Notas sobre Teoria dos Grupos para Programa de Iniciação Científica e Mestrado - PICME

Rodrigo Yuske Yamauchi

29 de abril de 2025

Sumário

Capítulo 1

Introdução a grupos

Definição 1.0.1. Seja um conjunto A e uma operação binária $A \cdot A \to A$, diz-se que $(A, \cdot)$ é um grupo quando são satisfeitas as condições necessárias a seguir:

I) $\forall \; a, b, c \in A, \quad a \cdot (b \cdot c) = (a \cdot b) \cdot c \quad$ (associatividade);

II) $\exists \; e \in A$ tal que $a \cdot e = a \quad$ (elemento neutro);

III) $\forall \; a \in A$, $\exists \; b \in A$, tal que $a \cdot b = e \quad$ (elemento inverso).

A partir deste momento, uma operação $a \cdot b$, tais que $a, b \in A$ e $(A, \cdot)$ é um grupo, também será denotada simplesmente por ab e o grupo poderá ser denotado pelo seu conjunto, e.g., A é um grupo.

(Generalização da Associatividade) Seja A um grupo, mostraremos que para $a_0 \dots a_n \in A$,

$$(a_0 \dots a_s)(a_{s+1} \dots a_n) = (a_0 \dots a_r)(a_{r+1} \dots a_n),$$

tal que $r, s \in \mathbb{N}$ e $0 < r < s < n$.

Para $n = 2$, é evidente que o que queremos mostrar é verdadeiro, uma vez que

$$(a_0 a_1) a_2 = a_0 (a_1 a_2)$$

é a própria condição de A ser um grupo.

Para $n > 2$ e por indução em n, suponhamos que $\forall n'$, tal que $n' < n$, seja verdade que

$$(a_0 \dots a_{s'})(a_{s'+1} \dots a_{n'}) = (a_0 \dots a_{r'})(a_{r'+1} \dots a_{n'}),$$

onde $0 < r' < s' < n'$.

Como $r < s < n$, temos pela hipótese da indução que, sendo $r' = r$, $s' = s - 1$ e $n' = s$,

$$\begin{aligned}(a_0 \dots a_s)(a_{s+1} \dots a_n) &= ((a_0 \dots a_{s-1})(a_s))\,(a_{s+1} \dots a_n) \\ &= ((a_0 \dots a_r)(a_{r+1} \dots a_s))\,(a_{s+1} \dots a_n) \\ &= (a_0 \dots a_r)\,((a_{r+1} \dots a_s)(a_{s+1} \dots a_n)) \\ &= (a_0 \dots a_r)(a_{r+1} \dots a_n),\end{aligned}$$

como queríamos provar. □

Enunciaremos o seguinte lema que nos será útil posteriormente:

Lema 1.0.2. Sejam $a, b, c \in A$, se

$$b \cdot a = c \cdot a \quad \Rightarrow \quad b = c.$$

Demonstração. Seja a' o elemento inverso de a,

$$\begin{gathered} b \cdot a \cdot a' = c \cdot a \cdot a' \\ b \cdot e = c \cdot e \\ \therefore b = c. \end{gathered}$$

□

Proposição 1.0.3. Sendo $(A, \cdot)$ um grupo, mostraremos agora a comutatividade e unicidade de $e \in A$, tal que $a \cdot e = a$, e de $a' \in A$, tal que $a \cdot a' = e$.

Para a comutatividade do elemento inverso, temos que

$$\begin{aligned} aa' &= e \\ &= a'(a')' \\ &= (a'e)(a')' \\ &= a'(e(a')') \\ &= a'((aa')(a')') \\ &= a'(a(a'(a')')) \\ &= a'(ae) = a'a, \end{aligned}$$

como queríamos mostrar. □
Quanto a comutatividade do elemento neutro,

$$ae = a(a'a) = (aa')a = ea,$$

como queríamos. □
Provaremos a unicidade do elemento neutro por contradição, seja $e' \neq e$ um elemento neutro do grupo, tem-se então que

$$\begin{aligned} e'a &= a \\ &= ea, \end{aligned}$$

então, pelo Lema 1.0.2, $e' = e$ e entramos em contradição, como queríamos mostrar.
□
A fim de provar a unicidade do elemento inverso, consideremos $b, b' \in A$, tais que ambos sejam elementos inversos de a. Assim,

$$\begin{aligned} &b \cdot a = e = b' \cdot a \\ &\therefore b = b', \end{aligned}$$

pelo lema acima novamente, como queríamos mostrar. □

A partir de agora, denotaremos por a^{-1} o único elemento inverso de $a \in A$.

Note que agora é possível **redefinir** o conceito de grupo já com a unicidade e comutatividade dos elementos neutro e inverso e com a generalidade da associatividade, visto que estes todos são consequências diretas da definição mais abstrata.

Alguns **exemplos** notáveis de grupos são descritos a seguir.

Exemplo 1) O conjunto dos inteiros com a operação usual de soma é um grupo infinito, i.e., com um número infinito de elementos. Tal conjunto é denotado por $(\mathbb{Z}, +)$.

Exemplo 2) O conjunto das classes de equivalência módulo n, i.e., $\{\overline{0}, \ldots, \overline{n-1}\}$ e a soma dessas classes denotada por $\bigoplus_n$ formam um grupo $(\mathbb{Z}/n\mathbb{Z}, \bigoplus_n)$ finito de n elementos. Esse exemplo de grupo será melhor definido e mais explorado posteriormente

Exemplo 3) O conjunto das permutações[1] de n elementos com a operação de composição de funções $\circ$ é um grupo e é denotado por S_n.

Assim, se $n = 3$,

$$S_3 = \left\{ \begin{pmatrix} 123 \\ 123 \end{pmatrix}, \begin{pmatrix} 123 \\ 213 \end{pmatrix}, \begin{pmatrix} 123 \\ 321 \end{pmatrix}, \begin{pmatrix} 123 \\ 132 \end{pmatrix}, \begin{pmatrix} 123 \\ 231 \end{pmatrix}, \begin{pmatrix} 123 \\ 312 \end{pmatrix} \right\},$$

onde a notação $\binom{123}{abc}$ representa a função tal que $f(1) = a$, $f(2) = b$ e $f(3) = c$.

Por fim, definimos ainda o que é um grupo abeliano, um exemplo importante de grupo a ser estudado mais a frente.

Definição 1.0.4. Um grupo A *abeliano* ou *comutativo* é um grupo em que a seguinte propriedade é satisfeita:

$$ab = ba, \ \forall a, b \in A.$$

[1]Relação de bijeção entre um dado conjunto A e $\{0, \ldots, |A-1|\}$.

Capítulo 2

Subgrupos

Definição 2.0.1. Seja A um grupo e $H \subseteq A$ não vazio, então se H com a mesma operação de A, tal que $H \cdot H \to H$, também é um grupo, o chamaremos de subgrupo de A e denotaremos por $H \leq A$. Ou seja, para que H seja um subgrupo de A as seguintes condições devem ser satisfeitas:

I) $\forall \;\; a, b, c \in H, \quad a \cdot (b \cdot c) = (a \cdot b) \cdot c$ (associatividade);

II) $\exists\; e \in H$ tal que $a \cdot e = a$ (elemento neutro);

III) $\forall \;\; a \in H$, $\exists\; b \in A$, tal que $a \cdot b = e$ (elemento inverso);

IV) $\forall a, b \in H$, $a \cdot b \in H$ (operação binária fechada).

Proposição 2.0.2. Seja $H \subseteq A$ não vazio. Então, $H \leq A$ se, e somente se, as seguintes condições são satisfeitas:

1. $\forall a, b \in H$, $a \cdot b \in H$;
2. $\forall a \in H$, $a^{-1} \in H$.

Demonstração. Sendo $H \leq A$, então a primeira condição é imediatamente satisfeita. E, como $a \in A$ tem um único elemento inverso $a^{-1} \in A$, se $a \in H$, então $a^{-1} \in H$ pela condição da existência de elemento inverso para que H seja subgrupo. Reciprocamente, se H satisfaz a primeira condição da proposição, claramente é satisfeita a condição de operação binária fechada de subgrupo. Ademais, como vale a associatividade para elementos de A e $H \subseteq A$, então consequentemente vale a associatividade para elementos de H. Ora, e se existe elemento inverso para todo elemento de $h \in H$, $hh^{-1} = e$, tal que $e \in A$, e pela condição de operação binária fechada, $e \in H$. Assim, é garantido a existência de elemento neutro e inverso $\forall h$. □

Alguns exemplos de subgrupos são descritos a seguir:

Exemplo 1) O subconjunto $\{e\}$ forma um subgrupo para todo grupo, onde e é o elemento neutro do grupo.

Exemplo 2) O subconjunto $H \subseteq A$, tal que $A \subseteq H$, i.e., o próprio conjunto A é subgrupo de A.

Definição 2.0.3. Seja $S \subseteq A$ um subconjunto não vazio, onde A é um grupo. Definimos

$$\langle S \rangle = \{s_0 s_1 s_2 \dots s_n \mid n \in \mathbb{N}, s_i \in S \text{ ou } s_i^{-1} \in S\}.$$

Ademais, se $a \in A$, notaremos $\langle \{a\} \rangle$ diretamente como $\langle a \rangle$.

Proposição 2.0.4. Sejam $S \subseteq A$ um subconjunto não vazio e A um grupo, então $\langle S \rangle$ é um subgrupo de A.

Demonstração. Basta provar a proposição 2.0.2. Seja $x, y \in \langle S \rangle$,

$$x = a_0 a_1 \dots a_n, \text{ com } a_i \in S \text{ ou } a_i^{-1} \in S.$$

$$y = b_0 b_1 \dots b_m, \text{ com } b_i \in S \text{ ou } b_i^{-1} \in S.$$

Ora, $xy = a_0 a_1 \dots a_n b_0 b_1 \dots b_m$, tal que todos os fatores são elementos de S ou são o inverso de um elemento de S. Ademais, $x^{-1} = a_0^{-1} a_1^{-1} \dots a_n^{-1}$, tal que todos os fatores são elementos de S ou inverso de um elemento de S. Assim, $xy, x^{-1} \in \langle S \rangle$, como queríamos. □

Dessa forma, a partir de agora chamaremos $\langle S \rangle$ por **subgrupo gerado pelo subconjunto** S, onde S é o **conjunto gerador**.

Definição 2.0.5. Um grupo é dito **cíclico** quando ele pode ser gerado por um elemento, i.e., $\exists a \in A$ tal que $A = \langle a \rangle$. Note que $\langle a \rangle = \{a^n \mid n \in \mathbb{Z}\}$.

Definição 2.0.6. Chamaremos de **ordem** de um grupo A, o número de elementos de A, e será denotada por $|A|$. Além disso, se um grupo é gerado por um elemento a, a ordem de a será a ordem do subgrupo gerado por a, i.e., $|a| = |\langle a \rangle|$.

Teorema 2.0.7. Sejam A um grupo e $a \in A$, tal que a ordem de a, $|a| = m$, é finita. Então m é o menor inteiro positivo tal que $a^m = e$, onde e é o elemento neutro de A.

Demonstração. Primeiro mostraremos que, sendo $|a|$ finita, existe um inteiro positivo k tal que $a^k = e$. Temos a seguinte generalização para $\langle a \rangle$:

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

tal que $|a| = m$. Assim, devem existir, sem perda de generalidade, $p, q \in \mathbb{Z}$, tal que $p > q$ e $a^p = a^q$. Ora,

$$\begin{aligned} a^p \cdot a^{-q} &= a^q \cdot a^{-q} \\ a^{p-q} &= e, \end{aligned}$$

portanto, como $p - q > 0$, $\exists k > 0$, tal que $a^k = e$.

Agora, considere a sequência de potências de a:

$$e, a^1, a^2, \ldots, a^{k'-1},$$

onde k' é o menor inteiro k, tal que $a^k = e$. Mostraremos que todos os elementos dessa sequência são distintos. Para $k' = 1$, há apenas um elemento, e é imediata a validade da afirmação. Para $k' > 1$, suponhamos, sem perda de generalidade, $p, q \in \mathbb{Z}_{\geq 0}$, tal que $q < p < k'$. Ora,

$$\begin{aligned} a^p \cdot a^{-q} &= a^q \cdot a^{-q} \\ a^{p-q} &= e, \end{aligned}$$

porém, como $0 < p - q < k'$, entramos em contradição, já que k' é o menor inteiro tal que essa relação é verdadeira. Portanto, a sequência de potências de a:

$$e, a^1, a^2, \ldots, a^{k'-1}$$

possui todos elementos distintos.

Por fim, basta mostrar que $k' = m$. Para isso, consideremos $n \in \mathbb{Z}$. Pelo algoritmo de Euclides, pode-se escrever $n = qk' + r$, tal que $0 \leq r < k'$. Assim,

$$a^n = a^{qk'+r} = a^{qk'} \cdot a^r = e \cdot a^r = a^r.$$

Isso significa que para qualquer n, a^n encontra-se na sequência de elementos distintos enunciada acima. Portanto,

$$\langle a \rangle = \{a^n \mid n \in \mathbb{Z}\} = \{e, a^1, a^2, \ldots, a^{k'-1}\},$$

e ainda, como $|a| = m$, $m = k'$, como queríamos mostrar. $\square$

Capítulo 3

Classes Laterais

Definição 3.0.1. Sejam $S \leq A$, A um grupo e $a \in A$, define-se como **classe lateral à esquerda de S em A** o subconjunto de A

$$aS = \{as \mid s \in S\}.$$

(uma **classe lateral à direita é definida por** $Sa = \{sa \mid s \in S\}$).
Analogamente, pode-se definir a seguinte relação

$$y \sim_E a \ \Leftrightarrow \exists \ s \in S \ \text{ tal que y = as.}$$

Assim, a **classe lateral à esquerda de** S pode também ser escrita como

$$aS = \{y \in A \mid y \sim_E a\}$$

Proposição 3.0.2. A relação

$$y \sim_E a \ \Leftrightarrow \exists \ s \in S \ \text{ tal que y = as}$$

é uma relação de equivalência[a].

[a]Uma relação de equivalência é uma relação que seja reflexiva, simétrica e transitiva

Demonstração. Primeiramente, provaremos que a relação é reflexiva, i.e., $a \sim_E a$. Ora, $\forall a \in A$,

$$ae \in A,$$

onde e é o elemento identidade do subgrupo S.

Mostraremos agora que a relação é simétrica, i.e., se $y \sim_E a$, então $a \sim_E y$. Ora, se $\exists s \in S$ tal que $y = as$, então

$$\begin{aligned} y &= as \\ ys^{-1} &= ass^{-1} \\ ys^{-1} &= a, \end{aligned}$$

onde $s^{-1} \in S$, uma vez que S é um subgrupo.

Finalmente, mostraremos que a relação é transitiva, i.e., se $y \sim_E a$ e $a \sim_E b$, onde $a, b \in A$, então $y \sim_E b$. Ora, se $\exists s \in S$ tal que $y = as$ e $\exists t \in S$ tal que $a = bt$, então

$$\begin{aligned} y &= as \\ &= bts \\ &= bu, \end{aligned}$$

onde $u = ts \in S$, uma vez que S é um subgrupo. Assim, a relação apresentada é uma relação de equivalência, como queríamos mostrar. □

Lema 3.0.3. Se $\sim$ é uma relação de equivalência em A, então o conjunto de todas as classes de equivalência definidas por $\sim$, forma uma partição de A.

Demonstração. Consideraremos a seguinte notação para uma classe de equivalência: $[a] = \{b \in A \mid a \sim b\}$. Precisamos, então, mostrar que

a) cada elemento do conjunto é não vazio;

b) os elementos são disjuntos entre si;

c) a união de todos os elementos (classes de equivalência) formam A.

Ora, $\forall a \in A$, $a \sim a$ é garantido pela definição de relação de equivalência. Assim, $a \in [a]$, ou seja, $[a] \neq \emptyset$.

Por contraposição mostraremos que os elementos do conjunto são disjuntos entre si, i.e., se $[a] \cap [b] \neq \emptyset$, então $[a] = [b]$. Ora, se a intersecção entre $[a]$ e $[b]$ não é o conjunto vazio,

$$\exists c \mid a \sim c \text{ e } b \sim c,$$

e consequentemente $c \sim a$ e $c \sim b$. Assim, pelas propriedades de simetria e transitividade,

$$\forall x \in [a] \mid x \sim a \Rightarrow x \sim c \Rightarrow x \sim b,$$

ou seja, $x \in [b]$, ou ainda, $[a] \subseteq [b]$. A mesma lógica pode ser aplicada para provar $[b] \subseteq [a]$. Portanto, $[a] = [b]$, como queríamos.

Por fim, mostraremos que a união de todos os elementos formam A. Ora, $\forall a \in A$, todo elemento da classe de equivalência $[a]$ pertence à A, assim, a união de todas as classes de equivalência é subconjunto de A. Para o caminho inverso, tem-se que $\forall a \in A$, $a \in [a]$. Como $[a]$ pertence a união de todas as classes de equivalência, então A é subconjunto da união de todas as classes de equivalência. Portanto, $A = \bigcup_{a\in A}[a]$, como queríamos, concluindo a prova. □

Definição 3.0.4. A cardinalidade do conjunto de classes laterais à esquerda de S em A é o **índice** de S em A, denotado por $(A : S)$.

Proposição 3.0.5. Todas as classes laterais de S em A têm a mesma cardinalidade, que é igual a $|S|$.

Demonstração. Ora, $S \to aS$ é claramente uma bijeção de cada classe lateral com S. O mesmo pode ser afirmado sobre as classes laterais à direita. □

Teorema 3.0.6. (Teorema de Lagrange) Sejam A um grupo finito e $S \leq A$. Então $|S| \cdot (A : S) = |A|$.

Demonstração. Como mostrado pelo lema 3.0.3, o conjunto das classes laterais à esquerda de S em A formam uma partição de A. Ademais, pela proposição 3.0.5, a cardinalidade de cada classe lateral é igual à cardinalidade de S. Assim,

$$|A| = |S| \cdot (A : S),$$

como queríamos mostrar. □

Teorema 3.0.7. (Pequeno Teorema de Fermat) Seja p um número primo, então para a não múltiplo de p

$$a^{p-1} \equiv 1(mod\ p).$$

Demonstração. Denotando o módulo p de um número k por $\overline{k}$, tem-se que

$$\overline{a} \in \mathbb{Z}/p\mathbb{Z} \backslash \{\overline{0}\}.$$

Ora, $\mathbb{Z}/p\mathbb{Z}$ é um grupo com a operação de multiplicação $\odot$, tal que $\overline{1}$ é o elemento neutro e para $a, b \in \mathbb{Z}/p\mathbb{Z}$, $\overline{a} \odot \overline{b} = \overline{ab}$. A cardinalidade desse grupo é $p - 1$.

Assim, pelo teorema 3.0.6, $|\langle\overline{a}\rangle|$ divide a cardinalidade de $\mathbb{Z}/p\mathbb{Z}$. E, pelo teorema 2.0.7,

$$\begin{aligned}\overline{a}^{(p-1)} &= \overline{a}^{(k\cdot|\langle a\rangle|)} = \overline{1}^{(k)}\\ &= \overline{1},\end{aligned}$$

ou seja,

$$a^{p-1} \equiv 1(mod\ p),$$

como queríamos. $\square$

Capítulo 4

Subgrupos Normais e Grupos Quocientes

Um caso importante no estudo da teoria de grupos, que nos será útil mais a frente, para um grupo A e um subgrupo $H \leq A$, é quando a função com operação herdada de A

$$(xH, yH) \mapsto xyH, \tag{4.1}$$

para $x, y \in A$, está bem definida, isto é, quando o conjunto de subconjuntos de A forma um grupo.

Proposição 4.0.1. $(xH, yH) \mapsto xyH$ estar bem definida é equivalente a $aha^{-1} \in H, \forall h \in H$, tal que $a \in A$.

Demonstração. Para que a operação seja bem definida, duas entradas iguais na função devem resultar na mesma saída. Isto é, sejam (x_1H, y_1H) e (x_2H, y_2H) iguais, então $x_1y_1H = x_2y_2H$.

Assim, sejam duas entradas iguais

$$x_1h_1 = x_2h_2$$

$$y_1j_1 = y_2j_2,$$

tais que $\exists h2, \forall h1 \in H$ e $\exists j2, \forall j1 \in H$.

$$\Rightarrow x_1 = x_2h_2h_1^{-1}$$

$$y_1 = y_2j_2j_1^{-1}$$

Disso, é verdade então que

$$\begin{aligned}(y_2^{-1}x_2^{-1})x_1y_1 &= (y_2^{-1}x_2^{-1})x_2h_2h_1^{-1}y_2j_2j_1^{-1}\\ &= y_2^{-1}h_2h_1^{-1}y_2j_2j_1^{-1}.\end{aligned}$$

Ora, como apontado acima que a operação estar bem definida acontece quando $x_1y_1H = x_2y_2H$, i.e., $(y_2^{-1}x_2^{-1})x_1y_1 \in H$, tem-se que

$$\begin{aligned}(y_2^{-1}x_2^{-1})x_1y_1 \in H &\Leftrightarrow (y_2^{-1}x_2^{-1})x_2h_2h_1^{-1}y_2j_2j_1^{-1} \in H\\ &\Leftrightarrow y_2^{-1}h_2h_1^{-1}y_2j_2j_1^{-1} \in H\\ &\Leftrightarrow y_2^{-1}h_2h_1^{-1}y_2 \in H,\end{aligned}$$

pois $j_2j_1^{-1} \in H$.

Tomando $h = h_2h_1^{-1}$, relembremos que h_2 é um elemento não arbitrário e h_1 é um elemento arbitrário, assim, h também é um elemento arbitrário e pode-se concluir que

$$x_1y_1H = x_2y_2H \Leftrightarrow (y_2^{-1}x_2^{-1})x_1y_1 \in H \Leftrightarrow y_2^{-1}hy_2 \in H, \tag{4.2}$$

$\forall h \in H$, tal que $y_2 \in A$, como queríamos mostrar. □

Proposição 4.0.2. Seja $H \leq A$, onde A é um grupo. Então as afirmações seguintes são todas equivalentes:

0. $(xH, yH) \mapsto xyH$ estar bem definida;
1. $aHa^{-1} \subseteq H$, $\forall a \in A$;
2. $aHa^{-1} = H$, $\forall a \in A$;
3. $aH = Ha$, $\forall a \in A$.

Demonstração. Que o item 0 $\Leftrightarrow$ item 1 já foi provado pela proposição 4.0.1. Para mostrar que 1 $\Rightarrow$ 2, consideremos $h \in H$ e $a \in A$,

$$h = a^{-1}(aha^{-1})a \in a^{-1}(aHa^{-1})a \subseteq a^{-1}Ha = bHb^{-1},$$

$\forall b \in A$.

Ademais, é imediato que 2 $\Rightarrow$ 1. Por fim, que 2 $\Leftrightarrow$ 3 é óbvio uma vez que

$$aHa^{-1} = H \Leftrightarrow aHa^{-1}a = aH = Ha.$$

□

Definição 4.0.3. Chama-se de *subgrupo normal* de um grupo A (denotado por $H \trianglelefteq A$) um subgrupo $H \leq A$ tal que H satisfaça uma (e, portanto, todas) das afirmações da proposição anterior. Nota-se ainda que como nesse caso as classes laterais à direita de H e à esquerda de H são iguais, elas serão chamadas simplesmente por *classes laterais*.

Alguns exemplos de subgrupos normais estão descritos a seguir:

Exemplo 1) O subgrupo $\{e\}$ e o próprio grupo A são subgrupos normais de A;

Exemplo 2) O subgrupo (chamado de centro de A)

$$Z(A) = \{x \in A | xa = ax, \forall a \in A\} \triangleleft A.$$

Ou ainda, mais geralmente, se $H < Z(A)$, então $H \triangleleft A$. A prova disso vem diretamente da afirmação 3 da proposição 4.0.2;

Exemplo 3) Se um grupo A é abeliano (rever definição 1.0.4), então todo subgrupo de A é normal em A. A prova disso vem diretamente do item anterior, uma vez que o centro de um grupo abeliano é o próprio grupo.

Teorema 4.0.4. Considere um subgrupo normal H de um grupo A. Então, o conjunto das classes laterais, com operação induzida de A, é também um grupo. Note que esse grupo não é subgrupo de A.

Demonstração. O conjunto das classes laterais é dado por

$$\{aH | \ a \in A\}.$$

Assim, sejam $a, b \in A$,

$$\begin{aligned} aH \cdot bH &= aH \cdot Hb \\ &= aHb \\ &= abH, \end{aligned}$$

como $ab \in A$, mostramos que a operação induzida de A para o conjunto das classes laterais é fechada. Ademais, uma vez que a operação é induzida, temos garantida a associatividade, pois, sejam $a, b, c \in A$,

$$(aH \cdot bH) \cdot cH = (abc)H = aH \cdot (bH \cdot cH).$$

Agora, consideremos e o elemento identidade de A e $a \in A$, então

$$eH \cdot aH = (ea)H = aH,$$

i.e., $eH = H$ é o elemento identidade do grupo das classes laterais. Por fim, sejam $a \in A$ e $a^{-1} \in A$ o elemento inverso de a. Então,

$$aH \cdot a^{-1}H = (aa^{-1})H = eH,$$

i.e. $a^{-1}H$ é o elemento inverso da classe aH. $\square$

Definição 4.0.5. Sejam A um grupo e $H \leq A$ um subgrupo, então o grupo de todas suas classes laterais (denotado por A/H) com a operação induzida de A é chamado de *grupo quociente* de A por H.

Proposição 4.0.6. Sejam A um grupo e A' seu subgrupo dos comutadores, i.e., $\langle\{xyx^{-1}y^{-1}|x, y \in A\}\rangle$. Então,

1. A/A' é abeliano;
2. A' é o menor subgrupo normal de A com a propriedade do item anterior. Ou seja, se $H \triangleleft A$ é tal que A/H é abeliano, então $A' \subseteq H$.

Demonstração. Para o item 1, consideremos $a, b \in A$, então, como $(b^{-1}a^{-1}ba) \in A'$,

$$aA' \cdot bA' = abA' = ab(b^{-1}a^{-1}ba)A' = baA' = bA' \cdot aA'. \square$$

Para o item 2, suponhamos um grupo A e um subgrupo $H \leq A$, tal que A/H seja abeliano. Então, para $a, b \in A$,

$$abH = aH \cdot bH = bH \cdot aH = baH.$$

Ora, multiplicando ambas as extremidades da equação pela esquerda por $(ba)^{-1}$, tem-se

$$a^{-1}b^{-1}abH = H,$$

ou seja, $A' \subseteq H$. $\square$

Capítulo 5

Homomorfismos de Grupos

Definição 5.0.1. Sejam $(A, \cdot)$ e $(\mathcal{A}, \times)$ dois grupos. A função $f : A \to \mathcal{A}$ é dita um *homomorfismo* se
$$f(a \cdot b) = f(a) \times f(b),\ \forall a, b \in A.$$

Alguns exemplos de homomorfismos de grupos estão descritos a seguir:

Exemplo 1) Identidade: $Id : (A, \cdot) \to (A, \cdot)$, $Id(a) = a,\ a \in A$.

Exemplo 2) Trivial: $e : A \to \mathcal{A}$, $e(a) = e_{\mathcal{A}}, \forall a \in A$.

Exemplo 3) Projeção Canônica: Sendo $H \triangleleft A$, então $\phi : A \to A/H$, $\phi(a) = aH = Ha$.

Exemplo 4) Sejam A é um grupo abeliano e $n \in \mathbb{Z}$ fixo, então $\phi_n : A \to A$, $\phi_n(a) = a^n$ é um homomorfismo.

Exemplo 5) Seja $a \in A$ fixo, então $\mathcal{I}_a : A \to A$, $\mathcal{I}_a(x) = axa^{-1},\ x \in A$, é um homomorfismo bijetivo.

Demonstração. Primeiramente, mostraremos que $\mathcal{I}_a$ é um homomorfismo. Ora,

$$\begin{aligned}
\mathcal{I}_a(xy) &= axya^{-1} \\
&= ax(a^{-1}a)ya^{-1} \\
&= (axa^{-1})(aya^{-1}) \\
&= \mathcal{I}_a(x)\mathcal{I}_a(y).
\end{aligned}$$

Ademais, mostraremos que $\mathcal{I}_a$ é bijetiva. Uma função é bijetiva se, e somente se, a função admite inversa (a demonstração disso é encontrada facilmente na internet).

Assim, mostraremos que $\mathcal{I}_a^{-1}(x) = a^{-1}xa$ é a inversa de $\mathcal{I}_a$. Ora, $\forall x \in A$,

$$\begin{aligned}\mathcal{I}_a^{-1}(\mathcal{I}_a(x)) &= a^{-1}(axa^{-1})a \\ &= (a^{-1}a)x(a^{-1}a) \\ &= x,\end{aligned}$$

e, logo, a função é bijetora. $\square$

Algumas propriedades importantes de homomorfismo de grupos está listada a seguir. Seja $f : (A, \cdot) \to (\mathcal{A}, \times)$, então:

1. $f(e_A) = e_{\mathcal{A}}$.
   A demonstração disso vem de que

$$f(e_A) = f(e_A \cdot e_A) = f(e_A) \times f(e_A) \Rightarrow f(e_A) = e_{\mathcal{A}}.$$

2. $f(a^{-1}) = f(a)^{-1}$.
   A demonstração disso vem de que $e_{\mathcal{A}} = f(a \cdot a^{-1}) = f(a) \times f(a^{-1})$

$$\Rightarrow f(a)^{-1} = f(a)^{-1} \times e_{\mathcal{A}} = f(a)^{-1} = f(a^{-1}).$$

3. chama-se por *núcleo* do homomorfismo f o subgrupo normal de A

$$kerf := \{a \in A \mid f(a) = e_{\mathcal{A}}\}.$$

   A prova de que $kerf < A$ vem de que, sejam $x, y \in kerf$, então

$$f(x \cdot y) = f(x) \times f(y) = e_{\mathcal{A}}.$$

$$f(x^{-1}) = f(x)^{-1} = e_{\mathcal{A}}.$$

   Ademais, tem-se que $kerf \lhd A$ pois, para qualquer $a \in A$,

$$f(axa^{-1}) = f(a) \times f(x) \times f(a)^{-1} = f(a) \times f(a)^{-1} = e_{\mathcal{A}}$$

$$\Rightarrow axa^{-1} \in kerf. \ \square$$

4. chama-se por *imagem* de f o subgrupo de $\mathcal{A}$

$$Im(f) = \{y \in \mathcal{A} \mid y = f(a) \text{ para algum } a \in A\}.$$

   A prova que $Im(f) < \mathcal{A}$ vem de que, sejam $x, y \in Im(f)$, então $\exists a, b \in A$ tais que

$$x \times y = f(a) \times f(b) = f(a \cdot b) \in Im(f).$$

$$e_{\mathcal{A}} = f(e_A) = f(a \cdot a^{-1}) = f(a) \times f(a^{-1}) = x \times x^{-1}$$
$$\Rightarrow x^{-1} = f(a^{-1}) \in Im(f).$$

5. se $H \leq A$, então $f(H) \leq \mathcal{A}$ e $f^{-1}(f(H)) = Hkerf$.
   A prova que $f(H) \leq \mathcal{A}$ vem de que, sendo $x, y \in f(H)$, então $\exists a, b \in H$ tais que
$$x \times y = f(a) \times f(b) = f(a \cdot b) \in f(H).$$
$$e_{\mathcal{A}} = f(e_A) = f(a \cdot a^{-1}) = f(a) \times f(a^{-1}) = x \times x^{-1}$$
$$\Rightarrow x^{-1} = f(a^{-1}) \in f(H).$$
   Ademais, provaremos que $f^{-1}(f(H)) = Hkerf$. Sejam $h \in H$ e $k \in kerf$, então
$$f(h \cdot k) = f(h) \times f(k) = f(h) \times e_{\mathcal{A}} = f(h) \in f(H)$$
$$\Rightarrow Hkerf \subseteq f^{-1}(f(H)).$$
   A inclusão contrária vem de que seja $x \in f^{-1}(f(H))$, então
$$f(x) \in f(H),$$
   assim, $\exists h \in H$, tal que $f(x) = f(h)$. Dessa forma,
$$f(h)^{-1} f(x) = e_{\mathcal{A}} \ \Rightarrow \ h^{-1}x \in kerf.$$
   Então,
$$x = h(h^{-1}x) \in Hkerf. \ \square$$

6. $kerf = \{e_A\} \Leftrightarrow f$ é injetiva.
   Para a função ser injetiva, para quaisquer $a, b \in A$, se $f(a) = f(b)$, então $a = b$. Ora, sejam $a, b \in kerf$, então
$$f(a) = f(b) = e_{\mathcal{A}}.$$
   Sabemos que $f(e_A) = e_{\mathcal{A}}$ para qualquer homomorfismo. Assim,
$$a = b \Leftrightarrow kerf = \{e_A\}. \ \square$$

7. se $\mathcal{O}(x)$ é finita, então $\mathcal{O}(f(x))$ divide $\mathcal{O}(x)$.
   A prova disso vem de que
$$x^{\mathcal{O}(x)} = e_A.$$
   Assim,
$$e_{\mathcal{A}} = f(e_A) = f(x^{\mathcal{O}(x)}) = f(x)^{\mathcal{O}(x)},$$
   i.e., $\mathcal{O}(f(x))$ divide $\mathcal{O}(x)$.

8. seja $g : (\mathcal{A}, \times) \to (\mathcal{H}, \odot)$ um outro homomorfismo, então a composição

$$g \circ f : (A, \cdot) \to (\mathcal{H}, \odot)$$

também é um homomorfismo.
A prova disso vem de que

$$g \circ f(x \cdot y) = g(f(x \cdot y)) = g(f(x) \times f(y)) = g(f(x)) \odot g(f(y)) = (g \circ f(x)) \odot (g \circ f(y)). \square$$

Definição 5.0.2. Seja $f : A \to \mathcal{A}$ um homomorfismo. f é chamado de *isomorfismo* se existe um homomorfismo $g : \mathcal{A} \to A$ tal que $f \circ g = id_{\mathcal{A}}$ e $g \circ f = id_A$. Utilizaremos a notação $A \simeq \mathcal{A}$ para denotar a relação de isomorfismo entre os grupos.

Proposição 5.0.3. Seja $f : (A, \cdot) \to (\mathcal{A}, \times)$ um homomorfismo, então f é um isomorfismo se, e somente se, f é bijetora.
Prova: Pelo Teorema de Cantor-Bernstein-Schroeder[a], tem-se que $(\Rightarrow)$ é imediato. Ademais, suponhamos que f é bijetiva, então $\forall x, y \in \mathcal{A}$,

$$\begin{aligned} f^{-1}(x \times y) &= f^{-1}(f(a) \times f(b)) \\ &= f^{-1}(f(a \cdot b)) \\ &= a \cdot b \\ &= f^{-1}(x) \cdot f^{-1}(y), \end{aligned}$$

tais que $a = f^{-1}(x), b = f^{-1}(y) \in A$. Assim, mostramos que $(\Leftarrow)$ também é verdadeira. $\square$

[a] O qual diz que se existe injeção de $A \to B$ e de $B \to A$, então existe uma bijeção $A \to B$.

Proposição 5.0.4. Seja $f : A \to \mathcal{A}$ um homomorfismo injetivo de grupos. Então

$$\mathcal{O}(f(x)) = \mathcal{O}(x), \ \forall x \in A.$$

Demonstração. A ordem de $f(x)$ é dada pela cardinalidade do subgrupo gerado por $f(x)$, i.e., $|\langle f(x) \rangle|$. Como já apontado ao analisar subgrupos gerados por um único elemento, podemos escrever isso também como

$$|\{f(x)^n \mid n \in \mathbb{Z}\}|.$$

Como já mostrado,

$$\langle x \rangle = \{e, x, x^2, x^3, \ldots, x^{\mathcal{O}(x)-1}\},$$

onde todos os elementos são distintos.
Uma vez que a função f é um homomorfismo injetivo, tem-se

$$f(x^n) = f(\underbrace{x \cdot x \cdot (\dots) \cdot x}_{n \text{ elementos}}) = \underbrace{f(x) \times f(x) \times (\dots) \times f(x)}_{n \text{ elementos}},$$

tal que para cada entrada $a \neq b$, com $a, b \in A$, $f(a) \neq f(b)$. Assim, $\mathcal{O}(x) = \mathcal{O}(f(x))$. □

Teorema 5.0.5. (Primeiro Teorema do Isomorfismo). Seja $f : A \to \mathcal{A}$ um homomorfismo de grupos. Então,

$$Im(f) \simeq A/ker(f).$$

Demonstração. Provaremos primeiramente que o isomorfismo dado por

$$\phi : A/ker(f) \to Im(f)$$

$$f(x) = \phi(x \cdot ker(f))$$

é bem definido, i.e., se

$$\forall x, y \in A,\ xker(f) = yker(f) \Rightarrow \phi(xker(f)) = \phi(yker(f)).$$

Ora,

$$\begin{aligned} & xker(f) = yker(f) \\ \Leftrightarrow \quad & y^{-1}x \in ker(f) \\ \Leftrightarrow \quad & f(y^{-1}x) = e_{\mathcal{A}} \\ \Leftrightarrow \quad & f(y)^{-1} \times f(x) = e_{\mathcal{A}} \\ \Leftrightarrow \quad & f(x) = f(y). \end{aligned}$$

Portanto, ϕ é bem definida.

ϕ também é um homomorfismo uma vez que

$$\phi(xker(f) \cdot yker(f)).$$

Como $ker(f) < A$,

$$\begin{aligned} \phi(xker(f) \cdot yker(f)) &= \phi(xyker(f)) \\ &= f(xy) \\ &= f(x)f(y) \\ &= \phi(xker(f))\phi(yker(f)). \end{aligned}$$

Ademais, mostraremos que ϕ é injetiva. Ora, mostramos que

$$f(x) = f(y) \Leftrightarrow xker(f) = yker(f).$$

Assim, pela definição de ϕ,

$$\phi(xker(f)) = \phi(yker(f)) \Leftrightarrow xker(f) = yker(f),$$

que é a definição de injetividade.

Mostraremos por fim a subjetividade de ϕ. Ora, tem-se que

$$Im(\phi) = \phi(Aker(f)) = f(A) = Im(f),$$

i.e., a imagem de ϕ é equivalente ao seu contra-domínio ($Img(f)$), como queríamos.

O diagrama comutativo abaixo ilustra essa prova.

$$\begin{tikzcd}
& A \arrow[dl] \arrow[dr, "f"] \arrow[d, phantom, "\circlearrowleft"] & \\
A/ker(f) \arrow[rr, "\phi"'] & & Im(f) \subseteq \mathcal{A}
\end{tikzcd}$$

□

Neste momento, enunciaremos um lema que será útil para o próximo teorema.

Lema 5.0.6. Sejam $H \leq A$ um subgrupo e $N \triangleleft A$ um subgrupo normal. Então,

$$H \cap N \triangleleft H.$$

Demonstração. Uma vez que sendo ambos H e N subgrupos de A, a associatividade, o elemento identidade e inversa de cada elemento nos subgrupos são herdados de A. Assim, sejam $x, y \in H \cap N$, então $x, y \in H$ e $x, y \in N$. Como $xy^{-1} \in H$ e $xy^{-1} \in N$, $xy^{-1} \in H \cap N$, i.e., a operação é fechada e para todo elemento existe elemento inverso correspondente. Assim, $H \cap N$ é um subgrupo de H. Ademais, seja $h \in H$ e $x \in H \cap N$, então

$$hxh^{-1} \in H,$$

pois $x \in H$ e a operação é fechada. Além disso,

$$hxh^{-1} \in N,$$

pois $x \in N$ e N é um subgrupo normal. Portanto,

$$hxh^{-1} \in H \cap N,$$

i.e., $H \cap N$ é subgrupo normal de H. □

Teorema 5.0.7. (Segundo Teorema do Isomorfismo). Sejam $H \leq A$ um subgrupo e $N \triangleleft A$ um subgrupo normal. Então,

$$\frac{H}{H \cap N} \simeq \frac{HN}{N}.$$

Demonstração. Temos pel o Lema 5.0.6 que

$$H \cap N \triangleleft H.$$

Agora, seja $f : H \to HN/N$, $f(h) = hN$. Mostraremos que f é um homomorfismo já que

$$\begin{aligned} f(h_1h_2) &= (h_1h_2)N \\ &= (h_1N)(h_2N) \\ &= f(h_1)f(h_2). \end{aligned}$$

Notemos agora que

$$\begin{aligned} ker(f) &= \{h \in H \mid hN = e_{HN/N} = N\} \\ &= \{h \in H \mid h \in N, \} \end{aligned}$$

i.e., $ker(f) = H \cap N$.

Por fim, mostraremos que f é sobrejetora. Ora, pela definição,

$$f(h) \in HN/N \Rightarrow f(H) \subseteq HN/N.$$

E, por sua vez, qualquer elemento de HN/N,

$$hnN = hN = f(h) \in f(H) \Rightarrow HN/N \subseteq f(H)$$

$$\Rightarrow f(H) = HN/N,$$

i.e., f é sobrejetora.

Dessa forma, pelo Teorema 5.0.5, tem-se que

$$f(H) \simeq H/kerf(f) \Rightarrow \frac{HN}{N} \simeq \frac{H}{H \cap N}.$$

□

Teorema 5.0.8. (Terceiro Teorema do Isomorfismo). Sejam H e N subgrupos normais de A, tais que $N \subseteq H \subseteq A$. Então,

$$\frac{A/N}{H/N} \simeq A/H.$$

Demonstração. Primeiramente, mostraremos que $N \triangleleft H$, o que é imediato uma vez que $H \subseteq A$ e $N \triangleleft A$.

Agora, seja a função $f : A/N \to A/H$, tal que $f(aN) = aH$. Mostraremos que ela é bem definida. Ora, sejam

$$xN = yN.$$

Então,

$$y^{-1}x \in N \subseteq H,$$

ou seja,

$$y^{-1}x \subseteq H \Rightarrow xH = yH,$$

e a função é bem definida.

A prova que f é um homomorfismo vem de que

$$\begin{aligned} f(xN)f(yN) &= (xH)(yH) \\ &= xyH \\ &= f(xyN) \\ &= f((xN)(yN)). \end{aligned}$$

Ademais, tem-se que

$$\begin{aligned} ker(f) &= \{xN \in A/N \mid f(xN) = e_{A/H}\} \\ &= \{xN \in A/N \mid xH = H\} \\ &= \{xN \in A/N \mid x \in H\} \\ &= H/N. \end{aligned}$$

Além disso, das propriedades do homomorfismo, sabe-se que o $ker(f) = H/N$ é subgrupo normal do domínio de f, isto é, A/N.

Por fim, f é sobrejetiva já que, sendo $aH \in A/H$, claramente,

$$aH = f(aN) \in f(A/N).$$

Assim,

$$f(A/N) = A/H.$$

Dessa forma, pelo Teorema 5.0.5, tem-se que

$$f(A/N) \simeq (A/N)/kerf(f) \Rightarrow A/H \simeq \frac{A/N}{H/N}.$$

$\square$

Enunciaremos agora alguns lemas sobre funções e sobre homomorfismos de grupos que nos serão úteis para o próximo teorema.

Definição 5.0.9. Seja uma função $f : X \to Y$, então, sendo $A \subseteq X$ e $B \subseteq Y$, definimos

$$f(A) = \{y \in Y \mid y = f(a), \text{ para algum } a \in A\},$$

e definimos como sendo a *pré-imagem* de f

$$f^{-1}(B) = \{x \in X \mid f(x) \in B\}.$$

Lema 5.0.10. Sejam uma função $f : X \to Y$ e $A \subseteq X$ e $B \subseteq Y$, é verdade que:

1. $f(f^{-1}(B)) \subseteq B$; ou ainda $f(f^{-1}(B)) = B$, sse f é sobrejetora;
2. $f^{-1}(f(A)) \supseteq A$; ou ainda $f^{-1}(f(A)) = A$, sse f é injetora.

Demonstração. Para a primeira afirmação, tem-se que

$$\begin{aligned} f(f^{-1}(B)) &= f(\{x \in X \mid f(x) \in B\}) \\ &\subseteq B. \end{aligned}$$

Ademais, se f é sobrejetora, seja $b \in B$,

$$\exists x \in X \mid f(x) = b.$$

Ora, então $x \in f^{-1}(B)$ pela definição de pré-imagem, e

$$b = f(x) \in f(f^{-1}(B)).$$

Já para a segunda afirmação, tem-se

$$\begin{aligned} f^{-1}(f(A)) &= f^{-1}(\{y \in Y \mid y = f(a), \text{ para algum } a \in A\}) \\ &= \{x \in X \mid f(x) \in \{y \in Y \mid y = f(a), \text{ para algum } a \in A\}\} \\ &= \{x \in X \mid f(x) = f(a), \text{ para algum } a \in A\} \\ &\supseteq A. \end{aligned}$$

Além disso, se f é injetora, seja $z \in f^{-1}(f(A))$. Então, pela definição de pré-imagem,

$$f(z) = f(a) \in f(A),$$

para algum $a \in A$. Ora, como f é injetora,

$$z = a \in A.$$

$\square$

Note que se uma função f^{-1} satisfaz $f(f^{-1}(B)) = B$ e $f^{-1}(f(A)) = A$, ela é também é a função inversa de f.

Lema 5.0.11. Seja um homomorfismo de grupos $\phi : A \to H$, então, sendo $X \leq A$ e $Y \leq H$ subgrupos, é verdade que:

1. $\phi(\phi^{-1}(Y)) = Y \cap Im(\phi)$;
2. $\phi^{-1}(\phi(X)) = Xker(\phi)$.

Demonstração. Para a primeira afirmação, tem-se que $\phi(\phi^{-1}(Y)) \subseteq Y$ pelo lema anterior (5.0.10) e ainda, por definição, $\phi(\phi^{-1}(Y)) \subseteq Im(\phi)$. Assim,

$$\phi(\phi^{-1}(Y)) \subseteq Y \cap Im(\phi).$$

Ademais, sendo $z \in Y \cap Im(\phi)$, $\exists a \in A$, tal que

$$\phi(a) = z \in Y.$$

Ora, então, pela definição de pré-imagem,

$$a \in \phi^{-1}(Y)$$

$$\Rightarrow z = \phi(a) \in \phi(\phi^{-1}(Y)).$$

Já para a segunda afirmação, tem-se que $\phi^{-1}(\phi(X)) = Xker(\phi)$ pela propriedade do isomorfismo já provada (ver propriedade 5).

E ainda, caso ϕ seja injetora, $ker(\phi) = \{e_A\}$ e $Xker(\phi) = X$, e assim

$$\phi^{-1}(\phi(X)) = X.$$

□

Lema 5.0.12. O homomorfismo (projeção canônica)

$$\phi : A \to A/H,$$

onde $H \lhd A$, é sobrejetiva. E, ainda,

$$ker(\phi) = H.$$

Demonstração. Seja $z \in A/H$, então como $z = aH$ e $a \in A$,

$$z = aH = \phi(a) \in \phi(A),$$

ou seja, ϕ é sobrejetiva.

Além disso, provaremos que o $ker(f) = H$. Ora,

$$\begin{aligned} ker(f) &= \{a \in A \mid f(a) = H\} \\ &= \{a \in A \mid aH = H\} \\ &= \{a \in A \mid a \in H\} \\ &= H. \end{aligned}$$

□

Teorema 5.0.13. (Teorema da Correspondência). Seja $N \lhd A$ um subgrupo normal. Então, o homomorfismo $f : A \to A/N$ (projeção canônica) induz uma correspondência bijetiva entre o conjunto $\mathcal{L}_N$ dos subgrupos de A que contêm N e o conjunto $\mathcal{L}$ dos subgrupos de A/N, dada por:

$$\hat{f} : V \in \mathcal{L}_N \longmapsto f(V) = V/N \in \mathcal{L}.$$

Ademais, $\hat{f}^{-1} : \mathcal{L} \to \mathcal{L}_N$, tal que $H \mapsto f^{-1}(H)$, é função inversa de $\hat{f}$.
Além disso, sejam $X \in \mathcal{L}_N$ e $Y \in \mathcal{L}$,

i. $X \lhd A \Rightarrow f(X) \lhd Im(f)$;

ii. $Y \lhd Im(f) \Rightarrow f^{-1}(Y) \lhd A$.

Demonstração. Mostraremos inicialmente que $V/N \leq A/N$. Sendo $x, y \in V/N$, $\exists a, b \in V$ tais que

$$xy = (aN)(bN),$$

e como $N \lhd A$ e $N \subseteq V \leq A$,

$$xy = abN \in V/N,$$

já que $ab \in V$. Ademais,

$$x^{-1} = (aN)^{-1} = a^{-1}N \in V/N,$$

já que $a^{-1} \in V$. Assim, mostramos que

$$V/N \leq A/N,$$

i.e., V/N é subgrupo de A/N e $V/N \in \mathcal{L}$.
Mostraremos agora que $\hat{f}$ é bijetora ao mostrar que a função pré-imagem

$$\hat{f}^{-1} : H \mapsto f^{-1}(H) \in \mathcal{L}_N$$

é função inversa de $\hat{f}$.

Ora, pelo lema 5.0.12, f é sobrejetora. Seja $H \in \mathcal{L}$, vamos provar agora que $\exists K \leq A$, tal que

$$H = K/N.$$

Mostraremos inicialmente que essa afirmação é equivalente a

$$H \leq A/N \Rightarrow H = f^{-1}(H)/N.$$

Seja $K := f^{-1}(H)$. Então, devemos mostrar que $K \leq A$ e $N \subseteq K$. Suponhamos $x, y \in K = f^{-1}(H)$. É verdade, portanto, que

$$f(x), f(y) \in H.$$

Como H é um grupo,

$$\begin{array}{lc} & f(x)f(y) \in H \\ \Rightarrow & f(xy) \in H \\ \Rightarrow & xy \in f^{-1}(H) = K. \end{array}$$

Ademais, como $f(x) \in H$,

$$\begin{array}{lc} & f(x)^{-1} \in H \\ \Rightarrow & f(x^{-1}) \in H \\ \Rightarrow & x^{-1} \in f^{-1}(H) = K. \end{array}$$

E, portanto, $K \leq A$.

Mostraremos agora que sendo $n \in N$, $n \in K$. Ora,

$$\begin{array}{lc} \Rightarrow & f(n) = nN \in H \\ \Rightarrow & n \in f^{-1}(H) = K \\ \Rightarrow & N \subseteq K. \end{array}$$

Provaremos agora que $H = f^{-1}(H)/N$.

($\supseteq$) Seja $x \in f^{-1}(H)/N$. Então $\exists y \in f^{-1}(H)$, tal que

$$x = yN.$$

Uma vez que f é sobrejetora e $f^{-1}(H) \subseteq A$,

$$x = yN = f(y) \in H.$$

($\subseteq$) Seja $h \in H \leq A/N$. Podemos escrever h como

$$h = aN = f(a),$$

onde $a \in A$. Assim,

$$f(a) \in H \Rightarrow a \in f^{-1}(H).$$

Ora, então,

$$h = aN \in f^{-1}(H)/N.$$

Demonstrado que $f(K) = K/N$ para algum $K \leq A$ e $N \triangleleft K$,

$$H = f(K) \in f(\mathcal{L}_N)$$

$$\Rightarrow \mathcal{L} \subseteq f(\mathcal{L}_N),$$

e $\hat{f}$ é sobrejetora. Assim, pelo lema 5.0.10,

$$\hat{f}(\hat{f}^{-1}(\mathcal{L})) = \mathcal{L}.$$

Além disso, já mostramos que $ker(f) = N$. Assim, sendo $V \in \mathcal{L}_N$,

$$\hat{f}^{-1}(\hat{f}(V)) = f^{-1}(f(V)) = V ker(f) = VN = V$$

$$\Rightarrow \hat{f}^{-1}(\hat{f}(\mathcal{L}_N)) = \mathcal{L}_N,$$

i.e., $\hat{f}$ é injetora. Assim, mostramos que $\hat{f}^{-1}$ é inversa de $\hat{f}$ e $\hat{f}$ é bijetora.

Por fim,

(i.) Seja $b \in f(A) = Im(f)$. Como f é sobrejetiva, $b = f(a)$, para algum $a \in A$. Então, uma vez que $X \triangleleft A$, $Xa = aX$, e

$$bf(X) = f(a)f(X) = f(aX) = f(Xa) = f(X)f(a) = f(X)b.$$

Portanto, pela definição de normalidade de grupos,

$$f(X) \triangleleft Im(f).$$

(ii.) Sendo $Y \triangleleft Im(f)$, queremos mostrar que $f^{-1}(Y) \triangleleft A$. Isso é equivalente a mostrar que, $\forall a \in A$,

$$af^{-1}(Y)a^{-1} \subseteq f^{-1}(Y) \Leftrightarrow f(af^{-1}(Y)a^{-1}) \subseteq Y \Leftrightarrow f(a)Yf(a)^{-1} \subseteq Y.$$

Ora, como $Y \triangleleft Im(f)$,

$$f(a)Yf(a)^{-1} \subseteq Y, \ \forall a \in A,$$

como queríamos. $\square$

Capítulo 6

Produto Direto de Grupos

Veremos agora uma maneira de se obter um grupo a partir de dois grupos quaisquer.

Definição 6.0.1. Sejam dois grupos A e B, o produto direto $A \times B$ é definido em termo de **componentes** (pares ordenados (a, b), tais que $a \in A$ e $b \in B$) e pelo produto cartesiano desses pares ordenados, i.e.,

$$(a_1, b_1) \cdot (a_2, b_2) = (a_1 a_2, b_1 b_2),$$

onde $(a_1 a_2, b_1 b_2)$ também é um elemento de $A \times B$ e, logo, a operação é fechada.

Proposição 6.0.2. O produto direto $A \times B$ satisfaz os axiomas de grupo e, logo, é um grupo.

Demonstração. Primeiramente, mostraremos que a operação é associativa. Ora,

$$\begin{aligned}
((a_1, b_1) \cdot (a_2, b_2)) \cdot (a_3, b_3) &= (a_1 a_2, b_1 b_2) \cdot (a_3, b_3) \\
&= ((a_1 a_2) a_3, (b_1 b_2) b_3) \\
&= (a_1 (a_2 a_3), b_1 (b_2 b_3)) \\
&= (a_1, b_1) \cdot (a_2 a_3, b_2 b_3) \\
&= (a_1, b_1) \cdot ((a_2, b_2) \cdot (a_3, b_3)).
\end{aligned}$$

Mostraremos agora que a operação tem elemento inverso e identidade. Seja $a \in A$ e $b \in B$, então,

$$(a, b) \cdot (a^{-1}, b^{-1}) = (aa^{-1}, bb^{-1}) = (id_A, id_B),$$

onde (id_A, id_B) é claramente a identidade da operação. $\square$

Buscaremos agora descobrir as condições para que um grupo seja isomorfo a algum produto direto de grupos.

Enunciaremos para isso, um lema que nos será útil para provar essas condições.

Lema 6.0.3. Sejam $A_1, A_2, \dots A_n$ subgrupos de um grupo A, então, dadas as seguintes suposições:

1. $A = A_1A_2 \dots A_n$;
2. $A_i \lhd A, \forall i = 1, \dots, n$;
3. $A_i \cap (A_1 \dots A_{i-1}A_{i+1} \dots A_n) = \{e\}, \forall i = 1, \dots, n$;
4. $\forall a \in A,$ existem únicos $a_1 \in A_1, a_2 \in A_2, \dots, a_n \in A_n$, tais que $a = a_1a_2 \dots a_n$;
5. $\forall i, j$, tais que $1 \leq i, j \leq n$, sendo $a_i \in A_i$ e $a_j \in A_j$, $a_ia_j = a_ja_i$;

é verdade que 1., 2., 3. $\Leftrightarrow$ 4., 5..

Demonstração. Começaremos mostrando que $(1., 2., 3. \Rightarrow 4.)$. Seja $a = a_1a_2 \dots a_n \in A$, sendo $a_1 \in A_1, a_2 \in A_2, \dots, a_n \in A_n$. Suponhamos $b_1 \in A_1, b_2 \in A_2, \dots, b_n \in A_n$, tais que $a = b_1b_2 \dots b_n$. Assim,

$$a_1a_2 \dots a_n = b_1b_2 \dots b_n$$

$$\begin{aligned}
\Rightarrow \qquad & a_1 = b_1b_2 \dots b_n(a_2 \dots a_n)^{-1} \\
\Rightarrow \qquad & a_1 = b_1b_2 \dots b_na_n^{-1} \dots a_2^{-1} \\
\Rightarrow \qquad & b_1^{-1}a_1 = b_2 \dots b_na_n^{-1} \dots a_2^{-1} \\
\Rightarrow \qquad & b_1^{-1}a_1 \in A_2 \dots A_nA_n \dots A_2.
\end{aligned}$$

Ora, como $A_i \lhd A, \forall i = 1, \dots, n$, por comutatividade, i.e., $A_iA_j = A_jA_i$ para $1 \leq j \leq n$, tem-se

$$\begin{aligned}
b_1^{-1}a_1 &\in A_2A_2A_3A_3 \dots A_{n-1}A_{n-1}A_nA_n \\
&\in A_2A_3 \dots A_{n-1}A_n.
\end{aligned}$$

Assim, pela propriedade (3.),

$$b_1^{-1}a_1 = e \Rightarrow a_1 = b_1.$$

Analogamente, fazemos o mesmo procedimento em tal igualdade a fim de chegar que $a_2 = b_2, a_3 = b_3, \dots, a_n = b_n$. Dessa forma, mostramos indutivamente a propriedade (4.).

Agora, mostraremos que $(1., 2., 3. \Rightarrow 5.)$. Sejam $a_i \in A_i$ e $a_j \in A_j$. Então, um elemento da forma
$$a_i a_j a_i^{-1} a_j^{-1}$$
é tal que
$$(a_i a_j a_i^{-1}) a_j^{-1} \in A_j,$$
uma vez que $A_j \lhd A$.
Ainda, como $A_i \lhd A$,
$$a_i (a_j a_i^{-1} a_j^{-1}) \in A_i.$$
Ora, então pela propriedade (3.),
$$a_i a_j a_i^{-1} a_j^{-1} \in A_i \cap A_j = \{e\}.$$
Assim,
$$a_i a_j = a_j a_i,$$
como queríamos mostrar.

Finalmente, mostraremos que $(4., 5. \Rightarrow 1., 2., 3.)$. A propriedade (1.) é claramente satisfeita a partir da propriedade (4.)

Para mostrar que a propriedade (2.) é satisfeita, queremos mostrar que
$$aA_i a^{-1} \subseteq A_i, \forall a \in A \text{ e } \forall i = 1, \ldots, n.$$
Pela propriedade (4.) ou (1.), temos que a pode ser escrito da forma
$$a = a_1 a_2 \ldots a_n.$$
Então, fixado $i \in \{1, \ldots, n\}$, seja $x \in A_i$. Pela comutatividade da propriedade (5.) e por $a_i x a_i^{-1} \in A_i$,
$$\begin{aligned} axa^{-1} &= a_1 \ldots a_i \ldots a_n x (a_1 \ldots a_i \ldots a_n)^{-1} \\ &= a_1 \ldots a_i \ldots a_n x a_n^{-1} \ldots a_i^{-1} \ldots a_1^{-1} \\ &= a_1 \ldots a_i x \ldots a_n a_n^{-1} \ldots a_i^{-1} \ldots a_1^{-1} \\ &= a_1 \ldots (a_i x a_i^{-1}) \ldots a_1^{-1} \\ &= a_1 a_1^{-1} a_2 a_2^{-1} \ldots (a_i x a_i^{-1}) \\ &= a_i x a_i^{-1} \\ &\in A_i, \end{aligned}$$
como queríamos.

Por fim, mostraremos que a propriedade (3.) é satisfeita. Para isso, seja um elemento $x \in A_i \cap A_1 \ldots A_{i-1} A_{i+1} \ldots A_n$. Como $x \in A_i$, então pela propriedade (4.),
$$x = a_1 a_2 \ldots a_n, \text{ com } a_j = e \in A_j \text{ para } j \neq i \text{ e } a_i = x.$$

Ora, como $x \in A_1 \dots A_{i-1}A_{i+1} \dots A_n$,

$$x = b_1 \dots b_{i-1}b_ib_{i+1} \dots b_n, \text{com } b_j \in A_j \text{ e } b_i = e.$$

Utilizando ainda a propriedade (4.), existem únicos $a_1 \in A_1$, $a_2 \in A_2$, ..., $a_n \in A_n$. Assim, $a_1 = b_1, a_2 = b_2, \dots, a_n = b_n$, i.e.,

$$a_i = b_i \Rightarrow x = e,$$

e portanto,

$$A_i \cap (A_1 \dots A_{i-1}A_{i+1} \dots A_n) = \{e\},$$

como queríamos mostrar.

□

Teorema 6.0.4. Sejam $A, H_1, \dots, H_n$ grupos. O grupo A é isomorfo ao grupo $H_1 \times \cdots \times H_n$ se, e somente se, A possui os subgrupos $A_1 \simeq H_1, \dots, A_n \simeq H_n$ tais que:

1. $A = A_1A_2 \dots A_n$.
2. $A_i \lhd A, \forall i = 1, \dots, n$.
3. $A_i \cap (A_1 \dots A_{i-1}A_{i+1} \dots A_n) = \{e\}, \forall i = 1, \dots, n$.

Demonstração. ($\Leftarrow$) Seja $f : A \to A_1 \times \cdots \times A_n$ uma relação, tal que

$$f(a) = (a_1, \dots, a_n),$$

onde $a = a_1a_2 \dots a_n$ com $a_1 \in A_1, a_2 \in A_2, \dots, a_n \in A_n$.

Mostraremos agora que f é uma função bem definida. Sejam $a = b \in A$, então,

$$a = a_1a_2 \dots a_n, \text{tais que } a_1 \in A_1, a_2 \in A_2, \dots, a_n \in A_n$$

$$b = b_1b_2 \dots b_n, \text{tais que } b_1 \in A_1, b_2 \in A_2, \dots, b_n \in A_n.$$

Ora, pela propriedade (4.) do Lema 6.0.3,

$$a_1 = b_1, a_2 = b_2, \dots, a_n = b_n.$$

Assim,

$$f(a) = f(b),$$

como queríamos.

Ademais, mostraremos que f é um homomorfismo, aplicando a propriedade (5.) do Lema 6.0.3.

$$\begin{aligned} f(ab) &= f(a_1 \dots a_n b_1 \dots b_n) \\ &= f(a_1 b_1 \dots a_n b_n) \\ &= (a_1 b_1, \dots, a_n b_n) \\ &= (a_1, \dots, a_n) \times (b_1, \dots, b_n) \\ &= f(a) \times f(b). \end{aligned}$$

Finalmente, mostraremos que f é uma bijeção. Ora, sejam $f(a) = f(b)$ para $a, b \in A$,

$$\begin{aligned} & f(a) = f(b) \\ \Rightarrow & (a_1, \dots, a_n) = (b_1, \dots, b_n) \end{aligned}$$

$$\therefore a_1 = b_1, \dots, a_n = b_n,$$

i.e., $a = b$ (f é injetora).

Para a sobrejetividade, consideremos um elemento $y \in A_1 \times \cdots \times A_n$. Então, pela definição de produto direto,

$$y = (a_1, \dots, a_n),$$

tais que $a_1 \in A_1, a_2 \in A_2, \dots, a_n \in A_n$. Uma vez que, pela propriedade (1.), $A = A_1 A_2 \dots A_n$,

$$y \in f(a),$$

como queríamos.

Finalmente, mostraremos que a função $F : A_1 \times \cdots \times A_n \to H_1 \times \cdots \times H_n$, tal que $F : (a_1, \dots, a_n) \mapsto (f_1(a_1), \dots, f_n(a_n))$, é uma bijeção. Seja f_i a relação de isomorfismo entre A_i e H_i, $f_i : A_i \to H_i$. A função F está bem definida uma vez que, sendo $(a_1, \dots, a_n), (b_1, \dots, b_n) \in A_1 \times \cdots \times A_n$, tais que $(a_1, \dots, a_n) = (b_1, \dots, b_n)$, é verdade que $a_i = b_i, \forall i = 1, \dots, n$. Assim, como f_i é um isomorfismo,

$$f_i(a_i) = f_i(b_i).$$

Portanto, tem-se que

$$F((a_1, \dots, a_n)) = (f_1(a_1), \dots, f_n(a_n)) = (f_1(b_1), \dots, f_n(b_n)) = F((b_1, \dots, b_n)).$$

Mostraremos agora a injetividade de F. Sejam $(a_1, \dots, a_n), (b_1, \dots, b_n) \in A_1 \times \cdots \times A_n$, tais que $F((a_1, \dots, a_n)) = F((b_1, \dots, b_n))$. Então, é verdade que

$$(f_1(a_1), \dots, f_n(a_n)) = (f_1(b_1), \dots, f_n(b_n)).$$

Temos, assim, que $f_i(a_i) = f_i(b_i)$. Ora, como f_i é um isomorfismo, $a_i = b_i$ e, então,

$$(a_1, \ldots, a_n) = (b_1, \ldots, b_n).$$

Resta-nos agora mostrar a sobrejetividade de F. Para isso, consideremos $(h_1, \ldots, h_n) \in H_1 \times \cdots \times H_n$. Ora, como já assumimos que existe f_i tal que $A_i \simeq H_i$, temos que

$$\exists a_i, \text{ tal que } f_i(a_i) = h_i, \text{ para } i = \{1, \ldots, n\}.$$

Assim, podemos escrever que

$$(h_1, \ldots, h_n) = (f_1(a_1), \ldots f_n(a_n)) \in F(A_1 \times \cdots \times A_n).$$

($\Rightarrow$) Suponhamos $\phi : A \to H_1 \times \cdots \times H_n$ um isomorfismo de grupos. Mostraremos que A contém os subgrupos $A_1 \simeq H_1, \ldots, A_n \simeq H_n$ (com as condições citadas no teorema). Sendo $X_i = Y_1 \times Y_2 \times \cdots \times Y_n$, tal que $Y_j = \{e\}$ se $j \neq i$ e $Y_j = H_i$ se $j = i$ com $i = 1, ..., n$, definimos

$$A_i := \phi^{-1}(X_i) \subseteq A.$$

É verdade que X_i é subgrupo de $H_1 \times \cdots \times H_n$ uma vez que sendo $a, b \in X_i$, $a = (x_1, \ldots, x_n)$ e $b = (y_1, \ldots, y_n)$, tais que $x_j = y_j = e$ se $j \neq i$. Então,

$$\begin{aligned}
ab^{-1} &= (x_1, \ldots, x_n)(y_1, \ldots, y_n)^{-1} \\
&= (x_1, \ldots, x_n)(y_1^{-1}, \ldots, y_n^{-1}) \\
&= (x_1 y_1^{-1}, \ldots, x_i y_i^{-1}, \ldots, x_n y_n^{-1}) \\
&= (e, \ldots, e, x_i y_i^{-1}, e, \ldots, e) \\
&\in X_i.
\end{aligned}$$

Ademais, precisamos mostrar que A_i é subgrupo de A. Dados $a, b \in A_i$, tem-se, por ϕ ser um isomorfismo, que $\phi(a), \phi(b) \in X_i$. Ora,

$$\phi(a)\phi(b)^{-1} = \phi(a)\phi(b^{-1}) = \phi(ab^{-1}) \in X_i.$$

Então,

$$ab^{-1} \in \phi^{-1}(X_i) = A_i.$$

Queremos mostrar ainda que $A_i \simeq H_i$. Seja, então, a função

$$\begin{aligned}
\phi_i : X_i &\to H_i \\
(h_1, \ldots, h_n) &\mapsto h_i.
\end{aligned}$$

ϕ_i é um homomorfismo já que, dados $a, b \in X_i$, $a = (x_1, \ldots, x_n)$ e $b = (y_1, \ldots, y_n)$, tais que $x_j = y_j = e$ se $j \neq i$,

$$\begin{aligned}
\phi_i(ab) &= \phi_i((x_1, \ldots, x_n)(y_1, \ldots, y_n)) \\
&= \phi_i((x_1y_1, \ldots, x_iy_i, \ldots, x_ny_n)) \\
&= x_iy_i \\
&= \phi_i(a)\phi_i(b).
\end{aligned}$$

ϕ_i também é sobrejetiva, pois sendo $h_i \in H_i$ e

$$x_i := (h_1, \ldots, h_i, \ldots, h_n) \in X_i,$$

com $h_j = e$, se $j \neq i$, tem-se que

$$h_i = \phi_i(x_i).$$

Além disso, ϕ_i é injetiva uma vez que para $(a_1, \ldots, a_n), (b_1, \ldots, b_n) \in X_i$, tais que

$$\phi_i((a_1, \ldots, a_n)) = \phi_i((b_1, \ldots, b_n)),$$

é verdade que $a_i = b_i$. Então,

$$(a_1, \ldots, a_n) = (b_1, \ldots, b_n),$$

uma vez que $a_j = b_j = e$ se $j \neq i$. Mostrado que ϕ_i é um isomorfismo, então,

$$\phi_i \circ \phi(A_i) = \phi_i(\phi(A_i)) = \phi_i(\phi(\phi^{-1}(X_i))) = \phi_i(X_i) = H_i$$

Portanto, podemos afirmar que

$$A_i \simeq_{\phi_i \circ \phi} H_i,$$

como queríamos.

Quanto à propriedade (1.), seja $a \in A$, como ϕ é uma bijeção, $\phi^{-1}(H_1 \times \cdots \times H_n) = A$. Ora, pela definição de produto direto de grupos,

$$H_1 \times \cdots \times H_n = X_1X_2 \ldots X_n.$$

Assim,

$$\begin{aligned}
\phi^{-1}(X_1X_2 \ldots X_n) &= A \\
\phi^{-1}(X_1)\phi^{-1}(X_2) \ldots \phi^{-1}(X_n) &= A \\
A_1A_2 \ldots A_n &= A,
\end{aligned}$$

como queríamos.
A propriedade (3.) vem de que

$$\begin{aligned}
Y &= A_i \cap (A_1 \dots A_{i-1} A_{i+1} \dots A_n) \\
&= \phi^{-1}(X_i) \cap \phi^{-1}(X_1 \dots X_{i-1} X_{i+1} \dots X_n) \\
&= \phi^{-1}(\{e\} \times \cdots \times \{e\} \times H_i \times \{e\} \times \cdots \times \{e\}) \cap \phi^{-1}(H_1 \times \cdots \times H_{i-1} \times \{e\} \times H_{i+1} \times \cdots \times H_n) \\
&= \{e\}.
\end{aligned}$$

Quanto à propriedade (2.), queremos mostrar que $aA_ia^{-1} \subseteq A_i, \forall i = 1, 2, \dots, n, \forall a \in A$. Ora,

$$\begin{aligned}
\phi(aA_ia^{-1}) &= \phi(a)\phi(A_i)\phi(a^{-1}) \\
&= (h_1, h_2, \dots, h_n)(\{e\} \times \cdots \times \{e\} \times H_i \times \{e\} \times \cdots \times \{e\})(h_1^{-1}, h_2^{-1}, \dots, h_n^{-1}) \\
&= (h_1h_1^{-1}, \dots, h_{i-1}h_{i-1}^{-1}, h_iH_ih_i^{-1}, h_{i+1}h_{i+1}^{-1}, \dots, h_nh_n^{-1}) \\
&= \{e\} \times \cdots \times \{e\} \times H_i \times \{e\} \times \cdots \times \{e\} \\
&= \phi(A_i).
\end{aligned}$$

Como ϕ é bijetora,

$$aA_ia^{-1} = A_i,$$

como queríamos mostrar. $\square$

Capítulo 7

Grupos de Permutações

Antes de propriamente discorrer sobre grupos de permutações, enunciaremos algumas definições e proposições que serão úteis para isso.

Definição 7.0.1. Chama-se de **conjunto subjacente** de um grupo A o conjunto de A sem a estrutura de grupo.

Proposição 7.0.2. Seja C um conjunto. Então, $(Bij(C), \circ)$ é um grupo, onde

$$Bij(C) = \{f : C \to C \mid \text{f é uma bijeção}\}$$

e $\circ$ é a operação de composição de funções.
Esse grupo é designado por $\mathcal{P}(C)$.

Demonstração. A fim de provar que $\mathcal{P}(C)$ é de fato um grupo começamos mostrando que, sendo $f, g \in \mathcal{P}(C)$, então $f \circ g \in \mathcal{P}(C)$, i.e., que a operação é fechada. Como f e g são bijetoras pela definição do conjunto $Bij(C)$, tem-se que

$$f \circ g : C \to C.$$

Sendo $c, d \in C$, se $f \circ g(c) = f \circ g(d)$, então,

$$f(g(c)) = f(g(d)) \Leftrightarrow f^{-1}(f(g(c))) = f^{-1}(f(g(d))) \Leftrightarrow g(c) = g(d) \Leftrightarrow g^{-1}(g(c)) = g^{-1}(g(d)) \Leftrightarrow c = d,$$

ou seja, $f \circ g$ é injetiva. Além disso, seja $c \in C$. Ora, como f é sobrejetora, $\exists x \in C$ tal que $f(x) = c$. E, como g é sobrejetora, $\exists y \in C$ tal que $g(y) = x$. Assim,

$$f(g(y)) = c,$$

isto é, $f \circ g$ é sobrejetora. Logo, $f \circ g$ é bijetora e é elemento de $\mathcal{P}(C)$.

Sejam $f, g, h \in \mathcal{P}(C)$, mostraremos que a operação de composição é associativa. Assim,

$$f \circ (g \circ h)(C) = f \circ (g(h(C))) = f(g(h(C))) = (f \circ g)(h(C)) = (f \circ g) \circ h(C).$$

Por fim, resta mostrar que o grupo admite elemento identidade e inversa. Ora, para $f \in \mathcal{P}(C)$, como f é bijetora, $\exists g \in \mathcal{P}(C)$ tal que $g = f^{-1}$. Assim,

$$f \circ g(C) = Id_{\mathcal{P}(C)},$$

onde

$$Id_{\mathcal{P}(C)} : c \mapsto c.$$

□

Um conjunto de grupos bastante útil no estudo de grupos finitos é dos grupos de permutações. Assim, a proposição 7.0.3 a seguir mostra que qualquer grupo finito é isomorfo a um subgrupo de um grupo de permutações.

Teorema 7.0.3. (Cayley) Seja A um grupo finito, tal que $n = |A|$, e A_0 o conjunto subjacente a A. Então,

$$\begin{aligned} T : A &\to \mathcal{P}(A_0) \quad \simeq S_n \\ a &\mapsto T_a : A_0 \xrightarrow{\sim} A_0 \\ & \qquad\qquad x \ \mapsto ax, \end{aligned}$$

é um homomorfismo injetivo.

Demonstração. Mostraremos inicialmente que T está bem definida. Sejam $a_1, a_2 \in A$ e $a_1 = a_2$, então $T_{a_1}(x_i) = a_1 x_i = a_2 x_i = T_{a_2}(x_i), \forall x_i \in A_0$. Assim, $T_{a_1} = T_{a_2}$.

Agora, mostraremos que T é um homomorfismo. Sejam $a_1, a_2 \in A$, então $T_{a_1 a_2}(x_i) = (a_1 a_2)x_i = a_1(a_2 x_i) = T_{a_1}(T_{a_2}(x_i))$. Assim, $T_{a_1 a_2} = T_{a_1} T_{a_2}$.

Por fim, mostraremos que T é injetivo. Tem-se que se $a \in ker(T)$, então $T_a = Id_{A_0}$. Ora, se $T_a = Id_{A_0}$, então $ax = x, \forall x \in A_0$. Assim, $a = e$, e portanto $ker(T) = \{e\}$, o que implica que T é injetivo, pelas propriedades do homomorfismo. □

Definição 7.0.4. Uma permutação $\alpha \in S_n$ é um *r-ciclo* se existem $a_1, a_2, \ldots, a_r \in \{1, \ldots, n\}$ distintos tais que $\alpha(a_1) = a_2$, $\alpha(a_2) = a_3$, $\ldots$, $\alpha(a_{r-1}) = a_r$, $\alpha(a_r) = a_1$, e os demais elementos de $\{1, \ldots, n\}$ são mapeados a eles mesmos. Esse *r-ciclo* é denotado por $(a_1 \ldots a_r)$, onde r é o *comprimento* do ciclo.

É interessante apontar que 2-ciclos são chamados de *transposições*.

Alguns **exemplos** interessantes de r-ciclos em S_5 são listados a seguir.

Exemplo 1) $\binom{12345}{23451}$ é um 5-ciclo com uma possível representação (12345).

Exemplo 2) $\binom{12345}{32145}$ é uma transposição com possível representação (13).

Exemplo 3) O único 1-ciclo é a identidade $\binom{12345}{12345}$ com possível representação (1).

Definição 7.0.5. Sejam $\alpha, \beta \in S_n$ um r$_1$-ciclo e um r$_2$-ciclo. α e β são ditas disjuntas se $\forall a \in \{1, 2, \ldots, n\}$, tem-se **ou** $\alpha(a) = a$ **ou** $\beta(a) = a$.

Proposição 7.0.6. Dados $\alpha, \beta \in S_n$ dois ciclos disjuntos, então $\alpha\beta = \beta\alpha$.

Demonstração. Ora, por definição, $\forall a \in \{1, 2, \ldots, n\}$, $\alpha(a) = a$ **ou** $\beta(a) = a$. Assim, para o caso em que $\alpha(a) = a$,

$$\alpha(\beta(a)) = \beta(a) = \beta(\alpha(a)).$$

Já para o caso em que $\beta(a) = a$,

$$\alpha(\beta(a)) = \alpha(a) = \beta(\alpha(a)).$$

Portanto, $\alpha\beta = \beta\alpha$. □

Proposição 7.0.7. Seja $\alpha \in S_n$ um r-ciclo. Mostre que a ordem de α é igual a r.

Demonstração. Para mostrarmos que a ordem de α é igual a r, mostraremos que $\alpha^r = Id = (1)$ e que r é o menor inteiro positivo com essa propriedade.

Primeiro, vamos mostrar que $\alpha^r = Id$. Isso significa que $\alpha^r(a_i) = a_i$ para todo $i = 1, \ldots, r$. Mas isso é verdade por definição de r-ciclo, pois $\alpha(a_i) = a_{i+1}$ para $i = 1, \ldots, r-1$ e $\alpha(a_r) = a_1$. Então, aplicando α repetidamente r vezes, temos que $\alpha^r(a_i) = a_{i+r} = a_i$, onde usamos a aritmética modular para simplificar o índice, tal que $\alpha(a_i) = a_{i+1}$, $\alpha(a_{i+1}) = a_{i+2}$, $\ldots$, $\alpha(a_{i+(r-i-1)}) = a_r$ e $\alpha(a_r) = a_1$, $\ldots$, $\alpha(a_{i-1}) = a_i$. Como existem i elementos entre a_{i-1} e a_r e existem $r - i$ elementos entre $a_{i+(r-i-1)}$ e a_i, então $\alpha^r(a_i) = a_i$.

Para mostrar que r é o menor inteiro positivo que satisfaz essa propriedade, suponhamos que exista um inteiro positivo $s < r$, tal que $\alpha^s = Id$. Ora, isso contradiz a definição de r-ciclo, pois teríamos que $\alpha^s(a_i) = a_{i+s} = a_i$, o que significa que $s = 0$ ou $s = r$. Mas s não pode ser zero, pois é um inteiro positivo. E $s \neq r$, pois assumimos que $s < r$. Portanto, r é o menor inteiro positivo com essa propriedade. □

Proposição 7.0.8. Sejam $\alpha_1, \ldots, \alpha_t \in S_n$ ciclos disjuntos de comprimentos $r_1, \ldots, r_t$, respectivamente, Mostre que o produto $\alpha_t \ldots \alpha_1$ tem ordem igual a $MMC\{r_1, \ldots, r_t\}$.

Demonstração. Mostraremos primeiramente, utilizando a proposição 7.0.6, que, sendo $\alpha, \beta \in S_n$ dois ciclos disjuntos, então $(\alpha\beta)^k = \alpha^k\beta^k$, $\forall k \in \mathbb{N}$. Ora,

$$(\alpha\beta)^k = \underbrace{\alpha\beta}_{k \text{ vezes}} = \underbrace{\alpha}_{k \text{ vezes}} \underbrace{\beta}_{k \text{ vezes}} = \alpha^k\beta^k.$$

Ademais, com a proposição 7.0.7, tem-se que

$$(\alpha_t \dots \alpha_1)^{MMC\{r_1,\dots,r_t\}} = \alpha_t^{MMC\{r_1,\dots,r_t\}} \dots \alpha_1^{MMC\{r_1,\dots,r_t\}} = Id,$$

pois $MMC\{r_1, \dots, r_t\}$ é múltiplo de cada r_i.

Por fim, mostraremos que $MMC\{r_1, \dots, r_t\}$ é o menor inteiro positivo que satisfaz a propriedade, e logo é a ordem do produto. Ora, seja $s < MMC\{r_1, \dots, r_t\}$ um inteiro positivo, tal que $(\alpha_t \dots \alpha_1)^s = Id$. Então, $\alpha_t^s \dots \alpha_1^s = Id$. Isso implica que $a_i^s = Id$, $\forall i = 1, \dots, t$. Todavia, isso contradiz com o fato de que a ordem de cada α_i ser igual a r_i. Logo, $MMC\{r_1, \dots, r_t\}$ é igual a ordem do produto $\alpha_t \dots \alpha_1$. □

Proposição 7.0.9. Seja $\alpha \in S_n$ e $\alpha \neq Id$. Então, α é igual a um produto de ciclos disjuntos de comprimentos ≥ 2, tal que a fatoração é única a menos da ordem dos fatores.

Demonstração. Primeiramente, mostraremos a existência de um produto de ciclos disjuntos de comprimento ≥ 2 que seja igual a α. Seja i um elemento em $\{1, 2, \dots, n\}$ tal que $\alpha(i) \neq i$. Considere $r \in \mathbb{N}$, tal que r seja o menor valor que satisfaça $\alpha^r(i) = i$, i.e., criamos um ciclo σ_1. Agora, considere o conjunto $\{1, 2, \dots, n\} \setminus \{i, \alpha(i), \alpha^2(i), \dots, \alpha^{r-1}(i)\}$. Se este conjunto não estiver vazio, escolha um elemento j nele e construa o ciclo σ_2 da mesma forma. Continue este processo até que todos os elementos de $\{1, 2, \dots, n\}$ tenham sido incluídos em um ciclo. Note que cada ciclo construído terá comprimento ≥ 2, pois $\alpha \neq \mathrm{Id}$. Afirmamos que $\alpha = \sigma_1\sigma_2 \dots \sigma_k$, onde σ_i são os ciclos construídos. Isso ocorre porque, para qualquer elemento x em $\{1, 2, \dots, n\}$, $\alpha(x)$ é dado pela ação do ciclo que contém x. Como os ciclos são disjuntos, a ordem em que eles são multiplicados não importa, pela proposição 7.0.6.

Quanto à unicidade da fatoração, suponhamos

$$\alpha = \sigma_1\sigma_2 \dots \sigma_k = \tau_1\tau_2 \dots \tau_l,$$

onde σ_i e τ_j são ciclos disjuntos de comprimento ≥ 2. Seja x um elemento em $\{1, 2, \dots, n\}$. Sem perda de generalidade, suponha que x esteja no ciclo σ_1. Como $\alpha(x) = \sigma_1(x)$, então $\tau_j(x) = \sigma_1(x)$ para algum j. Como τ_j é um ciclo, $\tau_j^s(x) = \sigma_1^s(x)$ para todo $s \in \mathbb{N}$. Em particular, se r é o comprimento do ciclo σ_1, então $\tau_j^r(x) = \sigma_1^r(x) = i$. Portanto, o ciclo τ_j contém todos os elementos do ciclo σ_1. Como σ_1 e τ_j são disjuntos, eles devem ser iguais. Analogamente, podemos mostrar que cada ciclo σ_i é igual a algum ciclo τ_j.

Portanto, $k = l$ e, a menos de reordenação, $\sigma_i = \tau_i$ para todo i.

Concluímos que a fatoração de α em ciclos disjuntos é única a menos da ordem dos fatores. $\square$

Proposição 7.0.10. Considere as seguintes proposições:

a) Todo elemento de S_n pode ser escrito como um produto de transposições.

b) $S_n = \langle (1\ 2), (1\ 3), \ldots, (1\ n) \rangle$.

c) $S_n = \langle (1\ 2), (2\ 3), (3\ 4), \ldots, (n-1\ n) \rangle$.

Demonstração. Para o item (a), note que o produto de transposições $(a\ b)(a\ b) = ()$ é uma maneira de escrever o elemento identidade de S_n, $\forall n \geq 2$. Agora, para $\alpha \in S_n \setminus Id$, considere a proposição 7.0.9. Assim,

$$\alpha = \sigma_1 \sigma_2 \ldots \sigma_k,$$

onde $\sigma_1, \sigma_2, \ldots, \sigma_k$ são ciclos disjuntos de ordem maior ou igual a 2. Ora, note que, para $1 \leq i \leq k$, tem-se que, para j-ciclos sem perda de generalidade,

$$\begin{aligned} \sigma_i &= (x_{i1} x_{i2} \ldots x_{ij}) \\ &= (x_{i1} x_{ij})(x_{i1} x_{i(j-1)}) \ldots (x_{i1} x_{i2}). \end{aligned}$$

Assim, α pode ser reescrita como um produto de transposições,

$$\alpha = ((x_{11} x_{1j})(x_{11} x_{1(j-1)}) \ldots (x_{11} x_{12})) \ldots ((x_{k1} x_{kj})(x_{k1} x_{k(j-1)}) \ldots (x_{k1} x_{k2})),$$

como queríamos mostrar.

É claro que $\langle (1\ 2), (1\ 3), \ldots, (1\ n) \rangle \leq S_n$. Uma vez provado o item (a), é suficiente para o item (b) mostrar que toda transposição $(i\ j)$ pode ser escrito como um produto dos elementos do subgrupo gerado $\langle (1\ 2), (1\ 3), \ldots, (1\ n) \rangle$. Ora,

$$(i\ j) = (1\ i)(1\ j)(1\ i),$$

se $i \neq j$, como queríamos.

Para o item (c), é claro que $\langle (1\ 2), (2\ 3), (3\ 4), \ldots, (n-1\ n) \rangle \leq S_n$, e é suficiente mostrar que toda transposição $(1\ i) \in \langle (1\ 2), (2\ 3), (3\ 4), \ldots, (n-1\ n) \rangle$. Considerando a prova do item (b), tem-se que para $i = 2$,

$$(1\ 2) \in \langle (1\ 2), (2\ 3), (3\ 4), \ldots, (n-1\ n) \rangle.$$

Por indução em i, $\forall i \geq 2$, e adotando-se a hipótese de que

$$(1\ i) \in \langle (1\ 2), (2\ 3), (3\ 4), \ldots, (n-1\ n) \rangle$$

,

$$(1\ i)(i\ i+1)(1\ i) = (1\ i+1).$$

Assim, $\forall i \geq 2$,

$$(1\ i) \in \langle (1\ 2), (2\ 3), (3\ 4), \ldots, (n-1\ n) \rangle,$$

como queríamos mostrar. □

Proposição 7.0.11. Seja $\alpha \in S_n$, tal que $\alpha = \sigma_1\sigma_2 \ldots \sigma_k$ é uma fatoração qualquer como produto de transposições. Então a paridade de k é única, isto é, ou k é sempre par para qualquer fatoração de α em transposições, ou k é sempre ímpar para qualquer fatoração de α em transposições. Em outras palavras, a paridade do número de transposições numa fatoração de uma permutação $\alpha \in S_n$ é invariante. Essa paridade define a paridade (ou sinal) da permutação.

Demonstração. Vide demonstração da proposição V.10.5 do livro Elementos de Álgebra [1]. □

Definição 7.0.12. Seja α um elemento de S_n. α é dito permutação par se α é escrito como um produto de uma quantidade par de transposições.

Proposição 7.0.13. Seja $A_n = \{\alpha \in S_n \mid \alpha \text{ é permutação par}\}$. É verdade que $A_n \leq S_n$ de índice 2. (A_n é chamado de grupo alternado ou grupo de permutações pares)

Demonstração. Considere a função $\psi : S_n \to \{1, -1\}$, onde $\{1, -1\} = (\mathbb{Z}/2\mathbb{Z})^*$ (único grupo multiplicativo de dois elementos), tal que $\psi(\alpha) = 1$ se α é par e $\psi(\alpha) = -1$ se α é ímpar. Note que ψ é bem definida pela proposição 7.0.9. Mostraremos agora que ψ é um homomorfismo. Considere $\alpha, \beta \in S_n$. Para o primeiro caso e sem perda de generalidade, considere também que α seja par e β seja ímpar, então

$$\psi(\alpha\beta) = -1 = \psi(\alpha)\psi(\beta).$$

Considere agora o caso em que ambos α e β são pares (cuja demonstração é análoga ao caso em que ambos são ímpares),

$$\psi(\alpha\beta) = +1 = \psi(\alpha)\psi(\beta).$$

Isso mostra que ψ é um homomorfismo. Ora, como S_n possui tantos elementos ímpares quantos pares, tem-se que ψ é um homomorfismo sobrejetivo. □

Proposição 7.0.14. Seja H um subgrupo de S_n, então ou $H < A_n$ ou o índice $(H : H \cap A_n) = 2$.

Demonstração. Consideremos o homomorfismo

$$\psi : S_n \to \{1, -1\},$$

definido por

$$\psi(\alpha) = \begin{cases} 1, & \text{se } \alpha \text{ é par,} \\ -1, & \text{se } \alpha \text{ é ímpar.} \end{cases}$$

Restrinjimos ψ a H e consideramos a função

$$\psi|_H : H \to \{1, -1\}.$$

Como ψ é um homomorfismo, sua restrição $\psi|_H$ também o é. Note que o núcleo de $\psi|_H$ é dado por

$$\ker(\psi|_H) = \{\alpha \in H \mid \psi(\alpha) = 1\},$$

isto é,

$$\ker(\psi|_H) = H \cap A_n.$$

Pelo Primeiro Teorema de Isomorfismo, temos

$$H/(H \cap A_n) \simeq \operatorname{im}(\psi|_H).$$

Como $\operatorname{im}(\psi|_H)$ é um subgrupo de $\{1, -1\}$, e este possui apenas dois subgrupos (o trivial $\{1\}$ e o próprio $\{1, -1\}$), temos duas possibilidades:

1. Se $\operatorname{im}(\psi|_H) = \{1\}$, então $\psi(\alpha) = 1$ para todo $\alpha \in H$; ou seja, todos os elementos de H são pares, isto é, $H \leq A_n$.

2. Se $\operatorname{im}(\psi|_H) = \{1, -1\}$, então $H/(H \cap A_n)$ é isomorfo a $\{1, -1\}$ e, portanto, tem exatamente 2 elementos. Assim,

$$[H : H \cap A_n] = 2.$$

Logo, ou H está contido em A_n ou $[H : H \cap A_n] = 2$, como queríamos demonstrar. □

Definição 7.0.15. Considere $n \geq 2$. Se $\rho \in S_n$ e se $\rho = (a_{11} \dots a_{1r_1}) \dots (a_{t1} \dots a_{tr_t})$ é sua decomposição em ciclos disjuntos com $r_1 \leq r_2 \leq \cdots \leq r_t$, então

$$\{r_1, \dots, r_t\}$$

é chamado de *tipo de decomposição* de ρ.

Lema 7.0.16. Considere $n \geq 2$. Para uma permutação $\rho \in S_n$, tal que $\rho = (a_{11} \dots a_{1r_1}) \dots (a_{t1} \dots a_{tr_t})$ a sua decomposição em ciclos disjuntos, tem-se as seguintes afirmações:

a) Se $\sigma \in S_n$, então a permutação par $\sigma\rho\sigma^{-1}$ tem a decomposição em ciclos disjuntos
$$\sigma\rho\sigma^{-1} = (\sigma(a_{11}) \dots \sigma(a_{1r_1})) \dots (\sigma(a_{t1}) \dots \sigma(a_{tr_t})).$$

b) Reciprocamente, se $\rho, \rho' \in S_n$ são permutações com o mesmo tipo de decomposição, então existe $\sigma \in S_n$ tal que $\rho' = \sigma\rho\sigma^{-1}$.

c) Se as permutações $\rho, \rho' \in S_n$ têm o mesmo tipo de decomposição e se as permutações ρ e ρ' deixam pelo menos duas letras fixas, então existe $\mu \in A_n$ tal que $\rho' = \mu\rho\mu'$.

Demonstração. **(a)** Seja $\sigma \in S_n$ e considere um dos ciclos de ρ, digamos,

$$\gamma = (a_{11}\, a_{12}\, \dots\, a_{1r_1}).$$

Seja $x = \sigma(a_{11})$. Então, temos:

$$\sigma\rho\sigma^{-1}(x) = \sigma\Big(\rho\big(\sigma^{-1}(x)\big)\Big) = \sigma\Big(\rho(a_{11})\Big) = \sigma(a_{12}).$$

De forma similar, para $j = 1, \dots, r_1$, definindo $x_j = \sigma(a_{1j})$, obtemos

$$\sigma\rho\sigma^{-1}(x_j) = \sigma\Big(\rho(a_{1j})\Big) = \sigma(a_{1,j+1}),$$

com a convenção de que $a_{1,r_1+1} = a_{11}$. Assim, a ação de $\sigma\rho\sigma^{-1}$ sobre os elementos $\sigma(a_{11}), \sigma(a_{12}), \dots, \sigma(a_{1r_1})$ corresponde ao ciclo

$$\begin{aligned}(\sigma(a_{12})\, \sigma(a_{13})\, \dots\, \sigma(a_{1r_1+1})) &= (\sigma(a_{1r_1+1})\, \sigma(a_{12})\, \dots\, \sigma(a_{1r_1})) \\ &= (\sigma(a_{11})\, \sigma(a_{12})\, \dots\, \sigma(a_{1r_1})).\end{aligned}$$

Como os ciclos da decomposição de ρ são disjuntos, o mesmo argumento vale para cada um deles e, portanto,

$$\sigma\rho\sigma^{-1} = \big(\sigma(a_{11})\, \sigma(a_{12})\, \dots\, \sigma(a_{1r_1})\big) \cdots \big(\sigma(a_{t1})\, \sigma(a_{t2})\, \dots\, \sigma(a_{tr_t})\big).$$

(b) Suponha que as decomposições em ciclos disjuntos de ρ e ρ' sejam

$$\rho = (a_{11}\, a_{12}\, \dots\, a_{1r_1})\, (a_{21}\, a_{22}\, \dots\, a_{2r_2}) \cdots (a_{t1}\, a_{t2}\, \dots\, a_{tr_t})$$

e

$$\rho' = (b_{11}\, b_{12}\, \ldots\, b_{1r_1})\,(b_{21}\, b_{22}\, \ldots\, b_{2r_2})\,\cdots\,(b_{t1}\, b_{t2}\, \ldots\, b_{tr_t}).$$

Como os ciclos correspondentes possuem o mesmo comprimento, podemos definir uma bijeção $\sigma : \{1, 2, \ldots, n\} \to \{1, 2, \ldots, n\}$ da seguinte maneira:

$$\sigma(a_{ij}) = b_{ij}, \quad \text{para } i = 1, \ldots, t \text{ e } j = 1, \ldots, r_i,$$

e, se existirem pontos fixos (isto é, elementos que não aparecem em nenhuma das notações dos ciclos), definimos σ de modo que eles se mantenham fixos. Assim, $\sigma \in S_n$.

Pela parte (a), temos

$$\sigma\,\rho\,\sigma^{-1} = \big(\sigma(a_{11})\,\sigma(a_{12})\,\ldots\,\sigma(a_{1r_1})\big)\cdots\big(\sigma(a_{t1})\,\sigma(a_{t2})\,\ldots\,\sigma(a_{tr_t})\big).$$

Pela definição de σ, isto é

$$\sigma\,\rho\,\sigma^{-1} = (b_{11}\, b_{12}\, \ldots\, b_{1r_1})\,(b_{21}\, b_{22}\, \ldots\, b_{2r_2})\,\cdots\,(b_{t1}\, b_{t2}\, \ldots\, b_{tr_t}) = \rho',$$

o que prova o item (b).

(c) Pela parte (b), existe $\sigma \in S_n$ tal que

$$\rho' = \sigma\,\rho\,\sigma^{-1}.$$

Se σ for par (isto é, $\sigma \in A_n$), basta tomar $\mu = \sigma$.

Caso contrário, suponha que σ seja ímpar. Como tanto ρ quanto ρ' deixam pelo menos duas letras fixas, seja $i, j \in \{1, 2, \ldots, n\}$ tais que

$$\rho(i) = i, \quad \rho(j) = j, \quad \rho'(i) = i, \quad \rho'(j) = j.$$

Considere a transposição $\tau = (i\, j)$. Pela definição de transposição, τ é ímpar e, como i e j são pontos fixos de ρ e de ρ', temos que τ comuta com ambas as permutações. Definindo

$$\mu = \tau\,\sigma,$$

observamos que $\mu \in A_n$, pois o produto de duas permutações ímpares é par. De fato,

$$\mu\,\rho\,\mu^{-1} = \tau\,\sigma\,\rho\,\sigma^{-1}\,\tau^{-1}.$$

Como $\tau^{-1} = \tau$ e τ comuta com ρ' (já que ρ' fixa i e j), obtemos

$$\mu\,\rho\,\mu^{-1} = \tau\,\rho'\,\tau = \rho'.$$

Portanto, existe $\mu \in A_n$ tal que $\rho' = \mu\,\rho\,\mu^{-1}$, concluindo o item (c). $\square$

Proposição 7.0.17. Para $n \geq 3$:

a) Todo elemento de A_n é um produto de 3-ciclos.

b) Sejam $a, b \in \{1, 2, \ldots, n\}$, com $a \neq b$, então

$$A_n = \langle \{abl \mid l = 1, 2, \ldots, n; l \neq a, b\} \rangle.$$

Demonstração. **(a)** Seja $\alpha \in A_n$. Pela Proposição 7.0.11, a paridade do número de transposições numa fatoração de α é invariante; portanto, por ser par, α pode ser escrita como um produto de um número par de transposições:

$$\alpha = \tau_1 \tau_2 \cdots \tau_{2k}, \quad \tau_i \text{ transposições.}$$

Agrupando as transposições em pares, temos:

$$\alpha = (\tau_1 \tau_2)(\tau_3 \tau_4) \cdots (\tau_{2k-1} \tau_{2k}).$$

Mostraremos que cada produto $\tau_{2i-1}\tau_{2i}$ pode ser escrito como produto de 3-ciclos.

Caso 1: Se as duas transposições compartilham um elemento, isto é, se

$$\tau_{2i-1} = (a\,b) \quad \text{e} \quad \tau_{2i} = (b\,c),$$

com a, b, c distintos, e sem perda de generalidade, então:

$$(a\,b)(b\,c) = (a\,b\,c),$$

ou seja, o produto é um 3-ciclo.

Caso 2: Se as transposições são disjuntas, isto é, se

$$\tau_{2i-1} = (a\,b) \quad \text{e} \quad \tau_{2i} = (c\,d),$$

com a, b, c, d todos distintos, então pode-se verificar que:

$$(a\,b)(c\,d) = (a\,b)(a\,c)(a\,c)(c\,d) = (a\,c\,b)(a\,c\,d).$$

Ou seja, o produto de duas transposições disjuntas pode ser escrito como produto de dois 3-ciclos.

Em ambos os casos, cada par de transposições é expresso como produto de 3-ciclos. Assim, α, que é o produto de um número par de transposições, pode ser reagrupada em produtos de 3-ciclos. Concluímos que todo elemento de A_n pode ser escrito como produto de 3-ciclos.

(b) Seja fixos $a, b \in \{1, 2, \ldots, n\}$ com $a \neq b$. Pela parte (a), sabemos que A_n é gerado por 3-ciclos. Mostraremos que, a partir dos 3-ciclos da forma

$$(a\,b\,l), \quad l \in \{1, 2, \ldots, n\} \text{ e } l \neq a, b,$$

é possível obter qualquer 3-ciclo de S_n (e, portanto, de A_n).

Seja $(x\,y\,z)$ um 3-ciclo arbitrário. Pela Proposição 7.0.16 (parte (b)), como todos os 3-ciclos possuem o mesmo tipo de decomposição, existe $\sigma \in S_n$ tal que

$$(x\,y\,z) = \sigma\,(a\,b\,l)\,\sigma^{-1},$$

para algum $l \neq a, b$.

Contudo, para garantir que o conjugador pertença a A_n, observe que, se σ não for par, como $n \geq 3$ existem pelo menos três letras e, portanto, podemos compor σ com uma transposição que fixe a e b (por exemplo, uma transposição $\tau = (l_1\,l_2)$ com $l_1, l_2 \notin \{a, b\}$) de modo que $\mu = \tau\sigma \in A_n$. Note que, como a e b estão fixos por essa transposição, temos:

$$\mu\,(a\,b\,l)\,\mu^{-1} = \tau\,\sigma\,(a\,b\,l)\,\sigma^{-1}\,\tau^{-1} = \tau\left(\sigma\,(a\,b\,l)\,\sigma^{-1}\right)\tau^{-1} = \sigma\,(a\,b\,l)\,\sigma^{-1},$$

pois τ comuta com o 3-ciclo $\sigma\,(a\,b\,l)\,\sigma^{-1}$ (já que os pontos a e b permanecem fixos).

Portanto, qualquer 3-ciclo é conjugado (por um conjugador par) a um 3-ciclo da forma $(a\,b\,l)$. Como A_n é gerado pelos 3-ciclos, conclui-se que

$$A_n = \langle\, \{(a\,b\,l) \mid l \in \{1, 2, \ldots, n\},\, l \neq a, b\}\,\rangle\,.$$

□

Definição 7.0.18. Um grupo A é *simples* se A e $\{e\}$ são seus únicos subgrupos normais.

Teorema 7.0.19. Seja $n = 3$ ou $n \geq 5$. Então A_n é um grupo simples.

Demonstração. Seja N um subgrupo normal não trivial de A_n. Nosso objetivo é mostrar que $N = A_n$.

Caso 1: $n = 3$**.** Observa-se que A_3 possui exatamente 3 elementos, ou seja, $A_3 \simeq \mathbb{Z}/3\mathbb{Z}$ é um grupo cíclico de ordem primo. Assim, os únicos subgrupos (e, em particular, os únicos subgrupos normais) de A_3 são $\{e\}$ e A_3. Portanto, A_3 é simples.

Caso 2: $n \geq 5$**.** Seja $1 \neq \tau \in N$. Pela Proposição 7.0.17, todo elemento de A_n pode ser escrito como um produto de 3-ciclos. Existem duas possibilidades:

(a) Se τ é um 3-ciclo, então temos um 3-ciclo não trivial em N.

(b) Se τ não é um 3-ciclo, considere sua decomposição em ciclos disjuntos. Em algum dos fatores haverá um ciclo de comprimento diferente de 1 e, utilizando as técnicas já demonstradas (por exemplo, o fato de que o produto de duas transposições disjuntas pode ser escrito como o produto de dois 3-ciclos, como na igualdade

$$(a\,b)(c\,d) = (a\,c\,b)(a\,c\,d),$$

que foi verificada anteriormente), pode-se encontrar, por conjugação, um 3-ciclo que esteja contido em N.

Em ambos os casos, concluímos que N contém um 3-ciclo não trivial.

Pela Proposição 7.0.17 (item (b)) e pelo Lema 7.0.16 (parte (c)), todos os 3-ciclos de A_n são conjugados entre si (na medida em que cada 3-ciclo deixa pelo menos duas letras fixas, o que ocorre para $n \geq 5$). Como N é normal, se contém um 3-ciclo ρ, então para todo $\sigma \in A_n$ temos

$$\sigma\,\rho\,\sigma^{-1} \in N.$$

Ou seja, N contém todos os 3-ciclos de A_n.

Por fim, como A_n é gerado pelos 3-ciclos (vide Proposição 7.0.17, item (b)), temos que $N = A_n$.

Assim, os únicos subgrupos normais de A_n são $\{e\}$ e A_n, o que, de acordo com a Definição 7.0.18, significa que A_n é simples. □

Proposição 7.0.20. O conjunto $K \subset S_4$ dado por

$$K = \{id, (12)(34), (13)(24), (14)(23)\}$$

é um grupo abeliano.

Demonstração. Para provar que K é um grupo, basta verificar que K é não-vazio, fechado sob a operação de composição e que todo elemento tem seu inverso em K. É claro que $K \neq \varnothing$.

Em seguida, mostraremos o fechamento explicitamente montando a tabela de multiplicação dos elementos de K. Considere a seguinte tabela:

$\cdot$	id	$(12)(34)$	$(13)(24)$	$(14)(23)$
id	id	$(12)(34)$	$(13)(24)$	$(14)(23)$
$(12)(34)$	$(12)(34)$	id	$(14)(23)$	$(13)(24)$
$(13)(24)$	$(13)(24)$	$(14)(23)$	id	$(12)(34)$
$(14)(23)$	$(14)(23)$	$(13)(24)$	$(12)(34)$	id

- A linha referente ao elemento id mostra que, para qualquer $g \in K$, $id \cdot g = g$.

- Observa-se que as demais linhas possuem como produto elementos que pertencem a K. Por exemplo:
  - $(12)(34) \cdot (13)(24) = (14)(23) \in K$.
  - $(13)(24) \cdot (14)(23) = (12)(34) \in K$.

Como K satisfaz o fechamento sob a operação e a existência de inversos, concluímos que K é um grupo. Além disso, pela tabela de multiplicação é claro pela simetria que K é abeliano, pois a multiplicação é comutativa. Assim, K é um grupo abeliano. $\square$

Definição 7.0.21. O grupo de quatro elementos

$$K = \{id, (12)(34), (13)(24), (14)(23)\}$$

é chamado de *grupo de Klein*.

Proposição 7.0.22. Sejam a, b, c, d quatro elementos distintos de $\{1, 2, 3, 4\}$. Então, para todo $x \in S_4$, temos:

$$x\left((a\,b)(c\,d)\right)x^{-1} = \left(x(a)\,x(b)\right)\left(x(c)\,x(d)\right).$$

Em particular, se x é um 3-ciclo, então $x\left((a\,b)(c\,d)\right)x^{-1}$ é uma dupla transposição.

Demonstração. Observe que a proposição é um caso particular do Lema 7.0.16 (parte (a)). Assim, tem-se

$$x\left((a\,b)(c\,d)\right)x^{-1} = \left(x(a)\,x(b)\right)\left(x(c)\,x(d)\right),$$

que é uma dupla transposição. $\square$

Teorema 7.0.23. Os únicos subgrupos normais do grupo alternado A_4 são $\{id\}$, A_4 e o grupo de Klein (denotado aqui por K).

Demonstração. Sabemos que o grupo simétrico S_4 tem ordem $4! = 24$. Seus elementos podem ser classificados e expressos como produtos de transposições (2-ciclos) da seguinte maneira:

1. **Identidade:**

$$id.$$

2. **Transposições (2-ciclos):** 6 elementos

$$(12),\ (13),\ (14),\ (23),\ (24),\ (34).$$

3. **3-ciclos:** 8 elementos Cada 3-ciclo pode ser escrito como o produto de 2 transposições, pois

$$(a\,b\,c) = (a\,c)(a\,b).$$

Por exemplo, temos:

$$(123) = (13)(12), \quad (132) = (12)(13),$$

e os demais 3-ciclos:

$$(124),\ (142),\ (134),\ (143),\ (234),\ (243).$$

4. **4-ciclos:** 6 elementos Cada 4-ciclo pode ser escrito como produto de 3 transposições. Por exemplo:

$$(1234) = (14)(13)(12).$$

Assim, temos os 4-ciclos:

$$(1234),\ (1243),\ (1324),\ (1342),\ (1423),\ (1432).$$

5. **Duplas transposições (produto de duas transposições disjuntas):** 3 elementos Estes já estão na forma desejada:

$$(12)(34),\ (13)(24),\ (14)(23).$$

A soma dos elementos é:

$$1 + 6 + 8 + 6 + 3 = 24.$$

Cada elemento de S_4 pode ser escrito como produto de transposições. Filtrando os elementos de S_4 que possuem uma expressão em transposições com número par de fatores, obtemos o grupo alternado A_4. Assim, temos:

$$A_4 = \{\, id, (123), (132), (124), (142), (134), (143), (234), (243), (12)(34), (13)(24), (14)(23)\, \}.$$

Para provar que $K \triangleleft A_4$, basta mostrar que, para todo $a \in A_4$ e todo $k \in K$,

$$a\,k\,a^{-1} \in K.$$

Fazemos isso em três casos:

Caso 1: $a = e$.
Temos
$$e\,k\,e^{-1} = k \in K.$$

Caso 2: a é uma dupla transposição, ou seja, $a \in K$.
Como K é abeliano, $ak = ka$ e portanto
$$a\,k\,a^{-1} = k\,a\,a^{-1} = k \in K.$$

Caso 3: a é um 3-ciclo.
Tome
$$a = (p\,q\,r),$$
onde $\{p, q, r\} \subseteq \{1, 2, 3, 4\}$, e
$$k = (i\,j)(\ell\,m) \in K, \quad \{i, j, \ell, m\} = \{1, 2, 3, 4\}.$$
Então, pela proposição 7.0.22,
$$a\,k\,a^{-1} = \big(a(i)\;a(j)\big)\,\big(a(\ell)\;a(m)\big),$$
que é novamente uma dupla de transposições disjuntas, isto é,
$$a\,k\,a^{-1} \in \{(12)(34),\,(13)(24),\,(14)(23)\} = K.$$

Em todos os casos concluímos $a\,k\,a^{-1} \in K$, i.e., K é subgrupo normal de A_4.

Resta mostrar que esses são os únicos subgrupos normais de A_4.

Assim, suponhamos $H \leq A_4$, tal que $H \neq \{id\}$. Se H possui 3-ciclos, digamos (123), então também possui $(123)^{-1} = (132)$, assim como $(324)(132)(324)^{-1} = (124)$, pela definição de subgrupo normal. Ora, pela proposição 7.0.17, $A_4 = \langle (123), (124) \rangle = H$.

Por fim, se H não possui 3-ciclos, então deve possuir alguma dupla transposição, digamos $(12)(34)$. Assim, H contêm também $(234)(12)(34)(234)^{-1} = (13)(24)$ e $(12)(34)(13)(24) = (14)(23)$. Assim, $H = K$, mostrando a unicidade dos três subgrupos. □

Proposição 7.0.24.

a) Seja $n = 3$ ou $n \geq 5$. Então os únicos subgrupos normais de S_n são $\{id\}$, A_n e S_n.

b) Seja $n = 4$. Então os únicos subgrupos normais de S_4 são $\{id\}$, A_4, o grupo de Klein K e S_4.

Proposição 7.0.25.

a) Seja $n = 3$ ou $n \geq 5$. Então os únicos subgrupos normais de S_n são $\{id\}$, A_n e S_n.

b) Seja $n = 4$. Então os únicos subgrupos normais de S_4 são $\{id\}$, A_4, o grupo de Klein K e S_4.

Demonstração. a) É claro que $\{id\}$, A_n e S_n são subgrupos normais de S_n.

Mostraremos agora a unicidade dos mesmos. Seja $H \triangleleft S_n$. Consideremos também o homomorfismo $\psi : H \to (\mathbb{Z}/2\mathbb{Z})^*$, já visto anteriormente com $\psi(\alpha) = 1$ se α é par e $\psi(\alpha) = -1$ se α é ímpar, para $\alpha \in S_n$.

Note que se H não contém um elemento ímpar, então $H \subseteq A_n$. Como H é normal em S_n, então $H \triangleleft A_n$. Assim, pelo teorema 7.0.19, temos que $H = A_n$ ou $H = \{id\}$. Se H contém um elemento ímpar, pela proposição 7.0.14, tem-se que ou o índice $(H : H \cap A_n) = 2$ ou $H < A_n$. Assim, dividiremos em casos: Caso $H < A_n$: Como $H \triangleleft S_n$, temos que H é normal em A_n e, portanto, $H = A_n$ ou $H = \{id\}$, pelo teorema 7.0.19.

Caso $(H : H \cap A_n) = 2$: Como $H \triangleleft S_n$, então $H \cap A_n \triangleleft A_n$. E, pelo teorema 7.0.19, tem-se que $H \cap A_n = \{id\}$ ou $H \cap A_n = A_n$. Assim, $|H| = 2$ ou $H = S_n$, respectivamente.

Caso $|H| = 2$, ou seja, $H \cap A_n = \{id\}$. Assim, $H = \{id, \tau\}$, onde τ é uma transposição. Ora, como H é um subgrupo, $\tau^2 = id \in H$. Além disso, como H é normal, para qualquer $\sigma \in S_n$, $\sigma\tau\sigma^{-1} \in H$. Assim, $\sigma\tau\sigma^{-1} = id$ ou $\sigma\tau\sigma^{-1} = \tau$. No entanto, isso implica que τ comuta com todos os elementos de S_n, o que é uma contradição, pois τ não comuta com todas as permutações. Portanto, H não pode ter ordem 2.

Concluímos que os únicos subgrupos normais de S_n são $\{id\}$, A_n e S_n.

b) Para $n = 4$, sabemos que A_4 possui exatamente três subgrupos normais: $\{id\}$, A_4, e o grupo de Klein K, conforme demonstrado no teorema 7.0.23. Como $A_4 \triangleleft S_4$ e $(S_4 : A_4) = 2$, pelo Teorema da Correspondência, tem-se uma bijeção entre o conjunto dos subgrupos de S_4 que contêm A_4 e o conjunto dos subgrupos de S_4/A_4, logo, qualquer subgrupo normal de S_4 que não esteja contido em A_4 deve ser igual a S_4. Além disso, qualquer subgrupo normal de S_4 que esteja contido em A_4 deve ser um dos subgrupos normais de A_4, ou seja, $\{id\}$, A_4, ou K. Portanto, os únicos subgrupos normais de S_4 são $\{id\}$, A_4, K, e S_4.

□

Capítulo 8

Grupos Solúveis

Definição 8.0.1. Seja G um grupo. Uma série subnormal de G, denotada aqui por $(*)$ é uma sequência de subgrupos

$$\{e\} = G_0 \triangleleft G_1 \triangleleft G_2 \triangleleft \cdots \triangleleft G_n = G,$$

tal que cada G_i é um subgrupo normal de G_{i+1} para $i = 0, 1, \ldots, n-1$.

Observa-se que os *grupos quocientes* da série $(*)$ são os grupos G_{i+1}/G_i, para $i = 0, 1, \ldots, n-1$.

Definição 8.0.2. O *comprimento* de uma série subnormal $(*)$ é o número de fatores quocientes G_{i+1}/G_i que não são triviais.

Definição 8.0.3. Uma série subnormal $(*)$ é um *refinamento* de outra série subnormal $(*)$ se pode ser obtida de $(*)$ pela inserção de subgrupos normais intermediários. O refinamento é dito próprio se insere ao menos um novo subgrupo normal não presente originalmente em $(*)$.

Definição 8.0.4. Uma série subnormal é chamada de *série de composição* de G se não admite refinamento próprio.
Em particular, em uma série de decomposição, cada quociente é um grupo simples, pois caso contrário haveria como inserir um subgrupo normal próprio em G_{i+1}/G_i, refinando a série.

Proposição 8.0.5. Existem grupos que não admitem série de composição.

Demonstração. Por exemplo, o grupo aditivo $(\mathbb{Z}, +)$ não admite série de composição. Suponha, por contradição, que $\mathbb{Z}$ admita uma série de composição

$$0 = G_0 \lhd G_1 \lhd G_2 \lhd \cdots \lhd G_n = \mathbb{Z}.$$

Sabemos que para toda série de composição, cada fator quociente G_{i+1}/G_i é um grupo simples. Vamos analisar o primeiro subgrupo da série, G_1. Qualquer subgrupo não-trivial de $\mathbb{Z}$ é da forma $m\mathbb{Z}$ para algum inteiro $m > 0$. Assim, $G_1 = m\mathbb{Z}$ para algum $m > 0$. Considere agora o quociente $G_1/G_0 = G_1/0 \cong m\mathbb{Z}$. Este quociente é isomorfo a $\mathbb{Z}$, pois $m\mathbb{Z} \cong \mathbb{Z}$ (pelo isomorfismo $f : \mathbb{Z} \to m\mathbb{Z}$ dado por $f(k) = mk$). Porém, $\mathbb{Z}$ não é um grupo simples, pois contém $2\mathbb{Z}$ como subgrupo normal diferente de 0 e diferente do próprio $\mathbb{Z}$. Por definição, um grupo simples não pode conter subgrupos normais além do trivial e do próprio grupo. Isto contradiz a exigência de que todos os fatores quocientes numa série de composição sejam grupos simples. Portanto, $(\mathbb{Z}, +)$ não admite série de composição. □

Proposição 8.0.6. Todo grupo finito $G \neq \{e\}$ admite uma série de composição.

Demonstração. Demonstraremos por indução sobre a ordem $|G|$ do grupo. **Base:** Se $|G| = 1$, então $G = \{e\}$, que é o caso trivial excluído pelo enunciado. Se $|G| = p$ é um número primo, então G é um grupo simples (pois qualquer subgrupo tem ordem 1 ou p pelo Teorema de Lagrange). Neste caso, a série

$$e = G_0 \lhd G_1 = G$$

é uma série de composição, pois $G_1/G_0 \cong G$ é simples.
Hipótese de indução: Suponha que todo grupo finito de ordem menor que $|G|$ admite uma série de composição.
Passo indutivo: Para um grupo G de ordem $|G| > p$, consideramos dois casos:
Caso 1: Se G é simples, então a série $e \lhd G$ é uma série de composição, pois $G/e \cong G$ é simples.
Caso 2: Se G não é simples, então existe um subgrupo normal N de G tal que $e \neq N \neq G$. Como $|N| < |G|$, pela hipótese de indução, N admite uma série de composição:

$$e = N_0 \lhd N_1 \lhd N_2 \lhd \cdots \lhd N_k = N$$

Além disso, o grupo quociente G/N também tem ordem menor que $|G|$, portanto, pela hipótese de indução, G/N admite uma série de composição:

$$N/N = H_0/N \lhd H_1/N \lhd H_2/N \lhd \cdots \lhd H_m/N = G/N$$

onde $H_0 = N \lhd H_1 \lhd H_2 \lhd \cdots \lhd H_m = G$ é uma sequência de subgrupos de G contendo N. Podemos então combinar estas duas séries para formar uma série subnormal para G:

$$e = N_0 \lhd N_1 \lhd N_2 \lhd \cdots \lhd N_k = N = H_0 \lhd H_1 \lhd H_2 \lhd \cdots \lhd H_m = G$$

Esta série é uma série de composição para G, pois:

Os quocientes N_{i+1}/N_i são simples, pois vêm da série de composição de N. Os quocientes H_{j+1}/H_j são isomorfos a $(H_{j+1}/N)/(H_j/N)$, que são simples, pois vêm da série de composição de G/N.

Portanto, todo grupo finito admite uma série de composição. $\square$

Definição 8.0.7. Duas séries subnormais de um grupo G

$$e = G_0 \lhd G_1 \lhd G_2 \lhd \cdots \lhd G_n = G$$

e

$$e = H_0 \lhd H_1 \lhd H_2 \lhd \cdots \lhd H_m = G$$

são ditas *equivalentes* se $n = m$ e existe uma permutação π do conjunto $1, 2, \ldots, n$ tal que $G_i/G_{i-1} \cong H_{\pi(i)}/H_{\pi(i)-1}$ para $i = 1, 2, \ldots, n$. Em outras palavras, duas séries subnormais são equivalentes se elas possuem o mesmo número de fatores quocientes e estes fatores são isomorfos entre si, possivelmente em ordem diferente.

Referências Bibliográficas

[1] Arnaldo GARCIA and Yves LEQUAIN. *Elementos de Álgebra*. IMPA, Rio de Janeiro, 6. ed. edition, 2013. ISBN 978-85-244-0190-9.