UNIVERSIDADE FEDERAL DO SUL E SUDESTE DO PARÁ
INSTITUTO DE CIÊNCIAS EXATAS
FACULDADE DE MATEMÁTICA

RAFAEL NUNES VALE

CARACTERIZAÇÃO DOS GRUPOS SOLÚVEIS

MARABÁ
2023

UNIVERSIDADE DO SUL E SUDESTE DO PARÁ
INSTITUTO DE CIÊNCIAS EXATAS
FACULDADE DE MATEMÁTICA

RAFAEL NUNES VALE

CARACTERIZAÇÃO DOS GRUPOS SOLÚVEIS

Trabalho de conclusão de curso apresentado ao curso de licenciatura em Matemática da Universidade Federal do Sul e Sudeste do Pará orientado pelo Prof. Dr. Yerko Contreras Rojas como pré-requisito para a obtenção do título de licenciado em matemática.

MARABÁ
2023

Dados Internacionais de Catalogação na Publicação (CIP)
Universidade Federal do Sul e Sudeste do Pará
Biblioteca Setorial Campus II

V149c Vale, Rafael Nunes
Caracterização dos grupos solúveis / Rafael Nunes Vale. — 2023.
48 f.

Orientador (a): Yerko Contreras Rojas

Trabalho de Conclusão de Curso (graduação) - Universidade Federal do Sul e Sudeste do Pará, Instituto de Ciências Exatas, Faculdade de Matemática, Curso de Licenciatura em Matemática, Marabá, 2023.

1. Matemática - Álgebra. 2. Teoria de grupos. 3. Grupos Abelianos. 4. Grupos Solúveis. I. Contreras Rojas, Yerko, orient. II. Título.

CDD: 22. ed.: 512.2

Elaborado por Marcelo da Silva Gomes – CRB-2/1208

RAFAEL NUNES VALE

CARACTERIZAÇÃO DOS GRUPOS SOLÚVEIS

Trabalho de conclusão de curso apresentado ao curso de licenciatura em Matemática da Universidade Federal do Sul e Sudeste do Pará orientado pelo Prof. Dr. Yerko Contreras Rojas como pré-requisito para a obtenção do título de licenciado em matemática.

Marabá, Dezembro de 2023

BANCA EXAMINADORA

Prof° Dr. Claudionei Pereira de Oliveira

Prof° Dr. João Carlos Pantoja Fortes

Prof° Dr. Yerko Contreras Rojas

"À minha família e amigos."

AGRADECIMENTOS

Primeiramente agradeço a Deus pelo dom da vida e pelo sustento. À minha família pelo apoio financeiro e, principalmente, emocional. Em especial, agradeço a minha irmã Maria de Lara e meu cunhado Cleiton que, por um período, me receberam em sua casa. Agradeço aos meus pais, Timóteo e Hermínia, que em nenhum momento da minha vida faltaram comigo.

Por fim, agradeço a UNIFESSPA por me acolher e pela oportunidade que me foi ofertada. Aos amigos que fiz durante esses quatro anos de curso, toda gratidão. Principalmente aos mais próximos que me auxiliaram nessa caminhada sendo excelentes companheiros de estudos. Não irei citar todos nominalmente, mas saibam que todos possuem a minha eterna amizade.

"E com uma letra bem pequena, lá estava escrito no seu epitáfio: tentou ser, não conseguiu; tentou ter, não possuiu; tentou continuar, não prosseguiu; e nessa vida de expectativas frustradas tentou até amar... Pois bem, não conseguiu, e aqui está."

(Autor desconhecido)

RESUMO

Desde o princípio da teoria de grupos, os pesquisadores tem voltado sua atenção em entender a relação entre polinômios e o grupo de permutações das suas raízes. Problemas desse tipo induziram o estudo da solução de equações polinomiais mediante a radicais, as quais foram profundamente estudadas por Galois garantindo que uma equação polinomial é resolúvel por meio de radicais se, e somente se, o grupo de Galois associado a tal equação for solúvel. Esse resultado gerou interesse nessa classe de grupos criando novas interpretações e aproximações a esse objeto de estudo.

Atualmente a classe dos grupos solúveis de comprimento derivado menor ou igual a d, pode ser entendida como uma classe muito próxima à classe de grupos abelianos. A medida em que o d se faz menor, um grupo com comprimento derivado d está mais "próximo"de ser abeliano.

Lembremos que um grupo se diz solúvel se o mesmo possui uma série subnormal com fatores abelianos. Quanto menor o comprimento dessa série, menor a quantidade de extensões entre grupos abelianos deve ser feita para obtermos o grupo em questão.

Dada a importância da classe dos grupos solúveis, apresentaremos nesse trabalho uma caracterização dos grupos solúveis finitos a partir da série derivada e da série de composição, mostrando que os grupos solúveis possuem uma caracterização semelhante a caracterização dos grupos abelianos, evidenciando a proximidade desses objetos.

Palavras-chave: Teoria de grupos, Grupos Abelianos, Grupos Solúveis.

ABSTRACT

Since the beginning of group theory, researchers have focused their attention on understanding the relationship between polynomials and the group of permutations of their roots. Problems of this type led to the study of the solution of polynomial equations using radicals, which were deeply studied by Galois, ensuring that a polynomial equation is solvable using radicals if, and only if, the Galois group associated with such an equation is soluble. This result generated interest in this class of groups, creating new interpretations and approaches to this object of study.

Currently, the class of soluble groups with derived length less than or equal to d can be understood as a class very close to the class of abelian groups. As d becomes smaller, a group with derived length d is "closer"to being abelian.

Let us remember that a group is said to be soluble if it has a subnormal series with abelian factors. The shorter the length of this series, the fewer extensions between abelian groups must be made to obtain the group in question.

Given the importance of the class of soluble groups, in this work we will present a characterization of finite soluble groups based on the derived series and the composition series, showing that the soluble groups have a characterization similar to the characterization of abelian groups, highlighting the proximity of these objects.

Keywords: Theory of Groups, Abelian Groups, Solvable Groups.

Sumário

Introdução

Muitos dos estudos em teoria de grupos são baseados no fato da operação do grupo não ser abeliana. Quando nos restringimos a grupos finitos e finitamente gerados possuímos uma caracterização completa dos grupos abelianos, apresentaremos no segundo capitulo desse trabalho a caracterização dos grupos abelianos finitos. Dado que os grupos abelianos estão amplamente caracterizados temos muito interesse em grupos não-abelianos tornando-se natural o estudo de classes de grupos definidos pensando em quão perto estão da classe de grupos abelianos.

Buscando se aproximar do conceito de grupos abelianos, um primeiro passo é pensar em grupos que são extensão de um grupo abeliano por outro abeliano, em outras palavras, um grupo G que possui um subgrupo normal abeliano H tal que o grupo quociente G/H é também abeliano. Esses grupos são chamados de metabelianos, e desde um ponto de vista (do comprimento derivado) podem ser vistos como muito próximos de serem abelianos.

Desejando seguir com essa ideia, podemos pensar em extensões de um metabeliano com um grupo abeliano e, generalizando recursivamente esse processo, chegamos a formulação da definição de grupo solúvel. O conceito de grupo solúvel é um dos mais antigos na teoria de grupos sendo introduzido por E. Galois no começo do século XIX quando o mesmo estudava o problema de resolver equações algébricas mediante radicais, onde a cada equação era associado um grupo e esta era resolúvel mediante radicais se, e somente se, o grupo associado fosse solúvel.

Nesse contexto, este trabalho tem como objetivo apresentar uma caracterização dos grupos solúvel finitos tomando como base o trabalho do C. Polcino Miles [2] . No primeiro capitulo apresentaremos definições preliminares da teoria básica de grupos, que servirão como base para este trabalho. Em seguida, no segundo capítulo exibiremos uma caracterização para os grupos abelianos finitos. Por fim, o terceiro capitulo contem os principais resultados a respeito de grupos solúveis dando uma caracterização em termos da série derivada e uma caracterização dos grupos solúveis finitos em termos da série de composição.

Capítulo 1

Resultados Preliminares

Neste capítulo, apresentaremos os resultados chaves estudados em um curso de Fundamentos de Álgebra que servirão como base para este trabalho . Devido o caráter introdutório algumas demonstrações serão omitidas podendo ser consultadas em [1, 2, 3, 4, 5].

Iniciaremos com o conceito de grupo, estrutura que é a base desse trabalho, e apresentando algumas propriedades inicias. Em sequência, definiremos um subgrupo e exibiremos resultados imediatos a partir da sua definição.

1.1 Grupos e Subgrupos

Definição 1.1.1. *Se G é um conjunto não vazio, uma operação binária sobre G é uma função*

$$\begin{array}{rccc} \cdot : & G \times G & \to & G \\ & (x, y) & \mapsto & x \cdot y \end{array}$$

Tanto a imagem quanto a função podem ser denotadas de distintas formas. Neste trabalho utilizaremos a notação multiplicativa onde a operação será denotada por "$\cdot$"e a imagem do par (x, y) será denotada por $x.y$ ou xy.

Definição 1.1.2. *Um Grupo é um conjunto G não vazio munido de uma operação binaria, $(G, \cdot)$, que satisfaz as propriedades*

I) *Associativa: Para todo a, b, $c \in G$ temos que $(ab)c = a(bc)$.*

II) *Existência de elemento neutro: $\exists\ e \in G$ tal que $\forall\ a \in G$ $ea = ae = a$.*

III) *Existência de inversos: $\forall\ a \in G\ \exists\ a^{-1} \in G$ tal que $aa^{-1} = a^{-1}a = e$.*

Definição 1.1.3. *Um Grupo se diz abeliano ou comutativo quando satisfaz a seguinte propriedade:*

IV) *Comutativa:*
$\forall\ a, b \in G$ *temos que* $ab = ba$.

Proposição 1.1.4. *O elemento neutro em um Grupo G é único.*

Demonstração. Sejam e, $\overline{e}$ elementos neutros de G, então $e = e\overline{e}$. Usando o fato de que e é elemento neutro temos que $e\overline{e} = \overline{e}$, logo $e = \overline{e}$.

□

Proposição 1.1.5. *Seja G um grupo, para cada* $a \in G$ *o elemento inverso de a* (a^{-1}) *é único.*

Demonstração. Sejam b e b' inversos de a em G, então $ba = ab = e = b'a = ab'$, logo $b = be = bab' = eb' = b'$.

□

Proposição 1.1.6. *Seja G um grupo, e* $a, b, x \in G$*, então:*

I) $ax = bx \Rightarrow a = b$.

II) $xa = xb \Rightarrow a = b$.

Demonstração. Observe que I) e II) podem serem provadas analogamente. Apresentamos aqui a prova de I).
Dado um $x \in G$, existe $x^{-1} \in G$, assim

$$axx^{-1} = bxx^{-1} \Rightarrow ae = be \Rightarrow a = b.$$

□

Proposição 1.1.7. *Seja G um grupo, então:*

I) $b \in G$ *e* $bb = b \Rightarrow b = e$.

II) $\forall\ a \in G\ (a^{-1})^{-1} = a$.

III) $\forall\ a, b \in G$ *temos que* $(ab)^{-1} = b^{-1}a^{-1}$.

Demonstração.
I) Se $b = bb \Rightarrow b^{-1}b = b^{-1}b \Rightarrow e = b$.
II) $(a^{-1})^{-1}a^{-1} = e$, mas $aa^{-1} = e$, pela Proposição 1.1.5 temos, enfim, que $(a^{-1})^{-1} = a$.
III) $(ab)b^{-1}a^{-1} = a(bb^{-1})a^{-1} = aea^{-1} = aa^{-1} = e$, logo $(ab)^{-1} = b^{-1}a^{-1}$.

□

Definiremos agora o conceito de grupo finito.

Definição 1.1.8. *Quando o conjunto G associado ao grupo tem cardinalidade (ou ordem) finita dizemos que o grupo é um grupo finito, caso contrario, dizemos que $(G, \cdot)$ é um grupo infinito.*

Definição 1.1.9. *Dizemos que a ordem de um elemento x em um grupo G, denotada por $|x|$, é o menor número inteiro n tal que $x^n = e$, quando esse número não existe dizemos que este elemento possui ordem infinita.*

Teorema 1.1.10. *Seja G um grupo e a um elemento de G de ordem n, então:*

i) *$a^k = e$ se, e somente se, n divide k.*

ii) *$a^i = a^j$ se, e somente se, $i \equiv j \pmod{n}$*

Demonstração. i) Supondo que $a^k = e$, pelo algorítimo da divisão existem únicos q e r inteiros tais que $k = nq + r$ com $0 \leq r < n$ assim,

$$e = a^k = a^{nq+r} = (a^n)^q a^r = e^q a^r = a^r$$

o que implica $r = 0$ devido $|a| = n$.
Supondo que n divide k, então $k = nq$, portanto

$$a^k = a^{nq} = (a^n)^q = e^q = e.$$

A demostração de ii) é uma aplicação direta de i). □

Antes de introduzimos a noção de subgrupo vamos falar sobre um subconjunto de um grupo ser fechado para a operação do grupo.

Seja G um grupo e H um subconjunto não vazio de G, dizemos que H é fechado para operação de G se para todo a, b pertencentes a H, ab também pertence a H, isto é, a operação binária de G restrita ao conjunto H também é uma operação binária em H.

Definição 1.1.11. *Seja G um grupo e H um subconjunto não vazio de G. Se H é um grupo com a operação de G (restrita a H), então H é dito um subgrupo de G, denotamos essa relação entre H e G por $H \leq G$.*

Os exemplos mais imediatos de subgrupos de um grupo G são o próprio grupo G e o conjunto unitário cujo único elemento é o elemento neutro de G, esses exemplos são chamados de subgrupos triviais.

Teorema 1.1.12. *Sejam G um grupo e H um subconjunto não vazio de G. H será um subgrupo de G se, e somente se, H for fechado para operação de G e para todo $a \in H$, $a^{-1} \in H$.*

Demonstração. $\Rightarrow$ O fato de H ser um grupo com a operação de G garante que H é fechado para operação de G e que todo elemento de H possui inversos em H.
$\Leftarrow$ Seja H um subconjunto de G diferente de vazio tal que

I) $\forall\ a, b \in H\ ab \in H$.

II) $\forall\ a \in H\ a^{-1} \in H$.

Como H é diferente de vazio, exite $a \in H$. Pela hipótese II), $a^{-1} \in H$ e pela hipótese I) temos que $aa^{-1} \in H$ e $aa^{-1} = e_G \in H$. Logo H tem elemento neutro. A associatividade em H vem do fato de G ser um grupo. Por fim, II) garante a existência de inversos em H, portanto H é um grupo com a operação de G.

□

Definição 1.1.13. *Se G é um grupo e $a \in G$, seja $\langle a \rangle$ o conjunto de todas as potencias inteiras de a, a saber $\langle a \rangle = \{a^n : n \in \mathbb{Z}\}$. Dizemos que G é um grupo cíclico se $\langle a \rangle = G$.*

Teorema 1.1.14. *Todo subgrupo de um grupo cíclico é também cíclico.*

Demonstração. Consultar [3]. □

1.2 Classes Laterais e Teorema de Lagrange

Vamos agora definir uma relação sobre um grupo G nos valendo de um subgrupo dado, com o intuito de construir novos grupos a partir dela.

Definição 1.2.1. *Seja $(G, \cdot)$ um grupo e $H \leq G$, dizemos que $a \equiv b\ (mod\ H)$ se $ab^{-1} \in H$. Denotaremos tal relação como $\equiv_H$.*

Vamos mostrar que $\equiv_H$ é uma relação de equivalência em G. Com efeito,

I) $\forall g \in G \qquad gg^{-1} = e \in H \Rightarrow g \equiv g(modH)$.

II) Se
$$\begin{aligned} a \equiv b(modH) &\Rightarrow ab^{-1} \in H \\ &\Rightarrow (ab^{-1})^{-1} \in H \\ &\Rightarrow ba^{-1} \in H \\ &\Rightarrow b \equiv a(modH). \end{aligned}$$

III) Se
$$\begin{aligned} a \equiv b(modH) \text{ e } b \equiv c(modH) &\Rightarrow (ab^{-1}) \in H \text{ e } (bc^{-1}) \in H \\ &\Rightarrow (ab^{-1})(bc^{-1}) \in H \\ &\Rightarrow ac^{-1} \in H \\ &\Rightarrow a \equiv c(modH). \end{aligned}$$

Proposição 1.2.2. *Se $a \in G$, então a classe de equivalência determinada por a via $\equiv_H$, $\overline{a}$, é o conjunto $Ha = \{ha / h \in H\}$.*

Demonstração. Seja $ha \in Ha$, desta forma $a(ha)^{-1} = aa^{-1}h^{-1} = h^{-1} \in H \Rightarrow a \equiv_H ha$, assim ha pertence a classe de equivalência de a. Portanto, $Ha \subset \overline{a}$. Agora, seja $b \in \overline{a}$, temos que $ab^{-1} \in H \Rightarrow ab^{-1} = h$, para algum $h \in H$. Assim, $h^{-1}a = b$, portanto $b \in Ha$. Desta forma, $\overline{a} \subset Ha$, logo $Ha = \overline{a}$.

□

Definição 1.2.3. *Para cada $a \in G$, a classe de equivalência Ha definida pela relação $\equiv_H$ é chamada classe lateral à direita, módulo H, determinada por a.*
Ainda, $G/\equiv_H = \{Hx \quad | \quad x \in G\}$ é o conjunto de todas as classes laterais distintas de G.

Uma consequência imediata da proposição anterior é que o conjunto das classes laterais à direita, módulo H, determina uma partição em G, ou seja:

a) Se $a \in G$, então $Ha \neq \emptyset$;

b) Se $a, b \in G$, então $aH = bH$ ou $aH \cap bH = \emptyset$;

c) A união de todas as classes laterias é igual a G.

Definição 1.2.4. *Seja H um subgrupo de G. O índice de H em G (denotado por $[G : H]$) é definido como o número de classes laterais à direita de H em G.*

O teorema que enunciaremos a seguir é fundamental pois limita a construção de subgrupos.

Teorema 1.2.5. *(Teorema de Lagrange) Seja H um subgrupo de um grupo finito G. Então $|H|$ divide $|G|$.*

Demonstração. Definindo em G a relação de equivalência $\equiv (\text{mod } H)$ segue que o conjunto S das classes laterais de H em G é finito. Supondo $|S| = n$ e $S = \{Hx_1, Hx_2, ..., Hx_n\}$, assim

$$G = Hx_1 \cup Hx_2 \cup \cdots \cup Hx_n$$

união disjunta, portanto

$$|G| = |Hx_1| + |Hx_2| + \cdots + |Hx_n|$$

Afirmando que $|G| = n|H|$ (e isto demonstra o teorema). De fato, basta mostrarmos que $|Hx_i| = |H|$, $\forall\ i, 1 \leq i \leq n$.

Seja

$$\begin{array}{rccl} f: & H & \to & Hx_i, \quad 1 \leq i \leq n \\ & h & \mapsto & hx_i \end{array}$$

uma função. A função f é evidentemente sobrejetora, além disso se $f(h) = f(h')$ tem-se $hx_i = h'x_i \Rightarrow h = h'$, ou seja, f é bijetiva e portanto $|H| = |Hx_i| \quad \forall i, 1 \leq i \leq n$, como queríamos demonstrar. □

Corolário 1.2.6. *Seja G um grupo finito. Então a ordem de um elemento $g \in G$ divide a ordem de G.*

Demonstração. A demonstração deste corolário consiste em lembrar que $|g| = |\langle g \rangle|$ e o teorema de Lagrange nos garante que a ordem deste subgrupo divide a ordem do grupo. □

Uma consequência imediata deste teorema é o seguinte resultado que caracteriza os grupos de ordem prima.

Teorema 1.2.7. *Todo grupo de ordem p, com p um número primo, é cíclico.*

Demonstração. Seja a um elemento de G diferente do elemento neutro. A ordem de $\langle a \rangle$ divide a ordem de G, pelo Teorema de Lagrange, mas como a ordem de G é igual a um número p primo então $|\langle a \rangle| = p$, deste modo $\langle a \rangle = G$. □

1.3 Subgrupo normal, Grupos Quocientes e Homomorfismos

Com o intuito de estudar novos exemplos de grupos focamos nossa atenção para os grupos quocientes. Com isso em mente, definimos abaixo um tipo especial de subgrupo.

Definição 1.3.1. *Um subgrupo N de um grupo G é chamado subgrupo normal se, para todo $x \in G$, vale a igualdade $xN = Nx$, equivalentemente o conjunto $xNx^{-1} = \{xnx^{-1} | n \in N\}$ coincide com N . Ou seja, a classe lateral à direita é igual a classe lateral à esquerda. Denotaremos $N \trianglelefteq G$ para dizer que N é normal em G.*

Definição 1.3.2. *Sejam G um grupo e N um subgrupo normal de G. O grupo quociente de G por N é o grupo dado pelo conjunto quociente G/N, induzido pela relação de equivalência congruência módulo N ($\equiv_N$), e a operação binaria*

$$\begin{array}{rccl} \cdot: & G/N \times G/N & \longrightarrow & G/N \\ & (Ng, Nh) & \longmapsto & Ng \cdot Nh = Ngh \end{array}$$

Definição 1.3.3. *Sejam $(G, \cdot)$ e $(H, *)$ grupos e f uma função $f : G \to H$, dizemos que f é um homomorfismo de grupos se para todo $a, b \in G$*

$$f(a \cdot b) = f(a) * f(b).$$

A definição acima nos permite interpretar um homomorfismo de grupos como uma função que respeita a operação dos grupos associados.

Proposição 1.3.4. *Seja $f : G \to H$ um homomorfismo de grupos, então*

I) $f(e_G) = e_H$.

II) Para todo $g \in G$, $f(g^{-1}) = f(g)^{-1}$.

Demonstração.

I) Como e_G é o elemento neutro de G e f é um homomorfismo de grupos temos que $f(e_G) = f(e_G \cdot e_G) = f(e_G) \cdot f(e_G)$, logo pela Proposição 1.1.7 $f(e_G) = e_H$.

II) Ao operar $f(g)$ com $f(g^{-1})$ obtemos que $f(g) \cdot f(g^{-1}) = f(gg^{-1}) = f(e_G) = e_H$, logo $f(g^{-1}) = f(g)^{-1}$.

□

Definição 1.3.5. *Seja $f : G \to H$ um homomorfismo de grupos. O núcleo de f, denotado por $ker(f)$, é o conjunto $ker(f) = \{g \in G / f(g) = e_H\}$ e a imagem de f, denotada por $Im(f)$, é o conjunto $Im(f) = \{f(g) / g \in G\}$.*

Teorema 1.3.6. *Seja $f : G \to H$ um homomorfismo de grupos. Temos que $Im(f) \leq H$ e $ker(f) \trianglelefteq G$.*

Demonstração. Provaremos primeiro que $Im(f) \leq H$. Pela Proposição 1.3.4 temos que $e_H \in Im(f)$. Seja $f(g) \in Im(f)$, como G é um grupo vai existir g^{-1} e como f é um homomorfismo temos que $f(g^{-1}) = (f(g))^{-1}$, logo $Im(f)$ é fechado para inversos. Sejam $f(g), f(h) \in Im(f)$, como f é um homomorfismo temos que $f(g)f(h) = f(gh) \in Im(f)$, assim $Im(f)$ é fechado logo é um subgrupo de H.

Agora provaremos que $ker(f) \trianglelefteq G$. Sejam $a, b \in ker(f)$, então $f(ab) = f(a)f(b) = e_H$, portanto $ab \in ker(f)$ logo $ker(f)$ é fechado. Se $a \in ker(f)$ então $f(a^{-1}) = (f(a))^{-1} = (e_H)^{-1} = e_H$, assim $ker(f)$ é fechado para inversos logo é um subgrupo de G. Ainda, temos que para $a \in ker(f)$, $f(gag^{-1}) = f(g)f(a)f(g^{-1}) = f(g)(f(g))^{-1} = e_H \ \forall g \in G$. Assim, $gag^{-1} \in ker(f) \ \forall g \in G$, logo $ker(f) \trianglelefteq G$. □

Teorema 1.3.7. *Um homomorfismo de grupos $\phi : G \to H$ é injetivo se, e somente se, $ker(\phi) = \{e_G\}$.*

Demonstração. Como ϕ é um homomorfismo de grupos temos que $\phi(e_G) = e_H$. Supondo que ϕ é injetivo, se $a \in ker(\phi) \Rightarrow \phi(a) = e_H$, portanto pela injetividade de ϕ temos que $a = e_H$, logo $ker(\phi) = \{e_G\}$.

Supondo que $ker(\phi) = \{e_G\}$, se $\phi(a) = \phi(b) \Rightarrow \phi(a)(\phi(b))^{-1} = e_H \Rightarrow \phi(ab^{-1}) = e_H \Rightarrow ab^{-1} \in ker(\phi)$, mas, por hipótese, $ker(\phi) = \{e_G\}$, portanto $ab^{-1} = e_G \Rightarrow a = b$, logo ϕ é injetivo. □

Definição 1.3.8. *Um isomorfismo de grupos é um homomorfismo de grupos bijetor. Quando existe um isomorfismo entre dois grupos G e H dizemos que G é isomorfo a H e denotamos $G \cong H$*

O isomorfismo é uma relação entre grupos importante na teoria de grupos porque nos permite comparar grupos. Dizer que dois grupos são isomorfos é dizer que os dois possuem a mesma estrutura.

Teorema 1.3.9. *(Primeiro teorema do isomorfismo) Seja $f : G \to H$ um homomorfismo de grupo. Então o quociente $G/ker(f)$ é isomorfo a $Im(f)$.*

Demonstração. Chamemos $K = ker(f)$ e considere a função $\overline{f}$ induzida por f

$$\begin{array}{rccc} \overline{f}: & G/K & \to & Im(f) \\ & gK & \mapsto & f(g) \end{array}$$

Verificaremos se $\overline{f}$ está bem definida. Seja $x \in gK$. Logo, $xK = gK$ e portanto é necessário que $f(x) = f(g)$. Como $x \equiv_K g$, segue que $xg^{-1} = h$, para algum $h \in K$. Logo $x = hg$, portanto $f(x) = f(hg) = f(h) \cdot f(g) = e_H \cdot f(g) = f(g)$, assim $\overline{f}$ está bem definida.

Vejamos agora que $\overline{f}$ é um homomorfismo. Sejam $xK, gK \in G/Ker(f)$, temos que $\overline{f}(xK \cdot gK) = \overline{f}(x \cdot gK) = f(x \cdot g) = f(x) \cdot f(g) = \overline{f}(xK) \cdot \overline{f}(gK)$, portanto $\overline{f}$ é um homomorfismo.

Verificaremos que $\overline{f}$ é sobrejetora. Seja $h \in Im(f)$, logo existe $g \in G$ tal que $f(g) = h$. Seja $gK \in G/K$, temos $\overline{f}(gK) = f(g) = h$, portanto $\overline{f}$ é sobrejetora.

Por fim verificamos que $\overline{f}$ é injetora. Sejam $gK, hK \in G/K$, tal que $\overline{f}(gK) = \overline{f}(hK)$. Logo $f(g) = f(h)$, portanto $f(gh^{-1}) = e_H$ logo $gh^{-1} \in K$ assim $gK = hK$.

□

Corolário 1.3.10. *(Segundo Teorema do Isomorfismo) Se K e N são subgrupos de um grupo G, com N normal em G, então $K/(N \cap K) \cong NK/N$.*

Demonstração. Definindo a função

$$\begin{array}{rccc} \phi: & K & \to & NK/N \\ & k & \mapsto & Nk. \end{array}$$

Dados $k, r \in K$, temos que

$$\phi(kr) = Nkr = NkNr = \phi(k)\phi(r),$$

portanto, ϕ é um homomorfismo.
Seja $Na \in NK/N$, logo existem $n \in N$ e $k \in K$ tais que $a = nk$ assim,

$$Na = Nnk = Nk = \phi(k)$$

desta forma, ϕ é sobrejetora.
Ainda, temos que $ker(\phi) = \{k \in K | \phi(k) = Nk = N\} = \{k \in K | k \in N\}$, o que implica $\ker(\phi) = K \cap N$. Logo, pelo primeiro teorema do isomorfismo,

$$K/K \cap N \cong NK/N.$$

□

Corolário 1.3.11. *(Terceiro Teorema do Isomorfismo) Se H e K são subgrupos normais de um grupo G tal que $K \leq H$, então H/K é um subgrupo normal em G/K e $(G/K)/(H/K) \cong G/H$.*

Demonstração. Definindo a função,

$$\begin{array}{rccc} \phi: & G/K & \to & G/H \\ & Kg & \mapsto & Hg. \end{array}$$

Temos que ϕ é claramente sobrejetora, e mais, $ker(\phi) = \{Kg \in G/H \mid \phi(Kg) = H\}$, portanto $ker(\phi) = \{Kg \mid g \in H\}$ o que implica $ker(\phi) = H/K$. Logo, H/K é um subgrupo normal de G/K e pelo primeiro teorema do isomorfismo, temos que

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

□

Definição 1.3.12. *Seja $\phi : G \to G'$ um homomorfismo de grupos e $H \leq G$, $H' \leq G'$. Definimos o conjunto imagem de H por ϕ como $\phi(H) = \{\phi(h) \,|\, h \in H\}$ e o conjunto imagem inversa de H' por ϕ como $\phi^{-1}(H') = \{g \in G \,|\, \phi(g) \in H'\}$.*

Teorema 1.3.13. *(Teorema da Correspondência) Seja $\phi : G \to G'$ um homomorfismo de grupos sobrejetor. Então:*

i) *Se $H \leq G \Rightarrow \phi(H) \leq G'$;*

ii) *Se $H' \leq G' \Rightarrow \phi^{-1}(H') \leq G$ e $ker(\phi) \subset \phi^{-1}(H')$;*

iii) *Se* $H \trianglelefteq G \Rightarrow \phi(H) \trianglelefteq G^{'}$;

iv) *Se* $H^{'} \trianglelefteq G^{'} \Rightarrow \phi^{-1}(H^{'}) \trianglelefteq G$;

v) *Se* $H \leq G$ *e* $ker(\phi) \subset H \Rightarrow \phi^{-1}(\phi(H)) = H$;

vi) *Se* $H^{'} \leq G^{'} \Rightarrow \phi(\phi^{-1}(H^{'})) = H^{'}$;

vii) *A função* $H \mapsto \phi(H)$ *é uma correspondência bijetora entre a família de subgrupos de* G *que contém o* $ker(\phi)$ *e a família de todos os subgrupos de* $G^{'}$. *Subgrupos normais de* G *correspondem a subgrupos normais de* $G^{'}$.

Demonstração.

i) Claramente $\phi(H) \neq \emptyset$ dado que $\phi(0) \in \phi(H)$. Sejam $\phi(h), \phi(h^{'}) \in \phi(H)$, então $\phi(h)\phi(h^{'}) = \phi(hh^{'}) \in \phi(H)$, assim $\phi(H)$ é fechado. Agora, seja $\phi(h) \in \phi(H)$ logo $\phi(h^{-1}) = \phi(h)^{-1}$ com $h^{-1} \in H \Rightarrow \phi(h)^{-1} \in \phi(H)$, assim $\phi(H)$ é fechado para inversos, logo $\phi(H)$ é um subgrupo de $G^{'}$;

ii) Claramente $\phi^{-1}(H') \neq \emptyset$. Sejam $a, b \in \phi^{-1}(H^{'})$, então $\phi(a), \phi(b) \in H^{'}$. Temos que, $\phi(a)\phi(b) = \phi(ab) \in H^{'}$, assim $\phi^{-1}(H^{'})$ é fechado. Também, dado $a \in \phi^{-1}(H')$ temos que $\phi(a) \in H'$ logo $\phi(a^{-1}) = \phi(a)^{-1} \in H' \Rightarrow \phi^{-1}(H^{'})$ é fechado para inversos assim $\phi^{-1}(H')$ é um subgrupo de G. Se $h \in ker(\phi) \Rightarrow \phi(h) = e_{G'} \in H^{'} \Rightarrow \phi(h) \in H^{'} \Rightarrow h \in \phi^{-1}(H^{'})$, logo $ker(\phi) \subset \phi^{-1}(H^{'})$;

iii) Seja $h \in H$, como $H \trianglelefteq G$ temos que $g^{-1}hg \in H \,\forall\, g \in G$. Desta forma, $\phi(g^{-1}hg) \in \phi(H)$, assim temos que $\phi(g^{-1})\phi(h)\phi(g) \in \phi(H)$, logo pela sobrejetividade de ϕ temos $\phi(H) \trianglelefteq G^{'}$;

iv) Seja $\phi(h) \in H^{'}$, como $H^{'} \trianglelefteq G^{'}$ então $(\phi(g))^{-1}\phi(h)\phi(g) \in H^{'} \,\forall\, \phi(g) \in G^{'}$. Desta forma $(\phi(g))^{-1}\phi(h)\phi(g) = \phi(g^{-1}hg) \in H^{'} \Rightarrow g^{-1}hg \in \phi^{-1}(H^{'}) \,\forall\, g \in G$, logo $\phi^{-1}(H^{'}) \trianglelefteq G$;

v) Seja $x \in \phi^{-1}(\phi(H)) \Rightarrow \phi(x) \in \phi(H)$. Desta forma, $\phi(x) = \phi(h)$ para algum $h \in H$. Assim, $\phi(x)(\phi(h))^{-1} = e_{G'} \Rightarrow \phi(xh^{-1}) = e_{G'} \Rightarrow xh^{-1} \in ker\phi \subset H$ e por fim $x = (xh^{-1})h \in H \Rightarrow x \in H$, logo $\phi^{-1}(\phi(H)) \subset H$. Por ultimo, se $h \in H \Rightarrow \phi(h) \in \phi(H) \Rightarrow h \in \phi^{-1}(\phi(H)) \Rightarrow H \subset \phi^{-1}(\phi(H))$, logo $\phi^{-1}(\phi(H)) = H$;

vi) Se $y \in \phi(\phi^{-1}(H^{'})) \Rightarrow y = \phi(x)$, para algum $x \in \phi^{-1}(H^{'}) \Rightarrow \phi(x) \in H^{'} \Rightarrow y \in H^{'} \Rightarrow \phi(\phi^{-1}(H^{'})) \subset H^{'}$. De forma análoga, se $h^{'} \in H^{'} \Rightarrow h^{'} = \phi(x)$ para algum $x \in G$, pois ϕ é sobrejetora, $\Rightarrow x \in \phi^{-1}(H^{'}) \Rightarrow \phi(x) \in \phi(\phi^{-1}(H^{'})) \Rightarrow h^{'} \in \phi(\phi^{-1}(H^{'}))$, logo $H^{'} \subset \phi(\phi^{-1}(H^{'}))$;

vii) Seja $H \leq G$ tal que $ker\phi \subset H$, assim pelo item i) $\phi(H) \leq G^{'}$ e pelo item v) $\phi^{-1}(\phi(H)) = H$, assim $H \mapsto \phi(H)$ é injetora. Seja $H^{'} \leq G^{'}$. Pelo item ii) $\phi^{-1}(H^{'}) \leq$

G e $ker\phi \subset \phi^{-1}(H')$ e pelo item vi) $\phi(\phi^{-1}(H')) = H'$, de onde segue que $H \mapsto \phi(H)$ é sobrejetora, logo bijetora. A segunda afirmação segue dos itens iii) e iv).

□

Corolário 1.3.14. *Se N é subgrupo normal de um grupo G, então cada subgrupo de G/N é da forma K/N onde K é um subgrupo de G que contém N. Ainda mais, K/N é normal em G/N se, e somente se, K for normal em G.*

Demonstração. Considere o homomorfismo canônico $\pi : G \to G/N$, dado por $\pi(g) = gN$. Temos que $ker\pi = \{g \in G \mid \pi(g) = gN = N\} \Rightarrow ker\pi = N$. Seja $K' \leq G/N$, pelo Teorema da Correspondência existe um subgrupo K de G contendo N tal que $K' = \pi(K) = K/N$. Ainda pelo teorema da Correspondência $K \trianglelefteq G$ se, e somente se, $K/N \trianglelefteq G/N$. □

1.4 Ação de Grupos

Definição 1.4.1. *Uma ação de um grupo sobre um conjunto é uma função*

$$\begin{array}{rccc} * : & G \times M & \to & M \\ & (g, m) & \mapsto & g * m \end{array}$$

tal que

i) $e_G * x = x \ \forall \ x \in M$

ii) $(g_1 g_2) * x = g_1 * (g_2 * x) \ \forall \ x \in M$ *e* $g_1, g_2 \in G$.

Quando tal ação é dada dizemos que G age em M.

Definição 1.4.2. *Seja H um subgrupo de um grupo G. Uma ação*

$$\begin{array}{ccc} H \times G & \to & G \\ (h, g) & \mapsto & hg \end{array}$$

dizemos que $h \in H$ é uma translação (esquerda) de G.

Definição 1.4.3. *Seja H um subgrupo de um grupo G. Uma ação*

$$\begin{array}{ccc} H \times G & \to & G \\ (h, g) & \mapsto & g^h = hgh^{-1} \end{array}$$

é chamada de conjugação por h, e o elemento hgh^{-1} é dito o conjugado de g.

Teorema 1.4.4. *Seja G um grupo que age sobre um conjunto M, temos que*

i) *A relação em M definida por*

$$x \sim y \Leftrightarrow gx = y$$

para algum $g \in G$, é um relação de equivalência.

ii) *Para cada $x \in M$ $G_x = \{g \in G : gx = x\}$, é um subgrupo de G.*

Demonstração. **i)** Vamos, inicialmente, demostrar que a relação definida acima é uma relação de equivalência. Temos que $x \sim x \Leftrightarrow gx = x$, para algum $g \in G$. Em particular, tomemos $g = e_G$, portanto $e_G x = x \Rightarrow x \sim x, \forall x \in M$. Agora,

$$x \sim y \Leftrightarrow gx = y$$

operando g^{-1} em ambos os lados, obtemos

$$gx = y$$

ou seja,

$$x = g^{-1}y \Rightarrow y \sim x.$$

Por fim, se $x \sim y$ e $y \sim z$, implica que $gx = y$ e $g_1 y = z$, com $g, g_1 \in G$. Logo

$$g_1 gx = z \Rightarrow x \sim z.$$

ii) Agora vamos mostrar que G_x é um subgrupo de G. Temos que, $e_G x = x$, $\forall\ x \in M$, portanto $e_G \in G_x$. Sejam $g, h \in G_x$ então $gx = hx = x$ logo $ghx = x$ assim $gh \in G_x$. Se $g \in G_x$, então $gx = x$, o que implica $x = g^{-1}x$, logo $g^{-1} \in G_x$. Desta forma, G_x é um subgrupo de G.

□

Definição 1.4.5. *As classes de equivalência da relação definida no Teorema 1.4.4 são chamadas de orbitas de G em M; a orbita de $x \in M$ é denotada por $\overline{x}$. O subgrupo G_x é chamado de estabilizador de x.*

Definição 1.4.6. *Se um grupo G age sobre ele mesmo por conjugação, então a orbita $\{gxg^{-1} \,|\, g \in G\}$ de $x \in G$ é chamada classe de conjugação de x. Se um subgrupo H age em G por conjugação o grupo $H_x = \{h \in H \,|\, hxh^{-1} = x\} = \{h \in H \,|\, hx = xh\}$ é chamado de centralizador de x em H e denotado por $C_H(x)$. Se H age por conjugação sobre o conjunto S de todos os subgrupos de G, então o subgrupo de H que deixa fixo $K \in S$, a saber $\{h \in H \,|\, hKh^{-1} = K\}$, é chamado de normalizador de K em H e é denotado por $N_H(K)$.*

Teorema 1.4.7. *Se um grupo G age sobre um conjunto M, então a cardinalidade da orbita de $x \in M$ é o índice $[G : G_x]$.*

Demonstração. Seja S o conjunto das classes laterias de G_x em G, definimos a função

$$\begin{array}{rccc} f: & S & \to & \overline{x} \\ & gG_x & \mapsto & gx. \end{array}$$

Tomando as imagens

$$gx = hx \Leftrightarrow h^{-1}gx = x$$

assim $h^{-1}g \in G_x$, o que implica $hG_x = gG_x$, portanto a função f está bem-definida.
Seja $h \in Imf$, logo existe um $g \in G$ tal que $gx = h$. Tomando $gG_x \in S$, temos que

$$f(gG_x) = gx = h$$

portanto f é sobrejetora.
Se

$$gx = hx,$$

pela Proposição 1.1.6,

$$g = h.$$

Assim, f é injetora, e portanto bijetora. □

Corolário 1.4.8. *Seja G um grupo finito e K um subgrupo de G.*

i) *O número de elementos de uma classe de conjugação de $x \in G$ é $[G : C_G(x)]$, a qual divide $|G|$.*

ii) *Se $\overline{x_1}, ..., \overline{x_n}$ $(x_i \in G)$ são classes de conjugação distintas de G, então*

$$|G| = \sum_{i=1}^{n} [G : C_G(x_i)];$$

iii) *O número de subgrupos de G em K é $[G : N_G(K)]$ a qual divide $|G|$.*

Demonstração. Temos que i) e iii) seguem imediatamente do Teorema de Lagrange.
Segue do Teorema 1.4.4 que a conjugação é uma relação de equivalência em G, portanto G é a união das classes de conjugação. □

Definição 1.4.9. *A equação $|G| = \sum_{i=1}^{n} [G : C_G(x_i)]$ como no Corolário 1.4.8 ii) é chamada de equação das classes de um grupo finito.*

Teorema 1.4.10. *Se um grupo G age sobre um conjunto M, então essa ação induz um homomorfismo $G \to S_M$, onde S_M é o grupo de todas as permutações de M.*

Demonstração. Seja $g \in G$, definimos a função

$$\begin{array}{rccc} \tau_g: & M & \to & M \\ & x & \mapsto & gx. \end{array}$$

Desde que $x = g^{-1}(gx)$, $\forall\ x \in M$, τ_g é sobrejetora.
Se $gx = gy$, com $x, y \in M$, temos

$$x = g^{-1}(gx) = g^{-1}(gy) = y$$

portanto τ_g é injetora, logo bijetora.
Agora definindo

$$\begin{array}{rccc} \tau: & G & \to & S_M \\ & g & \mapsto & \tau_g. \end{array}$$

Se $g, g^{'} \in G$, temos que

$$\tau(gg^{'}) = \tau_{gg'} = \tau_g \circ \tau_{g'}.$$

Portanto τ é um homomorfismo.

□

Corolário 1.4.11. *(Cayley) Se G é um grupo, então existe um homomorfismo injetor $G \to S_G$. Portanto, todo grupo é isomorfo a um grupo de permutações. Em particular todo grupo finito é isomorfo a um subgrupo do S_n, com $n = |G|$.*

Demonstração. Seja G agindo em si por translação à esquerda

$$\begin{array}{rccc} *: & G \times G & \to & G \\ & (g, x) & \mapsto & gx. \end{array}$$

Pelo Teorema 1.4.10, existe um homomorfismo

$$\begin{array}{rccc} \tau: & G & \to & S_G \\ & g & \mapsto & \tau_g \end{array}$$

em que $\tau_g(x) = gx$, $\forall\ x \in G$.
Se

$$\tau(g) = \tau_g = e_g,$$

então

$$gx = \tau_g(x) = x, \forall x \in G.$$

Em particular,

$$ge = e \Rightarrow g = e.$$

Portanto, τ é injetora.

A segunda afirmação é válida porque G é isomorfo a $Im(\tau)$, que por sua vez é um subgrupo de S_G. □

Definição 1.4.12. *Se G um grupo, então definimos o conjunto de todos os automorfismos de G como $AutG$. Esse conjunto é um grupo com a operações de composição de funções.*

Corolário 1.4.13. *Seja G um grupo, então*

i) *Para cada $g \in G$, a conjugação por g induz um automorfismo de G.*

ii) *Há um homomorfismo $G \to AutG$ cujo núcleo é o conjunto $Z(G) = \{g \in G : gx = xg, \forall x \in G\}$.*

Demonstração. i) Dada a conjugação

$$\begin{array}{rccc} \tau_g : & G & \to & G \\ & x & \mapsto & gxg^{-1}. \end{array}$$

Pelo Teorema 1.4.10 τ_g é uma bijeção, desta maneira, resta mostrar que τ_g é um homomorfismo.
Dados $x, y \in G$, temos que

$$\tau_g(xy) = gxyg^{-1} = gxg^{-1}gyg^{-1} = \tau_g(x)\tau_g(y).$$

Portanto, τ_g é um automorfismo de G.
ii) Seja G agindo sobre ele mesmo por conjugação. Por i) a imagem do homomorfismo $\tau : G \to S_G$ está contida em $AutG$. Claramente,

$$g \in ker(\tau) \Leftrightarrow \tau_g = Id_G \Leftrightarrow gxg^{-1} = \tau_g(x), \forall x \in G,$$

mas

$$gxg^{-1} = x \Leftrightarrow gx = xg,$$

portanto $ker\tau = Z(G)$.

□

Proposição 1.4.14. *O subgrupo normal $Z(G) = ker\tau$, do Corolário anterior, é chamado de centro de G. Um elemento $g \in G$ está em $Z(G)$ se, e somente se, a classe de conjugação de g consiste apenas de g.*

Demonstração. Se $g \in Z(G)$, então

$$gx = gx, \forall x \in G$$

logo, $\{xgx^{-1} \mid x \in G\} = \{g\}$.
Agora, supondo que $\{xgx^{-1} \mid x \in G\} = \{g\}$, temos que $xgx^{-1} = g$, $\forall\ x \in G$, portanto, g comuta com todo elemento de G, portanto $g \in Z(G)$.

□

Assim, se G é finito e $x \in Z(G)$, então $[G : C_G(x)] = 1$. Consequentemente, a equação da classe de G pode ser escrita como

$$|G| = |Z(G)| + \sum_{i=1}^{n} [G : C_G(x_i)]$$

onde $\overline{x_1}, ..., \overline{x_n}$ são classes de conjugação de G distintas e cada $[G : C_G(x_1)] > 1$.

Proposição 1.4.15. *Seja H um subgrupo de um grupo G e G age no conjunto M de todas as classes laterias a esquerda de H em G por translação à esquerda. Então o núcleo de $G \to S_M$ está contido em H.*

Demonstração. Seja o homomorfismo

$$\begin{array}{rccc} \tau: & G & \to & S_M \\ & g & \mapsto & \tau_g \end{array}$$

onde

$$\begin{array}{rccc} \tau_g: & M & \to & M \\ & xH & \mapsto & gxH. \end{array}$$

Se $g \in ker\tau$, então $\tau_g = Id_M$ e $gxH = xH\ \forall\ x \in G$. Em particular para $x = e, geH = eH = H$, o que implica $g \in H$. □

Corolário 1.4.16. *Se H é um subgrupo de G e $[G : H] = n$ e nenhum subgrupo normal não trivial de G está contido em H, então G é isomorfo a um subgrupo do S_n.*

Demonstração. Pela Proposição 1.4.15 o homomorfismo $\tau : G \to S_M$ tem o núcleo contido em H e por hipótese $ker\tau = \{e\}$, portanto é injetor. Assim, G é isomorfo a $Im\tau$, que por sua vez é um subgrupo do S_n, já que n é o número de classes laterais de H (a esquerda). □

Corolário 1.4.17. *Se H é um subgrupo de um grupo G finito de índice p, onde p é o menor primo que divide a ordem de G, então H é normal em G.*

Demonstração. Seja M o conjunto das classes laterais a esquerda de H em G, então S_M é isomorfo a um subgrupo de S_p já que $[G : H] = |M| = p$.
Se K é o núcleo de $G \to S_M$, então K é normal em G e está contido em H. Pelo Teorema do Isomorfismo G/K é isomorfo a algum subgrupo do S_p. Então, $|G/K|$ divide $|S_p| = p!$. Mas cada divisor de $|G/K|$ deve dividir $|G| = |K|[G : K]$, já que nenhum número menor

que p pode dividir $|G|$. Então $|G/K| = p$ ou $|G/K| = 1$.
No entanto, $|G/K| = [G : K] = [G : H][H : K] = p[G : K] \geq p$. Portanto, $|G/K| = p$ e $[H : K] = 1$, onde $H = K$, logo H é normal em G. □

1.5 Os Teoremas de Sylow

Lema 1.5.1. *Se um grupo H de ordem p^n (p primo) age em um conjunto finito S e se $S_0 = \{x \in S : hx = x \ \forall \ h \in H\}$, então $|S| \equiv |S_0| \ (mod\ p)$.*

Demonstração. Temos que uma orbita $\overline{x}$ tem exatamente um elemento se, e somente se, $x \in S_0$. Desta forma, S pode ser escrito com a união disjunta

$$S = S_0 \cup \overline{x_1} \cup ... \cup \overline{x_n},$$

com $|\overline{x_i}| > 1, i = 1, ..., n$. Assim,

$$|S| = |S_0| + |\overline{x_1}| + ... + |\overline{x_n}|.$$

Agora, dado que $|\overline{x_i}| > 1$ e $|\overline{x_i}| = [H : Hx_i]$ divide $|H| = p^n$ temos que p divide $|\overline{x_i}|$ para cada i. Portanto, $|S| \equiv |S_0|(modp)$. □

Teorema 1.5.2. *(Cauchy) Se G é um grupo finito cuja ordem é divisível por um primo p, então G contém um elemento de ordem p.*

Demonstração. Seja S o conjunto das p-uplas de elementos de um grupo G,

$$S = \{(a_1, a_2, ..., a_p)/a_i \in G, a_1 a_2 \cdots a_p = e\}$$

onde a_p é determinado univocamente como $(a_1 a_2 ... a_{p-1})^{-1}$, segue então que $|S| = n^{p-1}$, com $|G| = n$. Dado que p divide n, $|S| \equiv 0(modp)$. Seja o grupo $\mathbb{Z}_p$ agindo em S por permutação cíclica, isto é, seja $k \in \mathbb{Z}_p$

$$k(a_1, a_2, ..., a_p) = (a_{k+1}, a_{k+2}, ..., a_p, a_1, ..., a_k).$$

Temos que, dado $0 \in \mathbb{Z}_p$, então

$$0(a_1, a_2, ..., a_p) = (a_1, a_2, ..., a_p).$$

E se $k, k^{'} \in \mathbb{Z}_p$, então

$$\begin{aligned}(k + k^{'})(a_1, a_2, ..., a_p) &= (a_{k+k^{'}+1}, a_{k+k^{'}+2}, ..., a_p, a_1, ..., a_{k+k^{'}}) \\ &= k(a_{k^{'}+1}, a_{k^{'}+2}, ..., a_p, a_1, ..., a_{k^{'}}) \\ &= k(k^{'}(a_1, ..., a_p))\end{aligned}$$

portanto a ação está bem-definida. Agora, $(a_1, ..., a_p) \in S_0$ se, e somente se, $a_1 = ... = a_p$; claramente $(e, e, ..., e) \in S_0$, portanto $|S_0| \neq 0$. Pelo Lema 1.5.1 $|S| \equiv |S_0| \equiv 0(modp)$. Como $|S_0| \neq 0$, então existe pelo menos p elementos em S_0 e como p é primo, logo $p \geq 2$. Desta forma, existe $a \neq e$, tal que $(a, a, ..., a) \in S_0$ e ainda $a^p = e$, portanto $|a| = p$. □

Definição 1.5.3. *Um grupo onde todo elemento possui uma ordem igual a uma potência de um p primo (fixo), é chamado de p-grupo. Se H é um subgrupo de um grupo G e H é p-grupo, então H é dito p-subgrupo de G.*

Corolário 1.5.4. *Um grupo finito G é um p-grupo se, e somente se, $|G|$ é uma potência de p.*

Demonstração. Se G é um p-grupo e q um primo que divide $|G|$, então G contém um elemento de ordem q, pelo Teorema de Cauchy. Como, por hipótese, todo elemento de G é uma potência de p, então $p = q$. Portanto, $|G|$ é uma potência de p.
A volta vem imediatamente do Teorema de Lagrange. □

Corolário 1.5.5. *O centro $Z(G)$ de um p-grupo não trivial G contém mais de um elemento.*

Demonstração. Considerando a equação das classes

$$|G| = |Z(G)| + \sum [G : Z_G(x_i)]$$

temos que p divide cada $[G : Z_G(x_i)]$ e divide $|G|$, portanto divide $|Z(G)|$, desta forma, $|C(G)| = p^i$ com $i \geq 1$ particularmente $|Z(G)| \geq 2$. □

Lema 1.5.6. *Se H é um p-subgrupo de um grupo finito G, então*

$$[N_G(H) : H] \equiv [G : H](modp).$$

Demonstração. Seja S o conjunto das classes laterais a esquerda de H em G. Suponha que H age em S por translação à esquerda. Então $|S| = [G : H]$.
Seja $S_0 = \{xH \in S : hxH = xH, \forall h \in H\}$, então

$$\begin{aligned} xH \in S_0 &\Leftrightarrow hxH = xH, \forall h \in H \\ &\Leftrightarrow x^{-1}hxH = H, \forall h \in H \\ &\Leftrightarrow x^{-1}hx \in H, \forall h \in H \\ &\Leftrightarrow x^{-1}Hx = H \\ &\Leftrightarrow xHx^{-1} = H \\ &\Leftrightarrow x \in N_G(H). \end{aligned}$$

Portanto $|S_0|$ é o número de classes xH com $x \in N_G(H)$; isso é $|S_0| = [N_G(H) : H]$. Pelo Lema 1.5.1 $[N_G(H) : H] \equiv [G : H](modp)$. □

Corolário 1.5.7. *Se H é um p-subgrupo de um grupo finito G de modo que p divide $[G : H]$, então $N_G(H) \neq H$.*

Demonstração. Temos que $0 \equiv [G : H](modp)$ pela sua vez $[G : H] \equiv [N_G(H) : H](modp)$. Portanto,
$[N_G(H) : H] \geq 2$, logo $N_G(H) \neq H$. □

Teorema 1.5.8. *(Primeiro Teorema de Sylow) Seja G um grupo com ordem $p^n m$, com $n \geq 1$, p primo, e (p,m) = 1. Então G contém um subgrupo de ordem p^j para cada $1 \leq j \leq n$ e todo subgrupo de G de ordem p^i com $i < n$ é normal em algum subgrupo de ordem p^{i+1}.*

Demonstração. Como p divide $|G|$, então G contém um elemento g de ordem p, portanto um subgrupo $\langle g \rangle$ de ordem p pelo Teorema de Cauchy.

Assumindo que H é um subgrupo de G de ordem p^i $(1 \leq i < n)$. Então p divide $[G : H]$ e pelo Corolário 1.5.7 $H \neq N_G(H)$ lembremos também que pela definição do normalizador em G, H é normal em $N_G(H)$,e faz sentido falar do grupo quociente $N_G(H)/H$, por isso e como consequência do Lema 1.5.6, p divide $|N_G(H)/H|$ e $N_G(H)$ possui um subgrupo de ordem p novamente garantido pelo teorema de Cauchy. Pelo Teorema 1.3.13 esse grupo é da forma H_1/H onde H_1 é um subgrupo de $N_G(H)$ contendo H. Desde que H seja normal em $N_G(H)$, H é normal em H_1. Por fim, $|H_1| = |H||H_1/H| = p^i p = p^{i+1}$. □

Definição 1.5.9. *Um subgrupo P de um grupo finito G é chamado de p-subgrupo de Sylow (com p um número primo) se $|P| = p^i$ para algum $i \in \mathbb{Z}^+$ e p não divide $[G : P]$.*

Teorema 1.5.10. *(Segundo Teorema de Sylow) Se H é um p-subgrupo de um grupo finito G, e P é um p-subgrupo de Sylow de G qualquer, então exite um $x \in G$ tal que $H \leq xPx^{-1}$. Em particular, qualquer dois p-subgrupos de Sylow de G são conjugados.*

Demonstração. Seja S o conjuno das classes laterais a esquerda de P em G, e H age em S por translação à esquerda. Seja $S_0 = \{xP \in S/hxP = xP, \forall h \in G\}$, dado que $|S| = [G : P]$ então $|S_0| \equiv [G : P](mod\, p)$ pelo Lema 1.5.1. Mas p não divide $[G : P]$; desta forma $|S_0| \neq 0$ então existe $xP \in S_0$,

$$\begin{aligned} xP \in S_0 &\Leftrightarrow hxP = xP, \forall h \in H \\ &\Leftrightarrow x^{-1}hx \in P, \forall h \in H \\ &\Leftrightarrow x^{-1}Hx \leq P \\ &\Leftrightarrow H \leq xPx^{-1}. \end{aligned}$$

□

Teorema 1.5.11. *(Terceiro Teorema de Sylow) Se G é um grupo finito e p um primo, então o número de p-subgrupo de Sylow de G divide $|G|$ e ele é da forma $kp + 1$ para algum $k \geq 0$.*

Demonstração. Pelo segundo Teorema de Sylow o número de p-subgrupos de Sylow é o número de conjugados diferentes de um dado P, p-subgrupo de Sylow de G. Observemos também que esse número de conjugados diferentes coincide com o número $[G : N_G(P)]$, que por sua vez é um divisor de $|G|$.
Seja S o conjunto de todos p-subgrupos de Sylow de G e P agindo em S por conjugação. Então $Q \in S_0$ se, e somente se, $xQx^{-1} = Q \ \forall \ x \in P$.
A ultima condição, $xQx^{-1} = Q \ \forall \ x \in P$, é satisfeita se, e somente se, $P \leq N_G(Q)$ e desta forma P e Q são conjugados em $N_G(Q)$. Mas dado que Q é normal em $N_G(Q)$, isso ocorre se $Q = P$. Portanto, $S_0 = \{P\}$, logo $|S_0| = 1$, assim $|S| \equiv 1(mod\, p)$, então $|S| = kp + 1$. □

Teorema 1.5.12. *Se P é um p-subgrupo de Sylow de um grupo finito G, então*

$$N_G(N_G(P)) = N_G(P).$$

Demonstração. Toda conjugação de P é um p-subgrupo de Sylow de G, além disso P é um p-subgrupo de Sylow de qualquer subgrupo de G contendo P. Dado que P é normal em $N = N_G(P)$, P será o único p-subgrupo de Sylow de N pelo Segundo Teorema de Sylow. Então,

$$x \in N_G(N) \Rightarrow xNx^{-1} = N \Rightarrow xPx^{-1} \leq N \Rightarrow xPx^{-1} = P \Rightarrow x \in N$$

logo $N_G(N_G(P)) \leq N_G(P)$, sendo obvia a outra inclusão. □

Capítulo 2

Grupos Abelianos finitos

Apresentaremos nesse capítulo uma caracterização para os grupos abelianos finitos, onde todo grupo abeliano finito pode ser visto como produto direto de $\mathbf{Z}_p$, com p um número primo. Para tal, se faz necessário a definição de novos conceitos e alguns resultados a começar pelo produto direto entre grupos.

2.1 Produto Direto

Definição 2.1.1. *Sejam $G_1, G_2, ..., G_n$ grupos. Definimos a operação sobre o produto cartesiano $G_1 \times G_2 \times \cdots \times G_n$ da seguinte forma:*

$$(a_1, a_2, ..., a_n)(b_1, b_2, ..., b_n) = (a_1b_1, a_2b_2, ..., a_nb_n).$$

É fácil verificar que $G_1 \times G_2 \times \cdots \times G_n$ é um grupo com a operação definida acima: Se e_i é o elemento neutro de G_i então $(e_1, e_2, ..., e_n)$ é o elemento neutro de $G_1 \times G_2 \times \cdots \times G_n$ e $(a_1^{-1}, a_2^{-1}, ..., a_n^{-1})$ é o elemento inverso de $(a_1, a_2, ..., a_n)$. Esse grupo é chamado produto direto de $G_1 \times G_2 \times \cdots \times G_n$.

Enunciaremos a seguir resultados que mostram uma relação direta entre a normalidade de um subgrupo e a definição acima de produto direto entre grupos. Esses resultados iniciais nos mostram que um grupo abeliano finito G pode ser visto como produto direto entre dois subgrupos normais dada a condição de ambos serem disjuntos e cada elemento de G ser escrito de maneira unívoca como a operação de dois elementos, cada um pertencente a um desses subgrupos. Com esses resultados em mãos, na próxima subseção exibiremos duas caracterizações para os grupos abelianos finitos.

Lema 2.1.2. *Sejam M e N subgrupos normais de um grupo G, tal que $M \cap N = \langle e \rangle$. Se $a \in M$ e $b \in N$, então $ab = ba$.*

Demonstração. Considere $a^{-1}b^{-1}ab$. Como M é normal, $b^{-1}ab \in M$. Assim,

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

De maneira análoga,

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

Deste modo,

$$a^{-1}b^{-1}ab \in M \cap N = \langle e \rangle,$$

assim

$$a^{-1}b^{-1}ab = e$$

$$ab = ba.$$

□

Teorema 2.1.3. *Sejam $N_1, N_2, ..., N_k$ subgrupos normais de um grupo G, onde cada elemento em G pode ser escrito univocamente da forma $a_1a_2\cdots a_k$, com $a_i \in N_i$. Então G é isomorfo ao produto direto $N_1 \times N_2 \times \cdots \times N_k$.*

Demonstração. Definindo a função

$$\begin{array}{rccc} f: & N_1 \times N_2 \times \cdots \times N_k & \longrightarrow & G \\ & f(a_1, a_2, ..., a_k) & \longmapsto & a_1a_2\cdots a_k \end{array}$$

Como, por hipótese, todo elemento de G pode ser escrito da forma $a_1a_2\cdots a_k$ (com $a_i \in N_i$) f é sobrejetora.

Se $f(a_1, a_2, ..., a_k) = f(b_1, b_2, ..., b_k)$ então $a_1a_2\cdots a_k = b_1b_2\cdots b_k$, e pela unicidade da hipótese $a_i = b_i$ para cada i $(1 \geq i \geq k)$. Portanto, f é injetora.

Antes de mostrar que f é homomorfismo, veremos que os N_i são disjuntos dois a dois, ou seja $N_i \cap N_j = \langle e \rangle$ quando $i \neq j$.

Se $a \in N_i \cap N_j$ então a pode ser escrito como um produto de elementos dos N_i de duas formas

$$\begin{array}{ccccccccccccc} e\cdots e & a & e\cdots e & e & e\cdots e = a = e\cdots e & e & e\cdots e & a & e\cdots e. \\ & \uparrow & & \uparrow & & \uparrow & & \uparrow & \\ & N_i & & N_j & & N_i & & N_j & \end{array}$$

e assim, a hipótese de unicidade implica $a = e$. Portanto, $N_i \cap N_j = \langle e \rangle$ para $i \neq j$.

Para mostrar que f é um homomorfismo é necessário utilizar o Lema 2.1.2, que implica $a_ib_j = b_ja_i$ para $a_i \in N_i$ e $b_j \in N_j$. Portanto, temos que

$$\begin{aligned} f[(a_1, a_2, ..., a_k)(b_1, b_2, ..., b_k)] &= f(a_1b_1, ..., a_kb_k) \\ &= a_1b_1a_2b_2 \cdots a_kb_k \\ &= a_1a_2b_1b_2 \cdots a_kb_k \\ &= a_1a_2 \cdots a_kb_1b_2 \cdots b_k \\ &= f(a_1, a_2, ..., a_k)f(b_1, b_2, ..., b_k). \end{aligned}$$

Logo, f é um homomorfismo e assim, um isomorfismo.

□

Teorema 2.1.4. *Se M e N são subgrupos normais de um grupo G, de modo que $G = MN$ $(MN = \{mn : m \in M \text{ e } n \in N\})$ e $M \cap N = \langle e \rangle$, então $G \cong M \times N$.*

Demonstração. Por hipótese todo elemento de G é da forma mn, com $m \in M$ e $n \in N$. Supondo que um elemento pode ser escrito de duas formas, $mn = m_1n_1$ com $m, m_1 \in M$ e $n, n_1 \in N$. Então,

$$mn = m_1n_1,$$

segue que,

$$m_1^{-1}mn = n_1,$$

ou seja,

$$m_1^{-1}m = n_1n^{-1}.$$

Como $m_1^{-1}m \in M$ e $n_1n^{-1} \in N$, e ainda $M \cap N = \langle e \rangle$, temos que $m_1^{-1}m = e$. De onde, tem-se $m = m_1$; De modo análogo $n = n_1$. Portanto, todo elemento de G pode ser escrito univocamente da forma mn com $m \in M$ e $n \in N$, e assim, $G \cong M \times N$, pelo Teorema 2.1.3. □

2.2 Grupos Abelianos Finitos

Definição 2.2.1. *Se G é um grupo abeliano e p um número primo, então $G(p)$ denota o conjunto dos elementos de G cuja a ordem é uma potência de p; a saber*

$$G(p) = \{g \in G \,|\, |g| = p^n, n \geq 0\}.$$

É fácil ver que $G(p)$ é fechado para inversos e é não vazio pois $e \in G(p)$. Ainda, se $g, g_1 \in G(p)$ tal que $|g| = p^k$ e $|g_1| = p^s$ com $s < k$, então $(gg_1)^{p^k} = g^{p^k}g_1^{p^k} = eg_1^{p^{s+(k-s)}} = e^{p^{k-s}} = e$. Logo, $G(p)$ é fechado e, portanto, $G(p)$ é um subgrupo de G.

Esse subgrupo será útil em nosso objetivo de caracterizar os grupos abelianos pois, como veremos a seguir, todo grupo abeliano pode ser visto como um produto direto de

$G(p_i)$. Com tal objetivo em mente, enunciaremos o seguinte resultado que mostra que todo elemento de um grupo abeliano pode ser visto como produto de elementos de $G(p_i)$.

Lema 2.2.2. *Seja G um grupo abeliano e a um elemento G de ordem finita. Então $a = a_1a_2\cdots a_t$, com $a_i \in G(p_i)$, onde $p_1, p_2, ..., p_t$, são primos distintos que dividem a ordem de a.*

Demonstração. Vamos provar por indução sob o número de primos distintos que dividem a ordem de a. Se $|a|$ é divisível por um único primo p_1, então a ordem de a é igual a uma potência de p_1, portanto $a \in G(p_1)$. O Lema é verdadeiro nesse caso.

Assumindo por hipótese de indução que o Lema é valido para todo elemento cuja a ordem é divisível por um número $k-1$ de primos distintos e a $|a|$ é divisível por k primos distintos $p_1, p_2, ..., p_k$. Então $|a| = p_1^{r_1}\cdots p_k^{r_k}$, com cada $r_i > 0$. Seja $n = p_1^{r_1}$, $m = p_2^{r_2}\cdots p_k^{r_k}$, então $|a| = mn$. Temos que $(m, n) = 1$, e portanto é possível encontrar inteiros r, s tais que $mr + ns = 1$. Consequentemente

$$a = a^{mr+ns} = a^{mr}a^{ns}$$

mas $a^{mr} \in G(p_1)$ devido a que a possui ordem mn, pelo fato de

$$a^{(mr)n} = a^{(mn)r} = e^r = e$$

da mesma forma,

$$a^{(ns)m} = a^{(nm)s} = e^s = e.$$

Pelo Teorema 1.1.10 a ordem de a^{ns} divide m, um número inteiro com somente $k-1$ divisores distintos. Portanto, pela hipótese de indução $a^{ns} = a_2a_3\cdots a_k$, com $a_i \in G(p_i)$. Seja $a_1 = a^{mr}$, então

$$a = a_1a_2\cdots a_k,$$

com $a_i \in G(p_i)$. □

Dado o lema acima, nos resta mostrar que a expressão $a = a_1a_2\cdots a_t$, com $a_i \in G(p_i)$ é unívoca para podemos concluir que todo grupo abeliano finito pode ser visto como produto direto dos $G(p_i)$. Para tal, enunciamos o seguinte teorema.

Teorema 2.2.3. *Se G é um grupo abeliano finito, então*

$$G = G(p_1) \times G(p_2) \times \cdots \times G(p_t),$$

onde $p_1, p_2, ..., p_t$ são primos distintos que dividem a ordem de G.

Demonstração. Se $a \in G$, então $|a|$ divide $|G|$. Por isso, pelo Lema 2.2.2 $a = a_1a_2\cdots a_t$, com $a_i \in G(p_i)$ (onde $a_j = e$ se p_j não dividir $|a|$).

A prova que essa expressão é univoca consiste em supor $a_1a_2\cdots a_t = b_1b_2\cdots b_t$ com $a_i, b_i \in G(p_i)$. Dado que G é abeliano

$$a_1b_1^{-1} = (b_2a_2^{-1})(b_3a_3^{-1})\cdots(b_ta_t^{-1}).$$

Para cada i, a_i, $b_i \in G(p_i)$ e, por isso, possui ordem igual a uma potência de p_i, suponhamos que $(a_ib_i^{-1})^{p_i^{r_i}} = e$.

Seja $m = p_2^{r_2} \cdot p_t^{r_t}$, então $(a_ib_i^{-1})^m = e$ para $i \geq 2$, portanto

$$(a_1b_1^{-1})^m = (b_2a_2^{-1})^m \cdots (b_ta_t^{-1})^m = e\cdots e = e.$$

Consequentemente, a ordem de $a_1b_1^{-1}$ divide m pelo Teorema 1.1.10. Mas $a_1b_1^{-1} \in G(p_1)$, então sua ordem é uma potência de p_1. A única potência de p_1 que divide $m = p_2^{r_2}\cdots p_t^{r_t}$ é $p_1^0 = 1$. Portanto, $a_1b_1^{-1} = e$ e $a_1 = b_1$. Um argumento similar para $i = 2, .., t$ mostra que $a_i = b_i$ para todo i. Portanto cada elemento de G pode ser escrito univocamente da forma $a_1a_2\cdots a_t$, com $a_i \in G(p_i)$ e por isso, $G = G(p_1) \times G(p_2) \times \cdots \times G(p_t)$ pelo Teorema 2.1.3.

□

Lembrando que, se p é um primo então um grupo onde todos os elementos possuem ordem igual a uma potência de p é chamado p-grupo. Cada um dos $G(p_i)$ do Teorema 2.2.3 são um p-grupo. Portanto, todo grupo abeliano finito pode ser visto como o produto direto de p-grupos, nos restando provar, para alcançamos o objetivo de mostrar que todo grupo abeliano finito é um produto dos $\mathbf{Z_p}$, que cada $G(p_i)$ pode ser visto como produto direto de $\mathbf{Z_p}$. Para isso, enunciamos uma nova definição.

Definição 2.2.4. *Um elemento a de um p-grupo B é chamado um elemento de ordem máxima se $|b| \leq |a|$ para todo $b \in B$. Se $|a| = p^n$, então b possui ordem p^f com $f \leq n$. Assim, $b^{p^n} = (b^{p^f})^{p^{n-f}} = e^{p^{n-f}} = e$. Portanto, se a é um elemento de ordem máxima p^n em um p-grupo B, então $b^{p^n} = e$ para todo $b \in B$.*

Usando a definição acima, enunciamos o seguinte resultado que será vital para demostrarmos o teorema que caracteriza os grupos abelianos finitos. A demostração é longa e cheia de pequenos detalhes requerendo uma atenção especial do leitor.

Lema 2.2.5. *Seja G um p-grupo abeliano finito e a um elemento de ordem máxima em G. Então existe um subgrupo K de G tal que $G \cong \langle a\rangle \times K$.*

Demonstração. Considere os subgrupos H de G tais que $\langle a\rangle \cap H = \langle e\rangle$. Existe pelo menos um subgrupo $H = \langle e\rangle$, e como G é finito, existe um subgrupo K de G com ordem máxima satisfazendo $\langle a\rangle \cap K = \langle e\rangle$, assim para demostrar o Lema, pelo Teorema 2.1.4, basta mostrarmos que $G = \langle a\rangle K$.

Supondo que $G \neq \langle a\rangle K$, então existe $b \in G\,(b \neq e)$ tal que $b \notin \langle a\rangle K$. Seja n o menor inteiro positivo tal que $b^{p^n} \in \langle a\rangle K$ (esse n existe pelo fato de G ser um p-grupo finito, então, $b^{p^l} = e \in \langle a\rangle K$, para algum inteiro positivo l) então

$$b^{p^{n-1}} = c \notin \langle a\rangle K \tag{2.1}$$

e

$$b^{p^n} = c^p \in \langle a\rangle K$$

implicando em

$$c^p = a^t k\,(t \in \mathbb{Z}, k \in K) \tag{2.2}$$

Se a possuir ordem p^n, então $x^{p^n} = e$, $\forall x \in G$ pelo fato de a ser um elemento de ordem máxima em G. Consequentemente, por (2.2), temos

$$(a^t)^{p^{n-1}} k^{p^{n-1}} = (a^t k)^{p^{n-1}} = (c^p)^{p^{n-1}} = c^{p^n} = e$$

Portanto $(a^t)^{p^{n-1}} = (k^{p^{n-1}})^{-1} \in \langle a\rangle \cap K = \langle e\rangle$ e $(a^t)^{p^{n-1}} = e$. Ainda, p^n (ordem de a), pelo Teorema 1.1.10, divide tp^{n-1}, de onde segue que $p|t$, ou seja $t = pm(m \in \mathbb{Z})$. Portanto, $c^p = a^t k = a^{pm} k$ e consequentemente, $k = c^p (a^{pm})^{-1} = (c(a^m)^{-1})^p$. Seja

$$d = c(a^m)^{-1} \tag{2.3}$$

então $d^p = (c(a^m)^{-1})^p = k \in K$, mas $d \notin K$ (se $c(a^m)^{-1} = k' \in K \Rightarrow c = a^m k' \in \langle a\rangle K$, contradizendo 2.1).

É fácil provar que o conjunto $H = \{xd^z \,|\, x \in K, z \in \mathbb{Z}\}$ é um subgrupo de G e $K \subset H$. Temos que $d = ed \in H$, e $d \notin K$, assim H possui ordem maior que a ordem de K, mas K é o subgrupo de G com maior ordem tal que $\langle a\rangle \cap K = \langle e\rangle$, então nos resta verificar quem é $\langle a\rangle \cap H$.

Se w é um elemento não trivial de $\langle a\rangle \cap H$, então

$$w = a^s = k_1 d^r (k_1 \in K; s, r \in \mathbb{Z}). \tag{2.4}$$

Temos que p não divide r, caso contrário $r = py$, e isso implica que $d^r \in K$, logo $k_1 d^r \in K$ assim $k_1 d^{py} \in \langle a\rangle \cap K$, uma contradição ao fato de $w \neq e$. Consequentemente, $(p, r) = 1$,

então existem inteiros u, v tais que $pu + rv = 1$, então

$$\begin{aligned} c = c^1 = c^{pu+rv} &= (c^p)^u (c^r)^v \\ &= (a^t k)^u ((da^m)^r)^v \\ &= (a^t k)^u ((d)^r (a^m)^r)^v \\ &= (a^t k)^u (a^s k_1^{-1} (a^m)^r)^v \\ &= a^{tu+sv+mrv} k^u (k_1^v)^{-1} \in \langle a \rangle K, \end{aligned}$$

uma contradição por (2.1). Portanto, $G = \langle a \rangle K$ e pelo Teorema 2.1.4 $G = \langle a \rangle \times K$. □

Teorema 2.2.6. *(Teorema Fundamental dos Grupos Abelianos Finitos) Todo grupo abeliano finito G é um produto direto de grupos cíclicos, cada um com ordem igual a uma potência de primo.*

Demonstração. Pelo Teorema 2.2.3, G é um produto direto de subgrupos $G(p)$, onde cada primo p divide $|G|$ e $G(p)$ é um p-grupo.

Para completar a demonstração, é necessário mostrar que todo p-grupo abeliano finito H é um produto direto direto de grupos cíclicos, cada um com ordem igual a uma potência de um primo.

Provando por indução sob a ordem de H, a afirmação é verdadeira quando H possui ordem p pelo Teorema 1.2.7. Assumindo que a afirmação é verdadeira para todos os p-grupos de ordem menor que $|H|$ e a um elemento de ordem máxima em H. Então, pelo Lema 2.2.5, $H = \langle a \rangle \times K$. Por hipótese de indução K é um produto direto de grupos cíclicos, cada um com a ordem igual a uma potência de p. Portanto, a afirmação também vale para $H = \langle a \rangle \times K$. □

O teorema acima, com o auxilio do teorema fundamental da aritmética, caracteriza todos os grupos abelianos finitos G, demostrando que G pode ser visto como produto direto de grupos cíclicos de ordem prima.

Capítulo 3

Solubilidade

Nesse capítulo apresentaremos os principais resultados deste trabalho que consiste em exibir duas caracterizações para os grupos solúveis. Começaremos introduzindo o conceito de comutador que auxiliará na caracterização dos grupos solúveis. Como foi dito na introdução, os grupos solúveis podem ser vistos como próximos de serem abelianos, com isso em mente, a definição do comutador de dois elementos, definida abaixo, se torna natural pois em um grupo abeliano todo comutador é igual ao elemento neutro, portanto, voltaremos a nossa atenção aos comutadores não triviais.

3.1 Comutadores

Definição 3.1.1. *Dado dois elementos x, y de um grupo G, o comutador de x e y é o elemento*

$$[x, y] = x^{-1}y^{-1}xy \in G.$$

Mais geralmente, definimos um comutador simples de comprimento $n \geq 2$ por

$$[x_1, ..., x_n] = [[x_1, ..., x_{n-1}], x_n].$$

Dados dois subconjuntos H e K de um grupo G, denotaremos por $[H, K]$ o subgrupo de G gerado pelo conjunto

$$\{[h, k] : h \in H, k \in K\}.$$

Em particular, o grupo $G' = [G, G]$ chama-se subgrupo comutador ou subgrupo derivado de G.

Indutivamente podemos definir uma sequência de subgrupos da seguinte forma:

$$\begin{aligned} G^{(0)} &= G \\ G^{(1)} &= [G^{(0)}, G^{(0)}] = G' \\ &\vdots \\ G^{(n)} &= [G^{(n-1)}, G^{(n-1)}]. \end{aligned}$$

Definição 3.1.2. *O subgrupo $G^{(n)}$ definido acima chama-se o n-ésimo grupo derivado de G e a sequência*

$$G = G^{(0)} \geq G^{(1)} \geq \cdots \geq G^{(n)} \geq \cdots$$

chama-se a série derivada de G.

O lema a seguir enumera as principais propriedades do comutador.

Lema 3.1.3. *Sejam x, y, z e t elementos de um grupo G. Então:*

i) $[x, y] = 1$ *se e somente se* $xy = yx$;

ii) $[x, y]^{-1} = [y, x]$;

iii) $[x, y]^z = [x^z, y^z]$;

iv) $[xy, z] = [x, z]^y[y, z] = [x, z][[x, z], y][y, z]$;

v) $[x, yz] = [x, z][x, y]^z = [x, z][x, y][[x, y], z]$;

vi) $[x, y]z = z[x^z, y^z]$;

vii) $[x^y, z] = [x, z]^{[x,y]}[x, y, z]$;

viii) $[x^{yz}, t] = [x^y, t]^{[x^y,z]}[x^y, z, t]$;

ix) $[x, y, z] = [x, y]^{-1}[x, y]^z$;

x) *Se ϕ: $G \to H$ é um homomorfismo de grupos, então* $\phi([x, y]) = [\phi(x), \phi(y)]$.

Demonstração.

i) $[x, y] = 1 \Leftrightarrow x^{-1}y^{-1}xy = 1 \Leftrightarrow xy = yx$.

ii) $[x, y]^{-1} = (x^{-1}y^{-1}xy)^{-1} = y^{-1}x^{-1}yx = [y, x]$.

iii)

$$\begin{aligned}
[x, y]^z &= (x^{-1}y^{-1}xy)^z \\
&= z^{-1}x^{-1}y^{-1}xyz \\
&= z^{-1}x^{-1}zz^{-1}y^{-1}zz^{-1}xz^{-1}zyz \\
&= (x^{-1})^z(y^{-1})^z x^z y^z \\
&= (x^z)^{-1}(y^z)^{-1}x^z y^z \\
&= [x^z, y^z].
\end{aligned}$$

iv)

$$\begin{aligned}
[xy,z] &= (xy)^{-1}z^{-1}xyz \\
&= y^{-1}x^{-1}z^{-1}xyz \\
&= y^{-1}x^{-1}z^{-1}xzyy^{-1}z^{-1}yz \\
&= (y^{-1}x^{-1}z^{-1}xzy)(y^{-1}z^{-1}yz) \\
&= (x^{-1}z^{-1}xz)^y(y^{-1}z^{-1}yz) \\
&= [x,z]^y[y,z] \\
&= y^{-1}x^{-1}z^{-1}xyz \\
&= x^{-1}z^{-1}xzz^{-1}x^{-1}zxy^{-1}x^{-1}z^{-1}xyz \\
&= x^{-1}z^{-1}xz(x^{-1}z^{-1}xz)^{-1}y^{-1}x^{-1}z^{-1}xzyy^{-1}z^{-1}yz \\
&= x^{-1}z^{-1}xz[x^{-1}z^{-1}xz,y]y^{-1}z^{-1}yz \\
&= [x,z][[x,z],y][y,z].
\end{aligned}$$

v)

$$\begin{aligned}
[x,yz] &= x^{-1}z^{-1}y^{-1}xyz \\
&= x^{-1}z^{-1}xzz^{-1}x^{-1}y^{-1}xyz \\
&= (x^{-1}z^{-1}xz)(z^{-1}x^{-1}y^{-1}xyz) \\
&= [x,z][x,y]^z \\
&= x^{-1}z^{-1}y^{-1}xyz \\
&= x^{-1}z^{-1}xzx^{-1}y^{-1}xyy^{-1}x^{-1}yxz^{-1}x^{-1}y^{-1}xyz \\
&= (x^{-1}z^{-1}xz)(x^{-1}y^{-1}xy)(x^{-1}y^{-1}xy)^{-1}z^{-1}(x^{-1}y^{-1}xy)z \\
&= [x,z][x,y][(x^{-1}y^{-1}xy),z] \\
&= [x,z][x,y][[x,y],z].
\end{aligned}$$

vi)

$$\begin{aligned}
[x,y]z &= x^{-1}y^{-1}xyz \\
&= zz^{-1}x^{-1}y^{-1}xyz \\
&= z(x^{-1}y^{-1}xy)^z \\
&= z[x,y]^z \\
&= z[x^z,y^z].
\end{aligned}$$

vii)

$$\begin{aligned}
[x^y,z] &= [y^{-1}xy,z] \\
&= (y^{-1}xy)^{-1}z^{-1}y^{-1}xyz \\
&= y^{-1}x^{-1}yz^{-1}y^{-1}xyz \\
&= y^{-1}x^{-1}yxx^{-1}z^{-1}y^{-1}xyz \\
&= (x^{-1}y^{-1}xy)^{-1}x^{-1}z^{-1}y^{-1}xyz \\
&= (x^{-1}y^{-1}xy)^{-1}x^{-1}z^{-1}xzx^{-1}y^{-1}xyy^{-1}x^{-1}yxz^{-1}x^{-1}y^{-1}xyz \\
&= ((x^{-1}y^{-1}xy)^{-1}(x^{-1}z^{-1}xz)x^{-1}y^{-1}xy)(y^{-1}x^{-1}yx)z^{-1}(x^{-1}y^{-1}xy)z \\
&= (x^{-1}z^{-1}xz)^{(x^{-1}y^{-1}xy)}[(x^{-1}y^{-1}xy),z] \\
&= [x,z]^{[x,y]}[x,y,z].
\end{aligned}$$

viii)

$$\begin{aligned}
[x^{yz},t] &= [(yz)^{-1}xyz,t]\\
&= [z^{-1}y^{-1}xyz,t]\\
&= (z^{-1}y^{-1}xyz)^{-1}t^{-1}z^{-1}y^{-1}xyzt\\
&= z^{-1}y^{-1}x^{-1}yzt^{-1}z^{-1}y^{-1}xyzt\\
&= z^{-1}y^{-1}x^{-1}yz(y^{-1}xyy^{-1}x^{-1}y)t^{-1}(y^{-1}xyty^{-1}x^{-1}yz^{-1}y^{-1}xyzz^{-1}\\
&y^{-1}x^{-1}yzy^{-1}xyt^{-1}y^{-1}x^{-1}y)z^{-1}y^{-1}xyzt\\
&= (z^{-1}y^{-1}x^{-1}yzy^{-1}xy)(y^{-1}x^{-1}yt^{-1}y^{-1}xyt)(y^{-1}x^{-1}yz^{-1}y^{-1}xyz)\\
&(z^{-1}y^{-1}x^{-1}yzy^{-1}xy)(t^{-1}y^{-1}x^{-1}yz^{-1}y^{-1}xyzt)\\
&= (y^{-1}x^{-1}yz^{-1}y^{-1}xyz)^{-1}(y^{-1}x^{-1}yt^{-1}y^{-1}xyt)(y^{-1}x^{-1}yz^{-1}y^{-1}xyz)\\
&(y^{-1}x^{-1}yz^{-1}y^{-1}xyz)^{-1}t^{-1}(y^{-1}x^{-1}yz^{-1}y^{-1}xyz)t\\
&= (y^{-1}x^{-1}yt^{-1}y^{-1}xyt)^{(y^{-1}x^{-1}yz^{-1}y^{-1}xyz)}[(y^{-1}x^{-1}yz^{-1}y^{-1}xyz),t]\\
&= ((y^{-1}xy)^{-1}t^{-1}y^{-1}xyt)^{((y^{-1}xy)^{-1}z^{-1}y^{-1}xyz)}[((y^{-1}xy)^{-1}z^{-1}y^{-1}xyz),t]\\
&= [y^{-1}xy,t]^{[y^{-1}xy,z]}[[y^{-1}xy,z],t]\\
&= [x^{y},t]^{[x^{y},z]}[[x^{y},z],y]\\
&= [x^{y},t]^{[x^{y},z]}[x^{y},z,y].
\end{aligned}$$

ix)

$$\begin{aligned}
[x,y,z] &= [[x,y],z]\\
&= [x^{-1}y^{-1}xy,z]\\
&= (x^{-1}y^{-1}xy)^{-1}z^{-1}x^{-1}y^{-1}xyz\\
&= y^{-1}x^{-1}yxz^{-1}x^{-1}y^{-1}xyz\\
&= (y^{-1}x^{-1}yx)(z^{-1}x^{-1}y^{-1}xyz)\\
&= [y,x](x^{-1}y^{-1}xy)^{z}\\
&= [x,y]^{-1}[x,y]^{z}.
\end{aligned}$$

x)

$$\begin{aligned}
\phi([x,y]) = \phi(x^{-1}y^{-1}xy) &= \phi(x^{-1})\phi(y^{-1})\phi(x)\phi(y)\\
&= (\phi(x))^{-1}(\phi(y))^{-1}\phi(x)\phi(y)\\
&= [\phi(x),\phi(y)].
\end{aligned}$$

□

O lema a seguir nos mostra uma relação direta entre o grupo quociente e o subgrupo derivado. Tal resultado tem forte relação com a a solubilidade de um grupo como definiremos na subseção seguinte.

Lema 3.1.4. *Seja H um subgrupo normal de um grupo G. Então, o grupo quociente G/H é abeliano se e somente se $G' \subset H$.*

Demonstração. Assumindo que G/H é abeliano, então para quaisquer $x, y \in G$

$$\begin{aligned} xHyH = yHxH &\Leftrightarrow x^{-1}Hy^{-1}HxHyH = H \\ &\Leftrightarrow x^{-1}y^{-1}xyH = H \\ &\Leftrightarrow [x,y]H = H \\ &\Leftrightarrow [x,y] \in H \\ &\Leftrightarrow G' \in H. \end{aligned}$$

□

Definição 3.1.5. *Um subgrupo H de um grupo G diz-se um subgrupo característico se $\phi(H) = H$ para todo automorfismo $\phi : G \to G$. Para indicar que H é subgrupo característico de G escrevemos H car G.*

Todo subgrupo característico é em particular um subgrupo normal. Tal observação pode ser demostrada levando em consideração que a conjugação por um elemento fixo é um automorfismo, a saber

$$\begin{aligned} Inn_a : \ G &\to G \\ x &\mapsto a^{-1}xa. \end{aligned}$$

Assumindo que H é um subgrupo característico, então para todo $h \in H$, $a^{-1}ha \in H$. Tal raciocínio pode ser estendido a qualquer elemento de G, portanto $a^{-1}Ha \subset H$, $\forall$ $a \in G$ e isso ocorre se, e somente se $H \trianglelefteq G$.

Se $\phi : G \to G$ é um automorfismo e H um subgrupo característico de G, então a restrição de ϕ a H é um automorfismo de H. Desta observação segue facilmente que se K car H e H car G, então K car G.

Proposição 3.1.6. *Seja H um subgrupo de um grupo G. Se H é característico em G então H' também é característico em G. Em particular, $G^{(n)}$ é característico em G, para todo inteiro positivo n.*

Demonstração. Seja H car G e $H' = \langle [h,g] \rangle$ com $h, g \in H$. Como, por definição de homomorfismo, $\phi([a,b]) = [\phi(a), \phi(b)]$, e todo elemento de H' e um produto de comutadores, temos que

$$\phi(\langle [h,g] \rangle) = \langle [\phi(h), \phi(g)] \rangle = H'.$$

A segunda afirmação segue trivialmente.

□

A proposição anterior nos garante que a série derivada $G \geq G' \geq G^{(2)} \geq \cdots \geq G^{(n)}$, é uma cadeia normal. Por outro lado, o Lema 3.1.4 garante que os fatores dessa série são abelianos.

3.2 Grupos Solúveis

Definição 3.2.1. *Um grupo G diz-se solúvel se contém uma cadeia de subgrupos*

$$\{1\} = G_0 \leq G_1 \leq \cdots \leq G_n = G$$

tal que cada subgrupo G_{i-1} é normal em G_i e o grupo quociente G_i/G_{i-1}, $1 \geq i \geq n$, é abeliano.

Uma cadeia de subgrupos de G com a propriedade $G_{i-1} \trianglelefteq G_i$ chama-se uma série subnormal de G e os quocientes respectivas chamam-se os fatores da série. Quando todos os fatores são abelianos dizemos que a série é uma série subnormal abeliana.

A seguir, enunciaremos alguns exemplos de grupos solúveis.

Exemplo 3.2.2. *Todo grupo abeliano é solúvel.*

De fato, $\{1\} \trianglelefteq G$ é uma série subnormal com fatores abelianos.

Exemplo 3.2.3. *S_3 é solúvel.*

A série $\{1\} \leq A_3 \leq S_3$ é uma série subnormal com fatores abelianos. De fato, $\{1\} \trianglelefteq A_3$ e como $[S_3 : A_3] = 2$ logo $A_3 \trianglelefteq S_3$. Por fim, A_3 é isomorfo a $\mathbb{Z}_3$ e S_3/A_3 é isomorfo a $\mathbb{Z}_2$, portanto S_3/A_3 é abeliano.

Exemplo 3.2.4. *S_4 é solúvel.*

Considerando $H = \{e, (12)(34), (13)(24), (14)(23)\}$. A_4 é normal em S_4 pelo fato de $[S_4 : A_4] = 2$ e H é normal em A_4 pelo fato da ação por conjugação preservarem a estrutura cíclica das permutações. Desse modo, $\{1\} \leq H \leq A_4 \leq S_4$ é uma série subnormal com fatores abelianos.

Exemplo 3.2.5. *Todo p-grupo finito é solúvel.*

Seja G um grupo tal que $|G| = p^n$. Vamos demostrar a afirmação por indução em n.

Se $n = 0$, o resultado segue trivialmente. Agora, supondo que $|G| = p^n$ e o resultado é válido para $n - 1$.

Sabemos pelo corolário 1.5.5 que o centro de G possui mais de um elemento, portanto existe um elemento z pertencente ao centro de G cuja $|z| = p$. Desda forma, $|\frac{G}{<z>}| = p^{n-1}$ e por hipótese de indução existe

$$\{1\} = \frac{< z >}{< z >} \leq \frac{G_0}{< z >} \leq \cdots \leq \frac{G_t}{< z >} = \frac{G}{< z >}$$

uma série subnormal com fatores abelianos, onde cada $|\frac{G_{i+1}/<z>}{G_i/<z>}| = p$. Pelo teorema da correspondência cada G_i é um subnormal que contém $< z >$.

Segue do teorema do isomorfismo que

$$\frac{G_{i+1}/ < z >}{G_i/ < z >} \cong \frac{G_{i+1}}{G_i},$$

de onde segue que

$$\{1\} = G_0 \leq G_1 \leq \cdots \leq G_t = G$$

é uma série subnormal com fatores abelianos.

Exemplo 3.2.6. *Todo grupo G de ordem pq, p e q primos distintos é solúvel.*

Pelo Teorema de Sylow existe $P \leq G$ tal que $|P| = p$. Temos que o número de p-subgrupos de sylow de G será congruente a 1 modulo q e q divide o número de p-subgrupos de Sylow de G, assim como q é um primo temos que o numero de p-subgrupos de Sylow será igual a 1. Logo, $P \trianglelefteq G$, assim

$$\{1\} \leq P \leq G$$

é uma série normal com fatores abelianos, portanto G é solúvel.

O próximo teorema nos dá uma caracterização dos grupos solúveis em termos da série derivada. Como visto no teorema 3.1.4, o subgrupo derivado necessariamente precisa está contido no primeiro subgrupo da série subnormal de um grupo solúvel. O próximo resultado, no sentido oposto da série subnormal, nos mostra que o fato da série derivada se encerrar é condição necessária e suficiente para a normalidade de um grupo.

Teorema 3.2.7. *Um grupo é solúvel se e somente se sua série derivada termina, isto é, se existe um inteiro positivo n tal que $G^{(n)} = \{1\}$.*

Demonstração. Se existir um n natural tal que $G^{(n)} = \{1\}$, então

$$G \geq G' \geq G^{(2)} \geq \cdots \geq G^{(n)} = \{1\}$$

é uma série subnormal com fatores abelianos.

Se G é solúvel, existe uma série subnormal abeliana

$$G \geq G_1 \geq \cdots \geq G_n = \{1\}.$$

Como cada G_i/G_{i-1} é abeliano, pelo Lema 3.1.4 segue que $G^{(i)} \leq G_i, 1 \geq i \geq n$. Logo, em particular $G^{(n)} = \{1\}$. □

Corolário 3.2.8. *Subgrupos de grupos solúveis são solúveis.*

Demonstração. Seja

$$G = G_0 \geq G_1 \geq \cdots \geq G_n = \{1\},$$

uma série subnormal de G. Considere a série

$$H = H_0 \geq (H \cap G_1) \geq \cdots \geq (H \cap G_n) = \{1\},$$

segue que,

$$H \cap G_{i+1} = (H \cap G_i) \cap G_{i+1} \trianglelefteq H \cap G_i \, \forall \, i = 1, ..., n.$$

Pelo segundo Teorema do Isomorfismo, temos que

$$\frac{H \cap G_i}{H \cap G_{i+1}} = \frac{H \cap G_i}{(H \cap G_i) \cap G_{i+1}} \cong \frac{G_{i+1}(H \cap G_i)}{G_{i+1}} \leq \frac{G_i}{G_{i+1}};$$

Como G_i/G_{i+1} é abeliano $G_{i+1}(H \cap G_{i+1})/G_{i+1}$ também é abeliano; Logo

$$H = H_0 \geq (H \cap G_1) \geq \cdots \geq (H \cap G_n) = \{1\},$$

é uma série subnormal com fatores abelianos, logo H é solúvel. □

Lema 3.2.9. *Seja H um subgrupo normal de um grupo G. Se ambos H e G/H são solúveis então G é solúvel.*

Demonstração. Como G/H é solúvel, pelo Teorema 3.2.7, existe um n natural tal que $(G/H)^{(n)} = \{1\}$. Portanto $G^{(n)} \leq H$. Da mesma forma, como H é solúvel existe um m natural tal que $H^{(m)} = \{1\}$. Assim,

$$\begin{aligned} &G^{(n)} \leq H \\ &G^{(nm)} \leq H^{(m)} = \{1\}, \end{aligned}$$

logo G é solúvel.

□

O próximo teorema nos dá uma caracterização dos grupos solúveis a partir da série de composição, que mostra, semelhante aos grupos abelianos finitos, os grupos solúveis podem ser vistos a partir de extensões de grupos cíclicos de ordem prima comprovando a proximidade desses dois objetos.

Teorema 3.2.10. *Um grupo solúvel finito G contém uma série subnormal abelina cujos fatores são todos cíclicos de ordem prima.*

Demonstração. Vamos demonstrar o teorema por indução na ordem de G. Se $|G| = 1$ não há nada a se provar. Seja G um grupo solúvel de ordem n e suponha que o resultado vale para todo grupo solúvel com ordem menor que $|G|$. Se n for um número primo o resultado segue trivialmente já que $\{1\} \leq G$ é uma série subnormal com fatores cíclicos de ordem prima.

Se G é solúvel e não é de ordem prima, então G possui pelo menos um subgrupo normal N não trivial. Como N e G/N possuem ordem menor que G segue, da hipótese de indução, que ambos possuem uma série subnormal com fatores cíclicos de ordem prima.

Denotando $\overline{G} = G/N$, sejam

$$\{1\} \leq N_0 \leq \cdots \leq N_m = N$$

$$\{1\} \leq \overline{G_0} \leq \cdots \leq \overline{G_n} = \overline{G}$$

séries subnormais abelianas, com fatores cíclicos de ordem prima, para N e $\overline{G}$ respectivamente.

O Teorema do isomorfismo garante que

$$\frac{\overline{G}_i}{\overline{G}_{i-1}} = \frac{G_i/N}{G_{i-1}/N} \cong \frac{G_i}{G_{i-1}},$$

e o Teorema da Correspondência garante que $N \leq G_i$, com $i = 0, ..., m-1$.

Assim a cadeia

$$\{1\} = N_0 \leq N_1 \leq \cdots \leq N_m = N = G_0 \leq \cdots \leq G_n = G$$

é uma série subnormal abeliana para G com fatores cíclicos de ordem prima demostrando o resultado.

□

Referências Bibliográficas

[1] Adilson Gonçalves, **Introdução à álgebra**. 6º edição. IMPA, 2017.

[2] C. Polcino Milies, **Grupos Nilpotentes: uma introdução**. Matemática Universitária, n°34-junho 2003- pp.55-100.

[3] Hunderford, T. **Abstrat algebra: an introduction**. Cengage Learning, Third Edition, 2012.

[4] Hunderford, T. **Algebra**. Springer-Verlag, New York, 1980.

[5] Rotman, J. **An Introduction to the Theory of Groups**. Springer-Verlag, fourth edition, 1994.