UNIVERSIDADE TECNOLÓGICA FEDERAL DO PARANÁ

GUSTAVO FREIRE SCHAFHAUSER

SOBRE A CARACTERIZAÇÃO DE GRUPOS ABELIANOS FINITAMENTE GERADOS

CURITIBA

2022

GUSTAVO FREIRE SCHAFHAUSER

SOBRE A CARACTERIZAÇÃO DE GRUPOS ABELIANOS FINITAMENTE GERADOS

On the characterization of finitely generated abelian groups

Trabalho de Conclusão de Curso de Graduação apresentado como requisito para obtenção do título de Licenciado em Matemática do Curso de Licenciatura em Matemática da Universidade Tecnológica Federal do Paraná.

Orientador: Prof. Dr. Francismar Ferreira Lima

CURITIBA

2022

GUSTAVO FREIRE SCHAFHAUSER

SOBRE A CARACTERIZAÇÃO DE GRUPOS ABELIANOS FINITAMENTE GERADOS

Trabalho de Conclusão de Curso de Graduação apresentado como requisito para obtenção do título de Licenciado em Matemática do Curso de Licenciatura em Matemática da Universidade Tecnológica Federal do Paraná.

Data de aprovação: 30/junho/2022

Francismar Ferreira Lima
Doutorado
Universidade Tecnológica Federal do Paraná

Mari Sano
Doutorado
Universidade Tecnológica Federal do Paraná

Patrícia Massae Kitani
Doutorado
Universidade Tecnológica Federal do Paraná

CURITIBA
2022

RESUMO

Este trabalho consiste num estudo sistemático da Teoria de Grupos, partindo da definição de grupo e construindo a teoria necessária para a demonstração do Teorema Fundamental dos Grupos Abelianos Finitamente Gerados. Além disso, parte desse trabalho se dispõe a estudar temas paralelos ao caminho necessário para alcançar o teorema citado, visando proporcionar ao leitor uma base teórica para o entendimento de tais temas dentro da Teoria de Grupos. No decorrer do texto, são definidos conceitos e demonstrados resultados dentro de temas estruturais da teoria, como por exemplo, grupos e subgrupos, homomorfismos, ações de grupo, p-grupos, teoremas de Sylow, grupos abelianos finitos, grupos abelianos livres de posto finito e grupos abelianos finitamente gerados.

Palavras-chave: grupo abeliano finitamente gerado; grupo abeliano livre de posto finito; grupo abeliano finito; ação de grupo; teorema de sylow.

ABSTRACT

This work consists of a systematic study of Group Theory, starting from the definition of group and building the necessary theory for the proof of the Fundamental Theorem of Finitely Generated Abelian Groups. In addition, part of this work intends to study surrounding themes of the necessary path to reach the cited theorem, aiming to provide the reader with a theoretical basis for the understanding of such themes within Group Theory. Throughout the text, concepts are defined and results are proved within structural themes of the theory, such as groups and subgroups, homomorphisms, G-sets, p-groups, Sylow theorems, finite abelian groups, finite rank free abelian groups and finitely generated abelian groups.

Keywords: finitely generated abelian group; finite rank free abelian group; finite abelian group; g-sets; sylow theorem.

SUMÁRIO

1 INTRODUÇÃO

A Teoria de Grupos é um dos ramos mais estruturais da Álgebra Abstrata, com grande importância de estudo em si mesma e como uma valorosa ferramenta para outros ramos da Álgebra, como o estudo de anéis, módulos, corpos, entre outras estruturas, bem como sua utilidade para outras área, como por exemplo, a Teoria de Números, a Análise Combinatória, a Geometria e a Topologia.

Como área de estudo própria, parte da Teoria de Grupos se propõe a caracterizar certos tipos de grupos, a partir de propriedades que tais grupos possam apresentar, afim de melhorar o entendimento sobre tais grupos e descrevê-los utilizando-se de grupos já conhecidos.

Nesse sentido, o presente trabalho se propõe a fazer um estudo sistemático da Teoria de Grupos, iniciando na definição da estrutura de grupo e construindo o arcabouço teórico necessário para a demonstração do Teorema Fundamental dos Grupos Abelianos Finitamente Gerados, um importante teorema no qual grupos abelianos finitamente gerados são caracterizados como somas diretas de grupos cíclicos infinitos, os quais se assemelham a $\mathbb{Z}$, e grupos cíclicos de ordem finita, os quais se assemelham a $\mathbb{Z}/m\mathbb{Z}$ (o conjunto das classes de congruência da Aritmética dos Restos). Além disso, como objetivo secundário, perpassamos temas da Teoria de Grupos que não obrigatoriamente culminam no teorema citado, mas também são importantes para o estudo das estruturas de grupo.

Na construção desse arcabouço teórico, propusemo-nos a escrever esse trabalho da forma mais autocontida possível, dentro das limitações existentes num Trabalho de Conclusão de Curso, fazendo as demonstrações dos resultados e explorando detalhes que boa parte dos livros-texto deixam ”a cargo do leitor”, reservando-nos a opção de referenciar externamente resultados que fogem do escopo do trabalho.

Para esse estudo foi escolhido como principal referência o livro ”An Introduction to the Theory of Groups” de Joseph J. Rotman (ROTMAN, 1999), o qual abarca todos os temas da Teoria de Grupos necessários para o desenvolvimento desse trabalho e é geralmente utilizado como material introdutório para cursos de pós-graduação. Além disso, como referências auxiliares foram utilizadas as referências (ROTMAN, 2003) e (HUNGERFORD, 1974), ambos também utilizados a nível de pós-graduação, e também o livro (GARCIA; LEQUAIN, 2015), o qual é mais utilizado em cursos de graduação e é escrito em língua portuguesa.

No primeiro capítulo, abordaremos os conceitos mais básicos da Teoria de Grupos, começando na definição de grupos e passando pela construção de conceitos como subgrupos, subgrupos normais, classes laterais, grupos quocientes, homomorfismos de grupos e produtos diretos. Além da construção desses conceitos, provaremos resultados importantes para a construção da teoria, e em menor número, resultados específicos que serão necessários no decorrer do trabalho.

No segundo capítulo, estudaremos temas da teoria que servirão de ferramenta para nosso objetivo principal, além de mostrarmos resultados interessantes e pertinentes dentro dos

temas trabalhados. Iniciaremos estudando Ações de Grupo, as quais servirão como ferramenta para a demonstração de resultados posteriores, tanto no estudo de p-Grupos quando no estudo dos Teoremas de Sylow, ambos temas que permeiam a caracterização de grupos finitos.

No terceiro capítulo, avançaremos em direção ao nosso tema principal, os Grupos Abelianos. No âmbito dos grupos abelianos finitos faremos duas caracterizações para grupos desse tipo, nas decomposições advindas dos teoremas da Decomposição Primária e da Base. Seguindo com o tema, abordaremos grupos abelianos de forma mais geral (não obrigatoriamente finitos), generalizando alguns dos conceitos construídos anteriormente, introduzindo novos conceitos importantes como dos subgrupos de torção e dos grupos abelianos livre, para então culminá-los na caracterização de grupos abelianos finitamente gerados.

Por fim, concluiremos esse trabalho com algumas considerações.

2 CONCEITOS BÁSICOS DA TEORIA DE GRUPOS

Para o desenvolvimento desse trabalho, tomaremos como pré-requisito os conhecimentos acerca de temas como conjuntos, relações entre conjuntos, funções, aritmética e noções básicas de análise combinatória.

2.1 Grupos e subgrupos

Definição 1. Seja G um conjunto não vazio e $* : G \times G \longrightarrow G$ uma operação binária em G. $(G, *)$ é dito grupo se cumprir os seguintes três requisitos:

(i) $\forall\, a,\, b\, e\, c \in G,\, a * (b * c) = (a * b) * c$ (propriedade associativa);

(ii) $\exists\, e \in G;\, \forall\, g \in G,\, e * g = g$ (e é dito elemento neutro de G);

(iii) $\forall\, g \in G,\, \exists\, h \in G; h * g = e$ (h é dito inverso de g);

Caso o grupo cumpra este quarto requisito, será chamado de grupo abeliano:

(iv) $\forall\, g,\, h \in G,\, g * h = h * g$.

Nos casos onde não houver confusão quanto à operação $*$, ocultamos seu símbolo e escrevemos apenas ab ao invés de $a * b$.

Proposição 2. *Seja G um grupo e sejam $g,\, h,\, e \in G$ tais que $eg = g$ e $hg = e$. Então, $ge = g$ e $gh = e$.*

Demonstração. Dado $g \in G$, seja $h \in G$ tal que $hg = e$ e seja $x \in G$ tal que $x(gh) = e$.

Note que:

$$\begin{aligned} ghgh = g((hg)h) = g(eh) = gh \\ \implies x((gh)(gh)) = x(gh) \\ \implies (x(gh))(gh) = x(gh) = e \\ \implies e(gh) = e \\ \implies gh = e. \end{aligned}$$

Agora,

$$g = eg = (gh)g = g(hg) = ge.$$

■

Proposição 3. *Seja G um grupo, o elemento neutro de G é único e, dado $g \in G$, o inverso de g é único.*

Demonstração. Considere $e,\ e' \in G$ tais que $eg = g$ e $e'g = g, \forall\, g \in G$.

$$e = e'e = ee' = e'.$$

Logo, $e = e'$.
Dado $g \in G$, considere $h,\ h' \in G$ tais que $hg = e$ e $h'g = e$.

$$h = he = h(gh') = (hg)h' = eh' = h'.$$

Assim, $h = h'$. ■

Agora que mostramos a unicidade do elemento neutro e do inverso de um elemento dado, faz sentido fixarmos uma notação para eles. Assim, denotamos o elemento neutro de G por e_G ou apenas e (em grupos multiplicativos, também costuma-se denotar o elemento neutro por 1, enquanto em grupos aditivos, costuma-se denotar o elemento neutro por 0). E, dado $g \in G$, denotamos o elemento inverso de g por g^{-1} (essa notação permanece em grupos multiplicativos, enquanto denotamos o inverso de g por $-g$ em grupos aditivos).

Proposição 4. *Seja G um grupo e $g, h \in G$, então:*

(i) $(g^{-1})^{-1} = g$;

(ii) $(gh)^{-1} = h^{-1}g^{-1}$.

Demonstração. Note que,

$$(g^{-1})^{-1}g^{-1} = e$$
$$gg^{-1} = e$$

Pela unicidade do elemento inverso de g^{-1}, temos que $(g^{-1})^{-1} = g$.

Do mesmo modo,

$$(gh)^{-1}(gh) = e$$
$$(h^{-1}g^{-1})(gh) = h^{-1}(g^{-1}g)h = h^{-1}(eh) = h^{-1}h = e.$$

Pela unicidade do elemento inverso de gh, temos que $(gh)^{-1} = h^{-1}g^{-1}$. ■

Definição 5. Sejam G um grupo, $g \in G$ e $n \in \mathbb{Z}$. Definimos g^n recursivamente como:

- $g^0 = e$, se $n = 0$.
- $g^n = g^{n-1}g$, se $n \geq 1$.

- $g^n = (g^{-1})^{|n|}$, se $n < 0$.

Alguns exemplos de grupos são os formados pelos conjuntos numéricos com as operações usuais de soma ou produto, por exemplo:

Exemplo 6. $(\mathbb{Z}, +)$; $(\mathbb{Q}, +)$; $(\mathbb{R}, +)$; $(\mathbb{C}, +)$; $(\mathbb{Q}\backslash\{0\}, \cdot)$; $(\mathbb{R}\backslash\{0\}, \cdot)$; e $(\mathbb{C}\backslash\{0\}, \cdot)$.

Outros exemplos interessantes, formados por estruturas diferentes dos conjuntos numéricos, são:

Exemplo 7. Sendo $\mathbb{K}$ um corpo, o conjunto das matrizes quadradas inversíveis de ordem n com entradas em $\mathbb{K}$, dado por $GL_n(\mathbb{K}) = \{A \in M_{n\times n}(\mathbb{K});\ \det(A) \neq 0_{\mathbb{K}}\}$, quando munido do produto usual de matrizes $\cdot$, forma o grupo $(GL_n(\mathbb{K}), \cdot)$.

Exemplo 8. Dado um polígono de n lados, podemos construir o grupo D_{2n}, chamado de grupo diedral de um polígono regular de n lados, cujos elementos são rotações (de ângulos $\frac{2\pi k}{n}$ com $0 \leq k \leq n-1$) e reflexões desse polígono, e a operação é a composição das rotações e reflexões.

Exemplo 9. Sendo X um conjunto qualquer, considere $S_X = \{f : X \longrightarrow X;\ f \text{ é bijeção}\}$ e $\circ$ a composição usual de funções, teremos que $(S_X, \circ)$ é um grupo. É fácil ver que S_X será um grupo, pois dada uma bijeção, ela sempre admitirá inversa (que também será uma bijeção), além disso, é sabido que a composição de bijeções também é uma bijeção, e por fim, a função identidade, que é uma bijeção, será o elemento neutro desse grupo.

Exemplo 10. Nos casos em que X for finito, ou seja, $X = \{x_1, x_2, \ldots, x_n\}$, podemos deixar de lado o conjunto X e seus elementos para então trabalharmos apenas com o conjunto $I_n = \{1, 2, \ldots, n-1, n\}$, neste caso, denotaremos o grupo $(S_X, \circ)$ apenas por S_n e este será chamado grupo de permutações de n elementos ou grupo de simetria de n elementos. No grupo S_n, os elementos serão chamados permutações e cada elemento $\alpha \in S_n$ será uma função bijetora $\alpha : I_n \longrightarrow I_n$. Uma das formas de denotar os elementos de um grupo de permutações é utilizando uma notação matricial, onde tomamos $\alpha \in S_n$, calculamos $\alpha(1), \alpha(2), \ldots, \alpha(n)$ e, então, representamos α por uma matriz $2 \times n$ em que na primeira linha escrevemos os números $1, 2, \ldots, n$, domínio da função α, enquanto na segunda linha escrevemos suas respectivas imagens $\alpha(1), \alpha(2), \ldots, \alpha(n)$. Assim, teremos que:

$$\alpha = \begin{pmatrix} 1 & 2 & \cdots & n-1 & n \\ \alpha(1) & \alpha(2) & \cdots & \alpha(n-1) & \alpha(n) \end{pmatrix}.$$

Definição 11. Seja G um grupo e $H \subseteq G$ um subconjunto não vazio. H é dito subgrupo de G se H, munido com a operação $*$ de G, for um grupo. Denotamos que H é subgrupo de G escrevendo $H \leq G$ e escrevemos $H \lneq G$ quando quisermos denotar que H é um subgrupo próprio de G.

Um fato interessante é que, se $H \leq G$ e sendo e_G e e_H os elemento neutros de G e H, respectivamente, temos que $e_G = e_H$. Basta ver que $e_G = h^{-1}h = e_H$, para algum $h \in H \subseteq G$.

Além disso, dado $h \in H \subseteq G$, sejam h'_G e h'_H os elementos inversos de h em G e H, respectivamente, temos que $h'_G = h'_H$. Basta ver que:

$$h'_G = h'_G e = h'_G(hh'_H) = (h'_G h)h'_H = eh'_H = h'_H.$$

Alguns exemplos de subgrupos são:

Exemplo 12. Se G é um grupo, então $\{e\} \leq G$ e $G \leq G$.

Exemplo 13. Do Exemplo 6, temos que: $(\mathbb{Z}, +) \leq (\mathbb{Q}, +)$; $(\mathbb{Q}, +) \leq (\mathbb{R}, +)$; $(\mathbb{Z}, +) \leq (\mathbb{R}, +)$; $(\mathbb{Q}\backslash\{0\},\ \cdot) \leq (\mathbb{R}\backslash\{0\},\ \cdot)$.

Exemplo 14. Do Exemplo 7, $SL_n(\mathbb{K}) = \{A \in M_{n\times n}(\mathbb{K});\ \text{det}(A) = 1_{\mathbb{K}}\}$, isto é, o conjunto das matrizes quadradas de ordem n com determinante unitário é um subgrupo de $GL_n(\mathbb{K}) = \{A \in M_{n\times n}(\mathbb{K});\ \text{det}(A) \neq 0\}$.

Exemplo 15. $(n\mathbb{Z},+) \leq (\mathbb{Z},+)$, onde $n \in \mathbb{Z}$ é um número fixo e $n\mathbb{Z} = \{nz;\ z \in \mathbb{Z}\}$. De fato, basta ver que:

Dados $x,\ y \in n\mathbb{Z}$, $x = nz_1$ e $y = nz_2$. Assim $x+y = (nz_1)+(nz_2) = n(z_1+z_2) \in n\mathbb{Z}$, logo $n\mathbb{Z}$ é fechado.

Dados $a,\ b,\ c \in n\mathbb{Z}$, $a = nz_1$, $b = nz_2$ e $c = nz_3$.

Assim $a + (b + c) = nz_1 + (nz_2 + nz_3) = nz_1 + n(z_2 + z_3) = n(z_1 + z_2 + z_3) = n(z_1 + z_2) + nz_3 = (nz_1 + nz_2) + nz_3 = (a + b) + c$, ou seja, vale a associativa em $n\mathbb{Z}$.

$0 = n0 \in n\mathbb{Z}$, ou seja, $n\mathbb{Z}$ tem o elemento neutro.

Dado $x \in n\mathbb{Z}$, $-x = -(nz) = n(-z) \in n\mathbb{Z}$, ou seja, $n\mathbb{Z}$ contém os elementos inversos.

Proposição 16. *Dado G um grupo e $H \subseteq G$, $H \neq \varnothing$.*

$$H \leq G \iff \forall\, g,\ h \in H,\ gh^{-1} \in H.$$

Demonstração. $(\Rightarrow)$ Sendo H um subgrupo de G, temos que H é grupo e assim verifica-se que $\forall\, g,\ h \in H, gh^{-1} \in H$.

$(\Leftarrow)$ H é não vazio, logo $\exists\ g_0 \in H$. Segue que $g_0 g_0^{-1} = e \in H$ (ou seja, H contém o elemento neutro). Dado $g \in H$, $eg^{-1} = g^{-1} \in H$ (portanto, H contém seus elementos inversos). Dados $a,\ b$ e $c \in H \subseteq G$, $a(bc) = (ab)c$ (pois vale a associativa em G e com isso, também valerá em H). Por fim, dados $g,\ h \in H$, já sabemos que $h^{-1} \in H$ e, sendo assim, concluímos que $gh = g(h^{-1})^{-1} \in H$ (ou seja, H é fechado para a operação herdada de G).

Verificados os axiomas da definição de grupo, e sabendo que $H \subseteq G$, temos que $H \leq G$. ■

A proposição anterior é uma ferramenta muito útil para se determinar (e mostrar) quando um subconjunto de um grupo pode ou não ser um subgrupo, pois é equivalente à definição de subgrupo e é apenas um fato a ser verificado, em contraponto com a definição, onde é necessário verificar os três axiomas da definição de grupo.

Uma forma de construir novos subgrupos num grupo já conhecido é fazendo a interseção de subgrupos também já conhecidos.

Proposição 17. *Sejam H e K subgrupos de um grupo G. Então $H \cap K \leq G$. De modo geral, se $\{H_\lambda\}_{\lambda\in\Lambda}$ é uma família de subgrupos de G, onde Λ é um conjunto de índices, então* $\bigcap_{\lambda\in\Lambda} H_\lambda \leq G$

Demonstração. Note que $H \cap K \neq \varnothing$, visto que $e \in H \cap K$.

Dados $g,\ h \in H \cap K$, $g,\ h \in H$ e $g,\ h \in K \implies h^{-1}g \in H$ e $h^{-1}g \in K \implies h^{-1}g \in H \cap K \implies H \cap K \leq G$. A demonstração do caso geral é análoga. ■

Exemplo 18. Do Exemplo 15, temos que $2\mathbb{Z} \leq \mathbb{Z}$ e $3\mathbb{Z} \leq \mathbb{Z}$. Sendo assim, $2\mathbb{Z} \cap 3\mathbb{Z} \leq \mathbb{Z}$. Um fato interessante é que $2\mathbb{Z} \cap 3\mathbb{Z} = 6\mathbb{Z}$, basta notar que:

$2\mathbb{Z} = \{m = 2n \in \mathbb{Z};\ n \in \mathbb{Z}\} = \{m \in \mathbb{Z};\ 2 \mid m\}$ e $3\mathbb{Z} = \{m = 3n \in \mathbb{Z};\ n \in \mathbb{Z}\} = \{m \in \mathbb{Z};\ 3 \mid m\}$, assim $2\mathbb{Z} \cap 3\mathbb{Z} = \{m \in \mathbb{Z};\ 2 \mid m$ e $3 \mid m\} = \{m \in \mathbb{Z};\ 6 \mid m\} = 6\mathbb{Z}$.

Uma outra forma de construir subgrupos dentro de grupos já conhecidos é utilizando o conceito de subgrupo gerado.

Definição 19. Sejam G um grupo e $S \subseteq G$ um subconjunto. O conjunto gerado por S é dado por $\langle S\rangle = \{s_1 s_2 \cdots s_t;\ t \geq 1,\ s_i \in S$ ou $s_i^{-1} \in S,\ 1 \leq i \leq t\} \cup \{e\}$.

$\langle S\rangle$ é um subgrupo de G, pois:

Dados $g,\ h \in \langle S\rangle$, temos que $g = p_1 p_2 \cdots p_{t_1}$ e $h = q_1 q_2 \cdots q_{t_2}$, onde $h^{-1}g = (q_{t_2}^{-1} \cdots q_2^{-1} q_1^{-1})(p_1 p_2 \cdots p_{t_1}) = s_1 s_2 \cdots s_t \in \langle S\rangle$, tomando $t = t_1 + t_2$, $s_i = q_{(t_2+1-i)}^{-1}$, para $1 \leq i \leq t_2$, e $s_i = p_{(i-t_2)}$, para $t_2 + 1 \leq i \leq t_1 + t_2 = t$.

Logo, temos que $\langle S\rangle \leq G$.

Quando S for um conjunto finito, digamos $S = \{x_1,\ x_2,\ \ldots, x_n\}$, denotamos o subgrupo gerado por S apenas por $\langle x_1,\ x_2,\ \ldots,\ x_n\rangle$.

Também denotamos por $d(G)$ a quantidade mínima de geradores de G. Note que, como $\langle G\rangle = G$, temos que $d(G)$ sempre existirá e $d(G) \leq |G|$, sem excluir o caso onde $d(G) = \infty$.

Exemplo 20. Tomando $n = 3$ no Exemplo 10, temos que S_3 terá os seguintes elementos:

$$\sigma_1 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix},\ \sigma_2 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix},\ \sigma_3 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix},$$

$$\sigma_4 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix},\ \sigma_5 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix},\ \sigma_6 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}.$$

Tomando $\alpha = \sigma_5$ e $\beta = \sigma_2$, temos que $\langle \alpha,\ \beta \rangle = S_3$, e podemos representar os elementos de S_3 em função de α e β de acordo as seguintes igualdades:

$$\sigma_1 = \beta^2 = \alpha^3, \qquad \sigma_2 = \beta, \qquad \sigma_3 = \alpha\beta,$$

$$\sigma_4 = \beta\alpha, \qquad \sigma_5 = \alpha, \qquad \sigma_6 = \alpha^2.$$

Proposição 21. *Sejam G um grupo e $S \subseteq G$ um subconjunto de G. Então, o subgrupo $\langle S \rangle$ é igual a interseção de todos os subgrupos $H \leq G$ tais que $S \subseteq H$, isto é:*

$$\langle S \rangle = \bigcap_{S \subseteq H \leq G} H.$$

Demonstração. $(\supseteq)$ Note que $S \subseteq \langle S \rangle \leq G$, logo:

$$\langle S \rangle \supseteq \bigcap_{S \subseteq H \leq G} H.$$

$(\subseteq)$ Já sabemos que $\bigcap_{S \subseteq H \leq G} H \leq G$.

Seja $g \in \langle S \rangle$, então existe $t \geq 1$ e existem $s_1,\ s_2,\ \cdots,\ s_t$ tais que $s_i \in S$ ou $s_i^{-1} \in S$, $1 \leq i \leq t$, e $g = s_1 s_2 \cdots s_t$.

Perceba que $s_i \in \bigcap_{S \subseteq H \leq G} H$, $1 \leq i \leq t$. Como $\bigcap_{S \subseteq H \leq G} H$ é subgrupo de G, será fechado para operações feitas com seus elementos (em particular, operações feitas com os elementos s_i's). Logo $g = s_1 s_2 \cdots s_t \in \bigcap_{S \subseteq H \leq G} H \implies \langle S \rangle \subseteq \bigcap_{S \subseteq H \leq G} H$.

Assim, concluímos que:

$$\langle S \rangle = \bigcap_{S \subseteq H \leq G} H.$$

■

Corolário 22. *Sejam G um grupo e $S \subseteq G$ um subconjunto de G. Então $\langle S \rangle$ é o menor (no sentido de inclusão) subgrupo de G que contém S, isto é, se T é um subgrupo de G tal que $S \subseteq T \leq G$, então $\langle S \rangle \leq T$.*

Demonstração. Segue diretamente da proposição anterior. ■

Proposição 23. *Sejam G um grupo e $S,\ T$ subgrupos de G. Então o conjunto $ST = \{st;\ s \in S \text{ e } t \in T\}$ é subgrupo de G se, e somente se, $ST = TS$.*

Demonstração. $(\Rightarrow)$ Dado $g \in TS$, existem $s \in S$ e $t \in T$ tais que $g = ts$ e segue que $g^{-1} = s^{-1}t^{-1} \in ST$. Como $ST \leq G$ e $g^{-1} \in ST$, temos que $g = (g^{-1})^{-1} \in ST \implies TS \subseteq ST$.

Dado $h \in ST$, temos que $h^{-1} \in ST$ e assim, exitem $s_0 \in S$ e $t_0 \in T$ tais que $h^{-1} = s_0 t_0 \implies h = t_0^{-1} s_0^{-1} \in TS$, logo $ST \subseteq TS \implies ST = TS$.

($\Leftarrow$) Sejam $x,\ y \in ST$, $x = s_1t_1$ e $y = s_2t_2$, onde $s_1,\ s_2 \in S$ e $t_1,\ t_2 \in T$. $xy^{-1} = s_1t_1(s_2t_2)^{-1} = s_1t_1t_2^{-1}s_2^{-1} = s_1t_3s_2^{-1}$, onde $t_3 = t_1t_2^{-1}$. Como $t_3s_2^{-1} \in TS = ST$, existem $s_4 \in S$ e $t_4 \in T$ tais que $t_3s_2^{-1} = s_4t_4 \implies xy^{-1} = s_1t_3s_2^{-1} = s_1s_4t_4 = s_5t_4$, onde $s_5 = s_1s_4 \in S$. Logo $xy^{-1} = s_5t_4 \in ST \implies ST \leq G$. ■

Proposição 24. *Sejam G um grupo e $S,\ T$ subgrupos de G. Então $ST \leq G$ se, e somente se, $ST = \langle S \cup T \rangle$.*

Demonstração. ($\Leftarrow$) Trivial.

($\Rightarrow$) Por um lado, temos que $S \cup T \subseteq ST = \{st;\ s \in S \text{ e } t \in T\} \subseteq \langle S \cup T \rangle$, visto que $\langle S \cup T \rangle = \{x_1x_2 \cdots x_t;\ t \geq 1,\ x_i \in (S \cup T) \text{ ou } x_i^{-1} \in (S \cup T),\ 1 \leq i \leq t\} \cup \{e\}$.

Por outro lado, como $S \cup T \subseteq ST$, pela Proposição 21, temos que $\langle S \cup T \rangle \leq ST$.

Logo $ST = \langle S \cup T \rangle$. ■

Corolário 25. *Sejam G um grupo e $H_1,\ H_2,\ \ldots,\ H_n$ subgrupos de G. Então $H_1H_2...H_n \leq G$ se, e somente se, $H_1H_2...H_n = \langle \bigcup_{i=1}^{n} H_i \rangle$.*

Demonstração. A demonstração é análoga a da proposição anterior. ■

Definição 26. Seja G um grupo. A ordem de G como a cardinalidade do conjunto subjacente de G, e denotamos por $|G|$. Dado um elemento $g \in G$, definimos a ordem de g como $|g| = |\langle g \rangle|$.

Proposição 27. *Sejam G um grupo e $g \in G$. Se $|g| = n$, então $n = min\{m > 0; g^m = e\}$. Além disso, se m é um inteiro positivo tal que $g^m = e$, então $n \mid m$.*

Demonstração. Como $\langle g \rangle = \{g^m;\ m \in \mathbb{Z}\}$, e $|g| = n$, então deverão existir inteiros distintos $p,\ q \in \mathbb{Z}$ tais que $g^p = g^q$. Sem perda de generalidade, suponha $q < p$, então temos que $g^p = g^q \implies g^p(g^q)^{-1} = g^{p-q} = e$, ou seja, $p - q > 0$ é um inteiro tal que $g^{p-q} = e$.

Defina $b = \min\{m > 0;\ g^m = e\}$, para mostrarmos que $b = n$, mostraremos que $e, g, g^2, \ldots, g^{b-1}$, são elementos todos distintos e que $\langle g \rangle = \{e, g, g^2, \ldots, g^{b-1}\}$.

Suponha, por absurdo, que $g^{m_1} = g^{m_2}$ onde $m_1,\ m_2$ são inteiros distintos tais que $0 \leq m_1, m_2 \leq b - 1$. Sem perda de generalidade, suponha $m_2 > m_1$, logo $g^{m_2-m_1} = e$ e $0 \leq m_2 - m_1 \leq b - 1$, um absurdo com a minimalidade de b, logo devemos ter que $e, g, g^2, \ldots, g^{b-1}$, são elementos todos distintos.

É claro que $\{e, g, g^2, \ldots, g^{b-1}\} \subseteq \langle g \rangle$.

Agora, dado $x \in \langle g \rangle$, temos que $x = g^t$ onde $t \in \mathbb{Z}$. Fazendo a divisão euclidiana de t por b, existem $q, r \in \mathbb{Z}$ tais que $t = bq + r$, onde $0 \leq r \leq b - 1$.

Assim, $g^t = g^{bq+r} = (g^b)^q g^r = g^r$, onde $0 \leq r \leq b-1$, logo $g^t \in \{e,g,g^2,\ldots,g^{b-1}\} \implies \langle g \rangle \subseteq \{e, g, g^2, \ldots, g^{b-1}\}$.

Portanto, temos que $\langle g \rangle = \{e, g, g^2, \ldots, g^{b-1}\}$ e segue que $n = \min\{m > 0; g^m = e\}$.

Por fim, se m é um inteiro positivo tal que $g^m = e$, fazendo a divisão euclidiana de m por $n = |g|$, de forma análoga a feita anteriormente, a minimalidade de n garantirá que essa divisão tenha resto nulo, de onde concluiremos que $n \mid m$. ■

Definição 28. Seja G um grupo. Caso $d(G) < \infty$, isto é, a quantidade mínima de geradores para G é um número finito, dizemos que G é um grupo finitamente gerado.

Definição 29. Seja G um grupo, G é dito cíclico se puder ser gerado por um único elemento, isto é, se existir algum elemento $g \in G$ tal que $G = \langle g \rangle$.

Exemplo 30. $\mathbb{Z}$ é um grupo cíclico, pois $\langle 1 \rangle = \mathbb{Z}$.

Proposição 31. *Todo grupo cíclico G é abeliano.*

Demonstração. $G = \langle g \rangle$, para algum $g \in G$.

Dados $x, y \in G$, existem $m, n \in \mathbb{Z}$ tais que $x = g^m$ e $y = g^n$.

Segue que $xy = g^m g^n = g^{m+n} = g^{n+m} = g^n g^m = yx$.

Logo, G é abeliano. ■

Proposição 32. *Sejam G um grupo cíclico e $H \leq G$, então H é cíclico.*

Demonstração. Caso $H = \{e\}$, não há o que mostrar.

Caso $H \neq \{e\}$, seja g um gerador de G, defina $b = \min\{m > 0; g^m \in H\}$.

Dado $h \in H \leq G = \langle g \rangle$, $h = g^t$ para algum $t \in \mathbb{Z}$. Fazendo a divisão euclidiana de t por b, existem $q, r \in \mathbb{Z}$ tais que $t = bq + r$, onde $0 \leq r \leq b - 1$.

Assim, $h = g^t = g^{bq+r} = (g^b)^q g^r$, onde $0 \leq r \leq b - 1$. Tomando $(g^b)^{-q} \in H$ e multiplicando a igualdade pela esquerda, temos que $g^r = (g^b)^{-q}(g^b)^q g^r = (g^b)^{-q} h \in H$. Pela minimalidade de b, devemos ter que $r = 0 \implies h = (g^b)^q \implies h \in \langle g^b \rangle \implies H = \langle g^b \rangle$. ■

Corolário 33. *Para todo inteiro positivo $n \geq 1$, $n\mathbb{Z} = \{nk;\ k \in \mathbb{Z}\}$ é subgrupo de $\mathbb{Z}$, e além disso, todo subgrupo de $\mathbb{Z}$ é da forma $n\mathbb{Z}$.*

Demonstração. Do Exemplo 15, sabemos que $n\mathbb{Z} \leq \mathbb{Z}$.

Seja $H \leq \mathbb{Z}$, pelo proposição anterior, segue que $H = \langle m \rangle = \{mz;\ z \in \mathbb{Z}\} = m\mathbb{Z}$. ■

Definição 34. Seja G um grupo. O centro de G é o conjunto

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

$Z(G)$ é subgrupo pois, $Z(G) \neq \varnothing$, já que $e \in Z(G)$, e para todos $g,\ h \in Z(G)$ e todo $x \in G$.

$$\begin{aligned}(gh^{-1})x &= (h^{-1})gx = h^{-1}(xg) = h^{-1}x(e)g = h^{-1}x(hh^{-1})g \\ &= h^{-1}(xh)h^{-1}g = h^{-1}hxh^{-1}g = x(gh^{-1}) \implies Z(G) \leq G.\end{aligned}$$

Note que, se G é abeliano, então $Z(G) = G$.

Definição 35. Seja G um grupo e $h \in G$. O centralizador de h em G é o conjunto

$$C_G(h) = \{g \in G;\ gh = hg\}.$$

$C_G(h)$ é subgrupo de G pois, $C_G(h) \neq \varnothing$, já que $e \in C_G(h)$, e para todos $x,\ y \in C_G(h)$.

$$(xy^{-1})h = xy^{-1}he = xy^{-1}h(yy^{-1}) = xy^{-1}(hy)y^{-1} = xy^{-1}(yh)y^{-1}$$
$$= x(y^{-1}y)hy^{-1} = x(e)hy^{-1} = (xh)y^{-1} = (hx)y^{-1} = h(xy^{-1}) \implies C_G(h) \leq G.$$

Analogamente, se $H \leq G$, o centralizador de H em G é o subgrupo de G dado por

$$C_G(H) = \{g \in G;\ gh = hg,\ \forall\, h \in H\}.$$

Definição 36. Seja G um grupo e $x,\ y \in G$. A relação de equivalência "y é um conjugado de x em G" é dada por $y \sim x \iff \exists\, g \in G;\ y = gxg^{-1}$. De fato, $\sim$ é uma relação de equivalência pois:

(i) Dado $x \in G$, tome $e \in G$.
$exe^{-1} = x \iff x \sim x,\ \forall\, x \in G.$

(ii) Dados $x,\ y \in G$ tais que $x \sim y$.
$x \sim y \iff x = gyg^{-1} \implies xg = gy$
$\implies g^{-1}xg = y \implies (g^{-1})x((g^{-1})^{-1}) = y$, com $g^{-1} \in G \implies y \sim x.$

(iii) Dados $x,\ y,\ z \in G$ tais que $x \sim y$ e $y \sim z$.
$x \sim y$ e $y \sim z \iff x = gyg^{-1}$ e $y = hzh^{-1}$, com $g,\ h \in G$
$\implies x = g(hzh^{-1})g^{-1} = (gh)z(gh)^{-1}$, com $gh \in G \implies x \sim z.$

A classe de equivalência de um elemento x por essa relação é chamada classe de conjugação de x e é denotada por x^G.

Teorema 37. *Seja G um grupo finito. Então vale a seguinte igualdade:*

$$|G| = |Z(G)| + \sum_{x_i \notin Z(G)} |x_i^G|,$$

onde $x_i \notin x_j^G,\ \forall\, i \neq j$, isto é, cada x_i pertence a uma classe de conjugação diferente. Essa igualdade é chamada equação das classes de conjugação de G.

Demonstração. Como vimos anteriormente, "$y \sim x \iff \exists\, g \in G;\ y = gxg^{-1}$" é uma relação de equivalência. Logo $G = \dot{\bigcup_i} x_i^G$ onde cada x_i pertence à uma classe de conjugação diferente.

Note que, se $x_i \in Z(G) \iff \forall\, g \in G,\ gx_i = x_ig \iff \forall\, g \in G,\ gx_ig^{-1} = x_i \iff x_i^G = \{x_i\}$. Portanto $Z(G) = \dot{\bigcup_{x_i \in Z(G)}} x_i^G$.

Assim, segue que:

$$G = \dot{\bigcup_i} x_i^G = \left(\dot{\bigcup_{x_i \in Z(G)}} x_i^G \right) \dot{\bigcup} \left(\dot{\bigcup_{x_i \notin Z(G)}} x_i^G \right) = Z(G) \dot{\bigcup} \left(\dot{\bigcup_{x_i \notin Z(G)}} x_i^G \right).$$

E, por fim, temos que:

$$|G| = |Z(G)| + \sum_{x_i \notin Z(G)} |x_i^G|.$$

■

2.2 Classes laterais e Grupos Quocientes

No estudo da Aritmética, as classes de congruência módulo m são construídas a partir da relação de equivalência "congruência modulo m", onde dois inteiros a e b se relacionam se a diferença entre eles for um múltiplo de m, na notação usualmente utilizada, "$a \equiv b \mod m \iff m \mid a - b$". Tal construção permite simplificar a estrutura dos inteiros, facilitando problemas de divisibilidade e da aritmética dos restos. Pensando em $\mathbb{Z}$ como grupo, o conjunto dos múltiplos de um inteiro m pode ser visto como o subgrupo $H = m\mathbb{Z} \leq \mathbb{Z}$.

Fazendo a mesma construção para um grupo G qualquer e um subgrupo $H \leq G$, podemos obter resultados que, ao simplificar a estrutura de G, podem facilitar a resolução de certos problemas e ajudar no estudo da Teoria de Grupos, além de ser uma forma de construir novos grupos a partir de grupos e subgrupos já conhecidos.

Dado um grupo G e um subgrupo $H \leq G$, podemos construir uma relação de equivalência em G dada por: $x \underset{E}{\sim} y \iff y^{-1}x \in H$, utilizando a multiplicação à esquerda. De fato, temos que $\underset{E}{\sim}$ é uma relação de equivalência, pois:

Dado um grupo G e um subgrupo $H \leq G$, seja $\underset{E}{\sim}$ uma relação em G dada por: $x \underset{E}{\sim} y \iff y^{-1}x \in H$.

(i) (reflexiva) Como $H \leq G$, $e \in H \iff x^{-1}x \in H \iff x \underset{E}{\sim} x$, $\forall\, x \in G$.

(ii) (simétrica) Sejam $x,\ y \in G$ tais que $x \underset{E}{\sim} y$.

$x \underset{E}{\sim} y \iff y^{-1}x \in H \implies y^{-1}x = h \in H \implies y^{-1}x = h \implies (y^{-1}x)^{-1} = (h)^{-1}$
$\implies x^{-1}y = h^{-1} \implies x^{-1}y = h^{-1} \in H \iff y \underset{E}{\sim} x.$

(iii) (transitiva) Sejam $x,\ y,\ z \in G$ tais que $x \underset{E}{\sim} y$ e $y \underset{E}{\sim} z$.

$x \underset{E}{\sim} y$ e $y \underset{E}{\sim} z \iff y^{-1}x = h_1 \in H$ e $z^{-1}y = h_2 \in H$
$\implies z^{-1}x = (z^{-1}y)(y^{-1}x) = h_2h_1 \in H \implies z^{-1}x \in H \iff x \underset{E}{\sim} z.$

Portanto, $\underset{E}{\sim}$ é uma relação de equivalência em G.

A partir dessa relação de equivalência, podemos construir as classes de equivalência dessa relação. Dado um elemento $g \in G$, sua classe de equivalência será $\overline{g} = \{x \in G; x \underset{E}{\sim} g\}$. Note que $x \underset{E}{\sim} g \iff g^{-1}x = h \in H \iff x = gh$, onde $h \in H$. Devido a isso, podemos reescrever, e denotar a classe de equivalência $\overline{g}$ como $gH = \{gh;\ h \in H\}$, além disso, as classes de equivalência recebem o nome de classes laterais à esquerda e juntas formam o conjunto das classes laterais à esquerda de G por H, que é denotado por G/H.

Analogamente, toda essa construção pode ser feita utilizando a multiplicação à direita, a partir da relação: "$x \underset{D}{\sim} y \iff xy^{-1} \in H$", resultando na construção das classes laterais à direita dadas por $Hg = \{hg;\ h \in H\}$, que juntas formam o conjunto das classes laterais à direita. Também vale notar que a quantidade de classes laterais à esquerda e à direita é a mesma, o que pode ser mostrado pela bijeção $xH \mapsto Hx^{-1}$. No decorrer do texto utilizaremos a construção feita à esquerda e, quando não houver confusão, utilizaremos apenas "classe lateral" para nos referirmos à classe lateral à esquerda.

Além disso, visto que $\underset{E}{\sim}$ é uma relação de equivalência, as classes de equivalência formam uma partição de G e temos que:

(i) $\forall\, x,\ y \in G$, ou $xH = yH$ ou $xH \cap yH = \varnothing$.

(ii) $G = \bigcup\limits_{g \in G} gH$.

(iii) $G = \dot{\bigcup\limits_{t \in T}} tH$, onde T é um conjunto de representantes da partição de G.

Definição 38. Sejam G um grupo e $H \leq G$. A cardinalidade do conjunto das classes laterias G/H recebe o nome de índice de H em G e é denotado por $[G : H]$.

Lema 39. *Todas as classes laterais de H em G têm a mesma cardinalidade, igual à cardinalidade de H.*

Demonstração. Seja $xH = \{xh;\ h \in H\}$ uma classe lateral de H em G. Tome a função $f : H \longrightarrow xH$ dada por $f(h) = xh$.

f é injetora, pois: dados h_1 e $h_2 \in H$ tais que $f(h_1) = f(h_2) \implies xh_1 = xh_2 \implies h_1 = h_2$.

E f é sobrejetora, pois: dado $y = xh \in xH$, com $h \in H$, segue que $f(h) = xh$.

Como f é bijetora, segue que $|H| = |xH|$ e temos o resultado. ■

Teorema 40. ***(Teorema de Lagrange)***

Sejam G um grupo e $H \leq G$. Então:

$$|G| = [G : H] \cdot |H|.$$

Demonstração. Sabemos que $G = \dot{\bigcup_{t\in T}} tH$, onde T é um conjunto de representantes da partição em G feita pelas classes laterais de H. Sendo T um conjunto de representantes da partição, temos que $|T| = |G/H| = [G : H]$.

Caso $|G| < \infty$, temos que $H < \infty$ e $|G/H| < \infty$, e temos que:

$$|G| = |\dot{\bigcup_{t\in T}} tH| = \sum_{t\in T} |tH| = \sum_{t\in T} |H| = |T| \cdot |H| = [G : H] \cdot |H|. \tag{1}$$

Caso $|G| = \infty$ e $|H| = \infty$, vale a igualdade $G = [G : H] \cdot |H|$.

Caso $|G| = \infty$ e $|H| < \infty$, suponha por absurdo que $[G : H] < \infty$. Como $|H|$ e $[G : H] = |T|$ são ambos finitos, valem as manipulações feitas na equação (1), onde obtemos que $|G| < \infty$, um absurdo. Logo, devemos ter que $[G : H] = \infty$ e vale a igualdade $|G| = [G : H] \cdot |H|$. ■

Corolário 41. *Seja G um grupo finito e $H,\ K$ subgrupos tais que $K \leq H \leq G$, então $[G : K] = [G : H]\,[H : K]$*

Demonstração. Usando o Teorema de Lagrange para $H \leq G$, $K \leq G$ e $K \leq H$, respectivamente, teremos:

$$(1) \quad |G| = [G : H] \cdot |H|,$$
$$(2) \quad |G| = [G : K] \cdot |K| \text{ e}$$
$$(3) \quad |H| = [H : K] \cdot |K|.$$

De onde segue que:

$$\begin{aligned} &\overset{(1),(3)}{\Longrightarrow} |G| = [G : H] \cdot [H : K] \cdot |K| \\ &\Longrightarrow {}^{|G|}/_{|K|} = [G : H] \cdot [H : K] \\ &\overset{(2)}{\Longrightarrow} [G : K] = [G : H] \cdot [H : K]\,. \end{aligned}$$

■

Corolário 42. *Sejam p um número primo e G um grupo finito com ordem p, então G é cíclico.*

Demonstração. Seja $g \in G$ tal que $g \neq e$. $|g| = |\langle g\rangle|$, logo, pelo Teorema de Lagrange, $|g|$ divide $|G| = p$.

Sendo $g \neq e$, sabemos que $|g| \neq 1$. Como p é primo, devemos ter que $|g| = p$.

Logo, $G = \langle g\rangle$, isto é, G é cíclico. ■

Anteriormente, dissemos que uma forma de construir novos grupos é a partir de grupos e subgrupos já conhecidos, e então introduzimos o conceito de classes laterais com o objetivo de construir grupos induzindo a operação de G às classes laterais de G por H.

Porém, a operação induzida $(xH, yH) \longrightarrow xyH$ nem sempre estará bem definida, e assim se faz necessária a definição dos grupos onde ocorrerá a boa definição.

Proposição 43. *Sejam G um grupo e $H \leq G$. As seguintes afirmações são equivalentes:*

(i) A operação induzida às classes laterais de H está bem definida.

(ii) Para todo $g \in G$, $gHg^{-1} \subseteq H$.

(iii) Para todo $g \in G$, $gHg^{-1} = H$.

(iv) Para todo $g \in G$, $gH = Hg$.

Demonstração. $(i) \implies (ii)$: Para demonstrar essa implicação, tomaremos duas representações diferentes para duas classes laterais, e estando bem definida, deveremos ter o mesmo resultado independentemente da representação adotada.

Sejam $x, g \in G$, dados $h, k \in H$, tome $\overline{x} = xh^{-1}$ e $\overline{g^{-1}} = g^{-1}k$. Sabemos que $xH = \overline{x}H$ e $g^{-1}H = \overline{g^{-1}}H$.

A operação está bem definida, logo teremos $xg^{-1}H = xHg^{-1}H = \overline{x}H\overline{g^{-1}}H = \overline{x}\overline{g^{-1}}H \implies xg^{-1}H = \overline{x}\overline{g^{-1}}H = xh^{-1}g^{-1}kH \implies xg^{-1}H = xh^{-1}g^{-1}H \implies (xh^{-1}g^{-1})^{-1}xg^{-1} \in H$, mas $(xh^{-1}g^{-1})^{-1}xg^{-1} = ghx^{-1}xg^{-1} = ghg^{-1} \in H$, para quaisquer $g \in G$ e $h \in H \implies gHg^{-1} \subseteq H$, para todo $g \in G$.

$(i) \impliedby (ii)$: Dados $x, \overline{x}, y, \overline{y} \in G$, tais que $xH = \overline{x}H$ e $yH = \overline{y}H$, teremos que $\overline{x} = xh$ e $\overline{y} = yk$, onde $h, k \in H$.

$y^{-1}Hy \subseteq H$, em particular, teremos $y^{-1}h^{-1}y \in H$, mas $y^{-1}h^{-1}y = y^{-1}h^{-1}x^{-1}xy = (xhy)^{-1}xy \in H \implies xyH = xhyH \implies xyH = xhykH \implies xyH = \overline{xy}H$. Logo a operação $(xH, yH) \longrightarrow xyH$ está bem definida.

$(ii) \implies (iii)$: $\forall\ g \in G$ e $\forall\ h \in H$, $g^{-1}hg \in H$, pois $g^{-1}Hg \subseteq H$, logo $h = g(g^{-1}hg)g^{-1} \in gHg^{-1} \implies H \subseteq gHg^{-1}$.

$(ii) \impliedby (iii)$: Trivial.

$(iii) \implies (iv)$: Dado $g \in G$, para todo $x \in gH$, $x = gh$ onde $h \in H$. Note que, como $gHg^{-1} \subseteq H$, $ghg^{-1} = h' \in H$ e teremos que $x = gh = ghg^{-1}g = h'g \in Hg$. Logo $gH \subseteq Hg$.

A inclusão $Hg \subseteq gH$ é análoga. E então temos que $gH = Hg$, para todo $g \in G$.

$(iv) \implies (ii)$: Sejam $g \in G$ e $h \in H$. Como $gH = Hg$, temos que $gh = h'g$ para algum $h' \in H$. Logo $ghg^{-1} = h'gg^{-1} = h' \in H \implies gHg^{-1} \subseteq H$. ■

Definição 44. Dados G um grupo e $H \leq G$, H é dito um subgrupo normal de G se satisfaz uma (e consequentemente, todas) das afirmações da proposição anterior. Denotamos por $H \triangleleft G$ quando H é subgrupo normal de G.

Note que os subgrupos normais $H \triangleleft G$ são os subgrupos nos quais o conjunto quociente G/H, munido da operação induzida, é um grupo, o qual chamaremos de grupo quociente. No decorrer do texto, não faremos diferenciação de notação entre conjunto quociente de H por G e o grupo quociente construído a partir do conjunto quociente munido da operação induzida.

Exemplo 45. Sejam $G = GL_n(\mathbb{K})$ e $H = SL_n(\mathbb{K})$, H será subgrupo normal de G.

Basta ver que, para todos $X \in GL_n(\mathbb{K})$ e $Y \in SL_n(\mathbb{K})$, verificamos pelas propriedades do determinante que:

$$\text{det}(XYX^{-1}) = \text{det}(X)\text{det}(Y)\text{det}(X^{-1}) = \text{det}(X)1_{\mathbb{K}}\text{det}(X)^{-1} = 1_{\mathbb{K}}.$$

Logo, $XYX^{-1} \in SL_n(\mathbb{K})$. De onde concluímos que $SL_n(\mathbb{K}) \triangleleft GL_n(\mathbb{K})$.

Proposição 46. *Sejam G um grupo, $H \leq G$ e $N \triangleleft G$, então $H \cap N \triangleleft H$.*

Demonstração. Pela Proposição 17, sabemos que $H \cap N \leq G$ e, como $H \cap N \subseteq H$, temos $H \cap N \leq H$.

Sejam $h \in H \subseteq G$ e $n \in H \cap N \subseteq N$. $hnh^{-1} \in H$, pois ambos $h, n \in H$ e H é fechado para sua operação. Por outro lado, $hnh^{-1} \in N$ pela normalidade de N em G.

Logo $hnh^{-1} \in H \cap N \implies H \cap N \triangleleft H$. ■

Corolário 47. *Sejam G um grupo e H, N subgrupos de G tais que $N \leq H \leq G$ e $N \triangleleft G$. Então $N \triangleleft H$.*

Demonstração. Segue diretamente da proposição anterior. ■

Exemplo 48. O centro de G (Definição 34) é subgrupo normal de G. Basta ver que: $\forall\, z \in Z(G)$ e $\forall\, g \in G$, $gzg^{-1} = z \implies gZ(G)g^{-1} \subseteq Z(G)$, $\forall\, g \in G \implies Z(G) \triangleleft G$.

Teorema 49. *Se $G/Z(G)$ é cíclico, então G é abeliano.*

Demonstração. $G/Z(G)$ é cíclico $\implies G/Z(G) = \langle \overline{g} \rangle$, para algum $\overline{g} \in G/Z(G)$.

Dados $x,\ y \in G$, $\overline{x} = \overline{g}^m$ e $\overline{y} = \overline{g}^n$, onde $m,\ n \in \mathbb{Z}$.

$\overline{x} = \overline{g}^m = \overline{g^m} \iff x = g^m z_1$ e $\overline{y} = \overline{g}^n = \overline{g^n} \iff y = g^n z_2$, onde $z_1,\ z_2 \in Z(G)$.

$xy = g^m z_1 g^n z_2 = g^m g^n z_1 z_2 = g^{m+n} z_2 z_1 = g^{n+m} z_2 z_1 = g^n g^m z_2 z_1 = g^n z_2 g^m z_1 = yx$.

Portanto, G é abeliano. ■

Definição 50. Se $H \leq G$, então o normalizador de H em G é o conjunto dado por $N_G(H) = \{g \in G;\ gHg^{-1} = H\}$.

$N_G(H)$ é subgrupo pois:

$N_G(H) \neq \varnothing$, já que $e \in N_G(H)$.

Dados $x, y \in N_G(H)$, $yHy^{-1} = H \implies yH = Hy$.

$(xy^{-1})H(xy^{-1})^{-1} = xy^{-1}Hyx^{-1} = xy^{-1}(Hy)x^{-1} = xy^{-1}(yH)x^{-1} = x(H)x^{-1} = H$.

Logo, $N_G(H) \leq G$.

Proposição 51. *$N_G(H)$ é o maior subgrupo de G onde H é normal.*

Demonstração. Por definição, temos que $H \triangleleft N_G(H)$.

Agora, seja K tal que $H \triangleleft K \leq G$. Dado $k \in K$, $kHk^{-1} = H \implies k \in N_G(H) \implies K \subseteq N_G(H)$. ■

Proposição 52. *Sejam H e N subgrupos de G. Se $N \triangleleft G$, então $N \triangleleft HN \leq G$.*

Demonstração. Seja $g_1 \in HN$, $g_1 = h_1n_1$ onde $h_1 \in H$ e $n_1 \in N$.

Temos que $g_1 = h_1n_1 = h_1n_1(e) = h_1n_1(h_1^{-1}h_1) = (h_1n_1h_1^{-1})h_1 \in NH$, pois como $N \triangleleft G$, $h_1n_1h_1^{-1} \in N$. Logo $HN \subseteq NH$.

Seja $g_2 \in NH$, $g_2 = n_2h_2$ onde $n_2 \in N$ e $h_2 \in H$.

Temos que $g_2 = n_2h_2 = (e)n_2h_2 = (h_2h_2^{-1})n_2h_2 = h_2(h_2^{-1}n_2h_2) \in HN$, pois como $N \triangleleft G$, $h_2^{-1}n_2h_2 \in N$. Portanto $NH \subseteq HN$.

Como $HN = NH$, segue pela Proposição 23 que $HN \leq G$. Agora, dados $g \in HN$ e $n \in N$, $g = h_0n_0$ e então $gng^{-1} = (h_0n_0)n(h_0n_0)^{-1} = h_0(n_0nn_0^{-1})h_0^{-1} \in h_0Nh_0 \subseteq N$, pois $N \triangleleft G$, logo $gNg^{-1} \subseteq N$ e segue que $N \triangleleft HN$. ■

Corolário 53. *Sejam H e N subgrupos normais de G, então $HN \triangleleft G$. Além disso, se $H_1, \ldots, H_n$ são subgrupos normais de G, então $H_1H_2 \ldots H_n \triangleleft G$.*

Demonstração. Pela proposição anterior, já sabemos que $HN \leq G$.

Sejam $g \in G$ e $x \in HN$, $x = hn$ onde $h \in H$ e $n \in N$.

$gxg^{-1} = ghng^{-1} = (ghg^{-1})(gng^{-1}) \in HN$, visto que $ghg^{-1} \in H \triangleleft G$ e $gng^{-1} \in N \triangleleft G$.

Logo, $HN \triangleleft G$.

Para o caso mais geral, o resultado é trivial usando indução sobre n. ■

2.3 Homomorfismos

Definição 54. Sejam $(G, \cdot)$ e $(H, *)$ grupos. Se $\varphi : G \longrightarrow H$ é uma função tal que

$$\varphi(x \cdot y) = \varphi(x) * \varphi(y),$$

então φ será chamado homomorfismo de grupos.

Caso φ seja uma bijeção, φ será chamado isomorfismo de grupos, também diremos que os grupos $(G, \cdot)$ e $(H, *)$ são isomorfos e denotaremos essa relação por $(G, \cdot) \cong (H, *)$ ou, fazendo um abuso de notação, $(G, \cdot) = (H, *)$.

Exemplo 55. Sejam G um grupo e $H \triangleleft G$. $\pi : G \longrightarrow G/H$, dada por $g \longmapsto gH$, é um homomorfismo sobrejetor, o qual é chamado homomorfismo projeção canônica e seu núcleo é $\ker(\pi) = H$.

Proposição 56. *Sejam G e H grupos e $\varphi : G \longrightarrow H$ um homomorfismo. Então:*

(i) $\varphi(e_G) = e_H$.

(ii) Dado $g \in G$, $\varphi(g^{-1}) = \varphi(g)^{-1}$.

(iii) Dados $g \in G$ *e* $n \in \mathbb{Z}$, $\varphi(g^n) = \varphi(g)^n$.

Demonstração.

(i) Sabemos que $e_G = e_G e_G$, logo $\varphi(e_G) = \varphi(e_G e_G) = \varphi(e_G)\varphi(e_G) \implies \varphi(e_G) = e_H$.

(ii) $e_G = gg^{-1} \implies \varphi(e_G) = \varphi(gg^{-1}) = \varphi(g)\varphi(g^{-1}) \implies e_H = \varphi(g)\varphi(g^{-1}) \implies \varphi(g^{-1}) = \varphi(g)^{-1}$.

(iii) Caso $n = 0$, teremos $\varphi(g^0) = \varphi(e_G) = e_H$ e $\varphi(g)^0 = e_H \implies \varphi(g^0) = \varphi(g)^0$.

Caso $n \geq 1$, faremos indução sobre n. $\varphi(g^1) = \varphi(g) = \varphi(g)^1$. Suponha que $\varphi(g^n) = \varphi(g)^n$ para algum $n \in \mathbb{N}$. Segue $\varphi(g^{n+1}) = \varphi(g^n g^1) = \varphi(g^n)\varphi(g^1) = \varphi(g)^n\varphi(g)^1 = \varphi(g)^{n+1}$. ■

Definição 57. Sejam G e H grupos e $\varphi : G \longrightarrow H$ um homomorfismo, então o núcleo de φ é o conjunto denotado por $\ker(\varphi) = \{g \in G;\ \varphi(g) = e_H\}$.

Proposição 58. *Sejam G e H grupos e $\varphi : G \longrightarrow H$ um homomorfismo, então:*

(i) ker$(\varphi) \triangleleft G$.

(ii) im$(\varphi) \leq H$.

(iii) φ *é injetor se, e somente se, ker*$(\varphi) = \{e_G\}$.

Demonstração.

(i) $\ker(\varphi) \leq G$ pois, dados $x, y \in \ker(\varphi)$, $\varphi(xy^{-1}) = \varphi(x)\varphi(y^{-1}) = \varphi(x)\varphi(y)^{-1} = e_H e_H^{-1} = e_H \implies xy^{-1} \in \ker(\varphi) \implies \ker(\varphi) \leq G$.

Dado $g \in G$, tome $gxg^{-1} \in g(\ker(\varphi))g^{-1}$, onde $x \in \ker(\varphi)$.

Segue que $\varphi(gxg^{-1}) = \varphi(g)\varphi(x)\varphi(g^{-1}) = \varphi(g)\varphi(g)^{-1} = e_H \implies gxg^{-1} \in \ker(\varphi) \implies g(\ker(\varphi))g^{-1} \subseteq \ker(\varphi) \implies \ker(\varphi) \triangleleft G$.

(ii) Dados $h_1,\ h_2 \in \text{im}(\varphi)$, existem $g_1,\ g_2 \in G$ tais que $\varphi(g_1) = h_1$ e $\varphi(g_2) = h_2$, e então segue que $h_1 h_2^{-1} = \varphi(g_1)\varphi(g_2)^{-1} = \varphi(g_1)\varphi(g_2^{-1}) = \varphi(g_1 g_2^{-1}) \implies h_1 h_2^{-1} \in \text{im}(\varphi) \implies \text{im}(\varphi) \leq H$.

(iii) $(\Rightarrow)$ Dado $g \in \ker(\varphi)$, $\varphi(g) = e_H$. Como $\varphi(e_G) = e_H \implies g = e_G \implies \ker(\varphi) = \{e_G\}$.

$(\Leftarrow)$ Dados $g_1,\ g_2 \in G$ tais que $\varphi(g_1) = \varphi(g_2)$, teremos que $e_H = \varphi(g_1)\varphi(g_2)^{-1} = \varphi(g_1 g_2^{-1}) \implies g_1 g_2^{-1} \in \ker(\varphi) = \{e_G\} \implies g_1 g_2^{-1} = e_G \implies g_1 = g_2 \implies \varphi$ é injetor. ■

Teorema 59. ***(1º Teorema de Isomorfismo)*** *Sejam $G,\ H$ grupos e $\varphi : G \longrightarrow H$ um homomorfismo, então $G/$ker$(\varphi) \cong$ im(φ).*

Demonstração. Seja $K = \ker(\varphi)$, sabemos que $K \lhd G$, logo G/K é um grupo. Tome $\pi : G/K \longrightarrow H$ dada por $\pi(gK) = \varphi(g)$.

π está bem definida pois, dados $xK,\ yK \in G/K$ tais que $xK = yK$, $xK = yK \implies xy^{-1} \in K \implies e_H = \varphi(xy^{-1}) = \varphi(x)\varphi(y)^{-1} \implies \varphi(x) = \varphi(y) \implies \pi(xK) = \pi(yK)$.

π é um homomorfismo pois, dados $xK,\ yK \in G/K$, $\pi(xK \cdot yK) = \pi((xy)K) = \varphi(xy) = \varphi(x)\varphi(y) = \pi(xK)\pi(yK)$.

Por fim, π é injetor pois, dado $gK \in G/K$ tal que $\pi(gK) = e_H$, $\pi(gK) = e_H \implies \varphi(g) = e_H \implies g \in K = \ker(\varphi) \implies gK = K = e_{G/K} \implies \ker(\pi) = \{e_{G/H}\}$.

Sendo π um homomorfismo injetor, ao restringirmos seu contradomínio à sua imagem, teremos π sobrejetor em $\text{im}(\varphi)$, fazendo com que $\pi : G/K \longrightarrow \text{im}(\varphi)$ seja um isomorfismo, e portanto, temos $G/K = G/\ker(\varphi) \cong \text{im}(\varphi)$. ■

Teorema 60. ***(2º Teorema de Isomorfismo)***

Sejam G um grupo e $N,\ T$ subgrupos de G, com $N \lhd G$. Então $(N \cap T) \lhd T$ e

$$\frac{TN}{N} \cong \frac{T}{(T \cap N)}.$$

Demonstração. Pela Proposição 52, sabemos que $N \lhd TN \leq G$, logo faz sentido considerar o grupo quociente TN/N.

Seja $\pi : TN \longrightarrow TN/N$ o homomorfismo projeção canônica. Tome $\pi' = \pi\big|_T$. Teremos que $\ker(\pi') = \{t \in T;\ \pi'(t) = N\} = \{t \in T;\ tN = N\} = \{t \in T;\ t \in N\} = T \cap N$.

E segue, pelo 1º Teorema de Isomorfismo (59), que $T/(T \cap N) \cong \text{im}(\pi')$.

Por outro lado, dado $\overline{x} \in TN/N$, $\overline{x} = (tn)N = tN = \pi'(t) \in \pi'(T) = \text{im}(\pi')$, ou seja, π' é sobrejetora e temos $\text{im}(\pi') = TN/N$. De onde concluímos que:

$$\frac{TN}{N} \cong \frac{T}{(T \cap N)}.$$

■

Teorema 61. ***(3º Teorema de Isomorfismo)***

Sejam $K \leq H \leq G$, com H e K ambos normais em G. Então $H/K \lhd G/K$ e

$$\frac{(G/K)}{(H/K)} \cong \frac{G}{H}.$$

Demonstração. Seja $\pi : G/K \longrightarrow G/H$ dada por $\pi(gK) = gH$.

π está bem definida pois, $g_1K = g_2K \implies g_1 = g_2k$, onde $k \in K$, e segue que $\pi(g_1K) = g_1H = g_2kH = g_2H = \pi(g_2K)$.

π é homomorfismo pois, dados $xK,\ yK \in G/K$, $\pi(xKyK) = \pi(xyK) = xyH = xHyH = \pi(xK)\pi(yK)$. Pelo 1º Teorema de Isomorfismo (59), temos que $(G/K)/\text{ker}(\pi) \cong \text{im}(\pi)$.

Por um lado, temos que

$$\begin{aligned}\text{ker}(\pi) = \{gK \in G/K;\ \pi(gK) = H\} &= \{gK \in G/K;\ gH = H\} \\ &= \{gK \in G/K;\ g \in H\} = H/K.\end{aligned}$$

Por outro lado, dado $gH \in G/H$, temos que $g \in G$ e $\pi(gK) = gH$, logo π é sobrejetora e temos $\text{im}(\pi) = G/H$.

Logo,

$$\frac{(G/K)}{\text{ker}(\pi)} \cong \text{im}(\pi) \iff \frac{(G/K)}{(H/K)} \cong \frac{G}{H}.$$

■

Teorema 62. *Seja G um grupo cíclico.*

(i) Se $|G| = \infty$, então $G \cong \mathbb{Z}$.

(ii) Se $|G| = n < \infty$, então $G \cong \mathbb{Z}/n\mathbb{Z}$.

Demonstração. G é cíclico, logo $\langle g \rangle = G$ para algum $g \in G$.

Tome $\varphi : \mathbb{Z} \longrightarrow G$ dada por $\varphi(m) = g^m$.

φ é homomorfismo pois, dados $m_1,\ m_2 \in \mathbb{Z}$, $\varphi(m_1 + m_2) = g^{m_1+m_2} = g^{m_1}g^{m_2} = \varphi(m_1)\varphi(m_2)$.

Além disso, φ é sobrejetor pois, dado $x \in G = \langle g \rangle$, existe $m_0 \in \mathbb{Z}$ tal que $x = g^{m_0} = \varphi(m_0)$.

Pelo 1º Teorema de Isomorfismo, temos que $\mathbb{Z}/ker(\varphi) \cong G$.

Agora basta analisarmos $ker(\varphi)$:

(i) Se $|G| = \infty$, $|g| = \infty \implies g^t = e$, onde $t \in \mathbb{Z}$, ocorre somente com $t = 0$. Logo, temos que $ker(\varphi) = \{m \in \mathbb{Z};\ \varphi(m) = g^m = 0\} = \{0\}$. De onde temos que $G \cong \mathbb{Z}/\{0\} = \mathbb{Z}$.

(ii) Se $|G| = n$, $|g| = n \implies g^t = e,\ t \in \mathbb{Z} \iff t = nq$, onde $q \in \mathbb{Z} \iff t \in n\mathbb{Z}$. Portanto $G \cong \mathbb{Z}/n\mathbb{Z}$. ■

Teorema 63. ***(Teorema de Cayley)***

Seja G um grupo, então existe um subgrupo $H \leq S_G$ tal que $G \cong H$. Além disso, se G é finito com ordem n, G será isomorfo à um subgrupo do grupo de permutações S_n.

Demonstração. Consideremos inicialmente G apenas como conjunto. Recapitulando o Exemplo 9, temos que $S_G = \{f : G \longrightarrow G;\ f \text{ é bijeção}\}$.

Dado $g \in G$, tome $f_g : G \longrightarrow G$ dada por $f_g(x) = gx$, mostraremos que f_g é uma bijeção.

Sejam $x_1, x_2 \in G$ tais que $f_g(x_1) = f_g(x_2) \implies gx_1 = gx_2 \implies x_1 = x_2$, logo f_g é injetora.

Dado $y \in G$, tome $(g^{-1}y) \in G$ e teremos que $y = gg^{-1}y = f_g(g^{-1}y)$, logo f_g é sobrejetora.

Portanto, f_g é uma bijeção e temos $f_g \in S_G$.

Defina agora:

$$\begin{aligned} \psi : G &\longrightarrow S_G \\ g &\longmapsto \psi(g) = f_g : G \longrightarrow G \\ & \qquad g \longmapsto f_g(x) = gx \end{aligned}$$

Mostraremos que ψ é um homomorfismo injetor.

Note que, dados $g,h \in G$, para todo $x \in G$, $f_g \circ f_h(x) = f_g(f_h(x)) = g(hx) = (gh)x = f_{gh}(x) \implies f_g \circ f_h = f_{gh}$.

ψ é um homomorfismo pois, dados $g, h \in G$,

$$\psi(g)\psi(h) = f_g \circ f_h = f_{gh} = \psi(gh).$$

Dado $g \in \ker(\psi)$, teremos que $\psi(g) = f_g$ é tal que $f_g(x) = x$ para todo $x \in G$. Em particular, temos que $f_g(e) = e \implies ge = e \implies g = e \implies \ker(\psi) = \{e\}$. Logo ψ é injetora.

Sendo ψ um homomorfismo injetor, pelo 1º Teorema de Isomorfismo (59), temos que $G \cong \text{im}(\psi) \leq S_G$. ■

Corolário 64. *Dado $n \in \mathbb{N}$, existe somente uma quantidade finita (a menos de isomorfismo) de grupos com ordem n.*

Demonstração. Pelo Teorema de Cayley, temos que G será isomorfo a algum subgrupo de S_G. Se $|G| = n$, teremos que $S_G \cong S_n$ e $|S_n| = n!$.

Para tomarmos um subconjunto de S_n com exatamente n elementos, deveremos escolher n elementos dentre os $n!$ que compõem S_n, e isso poderá ser feito de $\binom{n!}{n}$ formas diferentes.

Dado $H \leq S_n$ com $|H| = n$, H deverá figurar entre os $\binom{n!}{n}$ subconjuntos possíveis com n elementos, o que limita a quantidade de subgrupos H possíveis nessas condições.

Como G deverá ser isomorfo à algum desses subgrupos H, e existem somente finitos subgrupos $H \leq S_n$ tais que $|H| = n$, existirá somente uma quantidade finita de grupos G com n elementos. ■

Lema 65. *Sejam G e G^* grupos, $\varphi : G \longrightarrow G^*$ um homomorfismo e $S^* \leq G^*$. Então $\varphi^{-1}(S^*) = \{s \in G;\ \varphi(s) \in S^*\} \leq G$ e $\ker(\varphi) \leq \varphi^{-1}(S^*)$.*

Demonstração. Dados x e $y \in \varphi^{-1}(S^*)$, $\varphi(x)$ e $\varphi(y) \in S^*$, e temos que $\varphi(xy^{-1}) = \varphi(x)\varphi(y^{-1}) = \varphi(x)\varphi(y)^{-1}$, mas $\varphi(x)\varphi(y)^{-1} \in S^* \leq G^*$, logo $xy^{-1} \in \varphi^{-1}(S^*)$ e segue que $\varphi^{-1}(S^*) \leq G$.

Agora, $e_{G^*} \in S^*$, logo, se $g \in \ker(\varphi)$, teremos $\varphi(g) = e_{G^*} \in S^* \implies \ker(\varphi) \subseteq \varphi^{-1}(S^*)$.

Já sabemos que $\ker(\varphi) \leq G$, o que garante que $\ker(\varphi)$ seja um grupo. Sabendo que $\ker(\varphi) \subseteq \varphi^{-1}(S^*)$, concluímos que $\ker(\varphi) \leq \varphi^{-1}(S^*)$. ■

Teorema 66. ***(Teorema da Correspondência)***

Seja $K \triangleleft G$ e seja $\varphi : G \longrightarrow G/K$ a projeção canônica. Então $S \overset{\pi}{\longmapsto} \varphi(S) = S/K$ é uma bijeção da família de subgrupos de G que contém K para a família de todos os subgrupos de G/K.

Além disso, sendo S, T subgrupos de G tais que $K \leq S$ e $K \leq T$, e denotando S/K por S^*, segue que:

(i) $T \leq S$ se, e somente se, $T^* \leq S^*$, e então $[S : T] = [S^* : T^*]$.

(ii) $T \triangleleft S$ se, e somente se, $T^* \triangleleft S^*$, e então $S/T \cong S^*/T^*$.

Demonstração. Sejam S e T subgrupos de G contendo K, se $S/K = T/K$, dado $sK \in S/K$, existe $t \in T$ tal que $sK = tK$, e disto temos que $s = tk$ para algum $k \in K$. Como $K \leq T$, $s = tk \in T \implies S \subseteq T$. Analogamente, $T \subseteq S$, e segue que $S = T$. Logo, $S \overset{\pi}{\longmapsto} \varphi(S) = S/K$ é injetora.

Agora, dado $A \leq G/K$, pelo lema anterior, temos que $\varphi^{-1}(A) \leq G$, $K = \ker(\varphi) \leq \varphi^{-1}(A)$ e, como φ é sobrejetora, $\varphi(\varphi^{-1}(A)) = A$. Ou seja, $S \overset{\pi}{\longmapsto} \varphi(S) = S/K$ é sobrejetora, e assim, temos que $S \overset{\pi}{\longmapsto} \varphi(S) = S/K$ é uma bijeção.

(i) : Sejam T, S subgrupos de G tais que $K \leq T \leq S$, então $T^* = \varphi(T) \subseteq \varphi(S) = S^* \implies T^* \leq S^*$. Por outro lado, se $T^* \leq S^*$, então $T^* \subseteq S^* \implies T = \varphi(T^*)^{-1} \subseteq \varphi(S^*)^{-1} = S \implies S \leq T$.

Para mostrarmos que $[S : T] = [S^* : T^*]$, defina $\alpha : S/T \longrightarrow S^*/T^*$ dada por $\alpha(sT) = \varphi(s)T^*$.

α é injetora, pois, dados $sT, s'T \in S/T$ tais que $\alpha(sT) = \alpha(s'T) \implies \varphi(s)T^* = \varphi(s')T^* \implies \varphi(s')^{-1}\varphi(s) = \varphi(s'^{-1}s) \in T^* = \varphi(T) \implies \varphi(s'^{-1}s) = \varphi(t)$, onde $t \in T \implies \varphi(s'^{-1}s)\varphi(t)^{-1} = \varphi(s'^{-1}st^{-1}) = e \implies s'^{-1}st^{-1} \in \ker(\varphi) = K \subseteq T \implies s'^{-1}st^{-1} \in T \implies st^{-1}T = s'T \implies sT = s'T$.

α é sobrejetora pois, dado $s^*T^* \in S^*/T^*$, $s^* \in S^*$, logo $s^* = sK$ com $s \in S$. Tome $sT \in S/T$, como $\varphi(s) = sK$, segue que $s^*T^* = (sK)T^* = \varphi(s)T^* = \alpha(sT)$.

Sendo α uma bijeção, temos que $|S/T| = |S^*/T^*| \implies [S : T] = [S^* : T^*]$.

(ii) : Se $T \triangleleft S$, tome $s^* \in S^*$ e $t^* \in T^*$, $s^*t^*(s^*)^{-1} = sKtK(sK)^{-1}$. Como $K \triangleleft G$, segue que $sKtK(sK)^{-1} = sKtKs^{-1}K = sts^{-1}K$, e como $T \triangleleft S$, $sts^{-1} = t' \in T \implies sKtK(sK)^{-1} = sts^{-1}K = t'K \implies s^*t^*(s^*)^{-1} = t'^*$. Logo $T^* \triangleleft S^*$.

Se $T^* \triangleleft S^*$, tome $s \in S$ e $t \in T$. $\varphi(sts^{-1}) = sts^{-1}K = sKtKs^{-1}K = sKtK(sK)^{-1} = s^*t^*(s^*)^{-1}$ e $s^*t^*(s^*)^{-1} \in T^* \triangleleft S^* \implies \varphi(sts^{-1}) \in T^* = \varphi(T)$, logo existe um $t' \in T$ tal que $\varphi(sts^{-1}) = \varphi(t') \implies \varphi(sts^{-1})\varphi(t')^{-1} = \varphi(sts^{-1}(t')^{-1}) = K \implies sts^{-1}(t')^{-1} \in \ker(\varphi) = K \leq T \implies sts^{-1}(t')^{-1} \in T \implies sts^{-1} = sts^{-1}(t')^{-1}(t') \in T \implies T \triangleleft S$.

Por fim, pelo 3º Teorema de Isomorfismo (61), segue que $S/T \cong S^*/T^*$. ■

Proposição 67. *Seja M um subgrupo maximal de G. Se $M \triangleleft G$ então $[G : M]$ é um número primo.*

Demonstração. O Teorema da Correspondência nos mostra que existe uma bijeção entre os subgrupos H tais que $M \leq H \leq G$ e os subgrupos $H/M \leq G/M$. Sendo M maximal, devemos ter $H = M$ ou $H = G$, e então $H/M = M/M$ ou $H/M = G/M$, isto é, G/M não admite subgrupos próprios.

Sendo $\overline{g} \in G/M$, $\overline{g} \neq M$, temos que $\langle \overline{g} \rangle$ é um subgrupo não trivial de G/M. Logo, $\langle \overline{g} \rangle = G/M$, ou seja, G/M é cíclico.

Se $|G/M| = \infty$, temos pelo Teorema 62, $G/M \cong \mathbb{Z}$, um absurdo, visto que $\mathbb{Z}$ admite infinitos subgrupos da forma $n\mathbb{Z}$.

Se $|G/M| = n < \infty$, novamente pelo Teorema 62, temos que $G/M \cong \mathbb{Z}/n\mathbb{Z}$. Dado m inteiro tal que $m \mid n$, temos que $n\mathbb{Z} \leq m\mathbb{Z} \leq \mathbb{Z}$ e então $m\mathbb{Z}/n\mathbb{Z} \leq \mathbb{Z}/n\mathbb{Z}$. Mas $\mathbb{Z}/n\mathbb{Z} \cong G/M$ não admite subgrupos próprios, logo devemos ter que $m\mathbb{Z}/n\mathbb{Z} = n\mathbb{Z}/n\mathbb{Z}$ ou $m\mathbb{Z}/n\mathbb{Z} = \mathbb{Z}/n\mathbb{Z}$, de onde segue que $m\mathbb{Z} = n\mathbb{Z}$ ou $m\mathbb{Z} = \mathbb{Z} \implies m = n$ ou $m = 1$. Em suma, obtivemos que $m \mid n \implies m = n$ ou $m = 1$.

Portanto, n é um número primo e temos que $[G : M] = |G/M| = n$ é primo. ■

2.4 Produto Direto Finito

Definição 68. Sejam $(H, \cdot)$ e $(K, *)$ grupos, então o produto direto de H e K, denotado por $H \times K$, é o grupo formado pelos pares ordenados $(h,\ k)$, onde $h \in H$ e $k \in K$, e a operação é definida por $(h, k) \circ (x, y) = (h \cdot x,\ k * y)$. Na notação aditiva, chamamos o produto direto de soma direta e denotamos por $H \oplus K$.

Vale notar que, para o produto direto $H \times K$, teremos que $e_{H\times K} = (e_H,\ e_K)$ e, dado $(h,\ k) \in H \times K$, $(h,\ k)^{-1} = (h^{-1},\ k^{-1})$. Além disso, os grupos H e K são ditos componentes diretas de $H \times K$, e o grupo $H \times K$ contém réplicas isomorfas de suas componentes da forma $H \cong H \times \{e_K\} \leq H \times K$ e $K \cong \{e_H\} \times K \leq H \times K$.

Proposição 69. *Sejam G um grupo e $H,\ K \triangleleft G$. Se $HK = G$ e $H \cap K = \{e\}$, então $G \cong H \times K$.*

Demonstração. Dado $g \in G = HK$, $g = hk$ onde $h \in H$ e $k \in K$.

Fato: h e k são unicamente determinados por g.

Tome $h_1,\ h_2 \in H$ e $k_1,\ k_2 \in K$ tais que $g = h_1k_1 = h_2k_2$. Logo $h_2^{-1}h_1 = k_2k_1^{-1} \in H \cap K = \{e\} \implies h_2^{-1}h_1 = e = k_2k_1^{-1} \implies h_1 = h_2$ e $k_1 = k_2$.

Sendo h e k unicamente determinados por g, a aplicação $\varphi : G \longrightarrow H \times K$, dada por $\varphi(g) = (h, k)$, estará bem definida.

Dados x e $y \in G = HK$, $x = hk$ e $y = h'k'$, onde $h,\ h' \in H$ e $k,\ k' \in K$. Considere o elemento $h'kh'^{-1}k^{-1}$.

$h'(kh'^{-1}k^{-1}) \in H$ pois $H \triangleleft G$.

$(h'kh'^{-1})k^{-1} \in K$ pois $K \triangleleft G$.

Logo $h'kh'^{-1}k^{-1} \in H \cap K = \{e\} \implies h'kh'^{-1}k^{-1} = e \implies h'k = kh'$.

Dessa forma, φ será homomorfismo, pois, $\varphi(xy) = \varphi(hkh'k') = \varphi(hh'kk') = (hh',\ kk') = (h,\ k)(h',\ k') = \varphi(x)\varphi(y)$.

Dado $g_0 \in \ker(\varphi)$, $g_0 = h_0k_0$ e $\varphi(g) = (h_0,\ k_0) = (e,\ e) \implies h_0 = e$ e $k_0 = e \implies g_0 = ee = e \implies \ker(\varphi) = \{e\}$. Logo, φ é injetora.

Dado $(a,\ b) \in H \times K$, temos que $ab \in G$ e $\varphi(ab) = (a,\ b)$. φ é sobrejetora.

Por fim, temos que φ é um homomorfismo bijetor, isto é, um isomorfismo, e segue que $G \cong H \times K$. ■

Corolário 70. *Sejam p e q inteiros positivos tais que mdc$(p,\ q) = 1$. Então $\mathbb{Z}/(pq)\mathbb{Z} \cong \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/q\mathbb{Z}$.*

Demonstração. Seja g um gerador de $\mathbb{Z}/(pq)\mathbb{Z}$, temos que $|g| = pq$.

Considere $\langle g^q\rangle \leq \mathbb{Z}/(pq)\mathbb{Z}$ e $\langle g^p\rangle \leq \mathbb{Z}/(pq)\mathbb{Z}$.

$|g^q| = p$ e $|g^p| = q$, logo $\langle g^q\rangle \cong \mathbb{Z}/p\mathbb{Z}$ e $\langle g^p\rangle \cong \mathbb{Z}/q\mathbb{Z}$.

Dado $x \in \mathbb{Z}/(pq)\mathbb{Z}$, $x = g^n$ para algum inteiro n.

Como mdc$(p,\ q) = 1$, existem inteiros r e s tais que $rp + sq = 1 \implies nrp + nsq = n \implies x = g^n = g^{nrp+nsq} = g^{nrp}g^{nsq} = (g^p)^{nr}(g^q)^{ns} \in \langle g^p\rangle\langle g^q\rangle$.

Agora, dado $y \in \langle g^p\rangle \cap \langle g^q\rangle$, $y = (g^p)^{n_1} = (g^q)^{n_2} \implies g^{pn_1} = g^{qn_2} \implies g^{pn_1}(g^{qn_2})^{-1} = g^{pn_1-qn_2} = \overline{0} \in \mathbb{Z}/(pq)\mathbb{Z} \implies pn_1 - qn_2 = m(pq),\ m \in \mathbb{Z} \implies p(n_1-mq) = qn_2 \implies p \mid n_2 \implies n_2 = pk, k \in \mathbb{Z}$. Logo $y = g^{qn_2} = g^{qpk} = (g^{pq})^k = \overline{0} \implies \langle g^p\rangle \cap \langle g^q\rangle = \{\overline{0}\}$.

Pela proposição anterior, segue que $\mathbb{Z}/(pq)\mathbb{Z} \cong \langle g^q\rangle \times \langle g^p\rangle \cong \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/q\mathbb{Z}$. ■

Teorema 71. *Sejam G um grupo e $H_1,\ \ldots,\ H_n$ subgrupos normais de G. Se $G = \langle \bigcup_{i=1}^{n} H_i\rangle$ e, para todo j, $H_j \bigcap \langle \bigcup_{\substack{i=1 \\ i\neq j}}^{n} H_i\rangle = \{e\}$, então $G \cong H_1 \times \ldots \times H_n$.*

Demonstração. Sendo $H_1, \ldots, H_n$ subgrupos normais temos, pelo Corolário 53, que $H_1H_2\ldots H_n \leq G$, e pela Proposição 25, que $H_1H_2\ldots H_n = \langle \bigcup_{i=1}^{n} H_i\rangle = G$.

Fato (1): dado $g \in G = H_1\ldots H_n$, existem únicos $h_1 \in H_1,\ \ldots\ , h_n \in H_n$ tais que $g = h_1\ldots h_n$.

Seja $g = x_1\ldots x_n = y_1\ldots y_n$ onde $x_i,\ y_i \in H_i$.

Multiplicando à esquerda por y_1^{-1} e à direita por $x_n^{-1}...x_2^{-1}$ em $x_1...x_n = y_1...y_n$, teremos:

$$\underbrace{y_1^{-1}x_1}_{\in H_1} = \underbrace{y_2...y_n x_n^{-1}...x_2^{-1}}_{\in \langle \bigcup_{\substack{i=1 \\ i\neq j}}^{n} H_i \rangle} \in H_1 \bigcap \langle \bigcup_{\substack{i=1 \\ i\neq 1}}^{n} H_i \rangle = \{e\} \implies y_1^{-1}x_1 = e \implies x_1 = y_1.$$

Analogamente, obtemos que $x_2 = y_2$, ... , $x_n = y_n$, o que mostra o Fato (1).

Logo, a função

$$\pi : G = H_1...H_n \longrightarrow H_1 \times ... \times H_n$$

$$g = h_1...h_n \longmapsto (h_1, \ ... \ , \ h_n)$$

estará bem definida e será injetora, devido a unicidade dos h_i na decomposição $g = h_1...h_n$.

Além disso, π é sobrejetora, pois dado $(h_1, \ ... \ , \ h_n) \in H_1 \times ... \times H_n$, $(h_1, \ ... \ , \ h_n) = \varphi(h_1...h_n)$. Portanto, temos que π é bijetora.

Fato (2): para cada $j \neq i$, dados $x \in H_j$ e $y \in H_i$, $xy = yx$.

Considere o elemento $xyx^{-1}y^{-1}$.

$xyx^{-1}y^{-1} = (xyx^{-1})y^{-1} \in H_i$, pois $H_i \triangleleft G$, e $xyx^{-1}y^{-1} = x(yx^{-1}y^{-1}) \in H_j$, pois $H_j \triangleleft G$, logo $xyx^{-1}y^{-1} \in H_j \cap H_i = \{e\} \implies xyx^{-1}y^{-1} = e \implies xy = yx$, o que mostra o Fato (2).

Dados $a = a_1...a_n$ e $b = b_1...b_n \in G$, utilizando o Fato (2), podemos comutar os pares de elementos afim de obter $ab = a_1...a_n b_1...b_n = a_1b_1...a_nb_n$, o que nos permite mostrar que π é homomorfismo pois, $\pi(ab) = \pi(a_1b_1...a_nb_n) = (a_1b_1, \ ... \ , \ a_nb_n) = (a_1, \ ... \ , \ a_n)(b_1, \ ... \ , \ b_n) = \pi(a)\pi(b)$.

Sendo π um homomorfismo bijetor, temos que π é um isomorfismo e segue que

$$G \cong H_1 \times ... \times H_n.$$

■

3 FERRAMENTAS INTERESSANTES PARA O ESTUDO DE GRUPOS

3.1 Ação de Grupos

Definição 72. Seja X um conjunto não-vazio e G um grupo. Uma ação de G em X é uma função $\alpha : G \times X \longrightarrow X$, tal que:

(i) $\alpha(e, x) = x, \forall\, x \in X$, onde e é o elemento neutro de G.

(ii) $\alpha(g, \alpha(h, x)) = \alpha(gh, x), \forall\, g, h \in G$ e $\forall\, x \in X$.

Quando não houver confusão sobre a ação α, escreveremos apenas $g \cdot x$ ou gx ao invés de $\alpha(g, x)$. Nesses casos, também ocultamos o nome da ação α e apenas dizemos que G age em X. Reescrevendo as condições acima nessa notação, teremos:

(i) $e \cdot x = x, \forall\, x \in X$, onde e é o elemento neutro de G.

(ii) $g \cdot (h \cdot x) = (gh) \cdot x, \forall\, g, h \in G$ e $\forall\, x \in X$.

Exemplo 73. Sejam G um grupo e X um conjunto, a ação $g \cdot x = x, \forall\, g \in G$ e $\forall\, x \in X$, é chamada ação trivial.

Exemplo 74. Dado um grupo $(G, *)$, podemos tomar X como o próprio G. G pode agir em si mesmo utilizando a própria operação $*$. Nesse caso, a ação $g \cdot x = g * x$ é chamada translação à esquerda, enquanto ação $g \cdot x = x * g$ é chamada translação à direita.

Exemplo 75. Dado um conjunto X, podemos tomar $G = S_X$ (descrito no Exemplo 9) e construir a ação α dada por $\sigma \cdot x = \sigma(x)$, com $\sigma \in S_X$ e $x \in X$.

Exemplo 76. Seja G um grupo e $H \leq G$. H age em G pela ação $h \cdot x = hx$. Esta ação recebe o nome de translação esquerda de G por H.

Da mesma forma, é possível construir a translação direita de G por H, tomando $h \cdot x = xh$.

Exemplo 77. Dado um grupo G, a conjugação de G por G pode ser vista como uma ação, tomando $g \cdot x = gxg^{-1}$. Da mesma forma, se $H \leq G$, podemos conceber a ação $h \cdot x = hxh^{-1}$. A conjugação define uma ação, visto que:

Dados $h_1, h_2 \in H$ e $x \in G$,

(i) $h_1 \cdot (h_2 \cdot x) = h_1 \cdot (h_2 x h_2^{-1}) = h_1(h_2)xh_2^{-1}h_1^{-1} = (h_1h_2)x(h_1h_2)^{-1} = (h_1h_2) \cdot x$.

(ii) $e \cdot x = exe^{-1} = x$.

De forma análoga, $H \leq G$ pode agir por conjugação em outras estruturas de G, como por exemplo, no conjunto de todos os subgrupos de G ou então no conjunto de conjugados de um subgrupo K em G.

Proposição 78. *Dados G um grupo e X um conjunto. Cada ação $\alpha : G \times X \longrightarrow X$ induz um homomorfismo $\varphi : G \longrightarrow S_X$ e vice-versa.*

Demonstração. Primeiramente vamos mostrar que, para cada ação $\alpha : G \times X \longrightarrow X$ temos um homomorfismo $\varphi : G \longrightarrow S_X$:

Dado $g \in G$, tome $\sigma_g : X \longrightarrow X$ dada por $\sigma_g(x) = g \cdot x$.

Dados x_1 e $x_2 \in X$ tais que $\sigma_g(x_1) = \sigma_g(x_2)$. Temos que:

$$\sigma_g(x_1) = \sigma_g(x_2) \implies g \cdot x_1 = g \cdot x_2 \implies g^{-1} \cdot (g \cdot x_1) = g^{-1} \cdot (g \cdot x_2)$$
$$\implies (g^{-1}g) \cdot x_1 = (g^{-1}g) \cdot x_2 \implies e \cdot x_1 = e \cdot x_2 \implies x_1 = x_2.$$

Logo, σ_g é injetora.

Além disso, dado $x \in X$, $g^{-1} \cdot x \in X$ e $x = g \cdot (g^{-1} \cdot x) = \sigma_g(g^{-1} \cdot x) \in Im(\sigma_g)$. Portanto, σ_g é sobrejetora.

Assim, concluímos que σ_g é bijetora e que $\sigma_g \in S_X$.

Tome agora $\varphi : G \longrightarrow S_X$ definida por $\varphi(g) = \sigma_g$. Dados $g,\ h \in G$, $\varphi(gh) = \sigma_{gh} = \sigma_g \circ \sigma_h = \varphi(g) \circ \varphi(h)$.

A igualdade $\sigma_{gh} = \sigma_g \circ \sigma_h$ é válida pois:

$\sigma_{gh}(x) = (gh) \cdot x = g \cdot (h \cdot x) = \sigma_g(\sigma_h(x)) = (\sigma_g \circ \sigma_h)(x),\ \forall\, x \in X.$

Logo, temos que $\varphi : G \longrightarrow S_X$ é homomorfismo induzido pela ação α.

Agora vamos mostra que, para cada homomorfismo $\varphi : G \longrightarrow S_X$ temos uma ação $\alpha : G \times X \longrightarrow X$.

Dado um homomorfismo $\varphi : G \longrightarrow S_X$, defina $\alpha : G \times X \longrightarrow X$ por $g \cdot x = (\varphi(g))(x)$. Dados $g,\ h \in G$, $x \in X$ e sendo e o elemento neutro de G, temos que:

(i) $e \cdot x = \varphi(e)(x) = id(x) = x$

(ii) $g \cdot (h \cdot x) = (\varphi(g))((\varphi(h))(x)) = ((\varphi(g)) \circ (\varphi(h)))(x) = (\varphi(gh))(x) = (gh) \cdot x.$

Assim, concluímos que α é uma ação induzida pelo homomorfismo φ. ■

Exemplo 79. A ação trivial (descrita no Exemplo 73) induz o homomorfismo nulo de G em S_X.

O conceito de ação induz a definição de certas estruturas nos grupos que agem e nos conjuntos que recebem a ação.

Seja G um grupo agindo em X. Podemos definir a relação $\sim$ em X dada por $x \sim y \iff x = g \cdot y$, para algum $g \in G$, que será uma relação de equivalência. De fato:

Se G é um grupo agindo sobre X e sendo $x \sim y \iff x = g \cdot y$, para algum $g \in G$, temos que:

(i) (reflexiva) $x = e \cdot x \implies x \sim x,\ \forall\, x \in X.$

(ii) (simétrica) Sejam $x,\ y \in X$ tais que $x \sim y$.

$$x \sim y \iff x = g \cdot y,\ g \in G \implies g^{-1} \cdot x = g^{-1} \cdot (g \cdot y) = (g^{-1}g) \cdot y = e \cdot y = y$$
$$\implies y = g^{-1} \cdot x,\ g^{-1} \in G \implies y \sim x.$$

(iii) (transitiva) Sejam $x,\ y,\ z \in G$ tais que $x \sim y$ e $y \sim z$.

$$x \sim y \text{ e } y \sim z \iff x = g_1 \cdot y \text{ e } y = g_2 \cdot z,\ g_1,\ g_2 \in G$$
$$\implies x = g_1 \cdot y = g_1 \cdot (g_2 \cdot z) = (g_1 g_2) \cdot z,\ g_1,\ g_2 \in G \implies x \sim z.$$

Ou seja, $\sim$ é uma relação de equivalência em X.

Definição 80. A classe de equivalência $\overline{x}$, correspondente a relação de equivalência definida anteriormente, recebe o nome de órbita de x, e é denotada por $G \cdot x$. Note que

$$G \cdot x = \{y \in X;\ y \sim x\} = \{y \in X;\ y = g \cdot x,\ g \in G\} = \{g \cdot x \in X;\ g \in G\}.$$

Além disso, visto que órbitas são classes de equivalências, elas formam uma partição em X e temos que:

(i) $\forall\, x,\ y \in X$, ou $G \cdot x = G \cdot y$ ou $G \cdot x \cap G \cdot y = \varnothing$.

(ii) $X = \bigcup\limits_{x \in X} G \cdot x$.

(iii) $X = \dot{\bigcup\limits_{x \in T}} G \cdot x$, onde T é um conjunto de representantes da partição.

Outra estrutura interessante a ser definida, induzida pelo conceito de ação, é o de estabilizador.

Definição 81. Seja G um grupo agindo em X e seja $x \in X$. O subgrupo estabilizador de x, ou subgrupo de isotropia de x denotado por G_x, será o subgrupo $G_x = \{g \in G;\ g \cdot x = x\} \leq G$. G_x realmente será subgrupo de G pois:

Dados $g,\ h \in G_x$, sabemos que $g \cdot x = x$ e $h \cdot x = x$. $h \cdot x = x \implies h^{-1} \cdot (h \cdot x) = h^{-1} \cdot x \implies (h^{-1}h) \cdot x = h^{-1} \cdot x \implies x = h^{-1} \cdot x \implies h^{-1} \in G_x$.

Segue que $(gh^{-1}) \cdot x = g \cdot (h^{-1} \cdot x) = g \cdot x = x \implies gh^{-1} \in G_x$.

Portanto $G_x \leq G$.

A definição de órbita e do subgrupo estabilizador nos permite visualizar de uma nova forma várias estruturas de grupo já conhecidas.

Exemplo 82. Seja G um grupo agindo em si mesmo por conjugação (vide Exemplo 77). Neste caso, a órbita $G \cdot x$ de um elemento $x \in G$ coincide com a classe de conjugação de x, isto é, $G \cdot x = \{gxg^{-1} \in G;\ g \in G\} = x^G$.

Se H, subgrupo de G, age em G por conjugação, o subgrupo estabilizador H_x coincide com o $C_H(x)$, o centralizador de x em H. E caso $H = G$, $G_x = C_G(x)$.

No caso de H agindo por conjugação no conjunto dos subgrupos de G, isto é, pela ação $h \cdot K = hKh^{-1}$, a órbita de K coincide com o conjunto dos conjugados de K em H e o

subgrupo estabilizador de K (H_K) coincide com $N_H(K)$, o normalizador de K em H. E caso $H = G$, $G_K = N_G(K)$. Vale notar que todo subgrupo de K é normal em $N_G(K)$, e que $K \triangleleft G$ se, e somente se, $G_K = N_G(K) = K$.

Um teorema interessante ligando os conceitos de órbita e de estabilizador, definidos anteriormente, é o seguinte:

Teorema 83. ***(Teorema da Órbita-Estabilizador)***

Seja G um grupo agindo em X e seja $x \in X$. Então a cardinalidade da órbita de x é igual ao índice do subgrupo estabilizador de x em G, isto é:

$$|G \cdot x| = [G : G_x] .$$

Demonstração. Dado $x \in X$, defina $f : G \cdot x \longrightarrow \frac{G}{G_x}$ onde $f(g \cdot x) = gG_x$.

f está bem definida pois: dados $g \cdot x,\ h \cdot x \in G \cdot x$ tais que $g \cdot x = h \cdot x$, segue que $g \cdot x = h \cdot x \Longrightarrow (h^{-1}g) \cdot x = x \Longrightarrow h^{-1}g \in G_x \Longrightarrow gG_x = hG_x \Longrightarrow f(g \cdot x) = f(h \cdot x)$.

f é injetora, pois: dados $g \cdot x,\ h \cdot x \in G \cdot x$ tais que $f(g \cdot x) = f(h \cdot x)$, temos que $f(g \cdot x) = f(h \cdot x) \Longrightarrow gG_x = hG_x \Longrightarrow h^{-1}g \in G_x \Longrightarrow (h^{-1}g) \cdot x = x \Longrightarrow g \cdot x = h \cdot x$.

f é sobrejetora, pois: dado $gG_x \in G/G_x$ temos que $g \in G$, tomando $g \cdot x \in G \cdot x$ segue que $f(g \cdot x) = gG_x$.

Assim, segue que f é bijetora e concluímos que $|G \cdot x| = [G : G_x]$. ■

A partir desse resultado, podemos obter vários corolários interessantes.

Corolário 84. *Seja G um grupo agindo em X e $x \in X$, então $|G| = |G \cdot x| \cdot |G_x|$.*

Demonstração. Do teorema anterior, temos que $|G \cdot x| = [G : G_x]$. Utilizando o Teorema de Lagrange (40), temos que $|G| = |G_x| \cdot [G : G_x]$. Portanto, $|G| = |G_x| \cdot |G \cdot x|$. ■

Ou seja, dado um grupo G agindo num conjunto X e $x \in X$, a ordem do grupo G pode ser obtida como o produto entre a cardinalidade da órbita de x e a ordem do subgrupo estabilizador de x. Esse corolário nos dá uma nova ferramenta para contar os elementos de um grupo.

Corolário 85. *Seja G um grupo e $x \in G$, então $|x^G| = [G : C_G(x)]$.*

Demonstração. Tome $\alpha : G \times G \longrightarrow G$ a ação conjugação. Do Exemplo 82 temos que $G \cdot x = x^G$ e que $G_x = C_G(x)$. Pelo Teorema da Órbita-Estabilizador (83) segue que:

$$|x^G| = |G \cdot x| = [G : G_x] = [G : C_G(x)] \implies |x^G| = [G : C_G(x)] .$$

■

Corolário 86. *Seja G um grupo, $H \leq G$ e $X = \{gHg^{-1};\ g \in G\}$ o conjunto dos conjugados de H em G, então o número de conjugados de H em G será $|X| = [G : N_G(H)]$.*

Demonstração. Tome $\alpha : G \times \{\text{subgrupos de } G\} \longrightarrow \{\text{subgrupos de } G\}$ a ação conjugação. Por definição, temos que $G \cdot H = \{gHg^{-1};\ g \in G\} = X$ e do Exemplo 82 sabemos que $G_H = N_G(H)$. Utilizando o Teorema da Órbita-Estabilizador (83) segue que:

$$|X| = |G \cdot H| = [G : G_H] = [G : N_G(H)] \implies |X| = [G : N_G(H)]\,.$$

■

Proposição 87. *Seja G um grupo agindo em X e $x, y \in X$ tais que $y = gx$, para algum $g \in G$. Então $G_y = gG_xg^{-1}$ e $|G_x| = |G_y|$.*

Demonstração. Dado $gug^{-1} \in gG_xg^{-1}$, $ux = x$.

$$(gug^{-1})y = gug^{-1}gx = gux = gx = y$$
$$\implies (gug^{-1}) \in G_y \implies (gG_xg^{-1}) \subseteq G_y.$$

E, dado $v \in G_y$, $vy = y$.

$$vy = y \implies vgx = gx \implies g^{-1}vgx = g^{-1}gx = x$$
$$\implies (g^{-1}vg) \in G_x \implies v = g(g^{-1}vg)g^{-1} \in (gG_xg^{-1})$$
$$\implies G_y \subseteq (gG_xg^{-1}).$$

Portanto, temos que $G_y = gG_xg^{-1}$.

Agora, dado $g \in G$, tome $\varphi_g : G \longrightarrow G$ dada por $\varphi_g(u) = gug^{-1}$. A função φ_g é um isomorfismo e sendo assim, a restrição $\varphi_g\big|_{G_x} : G_x \longrightarrow \text{Im}\left(\varphi_g\big|_{G_x}\right)$ também será isomorfismo.

De onde concluímos que $|G_x| = |\text{Im}\left(\varphi_g\big|_{G_x}\right)| = |gG_xg^{-1}| = |G_y|$. ■

Definição 88. Uma ação de G em X é dita transitiva se ela tem somente uma órbita, isto é, se para todos $x,\ y \in X$, existe $g \in G$ tal que $y = g \cdot x$. Nesse caso, também dizemos que G age transitivamente em X.

Exemplo 89. A ação translação à esquerda (Exemplo 74) é transitiva. Basta ver que, dado $x \in G, \forall\, y \in G,\ yx^{-1} \in G \implies y = (yx^{-1})x \in G \cdot x \implies G = G \cdot x$.

Exemplo 90. Seja $H \leq G$, então G age transitivamente, pela ação translação à esquerda, em G/H.

Demonstração. Dado $xH \in G/H$, $\forall\, yH \in G/H$, $yx^{-1} \in G$ e temos que

$$yH = (yx^{-1})(xH) \in G \cdot xH \implies G/H = G \cdot xH.$$

■

Exemplo 91. $H \leq G$, G age transitivamente, pela ação conjugação, no conjunto dos conjugados de H em G.

Demonstração. Seja $X = \{tHt^{-1};\ t \in G\}$, dado $tHt^{-1} \in X$, $\forall\ sHs^{-1} \in X$, tome $g = st^{-1} \in G$.

$$gtHt^{-1}g^{-1} = st^{-1}tHt^{-1}(st^{-1})^{-1} = st^{-1}tHt^{-1}ts^{-1} = sHs^{-1}$$

$$\implies sHs^{-1} = gtHt^{-1}g^{-1} \in G \cdot (tHt^{-1}).$$

Logo, a ação é transitiva. ■

Proposição 92. *Seja $\alpha : G \times X \longrightarrow X$ uma ação e seja $\tilde{\alpha} : G \longrightarrow S_X$ onde $\tilde{\alpha}(g) : X \longrightarrow X$ dado por $(\tilde{\alpha}(g))(x) = \alpha(g,x)$, $\forall\, x \in X$. Então valem as seguintes afirmações:*

(i) Se $K = ker(\tilde{\alpha})$, então G/K age em X pela ação $(gK)x = gx$.

(ii) Se G age transitivamente, então G/K também o faz.

(iii) Se G age transitivamente, então $|ker(\tilde{\alpha})| \leq {}^{|G|}/_{|K|}$.

Demonstração.

(i) Sabemos que $\tilde{\alpha}$ é um homomorfismo pela demonstração da Proposição 78.

$K = \ker(\tilde{\alpha}) \implies \forall\, x \in X,\ Kx = ex = x$.

Dados $gK, hK \in G/K$, $(gK)(hKx) = (gK)(hx) = g(hx) = (gh)x = (gh)Kx = ((gK)(hK))x$. Logo, G/K age em X.

(ii) Suponha que G age transitivamente.

Dado $x \in X$, $G/K \cdot x = \{gKx \in X;\ gK \in G/K\}$. $\forall\, y \in X$, $y \in G \cdot x$, logo $\exists\, g' \in G$ tal que $y = g'x$.

Tome $g'K \in G/K$.

$g'Kx = g'x = y \implies y = g'Kx \in G/K \cdot x$. Portanto, G/K age transitivamente.

(iii) $G \cdot x = X$ pois G age transitivamente, logo $|G \cdot x| = |X|$. Pelo Corolário 84, sabemos que $|G| = |G_x| \cdot |G \cdot x| \implies |G| = |G_x| \cdot |X| \implies |G_x| = {}^{|G|}/_{|X|}$.

Por outro lado, $\ker(\tilde{\alpha}) = \{g \in G;\ \tilde{\alpha}(g) = \mathrm{id} \in S_X\}$. Logo, se $g \in \ker(\tilde{\alpha})$, então $gx = \mathrm{id}(x) = x \implies g \in G_x \implies \ker(\tilde{\alpha}) \subseteq G_x \implies |\ker(\tilde{\alpha})| \leq |G_x| = {}^{|G|}/_{|X|}$. ■

3.2 p-Grupos

Definição 93. Sejam p um número primo e G um grupo, não necessariamente finito. G é um p-grupo se todo elemento tem como ordem uma potência de p. Vale notar que, se G é p-grupo, todo $H \leq G$ também o será.

Caso H seja um p-grupo e $H \leq G$ para algum grupo G, também diremos que H é um p-subgrupo de G.

Exemplo 94. O grupo $\mathbb{Z}/27\mathbb{Z}$ é um 3-grupo, visto que as ordens de seus elementos deverão ser $3, 9$ ou 27, os divisores de $|\mathbb{Z}/27\mathbb{Z}| = 27$.

Exemplo 95. Considere o grupo multiplicativo $(\mathbb{C}/\{0\}, \cdot)$, $G = \{-1, 1, i, -i\} \leq (\mathbb{C}/\{0\}, \cdot)$ é um 2-subgrupo de $\mathbb{C}/\{0\}$.

Proposição 96. *Seja $H \triangleleft G$. Se H e G/H são ambos p-grupos, então G é um p-grupo.*

Demonstração. Dado $g \in G$, como G/H é p-grupo, segue que $(gH)^{p^n} = eH$, para algum $n \geq 1$.

$(gH)^{p^n} = eH \Longrightarrow (gH)^{p^n} = (g^{p^n})H = eH \Longrightarrow g^{p^n} \in H$.

Como H é p-grupo e $g^{p^n} \in H$, segue que $(g^{p^n})^{p^m} = g^{p^n \cdot p^m} = g^{p^{n+m}} = e \Longrightarrow g^{p^{n+m}} = e$.

Logo g tem como ordem uma potência de p e, sendo assim, G é um p-grupo. ■

Lema 97. *Se G é um grupo abeliano finito e p um número primo tal que p divide $|G|$, então existe um elemento em G com ordem p.*

Demonstração. Se $|G| = 1$, não existe tal p e não há o que fazer.

Se $|G| > 1$, suponha por indução que esse lema vale para todos grupos com ordem menor que $|G|$.

Se $|G| = p$, G é cíclico e qualquer gerador de G tem ordem p.

Se $|G| = n > p$, tome $H \leq G$ tal que $1 < |H| < |G|$. Tal H existe, pois, dado $h \in G$ com $h \neq e$, se $\langle h \rangle \neq G$, basta tomar $H = \langle h \rangle$, se $\langle h \rangle = G$, $h^p \neq e$ e então basta tomar $H = \langle h^p \rangle$, $\langle h^p \rangle$ serve pois $|\langle h^p \rangle| = |\{e, h^p, (h^p)^2, \ldots, (h^p)^{n/p - 1}\}| = {}^n/_p < n = |G|$.

Se p divide $|H|$, pela hipótese de indução, $\exists\, x \in H \subseteq G$ tal que $|x| = p$.

Se p não divide $|H|$. Pelo Teorema de Lagrange (40), temos que $|G| = |H| \cdot [G : H] \Longrightarrow p \,\big|\, |G| = |H| \cdot [G : H] \Longrightarrow p \,\big|\, [G : H] = |G/H| < |G|$.

G é abeliano, logo $H \triangleleft G$ e G/H é grupo.

Pela hipótese de indução, $\exists\, \overline{x} \in G/H$ tal que $|\overline{x}| = p$. Tome $\varphi : G \longrightarrow G/H$ o homomorfismo projeção canônica, sejam $x \in G$ tal que $\varphi(x) = \overline{x}$ e $r = |x|$.

$\varphi(x^r) = \varphi(e) = e$ e, por outro lado, $\varphi(x^r) = (\varphi(x))^r = \overline{x}^r$

$\Longrightarrow p|r \Longrightarrow r = kp,\ k \in \mathbb{Z} \Longrightarrow (x^k)^p = x^{kp} = x^r = e \Longrightarrow |x^k| = p$ com $x^k \in G$. ■

Teorema 98. *Se G é um grupo finito e p um número primo tal que p divide $|G|$, então existe um elemento em G com ordem p.*

Demonstração. Se G é abeliano, basta utilizar o Lema 97.

Suponha que G não é abeliano, logo $\exists\, x \in G$ tal que $x \notin Z(G)$.

Sabemos pelo Corolário 85 que $|x^G| = [G : C_G(x)]$.

$x \notin Z(G) \implies x^G \neq \{x\} \implies |x^G| = [G : C_G(x)] > 1 \implies |C_G(x)| < |G|$.

Suponha por indução que esse teorema vale para todo grupo com ordem menor que $|G|$.

Se p divide $|C_G(x)|$ e $|C_G(x)| < |G|$, pela hipótese de indução, $\exists\, y \in C_G(x) \subseteq G$ tal que $|y| = p$.

Se p não divide $|C_G(x)|$, então $p \,\big|\, [G : C_G(x)] = |x^G|$, pois $p \,\big|\, |G|$ e pelo Teorema de Lagrange (40) sabemos que $|G| = |C_G(x)| \cdot [G : C_G(x)]$.

Tomando a equação de classes de G (Teorema 37), temos que:

$$|G| = |Z(G)| + \sum_{x_i \notin Z(G)} |x_i^G|,$$

onde cada x_i pertence a uma classe de conjugação diferente.

Se p divide $C_G(x_i)$ para algum x_i, basta usar a argumentação anterior com a hipótese da indução.

Se p não divide $C_G(x_i)$ para todos x_i, então $p \,\big|\, [G : C_G(x_i)] = |x_i^G| \implies p \,\big|\, \sum_{x_i \notin Z(G)} |x_i^G|$. Como $p \,\big|\, |G| = |Z(G)| + \sum_{x_i \notin Z(G)} |x_i^G|$, segue que $p \,\big|\, |Z(G)$.

$Z(G)$ é abeliano, logo, pelo Lema 97, $\exists\, y \in Z(G) \subseteq G$ tal que $|y| = p$. ■

Corolário 99. *G é um p-grupo finito se, e somente se, $|G|$ é uma potência de p.*

Demonstração. $(\Rightarrow)$ G é um p-grupo finito.

Suponha, por absurdo, que um número primo $q \neq p$ divide $|G|$. Pelo Teorema 98, $\exists g \in G$ tal que $|g| = q$ e sabemos que $q \neq p^n$, $\forall\, n \in \mathbb{Z}$, um absurdo pois G é p-grupo.

$(\Leftarrow)$ $|G| = p^m$, com $m \geq 1$.

$\forall\, g \in G$, $|g|$ divide $|G| \implies |g| = p^n$, onde $1 \leq n \leq m$. Logo, G é um p-grupo finito. ■

Proposição 100. *Se $G \neq \{e\}$ é um p-grupo finito, então $Z(G) \neq \{e\}$.*

Demonstração. G é um p-grupo finito, logo, $|G| = p^m$, com $m \geq 1$.

Tome a equação das classes de conjugação de G (Teorema 37) junto do Corolário 85.

$$|G| = |Z(G)| + \sum_{x_i \notin Z(G)} [G : C_G(x_i)]\,.$$

$x_i \notin Z(G) \implies C_G(x_i)$ é um subgrupo próprio de $G \implies |C_G(x_i)| < |G| = p^m$, e como $|C_G(x_i)|$ divide $|G|$, temos que $|C_G(x_i)| = p^{n_i}$, com $1 \leq n_i < m \implies [G : C_G(x_i)] = p^{m-n_i}$.

Assim, p divide $[G : C_G(x_i)] \implies p \Big| \sum_{x_i \notin Z(G)} [G : C_G(x_i)]$.

Como p também divide $|G|$, temos que $p \Big| |Z(G)| = |G| - \sum_{x_i \notin Z(G)} [G : C_G(x_i)]$. Pelo Lema 97, existe um elemento $z \in Z(G)$, $z \neq e$, tal que $z^p = e$, e assim concluímos que $Z(G) \neq \{e\}$.

■

Corolário 101. *Se p é primo, então todo grupo de ordem p^2 é abeliano.*

Demonstração. Seja G um grupo tal que $|G| = p^2$, com p primo. Pelo Corolário 99, sabemos que G é p-grupo e, pelo resultado anterior, temos que $Z(G) \neq \{e\}$.

$Z(G) \neq \{e\} \implies |Z(G)| = p$ ou p^2.

Se $|Z(G)| = p^2 \implies Z(G) = G \implies G$ é abeliano.

Se $|Z(G)| = p \implies [G : Z(G)] = |G/Z(G)| = p \implies G/Z(G)$ é cíclico e, pelo Teorema 49, temos que G é abeliano também. ■

Teorema 102. *Seja G um p-grupo finito, então valem as seguintes afirmações:*

(i) $H \lneqq G$, isto é, H é subgrupo próprio de $G \implies H \lneqq N_G(H)$.

(ii) Todo subgrupo maximal de G é normal e tem índice p.

Demonstração.

(i) Se $H \lhd G$, então $N_G(H) = G$ e segue que H é próprio em $N_G(H)$.

Se $H \not\lhd G$, $N_G(H) \neq G$. Seja X o conjunto de todos os conjugados de H em G, isto é, $X = \{gHg^{-1};\ g \in G\}$. Pelo Corolário 86 segue que $|X| = [G : N_G(H)]$.

Sendo G um p-grupo finito, sabemos que $|G| = p^n$ para algum $n \in \mathbb{N}$, e como $[G : N_G(H)]$ divide $|G|$, temos que $|X| = [G : N_G(H)] = p^m$ onde $0 < m < n$.

Consideremos agora H agindo por conjugação em X, $H = eHe^{-1} \in X$ e a órbita de H será $H \cdot H = \{H\}$ visto que $\forall\, h \in H$, $hHh^{-1} = H$.

Por um lado, sabemos que a cardinalidade de cada órbita gerada pela ação de H em X deve dividir $|H|$, que é uma potência de p, devido o Corolário 84. Por outro lado, como as órbitas formam uma partição de X, o somatório de suas cardinalidades deve ser igual à $|X| = p^m$. Como $|\{H\}| = 1$, devem existir pelo menos outras $p - 1$ órbitas em X com cardinalidade 1.

Assim, existirá um conjugado $g_0Hg_0^{-1} \neq H$ com órbita $\{g_0Hg_0^{-1}\}$ e teremos que $\forall\, h \in H$, $hg_0Hg_0^{-1}h^{-1} = g_0Hg_0^{-1} \implies g_0^{-1}hg_0Hg_0^{-1}h^{-1}g_0 = H \implies g_0^{-1}hg_0 \in N_G(H)$.

Suponha por absurdo que $\forall\, h \in H$, $g_0^{-1}hg_0 \in H \implies$
$h = g_0(g_0^{-1}hg_0)g_0^{-1} \in g_0Hg_0^{-1} \implies H \subseteq g_0Hg_0^{-1}$, como $|H| = |g_0Hg_0^{-1}|$, temos que $H = g_0Hg_0^{-1}$, um absurdo. Logo existe $h_0 \in H$ tal que $g_0^{-1}h_0g_0 \notin H$ e como $g_0^{-1}h_0g_0 \in N_G(H)$, segue que H é subgrupo próprio de $N_G(H)$.

(ii) Dado H subgrupo maximal em G, temos $H \lneqq G$, e por (i), segue que $H \lneqq N_G(H) \implies N_G(H) = G$, ou seja, $H \lhd G$. Pela Proposição 67, segue que $[G : H] = p$. ■

Lema 103. *Dados $n > 0$ e $q \in \mathbb{Q}$, $q > 0$, existe somente uma quantidade finita de n-uplas $(i_1, \ldots, i_n)$ de inteiros positivos tais que:*

$$q = \sum_{j=1}^{n} \left(\frac{1}{i_j} \right).$$

Demonstração. Para a demonstração, veja "Lemma 4.9", p. 77, (ROTMAN, 1999). ■

Teorema 104. *Para todo $n \geq 1$, existe apenas uma quantidade finita de grupos finitos com exatamente n classes de conjugação.*

Demonstração. Seja G um grupo finito com exatamente n classes de conjugação. Tomemos a equação das classes de conjugação (Teorema 37) junto do Corolário 85:

$$|G| = |Z(G)| + \sum_{x_j \notin Z(G)} [G : C_G(x_j)].$$

Sabendo que $Z(G)$ é formado pelas classes de conjugação com apenas um elemento, se $m = |Z(G)|$ e n for o número total de classes de conjugação de G, podemos reescrever a equação como:

$$|G| = |Z(G)| + \sum_{j=m+1}^{n} [G : C_G(x_j)].$$

Dividindo ambos os lados da igualdade por $|G|$, teremos que:

$$1 = \frac{|G|}{|G|} = \frac{m}{|G|} + \frac{\sum_{j=m+1}^{n} [G : C_G(x_j)]}{|G|} = \underbrace{\frac{1}{|G|} + \ldots + \frac{1}{|G|}}_{m \text{ vezes}} + \sum_{j=m+1}^{n} \frac{[G : C_G(x_j)]}{|G|}$$

$$= \underbrace{\frac{1}{|G|} + \ldots + \frac{1}{|G|}}_{m \text{ vezes}} + \sum_{j=m+1}^{n} \frac{1}{|C_G(x_j)|}.$$

Tomando $i_j = |G|$ para $1 \leq j \leq m$ e $i_j = |C_G(x_j)|$ para $m + 1 \leq j \leq n$, temos que $1 = \sum_{j=1}^{n} \left(\frac{1}{i_j} \right)$. Pelo lema anterior, existe somente uma quantidade finita de n-uplas satisfazendo essa equação, logo existirá um número M igual ao maior valor entre todos os i_j's possíveis. Portanto, se G é um grupo finito com exatamente n classes de conjugação, $|G|$ será no máximo M.

Assim, dado $n \in \mathbb{N}$, os grupos finitos com exatamente n classes de conjugação deverão ter ordem no máximo $|M|$, ou seja, teremos uma quantidade finita de ordens possíveis para esses grupos. E dada uma ordem, pelo Corolário 64, sabemos que existirá uma quantidade finita de grupos com tal ordem.

De onde concluímos que existirá uma quantidade finita de grupos finitos com exatamente n classes de conjugação. ■

Teorema 105. *Se $|G| = p^n$, com p primo, e se $0 \leq k \leq n$, então G contém um subgrupo normal de ordem p^k.*

Demonstração. Para demonstrar esse resultado, faremos indução sobre n.

Caso $n = 0$: $|G| = \{e\}$ e não há o que mostrar.

Suponha que o resultado vale para $n - 1$:

Dado k tal que $0 \leq k \leq n$.

Se $k = 0$, teremos que $p^k = p^0 = 1$ e $H = \{e\}$ é um subgrupo normal de ordem p^k.

Se $k \neq 0$, então $1 \leq k \leq n$.

Pela Proposição 100, sabemos que $Z(G) \neq \{e\}$. Como $Z(G)$ é um p-subgrupo finito, pelo Teorema 98, existe $a \in Z(G)$ com ordem p.

$\langle a \rangle \triangleleft G$, logo $G^* = G/\langle a \rangle$ é grupo e $|\langle a \rangle| = p \implies |G^*| = |G/\langle a \rangle| = p^{n-1}$.

Como $G/\langle a \rangle$ é um grupo com ordem p^{n-1}, vale a hipótese de indução e, para todo s tal que $0 \leq s \leq (n-1)$, existe um subgrupo $H^* \triangleleft G/\langle a \rangle$ com $|H^*| = p^s$.

$1 \leq k \leq n \implies 0 \leq k-1 \leq n-1$, assim, tomemos $s = k - 1$. Pelo Teorema da Correspondência 66, segue que existe um subgrupo $H \triangleleft G$ tal que $H^* = H/\langle a \rangle$ e $[G : H] = [G^* : H^*] = \frac{p^{n-1}}{p^s} = p^{n-(s+1)} \implies |H| = p^{s+1} = p^{(k-1)+1} = p^k$.

Assim, temos que H é um subgrupo normal em G com ordem p^k, com $0 \leq k \leq n$. ■

3.3 Teoremas de Sylow

Definição 106. Seja p um número primo, então $P \leq G$ é p-subgrupo de Sylow de G se P for um p-subgrupo e for maximal em relação a outros p-subgrupos de G, isto é, se $Q \lneq G$ é um p-subgrupo e $P \leq Q$, então $P = Q$.

Lema 107. *Se p é um número primo e b um inteiro positivo tal que $p \nmid b$, então, para todo $n \geq 0$, p não divide o coeficiente binomial $\binom{bp^n}{p^n}$.*

Demonstração. Para a demonstração, veja "Lemma 4.16", p. 80, (ROTMAN, 1999). ■

Teorema 108. ***(1º Teorema de Sylow)*** *Seja p um número primo e G um grupo finito, então G tem pelo menos um p-subgrupo de Sylow.*

Demonstração. Caso p não divida $|G|$, $p^0 = 1$ será a maior potência de p que divide $|G|$, sendo assim $\{e\}$ será o único p-subgrupo de G, e então $\{e\}$ será o único p-subgrupo de Sylow de G.

Caso p divida $|G|$, podemos escrever $|G| = bp^n$, onde p^n é a maior potência de p que divide $|G|$, com isso, também temos que mdc$(b,\ p) = 1$.

Seja $X = \{S \subseteq G;\ |S| = p^n\}$. X é a família de subconjuntos de G com p^n elementos, sendo assim, teremos que $|X| = \binom{bp^n}{p^n}$. Pelo lema anterior, sabemos que $p \nmid \binom{bp^n}{p^n} = |X|$.

Considere G agindo em X via translação à esquerda, isto é, pela ação dada por $g \cdot S = \{gs \in G;\ s \in S\}$, onde $g \in G$ e $S \in X$. Sabemos que essas órbitas formam uma partição de X, sendo t a quantidade de órbitas dessa ação, tome $\{S_1, ..., S_t\}$ um conjunto de representantes dessa partição e teremos:

$$X = \bigdot{\bigcup_{1 \leq i \leq t}} G \cdot S_i \implies |X| = \sum_{1 \leq i \leq t} |G \cdot S_i|.$$

Note que, caso p divida $|G \cdot S_i|$ para $1 \leq i \leq t$, teríamos que $p \mid \sum_{1 \leq i \leq t} |G \cdot S_i| = |X|$, uma contradição.

Logo, deve existir pelo menos uma órbita $G \cdot S_{i_0}$, com $1 \leq i_0 \leq t$, tal que $p \nmid |G \cdot S_{i_0}|$. Assim, tomando o subgrupo estabilizador $G_{S_{i_0}}$, teremos que pelo Teorema da Órbita-Estabilizador (83) que $\left[G : G_{S_{i_0}}\right] = |G \cdot S_{i_0}|$.

Como $p \nmid \left[G : G_{S_{i_0}}\right]$ e $bp^n = |G| = \left[G : G_{S_{i_0}}\right] \cdot |G_{S_{i_0}}|$. Devemos ter que $|G_{S_{i_0}}| = b'p^n \geq p^n$, onde b' divide b.

Por outro lado, dados $g \in G_{S_{i_0}}$ e $s \in S_{i_0}$, $gs \in g \cdot S_{i_0} = S_{i_0}$, e dado $h \in G_{S_{i_0}}$, $h \neq g$, teremos que $gs \neq hs$. Fixado $s_0 \in S_{i_0}$, teremos que a aplicação $G_{S_{i_0}} \longrightarrow S_{i_0}$ dada por $g \longmapsto gs_0$ será injetora, logo $|G_{S_{i_0}}| \leq |S_{i_0}| = p^n$. Assim, devemos ter que $|G_{S_{i_0}}| = b'p^n \leq p^n \implies b' = 1$ e $|G_{S_{i_0}}| = p^n$, pelo Corolário 99, temos que $G_{S_{i_0}}$ é um p-subgrupo de G.

Seja Q um p-subgrupo de G tal que $Q \subsetneq G$ e $G_{S_{i_0}} \leq Q$, ainda pelo Corolário 99 $|Q|$ é uma potência de p e como $G_{S_{i_0}} \leq Q$, $|Q|$ será tal que $|G_{S_{i_0}}| = p^n$ divide $|Q|$ e $|Q|$ divide $|G| = bp^n$ teremos que $|Q| = p^n \implies G_{S_{i_0}} = Q$. Logo, $G_{S_{i_0}}$ é um p-subgrupo de Sylow de G. ■

Lema 109. *Seja G um grupo finito e P um p-subgrupo de Sylow de G, então:*

(i) $|N_G(P)/P|$ e p são coprimos.

(ii) Dado $a \in G$, se $|a|$ é uma potência de p e $aPa^{-1} = P$, então $a \in P$.

Demonstração.

(i) Suponha por absurdo que $|N_G(P)/P|$ e p não são coprimos, como p é primo, devemos ter que p divide $|N_G(P)/P|$. Pelo Teorema 98, existe um elemento $hP \in N_G(P)/P$ com ordem p, logo, o subgrupo $S^* = \langle hP \rangle$ tem ordem p.

Pelo Teorema da Correspondência (66), existe um subgrupo $S \leq N_G(P)$ onde $P \triangleleft S$ e $S/P \cong S^*$. Como P e S/P são p-grupos, pela Proposição 96, também teremos que S é p-grupo. Uma contradição com a maximalidade de P.

(ii) $aPa^{-1} = P$, logo $a \in N_G(P)$. Suponha por absurdo que $a \notin P$, logo $aP \neq P \in N_G(P)/P$. $|a| = p^n$, para algum $n \geq 1$, logo $(aP)^{p^n} = a^{p^n}P = P \implies$ a ordem $|aP|$ divide p^n e como $(aP)^1 \neq P$ temos que a ordem $|aP| \neq 1$. Assim, $|aP| = p^k$, com $1 \leq k \leq n$.

$|aP| = |\langle aP \rangle|$ divide $|N_G(P)/P|$ pois $\langle aP \rangle \leq N_G(P)/P$ e p divide $|aP| = p^k \implies p$ divide $|N_G(P)|$, o que contradiz o item (i). ■

Teorema 110. ***(2º Teorema de Sylow)***

Seja P um p-subgrupo de Sylow de um grupo finito G. Se Q é um p-subgrupo de G, então Q está contido em algum conjugado de P por G.

Demonstração. Seja $X = \{gPg^{-1};\ g \in G\}$ o conjunto dos conjugados de P em G, considere P agindo via conjugação em X. $P = ePe^{-1} \in X$ e, para todo $x \in P$, $xPx^{-1} = P$. Logo $\{P\}$ é uma órbita com apenas um elemento. Iremos mostrar que $\{P\}$ é a única órbita com apenas um elemento.

Seja $g_0 \in G$ tal que $g_0Pg_0^{-1}$ tenha uma órbita com apenas um elemento, isto é, $P \cdot g_0Pg_0^{-1} = \{g_0Pg_0^{-1}\}$. Para todo $x \in P$, $xg_0Pg_0^{-1}x^{-1} = g_0Pg_0^{-1} \implies (g_0^{-1}xg_0)P(g_0^{-1}xg_0)^{-1} = P$, além disso, como $|x|$ é uma potência de p, $|(g_0^{-1}xg_0)|$ também será. Pelo item (ii) do lema anterior, $(g_0^{-1}xg_0) \in P,\ \forall\ x \in P \implies (g_0^{-1}Pg_0) \subseteq P$. Mas $|(g_0^{-1}Pg_0)| = |P| \implies P = g_0Pg_0^{-1}$. Portanto, $P \cdot P = \{P\}$ é a única órbita com apenas um elemento.

Pelo Teorema da Órbita-Estabilizador (83), teremos que a cardinalidade de cada órbita divide $|P|$, e sendo $\{P\}$ a única órbita de cardinalidade 1, as outras órbitas deverão ter como cardinalidade múltiplos de p, visto que $|P|$ é uma potência de p. Tais órbitas formam uma partição em X, e a soma de suas cardinalidades resultará em $|X|$, assim teremos $|X| \equiv 1 \mod p$.

Seja Q um p-subgrupo de G, considere agora Q agindo em $X = \{gPg^{-1};\ g \in G\}$ por conjugação. Pelo mesmo argumento, utilizando o Teorema da Órbita-Estabilizador, sabemos que a cardinalidade de cada órbita divide $|Q|$, e assim, deverão ser múltiplas de p. E como as órbitas dessa ação foram uma partição em X, sabemos que a soma dessas cardinalidades resultará em $|X|$. Sabendo que $|X| \equiv 1 \mod p$, deveremos ter pelo menos uma dessas órbitas com cardinalidade 1, isto é, existe $g_1 \in G$ tal que, para todo $q \in Q$, $qg_1Pg_1^{-1}q^{-1} = g_1Pg_1^{-1}$ e, de forma análoga, utilizando novamente o lema anterior, teremos que $(g_1^{-1}qg_1) \in P \implies (g_1^{-1}Qg_1) \subseteq P \implies Q \subseteq g_1Pg_1^{-1}$. ■

Corolário 111. *Seja P um p-subgrupo de Sylow de um grupo finito G. Então todos p-subgrupo de Sylow de G são conjugados de P.*

Demonstração. Seja Q um p-subgrupo de Sylow de G, pelo teorema anterior, existe $g \in G$ tal que $Q \subseteq gPg^{-1}$.

Note que, gPg^{-1} é um p-subgrupo pois, dado $gxg^{-1} \in gPg^{-1}$, $x \in P \implies |x| = p^n$ para algum $n \in \mathbb{N}$, e assim teremos que $(gxg^{-1})^{p^n} = \underbrace{(gxg^{-1})(gxg^{-1})...(gxg^{-1})}_{p^n \text{ vezes}} =$

$g(\underbrace{x...x}_{p^n \text{ vezes}})g^{-1} = gx^{p^n}g^{-1} = e$. Assim temos $Q \leq gPg^{-1}$. Pela maximalidade de Q temos $Q = gPg^{-1}$. ■

Corolário 112. *Seja p um número primo. Um grupo finito G tem um único p-subgrupo de Sylow P se, e somente se, $P \triangleleft G$.*

Demonstração. Sabemos que, se P é um p-subgrupo de Sylow, então seus conjugados também o serão. Se P é único, então seus conjugados deverão coincidir com P, logo $P \triangleleft G$. Por outro lado, se P é um p-subgrupo de Sylow e $P \triangleleft G$, então P será igual seus conjugados, de forma que haverá apenas um p-subgrupo de Sylow. ■

Teorema 113. ***(3º Teorema de Sylow)*** *Sejam G um grupo finito e p um número primo, se r_p é a quantidade de p-subgrupos de Sylow em G, então r_p divide $|G|$ e $r_p \equiv 1 \mod p$.*

Demonstração. Pelo Corolário 111, sabemos que dado P um p-subgrupo de Sylow de G, os p-subgrupos de Sylow de G serão todos conjugados de P. Sendo X o conjunto dos conjugados de P, $|X| = r_p$ será a quantidade de p-subgrupos de Sylow em G. Pelo desenvolvimento feito na demonstração do 2º Teorema de Sylow (110), já sabemos que $r_p \equiv 1 \mod p$. Por outro lado, pelo Corolário 86, temos que $r_p = [G : N_G(P)]$, e como $|G| = [G : N_G(P)]\,|N_G(P)|$, temos que r_p divide $|G|$.

Teorema 114. *Seja p um número primo e G um grupo finito. Se p^n, com $n \geq 0$, é a maior potência de p que divide $|G|$, então todo p-subgrupo de Sylow de G tem ordem p^n.*

Demonstração. Caso p não divida $|G|$, $p^0 = 1$ será a maior potência de p e sendo assim $\{e\}$ será o único p-subgrupo de G, sendo então $\{e\}$ o único p-subgrupo de Sylow de G.

Caso p divida $|G|$, podemos escrever $|G| = bp^n$, onde p^n é a maior potência de p que divide $|G|$, com isso, também temos que mdc$(b,\, p) = 1$. Seja P um p-subgrupo de Sylow de G. Para mostrar que $|P| = p^n$, mostraremos que $[G : P]$ e p são coprimos.

Sabemos que $P \leq N_G(P) \leq G$, e pelo Corolário 41, temos que $[G : P] = [G : N_G(P)]\,[N_G(P) : P]$, logo é suficiente provar que cada um dos fatores é coprimo com p.

$[G : N_G(P)] = r_p$ é o número de conjugados de P, pelo 3º Teorema de Sylow (113), temos que $[G : N_G(P)] \equiv 1 \mod p$ e segue que $[G : N_G(P)]$ e p são coprimos. Por outro lado, $[N_G(P) : P] = |N_G(P)/P|$ e p são coprimos pelo Lema 109.

P é p-grupo, logo $|P| = p^k$ com $k \leq n$, e $[G : P] = {}^{|G|}/_{|P|} = {}^{bp^n}/_{p^k} = bp^{n-k}$. Como p e $[G : P]$ são coprimos, devemos ter $n - k = 0 \implies n = k \implies |P| = p^n$. ■

Corolário 115. *Seja G um grupo finito e p um número primo. Se p^k divide $|G|$, então G tem um subgrupo de ordem p^k.*

Demonstração. Se p^k divide $|G|$, podemos escrever $|G| = bp^n$, onde $n \geq k$ e mdc$(b,\ p) = 1$. Dado P um p-subgrupo de Sylow de G, $|P| = p^n$ e vale o Teorema 105, logo existe um subgrupo $H \leq P \leq G$ com $|H| = p^k$. ■

Teorema 116. *Seja G um grupo finito e $K \triangleleft G$. Se P é um p-subgrupo de Sylow de K, para algum p primo, então $G = KN_G(P)$.*

Demonstração. Dado $g \in G$, $gKg^{-1} = K$ pois $K \triangleleft G$ e também $P \leq K \implies gPg^{-1} \leq gKg^{-1} = K$.

gPg^{-1} é um p-subgrupo pois, dado $gxg^{-1} \in gPg^{-1}$, $x \in P \implies |x| = p^n$ para algum $n \in \mathbb{N}$, e assim $(gxg^{-1})^{p^n} = \underbrace{(gxg^{-1})(gxg^{-1})...(gxg^{-1})}_{p^n \text{ vezes}} = g(\underbrace{x...x}_{p^n \text{ vezes}})g^{-1} = gx^{p^n}g^{-1} = e$.

gPg^{-1} é maximal em relação a outros p-subgrupos de K pois, se $Q \lneqq K$ é um p-subgrupo tal que $gPg^{-1} \leq Q \lneqq K \implies P \leq g^{-1}Qg \lneqq g^{-1}Kg = K$ e como P é maximal, segue que $P = g^{-1}Qg \implies gPg^{-1} = Q$.

Assim, gPg^{-1} é um p-subgrupo de Sylow de K, e pelo Corolário 111, segue que gPg^{-1} deverá ser um conjugado de P em K, isto é, existe $k \in K$ tal que $kPk^{-1} = gPg^{-1}$.

Por fim, $kPk^{-1} = gPg^{-1} \implies P = k^{-1}gPg^{-1}k \implies P = (k^{-1}g)P(k^{-1}g)^{-1} \implies (k^{-1}g) \in N_G(P) \implies g = k(k^{-1}g) \in KN_G(P),\ \forall\, g \in G \implies G = KN_G(P)$. ■

Os Teoremas de Sylow, junto dos resultados obtidos a partir deles, formam um conjunto de poderosas ferramentas no estudo de grupos finitos, possibilitando a classificação dos grupos de uma determinada ordem, explicitando cada grupo possível, e também fornecendo informações sobre os grupos em si e a existência de subgrupos.

4 SOBRE OS GRUPOS ABELIANOS

4.1 Grupos Abelianos finitos

No decorrer desta seção, iremos trabalhar apenas com grupos abelianos. Como é de costume, fazemos uso da notação aditiva. Desta forma, temos que:

ab	$a+b$
e	0
a^{-1}	$-a$
ab^{-1}	$a-b$
HK	$H+K$
aH	$a+H$
produto direto	soma direta
$H \times K$	$H \oplus K$
$\bigtimes H_i$	$\bigoplus H_i$

Definição 117. Seja p um número primo. Um grupo G é dito grupo p-primário se G for p-grupo e for abeliano.

Lema 118. *(generalização do Teorema de Bézout)*
Sejam $x_1, \ldots, x_n$ números inteiros e $d = mdc(x_1, \ldots, x_n)$. Então existem inteiros $a_1, \ldots, a_n$ tais que $a_1x_1 + \ldots + a_nx_n = d$.

Demonstração. Para a demonstração, veja "Theorem VI.2", p. 487, (ROTMAN, 1999). ■

Teorema 119. ***(Teorema da Decomposição Primária)***

Todo grupo abeliano finito G pode ser decomposto numa soma direta de grupos p-primários.

Demonstração. Sejam G um grupo finito e $n = |G|$. Para todo $g \in G$, sabemos que $ng = 0$. Para cada número primo p tal que $p \mid n$, defina:

$$G_p = \{x \in G;\ p^m x = 0, \text{ para algum inteiro } m \geq 1\}.$$

Note que $G_p \leq G$, pois dados $x,\ y \in G_p$, $p^{m_1}x = 0$ e $p^{m_2}y = 0$, basta tomarmos $m = \max\{m_1,\ m_2\}$ para termos que mmc$(p^{m_1},\ p^{m_2}) = p^m$, e assim, $p^m(x-y) = p^mx + p^m(-y) = p^mx - p^my = 0 - 0 = 0$.

Seja $n = p_1^{\alpha_1} \cdot ... \cdot p_t^{\alpha_t}$ a decomposição de n em números primos, onde p_i são primos distintos e $\alpha_i \geq 1$. Tome $n_i = \dfrac{n}{p_i^{\alpha_i}}$, note que se $d \mid n_i$, então $p_i \nmid d$, $1 \leq i \leq t$, e assim teremos que mdc$(n_1, \ ... \ , \ n_t) = 1$.

Pela generalização do Teorema de Bézout (118), existem inteiros s_i tais que $s_1 n_1 + \cdots + s_t n_t = 1$, e segue que:

$$s_1 n_1 x + \cdots + s_t n_t x = x, \ \forall \, x \in G.$$

Mas cada parcela $s_i n_i x \in G_{p_i}$, pois $p_i^{\alpha_i} s_i n_i x = s_i n x = 0$, logo $G = \langle \bigcup_{i=1}^{t} G_{p_i} \rangle$.

Dado $i \in \{1, \ ... \ , \ t\}$, tome $x \in G_{p_i} \cap \langle \bigcup_{\substack{j=1 \\ j \neq i}}^{t} G_{p_j} \rangle$.

Por um lado temos que $x \in G_{p_i} \implies p_i^{m_i} x = 0$, para algum inteiro $m_i \geq 1$.

Por outro lado, $x \in \langle \bigcup_{\substack{j=1 \\ j \neq i}}^{t} G_{p_j} \rangle \implies x = \sum_{\substack{j=1 \\ j \neq i}}^{t} x_{p_j}$, onde para cada j teremos que $x_{p_j} \in G_{p_j} \implies p_j^{m_j} x_{p_j} = 0$, para algum inteiro $m_j \geq 1$.

Tomando $q = \prod_{\substack{j=1 \\ j \neq i}}^{t} p_j^{m_j}$, temos que mdc$(q, \ p_i^{m_i}) = 1$, portanto, existem inteiros r e s tais que $rq + s p_i^{m_i} = 1$, de onde segue que $rqx + s p_i^{m_i} x = x$.

Porém $rqx + s p_i^{m_i} x = 0 + 0 = 0$, assim temos que $x = 0$ e $G_{p_i} \cap \langle \bigcup_{\substack{j=1 \\ j \neq i}}^{t} G_{p_j} \rangle = \{0\}$.

Como $G = \langle \bigcup_{i=1}^{t} G_{p_i} \rangle$ e, para $1 \leq i \leq t$, $G_{p_i} \cap \langle \bigcup_{\substack{j=1 \\ j \neq i}}^{t} G_{p_j} \rangle = \{0\}$, pelo Teorema 71, segue que $G = \bigoplus_{i=1}^{t} G_{p_i}$, isto é, G é uma soma direta dos subgrupos G_{p_i}, os quais são p-primários por definição. ■

Definição 120. Os subgrupos $G_p \leq G$, da demonstração anterior, recebem o nome de componentes p-primários de G.

Definição 121. Um conjunto finito $X = \{x_1, \ x_2, \ ... \ , \ x_r\}$ de elementos não nulos de um grupo abeliano G é dito independente se, dados $m_1, \ m_2, \ ... \ , \ m_r$ inteiros tais que $m_1 x_1 + m_2 x_2 + \cdots + m_r x_r = 0$, tivermos que $m_i x_i = 0$, $1 \leq i \leq r$.

A noção de independência definida anteriormente se assemelha em muito com a noção de independência linear dos espaços vetoriais. Por exemplo, se G for um grupo de ordem p, com p primo, então G será um espaço vetorial sobre o corpo $(\mathbb{Z}/p\mathbb{Z}, \ +, \ \cdot)$ e os conceitos de independência entre os elementos de G e independência linear entre os vetores de G, um $(\mathbb{Z}/p\mathbb{Z})$-espaço vetorial, serão equivalentes. Basta ver que

$$m_i x_i = 0 \iff p \mid m_i \iff \overline{m_i} = \overline{0},$$

onde $1 \leq i \leq r$, na notação da definição acima.

Lema 122. *Seja $\{x_1, \ ... \ , \ x_r\}$ um conjunto de elementos não nulos de um grupo abeliano G. Então $\{x_1, \ ... \ , \ x_r\}$ é independente se, e somente se, $\langle x_1, \ x_2, \ ... \ , \ x_r\rangle = \langle x_1\rangle \oplus ... \oplus \langle x_r\rangle$.*

Demonstração. $(\Rightarrow)$ Se $y \in \langle x_i\rangle \cap \langle\{x_j; \ j \neq i\}\rangle$, então existem inteiros $m_1, \ ... \ , \ m_r$ tais que $y = -m_i x_i = \sum_{j\neq i} m_j x_j \implies \sum_{k=1}^{r} m_k x_k = 0$.

Pela independência de $\{x_1, \ ... \ , \ x_r\}$, temos que $m_k x_k = 0$ para todo k, e em particular, $m_i x_i = 0$ e segue que $y = -m_i x_i = 0 \implies \langle x_i\rangle \cap \langle\{x_j; \ j \neq i\}\rangle = \{0\}$.

Assim, pelo Teorema 71, segue que $\langle x_1, \ x_2, \ ... \ , \ x_r\rangle = \langle x_1\rangle \oplus ... \oplus \langle x_r\rangle$.

$(\Leftarrow)$ Como $0 \in \langle x_1, \ x_2, \ ... \ , \ x_r\rangle$ tome $0 = \sum m_i x_i$.

Para cada j, temos que $-m_j x_j = \sum_{k\neq j} m_k x_k \in \langle x_j\rangle \cap \langle\{x_k; k \neq j\}\rangle = \{0\}$.

Portanto, para cada j, $m_j x_j = 0$ e temos que $\{x_1, \ ... \ , \ x_r\}$ é independente. ■

Definição 123. Seja p um número primo. Um grupo finito G é um p-grupo abeliano elementar se for isomorfo à $\underbrace{(\mathbb{Z}/p\mathbb{Z}) \times ... \times (\mathbb{Z}/p\mathbb{Z})}_{n \text{ vezes}}$ (em notação aditiva, $\underbrace{(\mathbb{Z}/p\mathbb{Z}) \oplus ... \oplus (\mathbb{Z}/p\mathbb{Z})}_{n \text{ vezes}}$), onde n é um número natural.

Corolário 124. *Sejam G um grupo abeliano finito e p um número primo tal que, para todo $g \in G$, $pg = 0$. Então G é um p-grupo abeliano elementar.*

Demonstração. Considere G enquanto um $(\mathbb{Z}/p\mathbb{Z})$-espaço vetorial, sendo $\{x_1, \ ... \ , \ x_r\}$ uma base do espaço vetorial G, temos que o subconjunto $\{x_1, \ ... \ , \ x_r\} \subseteq G$ é independente, pois a base é linearmente independente, e assim teremos que $G = \langle x_1, x_2, ..., x_r\rangle = \langle x_1\rangle \oplus ... \oplus \langle x_r\rangle$.

$\forall \ i \in \{1, \ 2, \ ... \ , \ r\}$, $px_i = 0 \implies |x_i| = p$. Assim, temos que $\langle x_i\rangle$ é um grupo cíclico de ordem p, pelo Teorema 62, $\langle x_i\rangle \cong \mathbb{Z}/p\mathbb{Z}$, onde $1 \leq i \leq r$, e então concluímos que:

$$G = \langle x_1\rangle \oplus ... \oplus \langle x_r\rangle \cong \underbrace{(\mathbb{Z}/p\mathbb{Z}) \oplus ... \oplus (\mathbb{Z}/p\mathbb{Z})}_{r \text{ vezes}}.$$

■

Lema 125. *Se $G = \langle x_1, \ ... \ , \ x_n\rangle$ e $a_1, \ ... \ , \ a_n$ são inteiros primos entre si, então existe um conjunto com n elementos que gera G no qual $a_1 x_1 + ... + a_n x_n$ é um de seus elementos.*

Demonstração. Para a demonstração, veja "Lemma 6.8", p. 130, (ROTMAN, 1999). ■

Teorema 126. ***(Teorema da Base)***

Todo grupo abeliano finito G pode ser decomposto numa soma direta de grupos cíclicos.

Demonstração. Seja n a menor cardinalidade de um subconjunto de elementos de G tal que G seja gerado por esses elementos. Podem existir vários subconjuntos $\{x_1, \ ... \ , \ x_n\} \subseteq G$ que geram G e da forma que definimos n, existirá pelo menos um. Agora, escolhamos um desses

subconjuntos tomando aquele que tiver o elemento com a menor ordem possível, digamos x_1 com ordem k.

Seja $H = \langle x_2, \ ... \ , \ x_n \rangle$, H é subgrupo próprio de G, devido a minimalidade de n. Fazendo indução na ordem de G, teremos que $|H| < |G|$ e então vale o teorema para H, ou seja, H é soma direta de grupos cíclicos.

Assim, basta mostrarmos que $G = \langle x_1 \rangle \oplus H$.

Já sabemos que $\big\langle \langle x_1 \rangle \cup H \big\rangle = \langle x_1, \ ... \ , \ x_n \rangle = G$. Tome $z \in \langle x_1 \rangle \cap H$ e suponha, por absurdo, $z \neq 0$. Temos que $z = a_1 x_1 = a_2 x_2 + ... + a_n x_n$, onde $a_1, \ ... \ , \ a_n \in \mathbb{Z}$ e $0 < a_1 < k$.

Seja $d = \text{mdc}(a_1, \ ... \ , \ a_n)$, defina $g = -({}^{a_1}/_{d})x_1 + ({}^{a_2}/_{d})x_2 + ... + ({}^{a_n}/_{d})x_n$. A ordem de g deverá ser menor que k, pois $dg = 0$ e $d \leq a_1 < k$.

Porém, como $({}^{a_1}/_{d}), \ ... \ , \ ({}^{a_n}/_{d})$ são primos entre si, pelo lema anterior, existirá um conjunto gerador de G com n elementos no qual figura g.

Contradizendo a minimalidade de k.

Logo, devemos ter que $z = 0$ e sendo assim, $\langle x_1 \rangle \cap H = \{0\}$. Utilizando o Teorema 71, segue que $G = \langle x_1 \rangle \oplus H$, isto é, G é uma soma direta de grupos cíclicos. ■

Corolário 127. *Todo grupo abeliano finito G pode ser decomposto numa soma direta de grupos cíclicos da forma $G = \bigoplus_{i=1}^{t} \langle x_i \rangle$ onde, sendo $m_i = |x_i|$, teremos $m_i \mid m_{i+1}$, $1 \leq i \leq t-1$.*

Demonstração. Utilizando o Teorema da Decomposição Primária (119), temos que $G = \bigoplus_{i=1}^{r} G_{p_i}$ onde os grupos G_{p_i} são p-primários.

Para cada grupo G_{p_i}, utilizando o Teorema da Base, teremos uma decomposição de G_{p_i} em grupos cíclicos. Para cada i, tomemos C_i o grupo cíclico de maior ordem que figura na decomposição de G_{p_i}, e seja $p_i^{\alpha_i} = |C_i|$.

Fazendo as devidas manipulações, substituindo os grupos G_{p_i} por suas decomposições na decomposição de G e alterando a ordem das componentes, conseguimos obter $G = K \oplus (C_1 \oplus ... \oplus C_r)$, onde K será a soma direta de todos as outras componentes restantes.

As ordens $|C_i| = p_i^{\alpha_i}$ são todas primas entre si, visto que p_i são todos primos distintos. Assim, pelo Corolário 70, temos que $C = (C_1 \oplus ... \oplus C_r)$ é um grupo cíclico de ordem $m = \prod_{i=1}^{r} p_i^{\alpha_i}$.

K é um grupo abeliano finito, logo podemos repetir esse processo para K, onde iremos obter $K = H \oplus D$, sendo D cíclico de ordem m' e uma soma direta de grupos cíclicos. Sendo D_i uma componentes na soma de D e originado na decomposição de G_{p_i}, teremos que $|D_i| = p_i^{\beta_i} \leq p_i^{\alpha_i}$, visto que C_i foi escolhido como grupo de maior ordem, logo $p_i^{\beta_i} \mid p_i^{\alpha_i}$, $1 \leq i \leq r$, e então $m' \mid m$.

Como G é finito, esse processo chegará ao fim após um número finito de repetições, digamos t vezes. Escrevendo $C = \langle x_t \rangle$, $m = m_t$, $D = \langle x_{t-1} \rangle$, $m' = m_{t-1}$, e assim por diante, teremos ao fim que $G = \bigoplus_{i=1}^{t} \langle x_i \rangle$ onde, $m_i = |x_i|$, teremos $m_i \mid m_{i+1}$, para $1 \leq i \leq t-1$. ■

Definição 128. Seja G um grupo abeliano finito, e $G = \bigoplus_{i=1}^{t} \langle x_i \rangle$ uma decomposição em soma direta de grupos cíclicos onde, sendo $m_i = |x_i|$, temos $m_i \mid m_{i+1}$, para $1 \leq i \leq t-1$. Então dizemos que os fatores invariantes de G são $(m_1, \ ... \ , \ m_t)$.

Proposição 129. *Se G e H são p-grupos abelianos elementares, então $d(G \oplus H) = d(G) + d(H)$.*

Demonstração. Para a demonstração, veja "Exercise 6.7", p. 130, (ROTMAN, 1999). ■

Definição 130. Seja m um inteiro positivo e G um grupo abeliano. Fixamos notação para os seguintes subgrupos de G:

(i) $mG = \{mg \in G; \ g \in G\}$

(ii) $G\,[m] = \{g \in G; \ mg = 0\}$.

De fato, tomando o homomorfismo $\varphi : G \longrightarrow G$ dada por $\varphi(g) = mg$, teremos $mG = \text{im}(\varphi)$ e $G\,[m] = \ker(\varphi)$, ambos subgrupos de G já conhecidos.

Proposição 131. *Se G é um grupo p-primário e $G = \bigoplus_{i=1}^{t} C_i$ uma decomposição em soma direta de grupos cíclicos. Então a quantidade de grupos cíclicos C_i com ordem maior ou igual à p^{n+1} é $d(p^nG/p^{n+1}G)$, o número mínimo de geradores para o grupo quociente $p^nG/p^{n+1}G$.*

Demonstração. Seja B_k a soma direta de todos os grupos cíclicos C_i com ordem p^k, e seja b_k a quantidade existente desses grupos. Agrupando os grupos C_i desta forma, teremos que $G = B_1 \oplus \cdots \oplus B_t$.

Dado n natural, temos que $p^nG = p^nB_{n+1} \oplus \cdots \oplus p^nB_t$, pois $p^nB_1 = ... = p^nB_n = 0$, e também $p^{n+1}G = p^{n+1}B_{n+2} \oplus ... \oplus p^{n+1}B_t$. Então:

$$p^nG/p^{n+1}G \cong \frac{p^nB_{n+1} \oplus p^nB_{n+2} ... \oplus p^nB_t}{p^{n+1}B_{n+2} \oplus ... \oplus p^{n+1}B_t} \cong p^nB_{n+1} \oplus \left(\frac{p^nB_{n+2}}{p^{n+1}B_{n+2}}\right) \oplus \cdots \oplus \left(\frac{p^nB_t}{p^{n+1}B_t}\right),$$

onde cada uma das componentes é, a menos de isomorfismo, um p-grupo abeliano elementar, soma direta dos grupos C_i.

Sendo C_i cíclico, temos que $d(C_i) = 1$, e sendo b_k a quantidade de grupos cíclicos C_i em cada componente, segue pela Proposição 129 que $d(p^nB_{n+1}) = b_{n+1}$, $d(p^nB_{n+2}/p^{n+1}B_{n+2}) = b_{n+2}$, e assim por diante, até $d(p^nB_t/p^{n+1}B_t) = b_t$.

Logo, pelo Proposição 129, segue que $d(p^nG/p^{n+1}G) = b_{n+1} + ... + b_t$. Sendo b_k a quantidade de grupos cíclicos C_i com ordem p^k, $b_{n+1} + ... + b_t$ representará a quantidade de grupos com ordem maior ou igual a p^{n+1} e temos o resultado. ■

Definição 132. Se G é um grupo finito p-primário e $n \in \mathbb{N}$, então:

$$U_p(n, \ G) = d(p^nG/p^{n+1}G) - d(p^{n+1}G/p^{n+2}G).$$

Note que, de acordo com teorema anterior, o número $U_p(n, G)$ nos informa, independentemente da decomposição em soma direta de grupos cíclicos adotada, a quantidade de grupos cíclicos com ordem p^{n+1} compondo G.

Sendo assim, quaisquer duas decomposições de G em soma direta de grupos cíclicos deverão ter a mesma quantidade de grupos cíclicos de mesma ordem.

Corolário 133. *Seja G um grupo p-primário, então quaisquer duas decomposições de G em soma direta de grupos cíclicos terão exatamente a mesma quantidade de grupos cíclicos de mesma ordem.*

Demonstração. A demonstração segue diretamente do teorema e da definição anterior. ■

Em outras palavras, o corolário anterior nos mostra que ao decompormos um grupo p-primário em soma direta de grupos cíclicos, essa decomposição será única, a menos da ordem em que figuram as componentes.

Proposição 134. *Sejam G e H grupos finitos p-primários. Então $G \cong H$ se, e somente se, $U_p(n,\ G) = U_p(n,\ H)$ para todo n natural.*

Demonstração. $(\Rightarrow)$ Seja $\varphi : G \longrightarrow H$ um isomorfismo. Para todo n natural temos que $\varphi(p^nG) = p^nH$, o que permite induzir um isomorfismo tal que $p^nG/p^{n+1}G \cong p^nH/p^{n+1}H$, e segue que:

$$\begin{aligned} U_p(n,\ G) &= d(p^nG/p^{n+1}G) - d(p^{n+1}G/p^{n+2}G) \\ &= d(p^nH/p^{n+1}H) - d(p^{n+1}H/p^{n+2}H) = U_p(n,\ H). \end{aligned}$$

$(\Leftarrow)$ $U_p(n,\ G) = U_p(n,\ H)$ para todo n natural, ou seja, ao decompormos G e H em soma direta de grupos cíclicos, teremos nas duas decomposições grupos cíclicos de mesma ordem figurando na mesma quantidade.

Como grupos cíclicos de mesma ordem são isomorfos e, neste caso, irão figurar em mesma quantidade em ambas decomposições, é possível construir um isomorfismo levando cada grupo cíclico da decomposição de G no seu correspondente na decomposição de H, decorrendo que $G \cong H$. ■

Definição 135. Se G é um grupo p-primário, então os divisores elementares de G são os números da sequência contendo $U_p(0,\ G)$ p's, $U_p(1,\ G)$ p^2's, ... , $U_p(t-1,\ G)$ p^t's, onde p^t é a ordem da componente cíclica de G de maior ordem da decomposição de G em soma direta de grupos cíclicos. Isto é, cada divisor elementar p^{n+1} figura $U_p(n, G)$ vezes na sequência.

Se G é um grupo abeliano finito, então seus divisores elementares são os divisores elementares de todas suas componentes p-primárias.

Note que, dado um grupo abeliano finito G, pelo Teorema da Decomposição Primária (119), podemos fazer sua decomposição em componentes p-primárias, as quais são determinadas pelos primos $p \mid |G|$. Sendo cada componente um grupo p-primário, pelo Teorema da Base (126), podemos decompô-las em grupos cíclicos de modo que as componentes cíclicas p-primárias de ordem p^{n+1} figurarão na decomposição $U_p(n, G)$ vezes. Ou seja, no fim desse processo, ao listarmos as ordens das componentes cíclicas p-primárias de G, teremos listado os divisores elementares de G.

Teorema 136. ***(Teorema Fundamental dos Grupos Abelianos Finitos)***

Sejam G e H grupos abelianos finitos. Então $G \cong H$ se, e somente se, G e H têm os mesmos divisores elementares.

Demonstração. $(\Rightarrow)$ Tome $\varphi : G \longrightarrow H$ um isomorfismo.

Dado p primo, considere a restrição $\varphi\big|_{G_p} : G_p \longrightarrow H$. $\varphi\big|_{G_p}$ será um homomorfismo injetor.

Se $g \in G_p \implies p^m g = 0, m \in \mathbb{Z} \implies p^m \varphi\big|_{G_p}(g) = \varphi\big|_{G_p}(p^m g) = \varphi\big|_{G_p}(0) = 0$, logo $\varphi\big|_{G_p}(G_p) \leq H_p$.

Dado $h \in H_p$, $p^{m'} h = 0$, $m' \in \mathbb{Z}$ e pela sobrejeção de φ, existe $x \in G$ tal que $\varphi(x) = h$. Logo, $0 = p^{m'} h = p^{m'} \varphi(x) = \varphi(p^{m'} x)$, de onde temos que $p^{m'} x \in \ker(\varphi) = \{0\}$, pois φ é injetor. Assim, devemos ter que $p^{m'} x = 0 \implies x \in G_p$.

Portanto, ao restringirmos o contradomínio à H_p, temos que $\varphi_p = \varphi\big|_{G_p} : G_p \longrightarrow H_p$ é sobrejetor, será isomorfismo e temos que $G_p \cong H_p$, para todo primo p.

Pela Proposição 134, segue que para todo primo p e $n \in \mathbb{N}$, $U_p(n, G_p) = U_p(n, H_p)$, de onde segue que G e H têm os mesmos divisores elementares.

$(\Leftarrow)$ Suponha que G e H tenham os mesmos divisores elementares.

Utilizando o Teorema da Decomposição Primária (119), façamos a decomposição de G e H em grupos p-primários e então, utilizando o Teorema da Base (126), façamos a decomposição de cada componente p-primária em grupos cíclicos, os quais serão p-primários.

Como observado anteriormente, G e H terem os mesmos divisores elementares significa que suas componentes cíclicas p-primárias de mesma ordem aparecem em mesma quantidade na decomposição de G e de H. Sendo duas componentes cíclicas de mesma ordem isomorfas entre si, é possível construir isomorfismos levando cada componente da decomposição de G em sua correspondente na decomposição de H, o que acarretará que $G \cong H$. ■

4.2 Grupos Abelianos

Definição 137. Seja G um grupo abeliano, então o conjunto de torção de G é definido e denotado por:

$$t(G) = \{g \in G;\ ng = 0, \text{ para algum inteiro não nulo } n\}.$$

$t(G)$ é subgrupo de G pois, $t(G) \neq \varnothing$, visto que $0 \in t(G)$.

E, dados x e $y \in t(G)$, existem n_1 e n_2 inteiros não nulos tais que $n_1 x = 0$ e $n_2 y = 0$, e segue que $(n_1 n_2)(x - y) = (n_1 n_2)x + (n_1 n_2)(-y) = (n_2(n_1 x)) - (n_1(n_2 y)) = 0 - 0 = 0$.

Exemplo 138. Seja $G = (\mathbb{C}/\{0\}, \cdot)$. Temos que

$$t(G) = \{z \in \mathbb{C}/\{0\};\ z^n = 1, \text{ para algum } n \in \mathbb{N}\} = \{\text{raízes da unidade}\}.$$

Definição 139. Seja G um grupo abeliano. G é dito grupo de torção se $t(G) = G$ e é dito grupo livre de torção se $t(G) = \{0\}$.

Proposição 140. *Seja G um grupo, então o grupo quociente $G/t(G)$ é livre de torção.*

Demonstração. Seja $g + t(G) \in t(G/t(G))$, existe um inteiro não nulo n tal que $n(g + t(G)) = 0$.

$n(g + t(G)) = 0 \implies ng + t(G) = 0 \implies ng \in t(G)$.

Como $ng \in t(G)$, existe um inteiro não nulo m tal que $m(ng) = 0 \implies (mn)g = 0 \implies g \in t(G) \implies g + t(G) = 0 \implies t(G/t(G)) = \{0\}$.

Ou seja, $G/t(G)$ é livre de torção. ■

A seguir, estudaremos grupos construídos a partir de produtos diretos infinitos (em notação aditiva, somas diretas infinitas). Nesse contexto, iremos generalizar o conceito de produto direto finito e, como é de costume na bibliografia, fazemos uma diferenciação entre os termos "produto direto" e "soma direta".

Definição 141. Sejam K um conjunto qualquer e $\{A_k;\ k \in K\}$ uma família de grupos.

O produto direto $\bigtimes_{k \in K} A_k$ é o grupo onde os elementos são todas as uplas $(a_k)_{k \in K}$ pertencentes ao produto cartesiano da família de grupos A_k e a operação é feita coordenada a coordenada, isto é, $(a_k) + (b_k) = (a_k + b_k)$.

A soma direta $\bigoplus_{k \in K} A_k$ é o subgrupo de $\bigtimes_{k \in K} A_k$ onde todos os elementos são uplas (a_k) em que $a_k \neq 0$ somente uma quantidade finita de vezes.

Vale notar que, no caso de produtos diretos finitos, ambas estruturas coincidirão e teremos $\bigoplus_{k \in K} A_k = \bigtimes_{k \in K} A_k$.

Lema 142. *Sejam G um grupo abeliano e $A \leq G$, então as seguintes afirmações são equivalentes:*

(i) Existe um subgrupo $B \leq G$ tal que $A \cap B = \{0\}$ e $A + B = G$.

(ii) Existe $B \leq G$ tal que, para cada $g \in G$, existem únicos $a \in A$ e $b \in B$ tais que $g = a + b$.

(iii) Existe um homomorfismo $\varphi : G/A \longrightarrow G$ *tal que* $\psi \circ \varphi \equiv 1_{G/A}$*, onde* $\psi : G \longrightarrow G/A$ *é a projeção canônica.*

(iv) Existe um homomorfismo $\pi : G \longrightarrow A$ *tal que* $\pi(a) = a$*, para todo* $a \in A$*.*

Demonstração. $(i) \Rightarrow (ii)$: Dado $g \in G = A + B$, tome $a_1,\ a_2 \in A$ e $b_1,\ b_2 \in B$ tais que $g = a_1 + b_1 = a_2 + b_2$. Logo $a_1 - a_2 = b_2 - b_1 \in A \cap B = \{0\} \implies a_1 - a_2 = 0 = b_2 - b_1 \implies a_1 = a_2$ e $b_1 = b_2$.

$(ii) \Rightarrow (iii)$ Dado $g + A \in G/A$, $g \in G$ e existem únicos $a_g \in A$ e $b_g \in B$ tais que $g = a_g + b_g \implies g + A = a_g + b_g + A = b_g + A$. Logo, a função $\varphi : G/A \longrightarrow G$ dada por $\varphi(g + A) = b_g$ estará bem definida.

Além disso, φ é homomorfismo pois, dado $h + A \in G/A$, teremos que $g + h = a_g + b_g + a_h + b_h = (a_g + a_h) + (b_g + b_h) = a' + b'$, onde $a' = a_g + a_h$ e $b' = b_g + b_h$, e de onde segue que $\varphi(g + A) + \varphi(h + A) = b_g + b_h = b' = \varphi(g + h + A)$.

Se $\psi : G \longrightarrow G/A$ é a projeção canônica, então, $\forall\ g + A \in G/A$, segue que $\psi \circ \varphi(g + A) = \psi(\varphi(g + A)) = \psi(b_g) = b_g + A = g + A \implies \psi \circ \varphi \equiv 1_{G/A}$.

$(iii) \Rightarrow (i)$ Dados $x + A,\ y + A \in G/A$ tais que $\varphi(x + A) = \varphi(y + A)$, teremos que $\psi(\varphi(x + A)) = \psi(\varphi(y + A)) \implies x + A = y + A$, logo φ é injetora e $\ker(\varphi) = \{0 + A\}$.

Seja $B = \text{im}(\varphi) \leq G$, dado $g \in A \cap B$, existe $x + A \in G/A$ tal que $\varphi(x + A) = g \implies x + A = \psi(\varphi(x + A)) = \psi(g) = 0 + A \implies x \in A \implies g = \varphi(x + A) = \varphi(0 + A) = 0 \implies A \cap B = \{0\}$.

Agora, dado $g \in G$, $\psi(g) = g + A \implies \varphi(\psi(g)) = \varphi(g + A) = b \in B = \text{im}(\varphi)$. E temos, $b + A = \psi(b) = \psi(\varphi(g + A)) = g + A \implies g - b = a \in A \implies g = a + b$, onde $a \in A$ e $b \in B$, logo $G = A + B$.

$(iv) \Rightarrow (i)$ Seja $B = \ker(\pi) \leq G$. $\pi(a) = a$ para todo $a \in A \implies A \cap B = \{0\}$.

Dado $g \in G$, $\pi(g) = a \in A$ e $\pi(a) = a$. Logo, $\pi(g - a) = 0$ e $g - a = b \in B = \ker(\pi) \implies g = a + b$, onde $a \in A$ e $b \in B$, logo $G = A + B$.

$(ii) \Rightarrow (iv)$ Dado $g \in G$, existem únicos $a \in A$ e $b \in B$ tais que $g = a + b$, e sendo a único, podemos tomar $\pi : G \longrightarrow A$ dada por $\pi(g) = a$.

π é homomorfismo pois, dados $g_1,\ g_2 \in G$, $g_1 = a_1 + b_1$ e $g_2 = a_2 + b_2 \implies g_1 + g_2 = a_1 + b_1 + a_2 + b_2 = (a_1 + a_2) + (b_1 + b_2)$ e segue que $\pi(g_1 + g_2) = a_1 + a_2 = \pi(g_1) + \pi(g_2)$.

Em particular, se $a \in A$, então $a = a + 0$ onde $0 \in B$. E segue que $\pi(a) = a$, para todo $a \in A$.

Como mostramos que $(i) \Rightarrow (ii) \Rightarrow (iii) \Rightarrow (i)$ e $(i) \Rightarrow (ii) \Rightarrow (iv) \Rightarrow (i)$, segue que as afirmações $(i),\ (ii),\ (iii)$ e (iv) são equivalentes. ■

Lema 143. *Sejam* G *um grupo abeliano e* $\{A_k;\ k \in K\}$ *uma família de subgrupos de* G*. As seguintes afirmações são equivalentes:*

(i) $G = \bigoplus_{k \in K} A_k$.

(ii) Para todo $g \in G$ existe uma única expressão da forma $g = \sum_{k\in K} a_k$, onde $a_k \in A_k$, os índices k são distintos, e $a_k \neq 0$ somente um número finito de vezes.

(iii) $G = \langle \bigcup_{k\in K} A_k \rangle$ e, para cada $j \in K$, $A_j \cap \langle \bigcup_{k\neq j} A_k \rangle = 0$.

Demonstração. $(i) \Rightarrow (ii)$: $G = \bigoplus_{k\in K} A_k$, logo, podemos tomar $\varphi : G \longrightarrow \bigoplus_{k\in K} A_k$ um isomorfismo.

Dado $g \in G$, tomemos duas expressões $g = \sum_{k\in K} a_k = \sum_{k\in K} b_k$.

$$(0)_{k\in K} = \varphi(g-g) = \varphi(g) - \varphi(g) = \varphi(\sum_{k\in K} a_k) - \varphi(\sum_{k\in K} b_k)$$

$$= (a_k)_{k\in K} - (b_k)_{k\in K} = (a_k - b_k)_{k\in K} \implies a_k - b_k = 0, \forall\, k \in K \implies a_k = b_k.$$

Logo, g é expresso de forma única.

$(i) \Leftarrow (ii)$: Para todo $g \in G$ existe uma única expressão $g = \sum_{k\in K} a_k$, onde $a_k \in A_k$, os índices k são distintos, e $a_k \neq 0$ somente um número finito de vezes. Logo, a função

$$\pi : G \longrightarrow \bigoplus_{k\in K} A_k$$

$$g = \sum_{k\in K} a_k \longmapsto (a_k)_{k\in K}$$

estará bem definida e será injetora, devido a unicidade dos a_k na expressão $g = \sum_{k\in K} a_k$.

π será sobrejetora pois, dado $a = (a_k)_{k\in K} \in \bigoplus_{k\in K} A_k$, $a_k \neq 0$ apenas para uma quantidade finita de índices k, e então $g = \sum_{k\in K} a_k \in \langle \bigcup_{k\in K} A_k \rangle \leq G \implies a = (a_k)_{k\in K} = \pi(g)$.

Por fim, π é homomorfismo, pois dado $h \in G$, $h = \sum_{k\in K} b_k$ e teremos

$$\pi(g+h) = \pi(\sum_{k\in K} a_k + \sum_{k\in K} b_k) = \pi(\sum_{k\in K} (a_k + b_k))$$

$$= (a_k + b_k)_{k\in K} = (a_k)_{k\in K} + (b_k)_{k\in K} = \pi(g) + \pi(h).$$

Onde temos que π é isomorfismo e $G \cong \bigoplus_{k\in K} A_k$.

$(ii) \Rightarrow (iii)$: Para todo $g \in G$ existe uma única expressão $g = \sum_{k\in K} a_k$, onde $a_k \in A_k$, os índices k são distintos, e $a_k \neq 0$ somente um número finito de vezes. Logo, temos que $G = \langle \bigcup_{k\in K} A_k \rangle$.

Dado $j \in K$, tome $x \in A_j \cap \langle \bigcup_{k\neq j} A_k \rangle$, $x \in A_j \implies x = a_j \in A_j$ e $x \in \langle \bigcup_{k\neq j} A_k \rangle \implies x = \sum_{k\neq j} a_k$.

Pela unicidade da expressão para x, teremos

$$x = a_j = 0 + ... + 0 + a_j + 0 + ... + 0 = \sum_{k \neq j} a_k \implies a_k = 0, \text{para todo } k.$$

Então $x = \sum_{k \neq j} a_k = 0 \implies A_j \cap \langle \bigcup_{k \neq j} A_k \rangle = \{0\}$.

$(ii) \Leftarrow (iii)$: Dado $g \in G = \langle \bigcup_{k \in K} A_k \rangle$, tomemos duas expressões $g = \sum_{k \in K} a_k = \sum_{k \in K} b_k$. Teremos que $0 = g - g = \sum_{k \in K} a_k - \sum_{k \in K} b_k = \sum_{k \in K} (a_k - b_k)$. Para cada $j \in K$, temos

$$\underbrace{b_j - a_j}_{\in A_j} = \underbrace{\sum_{k \neq j} a_k - b_k}_{\in \langle \bigcup_{k \neq j} A_k \rangle} \in A_j \cap \langle \bigcup_{k \neq j} A_k \rangle = \{0\}.$$

Assim, teremos que $b_j - a_j = 0 \implies a_j = b_j$ para todo $j \in K$, ou seja, g é expresso de forma única. ■

Anteriormente, introduzimos o conceito de independência (Definição 121) em conjuntos finitos de elementos não nulos de um grupo abeliano, e também mostramos um lema (122) caracterizando a independência entre esses elementos. Agora, faremos a generalização de ambos para quantidades infinitas.

Definição 144. Seja X um conjunto infinito de elementos não nulos de G, X é dito independente se todo subconjunto finito de X for independente.

Lema 145. *Um conjunto de elementos não nulos $X \subseteq G$ é independente se, e somente se,* $\langle X \rangle = \bigoplus_{x \in X} \langle x \rangle$.

Demonstração. $(\Rightarrow)$ X é independente.

Sabemos que $\langle X \rangle = \langle \bigcup_{x \in X} \langle x \rangle \rangle$.

Dado $x_0 \in X$, tome $y \in \langle x_0 \rangle \cap \langle X - \{x_0\} \rangle$, segue que $y = m_0 x_0$, para algum inteiro m_0, e $y = \sum_{i=1}^{n} m_i x_i$, onde n é natural, m_i são inteiros e x_i são elementos distintos de $X - \{x_0\}$.

Logo, $-m_0 x_0 + \sum_{i=1}^{n} m_i x_i = 0$ e pela independência de X, segue que $m_i = 0, 0 \leq i \leq n$.

Em particular, $m_0 = 0 \implies y = 0 \implies \langle x_0 \rangle \cap \langle X - \{x_0\} \rangle = \{0\}$. Pelo Lema 143, segue que $\langle X \rangle = \bigoplus_{x \in X} \langle x \rangle$.

$(\Leftarrow)$ $\langle X \rangle = \bigoplus_{x \in X} \langle x \rangle$.

Seja $\{x_1, x_2, ..., x_r\}$ um subconjunto finito de X. Dados m_i inteiros tais que $0 = \sum_{i=1}^{r} m_i x_i$, para cada j, temos que $-m_j x_j = \sum_{k \neq j} m_k x_k \in \langle x_j \rangle \cap \langle \{x_k; k \neq j\} \rangle$.

Pelo Lema 143, $\langle x_j \rangle \cap \langle \{x_k; k \neq j\} \rangle = \{0\}$, logo $-m_j x_j = 0$, para cada j.

Assim $m_j = 0$, $1 \leq j \leq r$, e segue que $\{x_1,\ x_2,\ ...\ ,\ x_r\}$ é independente e, consequentemente, X é independente. ■

Teorema 146. *Todo grupo de torção G pode ser decomposto numa soma direta de grupos p-primários.*

Demonstração. G é de torção, ou seja, todo elemento de G tem ordem finita.

Para cada primo p, considere o subgrupo p-primário

$$G_p = \{g \in G;\ p^m g = 0, \text{ para algum inteiro } m \geq 1\}.$$

Dado $g \in G$, $|g| = n_g$ e, fazendo a decomposição de n_g em fatores primos, temos

$$n_g = p_{g_1}^{\alpha_{g_1}} \cdot ... \cdot p_{g_r}^{\alpha_{g_r}}.$$

Para cada i, defina $n_{g_i} = \dfrac{n_g}{p_{g_i}^{\alpha_{g_i}}}$ e teremos que mdc$(n_{g_1},\ ...\ ,\ n_{g_r}) = 1$. Pela generalização do Teorema de Bézout (118), existem inteiros s_{g_i} tais que $s_{g_1} n_{g_1} + ... + s_{g_r} n_{g_r} = 1$ e daí segue que:

$$s_{g_1} n_{g_1} g + ... + s_{g_r} n_{g_r} g = g.$$

Note que para cada i, $p_{g_i}^{\alpha_{g_i}} s_{g_i} n_{g_i} g = 0 \implies s_{g_i} n_{g_i} g \in G_{p_{g_i}}$.

Logo $g \in \langle \bigcup\limits_{p \in P} G_p \rangle$, $\forall\ g \in G$, onde P é o conjunto dos números primos.

Para cada primo p, considere $g \in G_p \cap \langle \bigcup\limits_{q \neq p} G_q \rangle$.

$g \in G_p \implies p^{m_p} g = 0$, para algum $m_p \geq 1$.

$g \in \langle \bigcup\limits_{q \neq p} G_q \rangle \implies g = \sum\limits_{\substack{q \in P \\ q \neq p}} x_q$, onde $x_q \in G_q$ e $x_q \neq 0$ apenas um número finito de vezes. Para cada q, temos que $x_q \in G_q \implies q^{m_q} x_q = 0$.

Tomando $r = \prod\limits_{x_q \neq 0} q^{m_q}$, temos que mdc$(r, p^{m_p}) = 1$, e então existem $u,\ v$ inteiros tais que $ur + vp^{m_p} = 1 \implies urg + vp^{m_p} g = g \iff 0 + 0 = 0 = g \implies G_p \cap \langle \bigcup\limits_{q \neq p} G_q \rangle = \{0\}$.

Pelo Lema 143, temos que $G = \bigoplus\limits_{p \in P} G_p$. ■

Corolário 147. *Sejam G e H grupos de torção, então $G \cong H$ se, e somente se, $G_p \cong H_p$ para todo primo p.*

Demonstração. $(\Rightarrow)$ Seja $\varphi : G \longrightarrow H$ um isomorfismo.

Para cada primo p, considere $\varphi_p = \varphi\big|_{G_p}$, sabemos que $\varphi_p : G_p \longrightarrow$ im(φ_p) é isomorfismo.

Dado $h \in$ im(φ_p) existe $g \in G_p$ tal que $\varphi_p(g) = h$ e $p^m g = 0 \implies 0 = \varphi_p(p^m g) = p^m \varphi_p(g) = p^m h \implies h \in H_p \implies$ im$(\varphi_p) \subseteq H_p$.

Agora, dado $h \in H_p$, pela sobrejeção de φ, existe $g \in G$ tal que $\varphi(g) = h$ e $p^m h = 0 \implies \varphi(p^m g) = p^m \varphi(g) = p^m h = 0 \implies p^m g = 0 \implies g \in G_p \implies H_p \subseteq \text{im}(\varphi_p)$.

Logo $G_p \cong H_p$.

$(\Leftarrow)$ G e H são grupos de torção, logo podemos fazer a decomposição de ambos em soma direta de grupos p-primários, e cada uma de suas componentes p-primárias será isomorfa, pois $G_p \cong H_p$ para todo primo p. A partir dos isomorfismos entre as componentes, é possível construir um isomorfismo entre G e H, de onde teremos que $G \cong H$. ■

Definição 148. Um grupo abeliano F é tido abeliano livre se puder ser decomposto numa soma direta de grupos cíclicos infinitos, isto é, $F = \bigoplus_{x \in X} \langle x \rangle$, onde X é um subconjunto de F com elementos de ordem infinita, o qual é chamado de base de F. Além disso, a cardinalidade da base X será chamada de posto de F e denotada por $\text{rank}(F)$.

Visto que todo grupo cíclico infinito é isomorfo à $\mathbb{Z}$, podemos escrever $F = \bigoplus_{x \in X} \mathbb{Z}$, onde a quantidade de cópias de $\mathbb{Z}$ será $|X| = \text{rank}(F)$.

Exemplo 149. Considere o grupo multiplicativo $(\mathbb{Q}/\{0\}, \cdot)$.

Seja $G = \langle 2, 5 \rangle \leq (\mathbb{Q}/\{0\}, \cdot)$, G será um grupo abeliano livre.

Basta ver que, dado $q \in \langle 2, 5 \rangle$, $q = 2^m 5^n$, onde $m, n \in \mathbb{Z}$.

Assim, $\varphi : \mathbb{Z} \oplus \mathbb{Z} \longrightarrow \langle 2,5 \rangle$, dado por $(m,n) \longmapsto 2^m 5^n$, será um isomorfismo e teremos que $G = \langle 2, 5 \rangle \cong \mathbb{Z} \oplus \mathbb{Z}$.

Ou seja, G é um grupo abeliano livre de posto 2.

Além disso, resultados anteriores nos trazem informações sobre o grupo abeliano livre F e sua base X, por exemplo, o Lema 143 nos informa que, dado $u \in F$, existirá uma única expressão da forma $u = \sum_{x \in X} m_x x$, onde $m_x \in \mathbb{Z}$ e $m_x \neq 0$ somente um número finito de vezes. Outro fato relevante e que será utilizado futuramente é de que a base X é um conjunto independente, conforme o Lema 145.

Teorema 150. *Sejam F um grupo abeliano livre com base X, G um grupo abeliano e $f : X \longrightarrow G$ uma função. Então existe um único homomorfismo $\varphi : F \longrightarrow G$ que seja uma extensão de f, isto é, $\varphi(x) = f(x)$ para todo $x \in X$.*

Demonstração. Seja $u \in F$, existe uma única expressão $u = \sum_{x \in X} m_x x$ e, por isso, $\varphi : F \longrightarrow G$ dada por $u = \sum_{x \in X} m_x x \overset{\varphi}{\longmapsto} \varphi(u) = \sum_{x \in X} m_x f(x)$ estará bem definida.

Além disso, φ será um homomorfismo e uma extensão de f.

A unicidade é garantida, pois, dados os homomorfismos $\varphi_1,\ \varphi_2 : F \longrightarrow G$, extensões de f, e $u \in F$, teremos que:

$$\varphi_1(u) = \varphi_1\left(\sum_{x\in X} m_x x\right) = \sum_{x\in X} m_x \varphi_1(x) = \sum_{x\in X} m_x f(x)$$
$$= \sum_{x\in X} m_x f(x) = \sum_{x\in X} m_x \varphi_2(x) = \varphi_2\left(\sum_{x\in X} m_x x\right) = \varphi_2(u).$$

■

Corolário 151. *Todo grupo abeliano G é (isomorfo à) um grupo quociente de um grupo abeliano livre.*

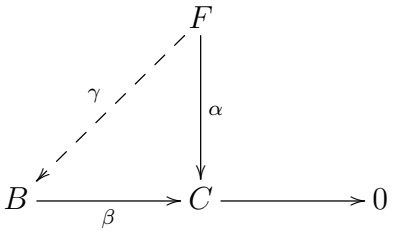
Demonstração. Seja $F = \overbrace{\mathbb{Z} \oplus ... \oplus \mathbb{Z}}^{|G| \text{ vezes}}$, denotemos por x_g o gerador da g-ésima cópia de $\mathbb{Z}$, onde $g \in G$. F é um grupo abeliano livre, com base $X = \{x_g;\ g \in G\}$.

Defina a função $f : X \longrightarrow G$ dada por $f(x_g) = g$, pelo teorema anterior, existe um homomorfismo φ que é uma extensão de f, e φ é sobrejetor, visto que f é sobrejetora.

Pelo 1º Teorema de Isomorfismo (59), $G \cong F/\ker(\varphi)$. ■

Teorema 152. ***(Teorema da Propriedade Projetiva)***

Seja $\beta : B \longrightarrow C$ um homomorfismo sobrejetor. Se F é um grupo abeliano livre e $\alpha : F \longrightarrow C$ um homomorfismo, então existe um homomorfismo $\gamma : F \longrightarrow B$ tal que o diagrama abaixo comuta, isto é, $\beta \circ \gamma = \alpha$.



Demonstração. Seja X uma base de F, para cada $x \in X$, $\alpha(x) \in C$ e, como β é sobrejetor, existe $b_x \in B$ tal que $\beta(b_x) = \alpha(x)$. Logo, pelo Axioma da Escolha, é possível definir uma função $f : X \longrightarrow B$ dada por $f(x) = b_x$.

Pelo Teorema 150, existe um homomorfismo $\gamma : F \longrightarrow B$ tal que $\gamma(x) = b_x$, para todo $x \in X$.

Dado $u \in F$, temos que $u = \sum_{x \in X} m_x x$ e segue que:

$$(\beta \circ \gamma)(u) = \beta(\gamma(u)) = \beta\left(\gamma\left(\sum_{x \in X} m_x x\right)\right) = \sum_{x \in X} m_x \beta(\gamma(x))$$

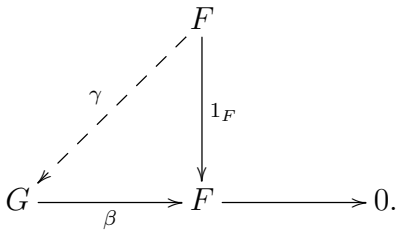
$$= \sum_{x \in X} m_x \beta(b_x) = \sum_{x \in X} m_x \alpha(x) = \alpha\left(\sum_{x \in X} m_x x\right) = \alpha(u) \implies \beta \circ \gamma = \alpha.$$

■

Corolário 153. *Seja G um grupo abeliano e $H \leq G$, se G/H é abeliano livre, então H é uma componente direta de G, isto é, $G = H \oplus K$, onde $K \leq G$ e $K \cong G/H$.*

Demonstração. Tome $F = G/H$ e seja $\beta : G \longrightarrow F$ a projeção canônica, β é um homomorfismo sobrejetor. F é um grupo abeliano livre e podemos tomar $1_F : F \longrightarrow F$ o homomorfismo identidade.

Pelo teorema anterior, existe um homomorfismo $\gamma : F \longrightarrow G$ tal que $\beta \circ \gamma = 1_F$, ou seja, o diagrama abaixo comuta.



Utilizando as equivalências entre os itens (iii) e (i) do Lema 142, existe $K \leq G$ tal que $H \cap K = \{0\}$ e $H + K = G$.

Como $H + K = G$ e $H \cap K = \{0\}$, pelo 2º Teorema de Isomorfismo (60), $G/H \cong K$.

Além disso, $H + K = G \implies \langle H \cup K \rangle = G$ e, pelo Lema 143, segue que $G = H \oplus K$.

■

4.3 Grupos Abelianos Finitamente Gerados

Proposição 154. *Seja G um grupo abeliano. G é finito se, e somente se, for finitamente gerado e todo elemento de G tiver ordem finita (em outras palavras, $t(G) = G$).*

Demonstração. $(\Rightarrow)$ Trivial.

$(\Leftarrow)$ Suponha que G seja finitamente gerado e que todo elemento de G tenha ordem finita.

G é finitamente gerado, então $G = \langle g_1, \ ... \ , \ g_n \rangle$, e sejam os inteiros positivos α_i as respectivas ordens dos geradores g_i, isto é, $\alpha_i = |g_i| < \infty$, $1 \leq i \leq n$.

Dado $g \in G$, $g = \sum_{i=1}^{n} m_i g_i$, onde, para cada i, teremos $0 \leq m_i \leq (\alpha_i - 1)$.

Dessa forma, a quantidade de valores que cada m_i pode assumir será α_i e assim, variando os inteiros m_i, podemos obter $\prod_{i=1}^{n} \alpha_i$ expressões diferentes para $g = \sum_{i=1}^{n} m_i g_i$. Portanto, existirão no máximo $\prod_{i=1}^{n} \alpha_i$ elementos em G e segue que G é um grupo finito. ■

Teorema 155. *Todo grupo abeliano finitamente gerado livre de torção G é um grupo abeliano livre.*

Demonstração. Seja G um grupo abeliano finitamente gerado. Faremos essa demonstração utilizando indução sobre n onde $G = \langle x_1, \ ... \ , \ x_n \rangle$.

Para $n = 1$, G será cíclico e como G é livre de torção, segue que $G \cong \mathbb{Z}$.

Suponha que o teorema vale para grupos com quantidade miníma de geradores menor que n.

Defina $H = \{g \in G; \ mg \in \langle x_n \rangle$ para algum inteiro positivo $m\}$, H é subgrupo de G e o quociente G/H será livre de torção, pois se $x + H \in t(G/H) \implies k(x + H) = 0$, onde $k \in \mathbb{Z} \implies kx \in H \implies (mk)x = m(kx) \in \langle x_n \rangle$ para algum inteiro positivo $m \implies x \in H \implies t(G/H) = \{0\}$.

Sendo G/H livre de torção e gerado por uma quantidade de elementos menor que n, pela hipótese de indução, temos que G/H é abeliano livre. Pelo Corolário 153, segue que $G = F \oplus H$ onde $F \cong G/H$ e então basta mostrarmos agora que H é um grupo cíclico de ordem infinita.

H é uma componente de G, logo também será finitamente gerado.

Seja $g \in H$, então existem inteiros não nulos m e k tais que $mg = kx_n$.

Defina $m' = \min\{\alpha \geq 1; \ \alpha g \in \langle x_n \rangle\}$ e façamos a divisão euclidiana de m por m'.

Teremos que existem $q, r \in \mathbb{Z}$ tais que $m = m'q + r$, onde $0 \leq r < m'$, de onde segue que $rg = (mg + (-q(m'g)) \in \langle x_n \rangle$. Pela minimalidade de m', temos que $r = 0$ e, segue que $m' \mid m$.

Sejam k_1 e k_2 inteiros tais que $k_1 x_n = mg$ e $k_2 x_n = mg \implies (k_1 - k_2)x_n = 0 \implies k_1 = k_2$, visto que G é livre de torção. Ou seja, para cada m, existe um único k tal que $mg = kx_n$. Denotemos por k' o inteiro tal que $m'g = k'x_n$. Também teremos que

$$m' \mid m \implies m = m't, \text{ onde } t \in \mathbb{Z} \implies kx_n = mg = tm'g = t(k'x_n) = k'tx_n,$$

logo, $k = k't$.

Note agora que, dados $m_1, m_2, k_1, k_2 \in \mathbb{Z}$ tais que $m_1 g = k_1 x_n$ e $m_2 g = k_2 x_n$, teremos que:

$$m_1 = m't_1, \text{ onde } t_1 \in \mathbb{Z} \implies k_1 = k't_1$$

$$\text{e } m_2 = m't_2, \text{ onde } t_2 \in \mathbb{Z} \implies k_2 = k't_2.$$

Logo,

$$\frac{k_1}{m_1} = \frac{k't_1}{m't_1} = \frac{k'}{m'}\frac{t_1}{t_1} = \frac{k'}{m'} = \frac{k'}{m'}\frac{t_2}{t_2} = \frac{k't_2}{m't_2} = \frac{k_2}{m_2}.$$

Portanto, podemos tomar $\varphi : H \longrightarrow \mathbb{Q}$ dada por $\varphi(g) = {}^{k}/_{m}$ e φ está bem definida.

φ é um homomorfismo, pois, dados $g, h \in H$, teremos que $m_g g = k_g x_n$ e $m_h h = k_h x_n$, e então:

$$m_g m_h(g+h) = m_g m_h g + m_g m_h h = m_h k_g x_n + m_g k_h x_n = (m_h k_g + m_g k_h)x_n.$$

E segue que:

$$\varphi(g) + \varphi(h) = \frac{k_g}{m_g} + \frac{k_h}{m_h} = \frac{k_g m_h + k_h m_g}{m_g m_h} = \varphi(g+h).$$

φ é injetor, pois, dado $g \in H$ tal que $\varphi(g) = {}^{k}/_{m} = 0 \implies k = 0 \implies mg = 0x_n \implies g = 0 \implies \ker(\varphi) = \{0\}$.

Logo $H \cong \text{im}(\varphi) \leq \mathbb{Q}$. Sendo H finitamente gerado, temos que $\text{im}(\varphi)$ também será, logo, podemos escrever $H \cong \text{im}(\varphi) = \langle {}^{a_1}/_{b_1}, \ \ldots \ , \ {}^{a_t}/_{b_t} \rangle \leq \mathbb{Q}$.

Seja $b = \prod_{i=1}^{t} b_i$, tome $\psi : \text{im}(\varphi) \longrightarrow \mathbb{Z}$, dada por $\psi(q) = bq$.

ψ é homomorfismo, pois, dados $q_1, \ q_2 \in \text{im}(\varphi)$, temos que $\psi(q_1 + q_2) = b(q_1 + q_2) = bq_1 + bq_2$.

Além disso, $\ker(\psi) = \{q \in \text{im}(\varphi); \ bq = 0\} = \{0\}$, visto que $\text{im}(\varphi) \cong H$ e H é livre de torção. Logo, temos que ψ é um homomorfismo injetor e segue que $\text{im}(\varphi) \cong \text{im}(\psi) \leq \mathbb{Z}$.

Por transitividade, $H \cong \text{im}(\psi) \leq \mathbb{Z}$, ou seja, H é isomorfo à um subgrupo de $\mathbb{Z}$, o qual será um grupo cíclico infinito, e com isso, temos que $G = F \oplus H$ é um grupo abeliano livre. ■

Teorema 156. ***(Teorema Fundamental dos Grupos Abelianos Finitamente Gerados)***

Todo grupo abeliano finitamente gerado G pode ser decomposto numa soma direta de grupos cíclicos primários e grupos cíclicos infinitos, onde a quantidade de componentes depende apenas de G.

Demonstração. Seja G um grupo abeliano finitamente gerado.

$G/t(G)$ é livre de torção, pelo teorema anterior, sabemos que $G/t(G)$ é abeliano livre e, pelo Corolário 153, temos que $G = t(G) \oplus F$ onde $F \cong G/t(G)$.

$t(G)$ é finitamente gerado, pela Proposição 154, temos que $t(G)$ é finito. Sendo $t(G)$ um grupo abeliano finito, podemos decompô-lo na soma direta de suas componentes p-primárias utilizando o Teorema da Decomposição Primária (119) e essa decomposição será única, a menos da ordem das componentes. Em seguida, podemos fazer a decomposição de cada componente p-primária em grupos cíclicos, a qual também será única, a menos da ordem dos componentes, em decorrência do Corolário 70, e de onde obteremos uma decomposição de $t(G)$ em grupos cíclicos primários.

Enquanto isso, $F = G/t(G)$ é abeliano livre, logo pode ser decomposto numa soma direta de grupos cíclicos infinitos, onde o número de componentes será rank$(G/t(G))$. Fazendo ambas decomposições, teremos G decomposto numa soma direta de grupos cíclicos primários e grupos cíclicos infinitos, como queríamos demonstrar. ■

Sabemos que grupos cíclicos são isomorfos à $\mathbb{Z}$ ou $\mathbb{Z}/n\mathbb{Z}$.

Tomando $M =$ rank$(G/t(G))$ e denotando por m_i as ordens das componentes cíclicas primárias da decomposição de $t(G)$.

Podemos reescrever a decomposição $G \cong G/t(G) \oplus t(G)$ da forma:

$$G \cong \underbrace{\mathbb{Z} \oplus ... \oplus \mathbb{Z}}_{M \text{ vezes}} \oplus \frac{\mathbb{Z}}{m_1\mathbb{Z}} \oplus \frac{\mathbb{Z}}{m_2\mathbb{Z}} \oplus ... \oplus \frac{\mathbb{Z}}{m_t\mathbb{Z}}.$$

Ou seja, toda a classe dos grupos abelianos finitamente gerados pode ser representada utilizando somas diretas do grupo $(\mathbb{Z}, +)$ e de grupos da forma $(\mathbb{Z}/n\mathbb{Z}, +)$.

5 CONSIDERAÇÕES FINAIS

Nesse trabalho construímos um arcabouço teórico sólido para a caracterização de grupos abelianos finitamente gerados, e pudemos explorar temas da Teoria de Grupos, como os abordados nos capítulos 3 e 4, que não são abordados durante o curso de Licenciatura em Matemática da UTFPR-CT.

Ao longo do trabalho, provamos importantes resultados para a Teoria de Grupos, como os teoremas de Lagrange, de Isomorfismo, da Correspondência, de Cayley, da Órbita-Estabilizador, de Sylow, e os que decompões grupos abelianos, entre outros.

Para o autor que vos escreve, esse trabalho serviu como uma oportunidade de estudar de forma sistemática os temas que aqui foram abordados, permitindo a formação de uma visão mais ampla dos conteúdos que compõem a base da Teoria de Grupos.

Do mesmo modo, acreditamos que o trabalho em questão possa servir de forma semelhante para estudantes de matemática que se interessem pelo tema, reunindo os conhecimentos necessários para a demonstração dos resultados propostos e possivelmente servindo como fonte de consulta para demonstrações mais detalhadas de tais resultados.

REFERÊNCIAS

GARCIA, A. L. P.; LEQUAIN, Y. A. E. **Elementos de Álgebra**. 6. ed. Rio de Janeiro: IMPA, 2015. 326 p.

HUNGERFORD, T. W. **Algebra**. 1. ed. New York: Springer-Verlag New York Inc., 1974. 504 p.

ROTMAN, J. J. **An Introduction to the Theory of Groups**. 4. ed. New York: Springer-Verlag New York Inc., 1999. 517 p.

ROTMAN, J. J. **Advanced Modern Algebra**. 2. ed. Hoboken: Prentice Hall, 2003. 1040 p.