1.2 Grupos

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Em consequência da Proposição 1.2.5 temos:

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

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

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

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

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

Podemos concluir que G é um grupo. $\square$

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

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

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

1.3 Homomorfismos de grupos

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

1.4 Subgrupos

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

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

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

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

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

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

(i) $e \in H$;

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

1.5 Teorema de Lagrange

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

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

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

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

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

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

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

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

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

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

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

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

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

1.6 Subgrupos normais e grupos quociente

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

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

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

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

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

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

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

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

Por 1.4.8, $\operatorname{Im}(f)$ e $f(H)$ são subgrupos de G'. Logo $f(H)$ é um subgrupo de $\operatorname{Im}(f)$. Sejam $x \in f(H)$ e $a \in \operatorname{Im}(f)$. 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 $\operatorname{Im}(f)$. ◻

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

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

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

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

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

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

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

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

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

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

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

munido da operação dada por

$$Hx \cdot Hy = Hxy.$$

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Demonstração: Consideremos os epimorfismos canónicos $\pi_N\colon G \to G/N$ e $\pi_H\colon G \to G/H$. Como $H \subseteq N = \mathrm{Ker}(\pi_N)$, existe, por 1.6.13, um único homomorfismo $\bar{\pi}_N\colon G/H \to G/N$ com $\bar{\pi}_N \circ \pi_H = \pi_N$. Seja $x \in G$. Então $Hx \in \mathrm{Ker}(\bar{\pi}_N) \Leftrightarrow \bar{\pi}_N(Hx) = N \Leftrightarrow \bar{\pi}_N \circ \pi_H(x) = N \Leftrightarrow \pi_N(x) = N \Leftrightarrow Nx = N \Leftrightarrow x \in N$. Assim, enquanto conjuntos, $\mathrm{Ker}(\bar{\pi}_N) = \{Hx \,|\, x \in N\} = N/H$. 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. $\square$

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