A Teoria dos Grupos teve origem nos trabalhos de Lagrange no século 18 ao considerar os grupos de permutações ou grupos simétricos que aparecem de forma natural nas relações entre coeficientes e raízes das equações polinomiais. O intuito de Lagrange era estudar a resolubilidade das equações algébricas de qualquer grau, em que não foi bem sucedido, mas abriu uma importante via.

Foi Cauchy quem, posteriormente, desenvolveu a teoria dos grupos simétricos, dando-lhe a feição que hoje ela tem.

A noção mais abstrata de grupo foi se impondo a partir dos trabalhos de Galois que associou a toda equação algébrica um grupo, relacionando a questão da resolubilidade das equações algébricas com certas propriedades que esses grupos deveriam ter.

Desde então, a Teoria de Grupos não parou de se desenvolver, tornando-se uma área da Matemática com inúmeras aplicações às outras áreas e notadamente à Física.

Aqui estudaremos apenas os aspectos mais elementares dessa teoria.

Grupos

Comecemos com um exemplo emblemático de grupo.

Seja C um conjunto não vazio. Definamos

$$S_C = \{\sigma : C \to C \ ; \ \sigma \ \text{ é uma bijeção}\} .$$

Um elemento de S_C é também chamado de *permutação* de C.

Em S_C temos a operação de composição de funções, que sabidamente tem as seguintes propriedades:

(i) É associativa.

(ii) Possui elemento neutro, que é a função identidade de C.

(iii) Cada bijeção possui um inverso para a composição, que é a bijeção inversa.

Vários conjuntos munidos de uma operação possuem as propriedades acima.

Por exemplo, os conjuntos dos inteiros $\mathbb{Z}$, dos racionais $\mathbb{Q}$, dos reais $\mathbb{R}$ e dos complexos $\mathbb{C}$, munidos com a adição, possuem essas propriedades. Por outro lado, se dos conjuntos $\mathbb{Q}$, $\mathbb{R}$ e $\mathbb{C}$ retirarmos o elemento zero, obtemos conjuntos que, com a operação de multiplicação, também satisfazem às propriedades acima mencionadas. Adiante, veremos mais exemplos.

Isto motiva a definição abstrata a seguir.

Um **grupo** $(G, *)$ consiste de um conjunto não vazio G munido de uma operação $*$, que possui as seguintes propriedades:

(i) Associatividade:
$$a * (b * c) = (a * b) * c, \quad \forall a, b, c \in G;$$

(ii) Existência de elemento neutro:
$$\exists e \in G, \text{ tal que } e * a = a * e = a, \quad \forall a \in G;$$

(iii) Existência de inverso:
$$\forall a \in G, \exists\ b \in G \text{ tal que } a * b = b * a = e.$$

Um grupo $(G, *)$ será dito **comutativo** ou **abeliano** quando

$$a * b = b * a, \quad \forall a, b \in G.$$

São grupos os seguintes conjuntos, com as correspondentes operações:

(a) $(S_C, \circ)$, sendo $\circ$ a composição de funções;

(b) $(A, +)$, sendo A um anel,

(c) $(A^*, \cdot)$ o conjunto dos elementos invertíveis de um anel com a operação de multiplicação do anel,

(d) $(S^1, \cdot)$, o conjunto dos números complexos de módulo 1,

(e) $(U_n, \cdot)$, o conjunto das raízes n-ésimas complexas da unidade, com a multiplicação.

Quando a operação $*$ de um grupo $(G, *)$ estiver subentendida, nos referiremos ao conjunto G como sendo o grupo.

Como foi feito para anéis, mostra-se que em um grupo G, são únicos o elemento neutro e o elemento inverso de um elemento dado.

Se a operação de G for representada multiplicativamente, o inverso de a, que é univocamente determinado por a, será denotado por a^{-1}, e por $-a$ na notação aditiva. Neste último caso, o elemento neutro é representado por 0.

A notação aditiva só será utilizada quando o grupo for abeliano.

É fácil verificar que
$(a^{-1})^{-1} = a \quad$ ou $\quad -(-a) = a$;
$(a \cdot b)^{-1} = b^{-1} \cdot a^{-1} \quad$ ou $\quad -(a+b) = -b + (-a)$.

Em um grupo G, temos a noção de **potenciação**, ou seja, se $a \in G$ e $n \in \mathbb{Z}$, define-se na notação multiplicativa

$$a^n = \begin{cases} a \cdot a \cdots a, & (n \text{ fatores}), \text{ se } n > 0 \\ e, & \text{se } n = 0 \\ a^{-1} \cdot a^{-1} \cdots a^{-1} & (|n| \text{ fatores}), \text{ se } n < 0 \end{cases}$$

Na notação aditiva, escrevemos

$$na = \begin{cases} a + a + \cdots + a, & (n \text{ parcelas}), \text{ se } n > 0 \\ 0, & \text{se } n = 0 \\ (-a) + (-a) + \cdots + (-a) & (|n| \text{ parcelas}), \text{ se } n < 0 \end{cases}$$

Para todos $a, b \in G$ e todos $m, n \in \mathbb{Z}$, as propriedades a seguir podem ser facilmente provadas por indução, respectivamente, na notação multiplicativa ou na notação aditiva:

(1)	$a^n \cdot a^m = a^{m+n}$	(1′)	$na + ma = (n+m)a$
(2)	$(a^n)^m = a^{nm}$	(2′)	$m(na) = (mn)a$
(3)	se $a \cdot b = b \cdot a$ então $(a \cdot b)^n = a^n \cdot b^n$	(3′)	$n(a+b) = na + nb$
(4)	$(a^n)^{-1} = a^{-n}$	(4′)	$-(na) = (-n)a$.

Grupos de permutações

Quando

$$C = I_n = \{1, 2, \ldots, n\},$$

o conjunto S_C, definido anteriormente, será denotado simplesmente por S_n e será chamado de *grupo simétrico*, ou *grupo de permutações* de n elementos. Pode-se provar por indução que S_n tem $n!$ elementos.

Como toda função é determinada quando se conhece a imagem de cada elemento do domínio, podemos representar um elemento $\sigma \in S_n$ do seguinte modo:

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

sendo $\sigma(1),\ \sigma(2),\ \ldots,\ \sigma(n)$ os elementos $(1, 2, \ldots, n)$ numa determinada ordem, isto é, uma permutação desses elementos.

Representaremos também a composição $\sigma \circ \tau$ por $\sigma \cdot \tau$ ou simplesmente por $\sigma\tau$.

Por exemplo,
$\tau = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 2 & 1 & 4 \end{pmatrix}$ é a bijeção $1 \mapsto 3$, $2 \mapsto 2$, $3 \mapsto 1$, $4 \mapsto 4$.

O elemento neutro de S_n é, portanto,

$$e = \begin{pmatrix} 1 & 2 & \cdots & n \\ 1 & 2 & \cdots & n \end{pmatrix}$$

e a composição, nessa notação, se efetua do seguinte modo:

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

Além disso,

$$\sigma^{-1} = \begin{pmatrix} 1 & 2 & \cdots & n \\ \sigma(1) & \sigma(2) & \cdots & \sigma(n) \end{pmatrix}^{-1} = \begin{pmatrix} \sigma(1) & \sigma(2) & \cdots & \sigma(n) \\ 1 & 2 & \cdots & n \end{pmatrix},$$

em que a última expressão deve ser rearrumada de modo que a primeira linha se transforme em $1, 2, \ldots, n$.

Se $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 2 & 4 & 1 \end{pmatrix}$ e $\tau = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 4 & 3 & 1 \end{pmatrix}$.

então,

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

Tem-se

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 4 & 2 & 5 & 1 \end{pmatrix}^{-1} = \begin{pmatrix} 3 & 4 & 2 & 5 & 1 \\ 1 & 2 & 3 & 4 & 5 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 5 & 3 & 1 & 2 & 4 \end{pmatrix}.$$

Determinamos a seguir a tabela da multiplicação em S_3. Para isto, descreveremos os elementos de S_3 de um modo especial.

Pondo

$$\sigma = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} \text{ e } \tau = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix},$$

temos

$$\sigma^2 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}, \sigma^3 = \tau^2 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix} = \text{e}.$$

Temos também

$$\sigma\tau = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} \text{ e } \sigma^2\tau = \tau\sigma = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}.$$

Portanto,

$$S_3 = \{\ e,\ \sigma,\ \sigma^2,\ \tau,\ \sigma\tau,\ \sigma^2\tau\ \}$$

e a tabela da multiplicação de S_3 é dada abaixo.

$\cdot$	e	σ	σ^2	τ	$\sigma\tau$	$\sigma^2\tau$
e	e	σ	σ^2	τ	$\sigma\tau$	$\sigma^2\tau$
σ	σ	σ^2	e	$\sigma\tau$	$\sigma^2\tau$	τ
σ^2	σ^2	e	σ	$\sigma^2\tau$	τ	$\sigma\tau$
τ	τ	$\sigma^2\tau$	$\sigma\tau$	e	σ^2	σ
$\sigma\tau$	$\sigma\tau$	τ	$\sigma^2\tau$	σ	e	σ^2
$\sigma^2\tau$	$\sigma^2\tau$	$\sigma\tau$	τ	σ^2	σ	e

estando $x \cdot y$ na linha do x e na coluna do y.

Para verificar a tabela acima é necessário lançar mão várias vezes das relações:

$$\sigma^3 = \tau^2 = e, \tau\sigma = \sigma^2\tau.$$

Por exemplo,

$$(\sigma\tau)(\sigma\tau) = \sigma(\tau\sigma)\tau = \sigma(\sigma^2\tau)\tau = \sigma^3\tau^2 = e.$$

Note que em S_3 temos que $\sigma\tau \neq \tau\sigma$, isto é, σ e τ não comutam, logo S_3 não é abeliano

Com relação ao grupo S_n, em geral, temos o seguinte resultado:

Para todo $n \geq 3$, S_n não é abeliano.

De fato, sejam τ' e τ definidas por $\tau'(1) = 2, \tau'(2) = 1$ e $\tau'(x) = x$ se $x \geq 3$; e $\tau(2) = 3, \tau(3) = 2$ e $\tau(x) = x$ se $x \neq 2, 3$. Temos, então, que $(\tau'\tau)(1) = 2$ e $(\tau\tau')(1) = 3$, logo $\tau'\tau \neq \tau\tau'$.

Subgrupos

Desenvolveremos a teoria de grupos na notação multiplicativa, valendo o que for provado também para a notação aditiva com as devidas adaptações.

Um subconjunto H de um grupo G é chamado **subgrupo** de G se $H \neq \emptyset$ e se, com a operação de G, for um grupo.

Para verificar que um subconjunto não-vazio H de G é um subgrupo de G, basta verificar que

(i) A operação de G é fechada em H, isto é, $ab \in H, \forall a, b \in H$.

(ii) O elemento neutro e de G pertence a H.

(iii) O inverso em G de todo elemento de H pertence a H.

Não é necessário verificar a associatividade da operação em H já que a operação é associativa em G. Também não é preciso verificar (ii), pois é consequência de (i) e (iii).

Por exemplo, um grupo G e o seu subconjunto $\{e\}$ são subgrupos de G. Esses são chamados de subgrupos triviais de G.

O grupo $(\mathbb{Z}, +)$ é um subgrupo de $(\mathbb{Q}, +)$ que é subgrupo de $(\mathbb{R}, +)$ que, por sua vez, é subgrupo de $(\mathbb{C}, +)$. Também $(U_n, \cdot)$ é subgrupo de $(S^1, \cdot)$, que é subgrupo de $(\mathbb{C}^*, \cdot)$.

Os subgrupos de $(\mathbb{Z}, +)$:

$\emptyset \neq H \subset \mathbb{Z}$ é um subgrupo de $\mathbb{Z}$ se, e somente se,

$$H = n\mathbb{Z} = \{m \in \mathbb{Z}; m = nx, \quad x \in \mathbb{Z}\} \quad \text{para algum} \quad n \in \mathbb{N} \cup \{0\}.$$

Para ver isto, basta provar que todo subgrupo de $\mathbb{Z}$ é um ideal de $\mathbb{Z}$, pois sendo esse anel principal, tem-se que $H = I(n) = n\mathbb{Z}$ para algum $n \in \mathbb{N} \cup \{0\}$.

De fato, sendo H um subgrupo de $\mathbb{Z}$, temos que é fechado para a adição. Por outro lado, se $b \in H$ e $c \in \mathbb{Z}$, temos que $bc = 0 \in H$, se $c = 0$, $bc = \pm b \in H$, se $c = \pm 1$. Finalmente, se $|c| > 1$,

$$bc = \pm b|c| = \pm b(1 + 1 + \cdots + 1) = \pm(b + b + \cdots + b) \in H,$$

onde o número de parcelas em $1 + 1 + \cdots + 1$ é $|c|$.

Note que sabemos que todo ideal $H \neq \{0\}$ de $\mathbb{Z}$ é gerado pelo menor inteiro positivo que pertence a H.

A seguir um critério útil para verificar se $H \subseteq G$ é um subgrupo.

Um subconjunto não vazio H de um grupo G é um subgrupo de G se, e somente se, para todos $a, b \in H$, tem-se que $ab^{-1} \in H$.

De fato, a implicação direta é óbvia, pois sendo $a, b \in H$ e H um subgrupo de G, temos que $b^{-1} \in H$ e, portanto, $ab^{-1} \in H$.

Reciprocamente, sendo $H \neq \emptyset$, tome $c \in H$, logo, por hipótese, $e = cc^{-1} \in H$. Seja $a \in H$, como $e \in H$, temos que $a^{-1} = ea^{-1} \in H$. Resta apenas provar o fechamento da operação de G em H. Sejam $a, b \in H$, logo, pelo que provamos acima, $b^{-1} \in H$ e, portanto, pela hipótese, $ab = a(b^{-1})^{-1} \in H$.

Eis uma maneira simples de se obter muitos subgrupos de um grupo G: Se $a \in G$, definimos, na notação multiplicativa,

$$\langle a \rangle = \{a^n; \quad n \in \mathbb{Z}\},$$

ou na notação aditiva

$$\langle a \rangle = \{na; \quad n \in \mathbb{Z}\}.$$

O subgrupo $\langle a \rangle$ será chamado de **subgrupo gerado** por a.

O próximo resultado nos mostrará que é ainda mais fácil verificar se um subconjunto finito de um grupo é ou não um subgrupo.

Sejam G um grupo e H um subconjunto finito e não vazio de G. Se H é fechado em relação à operação de G, então H é um subgrupo de G.

Basta mostrar que o elemento neutro e de G está em H e que o inverso de um elemento de H está em H. Seja $a \in H$, então $a^2, a^3, \ldots \in H$, pois H é fechado em relação à operação de G. Como H é finito, existem dois números naturais $m < n$ tais que $a^n = a^m$. Multiplicando por a^{-m} ambos os membros da igualdade acima, obtemos que $e = a^{n-m} \in H$.

Observe que se $n - m = 1$, temos que $a = e$ e o seu inverso é ele próprio, logo está em H. Se $n - m > 1$, então $a^{-1} = a^{n-m-1} \in H$ e o resultado está provado.

A **ordem** $|G|$ de um grupo G é a cardinalidade de G. Queremos comparar a ordem de um subgrupo H com a ordem de G. Se G tem um número finito de elementos, uma relação trivial, que decorre da inclusão $H \subseteq G$, é $|H| \leq |G|$.

Entretanto, por ser H um subgrupo de G, Lagrange provou que existe uma relação bem mais forte do que aquela acima. Para isto, é necessário introduzir um novo conceito.

Sejam $a \in G$ e H um subgrupo de G. Definem-se

$$aH = \{ah \,;\; h \in H\} \quad \text{e} \quad Ha = \{ha \,;\; h \in H\}.$$

O conjunto aH é chamado **classe lateral à esquerda** de a relativamente a H, enquanto que Ha é chamado **classe lateral à direita**. Em particular, $eH = He = H$.

Na notação aditiva, escreve-se $a + H$ em vez de aH. Por exemplo, se $G = \mathbb{Z}$ e $H = n\mathbb{Z}$, a classe lateral de $a \in \mathbb{Z}$ segundo H é dada por

$$a + n\mathbb{Z} = \{a + nx; \;\; x \in \mathbb{Z}\}.$$

Proposição Sejam G um grupo, H um subgrupo de G e a, b em G. Então

(i) $aH = bH$ se, e somente se, $b^{-1}a \in H$.

(ii) Se $aH \cap bH \neq \emptyset$, então $aH = bH$

(iii) $\bigcup_{x \in G} xH = G$.

(iv) Existe uma bijeção entre aH e H.

prova (i) Suponha que $aH = bH$. Como $a = ae \in aH$, segue-se que $a \in bH$, logo $a = bh$ para algum $h \in H$ e, portanto, $b^{-1}a = h \in H$.

Reciprocamente, suponha que $b^{-1}a \in H$. Seja $c \in aH$, logo $c = ah$ com $h \in H$, segue-se que $c = bb^{-1}ah$ com $h \in H$, logo $c = bh'$ com $h' = b^{-1}ah \in H$, daí vem que $c \in bH$, provando assim que $aH \subseteq bH$.

A inclusão $bH \subseteq aH$ se prova de modo semelhante.

(ii) Se $aH \cap bH \neq \emptyset$, então existe $c \in aH \cap bH$. Assim, podemos escrever $c = ah = bh'$, com $h, h' \in H$. Portanto, $b^{-1}a = h'h^{-1} \in H$. Pelo item (i) segue-se que $aH = bH$.

(iii) É claro que $\bigcup_{x\in G} xH \subseteq G$. Por outro lado, se $a \in G$, temos que $a \in aH \subseteq \bigcup_{x\in G} xH$ e, portanto, $G \subseteq \bigcup_{x\in G} xH$, provando assim a igualdade.

(iv) Considere a função

$$\begin{array}{rcl} f : H & \longrightarrow & aH \\ h & \longmapsto & ah \end{array}$$

que é sobrejetiva, pois, dado $y \in aH$, então y tem a forma $y = ah$ com $h \in H$ e, portanto, $f(h) = y$. Ela é injetora, pois se $f(h_1) = f(h_2)$, então, $ah_1 = ah_2$ e, portanto, por cancelamento de a, temos que $h_1 = h_2$.

Na proposição acima, pode-se trabalhar com as classes laterais à direita em vez das classes laterais à esquerda, obtendo resultados análogos. Nesse caso, a condição (i) lê-se

$$Ha = Hb \Longleftrightarrow ab^{-1} \in H.$$

O número de classes laterais à direita coincide com o número de classes laterais à esquerda, pois é uma bijeção a função $\varphi\colon \{aH;\ a \in G\} \to \{Hb;\ b \in G\}$, $\varphi(aH) = Ha^{-1}$. Esse número é chamado de *índice* de H em G, sendo denotado por $(G : H)$.

Teorema de Lagrange Sejam G um grupo finito e H um subgrupo de G. Então

$$|G| = (G : H) \cdot |H|.$$

Em particular a ordem de H divide a ordem de G.

Prova Da Proposição, segue-se que as classes laterais à esquerda de H em G formam uma partição de G por conjuntos que têm todos o mesmo número de elementos. Como $(G : H)$ é o número de classes laterais de H em G, então $|G| =$(G:H)$|H|$. Em particular, $|H|$ divide $|G|$.

Note que se G é infinito, então H é infinito, ou $(G : H)$ é infinito, logo a primeira afirmação no Teorema de Lagrange vale mesmo que G seja infinito.

Vamos determinar todos os subgrupos de
$S_3 = \{ e,\ \sigma,\ \sigma^2,\ \tau,\ \sigma\tau,\ \sigma^2\tau \}$.

Sendo S_3 finito, os subconjuntos de S_3 fechados em relação à operação são os subgrupos de S_3. Pelo Teorema de Lagrange, para que $H \subseteq S_3$ seja um subgrupo de S_3, é necessário que $|H|$ divida 6. Portanto, temos quatro casos a considerar.

Caso 1: $|H| = 1$. Neste caso, temos uma única possibilidade: $H = \{e\}$.

Caso 2: $|H| = 2$. As possibilidades são os conjuntos da forma $\{e, \sigma\}$, $\{e, \sigma^2\}$, $\{e, \tau\}$, $\{e, \sigma\tau\}$ e $\{e, \sigma^2\tau\}$. Entre eles somente os conjuntos $\{e, \tau\}$, $\{e, \sigma\tau\}$ e $\{e, \sigma^2\tau\}$ são fechados em relação à operação de S_3.

Caso 3: $|H| = 3$. Há somente as seguintes possibilidades: $H_1 = \{e, \tau, a\}$, $H_2 = \{e, \sigma\tau, b\}$, $H_3 = \{e, \sigma^2\tau, c\}$ ou $H_4 = \{e, \sigma, \sigma^2\}$. As três primeiras possibilidades devem ser excluídas, pois, caso contrário, $\{e, \tau\}$ seria um subgrupo de H_1, $\{e, \sigma\tau\}$ seria subgrupo de H_2 e $\{e, \sigma^2\tau\}$ seria subgrupo de H_3, o que, pelo Teorema de Lagrange, implicaria que 2 divide 3, absurdo.

Resta a possibilidade $H_4 = \{e, \sigma, \sigma^2\}$, que é um subconjunto fechado em relação à operação de S_3.

Caso 4: $|H| = 6$. Neste caso $H = S_3$.

Assim, os subgrupos de S_3 são:

$$\{e\},\ \{e, \tau\}, \{e, \sigma\tau\}, \{e, \sigma^2\tau\}, \{e, \sigma, \sigma^2\} \ \text{ e } \ S_3.$$

Dado um número que divide a ordem de um grupo, nem sempre existe um subgrupo com esse número de elementos, como teremos a oportunidade de constatar mais adiante. A determinação dos subgrupos de um grupo é bastante complexa e está longe de ter sido resolvida em geral. Existem alguns teoremas que garantem a existência de certos subgrupos de um grupo finito.