alpha(k)} \cdots a_{\alpha(n-1)}) a_n \\ &= (a_{\alpha(1)} \cdots a_{\alpha(n-1)}) a_n \\ &= (a_1 \cdots a_{n-1}) a_n \\ &= a_1 \cdots a_n. \end{aligned}$$

□

Notação 1.9.5. Se os grupos $G_1, \ldots, G_n$ são abelianos, o seu produto directo é também um grupo abeliano. Neste caso o produto cartesiano de $G_1, \ldots, G_n$ é também designado por *soma directa* de $G_1, \ldots, G_n$ e é denotado por $\bigoplus_{i=1}^{n} G_i$ ou por $G_1 \oplus \cdots \oplus G_n$.

Teorema 1.9.6. *Seja G um grupo abeliano finitamente gerado. Então existem números naturais únicos k e l e potências de números primos únicas $1 < n_1 \leq \cdots \leq n_l$ tais que*

$$G \cong \underbrace{\mathbb{Z} \oplus \cdots \oplus \mathbb{Z}}_{k \text{ vezes}} \oplus \mathbb{Z}_{n_1} \oplus \cdots \oplus \mathbb{Z}_{n_l}.$$

Demonstração: Uma demonstração encontra-se por exemplo em [1, 4.10.1.14] ou em [5, 3.13]. □

1.10 Grupos simétricos

Teorema 1.10.1. *(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 1.10.2. *Cada grupo finito G é isomorfo a um subgrupo de $S_{|G|}$.*

Notação 1.10.3. 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 1.10.4. 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 1.10.5. $|S_n| = n!$

Demonstração: Exercício. □

Definição 1.10.6. Uma permutação $\sigma \in S_n$ diz-se um *ciclo* se existem $k, i_1, \ldots, i_k \in \{1, \ldots, n\}$ tais que $\sigma(i_j) = i_{j+1}$ para $1 \leq j < k$, $\sigma(i_k) = i_1$ e $\sigma(i) = i$ para $i \notin \{i_1, \ldots, i_k\}$. O ciclo assim definido é denotado por $(i_1, \ldots, i_k)$. Aos ciclos da forma (i, j) com $i \neq j \in \{1, \ldots, n\}$ chama-se também *transposições*. Dois ciclos $(i_1, \ldots, i_k)$ e $(j_1, \ldots, j_l)$ dizem-se *disjuntos* se $\{i_1, \ldots, i_k\} \cap \{j_1, \ldots, j_l\} = \emptyset$.

Observações 1.10.7. (i) A identidade de $\{1, \ldots, n\}$ é um ciclo. 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 ciclos disjuntos, então $\alpha\beta = \beta\alpha$. Logo se $\alpha_1, \ldots \alpha_l \in S_n$ são ciclos dois a dois disjuntos, então $|\alpha_1 \cdots \alpha_l| = \text{mmc}(|\alpha_1|, \ldots, |\alpha_l|)$.

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

Proposição 1.10.8. *Cada permutação $\sigma \in S_n \setminus \{id\}$ pode ser factorizada em ciclos dois a dois disjuntos de $S_n \setminus \{id\}$.*

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

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

Note-se que este mínimo existe pois $\sigma^{n!} = id$ pelo pequeno teorema de Fermat 1.8.11. 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 ciclo 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 ciclos $(j_l, \sigma(j_l), \ldots, \sigma^{k_{j_l}-1}(j_l))$ 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 1.10.9. *S_n é gerado pelos ciclos.*

Exemplo 1.10.10. 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 1.10.11. É possível mostrar que a factorização de uma permutação $\sigma \in S_n \setminus \{id\}$ em ciclos dois a dois disjuntos de $S_n \setminus \{id\}$ é única a menos da ordem dos factores (exercício).

Proposição 1.10.12. *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 1.10.13. *S_n é gerado pelas transposições.*

Definição 1.10.14. 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 1.10.15. (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 1.10.16. *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 $\operatorname{sgn}(\alpha\beta)=(-1)^{r+s}=(-1)^{l+k-2m}=(-1)^l(-1)^k(-1)^{-2m}=(-1)^l(-1)^k=(-1)^k(-1)^l=\operatorname{sgn}(\alpha)\operatorname{sgn}(\beta)$. □

Observações 1.10.17. (i) 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 factorizado 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, um ciclo de ordem par é ímpar e um ciclo de ordem ímpar é par.

(ii) O núcleo do homomorfismo $\operatorname{sgn}\colon S_n\to\{1,-1\}$ é conhecido como *grupo alterno* A_n.

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;
- $(A, \cdot)$ 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.

Proposição 2.1.2. *O grupo aditivo de um anel é abeliano.*

Demonstração: Sejam A um anel e $a, b \in A$. Então $a + a + b + b = 1a + 1a + 1b + 1b = (1 + 1)a + (1 + 1)b = (1 + 1)(a + b) = 1(a + b) + 1(a + b) = a + b + a + b$. Logo $a + b = -a + a + a + b + b - b = -a + a + b + a + b - b = b + a$. □

Nota 2.1.3. Muitos autores não exigem a existência de um elemento neutro para a multiplicação na definição de um anel. Esses autores devem exigir na definição que o grupo aditivo de um anel seja abeliano. Sem o elemento 1, o grupo aditivo de um anel não é automaticamente abeliano.

Exemplos 2.1.4. (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 $\mathcal{M}_n(\mathbb{R})$ das matrizes reais $n \times n$ é um anel relativamente à adição e à multiplicação de matrizes.

(iv) O conjunto dos endomorfismos de um grupo abeliano G, $End(G)$, é um anel. A multiplicação é a composição de funções e a adição é dada por $(f + g)(x) = f(x) + g(x)$.

(v) Sejam A um anel e X um conjunto não vazio. O conjunto A^X das funções de X para A é um anel com as operações definidas por $(f+g)(x) = f(x)+g(x)$ e $(f \cdot g)(x) = f(x) \cdot g(x)$ $(x \in X)$.

(vi) 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.

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

Proposição 2.1.5. *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 2.1.6. Pela propriedade (ii) da proposição precedente, $(-1)x = x(-1) = -x$ para qualquer elemento x de um anel.

Proposição 2.1.7. *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 2.1.8. *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 2.1.9. 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 2.1.10. Um subanel B de um anel A é um anel relativamente à adição e à multiplicação de A.

Exemplos 2.1.11. (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 2.1.12. 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 2.1.13. (i) Um homomorfismo de anéis é um homomorfismo dos grupos aditivos.

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

Exemplos 2.1.14. (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.

(iii) Para qualquer anel A, a função constante $A \to \{0\}$, $x \mapsto 0$ é um epimorfismo de anéis.

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

Proposição 2.1.15. *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 2.1.16. *A função inversa de um isomorfismo de anéis $f \colon A \to B$ é um isomorfismo de anéis.*

Demonstração: Por 1.4.8, 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 2.1.17. *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 um anel, X um conjunto não vazio e $Y \subseteq X$. Então $\{f \colon X \to A \mid f(Y) \subseteq \{0\}\}$ é um ideal de A^X.

(iv) 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 1.7.5, $f(I)$ 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 1.5.8, $\bigcap_{k\in K} I_k$ 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 $\mathbb{Z}_4$, $(\bar{2}) = \bar{2}\mathbb{Z}_2 = \{\bar{0}, \bar{2}\}$.

Nota 2.2.9. Sejam A um anel e I e J ideais de A. Então tem-se $(I \cup J) = I + J = \{i + j \,|\, i \in I,\ j \in J\}$. O ideal $(\{ij \,|\, i \in I,\ j \in J\})$ é denotado por IJ. Note-se que, em geral, $IJ \neq \{ij \,|\, i \in I,\ j \in J\}$.

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.

(ii) Em $\mathbb{Q}$ e $\mathbb{R}$, os únicos ideais são os ideais principais (0) e (1).

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 um monomorfismo se e só se $I = \mathrm{Ker}(f)$.*

Demonstração: Por 1.7.13, 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 1.7.13, $\bar{f}$ é um monomorfismo se e só se $I = \mathrm{Ker}(f)$. □

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 1.7.17, 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. □

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 1.7.19, 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 1.7.19, 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. □

2.3 Domínios de integridade e corpos

Definição 2.3.1. Um elemento $a \neq 0$ de um anel A diz-se um *divisor de zero* se existe um elemento $b \neq 0$ em A tal que $ab = 0$ ou $ba = 0$. Um *domínio de integridade* é um anel comutativo com $1 \neq 0$ que não admite divisores de zero.

Exemplos 2.3.2. (i) $\mathbb{Z}$, $\mathbb{Q}$ e $\mathbb{R}$ são domínios de intregridade.

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

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

Observações 2.3.3. (i) Para um anel A, a condição $1 \neq 0$ é equivalente à condição $A \neq \{0\}$. Com efeito, se $1 \neq 0$, então $A \neq \{0\}$. Se $1 = 0$, então para qualquer $a \in A$, $a = 1a = 0a = 0$. Um anel com mais do que um elemento diz-se *não nulo*.

(ii) Um anel comutativo não nulo A é um domínio de integridade se e só se para quaisquer $a, b \in A$, $ab = 0$ implica $a = 0$ ou $b = 0$.

(iii) O elemento 1 de um anel não é um divisor de zero. Com efeito, se $1a = 0$ então $a = 0$.

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 com $1 \neq 0$ 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. Temos $1 + I \neq I$ pois senão teriamos $1 \in I$ e $I = A$. 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. O conjunto das unidades de um anel A é denotado por A^*. Um anel comutativo K diz-se um *corpo* se $K^* = K \setminus \{0\}$, isto é, se todos os elementos a menos de 0 são invertíveis.

Exemplos 2.3.10. (i) $\mathbb{Q}$ e $\mathbb{R}$ são corpos.

(ii) $\mathbb{Z}$ não é um corpo.

Observações 2.3.11. (i) Num corpo, $1 \neq 0$ pois 1 é invertível e 0 não. Logo um corpo tem sempre pelo menos dois elementos.

(ii) Um anel comutativo não nulo é um corpo se e só se todos os elementos diferentes de 0 são invertíveis. Com efeito, num anel não nulo, 0 não é invertível.

(iii) 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 $I = K$.

Proposição 2.3.12. *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 $1 \neq 0$ e K é comutativo, K é um domínio de integridade. □

Corolário 2.3.13. *Um anel comutativo A é um corpo se e só se $A \setminus \{0\}$ é um grupo relativamente à multiplicação de A.*

Proposição 2.3.14. *Qualquer domínio de integridade finito é um corpo.*

Demonstração: Se A é um domínio de integridade finito, então $(A\setminus\{0\}, \cdot)$ é um semigrupo finito. Por 2.3.4, este semigrupo satisfaz as leis do corte. Logo $(A \setminus \{0\}, \cdot)$ é um grupo e A é um corpo. □

Corolário 2.3.15. *$\mathbb{Z}_n$ é um corpo se e só se n é primo.*

Corolário 2.3.16. *(Teorema de Fermat) Sejam p um número primo e $a \in \mathbb{Z}$ tal que $a \not\equiv 0 \mod p$. Então $a^{p-1} \equiv 1 \mod p$.*

Demonstração: Como p é primo, $\mathbb{Z}_p$ é um corpo e $\mathbb{Z}_p \setminus \{\bar{0}\} = \mathbb{Z}_p^*$ é um grupo relativamente à multiplicação. Como $|\mathbb{Z}_p \setminus \{\bar{0}\}| = p-1$ e $a + p\mathbb{Z} \in \mathbb{Z}_p \setminus \{\bar{0}\}$, pelo pequeno teorema de Fermat, $(a+p\mathbb{Z})^{p-1} = a^{p-1} + p\mathbb{Z} = \bar{1}$, ou seja, $a^{p-1} \equiv 1 \mod p$. □

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 $(ac,bd) \sim (xu, yv)$. □

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

Proposição 2.3.19. *Seja A um domínio de integridade. Então o corpo de fracções $Q(A)$ é um corpo e a aplicação $A \to Q(A)$, $a \mapsto \dfrac{a}{1}$ é um monomorfismo de anéis.*

Demonstração: Exercício. □

Exemplos 2.3.20. (i) $Q(\mathbb{Z}) = \mathbb{Q}$.

(ii) Para qualquer corpo K, o monomorfismo $K \to Q(K)$, $a \mapsto \dfrac{a}{1}$ é um isomorfismo de anéis.

Definição 2.3.21. Seja A um anel. A *caracteristica* de A é definida por

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

Exemplos 2.3.22. Tem-se $\mathrm{car}(\mathbb{Z}) = \mathrm{car}(\mathbb{Q}) = \mathrm{car}(\mathbb{R}) = 0$ e $\mathrm{car}(\mathbb{Z}_n) = n$.

Notas 2.3.23. (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 $\mathrm{car}(A) = n$ se e só se $\mathrm{Ker}(f) = n\mathbb{Z}$. Segue-se que a caracteristica de A é o único número natural n tal que A contém um subanel isomorfo a $\mathbb{Z}/n\mathbb{Z}$.

Proposição 2.3.24. *A caracteristica de um domínio de integridade é ou* 0 *ou um número primo.*

Demonstração: Seja A um domínio de integridade com $\mathrm{car}(A) \neq 0$. Então o elemento 1 de A tem ordem finita e $\mathrm{car}(A) = |1|$. 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 $\mathrm{car}(A) = |1|$ é um número primo. □

Nota 2.3.25. Existe uma múltiplicação com a qual o grupo $\mathbb{Z}_2 \times \mathbb{Z}_2$ é um corpo. Este corpo tem caracteristica 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 $\mathbb{F}_{p^n}$.

Capítulo 3

Reticulados e Álgebras de Boole

3.1 Reticulados

Recorde-se que uma *relação de ordem parcial* num conjunto X é uma relação reflexiva, anti-simétrica e transitiva em X. Um *conjunto parcialmente ordenado (c.p.o.)* é um par $(X, \leq)$ em que X é um conjunto e $\leq$ é uma relação de ordem parcial em X.

Definição 3.1.1. Sejam $(X, \leq)$ um conjunto parcialmente ordenado e $A \subseteq X$. Um elemento $x \in X$ diz-se *majorante (minorante)* de A se para qualquer $a \in A$, $a \leq x$ ($x \leq a$). Um elemento $b \in X$ diz-se *supremo (ínfimo)* de A se b é um majorante (minorante) de A e se $b \leq x$ ($x \leq b$) para qualquer majorante (minorante) x de A.

Proposição 3.1.2. *Sejam $(X, \leq)$ um conjunto parcialmente ordenado e $A \subseteq X$. Se A admite um supremo (ínfimo), então este é único.*

Demonstração: Sejam b, c supremos de A. Então b e c são majorantes de A. Como b é um supremo de A, $b \leq c$. Como c é um supremo de A, $c \leq b$. Logo $b = c$. O caso do ínfimo é análogo. □

Notação 3.1.3. Seja $(X, \leq)$ um conjunto parcialmente ordenado. O supremo (ínfimo) de um subconjunto $A \subseteq X$ é, se existe, denotado por $\sup A$ ($\inf A$). O *supremo (ínfimo)* de dois elementos $a, b \in X$ é, se existe, o supremo (ínfimo) do conjunto $\{a, b\}$ e escreve-se $a \vee b = \sup\{a, b\}$ ($a \wedge b = \inf\{a, b\}$).

Definição 3.1.4. Um *reticulado de ordem* é um conjunto parcialmente ordenado não vazio em que existem o supremo e o ínfimo de cada dois elementos.

Exemplos 3.1.5. (i) Recorde-se que um c.p.o. $(X, \leq)$ diz-se *totalmente ordenado* se para quaisquer $a, b \in X$, $a \leq b$ ou $b \leq a$. Qualquer subconjunto de $\mathbb{R}$ com a ordem natural é totalmente ordenado. Qualquer conjunto totalmente ordenado não vazio é um reticulado

de ordem. Para quaisquer dois elementos a e b de um conjunto totalmente ordenado tem-se $a \vee b, a \wedge b \in \{a, b\}$, sendo $a \vee b = a \Leftrightarrow b \leq a$ e $a \wedge b = a \Leftrightarrow a \leq b$.

(ii) $\mathbb{N} \setminus \{0\}$ munido da relação $|$ dada por

$$a|b \Leftrightarrow a \text{ divide } b$$

é um reticulado de ordem. Neste reticulado, $a \vee b = \text{mmc}(a, b)$ e $a \wedge b = \text{mdc}(a, b)$.

(iii) Seja A um conjunto. O conjunto potência $\mathcal{P}(A)$ munido da relação $\subseteq$ é um reticulado de ordem. Para $X, Y \in \mathcal{P}(A)$, $X \vee Y = X \cup Y$ e $X \cap Y = X \cap Y$.

(iv) Seja G um grupo. O conjunto $Sub(G)$ dos subgrupos de G munido da relação $\subseteq$ é um reticulado de ordem. Para $H, K \in Sub(G)$, $H \vee K = \langle H \cup K \rangle$ e $H \wedge K = H \cap K$.

(v) Seja G um grupo. O conjunto $\mathcal{N}(G)$ dos subgrupos normais de G munido da relação $\subseteq$ é um reticulado de ordem. Para $H, K \in \mathcal{N}(G)$, $H \vee K = HK = \langle H \cup K \rangle$ e $H \wedge K = H \cap K$.

(vi) Seja A um anel. O conjunto $\mathcal{I}(G)$ dos ideais de A munido da relação $\subseteq$ é um reticulado de ordem. Para $I, J \in \mathcal{I}(A)$, $I \vee J = I + J = \langle I \cup J \rangle$ e $I \wedge J = I \cap J$.

Lema 3.1.6. *Sejam $(R, \leq)$ um reticulado de ordem, $a \in R$, $A \subseteq R$, $b = \sup A$ e $c = \inf A$. Então $a \vee b = \sup A \cup \{a\}$ e $a \wedge c = \inf A \cup \{a\}$.*

Demonstração: Tem-se $a \leq a \vee b$ e $x \leq b \leq a \vee b$ para todo o $x \in A$. Logo $a \vee b$ é um majorante de $A \cup \{a\}$. Seja $d \in R$ um majorante de $A \cup \{a\}$. Então d é um majorante de A, pelo que $b \leq d$. Por outro lado, $a \leq d$. Logo d é um majorante de $\{a, b\}$, pelo que $a \vee b \leq d$. Logo $a \vee b = \sup A \cup \{a\}$. A demonstração da outra igualdade é análoga.

Proposição 3.1.7. *Sejam $(R, \leq)$ um reticulado de ordem e $a, b, c \in R$. Então*

(a) (associatividade) $a \vee (b \vee c) = (a \vee b) \vee c$ e $a \wedge (b \wedge c) = (a \wedge b) \wedge c$;

(b) (comutatividade) $a \vee b = b \vee a$ e $a \wedge b = b \wedge a$;

(c) (idempotência) $a \vee a = a$ e $a \wedge a = a$;

(d) (absorção) $a \vee (a \wedge b) = a$ e $a \wedge (a \vee b) = a$.

Demonstração: As propriedades (b) e (c) são óbvias.

(a) Por 3.1.6 e (b), $a \vee (b \vee c) = \sup\{b, c\} \cup \{a\} = \sup\{a, b, c\} = \sup\{a, b\} \cup \{c\} = c \vee (a \vee b) = (a \vee b) \vee c$. Do mesmo modo, $a \wedge (b \wedge c) = (a \wedge b) \wedge c$.

(d) Como $a \wedge b \leq a$, $a \vee (a \wedge b) = a$. Como $a \leq a \vee b$, $a \wedge (a \vee b) = a$. □

Definição 3.1.8. Um *reticulado* é um triplo $(R, \vee, \wedge)$ em que R é um conjunto não vazio e $\vee$ e $\wedge$ são operações binárias em R que satisfazem as condições (a) - (d) da proposição 3.1.7. Muitas vezes indicaremos um reticulado simplesmente pelo símbolo do conjunto subjacente.

Proposição 3.1.9. *Sejam R um reticulado e $a, b \in R$. Então $a \vee b = b \Leftrightarrow a \wedge b = a$. No caso de um reticulado de ordem, estas condições são ainda equivalentes à condição $a \leq b$.*

Demonstração: Se $a \vee b = b$, então pela propriedade de absorção, $a \wedge b = a \wedge (a \vee b) = a$. Do mesmo modo, se $a \wedge b = a$, então $a \vee b = (a \wedge b) \vee b = b \vee (b \wedge a) = b$. É óbvio que no caso de um reticulado de ordem, $a \leq b \Leftrightarrow a \vee b = b$. □

Proposição 3.1.10. *Seja $R = (R, \vee, \wedge)$ um reticulado. Então a relação $\leq$ definida por $a \leq b \Leftrightarrow a \vee b = b$ é uma relação de ordem parcial em R e o conjunto parcialmente ordenado $(R, \leq)$ é um reticulado de ordem. As operações $\vee$ e $\wedge$ do reticulado de ordem $(R, \leq)$ são as operações $\vee$ e $\wedge$ do reticulado $R = (R, \vee, \wedge)$.*

Demonstração: Como $a \vee a = a$, $\leq$ é reflexiva. Sejam $a, b \in R$ tais que $a \leq b$ e $b \leq a$. Então $a \vee b = b$ e $b \vee a = a$. Como $a \vee b = b \vee a$, $a = b$. Logo $\leq$ é anti-simétrica. Sejam $a, b, c \in R$ tais que $a \leq b$ e $b \leq c$. Então $a \vee b = b$ e $b \vee c = c$. Logo $a \vee c = a \vee (b \vee c) = (a \vee b) \vee c = b \vee c = c$, ou seja, $a \leq c$. Logo $\leq$ é transitiva e portanto uma relação de ordem parcial.

Sejam $a, b \in R$. Tem-se $a \vee (a \vee b) = (a \vee a) \vee b = a \vee b$ e então $a \leq a \vee b$. Do mesmo modo, $b \leq b \vee a$. Como $a \vee b = b \vee a$, $a \vee b$ é um majorante de $\{a, b\}$. Seja x um majorante de $\{a, b\}$. Então $a \vee x = x$ e $b \vee x = x$. Logo $(a \vee b) \vee x = a \vee (b \vee x) = a \vee x = x$ e portanto $a \vee b \leq x$. Segue-se que $a \vee b = \sup\{a, b\}$. De maneira análoga mostra-se que $a \wedge b = \inf\{a, b\}$. Segue-se que $(R, \leq)$ é um reticulado de ordem e que as operações $\vee$ e $\wedge$ de $(R, \leq)$ são as operações $\vee$ e $\wedge$ do reticulado $R = (R, \vee, \wedge)$. □

Observação 3.1.11. As proposições 3.1.7, 3.1.9 e 3.1.10 estabelecem uma correspondência bijectiva entre reticulados e reticulados de ordem. Graças a esta correspondência podemos e vamos considerar um reticulado como um reticulado de ordem e vice versa. Em particular temos num reticulado a relação de ordem parcial $\leq$ definida por $a \leq b \Leftrightarrow a \vee b = b$. Pela proposição 3.1.9, tem-se $a \leq b \Leftrightarrow a \wedge b = a$.

3.2 Subreticulados, produtos e homomorfismos

Definição 3.2.1. Seja R um reticulado. Um subconjunto não vazio $S \subseteq R$ diz-se um *subreticulado* de R se para quaisquer $a, b \in S$, $a \vee b \in S$ e $a \wedge b \in S$.

Observação 3.2.2. Um subreticulado de um reticulado R é um reticulado relativamente às operações de R.

Exemplos 3.2.3. (i) Qualquer subconjunto não vazio de um reticulado totalmente ordenado R é um subreticulado de R.

(ii) Seja G um grupo. O reticulado $\mathcal{N}(G)$ dos subgrupos normais de G é um subreticulado do reticulado $Sub(G)$ dos subgrupos de G mas os reticulados $\mathcal{N}(G)$ e $Sub(G)$ não são, em geral, subreticulados do reticulado potência $\mathcal{P}(G)$.

Proposição 3.2.4. *Sejam R um reticulado e $(S_i)_{i\in I}$ uma familia não vazia de subreticulados de R. Então a intersecção $\bigcap_{i\in I} S_i$ é ou vazia ou um subreticulado de R.*

Demonstração: Exercício. □

Definição 3.2.5. Sejam R um reticulado e $X \subseteq R$ um subconjunto não vazio. O *subreticulado gerado por X*, $\langle X\rangle$, é a intersecção dos subreticulados de R 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 *subreticulado de R gerado pelos elementos $x_1, \ldots, x_n$*.

Exemplo 3.2.6. Sejam R um reticulado e $a, b \in R$. Então $\langle a, b\rangle = \{a, b, a \wedge b, a \vee b\}$.

Definição 3.2.7. O *produto* $\prod_{i=1}^{n} R_i = R_1 \times \cdots \times R_n$ dos reticulados $R_1, \ldots, R_n$ é o reticulado cujo conjunto subjacente é o produto cartesiano $R_1 \times \cdots \times R_n$ e cujas operações são definidas componente por componente.

Proposição 3.2.8. *Sejam $R_1, \ldots, R_n$ reticulados e $(a_1, \ldots, a_n), (b_1, \ldots, b_n) \in \prod_{i=1}^{n} R_i$. Então $(a_1, \ldots, a_n) \leq (b_1, \ldots, b_n)$ se e só se $a_i \leq b_i$ para todo o $i \in \{1, \ldots, n\}$.*

Demonstração: Tem-se $(a_1, \ldots, a_n) \leq (b_1, \ldots, b_n) \Leftrightarrow (a_1, \ldots, a_n) \vee (b_1, \ldots, b_n) = (b_1, \ldots, b_n) \Leftrightarrow (a_1 \vee b_1, \ldots, a_n \vee b_n) = (b_1, \ldots, b_n) \Leftrightarrow \forall i \in \{1, \ldots, n\}\ a_i \vee b_i = b_i \Leftrightarrow \forall i \in \{1, \ldots, n\}\ a_i \leq b_i$. □

Definição 3.2.9. Sejam R e R' dois reticulados. Uma aplicação $f\colon R \to R'$ diz-se um *homomorfismo de reticulados* se para quaisquer $a, b \in R$, $f(a \vee b) = f(a) \vee f(b)$ e $f(a \wedge b) = f(a) \wedge f(b)$. Um homomorfismo de reticulados diz-se um *monomorfismo* (*epimorfismo, isomorfismo*) se é injectivo (sobrejectivo, bijectivo). Um homomorfismo (isomorfismo) de reticulados $f\colon R \to R$ diz-se um *endomorfismo* (*automorfismo*) de reticulados. Os reticulados R e R' dizem-se *isomorfos*, $R \cong R'$, se existe um isomorfismo de reticulados entre eles.

Exemplos 3.2.10. (i) Sejam R um reticulado e S um subreticulado de R. Então a inclusão $S \to R$, $x \mapsto x$ é um monomorfismo de reticulados.

(ii) Seja $f\colon X \to Y$ uma função. Então a aplicação $\mathcal{P}(Y) \to \mathcal{P}(X)$, $A \mapsto f^{-1}(A)$ é um homomorfismo de reticulados. Este homomorfismo é um isomorfismo de reticulados se e só se a função f é bijectiva.

Proposição 3.2.11. *Sejam $f\colon R \to S$ e $g\colon S \to T$ dois homomorfismos de reticulados. Então $g \circ f\colon R \to T$ é um homomorfismo de reticulados.*

Demonstração: Exercício. □

Proposição 3.2.12. *Seja $f\colon R \to S$ um isomorfismo de reticulados. Então $f^{-1}\colon S \to R$ é um isomorfismo de reticulados.*

Demonstração: Exercício. □

Proposição 3.2.13. *Sejam $f\colon R \to R'$ um homomorfismo de reticulados, S um subreticulado de R e S' um subreticulado de R'. Então $f(S)$ é um subreticulado de R' e $f^{-1}(S')$ é ou vazio ou um subreticulado de R.*

Demonstração: Exercício. □

Notação 3.2.14. Seja $f\colon R \to R'$ um homomorfismo de reticulados. Escreve-se $\mathrm{Im}(f) = f(R)$.

Proposição 3.2.15. *Sejam $f\colon R \to S$ um homomorfismo de reticulados e $a, b \in R$ tais que $a \leq b$. Então $f(a) \leq f(b)$.*

Demonstração: Tem-se $a \vee b = b$ e então $f(a) \vee f(b) = f(a \vee b) = f(b)$. Logo $f(a) \leq f(b)$. □

Observação 3.2.16. Seja G um grupo. A inclusão $Sub(G) \to \mathcal{P}(G)$, $H \mapsto H$ é compatível com as relações de ordem parcial mas não é, em geral, um homomorfismo de reticulados.

Proposição 3.2.17. *Sejam R e S dois reticulados e $f\colon R \to S$ uma aplicação bijectiva. Então f é um isomorfismo de reticulados se e só se para quaisquer $a, b \in R$, $a \leq b \Leftrightarrow f(a) \leq f(b)$.*

Demonstração: Por 3.2.15 e 3.2.12, basta mostrar que f é um isomorfismo de reticulados se para quaisquer $a, b \in R$, $a \leq b \Leftrightarrow f(a) \leq f(b)$. Sejam $a, b \in R$. Tem-se $a, b \leq a \vee b$ e portanto $f(a), f(b) \leq f(a \vee b)$. Logo $f(a) \vee f(b) \leq f(a \vee b)$. Como f é sobrejectiva, existe $x \in R$ tal que $f(x) = f(a) \vee f(b)$. Como $f(a), f(b) \leq f(x) \leq f(a \vee b)$, tem-se $a, b \leq x \leq a \vee b$ e então $x = a \vee b$. Logo $f(a \vee b) = f(a) \vee f(b)$. De maneira análoga mostra-se que $f(a \wedge b) = f(a) \wedge f(b)$. Segue-se que f é um isomorfismo de reticulados. □

3.3 Relações de congruência e reticulados quociente

Definição 3.3.1. Seja R um reticulado. Uma relação de congruência em R é uma relação de equivalência $\equiv$ em R tal que para quaisquer $a, a', b, b' \in R$, se $a \equiv a'$ e $b \equiv b'$, então $a \vee b \equiv a' \vee b'$ e $a \wedge b \equiv a' \wedge b'$.

Exemplo 3.3.2. Seja $f\colon R \to R'$ um homomorfismo de reticulados. Então uma relação de congruência em R é dada por $x \equiv y \Leftrightarrow f(x) = f(y)$. Esta relação de congruência é chamada o *núcleo* de f.

Definição 3.3.3. Sejam R um reticulado e $\equiv$ uma relação de congruência em R. O *reticulado quociente* $R/\equiv$ é o conjunto quociente $R/\equiv$ munido das operações $\vee$ e $\wedge$ dadas por $[a] \vee [b] = [a \vee b]$ e $[a] \wedge [b] = [a \wedge b]$. Verifica-se facilmente que o reticulado quociente $R/\equiv$ é de facto um reticulado e que a aplicação $\pi\colon R \to R/\equiv$, $a \mapsto [a]$ é um epimorfismo de reticulados. Chama-se *epimorfismo canónico* a este epimorfismo.

Teorema 3.3.4. *Sejam $f\colon R \to R'$ um homomorfismo de reticulados, $\equiv$ uma relação de congruência em R tal que para quaisquer $x, y \in R$, $x \equiv y \Rightarrow f(x) = f(y)$ e $\pi\colon R \to R/\equiv$ o epimorfismo canónico. Então existe um único homomorfismo de reticulados $\bar{f}\colon R/\equiv \to R'$ tal que $\bar{f} \circ \pi = f$. O homomorfismo $\bar{f}$ é um monomorfismo se e só se $\equiv$ é o núcleo de f.*

Demonstração: Sejam $x, y \in R$ tais que $x \equiv y$. Então $f(x) = f(y)$. Segue-se que a aplicação $\bar{f}\colon R/\equiv \to R'$, $\bar{f}([x]) = f(x)$ está bem definida. Tem-se $\bar{f}([x] \vee [y]) = \bar{f}([x \vee y]) = f(x \vee y) = f(x) \vee f(y) = \bar{f}([x]) \vee \bar{f}([y])$ e $\bar{f}([x] \wedge [y]) = \bar{f}([x \wedge y]) = f(x \wedge y) = f(x) \wedge f(y) = \bar{f}([x]) \wedge \bar{f}([y])$. Logo $\bar{f}$ é um homomorfismo de reticulados. Por definição, $\bar{f} \circ \pi = f$. Seja $g\colon R/\equiv \to R'$ um homomorfismo de reticulados tal que $g \circ \pi = f$. Então para qualquer $x \in R$, $g([x]) = g \circ \pi(x) = f(x) = \bar{f} \circ \pi(x) = \bar{f}([x])$, pelo que $g = \bar{f}$.

Suponhamos que $\equiv$ é o núcleo de f. Sejam $x, y \in R$ tais que $\bar{f}([x]) = \bar{f}([y])$. Então $f(x) = f(y)$ e $x \equiv y$. Segue-se que $[x] = [y]$ e então que $\bar{f}$ é um monomorfismo. Suponhamos inversamente que $\bar{f}$ é um monomorfismo. Sejam $x, y \in R$ tais que $f(x) = f(y)$. Então $\bar{f}([x]) = f(x) = f(y) = \bar{f}([y])$. Logo $[x] = [y]$ e portanto $x \equiv y$. Segue-se que $\equiv$ é o núcleo de f. □

Corolário 3.3.5. *(Teorema do homomorfismo) Sejam $f\colon R \to R'$ um homomorfismo de reticulados e $\equiv$ o núcleo de f. Então um isomorfismo de reticulados $R/\equiv \to \mathrm{Im}(f)$ é dado por $[a] \mapsto f(a)$.*

3.4 Reticulados distributivos e modulares

Definição 3.4.1. Um reticulado R diz-se *distributivo* se para quaisquer três elementos $a, b, c \in R$, $a \wedge (b \vee c) = (a \wedge b) \vee (a \wedge c)$.

Proposição 3.4.2. *Um reticulado R é distributivo se e só se para quaisquer três elementos $a, b, c \in R$, $a \vee (b \wedge c) = (a \vee b) \wedge (a \vee c)$.*

Demonstração: Suponhamos primeiramente que R é distributivo. Sejam $a, b, c \in R$. Então $(a \vee b) \wedge (a \vee c) = ((a \vee b) \wedge a) \vee ((a \vee b) \wedge c) = a \vee ((a \vee b) \wedge c) = a \vee (c \wedge (a \vee b)) = a \vee ((c \wedge a) \vee (c \wedge b)) = (a \vee (c \wedge a)) \vee (c \wedge b) = a \vee (c \wedge b) = a \vee (b \wedge c)$.

Suponhamos inversamente que para quaisquer três elementos $a, b, c \in R$, $a \vee (b \wedge c) = (a \vee b) \wedge (a \vee c)$. Sejam $a, b, c \in R$. Então $(a \wedge b) \vee (a \wedge c) = ((a \wedge b) \vee a) \wedge ((a \wedge b) \vee c) = a \wedge ((a \wedge b) \vee c) = a \wedge (c \vee (a \wedge b)) = a \wedge ((c \vee a) \wedge (c \vee b)) = (a \wedge (c \vee a)) \wedge (c \vee b) = a \wedge (c \vee b) = a \wedge (b \vee c)$. Logo R é distributivo. □

Observação 3.4.3. Sejam R um reticulado distributivo e $a, b, c \in R$. Como $\vee$ e $\wedge$ são comutativas, tem-se $(a \vee b) \wedge c = (a \wedge c) \vee (b \wedge c)$ e $(a \wedge b) \vee c = (a \vee c) \wedge (b \vee c)$.

Exemplos 3.4.4. (i) O conjunto potência de um conjunto é um reticulado distributivo.

(ii) Qualquer reticulado totalmente ordenado R é distributivo. Com efeito, sejam $a, b, c \in R$. Se $b, c \leq a$, então $a \wedge (b \vee c) = b \vee c = (a \wedge b) \vee (a \wedge c)$. Se $a \leq b$ e $a \leq c$, então $a \wedge (b \vee c) = a = a \vee a = (a \wedge b) \vee (a \wedge c)$. Se $a \leq b$ e $c \leq a$, então $a \wedge (b \vee c) = a = a \vee c = (a \wedge b) \vee (a \wedge c)$. Se $b \leq a$ e $a \leq c$, então $a \wedge (b \vee c) = a = b \vee a = (a \wedge b) \vee (a \wedge c)$.

(iii) Considere o grupo de Klein $V = \{e, a, b, ab\}$. O reticulado $Sub(V) = \mathcal{N}(V) = \{\{e\}, \{e, a\}, \{e, b\}, \{e, ab\}, V\}$ não é distributivo. Com efeito, $\{e, a\} \wedge (\{e, b\} \vee \{e, ab\}) = \{e, a\} \cap (\{e, b\} \cdot \{e, ab\}) = \{e, a\} \cap V = \{e, a\}$ mas $(\{e, a\} \wedge \{e, b\}) \vee (\{e, a\} \wedge \{e, ab\}) = (\{e, a\} \cap \{e, b\}) \cdot (\{e, a\} \cap \{e, ab\}) = \{e\} \cdot \{e\} = \{e\}$.

Definição 3.4.5. Um reticulado R diz-se *modular* se para quaisquer $a, b, c \in R$, $b \leq a \Rightarrow a \wedge (b \vee c) = b \vee (a \wedge c)$.

Observação 3.4.6. Um reticulado R é modular se e só se para quaisquer $a, b, c \in R$, $b \leq a \Rightarrow a \wedge (b \vee c) = (a \wedge b) \vee (a \wedge c)$. Por conseguinte, qualquer reticulado distributivo é modular.

Lema 3.4.7. *Sejam R um reticulado e $a, b, c \in R$. Então $(a \wedge b) \vee (a \wedge c) \leq a \wedge (b \vee c)$.*

Demonstração: Tem-se $a \wedge b \leq a$ e $a \wedge b \leq b \leq b \vee c$. Logo $a \wedge b \leq a \wedge (b \vee c)$. Do mesmo modo, $a \wedge c \leq a \wedge (b \vee c)$. Portanto $(a \wedge b) \vee (a \wedge c) \leq a \wedge (b \vee c)$. □

Proposição 3.4.8. *Seja G um grupo. Então o reticulado $\mathcal{N}(G)$ dos subgrupos normais de G é modular.*

Demonstração: Sejam $A, B, C \in \mathcal{N}(G)$ tais que $B \subseteq A$. Por 3.4.7, basta mostrar que $A \cap (BC) \subseteq B(A \cap C)$. Seja $x \in A \cap (BC)$ e sejam $b \in B$ e $c \in C$ tais que $x = bc$. Então $c = b^{-1}x \in BA \subseteq AA = A$, pelo que $c \in A \cap C$. Logo $x = bc \in B(A \cap C)$. □

3.5 Álgebras de Boole

Notação 3.5.1. Seja R um reticulado em que $\inf R$ e $\sup R$ existem. Escreve-se $0 = \inf R$ e $1 = \sup R$.

Definição 3.5.2. Sejam R um reticulado com 0 e 1 e $a \in R$. Um elemento a' diz-se um *complemento* de a se $a \vee a' = 1$ e $a \wedge a' = 0$.

Proposição 3.5.3. *Sejam R um reticulado distributivo com 0 e 1 e $a \in R$. Se a admite um complemento, então este é único.*

Demonstração: Sejam a' e $\bar{a}$ complementos de a. Então $a' = a' \vee 0 = a' \vee (a \wedge \bar{a}) = (a' \vee a) \wedge (a' \vee \bar{a}) = 1 \wedge (a' \vee \bar{a}) = a' \vee \bar{a}$. Do mesmo modo, $\bar{a} = \bar{a} \vee a'$. Logo $a' = \bar{a}$. □

Definição 3.5.4. Uma *álgebra de Boole* é um reticulado distributivo com 0 e 1 em que todos os elementos têm um complemento. O complemento de um elemento a de uma álgebra de Boole é denotado por a'.

Exemplos 3.5.5. (i) Seja X um conjunto. Então o conjunto potência $\mathcal{P}(X)$ é uma álgebra de Boole. Tem-se $0 = \emptyset$, $1 = X$ e $A' = X \setminus A$ para todo o $A \in \mathcal{P}(X)$.

(ii) O reticulado totalmente ordenado $\{0, 1\}$ é uma álgebra de Boole. Tem-se $0' = 1$ e $1' = 0$.

Proposição 3.5.6. *Seja B uma álgebra de Boole.*

(i) $0' = 1$ *e* $1' = 0$.

(ii) Para quaisquer $a, b \in B$, $a' = b \Leftrightarrow b' = a$.

(iii) Para todo o $a \in B$, $a'' = a$.

(iv) (Leis de de Morgan) Para quaisquer $a, b \in B$, $(a \vee b)' = a' \wedge b'$ *e* $(a \wedge b)' = a' \vee b'$.

(v) Para quaisquer $a, b \in B$, $a \leq b \Leftrightarrow b' \leq a' \Leftrightarrow a \wedge b' = 0$.

Demonstração: (i) Como $0 \leq 1$, $0 \vee 1 = 1$ e $0 \wedge 1 = 0$. Logo $0' = 1$ e $1' = 0$.

(ii) Sejam $a, b \in B$ Tem-se $a' = b \Leftrightarrow (a \vee b = 1$ e $a \wedge b = 0) \Leftrightarrow b' = a$.

(iii) Seja $a \in B$. Como $a' = a'$, por (ii), $a'' = a$.

(iv) Sejam $a, b \in B$. Tem-se $(a \vee b) \vee (a' \wedge b') = a \vee (b \vee (a' \wedge b')) = a \vee ((b \vee a') \wedge (b \vee b')) = a \vee ((b \vee a') \wedge 1) = (a \vee (b \vee a')) \wedge (a \vee 1) = (a \vee a' \vee b) \wedge 1 = a \vee a' \vee b = 1 \vee b = 1$ e $(a \vee b) \wedge (a' \wedge b') = (a \wedge (a' \wedge b')) \vee (b \wedge (a' \wedge b')) = (a \wedge a' \wedge b') \vee (b \wedge b' \wedge a') = (0 \wedge b') \vee (0 \wedge a') = 0 \vee 0 = 0$. Logo $(a \vee b)' = a' \wedge b'$. Segue-se que $(a' \vee b')' = a \wedge b$ e portanto que $(a \wedge b)' = a' \vee b'$.

(v) Sejam $a, b \in B$. Tem-se $a \leq b \Leftrightarrow a \wedge b = a \Leftrightarrow (a \wedge b)' = a' \Leftrightarrow a' \vee b' = a' \Leftrightarrow b' \leq a'$. Suponhamos que $a \leq b$. Como $b' \leq a'$, $a \wedge b' \leq a'$. Como $a \wedge b' \leq a$, $a \wedge b' \leq a \wedge a' = 0$. Logo $a \wedge b' = 0$. Suponhamos inversamente que $a \wedge b' = 0$. Então $a = a \wedge 1 = a \wedge (b \vee b') = (a \wedge b) \vee (a \wedge b') = (a \wedge b) \vee 0 = a \wedge b$. Logo $a \leq b$. □

Definição 3.5.7. Um anel A diz-se *booleano* se todos os seus elementos são idempotentes, isto é, se para todo o $a \in A$, $a^2 = a$.

Proposição 3.5.8. *Seja A um anel booleano. Então:*

(i) $\mathrm{car}(A) \leq 2$*;*

(ii) para todo o $a \in A$, $-a = a$;

(iii) A é comutativo.

Demonstração: (i) Tem-se $2 \cdot 1 = 1 + 1 = (1 + 1)^2 = 4 \cdot 1$ e portanto $2 \cdot 1 = 0$. Logo $\mathrm{car}(A) \leq 2$.

(ii) Por (i), para qualquer $a \in A$, $2a = 0$, ou seja, $-a = a$.

(iii) Sejam $a, b \in A$. Tem-se $a + b = (a + b)^2 = a^2 + ab + ba + b^2 = a + ab + ba + b$ e então $0 = ab + ba$. Logo, por (ii), $ab = -ba = ba$. □

Estabelecemos a seguir uma correspondência bijectiva entre álgebras de Boole e anéis booleanos.

Definição 3.5.9. Seja B uma álgebra de Boole. Define-se a *diferênça simétrica* de dois elementos $a, b \in B$ por $a + b = (a \wedge b') \vee (a' \wedge b)$.

Teorema 3.5.10. *Seja B uma álgebra de Boole. Então $(B, +, \wedge)$ é um anel booleano.*

Demonstração: Sejam $a, b, c \in B$. Tem-se

$$\begin{aligned}
a + (b + c) &= (a \wedge (b + c)') \vee (a' \wedge (b + c)) \\
&= (a \wedge ((b \wedge c') \vee (b' \wedge c))') \vee (a' \wedge ((b \wedge c') \vee (b' \wedge c))) \\
&= (a \wedge ((b \wedge c')' \wedge (b' \wedge c)')) \vee (a' \wedge ((b \wedge c') \vee (b' \wedge c))) \\
&= (a \wedge ((b' \vee c) \wedge (b \vee c'))) \vee (a' \wedge ((b \wedge c') \vee (b' \wedge c))) \\
&= (a \wedge ((b' \wedge b) \vee (b' \wedge c') \vee (c \wedge b) \vee (c \wedge c'))) \vee (a' \wedge ((b \wedge c') \vee (b' \wedge c))) \\
&= (a \wedge (0 \vee (b' \wedge c') \vee (c \wedge b) \vee 0)) \vee (a' \wedge ((b \wedge c') \vee (b' \wedge c))) \\
&= (a \wedge ((b' \wedge c') \vee (c \wedge b))) \vee (a' \wedge ((b \wedge c') \vee (b' \wedge c))) \\
&= (a \wedge (b' \wedge c')) \vee (a \wedge (c \wedge b)) \vee (a' \wedge (b \wedge c')) \vee (a' \wedge (b' \wedge c)) \\
&= (a \wedge b' \wedge c') \vee (a \wedge c \wedge b) \vee (a' \wedge b \wedge c') \vee (a' \wedge b' \wedge c) \\
&= (a \wedge b \wedge c) \vee (a \wedge b' \wedge c') \vee (a' \wedge b \wedge c') \vee (a' \wedge b' \wedge c).
\end{aligned}$$

Como + é uma operação comutativa, segue-se que

$$\begin{aligned}(a+b)+c &= c+(a+b)\\ &= (c\wedge a\wedge b)\vee(c\wedge a'\wedge b')\vee(c'\wedge a\wedge b')\vee(c'\wedge a'\wedge b)\\ &= (a\wedge b\wedge c)\vee(a\wedge b'\wedge c')\vee(a'\wedge b\wedge c')\vee(a'\wedge b'\wedge c)\\ &= a+(b+c).\end{aligned}$$

Tem-se $0+a=(0\wedge a')\vee(0'\wedge a)=0\vee(1\wedge a)=1\wedge a=a$ e $a+a=(a\wedge a')\vee(a'\wedge a)=0\vee 0=0$. Logo $(B,+)$ é um grupo abeliano. O elemento neutro é 0 e cada elemento é o seu próprio simétrico. O par $(B,\wedge)$ é um monóide comutativo. O elemento neutro é 1. Tem-se

$$\begin{aligned}(a\wedge b)+(a\wedge c) &= ((a\wedge b)\wedge(a\wedge c)')\vee((a\wedge b)'\wedge(a\wedge c))\\ &= ((a\wedge b)\wedge(a'\vee c'))\vee((a'\vee b')\wedge(a\wedge c))\\ &= (((a\wedge b)\wedge a')\vee((a\wedge b)\wedge c'))\vee((a'\wedge(a\wedge c))\vee(b'\wedge(a\wedge c)))\\ &= (a\wedge b\wedge a')\vee(a\wedge b\wedge c')\vee(a'\wedge a\wedge c)\vee(b'\wedge a\wedge c)\\ &= 0\vee(a\wedge b\wedge c')\vee 0\vee(b'\wedge a\wedge c)\\ &= (a\wedge b\wedge c')\vee(a\wedge b'\wedge c)\\ &= (a\wedge(b\wedge c'))\vee(a\wedge(b'\wedge c))\\ &= a\wedge((b\wedge c')\vee(b'\wedge c))\\ &= a\wedge(b+c).\end{aligned}$$

Segue-se que $(B,+,\wedge)$ é um anel. Como $a^2=a\wedge a=a$ para todo o $a\in B$, este anel é booleano. □

Proposição 3.5.11. *Sejam B uma álgebra de Boole e $a,b\in B$. Então $a\vee b=a+b+ab$.*

Demonstração: Tem-se

$$\begin{aligned}
a+b+ab &= (((a'\wedge b)\vee(a\wedge b'))'\wedge(a\wedge b))\vee(((a'\wedge b)\vee(a\wedge b'))\wedge(a\wedge b)')\\
&= (((a'\wedge b)'\wedge(a\wedge b')')\wedge(a\wedge b))\vee(((a'\wedge b)\vee(a\wedge b'))\wedge(a'\vee b'))\\
&= (((a\vee b')\wedge(a'\vee b))\wedge(a\wedge b))\vee(((a'\wedge b)\vee(a\wedge b'))\wedge(a'\vee b'))\\
&= (((a\wedge a')\vee(a\wedge b)\vee(b'\wedge a')\vee(b'\wedge b))\wedge(a\wedge b))\vee\\
&\quad (((a'\wedge b)\vee(a\wedge b'))\wedge(a'\vee b'))\\
&= ((0\vee(a\wedge b)\vee(b'\wedge a')\vee 0)\wedge(a\wedge b))\vee(((a'\wedge b)\vee(a\wedge b'))\wedge(a'\vee b'))\\
&= (((a\wedge b)\vee(b'\wedge a'))\wedge(a\wedge b))\vee(((a'\wedge b)\vee(a\wedge b'))\wedge(a'\vee b'))\\
&= (((a\wedge b)\wedge(a\wedge b))\vee((b'\wedge a')\wedge(a\wedge b)))\vee\\
&\quad ((((a'\wedge b)\wedge a')\vee((a'\wedge b)\wedge b'))\vee(((a\wedge b')\wedge a')\vee((a\wedge b')\wedge b')))\\
&= ((a\wedge b)\vee 0)\vee(((a'\wedge b)\vee 0)\vee(0\vee(a\wedge b')))\\
&= (a\wedge b)\vee(a'\wedge b)\vee(a\wedge b')\\
&= (a\wedge(b\vee b'))\vee(a'\wedge b)\\
&= (a\wedge 1)\vee(a'\wedge b)\\
&= a\vee(a'\wedge b)\\
&= (a\vee a')\wedge(a\vee b)\\
&= 1\wedge(a\vee b)\\
&= a\vee b.
\end{aligned}$$

□

Teorema 3.5.12. *Seja B um anel booleano. Então B é uma álgebra de Boole relativamente às operações $\vee$ e $\wedge$ definidas por $a\vee b = a+b+ab$ e $a\wedge b = ab$. Para quaisquer dois elementos $a, b\in B$, $a+b = (a'\wedge b)\vee(a\wedge b')$.*

Demonstração: Como $(B,\cdot)$ é um monóide comutativo, a operação $\wedge$ é associativa e comutativa. Para todo o $a\in B$, $a\wedge a = a^2 = a$. Sejam $a, b, c\in B$. É óbvio que $a\vee b = b\vee a$. Tem-se $(a\vee b)\vee c = (a+b+ab)+c+(a+b+ab)c = a+b+c+ab+ac+bc+abc$ e portanto $a\vee(b\vee c) = (b\vee c)\vee a = b+c+a+bc+ba+ca+bca = a+b+c+ab+ac+bc+abc = (a\vee b)\vee c$. Como $-a = a$, $a\vee a = a+a+a^2 = a-a+a = a$. Tem-se $a\vee(a\wedge b) = a+ab+a^2b = a-ab+ab = a$ e $a\wedge(a\vee b) = a(a+b+ab) = a^2+ab+a^2b = a-ab+ab = a$. Logo $(B,\vee,\wedge)$ é um reticulado. Tem-se $0\wedge a = 0a = 0$ e portanto $0\leq a$. Logo $0 = \inf B$. Tem-se $1\wedge a = 1a = a$ e então $a\leq 1$. Logo $1 = \sup B$. Temos $a\wedge(b\vee c) = a(b+c+bc) = ab+ac+abc = ab+ac+a^2bc = ab+ac+abac = (a\wedge b)\vee(a\wedge c)$. Logo B é distributivo. Tem-se $a\vee(1+a) = a+(1+a)+a(1+a) = a+1+a+a+a^2 = 1$ e $a\wedge(1+a) = a(1+a) = a+a^2 = 0$. Logo $1+a$ é o complemento de a. Segue-se que $(B,\vee,\wedge)$ é uma álgebra de Boole. Temos $(a'\wedge b)\vee(a\wedge b') = (1+a)b+a(1+b)+(1+a)ba(1+b) = b+ab+a+ab+(1+a)(ba+b^2a) =$

$a + b + (1 + a)0 = a + b.$ □

Capítulo 4

Conceitos básicos em Álgebra Universal

4.1 Estruturas algébricas

Definição 4.1.1. Sejam A um conjunto e $n \in \mathbb{N}$. Uma *operação n-ária (interna)* em X é uma aplicação $A^n \to A$.

Observações 4.1.2. (i) Uma operação 2-ária é mesma coisa uma operação binária.

(ii) Para qualquer conjunto A, $A^0 = \{()\}$. Logo as operações 0-árias num conjunto A correspondem bijectivamente aos elementos de A.

Definição 4.1.3. Uma *estrutura algébrica* é um par $(A, (\mu_i)_{i\in I})$ em que A é um conjunto não vazio e $(\mu_i)_{i\in I}$ é uma familia de operações $\mu_i \colon A^{n_i} \to A$. A família $(n_i)_{i\in I}$ é o *tipo* da estrutura algébrica.

Nota 4.1.4. Muitas vezes usa-se o termo *álgebra* em vez de *estrutura algébrica*. Não usaremos esta terminologia porque o termo *álgebra* designa em primeiro lugar um espaço vectorial que é ao mesmo tempo um anel.

Exemplos 4.1.5. (i) Um grupóide é uma estrutura algébrica de tipo (2).

(ii) Um reticulado é uma estrutura algébrica de tipo $(2, 2)$.

(iii) Segundo a nossa definição, um monóide é uma estrutura algébrica de tipo (2) que satisfaz certas condições. Uma destas condições é a existência de um elemento neutro. Esta condição pode ser incorporada na estrutura de um monóide através de uma operação 0-ária e. Assim um monóide pode ser visto como uma estrutura algébrica $(M, (e, *))$ de tipo $(0, 2)$ que satisfaz as condições

- $x * (y * z) = (x * y) * z$;
- $e * x = x * e = x$.

De modo geral, é habitual descrever uma estrutura algébrica incorporando, na medida do possível, as condições de existência na estrutura como operações e especificando a estrutura algébrica depois através de condições universais.

(iv) Um grupo pode ser visto como uma estrutura algébrica $(G, (e, i, \cdot))$ de tipo $(0, 1, 2)$ que satisfaz as condições

- $x * (y * z) = (x * y) * z$;
- $e * x = x * e = x$;
- $i(x) * x = x * i(x) = e$.

(v) Um anel pode ser visto como uma estrutura algébrica $(A, (+, \cdot, 0, 1, -))$ de tipo $(2, 2, 0, 0, 1)$ que satisfaz as condições

- $x + (y + z) = x + (y + z)$;
- $0 + x = x + 0 = x$;
- $x + (-x) = -x + x = 0$;
- $x \cdot (y \cdot z) = (x \cdot y) \cdot z$;
- $1 \cdot x = x \cdot 1 = x$;
- $x \cdot (y + z) = (x \cdot y) + (x \cdot z)$;
- $(x + y) \cdot z = (x \cdot z) + (y \cdot z)$.

4.2 Subestruturas, produtos e homomorfismos

Definição 4.2.1. Seja $(A, (\mu_i)_{i\in I})$ uma estrutura algébrica de tipo $(n_i)_{i\in I}$. Um subconjunto não vazio $B \subseteq A$ diz-se uma subestrutura de $A, (\mu_i)_{i\in I}$ se para qualquer $i \in I$, $\mu_i(B^{n_i}) \subseteq B$.

Exemplo 4.2.2. Se consideramos um grupo como uma estrutura algébrica $(G, (e, i, \cdot))$ de tipo $(0, 1, 2)$ como no exemplo 4.1.5(iv), as subestruturas de um grupo são precisamente os seus subgrupos.

Observação 4.2.3. Sejam $(A, (\mu_i)_{i\in I})$ uma estrutura algébrica de tipo $(n_i)_{i\in I}$ e B uma subestrutura de $(A, (\mu_i)_{i\in I})$. Então $(B, (\mu_i|_{B^{n_i}} : B^{n_i} \to B)_{i\in I})$ é uma estrutura algébrica de tipo $(n_i)_{i\in I}$.

Proposição 4.2.4. *Sejam $(A,(\mu_i)_{i\in I})$ uma estrutura algébrica de tipo $(n_i)_{i\in I}$ e $(B_k)_{k\in K}$ uma família não vazia de subestruturasacr de $(A,(\mu_i)_{i\in I})$. Então a intersecção $\bigcap_{k\in K} B_k$ é ou vazia ou uma subestrutura de $(A,(\mu_i)_{i\in I})$.*

Demonstração: Suponhamos que $\bigcap_{k\in K} B_k \neq \emptyset$. Seja $i \in I$. Então para cada $l \in K$, $\mu_i((\bigcap_{k\in K} B_k)^{n_i}) \subseteq \mu_i(B_l^{n_i}) \subseteq B_l$. Logo $\mu_i((\bigcap_{k\in K} B_k)^{n_i}) \subseteq \bigcap_{k\in K} B_k$, pelo que $\bigcap_{k\in K} B_k$ é uma subestrutura de $(A,(\mu_i)_{i\in I})$. □

Os conceitos seguintes englobam as noções correspondentes para grupos, anéis e reticulados.

Definição 4.2.5. Sejam $(A,(\mu_i)_{i\in I})$ uma estrutura algébrica e $X \subseteq A$ um subconjunto não vazio. A *subestrutura gerada por* X, $\langle X\rangle$, é a intersecção das subestruturas de $(A,(\mu_i)_{i\in I})$ que contêm X.

Definição 4.2.6. Sejam $(A_1,(\mu_{1,i})_{i\in I}),\ldots,(A_m,(\mu_{m,i})_{i\in I})$ estruturas algébricas do mesmo tipo $(n_i)_{i\in I}$. O *produto* $\prod_{k=1}^{m}(A_k,(\mu_{k,i})_{i\in I})$ é a estrutura algébrica de tipo $(n_i)_{i\in I}$ cujo conjunto subjacente é o produto cartesiano $A_1\times\cdots\times A_m$ e cujas operações são definidas componente por componente, isto é, por $\mu_i() = (\mu_{1,i}(),\ldots,\mu_{m,i}())$ se $n_i = 0$ e por

$$\mu_i((a_{1,1},\ldots,a_{m,1}),\ldots,(a_{1,n_i},\ldots,a_{m,n_i})) = (\mu_{1,i}(a_{1,1},\ldots,a_{1,n_i}),\ldots,\mu_{m,i}(a_{m,1},\ldots,a_{m,n_i}))$$

se $n_i \neq 0$.

Definição 4.2.7. Sejam $(A,(\mu_i)_{i\in I})$ e $(A',(\mu'_i)_{i\in I})$ duas estruturas algébricas do mesmo tipo $(n_i)_{i\in I}$. Uma aplicação $f\colon A\to A'$ diz-se um *homomorfismo* de $(A,(\mu_i)_{i\in I})$ para $(A',(\mu'_i)_{i\in I})$ se para quaisquer $i\in I$ e $(a_1\ldots,a_{n_i})\in A^{n_i}$, $f(\mu_i(a_1\ldots,a_{n_i})) = \mu'_i(f(a_1),\ldots,f(a_{n_i}))$. Um homomorfismo diz-se um *monomorfismo* (*epimorfismo, isomorfismo*) se é injectivo (sobrejectivo, bijectivo). Um homomorfismo (isomorfismo) de uma estrutura algébrica $(A,(\mu_i)_{i\in I})$ para $(A,(\mu_i)_{i\in I})$ diz-se um *endomorfismo* (*automorfismo*) de estruturas algébricas. As estruturas algébricas $(A,(\mu_i)_{i\in I})$ e $(A',(\mu'_i)_{i\in I})$ dizem-se *isomorfos* se existe um isomorfismo de estruturas algébricas entre eles.

Exemplos 4.2.8. (i) Sejam $(A,(\mu_i)_{i\in I})$ uma estrutura algébrica e B uma subestrutura de $(A,(\mu_i)_{i\in I})$. Então a inclusão $B\to A$, $x\mapsto x$ é um monomorfismo de estruturas algébricas.

(ii) Considere o produto $\prod_{k=1}^{m}(A_k,(\mu_{k,i})_{i\in I})$ das estruturas algébricas $(A_1,(\mu_{1,i})_{i\in I}),\ldots,(A_m,(\mu_{m,i})_{i\in I})$ do mesmo tipo $(n_i)_{i\in I}$. Para cada $l\in\{1,\ldots,m\}$, a projecção $\prod_{k=1}^{m}A_k\to A_l$, $(a_1,\ldots,a_m)\mapsto a_l$ é um epimorfismo de estruturas algébricas.

Proposição 4.2.9. *Sejam $(A,(\mu_i)_{i\in I})$, $(B,(\mu_i)_{i\in I})$ e $(C,(\mu_i)_{i\in I})$ três estruturas algébricas do mesmo tipo $(n_i)_{i\in I}$ e $f\colon A\to B$ e $g\colon B\to C$ homomorfismos. Então $g\circ f\colon R\to T$ é um homomorfismo de $(A,(\mu_i)_{i\in I})$ para $(C,(\mu_i)_{i\in I})$.*

Demonstração: Sejam $i\in I$ e $(a_1\ldots,a_{n_i})\in A^{n_i}$. Tem-se

$$g(f(\mu_i(a_1\ldots,a_{n_i})))=g(\mu_i(f(a_1),\ldots,f(a_{n_i})))=\mu_i(g(f(a_1)),\ldots,g(f(a_{n_i}))).$$

Logo $g\circ f$ é um homomorfismo de $(A,(\mu_i)_{i\in I})$ para $(C,(\mu_i)_{i\in I})$. □

Proposição 4.2.10. *Sejam $(A,(\mu_i)_{i\in I})$ e $(B,(\mu_i)_{i\in I})$ duas estruturas algébricas do mesmo tipo $(n_i)_{i\in I}$ e f um isomorfismo de $(A,(\mu_i)_{i\in I})$ para $(B,(\mu_i)_{i\in I})$. Então f^{-1} é um isomorfismo de $(B,(\mu_i)_{i\in I})$ para $(A,(\mu_i)_{i\in I})$.*

Demonstração: Sejam $i\in I$ e $(b_1\ldots,b_{n_i})\in B^{n_i}$. Tem-se

$$\begin{aligned} f(f^{-1}(\mu_i(b_1\ldots,b_{n_i}))) &= \mu_i(b_1\ldots,b_{n_i})\\ &= \mu_i(f(f^{-1}(b_1)),\ldots,f(f^{-1}(b_{n_i})))\\ &= f(\mu_i(f^{-1}(b_1),\ldots,f^{-1}(b_{n_i}))).\end{aligned}$$

Como f é injectivo, $f^{-1}(\mu_i(b_1\ldots,b_{n_i})))=\mu_i(f^{-1}(b_1),\ldots,f^{-1}(b_{n_i}))$. Logo f^{-1} é um homomorfismo de $(B,(\mu_i)_{i\in I})$ para $(A,(\mu_i)_{i\in I})$. Como f^{-1} é bijectivo, f^{-1} é um isomorfismo. □

Proposição 4.2.11. *Sejam $(A,(\mu_i)_{i\in I})$ e $(A',(\mu_i)_{i\in I})$ duas estruturas algébricas do mesmo tipo $(n_i)_{i\in I}$, f um homomorfismo de $(A,(\mu_i)_{i\in I})$ para $(B,(\mu_i)_{i\in I})$, B uma subestrutura de $(A,(\mu_i)_{i\in I})$ e B' uma subestrutura de $(A',(\mu_i)_{i\in I})$. Então $f(B)$ é uma subestrutura de $(A',(\mu_i)_{i\in I})$ e $f^{-1}(B')$ é ou vazio ou uma subestrutura de $(A,(\mu_i)_{i\in I})$.*

Demonstração: Como $B\neq\emptyset$, $f(B)\neq\emptyset$. Sejam $i\in I$ e $b_1,\ldots,b_{n_i}\in B$. Então $\mu_i(b_1,\ldots,b_{n_i})\in B$ e portanto $\mu_i(f(b_1),\ldots,f(b_{n_i}))=f(\mu_i(b_1,\ldots,b_{n_i}))\in f(B)$. Segue-se que $f(B)$ é uma subestrutura de $(A',(\mu_i)_{i\in I})$.

Suponhamos que $f^{-1}(B')\neq\emptyset$. Sejam $i\in I$ e $a_1,\ldots,a_{n_i}\in f^{-1}(B')$. Então $\mu_i(f(a_1),\ldots,f(a_{n_i}))\in B'$ e portanto $f(\mu_i(a_1,\ldots,a_{n_i}))=\mu_i(f(a_1),\ldots,f(a_{n_i}))\in B'$. Logo $\mu_i(a_1,\ldots,a_{n_i})\in f^{-1}(B')$. Segue-se que $f^{-1}(B')$ é uma subestrutura de $(A,(\mu_i)_{i\in I})$. □

Notação 4.2.12. Sejam $(A,(\mu_i)_{i\in I})$ e $(A',(\mu_i)_{i\in I})$ duas estruturas algébricas do mesmo tipo $(n_i)_{i\in I}$ e f um homomorfismo de $(A,(\mu_i)_{i\in I})$ para $(B,(\mu_i)_{i\in I})$. Escreve-se $\mathrm{Im}(f)=f(A)$.

4.3 Relações de congruência e estruturas quociente

Definição 4.3.1. Seja $(A, (\mu_i)_{i\in I})$ uma estrutura algébrica de tipo $(n_i)_{i\in I}$. Uma relação de congruência em $(A, (\mu_i)_{i\in I})$ é uma relação de equivalência $\equiv$ em A tal que para quaisquer $i \in I$ e $a_1, \dots a_{n_i}, b_1, \dots b_{n_i} \in A$, se $a_k \equiv b_k$ para todo o $k \in \{1, \dots, n_i\}$, então $\mu_i(a_1, \dots, a_{n_i}) \equiv \mu_i(b_1, \dots, b_{n_i})$.

Exemplos 4.3.2. (i) Sejam $(A, (\mu_i)_{i\in I})$ e $(B, (\mu_i)_{i\in I})$ duas estruturas algébricas do mesmo tipo e f um homomorfismo de $(A, (\mu_i)_{i\in I})$ para $(B, (\mu_i)_{i\in I})$. Então uma relação de congruência em $(A, (\mu_i)_{i\in I})$ é dada por $x \equiv y \Leftrightarrow f(x) = f(y)$. Esta relação de congruência é chamada o *núcleo* de f. Note-se que se f é um homomorfismo de grupos e $\equiv$ é o núcleo de f, então $x \equiv y \Leftrightarrow xy^{-1} \in \mathrm{Ker}(f)$.

(ii) Sejam $G = (G, (e, i, \cdot))$ um grupo e $H \subseteq G$ um subgrupo normal. Então a relação $\sim_H$ dada por $x \sim_H y \Leftrightarrow x \cdot i(y) \in H$ é uma relação de congruência em G.

(iii) Sejam $A = (A, (+, \cdot, 0, 1, -))$ um anel e $I \subseteq A$ um ideal. Então a relação $\sim_I$ dada por $x \sim_I y \Leftrightarrow x - y \in I$ é uma relação de congruência em A.

Definição 4.3.3. Sejam $(A, (\mu_i)_{i\in I})$ uma estrutura algébrica de tipo $(n_i)_{i\in I}$ e $\equiv$ uma relação de congruência em $(A, (\mu_i)_{i\in I})$. A *estrutura quociente* $(A, (\mu_i)_{i\in I})/\equiv$ é a estrutura algébrica de tipo $(n_i)_{i\in I}$ cujo conjunto subjacente é o conjunto quociente $A/\equiv$ e cujas operações μ_i são dadas por $\mu_i([a_1], \dots, [a_{n_i}]) = [\mu_i(a_1, \dots, a_{n_i})]$. Chama-se *epimorfismo canónico* ao epimorfismo de $(A, (\mu_i)_{i\in I})$ para $(A, (\mu_i)_{i\in I})/\equiv$ dado por $a \mapsto [a]$.

Exemplos 4.3.4. Grupos quociente, anéis quociente e reticulados quociente são estruturas quociente.

Teorema 4.3.5. *Sejam $(A, (\mu_i)_{i\in I})$ e $(B, (\mu_i)_{i\in I})$ duas estruturas algébricas do mesmo tipo, f um homomorfismo de $(A, (\mu_i)_{i\in I})$ para $(B, (\mu_i)_{i\in I})$, $\equiv$ uma relação de congruência em $(A, (\mu_i)_{i\in I})$ tal que para quaisquer $x, y \in A$, $x \equiv y \Rightarrow f(x) = f(y)$ e $\pi\colon A \to A/\equiv$ o epimorfismo canónico. Então existe um único homomorfismo $\bar{f}$ de $(A, (\mu_i)_{i\in I})/\equiv$ para $(B, (\mu_i)_{i\in I})$ tal que $\bar{f} \circ \pi = f$. O homomorfismo $\bar{f}$ é um monomorfismo se e só se $\equiv$ é o núcleo de f.*

Demonstração: Sejam $x, y \in A$ tais que $x \equiv y$. Então $f(x) = f(y)$. Segue-se que a aplicação $\bar{f}\colon A/\equiv \to B$, $\bar{f}([x]) = f(x)$ está bem definida. Sejam $i \in I$ e $a_1, \dots, a_{n_i} \in A$. Tem-se

$$\begin{aligned}
\bar{f}(\mu_i([a_1], \dots, [a_{n_i}])) &= \bar{f}([\mu_i(a_1, \dots, a_{n_i})]) \\
&= f(\mu_i(a_1, \dots, a_{n_i})) \\
&= \mu_i(f(a_1), \dots, f(a_{n_i})) \\
&= \mu_i(\bar{f}([a_1]), \dots, \bar{f}([a_{n_i}])).
\end{aligned}$$

Logo $\bar{f}$ é um homomorfismo de $(A, (\mu_i)_{i\in I})/\equiv$ para $(B, (\mu_i)_{i\in I})$. Por definição, $\bar{f}\circ\pi = f$. Seja g um homomorfismo de $(A, (\mu_i)_{i\in I})/\equiv$ para $(B, (\mu_i)_{i\in I})$ tal que $g\circ\pi = f$. Então para qualquer $x \in A$, $g([x]) = g\circ\pi(x) = f(x) = \bar{f}\circ\pi(x) = \bar{f}([x])$, pelo que $g = \bar{f}$.

Suponhamos que $\equiv$ é o núcleo de f. Sejam $x, y \in A$ tais que $\bar{f}([x]) = \bar{f}([y])$. Então $f(x) = f(y)$ e $x \equiv y$. Segue-se que $[x] = [y]$ e então que $\bar{f}$ é um monomorfismo. Suponhamos inversamente que $\bar{f}$ é um monomorfismo. Sejam $x, y \in A$ tais que $f(x) = f(y)$. Então $\bar{f}([x]) = f(x) = f(y) = \bar{f}([y])$. Logo $[x] = [y]$ e portanto $x \equiv y$. Segue-se que $\equiv$ é o núcleo de f. □

Corolário 4.3.6. *(Teorema do homomorfismo) Sejam $(A, (\mu_i)_{i\in I})$ e $(B, (\mu_i)_{i\in I})$ duas estruturas algébricas do mesmo tipo, f um homomorfismo de $(A, (\mu_i)_{i\in I})$ para $(B, (\mu_i)_{i\in I})$ e $\equiv$ o núcleo de f. Então um isomorfismo de $(A, (\mu_i)_{i\in I})/\equiv$ para $(\mathrm{Im}(f), (\mu_i)_{i\in I})$ é dado por $[a] \mapsto f(a)$.*

Bibliografia

[1] António Antunes Monteiro, Isabel Teixeira de Matos, Álgebra - Um primeiro curso, Escolar Editora, 1995.

[2] B.A. Davey, H.A. Priestley, Introduction to Lattices and Order, Cambridge Mathematical Textbooks, Cambridge University Press, 1990.

[3] John R. Durbin, Modern Algebra - an introduction, John Wiley & Sons, 1995.

[4] George Grätzer, Universal Algebra, Second Edition. Springer Verlag, 1979.

[5] Nathan Jacobson, Basic Algebra I, 2nd edition, Dover Publications, 2009.

[6] Nathan Jacobson, Basic Algebra II, 2nd edition, Dover Publications, 2009.

[7] Serge Lang, Undergraduate Algebra, Third Edition, Undergraduate Texts in Mathematics, Springer Verlag, 2005.