Capítulo 1

Grupos

1.1 Grupóides, semigrupos e monóides

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

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

(ii) A 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 $X = \{x_1, \dots, x_n\}$ pode ser dada através de uma tabela da forma:

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Elementos invertíveis

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

e

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

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

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

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

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

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

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

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

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

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