



Instituto Federal de Educação, Ciência e Tecnologia de Goiás
Campus Valparaíso
Licenciatura Em Matemática

GRUPOS SOLÚVEIS E GRUPOS NILPOTENTES

SABRINA DE CASTRO PEREIRA LIMA

Trabalho de Conclusão de Curso – Licenciatura em Matemática

ORIENTADORA: PROF^a LUCIMEIRE ALVES DE CARVALHO

CO-ORIENTADOR: PROF. BRUNO DE PAULA MIRANDA

VALPARAÍSO DE GOIÁS

2021



Instituto Federal de Educação, Ciência e Tecnologia de Goiás
Campus Valparaíso
Licenciatura Em Matemática

GRUPOS SOLÚVEIS E GRUPOS NILPOTENTES

SABRINA DE CASTRO PEREIRA LIMA

Trabalho de conclusão de curso apresentado
como requisito parcial para a obtenção do
título de Licenciado em Matemática, do
Instituto Federal de Educação, Ciência e
Tecnologia, Campus Valparaíso-GO

ORIENTADORA: PROF^a LUCIMEIRE ALVES DE CARVALHO

CO-ORIENTADOR: PROF. BRUNO DE PAULA MIRANDA

Ficha catalográfica elaborada pelo bibliotecário Helio Lino Delfino (CRB-1/3031),
com os dados fornecidos pelo(a) autor(a).

L732g

Lima, Sabrina de Castro Pereira
Grupos solúveis e grupos nilpotentes / Sabrina de Castro
Pereira Lima. -- Valparaíso, 2021.
57 f. : il.

Orientadora: Lucimeire Alves de Carvalho.
Coorientador: Bruno de Paula Miranda.
TCC (Graduação - Licenciatura em Matemática) -
- Instituto Federal de Goiás, Campus Valparaíso
de Goiás, 2021.

1. Teoria de grupos - matemática. 2. Grupos solúveis
- matemática. 3. Grupo nilpotentes - matemática. I.
Carvalho, Lucimeire Alves de. II. Miranda, Bruno de
Paula. III. Título.

CDD 510



INSTITUTO FEDERAL
Goiás

MINISTÉRIO DA EDUCAÇÃO
SECRETARIA DE EDUCAÇÃO PROFISSIONAL E TECNOLÓGICA
INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA
PRÓ-REITORIA DE PESQUISA E PÓS-GRADUAÇÃO
SISTEMA INTEGRADO DE BIBLIOTECAS

TERMO DE AUTORIZAÇÃO PARA DISPONIBILIZAÇÃO NO REPOSITÓRIO DIGITAL DO IFG - ReDi IFG

Com base no disposto na Lei Federal nº 9.610/98, AUTORIZO o Instituto Federal de Educação, Ciência e Tecnologia de Goiás, a disponibilizar gratuitamente o documento no Repositório Digital (ReDi IFG), sem ressarcimento de direitos autorais, conforme permissão assinada abaixo, em formato digital para fins de leitura, download e impressão, a título de divulgação da produção técnico-científica no IFG.

Identificação da Produção Técnico-Científica

- | | |
|--|---|
| ☐ Tese | ☐ Artigo Científico |
| ☐ Dissertação | ☐ Capítulo de Livro |
| ☐ Monografia – Especialização | ☐ Livro |
| ☒ TCC - Graduação | ☐ Trabalho Apresentado em Evento |
| ☐ Produto Técnico e Educacional - Tipo: _____ | |

Nome Completo do Autor: Sabrina de Castro Pereira Lima

Matrícula: 20171150040029

Título do Trabalho: Grupos Solúveis e Grupos Nilpotentes

Autorização - Marque uma das opções

1. ☒ Autorizo disponibilizar meu trabalho no Repositório Digital do IFG (acesso aberto);
2. ☐ Autorizo disponibilizar meu trabalho no Repositório Digital do IFG somente após a data ____/____/____ (Embargo);
3. ☐ Não autorizo disponibilizar meu trabalho no Repositório Digital do IFG (acesso restrito).

Ao indicar a opção **2 ou 3**, marque a justificativa:

- ☐ O documento está sujeito a registro de patente.
☐ O documento pode vir a ser publicado como livro, capítulo de livro ou artigo.
☐ Outra justificativa: _____

DECLARAÇÃO DE DISTRIBUIÇÃO NÃO-EXCLUSIVA

O/A referido/a autor/a declara que:

- i. o documento é seu trabalho original, detém os direitos autorais da produção técnico-científica e não infringe os direitos de qualquer outra pessoa ou entidade;
- ii. obteve autorização de quaisquer materiais incluídos no documento do qual não detém os direitos de autor/a, para conceder ao Instituto Federal de Educação, Ciência e Tecnologia de Goiás os direitos requeridos e que este material cujos direitos autorais são de terceiros, estão claramente identificados e reconhecidos no texto ou conteúdo do documento entregue;
- iii. cumpriu quaisquer obrigações exigidas por contrato ou acordo, caso o documento entregue seja baseado em trabalho financiado ou apoiado por outra instituição que não o Instituto Federal de Educação, Ciência e Tecnologia de Goiás.

Valparaíso de Goiás, 07/04/2021.

Local

Data

Sabrina de C. Pereira Lima

Assinatura do Autor e/ou Detentor dos Direitos Autorais



INSTITUTO FEDERAL
Goiás

MINISTÉRIO DA EDUCAÇÃO
SECRETARIA DE EDUCAÇÃO PROFISSIONAL E TECNOLÓGICA
INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA DE GOIÁS
CÂMPUS VALPARAÍSO

Termo de Aprovação

SABRINA DE CASTRO PEREIRA LIMA

GRUPOS SOLÚVEIS E GRUPOS NILPOTENTES

Trabalho de Conclusão de Curso apresentado a Coordenação do Curso de Licenciatura em Matemática do Instituto Federal de Educação, Ciência e Tecnologia de Goiás – Câmpus Valparaíso de Goiás, como parte dos requisitos para a obtenção do título de Licenciada em Matemática.

Monografia defendida e aprovada, em doze de março de dois mil e vinte e um, pela banca examinadora constituída pelos seguintes membros:

BANCA EXAMINADORA

Profa. Dra. Lucimeire Alves de Carvalho
Presidente da banca / Orientadora
Instituto Federal de Educação, Ciência e Tecnologia de Goiás - IFG

Prof. Dr. Bruno de Paula Miranda
Instituto Federal de Educação, Ciência e Tecnologia de Goiás - IFG

Prof. Dr. Emerson Ferreira de Melo
Universidade de Brasília - UnB

Valparaíso de Goiás – GO

2021

Documento assinado eletronicamente por:

- Bruno de Paula Miranda, PROFESSOR ENS BASICO TECN TECNOLÓGICO, em 15/03/2021 17:38:51.
- Emerson Ferreira de Melo, EMERSON FERREIRA DE MELO - OUTROS - UNB (00038174000143), em 15/03/2021 17:28:44.
- Lucimeire Alves de Carvalho, PROFESSOR ENS BASICO TECN TECNOLÓGICO, em 12/03/2021 18:30:06.

Este documento foi emitido pelo SUAP em 12/03/2021. Para comprovar sua autenticidade, faça a leitura do QRCode ao lado ou acesse <https://suap.ifg.edu.br/autenticar-documento/> e forneça os dados abaixo:

Código Verificador: 140142

Código de Autenticação: df40d4ea73



AGRADECIMENTOS

Primeiramente quero agradecer a Deus, pois sem Ele não teria forças, fé e esperança para chegar até aqui. Faço minhas as palavras do salmista: "Eu te amo, ó Senhor, força minha" (Salmos 18:1).

Pessoas são presentes do céu nas nossas vidas. E eu não poderia deixar de agradecer ao meu esposo, Cid Júnior, por todo incentivo e apoio singulares durante esse processo acadêmico. O nosso amor gerou outros amores: João Victor, Isadora e Davi. Obrigada meus filhos por toda compreensão e apoio. Vocês são um orgulho pra mim!

À minha mãe, Maria Angélica, agradeço de coração por tudo. Você sempre acreditou em mim, e igualmente me incentivou das mais diversas formas. Ao meu pai, Humberto Pereira, também serei eternamente grata, pois sempre investiu em nós sem reservas.

Minha sogra, Gina Lima, é um exemplo pra mim. Obrigada por tudo!

Minha família é muito especial, e sei que todos sempre estiveram na torcida por cada conquista minha. Agradeço profundamente à minha irmã, meus sobrinhos, cunhados, meus avós, tios e primos.

Aos meus colegas de classe agradeço a parceria e companheirismo desses quatro anos de graduação.

Em especial quero agradecer aos meus professores do Instituto Federal de Goiás - Campus Valparaíso. Vocês me mostraram um outro lado da educação, um lado que eu nunca tinha visto e contemplado. Obrigada por cada palavra de encorajamento e ânimo.

Ao meu coorientador, Dr. Bruno de Paula Miranda, ofereço meus mais sinceros agradecimentos. A sua disponibilidade em me ajudar, tanto no Pibic como nesse trabalho, será sempre lembrada.

À minha orientadora, Dr^a Lucimeire Alves de Carvalho, queria encontrar as palavras mais sublimes para te agradecer por acreditar em mim e ajudar-me no que fosse preciso para a concretização desse sonho. Você é excelente no que faz, e vejo muita seriedade e dedicação no trabalho que desenvolve. Muito obrigada!!!

Neste trabalho estudaremos alguns conceitos relacionados aos grupos solúveis e aos grupos nilpotentes. Um dos conceitos mais antigos no estudo da teoria de grupos é o de grupos solúveis, que foi desenvolvido pelo famoso matemático Evariste Galois. Um grupo G é dito solúvel se contém uma cadeia de subgrupos $\{1\} = G_0 \leq G_1 \leq \dots \leq G_n = G$, tal que cada subgrupo G_{i-1} é normal em G_i e os grupos quocientes G_i/G_{i-1} , $1 \leq i \leq n$ são abelianos. As condições exigidas na definição de nilpotência são mais exigentes do que as definições de grupos solúveis. Então, um grupo é dito nilpotente se ele contém uma série de subgrupos tal que cada subgrupo G_{i-1} é normal em G e cada quociente G_i/G_{i-1} está contido no centro de G/G_{i-1} , $1 \leq i \leq n$. Essa série de subgrupos é chamada de uma série central de G , tendo como exemplos a série central superior ($\{1\} = \zeta_0(G) \leq \zeta_1(G) \leq \dots \leq \zeta_n(G) \leq \dots$) e a série central inferior ($G = \gamma_1(G) \geq \gamma_2(G) \geq \dots \geq \gamma_n(G) \geq \dots$). Para chegarmos ao objetivo do estudo apresentaremos algumas definições básicas como grupos, grupos de permutações, subgrupos, classes laterais, Teorema de Lagrange, subgrupos normais, grupo quociente e homomorfismo. Os teoremas de Sylow também serão abordados, pois nos garantem certos resultados para os grupos nilpotentes.

Palavras chave:

Teoria de Grupos, grupos solúveis, grupos nilpotentes

ABSTRACT

In this work we will study some concepts related to soluble groups and groups nilpotent. One of the oldest concepts in the study of group theory is that of soluble groups, which was developed by the famous mathematician Evariste Galois. A group G is said to be soluble if it contains a chain of subgroups $\{1\} = G_0 \leq G_1 \leq \dots \leq G_n = G$, such that each subgroup G_{i-1} is normal in G_i and the quotients groups $G_i/G_{i-1}, 1 \leq i \leq n$ are abelian. The conditions required in the definition of nilpotency are more demanding than the definitions of soluble groups. So, a group is said to be nilpotent if it contains a series of subgroups such that each subgroup G_{i-1} is normal in G and each quotient G_i/G_{i-1} is contained in the center of $G/G_{i-1}, 1 \leq i \leq n$. This series of subgroups is called a central series of G , having as examples the upper central series $(\{1\} = \zeta_0(G) \leq \zeta_1(G) \leq \dots \leq \zeta_n(G) \leq \dots)$ and the lower central series $(G = \gamma_1(G) \geq \gamma_2(G) \geq \dots \geq \gamma_n(G) \geq \dots)$. To reach the objective of the study, we will present some basic definitions such as groups, permutation groups, subgroups, classes laterals, Lagrange theorem, normal subgroups, quotient group and homomorphism. Sylow's theorems will also be discussed, as they guarantee us certain results for the groups nilpotent.

Key words:

Group theory, soluble groups, nilpotent groups

Agradecimentos	6
Resumo	7
Resumo	8
1 Conceitos Básicos	14
1.1 Grupos	14
1.2 Grupos de Permutações	17
1.3 Subgrupos	19
1.4 Classes Laterais, Teorema de Lagrange e aplicações	22
1.5 Subgrupos normais e grupo quociente	25
1.6 Homomorfismo	31
2 Estudo de um Grupo via Representações por Permutações	37
2.1 Representação de um grupo por permutações	37
2.2 Teoremas de Sylow	42
3 Solubilidade	46
3.1 Comutadores	46
3.2 Grupos Solúveis	49
4 Grupos Nilpotentes	55
4.1 Grupos Nilpotentes Finitos	58
Bibliografia	60

INTRODUÇÃO

Na história e no desenvolvimento da álgebra abstrata temos certos conjuntos básicos de suma importância: os grupos. Operando algebricamente seus elementos, ou seja, combinando dois elementos do conjunto podemos obter um terceiro elemento do mesmo conjunto, enfatizando que essas operações algébricas se sujeitam a certas propriedades que definem a estrutura do grupo.

A resolução de equações cúbicas por radicais foi descoberta entre os anos 1500 e 1515 por Scipione del Ferro (1456-1526). No entanto, já se sabia há muitos anos que as equações de grau um e dois também são resolúveis por radicais. Mas a grande questão era: "Será que toda equação algébrica poderia ser resolvida por radicais"? Com o intuito de se conseguir responder a esse questionamento, surgiram pesquisas relevantes que culminaram no conceito de *grupo*.

Por volta de 1770 Joseph Louis Lagrange (1736-1813) lança sua obra *Refléxions sur la résolution algébrique des équations* (Reflexões sobre a resolução algébrica de equações), aonde percebe de forma mais lúcida que a teoria das permutações (envolvendo as raízes da equação) seria de grande importância para a resolução de equações. Posteriormente, em 1824, Niels Henrik Abel (1802-1829) chega à conclusão de que não há fórmula geral por radicais para resolver as equações de grau ≥ 5 . Ainda prevalecia uma questão em aberto: geralmente essas equações de grau ≥ 5 não são resolúveis por radicais, mas alguns tipos o são, então o que as caracterizam matematicamente? E, em busca da resposta a esse problema, o matemático Evariste Galois (1811-1832) tem a ideia de associar a cada equação um grupo formado por permutações de suas raízes, condicionando a solubilidade por radicais a uma propriedade desse grupo. Na verdade, foi na obra de Galois que o conceito de grupo aparece pela primeira vez, até mesmo com esse nome.

Matemáticos como Ferdinand Georg Frobenius (1849-1917), William Burnside (1852-1927) e Issai Schur (1875-1936) publicaram trabalhos notáveis sobre a teoria dos grupos finitos antes da Primeira Guerra Mundial. Depois de 1928 outras contribuições foram feitas por Philip Hall (1904-1982), Helmut Wielandt (1910-2001), Richard Dagobert Brauer (1901-1977) e Daniel Gorenstein (1923-1992).

A definição moderna de grupos foi dada por Arthur Cayley (1821-1895), sucedendo então um desenvolvimento rápido e influente em todas as partes da matemática. Em geometria e em análise combinatória a noção de grupo tem um papel codificador, isto é, códigos baseados em teoria dos grupos ou em geometria algébrica. Os conceitos de grupo de permutação e de ação de um grupo são frequentemente utilizados para simplificar a contagem de um conjunto de objetos. Na Física e na Química os grupos estão intimamente relacionados com a teoria de representação, sendo também utilizados para classificar estruturas cristalinas e as simetrias das moléculas, dentre tantas outras aplicações.

Definição 1. *Seja G um conjunto não-vazio, munido de uma operação $\star$, tal que*

$$\begin{aligned}\star : G \times G &\longrightarrow G \\ (a, b) &\longmapsto a \star b.\end{aligned}$$

G é chamado de grupo se tem as seguintes propriedades:

- (i) *$a, b, c \in G$ implica que $a \star (b \star c) = (a \star b) \star c$ (associativo).*
- (ii) *Existe um elemento $e \in G$ tal que $a \star e = e \star a = a$ para todo $a \in G$ (existência de um elemento neutro em G).*
- (iii) *Para cada $a \in G$ existe um elemento $b \in G$ tal que $a \star b = b \star a = e$ (existência de inversos em G).*

Um tipo de grupo de particular importância neste estudo foi o dos grupos abelianos, que receberam esse nome em homenagem ao matemático norueguês Niels Henrik Abel. Um grupo G é dito abeliano se, para cada $a, b \in G$ vale que $a \star b = b \star a$.

Dentro da estrutura de grupos podemos considerar certos subconjuntos não-vazios. Esses conjuntos são considerados *subgrupos* de um grupo se, sob a mesma operação do grupo, o próprio subconjunto formar um grupo.

A *ordem* de um grupo diz respeito ao número de elementos do grupo. Se a ordem é finita, dizemos que o grupo é finito. Diante disso, podemos expor um dos teoremas mais conhecidos no estudo de grupos: *O Teorema de Lagrange*. Esse teorema nos diz que se G é um grupo finito e H é um subgrupo de G então a ordem de H divide a ordem de G .

Em um grupo podemos definir uma relação de equivalência com o intuito de visualizar o grupo por meio de suas classes de equivalência. Assim, se H é subgrupo de G , $a \in G$, então $Ha = \{ha | h \in H\}$ é chamado de classe lateral à direita de H em G . De forma análoga, podemos obter as classes laterais à esquerda de H em G . Um subgrupo é dito normal se toda classe lateral à esquerda é igual a uma classe lateral à direita. O conjunto das classes laterais munido da operação produto entre as classes vai ter uma estrutura de grupo, o qual denominamos grupo *quociente*.

Alguns grupos se relacionam com outros por meio de uma função compatível com as estruturas dos grupos. Isso nos dá a noção de *homomorfismo*, que é uma ideia central comum

a todos os aspectos da álgebra moderna. Por meio do homomorfismo $\rho : G \rightarrow \mathcal{G}$ também podemos tentar estudar um grupo G via um outro grupo $\mathcal{G}$, o que chamamos de estudo via representações.

Os Teoremas de Sylow nos garantem exemplos de grupos nilpotentes, além de ser o resultado mais geral na direção de uma recíproca ao Teorema de Lagrange.

Teorema 1 (Sylow). *Seja G um grupo finito de ordem $|G| = p^n m$, onde p é um inteiro primo que não divide m . Então:*

- (i) *G sempre contém p -subgrupos de Sylow e todo p -subgrupo de G está contido num p -subgrupo de Sylow.*
- (ii) *Todos os p -subgrupos de Sylow de G são conjugados entre si.*
- (iii) *Se n_p denota o número de p -subgrupos de Sylow de G , então $n_p \equiv 1 \pmod{p}$ e $n_p | m$.*

Para entendermos melhor os grupos solúveis definimos o conceito de *comutador*. Dados dois elementos x e y de um grupo G , o comutador de x e y é o elemento $[x, y] = x^{-1}y^{-1}xy \in G$. O grupo $G' = [G, G]$ é chamado subgrupo derivado de G . Agora podemos definir a sequência de subgrupos $G^{(n)} = [G^{(n-1)}, G^{(n-1)}]$, onde o subgrupo $G^{(n)}$ é chamado o n -ésimo grupo derivado de G e a sequência $G = G^{(0)} \geq G^{(1)} \geq \dots \geq G^{(n)} \geq \dots$ chama-se a sequência derivada de G . Definimos agora os grupos *solúveis*:

Definição 2. *Um grupo G é dito solúvel se contém uma cadeia de subgrupos*

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

tal que cada subgrupo G_{i-1} é normal em G_i e os grupos quocientes G_i/G_{i-1} , $1 \leq i \leq n$, são abelianos.

W. Burnside, em sua obra *Theory of Groups of Finite Order* (1897), prova a existência da série central de um p -grupo. Isso representou o início do estudo dos grupos nilpotentes. Um grupo G diz-se *nilpotente* se ele contém uma série de subgrupos

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

tal que cada subgrupo G_{i-1} é normal em G e cada quociente G_i/G_{i-1} está contido no centro de G/G_{i-1} , $1 \leq i \leq n$. Uma tal série de subgrupos de G diz-se uma *série central* de G .

Este trabalho está dividido em 4 capítulos. No primeiro capítulo há uma série de resultados da Teoria de Grupos imprescindíveis para um melhor entendimento dos resultados posteriores. No segundo capítulo foram estudadas as representações de um grupo por permutações e os Teoremas de Sylow. No terceiro capítulo abordamos a solubilidade, trabalhando os conceitos de comutadores, sequências derivadas e grupos solúveis. Por fim, o quarto capítulo foi dedicado aos conceitos de grupos nilpotentes e grupos nilpotentes finitos.

CAPÍTULO 1

CONCEITOS BÁSICOS

Neste capítulo vamos ver algumas definições e teoremas bem conhecidos da teoria de grupos que servirão de base para os capítulos seguintes.

Ao longo dos anos tem-se verificado que o conceito de grupo é um dos instrumentos mais importantes da matemática. Podemos citar a teoria das simetrias, onde os grupos podem ser usados para representar simetrias geométricas, associando um grupo que caracteriza e representa a simetria da figura. Na topologia algébrica, grupos são usados para descrever os invariantes de espaços topológicos, que são assim chamados porque não mudam se o espaço é submetido a uma transformação. Na análise combinatória, a noção de grupo de permutação e o conceito de ação de um grupo são frequentemente utilizados para simplificar a contagem de um conjunto de objetos.

1.1 Grupos

Definição 3. *Seja G um conjunto não-vazio, munido de uma operação $\star$, tal que*

$$\begin{aligned}\star : G \times G &\longrightarrow G \\ (a, b) &\longmapsto a \star b\end{aligned}$$

G é chamado de grupo se tem as seguintes propriedades:

- (i) *$a, b, c \in G$ implica que $a \star (b \star c) = (a \star b) \star c$ (lei associativa).*
- (ii) *Existe um elemento $e \in G$ tal que $a \star e = e \star a = a$ para todo $a \in G$ (existência de um elemento neutro em G).*
- (iii) *Para cada $a \in G$ existe um elemento $b \in G$ tal que $a \star b = b \star a = e$ (existência de inversos em G).*

Denotamos um grupo G com a operação $\star$ por $(G, \star)$.

OBSERVAÇÃO: Essa operação pode ser de vários tipos, como por exemplo, um produto ou uma soma. No caso da operação ser a multiplicação, denotaremos o inverso de a por a^{-1} . E no caso da operação ser a adição, denotaremos o inverso de a por $-a$.

EXEMPLOS:

1. Seja G o conjunto dos números inteiros ($\mathbb{Z}$), e a operação soma usual:

$$\begin{aligned} + : \mathbb{Z} \times \mathbb{Z} &\longrightarrow \mathbb{Z} \\ (a, b) &\longmapsto a + b \end{aligned}$$

- (i) A adição de inteiros é associativa.
 - (ii) $e = 0$ é elemento neutro com respeito à adição: $a + 0 = 0 + a = a$, $\forall a \in \mathbb{Z}$.
 - (iii) $\forall a \in \mathbb{Z}$, $b = -a$ é o inverso de a , pois $a + b = 0$.
2. Seja $A = \{1, -1\} \subset \mathbb{Z}$, defina em A o produto:

$$\begin{aligned} \cdot : A \times A &\longrightarrow A \\ (a, b) &\longmapsto a \cdot b \end{aligned}$$

- (i) Produto de inteiros é associativo.
- (ii) 1 é o elemento neutro.
- (iii) Cada elemento possui inverso multiplicativo. Note que com essa operação o inverso do elemento 1 é ele mesmo, e o inverso do (-1) é ele mesmo. Logo, todos os elementos tem inverso multiplicativo.

Vejamos agora uma classe importante de grupos.

Definição 4. Um grupo é chamado abeliano (ou comutativo) se, para cada $a, b \in (G, \star)$

$$a \star b = b \star a$$

EXEMPLO: Sejam $n > 1$ um inteiro e $\bar{r} = \{kn + r | k \in \mathbb{Z}, 0 \leq r < n\}$. Considerando o conjunto

$$\mathbb{Z}_n = \{\bar{0}, \bar{1}, \bar{2}, \dots, \overline{n-1}\},$$

e definindo a operação de adição sobre $\mathbb{Z}_n$ como sendo $\bar{x} + \bar{y} = \overline{x + y}$, temos que $(\mathbb{Z}_n, +)$ é um grupo abeliano. De fato,

i) Para todo $\bar{x}, \bar{y}, \bar{z} \in \mathbb{Z}_n$ temos:

$$\begin{aligned}\bar{x} + (\bar{y} + \bar{z}) &= x + (\overline{y + z}) = \overline{x + (y + z)} \\ &= \overline{(x + y) + z} = \overline{(x + y)} + \bar{z} \\ &= (\bar{x} + \bar{y}) + \bar{z}.\end{aligned}$$

ii) Para todo $x \in \mathbb{Z}_n$, note que:

$$\bar{x} + \bar{0} = \bar{x} + \bar{0} = \bar{x}, \text{ assim } \bar{0} \text{ é o elemento neutro.}$$

iii) Para todo $\bar{x} \in \mathbb{Z}_n$, tome $\overline{n - x} \in \mathbb{Z}_n$, então:

$$\bar{x} + \overline{n - x} = x + \overline{(n - x)} = \bar{n} = \bar{0}.$$

iv) Para todos $\bar{x}, \bar{y} \in \mathbb{Z}_n$,

$$\bar{x} + \bar{y} = \overline{x + y} = \overline{y + x} = \bar{y} + \bar{x}.$$

Portanto, $(\mathbb{Z}_n, +)$ é um grupo abeliano.

Daqui pra frente, ao invés da notação $(G, \star)$ iremos usar a notação multiplicativa $(G, \cdot)$ quando se tratar de um grupo genérico.

Lema 1. Dado $a, b \in G$, então as equações $a \cdot x = b$ e $y \cdot a = b$ têm soluções únicas para x e y em G . Em particular, valem as duas leis de cancelamento,

$$\begin{aligned}a \cdot u = a \cdot w &\text{ implica } u = w \\ u \cdot a = w \cdot a &\text{ implica } u = w\end{aligned}$$

Demonstração. Assuma $a \cdot u = a \cdot w$. Multiplicando por (a^{-1}) pela esquerda:

$$\begin{aligned}a^{-1} \cdot (a \cdot u) &= a^{-1} \cdot (a \cdot w) \\ (a^{-1} \cdot a) \cdot u &= (a^{-1} \cdot a) \cdot w \\ e \cdot u &= e \cdot w \Rightarrow u = w\end{aligned}$$

□

Lema 2. Se G é um grupo, então

- (a) O elemento neutro de G é único;
- (b) cada $a \in G$ existe um único inverso em G ;
- (c) para cada $a \in G$, $(a^{-1})^{-1} = a$;
- (d) para todo $a, b \in G$, $(a \cdot b)^{-1} = b^{-1} \cdot a^{-1}$.

Demonstração. No item (a) temos que se $e, f \in G$ são elementos neutros de G , então

$$\begin{aligned} e &= e \cdot f && \text{pois } f \text{ é elemento neutro,} \\ &= f && \text{pois } e \text{ é elemento neutro.} \end{aligned}$$

Portanto, $e = f$.

Para o item (b) consideremos $a \in G$, e sejam $x, y \in G$ dois elementos inversos de a . Temos:

$$\begin{aligned} x &= x \cdot e = x \cdot (a \cdot y) && \text{pois } y \text{ é inverso de } a, \\ &= (x \cdot a) \cdot y = e \cdot y = y && \text{pois } x \text{ é inverso de } a. \end{aligned}$$

Então $x = y$.

O item (c) segue da observação que $a^{-1} \cdot (a^{-1})^{-1} = e = a^{-1} \cdot a$; cancelando o a^{-1} da esquerda nos deixa com $(a^{-1})^{-1} = a$. Isso é análogo a $-(-5) = 5$, que é um resultado familiar no grupo de números reais sob adição.

O item (d) é a mais trivial delas, pois $(a \cdot b) \cdot (b^{-1} \cdot a^{-1}) = a \cdot (b \cdot b^{-1}) \cdot a^{-1} = a \cdot (e \cdot a^{-1}) = a \cdot a^{-1} = e$, e assim, pela própria definição do inverso $(a \cdot b)^{-1} = b^{-1} \cdot a^{-1}$. $\square$

Definição 5. O número de elementos de um grupo é chamado ordem do grupo, a qual denotamos por $|G|$. Se $|G|$ é finita, dizemos que G é um grupo finito.

A partir desse ponto deixaremos de indicar a operação do grupo, escrevendo G para denotar um grupo $(G, \cdot)$. E ao invés de escrever $a \cdot b$ para $a, b \in G$ devemos denotar essa operação como ab .

Vamos apresentar na próxima seção uma classe de exemplos de grupos.

1.2 Grupos de Permutações

Seja X um conjunto não vazio qualquer. Uma bijeção $f : X \rightarrow X$ é dita uma permutação de X . Vale ressaltar que uma bijeção é uma função injetiva e sobrejetiva.

EXEMPLOS:

1. Seja $X = \{1, 2, 3\}$ e $f : X \rightarrow X$ dada por

$$\begin{aligned} f(1) &= 2 \\ f(2) &= 3 \\ f(3) &= 1 \end{aligned}$$

f é uma permutação de X . Uma maneira conveniente de representarmos a permutação f é com a notação $(1, 2, 3)$, que podemos ler da seguinte maneira, da esquerda para a direita: "temos 1 levado em 2, que é levado em 3, que é levado em 1".

$$2. X = \{1, 2, 3, 4\}$$

$$f(1) = 2$$

$$f(2) = 4 \iff (1, 2, 4)(3) \text{ ou } (1, 2, 4)$$

$$f(4) = 1$$

$$f(3) = 3$$

Com esta notação a função identidade é denotada por (1) .

Note que quando um elemento é levado pela função $f(n) = n$ nele mesmo, na hora de escrever o ciclo ele não aparece no ciclo.

Definição 6. Sejam $f, g : X \longrightarrow X$ permutações, então a composição

$$\begin{aligned} f \circ g : X &\longrightarrow X \\ x &\longmapsto f(g(x)) \end{aligned}$$

é também uma permutação.

EXEMPLO: Seja $X = \{1, 2, 3, 4\}$, sendo $f = (1, 3, 4, 2)$ e $g = (2, 4, 1)$. Então $f \circ g = (1)(2)(3, 4) = (3, 4)$.

O conjunto de todas as permutações de um conjunto X é denotado por S_X . Em particular, se $X = \{1, 2, \dots, n\}$ usamos S_n .

Proposição 1. Para todo conjunto X não vazio, S_X munido da composição de funções

$$\begin{aligned} \circ : S_X \times S_X &\longrightarrow S_X \\ f, g &\longmapsto f \circ g \end{aligned}$$

é um grupo.

Demonstração. (i) Sejam f, g, h em S_X . Queremos mostrar que $(f \circ g) \circ h = f \circ (g \circ h)$.

Mas $(f \circ g) \circ h(x) = (f \circ g)(h(x))$ e $f \circ (g \circ h)(x) = f(g \circ h(x)) = f(g(h(x)))$. Logo, a composição é associativa.

(ii) Se $e = id X$, que é a função identidade, então $f \circ e(x) = f(e(x)) = f(x) \forall f \in S_X$ e $\forall x \in X \therefore e = id X$ é elemento neutro.

(iii) Se $f \in S_X$ é um bijeção, existe $g \in S_X$ tal que $f \circ g = g \circ f = e$.

□

Definição 7. O grupo $(S_X, \circ)$ é chamado grupo de permutações de X . No caso de $X = \{1, 2, \dots, n\}$ é comum chamar $(S_n, \circ)$ de grupo de simetrias ou grupo simétrico de ordem $n!$

Seja $f \in S_n$. Temos n possibilidades para a imagem $f(1)$, $(n-1)$ possibilidades para $f(2)$, $(n-2)$ possibilidades para $f(3)$, ..., 2 possibilidades para $f(n-1)$ e uma possibilidade para $f(n)$. Portanto, pelo princípio da multiplicação, f é uma das $n \cdot (n-1) \cdot (n-2) \cdot \dots \cdot 2 \cdot 1 = n!$ bijeções possíveis. Portanto $|S_n| = n!$

EXEMPLO: Quem são os elementos de S_3 ? S_3 é o conjunto das permutações de $\{1, 2, 3\}$ e tem ordem 6. Assim, $S_3 = \{(1), (1, 2), (1, 3), (2, 3), (1, 2, 3), (1, 3, 2)\}$. Uma observação a ser feita sobre esse grupo é que S_3 não é abeliano. De fato $(1, 2)(1, 2, 3) = (2, 3)$ que é diferente de $(1, 2, 3)(1, 2) = (1, 3)$.

1.3 Subgrupos

De todos os possíveis subconjuntos de um grupo, existem alguns deles especiais. São aqueles que de certa forma conseguem ser eles próprios grupos.

Definição 8. Um subconjunto não-vazio H de um grupo G é considerado um subgrupo de G (denotamos $H \leq G$) se, sob a mesma operação de G , o próprio H formar um grupo.

Naturalmente temos que se H é um subgrupo de G e K é um subgrupo de H , então K é um subgrupo de G .

Os próximos dois lemas apresentam critérios para decidir se um dado subconjunto de um grupo é um subgrupo.

Lema 3. Um subconjunto não vazio H do grupo G é um subgrupo de G se, e somente se,

(1) $a, b \in H$ implica que $ab \in H$;

(2) $a \in H$ implica que $a^{-1} \in H$.

Demonstração. Se H é um subgrupo de G , então é óbvio que (1) e (2) devem ser esperados, pois são propriedades inerentes a qualquer grupo.

Suponhamos que H é um subconjunto de G para o qual (1) e (2) são válidos. A fim de estabelecer que H é um subgrupo, tudo o que é necessário é verificar que $e \in H$ e que a lei associativa vale para elementos de H . Se a lei associativa vale para G , vale para H , que é um subconjunto de G . Se $a \in H$, por (2) $a^{-1} \in H$ e assim por (1) temos $aa^{-1} = e \in H$. Assim, está provado!

Veremos no próximo lema que no caso dos grupos finitos podemos dispensar (2). $\square$

OBSERVAÇÃO: É fácil mostrar que essas duas condições podem ser resumidas nas seguintes propriedades:

- (i) $e \in H$;
- (ii) $a, b \in H \Rightarrow ab^{-1} \in H$.

Lema 4. Se H é um subconjunto finito não vazio de um grupo G e H é fechado para a multiplicação, então $H \leq G$.

Demonstração. À luz do Lema 3, precisamos apenas mostrar que sempre que $a \in H$, então $a^{-1} \in H$. Suponha que $a \in H$, assim $a^2 = aa \in H, a^3 = a^2a \in H, \dots, a^m \in H$, uma vez que H é fechado para a multiplicação. Assim, a coleção infinita de elementos $a, a^2, \dots, a^m, \dots$ deve "caber" em H , que é um subconjunto finito de G . Portanto, deve haver repetições nesta coleção de elementos, isto é, para alguns inteiros r, s com $r > s > 0, a^r = a^s$. Pelo cancelamento em $G, a^{r-s} = e$ (onde e está em H); desde que $r - s - 1 \geq 0, a^{r-s-1} \in H$ e $a^{-1} = a^{r-s-1}$, uma vez que $aa^{r-s-1} = a^{r-s} = e$. Assim $a^{-1} \in H$, completando a prova. $\square$

Assim, para verificar se um subconjunto de um grupo finito é um subgrupo, basta verificar se ele é ou não fechado para a operação do grupo.

EXEMPLOS DE SUBGRUPOS:

1. Se G é um grupo, então $\{e\}$ e G são subgrupos de G . Ambos são chamados subgrupos triviais.
2. Seja G o grupo dos inteiros ($\mathbb{Z}$) munido da operação adição, H o subconjunto consistindo de todos os múltiplos de 5 (denotado por $5\mathbb{Z}$) é subgrupo de G . Semelhantemente, o subconjunto $n\mathbb{Z}$ pode ser definido como o subconjunto de G que consiste de todos os múltiplos de n , sendo um subgrupo para cada n .
3. Seja G um grupo qualquer. Considere o subconjunto $Z(G) = \{x \in G \mid xg = gx, \forall g \in G\}$. É fácil mostrar que esse subconjunto é um subgrupo de G , sendo chamado *centro* de G . Note que G é abeliano se, e somente se, $Z(G) = G$.
4. Seja C qualquer conjunto, $\mathcal{P}(C)$ o conjunto das permutações de C (bijeções de C em C), é um grupo sob a composição de funções. Se $x_0 \in C$, logo $H(x_0) = \{\phi \in \mathcal{P}(C) \mid \phi(x_0) = x_0\}$ é um subgrupo de $\mathcal{P}(C)$.

Definição 9 (Subgrupo gerado por um elemento). Sejam G um grupo e $a \in G$. O conjunto $\langle a \rangle = \{a^n \mid n \in \mathbb{Z}\}$ é um subgrupo de G , chamado de subgrupo gerado por a .

Nesta definição, a^n representa o elemento obtido da operação do elemento a por ele mesmo n vezes e, o inverso de cada a^n é denotado por a^{-n} . Já o elemento neutro é representado por 1 ou por a^0 . Nesta notação $a^n a^m = a^{n+m}$.

Se G é o grupo dos inteiros, a^n significa o inteiro na .

Note que um subgrupo gerado por a pode ser finito ou infinito.

EXEMPLOS:

1. Seja $G = \mathbb{Z}_6 = \{\bar{0}, \bar{1}, \bar{2}, \bar{3}, \bar{4}, \bar{5}\}$. Note que $\langle \bar{2} \rangle = \{\bar{0}, \bar{2}, \bar{4}\}$. Neste caso, temos que $\langle \bar{2} \rangle$ é finito, uma vez que ele é subgrupo de um grupo finito.
2. $G = S_3 = \{(1), (1, 2), (1, 3), (2, 3), (1, 2, 3), (1, 3, 2)\}$ munido da operação composição de funções. Quem é $\langle (1, 2, 3) \rangle$?
 $(1, 2, 3)^0 = (1)$
 $(1, 2, 3)^1 = (1, 2, 3)$
 $(1, 2, 3)^2 = (1, 2, 3)(1, 2, 3) = (1, 3, 2)$
 $(1, 2, 3)^3 = (1, 2, 3)^2(1, 2, 3) = (1, 3, 2)(1, 2, 3) = (1)$

$$\langle (1, 2, 3) \rangle = \{(1), (1, 2, 3), (1, 3, 2)\}$$

3. $G = \mathbb{Z}$ e $a = 2$. Quem é $\langle a \rangle$? Na notação aditiva, temos $\langle a \rangle = \{ia; i = 0, \pm 1, \pm 2, \dots\} \Rightarrow$
 $\langle a \rangle = \{\dots, -3a, -2a, -a, 0, a, 2a, 3a, \dots\} = \{\dots, -2 \cdot 2, -1 \cdot 2, 0, 1 \cdot 2, 2 \cdot 2, \dots\} = 2\mathbb{Z}$.

Definição 10. Um grupo G é dito cíclico quando existir $g \in G$ que gere todos os elementos de G . Da definição acima notamos que o subgrupo gerado por um elemento é um grupo cíclico. Neste caso, usa-se a notação $G = \langle g \rangle$.

Podemos observar que $(\mathbb{Z}, +)$ é um grupo cíclico gerado por 1.

Note que os grupos cíclicos são abelianos, mas a recíproca é falsa. Considere o conjunto $K = \{1, a, b, ab\}$. Definindo um produto em K , que é abeliano, temos o grupo de Klein. Nesse grupo todo elemento tem ordem 2, $|K| = 4$ e K não é cíclico.

Definição 11. Se g é um elemento do grupo G , a ordem de g é a ordem do subgrupo gerado por g ; ela será denotada por $o(g)$.

Proposição 2. Sejam g um elemento do grupo G e $\langle g \rangle$ o subgrupo gerado por g . Então as seguintes condições são equivalentes:

(i) A ordem $|\langle g \rangle|$ é finita.

(ii) Existe $t \geq 1$ tal que $g^t = e$.

Neste caso, denotando por n a ordem de $\langle g \rangle$, temos $\langle g \rangle = \{e, g, \dots, g^{n-1}\}$.

Demonstração. (i) $\Rightarrow$ (ii) Como $\langle g \rangle = \{g^m | m \in \mathbb{Z}\}$, e por hipótese o grupo $\langle g \rangle$ é finito, existem $p, q \in \mathbb{Z}, p \neq q$ tais que $g^p = g^q$. Supondo que $p > q$, e como $g^p = g^q$, então $g^{p-q} = e$. Assim, existe $t > 0$ tal que $g^t = e$.

(ii) $\Rightarrow$ (i) Considere o inteiro $r := \min\{t \geq 1 | g^t = e\}$. Vamos mostrar que $|\langle g \rangle| = r$. Para isso mostramos a seguinte afirmação:

Afirmção: $\langle g \rangle = \{e, g, g^2, \dots, g^{r-1}\}$ e os elementos $e, g, g^2, \dots, g^{r-1}$ são todos distintos.

DEMONSTRAÇÃO DA AFIRMAÇÃO: Suponha que $g^p = g^q$ com $0 \leq p, q \leq r-1$, $p \neq q$; podemos supor que $p > q$. Temos $g^{p-q} = e$ com $0 < p-q < r$ e isso contradiz a minimalidade de r . Logo $e, g, g^2, \dots, g^{r-1}$ são elementos distintos de G . Para provar que $\langle g \rangle = \{e, g, g^2, \dots, g^{r-1}\}$, devemos mostrar que $\forall m \in \mathbb{Z}, g^m = g^l$ para algum $0 \leq l < r$. Pelo algoritmo de Euclides, existem $q, l \in \mathbb{Z}$ tais que $m = qr + l$ com $0 \leq l < r$, e portanto temos que $g^m = g^{qr+l} = (g^r)^q \cdot g^l = e^q \cdot g^l = g^l$. $\square$

1.4 Classes Laterais, Teorema de Lagrange e aplicações

Com os conceitos a seguir vamos definir uma relação de equivalência em G para que possamos visualizar o grupo por meio de suas classes de equivalência.

Definição 12. *Seja G um grupo, $H \leq G$; para $a, b \in G$ dizemos que a é congruente a b módulo H , escrito como $a \equiv b \pmod{H}$ se $ab^{-1} \in H$.*

Lema 5. *A relação $a \equiv b \pmod{H}$ é uma relação de equivalência.*

Demonstração. Para ser uma relação de equivalência deve-se verificar as seguintes condições:

- (1) $a \equiv a \pmod{H}, \forall a \in G$;
- (2) $a \equiv b \pmod{H}$ implica $b \equiv a \pmod{H}, \forall a, b \in G$;
- (3) $a \equiv b \pmod{H}, b \equiv c \pmod{H}$ implica $a \equiv c \pmod{H}, \forall a, b, c \in G$.

Examinando cada uma das condições listadas:

- (1) Para mostrar que $a \equiv a \pmod{H}$ devemos provar, usando a própria definição de congruência $\pmod{H}$, que $aa^{-1} \in H$. Como $H \leq G$, $e \in H$, e como $aa^{-1} = e$, $aa^{-1} \in H$, o que queríamos demonstrar.
- (2) Suponha que $a \equiv b \pmod{H}$, isto é, suponha $ab^{-1} \in H$; queremos obter disso que $b \equiv a \pmod{H}$, ou, equivalentemente, $ba^{-1} \in H$. Desde que $ab^{-1} \in H$, que é um subgrupo de G , $(ab^{-1})^{-1} \in H$; mas, pelo Lema 2, $(ab^{-1})^{-1} = (b^{-1})^{-1}a^{-1} = ba^{-1}$, e então $ba^{-1} \in H$ e $b \equiv a \pmod{H}$.
- (3) Por fim, queremos que $a \equiv b \pmod{H}$ e $b \equiv c \pmod{H}$ implique em $a \equiv c \pmod{H}$. A primeira congruência se traduz em $ab^{-1} \in H$, a segunda em $bc^{-1} \in H$; usando que $H \leq G$, $(ab^{-1})(bc^{-1}) \in H$. No entanto, $ac^{-1} = aec^{-1} = a(b^{-1}b)c^{-1} = (ab^{-1})(bc^{-1})$, portanto $ac^{-1} \in H$ a partir do qual segue-se que $a \equiv c \pmod{H}$.

$\square$

Se G for o grupo de inteiros sob adição, e $H = n\mathbb{Z}$ for o subgrupo consistindo de todos os múltiplos de n , então em G a relação $a \equiv b \pmod{H}$, ou seja, $ab^{-1} \in H$, sob a notação aditiva é lida como $a - b$ é um múltiplo de n .

Definição 13. *Seja H subgrupo de G , $a \in G$, então $Ha = \{ha | h \in H\}$ é chamado de classe lateral à direita de H em G e $aH = \{ah | h \in H\}$ é chamado de classe lateral à esquerda de H em G .*

Os resultados que iremos apresentar daqui pra frente podem ser demonstrados tanto para classes laterais à esquerda quanto para classes laterais à direita de H . Sendo assim, sem perda de generalidade, usaremos apenas as classes laterais à direita para estes resultados.

Lema 6. *Para todo $a \in G$, $Ha = \{x \in G | a \equiv x \pmod{H}\}$.*

Demonstração. Seja $[a] = \{x \in G | a \equiv x \pmod{H}\}$. Primeiro mostramos que $Ha \subset [a]$. Se $h \in H$, então $a(ha)^{-1} = a(a^{-1}h^{-1}) = h^{-1} \in H$. Pela definição de congruência módulo H , isso implica que $ha \in [a]$ para cada $h \in H$, e então $Ha \subset [a]$.

Suponha agora que $x \in [a]$. Assim $ax^{-1} \in H$, então $(ax^{-1})^{-1} = xa^{-1}$ também está em H , ou seja, $xa^{-1} = h$ para algum $h \in H$. Multiplicando ambos os lados por a pela direita chegamos a $x = ha$, logo $x \in Ha$. Assim $[a] \subset Ha$. Tendo provado as duas inclusões $[a] \subset Ha$ e $Ha \subset [a]$, podemos concluir que $[a] = Ha$, que é a afirmação do lema. $\square$

$Ha = [a]$ é a classe de equivalência com respeito a relação $\equiv \pmod{H}$ de a em G , e essas classes de equivalência produzem uma decomposição de G em subconjuntos disjuntos. Assim, quaisquer duas classes laterais à direita de H em G são idênticas ou não têm nenhum elemento em comum.

Definição 14. *A cardinalidade do conjunto das classes laterais distintas à direita é o índice de H em G ; ele será denotado por $(G : H)$.*

O índice de H em G também é a cardinalidade do conjunto das classes laterais à esquerda de H em G , pois a função ϕ abaixo é uma bijeção:

$$\begin{aligned} \phi : \{\text{classes laterais à esquerda}\} &\longrightarrow \{\text{classes laterais à direita}\} \\ aH &\longmapsto Ha^{-1} \end{aligned}$$

Proposição 3. *Todas as classes laterais de H em G têm a mesma cardinalidade, igual à cardinalidade de H .*

Demonstração. A função

$$\begin{aligned} H &\longrightarrow Ha \\ h &\longmapsto ha \end{aligned}$$

é claramente uma bijeção. $\square$

EXEMPLO:

$$G = S_3 = \{(1), (1, 2), (1, 3), (2, 3), (1, 2, 3), (1, 3, 2)\}$$

$$H = \{(1), (1, 2, 3), (1, 3, 2)\}$$

$$H(1, 2) = \{(1, 2), (1, 3), (2, 3)\}$$

Teorema 2. *Seja $H \leq G$ então $H = Ha$ se, e somente se, $a \in H$.*

Com o conceito de classes laterais e a proposição 3 é possível mostrar um importante teorema dentro da teoria de grupos, denominado Teorema de Lagrange.

Teorema 3 (Teorema de Lagrange). *Sejam G um grupo finito e H um subgrupo de G . Então $|G| = |H|(G : H)$; em particular, a ordem e o índice de H dividem a ordem de G .*

Demonstração. Seja G um grupo finito e $H \leq G$ com $(G : H) = n$. Em cada uma das classes laterais temos $|H|$ elementos. Como $G = \bigcup_{i=0}^{n-1} Ha_i, a \in G$, temos

$$|G| = \sum_{i=0}^{n-1} |Ha_i| = n|H|$$

$$\therefore |H| \text{ divide } |G|$$

$$|G| = |H|(G : H)$$

□

Se G é um grupo abeliano e se H é um subgrupo de G , então $Ha = aH, \forall a \in G$.

Corolário 1. *Seja G um grupo finito e $a \in G$, então $o(a)$ divide $|G|$.*

Demonstração. Temos que $o(a) = |\langle a \rangle|$, onde $\langle a \rangle = \{1, a, a^2, a^3, \dots, a^{m-1}\}$ é subgrupo de G . Segue diretamente do Teorema de Lagrange que $|\langle a \rangle|$ divide $|G|$. □

Corolário 2. *Se G é um grupo finito e $a \in G$, então $a^{|G|} = e$.*

Demonstração. Pelo Corolário 1, $o(a)$ divide $|G|$; assim $|G| = m \cdot o(a)$. Portanto, $a^{|G|} = a^{m \cdot o(a)} = (a^{o(a)})^m = e^m = e$. □

Corolário 3. *Se G é um grupo finito cuja ordem é um número primo p , então G é um grupo cíclico.*

Demonstração. Primeiro, afirmamos que G não tem subgrupos não triviais. Seja H subgrupo de G , a ordem de H deve dividir $|G| = p$ deixando apenas duas possibilidades, $|H| = 1$ ou $|H| = p$. O primeiro deles implica $H = e$, enquanto o segundo implica que $H = G$. Seja $a \neq e \in G$ e $H = \langle a \rangle$, com $H \leq G$ e $H \neq \{e\}$, assim $H = G$. Isso diz que G é cíclico e que cada elemento em G é uma potência de a . □

Sabemos que se $H \leq G$ e $a \in G$, então Ha consiste em todos os elementos em G da forma ha onde $h \in H$. Sejam H, K dois subgrupos de G , seja $HK = \{x \in G \mid x = hk, h \in H, k \in K\}$. Será que este conjunto é um subgrupo de G ? Vamos ver um exemplo em S_3 : seja $H = \{(1), (1, 2)\}$ e $K = \{(1), (1, 3)\}$. Apenas usando a definição de HK podemos ver que HK consiste nos elementos $\{(1), (1, 3), (1, 2), (1, 3, 2)\}$. Como HK tem quatro elementos e 4 não é um divisor de 6 (a ordem de S_3), pelo Teorema de Lagrange HK não é um subgrupo de S_3 . Note também que $KH = \{(1), (1, 2), (1, 3), (1, 2, 3)\} \neq HK$. Há uma condição para que HK seja um subgrupo de G , que é verificada no próximo lema.

Lema 7. HK é um subgrupo de G se, e somente se, $HK = KH$.

Demonstração. Suponha, primeiro, que $HK = KH$; isto é, se $h \in H$ e $k \in K$, então $hk = k_1h_1$ para algum $k_1 \in K, h_1 \in H$. Para provar que HK é um subgrupo, devemos verificar se ele está fechado e cada elemento em HK tem seu inverso em HK . Primeiramente vamos mostrar o fechamento; então suponha que $x = hk \in HK$ e $y = h'k' \in HK$. Então $xy = hkh'k'$, mas como $kh' \in KH = HK, kh' = h_2k_2$ com $h_2 \in H, k_2 \in K$. Portanto, $xy = h(h_2k_2)k' = (hh_2)(k_2k') \in HK$ e HK é fechado. Também $x^{-1} = (hk)^{-1} = k^{-1}h^{-1} \in KH = HK$, então $x^{-1} \in HK$. Assim, HK é um subgrupo de G .

Por outro lado, se HK é um subgrupo de G , então para qualquer $h \in H, k \in K, h^{-1}k^{-1} \in HK$ e assim $kh = (h^{-1}k^{-1})^{-1} \in HK$. Assim, $KH \subset HK$. Agora, se x é qualquer elemento de $HK, x^{-1} = hk \in HK$ e então $x = (x^{-1})^{-1} = k^{-1}h^{-1} \in KH$, então $HK \subset KH$. Assim, $HK = KH$. $\square$

Corolário 4. Se H, K são subgrupos do grupo abeliano G , então HK é um subgrupo de G .

Teorema 4. Se H e K são subgrupos finitos de G de ordens $|H|$ e $|K|$, respectivamente, então

$$|HK| = \frac{|H| \cdot |K|}{|H \cap K|}$$

Pode-se ver a demonstração deste teorema em [4].

1.5 Subgrupos normais e grupo quociente

O conceito de subgrupo normal também foi criado por Galois. Esses subgrupos são fundamentais no estudo dos grupos solúveis, que veremos mais adiante. Informalmente, um subgrupo é dito normal se a classe lateral à esquerda é igual a classe lateral à direita determinada pelo mesmo elemento $g \in G, \forall g$.

Seja G um grupo e N um subgrupo de G . Queremos saber se é possível induzir em G uma operação sobre o conjunto das classes laterais à direita de N em G , tal que

$$(Na, Nb) \mapsto Nab.$$

Dados $a, b \in G$ e $k, n \in N$ quaisquer, então a e ka são representantes da mesma classe Na e, b e nb são representantes da mesma classe Nb . Logo, a operação induzida sobre as classes laterais à direita é bem definida se, e somente se,

$$Nab = Nkanb, \quad \forall a, b \in G, \quad \forall k, n \in N;$$

logo,

$$Nabb^{-1}a^{-1} = Nkanbb^{-1}a^{-1},$$

ou seja, $N = Nana^{-1}, \quad \forall a \in G, \quad \forall n \in N,$

e portanto

$$gng^{-1} \in N, \quad \forall g \in G, \quad \forall n \in N.$$

O que nos leva à definição.

Definição 15. Um subgrupo N de G é considerado um subgrupo normal de G se, para cada $g \in G$ e $n \in N$, $gng^{-1} \in N$. Escreveremos $N \triangleleft G$.

Se gNg^{-1} representa o conjunto de todos os $gng^{-1}, n \in N$, então $N \triangleleft G$ se, e somente se, $gNg^{-1} \subset N$ para cada $g \in G$.

Lema 8. $N \triangleleft G$ se, e somente se $gNg^{-1} = N$ para todo $g \in G$.

Demonstração. Se $gNg^{-1} = N$ para cada $g \in G$, certamente $gNg^{-1} \subset N$, então $N \triangleleft G$.

Suponha que $N \triangleleft G$. Assim, se $g \in G$, $gNg^{-1} \subset N$ e $g^{-1}Ng = g^{-1}N(g^{-1})^{-1} \subset N$. Agora, como $g^{-1}Ng \subset N$, $N = g(g^{-1}Ng)g^{-1} \subset gNg^{-1} \subset N$, logo $N = gNg^{-1}$. $\square$

Vamos enfatizar que o Lema 8 não diz que para todo $n \in N$ e todo $g \in G$, $gng^{-1} = n$. Isso pode não ocorrer. Consideremos o grupo G como S_3 e N como o subgrupo $\{(1), (1, 2, 3), (1, 3, 2)\}$. Se calcularmos $(1, 2)N(1, 2)^{-1}$, obteremos $\{(1), (1, 3, 2), (1, 2, 3)\}$, mas $(1, 3, 2) \neq (1, 2, 3)$. Tudo o que precisamos é que o conjunto de elementos gNg^{-1} seja igual ao conjunto de elementos N .

Por meio dos exemplos a seguir, vamos ver se uma classe lateral à esquerda é ou não igual a uma classe lateral à direita. Seja G o grupo S_3 e seja H o subgrupo $\{(1), (1, 2)\}$. Como $(G : H) = 3$, existem três classes laterais à direita e três classes laterais à esquerda de H em G .

Classes à direita	Classes à esquerda
$H = \{(1), (1, 2)\}$	$H = \{(1), (1, 2)\}$
$H(1, 2, 3) = \{(1, 2, 3), (2, 3)\}$	$(1, 2, 3)H = \{(1, 2, 3), (1, 3)\}$
$H(1, 3, 2) = \{(1, 3, 2), (1, 3)\}$	$(1, 3, 2)H = \{(1, 3, 2), (2, 3)\}$

Vemos que as classes laterais à direita e à esquerda diferem.

Em $G = S_3$, consideremos o subgrupo $N = \{(1), (1, 2, 3), (1, 3, 2)\}$. Como $(G : N) = 2$, existem duas classes laterais à esquerda e duas classes laterais à direita de N em G .

$$\begin{array}{ll} \text{Classes à direita} & \text{Classes à esquerda} \\ N = \{(1), (1, 2, 3), (1, 3, 2)\} & N = \{(1), (1, 2, 3), (1, 3, 2)\} \\ N(1, 2) = \{(1, 2), (1, 3), (2, 3)\} & (1, 2)N = \{(1, 2), (2, 3), (1, 3)\} \end{array}$$

Nesse caso vemos que cada classe lateral à esquerda de N em G é uma classe lateral à direita em G e vice-versa. Assim, para alguns subgrupos a noção de classe lateral à esquerda coincide com a de classe lateral à direita, enquanto para alguns subgrupos esses conceitos diferem.

Teorema 5. *O subgrupo N de G é um subgrupo normal de G se, e somente se, cada classe lateral à esquerda de N em G é uma classe lateral à direita de N em G .*

Demonstração. Se $N \triangleleft G$, então para todo $g \in G$, $gNg^{-1} = N$. Portanto $(gNg^{-1})g = Ng \Rightarrow gN = Ng$. Assim, a classe lateral à esquerda gN é a classe lateral à direita Ng .

Vamos supor que toda classe lateral à esquerda de N em G seja uma classe lateral à direita de N em G . Assim, para $g \in G$, $gN = Ng'$, g pode ser diferente de g' . Como $g = ge \in gN$, qualquer que seja a classe lateral à esquerda gN ela deve conter o elemento g ; no entanto, g está na classe lateral à direita Ng e duas classes laterais à direita distintas não possuem elemento comum. Portanto, esta classe lateral à direita é única. Assim, segue-se que $gN = Ng$. Em outras palavras, $gNg^{-1} = Ngg^{-1} = N$ e portanto N é um subgrupo normal de G . $\square$

OBSERVAÇÃO: Um grupo *simples* é um grupo que não possui subgrupos normais não triviais.

Proposição 4. *Se $(G : H) = 2$, então $H \triangleleft G$.*

Demonstração. Se $(G : H) = 2$ então existem duas classes laterais à direita, digamos H e Ha com $a \notin H$, a classe $aH \neq H$. Assim $aH = Ha$ e então $H \triangleleft G$. $\square$

O significado de HK , sempre que H, K são subgrupos de G já foi definido. Pode-se estender esta definição para subconjuntos arbitrários, e isso é feito definindo, para dois subconjuntos A e B de G , $AB = \{x \in G | x = ab, a \in A, b \in B\}$. O que podemos dizer quando $A = B = H$ é um subgrupo de G ? $HH = \{h_1h_2 | h_1, h_2 \in H\} \subset H$ uma vez que H é fechado para a multiplicação. Mas $HH \supset He = H$ desde que $e \in H$. Assim, $HH = H$.

Lema 9. *Um subgrupo N de G é um subgrupo normal de G se, e somente se, o produto de duas classes laterais à direita de N em G for novamente uma classe lateral à direita de N em G .*

Demonstração. ($\implies$) Suponha que $N \triangleleft G$ e que $a, b \in G$. Consideremos Na e Nb , duas classes laterais distintas à direita de N em G . Uma vez que $N \triangleleft G$, $aN = Na$ e assim

$$NaNb = N(aN)b = N(Na)b = Nab = Nab.$$

($\Leftarrow$) Se N é um subgrupo de um grupo G , de modo que para cada par de elementos a, b de G existe um elemento c de G tal que

$$NaNb = Nc. \quad (1)$$

Queremos mostrar que N é normal em G , ou seja, $Na = aN$ para todo a em G .

Segue-se de (1) que para qualquer $n_1, n_2 \in N$ existe um $n_3 \in N$ tal que

$$n_1an_2b = n_3c.$$

Colocando $n_1 = 1$ e $n_2 = 1$ (onde 1 denota a identidade de G), obtemos

$$ab = n_3c.$$

Portanto $NaNb = Nc = N(n_3c) = Nab$ (que $N(n_3c) = Nc$ decorre do fato de que N é um subgrupo de G). Por isso temos

$$NaNb = Nab \quad \forall a, b \in G. \quad (2)$$

O resto é fácil! Colocando $b = 1$ em (2), temos

$$NaN = Na \quad \forall a \in G. \quad (3)$$

De (3) segue-se que para qualquer $n_1, n_2 \in N$ existe um $n_3 \in N$ tal que

$$n_1an_2 = n_3a,$$

de modo que

$$an_2 = n_1^{-1}n_3a.$$

Escrevendo $n_4 = n_1^{-1}n_3$, nós obtemos

$$an_2 = n_4a.$$

Isso implica $aN \subseteq Na$. Da mesma forma, podemos mostrar que $Na \subseteq aN$. Por isso temos

$$aN = Na \quad \forall a \in G.$$

□

Suponha que $N \triangleleft G$. A fórmula $NaNb = Nab$, para $a, b \in G$ é altamente sugestiva, pois o produto das classes laterais à direita é uma classe lateral à direita. Com essa operação veremos que o conjunto de todas as classes laterais à direita vai ter uma estrutura de grupo. Denotamos

por G/N a coleção de classes laterais à direita de N em G (os elementos de G/N são certos subconjuntos de G) e usamos o produto dos subconjuntos de G para nos render um produto em G/N . Para este produto vale:

- (1) $X, Y \in G/N$ implica $XY \in G/N$; para $X = Na, Y = Nb$ para algum $a, b \in G$, e $XY = NaNb = Nab \in G/N$.
- (2) $X, Y, Z \in G/N$, então $X = Na, Y = Nb, Z = Nc$ com $a, b, c \in G$ e assim $(XY)Z = (NaNb)Nc = N(ab)Nc = N(ab)c = Na(bc)$ (desde que G é associativo) $= Na(Nbc) = Na(NbNc) = X(YZ)$. Então o produto em G/N satisfaz a lei associativa.
- (3) Considere o elemento $N = Ne \in G/N$. Se $X \in G/N, X = Na, a \in G$, então $XN = NaNe = Nae = Na = X$, e da mesma forma $NX = X$. Consequentemente, Ne é um elemento de identidade para G/N .
- (4) Suponha que $X = Na \in G/N$ (onde $a \in G$); assim, $Na^{-1} \in G/N$ e $NaNa^{-1} = Naa^{-1} = Ne$. Da mesma forma $Na^{-1}Na = Ne$. Portanto, Na^{-1} é o inverso de Na em G/N .

Definição 16. Se G é um grupo, $N \triangleleft G$, então G/N é também um grupo. É chamado de grupo quociente ou grupo de fatores de G por N .

Por definição sabemos que G/N indica a quantidade de classes laterais à direita de H em G , ou seja $|G/N| = (G : N)$, então no caso de G ser finito sabemos que:

Lema 10. Se G é um grupo finito e $N \triangleleft G$, então $|G/N| = \frac{|G|}{|N|}$

EXEMPLO: Seja G o grupo de inteiros sob adição e seja N o subgrupo formado por todos os múltiplos de 3. Como a operação em G é adição, vamos escrever as classes laterais de N em G como $N + a$ em vez de Na . Considere as três classes laterais $N, N + 1, N + 2$. Afirmamos que estas são todas as classes laterais de N em G . De fato, dado $a \in G, a = 3b + c$ onde $b \in G$ e $c = 0, 1$ ou 2 (c é o resto de uma divisão por 3). Assim, $N + a = N + 3b + c = (N + 3b) + c = N + c$ pois $3b \in N$. Assim, cada classe lateral é $N, N + 1$ ou $N + 2$, e $G/N = \{N, N + 1, N + 2\}$. Como adicionamos elementos em G/N ? Nossa fórmula $NaNb = Nab$ se traduz em: $(N + 1) + (N + 2) = (N + 3) = N$ desde que $3 \in N$; $(N + 2) + (N + 2) = N + 4 = N + 1$ e assim por diante. Sem ser específico, sente-se que G/N está intimamente relacionado ao $\text{mod } 3$ de inteiros sob adição. Claramente o que fizemos para 3, poderíamos fazer para qualquer inteiro n , caso em que o grupo de fatores deveria sugerir uma relação com os inteiros $\text{mod } n$ sob adição.

Proposição 5. Seja G um grupo e seja $Z(G)$ seu centro. Se o quociente $G/Z(G)$ é cíclico, então $Z(G) = G$. Em particular, o índice de $Z(G)$ em G nunca é igual a um número primo.

Demonstração. Se $G/Z(G)$ é cíclico, então existe $a \in G$ tal que $G/Z(G) = \langle aZ(G) \rangle = \langle \bar{a} \rangle$. Assim, dado $x \in G$, existe $n \in \mathbb{Z}$ tal que $\bar{x} = \bar{a}^n$, ou seja, $xZ(G) = (aZ(G))^n = a^n Z(G)$.

Logo $x^{-1}a^n \in Z(G)$, ou seja, existe $y \in Z(G)$ tal que $x^{-1}a^n = y$, ou ainda, $x = a^n y^{-1}$.

Então, para $x, u \in G$ existem $m, n \in \mathbb{Z}$ e $y_1, y_2 \in Z(G)$ tais que $x = a^m y_1^{-1}$ e $u = a^n y_2^{-1}$.

Dai

$$\begin{aligned} xu &= (a^m y_1^{-1})(a^n y_2^{-1}) = y_2^{-1}(a^m y_1^{-1})a^n = y_2^{-1}a^m(a^n y_1^{-1}) = \\ &= (y_2^{-1}a^n)(a^m y_1^{-1}) = (a^n y_2^{-1})(a^m y_1^{-1}) = ux \end{aligned}$$

Em particular, se $|G/Z(G)| = p$ então $G/Z(G)$ é cíclico e portanto abeliano, ou seja, $G = Z(G)$ o que implica $|G/Z(G)| = 1$ contradizendo o fato de que $|G/Z(G)| = p$. Logo, o índice do centro no grupo não pode ser um número primo. $\square$

O teorema a seguir é uma recíproca do Teorema de Lagrange no caso dos divisores primos da ordem do grupo.

Teorema 6 (TEOREMA DE CAUCHY PARA GRUPOS ABELIANOS). *Suponha que G seja um grupo abeliano finito e p divide $|G|$, onde p é um número primo. Então há um elemento $a \neq e \in G$ tal que $a^p = e$.*

Demonstração. Usaremos indução sobre $|G|$, ou seja, vamos assumir que o teorema é verdadeiro para todos os grupos abelianos com menos elementos do que G . Assim, mostraremos que o resultado é válido para G . Note que o teorema é verdadeiro para grupos com um único elemento.

Se G não tem subgrupos $H \neq \{e\}, G$, (subgrupos triviais), G deve ser cíclico de primeira ordem. Este primo deve ser p e G certamente tem $p - 1$ elementos $a \neq e$ satisfazendo $a^p = a^{|G|} = e$.

Suponha que G tenha um subgrupo $N \neq \{e\}, G$. Se p divide $|N|$, pela hipótese de indução, uma vez que $|N| < |G|$ e N é abeliano, existe um elemento $b \in N, b \neq e$, satisfazendo $b^p = e$ (como $b \in N \subset G$ temos o elemento que precisamos). Portanto, podemos assumir que $p \nmid |N|$. Como G é abeliano e $N \triangleleft G$, então G/N é um grupo. Além disso, $|G/N| = \frac{|G|}{|N|}$ e como $p \nmid |N|$, p divide $\frac{|G|}{|N|} < |G|$. Como G é abeliano, G/N é abeliano. Assim, pela hipótese de indução, existe um elemento $X \in G/N$ que satisfaz $X^p = e_1$, a identidade de $G/N, X \neq e_1$. Pela própria forma dos elementos de $G/N, X = Nb, b \in G$, de modo que $X^p = (Nb)^p = Nb^p$. Dado que $e_1 = Ne$, $X^p = e_1, X \neq e_1$, se traduz em $Nb^p = N, Nb \neq N$. Assim, $b^p \in N, b \notin N$. Usando o corolário 2, $(b^p)^{|N|} = e$. Ou seja, $b^{|N|p} = e$. Seja $c = b^{|N|}$. Certamente $c^p = e$. Para mostrar que c é um elemento que satisfaz a conclusão do teorema, devemos finalmente mostrar que $c \neq e$. No entanto, se $c = e, b^{|N|} = e$, e assim $(Nb)^{|N|} = N$. Combinando isso com $(Nb)^p = N, p \nmid |N|, p$ um número primo, descobrimos que $Nb = N$, e assim $b \in N$, uma contradição. Assim $c \neq e, c^p = e$ e completamos a indução. Isso prova o resultado. $\square$

1.6 Homomorfismo

A noção de homomorfismo é uma ideia central comum a todos os aspectos da álgebra moderna. Informalmente, podemos entender que um homomorfismo é uma função que leva elementos de um grupo em outro grupo, conservando a estrutura de ambos.

Definição 17. *Sejam $(G, \cdot)$ e $(\mathcal{G}, \times)$ dois grupos. Uma função $f : G \rightarrow \mathcal{G}$ é um homomorfismo se ela é compatível com as estruturas dos grupos, isto é, se*

$$f(a \cdot b) = f(a) \times f(b), \forall a, b \in G.$$

EXEMPLOS:

1. Seja $n \in \mathbb{Z}$ fixo. Então, $f_n : (\mathbb{Z}, +) \rightarrow (\mathbb{Z}, +)$, $f_n(z) = nz$ é um homomorfismo. Se $(G, \cdot)$ for um grupo abeliano, então $f_n : G \rightarrow G$, $f_n(g) = g^n$ é um homomorfismo.
2. Seja $f : (\mathbb{Z}, +) \rightarrow (\mathbb{C}^*, \cdot)$ definida por $f(n) = i^n$. A função f é um homomorfismo de grupos, pois $\forall n, m \in \mathbb{Z}$ temos

$$f(n + m) = i^{n+m} = i^n i^m = f(n) \cdot f(m).$$

3. Seja $f : (\mathbb{R}_+^*, \cdot) \rightarrow (\mathbb{R}, +)$ definida por $f(x) = \log(x)$. A função f é um homomorfismo de grupos, uma vez que $\forall x, y \in \mathbb{R}_+^*$ temos

$$f(xy) = \log(xy) = \log(x) + \log(y) = f(x) + f(y).$$

4. Seja $g \in G$ fixo. Então, $\mathcal{I}_g : G \rightarrow G$, $\mathcal{I}_g(x) = gxg^{-1}$, é um homomorfismo bijetivo.

Definição 18. *Seja $f : G \rightarrow \mathcal{G}$ um homomorfismo de grupos.*

- (i) *Se f é injetora, dizemos que f é um monomorfismo.*
- (ii) *Se f é sobrejetora, dizemos que f é um epimorfismo.*
- (iii) *Se f é bijetora, dizemos que f é um isomorfismo.*
- (iv) *Se $G = \mathcal{G}$, dizemos que f é um endomorfismo.*
- (v) *Se f é bijetora e $G = \mathcal{G}$, dizemos que f é um automorfismo.*

Os resultados a seguir são fundamentais no estudo de homomorfismos.

Sejam G e $\mathcal{G}$ grupos quaisquer. Denotaremos por e_G e $e_{\mathcal{G}}$ as identidades de G e $\mathcal{G}$, respectivamente.

Proposição 6. *Se $f : G \rightarrow \mathcal{G}$ é um homomorfismo de grupos, então $f(e_G) = e_{\mathcal{G}}$.*

Demonstração. Temos

$$f(e_G) = f(e_G \cdot e_G) = f(e_G) \times f(e_G).$$

Aplicando $f(e_G)^{-1}$ à direita em ambos os lados, obtemos

$$f(e_G) \cdot f(e_G)^{-1} = f(e_G) \times f(e_G) \times f(e_G)^{-1}$$

e assim,

$$e_G = f(e_G).$$

□

Definição 19. Seja $H \triangleleft G$, então $\varphi : G \longrightarrow G/H$, $\varphi(g) = gH$, é um homomorfismo sobrejetor chamado de projeção canônica.

Proposição 7. Sejam $f : G \rightarrow \mathcal{G}$ um homomorfismo de grupos e $g \in G$ qualquer. Então $f(g^{-1}) = f(g)^{-1}$.

Demonstração. De fato, $e_G = f(e_G) = f(g \cdot g^{-1}) = f(g) \times f(g^{-1})$

□

Proposição 8. Seja $f : G \rightarrow \mathcal{G}$ um homomorfismo de grupos. Se $J \leq G$, então $f(J) \leq \mathcal{G}$.

Demonstração. Primeiramente observamos que $f(J)$ é não-vazio, pois $e_G \in J$ e $f(e_G) \in f(J)$. Sejam $a, b \in f(J)$. Então $a = f(x)$ e $b = f(y)$, com $x, y \in J$. Portanto,

$$ab^{-1} = f(x)f(y)^{-1} = f(xy^{-1}) \in f(J)$$

Logo, $ab^{-1} \in f(J)$. Assim podemos concluir que $f(J) \leq \mathcal{G}$ e que a imagem de subgrupo através de um homomorfismo é um subgrupo.

□

Teorema 7. Se f é um homomorfismo de G em $\mathcal{G}$ então o conjunto $K = \{x \in G | f(x) = e_G\}$ é um subgrupo normal de G . Este subgrupo é denominado o kernel (ou núcleo) de f e denotado por $\ker(f)$.

Demonstração. A princípio devemos confirmar se o $\ker(f)$ é um subgrupo de G . Dados $x, y \in \ker(f)$, temos

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

então $\ker(f) \leq G$. Com relação à normalidade do $\ker(f)$, precisamos mostrar que

$$gxg^{-1} \in \ker(f), \forall g \in G \text{ e } \forall x \in \ker(f).$$

De fato,

$$f(gxg^{-1}) = f(g) \times f(x) \times f(g^{-1}) = f(g) \times e_G \times f(g)^{-1} = f(g) \times f(g)^{-1} = e_G.$$

□

O próximo resultado irá relacionar o kernel de um homomorfismo com a injetividade dele.

Proposição 9. *Seja $f : G \rightarrow \mathcal{G}$ um homomorfismo de grupos. Então f é um monomorfismo se, e somente se, $\ker(f) = \{e_G\}$.*

Demonstração. ($\implies$) Suponha que f é monomorfismo, ou seja, f é injetora. Como $f(e_G) = e_{\mathcal{G}}$, então $e_G \in \ker(f)$. Por outro lado, seja $x \in \ker(f)$. Assim,

$$f(x) = e_{\mathcal{G}} \Rightarrow f(x) = f(e_G) \Rightarrow x = e_G.$$

Portanto, $\ker(f) = \{e_G\}$.

($\impliedby$) Suponha que $\ker(f) = \{e_G\}$. Sejam $x, y \in G$ quaisquer. Suponha que,

$$\begin{aligned} f(x) = f(y) &\Rightarrow f(x)f(y)^{-1} = f(y)f(y)^{-1} \Rightarrow f(xy^{-1}) = e_{\mathcal{G}} \Rightarrow xy^{-1} \in \ker(f) \Rightarrow \\ &xy^{-1} = e_G \Rightarrow xy^{-1}y = e_Gy \Rightarrow x = y. \end{aligned}$$

□

Como já vimos, f é um isomorfismo de G em $\mathcal{G}$ se f é uma bijeção. Quando isso ocorre existe um homomorfismo $g : \mathcal{G} \rightarrow G$ tal que $f \circ g = id_{\mathcal{G}}$ e $g \circ f = id_G$. Dizemos que G e $\mathcal{G}$ são *isomorfos* quando existe um isomorfismo entre os grupos G e $\mathcal{G}$, e denotamos $G \simeq \mathcal{G}$.

Seja $G = \{a_1, a_2, \dots, a_n\}$ um grupo com ordem n munido de uma operação qualquer. Podemos entender como "funciona" o grupo por meio de uma tabela de operações:

G	a_1	a_2	$\dots$	a_n
a_1	$a_1 \cdot a_1$	$a_1 \cdot a_2$	$\dots$	$a_1 \cdot a_n$
a_2	$a_2 \cdot a_1$	$a_2 \cdot a_2$	$\dots$	$a_2 \cdot a_n$
$\vdots$	$\vdots$	$\vdots$	$\dots$	$\vdots$
a_n	$a_n \cdot a_1$	$a_n \cdot a_2$	$\dots$	$a_n \cdot a_n$

EXEMPLO: Consideremos o grupo $G = \{1, -1\}$ munido do produto usual de números reais.

G	1	-1
1	1	-1
-1	-1	1

Agora tome $\mathbb{Z}_2 = \{\bar{0}, \bar{1}\}$ com a soma definida por $\bar{a} + \bar{b} = \overline{a+b}$. Onde $\bar{0} + \bar{1} = \bar{1}$, $\bar{1} + \bar{1} = \bar{2} = \bar{0}$ e $\bar{0} + \bar{0} = \bar{0}$.

$\mathbb{Z}_2$	$\bar{0}$	$\bar{1}$
$\bar{0}$	$\bar{0}$	$\bar{1}$
$\bar{1}$	$\bar{1}$	$\bar{0}$

Percebemos que por mais que os grupos tenham elementos e operações de natureza distintas, as tabelas das operações dos grupos são de certa forma iguais. Portanto, para $G = \{1, -1\}$ com produto de reais e $\mathcal{G} = \mathbb{Z}_2 = \{\bar{0}, \bar{1}\}$ com a soma apresentada acima, vale que $G \simeq \mathcal{G}$.

Com efeito, defina a bijeção $f : G \rightarrow \mathcal{G}$ por $f(1) = \bar{0}$ e $f(-1) = \bar{1}$.

Podemos verificar que $f(a \cdot b) = f(a) + f(b) \forall a, b \in G$:

- (i) $f(1 \cdot 1) = f(1) = \bar{0} = \bar{0} + \bar{0} = f(1) + f(1)$
- (ii) $f(1 \cdot (-1)) = f(-1) = \bar{1} = \bar{0} + \bar{1} = f(1) + f(-1)$
- (iii) $f((-1) \cdot (-1)) = f(1) = \bar{0} = \bar{1} + \bar{1} = f(-1) + f(-1)$

$\therefore G$ e $\mathcal{G}$ são isomorfos.

Teorema 8 (1º Teorema do Isomorfismo). *Seja $f : (G, \cdot) \rightarrow (\mathcal{G}, \times)$ um homomorfismo de grupos. Então, a função induzida*

$$\bar{f} : \frac{G}{\ker(f)} \longrightarrow f(G)$$

$$g\ker(f) \longmapsto f(g)$$

é um isomorfismo.

Demonstração. A princípio vamos verificar que $\bar{f}$ é uma função bem definida, isto é, se $g\ker(f) = \tilde{g}\ker(f) \Rightarrow f(g) = f(\tilde{g})$. Mas, $g\ker(f) = \tilde{g}\ker(f)$ implica que $g = \tilde{g} \cdot k$, para algum $k \in \ker(f)$ e, portanto,

$$f(g) = f(\tilde{g} \cdot k) = f(\tilde{g}) \times f(k) = f(\tilde{g}) \times e_{\mathcal{G}} = f(\tilde{g}).$$

Agora, $\bar{f}$ é claramente uma função sobrejetora e, para $g, g' \in G$ obtemos

$$\bar{f}(g\ker(f) \cdot g'\ker(f)) = \bar{f}((gg')\ker(f)) = f(g \cdot g') = f(g) \times f(g') = \bar{f}(g\ker(f)) \times \bar{f}(g'\ker(f));$$

assim $\bar{f}$ é um homomorfismo. Agora,

$$\ker(\bar{f}) = \{g\ker(f) | f(g) = e_{\mathcal{G}}\} = \{g\ker(f) | g \in \ker(f)\} = \ker(f);$$

assim $\ker(\bar{f}) = \{e_{G/\ker(f)}\}$ ou seja, a função $\bar{f}$ é injetiva. □

O Teorema acima gera vários resultados importantes. Alguns deles são:

Corolário 5. *Seja $f : G \rightarrow \mathcal{G}$ um homomorfismo de grupos e seja $H \leq G$. Então a função*

$$\begin{aligned} \frac{H}{H \cap \ker(f)} &\longrightarrow f(H) \\ h \cdot (H \cap \ker(f)) &\longmapsto f(h) \end{aligned}$$

é um isomorfismo.

Corolário 6. *Seja $H \triangleleft G$. Então a função*

$$\begin{aligned} \{\text{subgrupos normais de } G \text{ que contem } H\} &\longleftrightarrow \{\text{subgrupos normais de } \frac{G}{H}\} \\ K &\longmapsto K/H \end{aligned}$$

é uma bijeção.

Teorema 9 (2º Teorema do Isomorfismo). *Sejam $H \triangleleft G$ e $K \leq G$. Então,*

$$\frac{K}{H \cap K} \simeq \frac{KH}{H}.$$

Demonstração. Já que $H \triangleleft G$, sabemos que KH é um subgrupo de G e que $HK = KH$. Claramente, $H \triangleleft G \Rightarrow H \triangleleft KH$ e, portanto, faz sentido considerar o grupo quociente KH/H . Considere o homomorfismo canônico $\varphi : KH \rightarrow KH/H$ e seja $\varphi|_K$ a sua restrição ao subgrupo $K \leq KH$, isto é:

$$\begin{aligned} \varphi|_K : K &\longrightarrow \frac{KH}{H} \\ k &\longmapsto kH \end{aligned}$$

Claramente, $\ker(\varphi|_K) = \{k \in K | kH = H\} = H \cap K$. Seja agora $\alpha \in KH/H$; temos $\alpha = (kh)H$ para algum $k \in K$ e algum $h \in H$; logo $\alpha = (kh)H = kH = \varphi|_K(k)$ e portanto $\varphi|_K$ é sobrejetor. Aplicando agora o 1º Teorema do Isomorfismo ao homomorfismo $\varphi|_K$, obtemos o teorema. $\square$

Teorema 10 (3º Teorema do Isomorfismo). *Sejam $K \leq H \leq G$ com $K \triangleleft G$ e $H \triangleleft G$. Então,*

$$\frac{G/K}{H/K} \simeq \frac{G}{H}$$

Demonstração. Consideremos o homomorfismo

$$\begin{aligned} \varphi : \frac{G}{K} &\longrightarrow \frac{G}{H} \\ gK &\longmapsto gH \end{aligned}$$

Pode-se verificar que a função φ está bem definida, pois $gK = \tilde{g}K \Rightarrow g = \tilde{g}k$ para algum $k \in K$. Logo nota-se que $gH = \tilde{g}kH = \tilde{g}H$, uma vez que $k \in K \subseteq H$. Obviamente,

φ é sobrejetora e $\ker(\varphi) = H/K$. Usando o 1º Teorema do Isomorfismo em φ , tem-se o teorema. $\square$

Definição 20. Dados dois grupos G, H , o produto direto de G por H é o conjunto $G \times H$ munido da função

$$\begin{aligned} * : (G \times H) \times (G \times H) &\longrightarrow (G \times H) \\ ((g_1, h_1), (g_2, h_2)) &\longmapsto (g_1 g_2, h_1 h_2). \end{aligned}$$

Se G é um grupo, e $H, K \leq G$, então $HK := \{hk \in G \mid h \in H, k \in K\}$

Teorema 11. G é (isomorfo ao) produto direto $H \times K$ se, e somente se:

- (i) H, K são normais em G ;
- (ii) $H \cap K = \{e\}$;
- (iii) $HK = G$.

Um grupo pode ser expresso em termos de grupos menos complexos, ou seja, podemos encontrar condições para que um grupo G seja isomorfo a um produto direto de grupos $G_1, \dots, G_n$.

Teorema 12. Sejam $G, G_1, \dots, G_n$ grupos. Então o grupo G é isomorfo ao grupo $G_1 \times \dots \times G_n$ se, e somente se, o grupo G possui subgrupos $H_1 \simeq G_1, \dots, H_n \simeq G_n$ tais que:

- (i) $G = H_1 \dots H_n$.
- (ii) $H_i \triangleleft G, \forall i = 1, \dots, n$.
- (iii) $H_i \cap (H_1 \dots H_{i-1} H_{i+1} \dots H_n) = \{e\}, \forall i = 1, \dots, n$.

CAPÍTULO 2

ESTUDO DE UM GRUPO VIA REPRESENTAÇÕES POR PERMUTAÇÕES

Se G e $\mathcal{G}$ são dois grupos e $\rho : G \rightarrow \mathcal{G}$ é um homomorfismo, é razoável esperar que algumas propriedades de G possam ser transportadas para $\mathcal{G}$ via o homomorfismo ρ . Assim podemos tentar estudar um grupo G via um outro grupo $\mathcal{G}$ e um homomorfismo $\rho : G \rightarrow \mathcal{G}$.

Dado um grupo G , uma *representação* de G é um homomorfismo ρ de G em algum grupo $\mathcal{G}$. Se $C = \{u_1, \dots, u_n\}$ é um conjunto de n elementos e $\mathcal{P}(C)$ é o grupo das permutações do conjunto C , uma representação do tipo $\rho : G \rightarrow \mathcal{P}(C)$ é chamada de *representação de G por permutações de grau n* .

2.1 Representação de um grupo por permutações

Definição 21. *Sejam G um grupo, C um conjunto e $\mathcal{P}(C)$ o grupo de permutações de C . Uma representação de G no grupo de permutações de C é um homomorfismo $\rho : G \rightarrow \mathcal{P}(C)$, isto é, uma função tal que $\rho(g_1 g_2) = \rho(g_1) \circ \rho(g_2)$. Diz-se também que o grupo G opera sobre o conjunto C .*

Dado um grupo G , podemos considerar G também como um conjunto; neste caso, para evitar confusões, utilizaremos o símbolo G_0 para designar o conjunto G .

Vejamos agora alguns exemplos de representação em grupos por permutações.

EXEMPLO 1: Seja G um grupo e seja $C = G_0$. Considere

$$\begin{aligned} \mathcal{I} : G &\longrightarrow \mathcal{P}(G_0) \\ g &\longmapsto \mathcal{I}_g : G_0 \rightarrow G_0 \\ &\quad a \mapsto ga g^{-1}. \end{aligned}$$

Como $\mathcal{I}$ é um homomorfismo, então é uma representação de G no grupo de permutações do conjunto G_0 .

EXEMPLO 2: Seja G um grupo e seja $C = G_0$. Considere

$$\begin{aligned} T : G &\longrightarrow \mathcal{P}(G_0) \\ g &\longmapsto T_g : G_0 \rightarrow G_0 \\ &a \mapsto ga. \end{aligned}$$

Assim, T é um homomorfismo e temos uma outra representação de G no grupo de permutações do conjunto G_0 .

EXEMPLO 3: Seja G um grupo e seja $C = \{\text{subgrupos de } G\}$. Considere a aplicação

$$\begin{aligned} \mathcal{I} : G &\longrightarrow \mathcal{P}(C) \\ g &\longmapsto \mathcal{I}_g : C \rightarrow C \\ &H \mapsto gHg^{-1}. \end{aligned}$$

Pode-se verificar que, $\forall g \in G$, a função $\mathcal{I}_g : C \rightarrow C$ é uma permutação de C e que a aplicação $\mathcal{I}$ é um homomorfismo. Portanto, a aplicação $\mathcal{I}$ é uma representação do grupo G no grupo de permutações do conjunto dos subgrupos de G .

Se todos os subgrupos de G forem normais (se G for abeliano, por exemplo) a representação é trivial (o homomorfismo é trivial).

EXEMPLO 4: Seja m um inteiro positivo. Sejam G um grupo e $C = \{\text{subgrupos de } G \text{ de ordem } m\}$. Considere

$$\begin{aligned} \mathcal{I} : G &\longrightarrow \mathcal{P}(C) \\ g &\longmapsto \mathcal{I}_g : C \rightarrow C \\ &H \mapsto gHg^{-1}. \end{aligned}$$

É óbvio que se H é um subgrupo de ordem m , então $\mathcal{I}_g(H) = gHg^{-1}$ também é subgrupo de ordem m e $\mathcal{I}_g$ é realmente uma função de C em C . Facilmente vemos que $\mathcal{I}_g$ é uma bijeção. De fato, se $H_1, H_2 \in C$ são tais que $\mathcal{I}_g(H_1) = \mathcal{I}_g(H_2)$, isto é, $gH_1g^{-1} = gH_2g^{-1}$, então $H_1 = g^{-1}(gH_1g^{-1})g = g^{-1}(gH_2g^{-1})g = H_2$ de modo que a função $\mathcal{I}_g$ é injetiva. Se $H \in C$, então também $g^{-1}Hg \in C$, e $H = g(g^{-1}Hg)g^{-1} = \mathcal{I}_g(g^{-1}Hg)$, de modo que $\mathcal{I}$ é sobrejetiva. Para finalizar, pode-se verificar que $\mathcal{I}$ é um homomorfismo. Assim, $\mathcal{I}$ é uma representação de G no grupo de permutações do conjunto dos subgrupos de G de ordem m . Se todos os subgrupos de G de ordem m forem normais a representação acima é trivial.

EXEMPLO 5: Seja G um grupo e seja $C = \{\text{Classes laterais à esquerda de } H \text{ em } G\} = \{aH | a \in G\}$, onde H é um subgrupo do grupo G . Considere a aplicação

$$\begin{aligned} T : G &\longrightarrow \mathcal{P}(C) \\ g &\longmapsto T_g : C \rightarrow C \\ aH &\mapsto gaH. \end{aligned}$$

De forma clara nota-se que T_g é uma bijeção. De fato, se $aH, bH \in C$ são tais que $T_g(aH) = T_g(bH)$, isto é, são tais que $gaH = gbH$, então $aH = g^{-1}gaH = g^{-1}gbH = bH$, de modo que T_g é injetiva. Se $cH \in C$, então $g^{-1}cH \in C$ e $cH = gg^{-1}cH = T_g(g^{-1}cH)$, de modo que T_g é sobrejetiva. Pra finalizar, facilmente se verifica que T é um homomorfismo. Portanto, T é uma representação de G no grupo de permutações do conjunto das classes laterais à esquerda de H em G . Note que $\ker(T) = \{g \in G | aga^{-1} \in H, \forall a \in G\} \subseteq H$.

EXEMPLO 6: Sejam G um grupo e $K \leq G$. Seja $H \leq G$ e seja $C = \{\text{Classes laterais à esquerda de } H \text{ em } G\} = \{aH | a \in G\}$. Considere a restrição a K do homomorfismo T definido no Exemplo 5, isto é, considere

$$\begin{aligned} T : K &\longrightarrow \mathcal{P}(C) \\ k &\longmapsto T_k : C \rightarrow C \\ aH &\mapsto kaH. \end{aligned}$$

Portanto, T é uma representação de K no grupo de permutações do conjunto das classes laterais à esquerda de H em G .

As representações definidas a partir da função $\mathcal{I} : g \mapsto \mathcal{I}_g$ são chamadas *representações por conjugação* e representações definidas a partir da função $T : g \mapsto T_g$ são chamadas *representações por translação, ou representações regulares*. Os exemplos 1, 3 e 4 são exemplos de representações por conjugação. Os exemplos 2, 5 e 6 são exemplos de representações por translação.

Sejam G um grupo, C um conjunto e seja $\rho : G \rightarrow \mathcal{P}(C)$ uma representação de G . Sobre o conjunto C , é definida a seguinte relação de equivalência:

$$\forall x, y \in C, x \sim y \Leftrightarrow \exists g \in G \text{ tal que } \rho(g)(x) = y.$$

Definição 22. *Seja $x \in C$. A órbita de x é o conjunto*

$$\mathfrak{D}(x) := \{y \in C | y \sim x\} = \{\rho(g)(x) | g \in G\}.$$

O estabilizador de x é o conjunto dos elementos de G que deixam o elemento x fixo, isto é

$$E(x) := \{g \in G | \rho(g)(x) = x\}.$$

O estabilizador $E(x)$ é um subgrupo de G .

O teorema abaixo mostra que existe uma relação entre a órbita de um elemento e o seu estabilizador.

Teorema 13. *Seja $\rho : G \longrightarrow \mathcal{P}(C)$ uma representação do grupo G no grupo de permutações do conjunto C . Seja $x \in C$. Então a aplicação ψ abaixo é uma bijeção:*

$$\begin{aligned}\psi : \mathfrak{D}(x) &\longrightarrow \{\text{Classes laterais à esquerda de } E(x) \text{ em } G\} \\ \rho(g)(x) &\longmapsto gE(x).\end{aligned}$$

Em particular, no caso de G ser um grupo finito, temos que $|\mathfrak{D}(x)| = (G : E(x))$ e que $|\mathfrak{D}(x)|$ divide $|G|$.

Demonstração. Antes de tudo, deve-se verificar que a aplicação ψ é bem definida no sentido de que a imagem $\psi(y)$ de um elemento $y \in \mathfrak{D}(x)$ não depende da escolha do elemento $g \in G$ utilizado para obter y a partir de x . Sejam $g_1, g_2 \in G$ tais que $\rho(g_1)(x) = \rho(g_2)(x)$; então aplicando $\rho(g_2^{-1})$ em ambos os lados e utilizando o fato de ρ ser um homomorfismo, obtemos $\rho(g_2^{-1}g_1)(x) = x$; assim, temos que $(g_2^{-1}g_1) \in E(x)$, logo $g_1 \in g_2E(x)$ e $g_1E(x) = g_2E(x)$.

A aplicação ψ é sobrejetora pois, se $gE(x)$ é uma classe lateral à esquerda de $E(x)$ em G , então temos que $gE(x) = \psi(y)$ com $y = \rho(g)(x)$.

Para verificar a injetividade de ψ , sejam $y_1 = \rho(g_1)(x)$ e $y_2 = \rho(g_2)(x)$ dois elementos de $\mathfrak{D}(x)$ tais que $\psi(y_1) = \psi(y_2)$, isto é, tais que $g_1E(x) = g_2E(x)$. Então temos $g_1^{-1}g_2 \in E(x)$, logo $\rho(g_1^{-1}g_2)(x) = x$, ou seja $\rho(g_1^{-1}) \circ \rho(g_2)(x) = x$ e, portanto, temos $y_2 = \rho(g_2)(x) = \rho(g_1) \circ \rho(g_1^{-1}) \circ \rho(g_2)(x) = \rho(g_1)(x) = y_1$. $\square$

Os conceitos de órbita e estabilizador de um elemento serão considerados em algumas das representações particulares nos seguintes exemplos:

EXEMPLO 1: Sejam G um grupo e $C = G_0$. Seja

$$\begin{aligned}\mathcal{I} : G &\longrightarrow \mathcal{P}(G_0) \\ g &\longmapsto \mathcal{I}_g : G_0 \rightarrow G_0 \\ &\quad x \mapsto gxg^{-1}.\end{aligned}$$

Seja $x \in G_0$. A órbita $\mathfrak{D}(x) = \{\mathcal{I}_g(x) | g \in G\} = \{gxg^{-1} | g \in G\}$ de um elemento $x \in G_0$ nesta representação por conjugação se chama a *classe de conjugação de x* , e se denota $\mathcal{Cl}(x)$. Os elementos de $\mathcal{Cl}(x)$ se chamam os *conjugados de x em G* . Observe que temos $\mathcal{Cl}(x) = \{x\} \Leftrightarrow gxg^{-1} = x, \forall g \in G \Leftrightarrow x \in Z(G)$. O estabilizador $E(x) = \{g \in G | \mathcal{I}_g(x) = x\} = \{g \in G | gxg^{-1} = x\} = \{g \in G | g \text{ comuta com } x\}$ de um elemento $x \in G_0$, nesta representação por conjugação se chama o *centralizador de x* , e se denota $Z(x)$.

Aqui, o Teorema 13 nos dá

$$|\mathcal{Cl}(x)| = \#\{\text{conjugados de } x \text{ em } G\} = (G : Z(x)).$$

Logo, o conjunto G_0 é igual à união disjunta das classes de conjugação. Em cada classe de conjugação escolhemos um representante x_α . Então temos $|G| = \sum_\alpha |\mathcal{Cl}(x_\alpha)|$, e assim

$$|G| = |Z(G)| + \sum_{x_\alpha \notin Z(G)} |\mathcal{Cl}(x_\alpha)|.$$

Esta igualdade se chama a *equação das classes de conjugação*.

Por meio desta equação pode-se tirar algumas conclusões interessantes:

AFIRMAÇÃO 1: Seja p um número primo e seja G um grupo de ordem p^n com $n \geq 1$. Então $Z(G)$ tem pelo menos p elementos.

Demonstração. Temos $|G| = |Z(G)| + \sum_{x_\alpha \notin Z(G)} |\mathcal{Cl}(x_\alpha)|$. Para elementos $x_\alpha \notin Z(G)$, temos $|\mathcal{Cl}(x_\alpha)| > 1$; pelo Teorema 13, sabemos que $|\mathcal{Cl}(x_\alpha)|$ divide $|G|$, isto é, divide p^n ; logo, $|\mathcal{Cl}(x_\alpha)|$ é um múltiplo de p , $\sum_{x_\alpha \notin Z(G)} |\mathcal{Cl}(x_\alpha)|$ é um múltiplo de p e portanto $|Z(G)| = |G| - \sum_{x_\alpha \notin Z(G)} |\mathcal{Cl}(x_\alpha)|$ é um múltiplo de p . Por outro lado, já que o elemento neutro pertence a $Z(G)$, temos $|Z(G)| \neq 0$. Portanto, o centro $Z(G)$ tem pelo menos p elementos. $\square$

AFIRMAÇÃO 2: Seja p um número primo. Então todo grupo G de ordem p^2 é abeliano.

Demonstração. Pela Afirmação 1, temos $|Z(G)| = p$ ou p^2 ; por outro lado, pela Proposição 5, sabemos que o centro de um grupo nunca pode ter índice no grupo igual a um primo; logo $|Z(G)| = p^2$ e portanto, o grupo G é abeliano. $\square$

EXEMPLO 2: Seja G um grupo e seja $C = \{\text{subgrupos de } G\}$. Considere a representação

$$\begin{aligned} \mathcal{I} : G &\longrightarrow \mathcal{P}(C) \\ g &\longmapsto \mathcal{I}_g : C \rightarrow C \\ &H \mapsto gHg^{-1}. \end{aligned}$$

A órbita $\mathfrak{D}(H) = \{\mathcal{I}_g(H) | g \in G\} = \{gHg^{-1} | g \in G\}$ de um subgrupo H se chama a *classe de conjugação* de H . Os elementos de $\mathfrak{D}(H)$ se chamam os *subgrupos conjugados* de H . Pode-se observar que temos $\mathfrak{D}(H) = \{H\} \Leftrightarrow H \triangleleft G$.

O estabilizador $E(H) = \{g \in G | \mathcal{I}_g(H) = H\} = \{g \in G | gHg^{-1} = H\}$ se chama o *normalizador* de H em G e será denotado por $N_G(H)$, sendo um subgrupo de G . Se $N_G(H) = G$ então $H \triangleleft G$. Aqui o Teorema 13 nos dá

$$\#\{\text{conjugados de } H \text{ em } G\} = (G : N_G(H)).$$

2.2 Teoremas de Sylow

Seja H um subgrupo de um grupo finito G . Pelo Teorema de Lagrange sabemos que $|H|$ divide $|G|$. Pode-se perguntar se a recíproca desse teorema vale, ou seja, se G é um grupo finito, $k \in \mathbb{N}$ e k divide $|G|$. Existe $H \leq G$ tal que $|H| = k$? A resposta no caso de grupos cíclicos é positiva, mas geralmente a resposta é negativa. Por exemplo, S_4 é o grupo das permutações de $\{1, 2, 3, 4\}$. Nesse grupo existe um subgrupo chamado A_4 , que tem índice 2 em S_4 , é de ordem 12 e não possui nenhum subgrupo de ordem 6.

O resultado mais geral na direção de uma recíproca ao Teorema de Lagrange são os Teoremas de Sylow.

Teorema 14 (1º Teorema de Sylow). *Sejam p um número primo e G um grupo de ordem $p^m b$ com $(p, b) = 1$. Então, para cada n , $0 \leq n \leq m$ existe um subgrupo H de G tal que $|H| = p^n$.*

Demonstração. Fazemos uma prova por indução sobre $|G|$.

Se $|G| = 1$, não há nada para fazer.

Se $|G| > 1$ supomos, como hipótese de indução, que o teorema vale para todos os grupos de ordem menor que $|G|$; queremos mostrar que o teorema vale também para o grupo G .

Seja n um inteiro positivo tal que p^n divida a ordem de G . Podemos considerar duas possibilidades:

- Existe um subgrupo próprio H de G tal que p^n divida a ordem de H . Neste caso, pela hipótese de indução, temos que H , e portanto G , possui um subgrupo de ordem p^n .
- Não existe um subgrupo próprio H de G tal que p^n divida a sua ordem. Neste caso, consideremos a equação das classes de conjugação:

$$|G| = |Z(G)| + \sum_{x_\alpha \notin Z(G)} |\mathcal{Cl}(x_\alpha)| = |Z(G)| + \sum_{x_\alpha \notin Z(G)} (G : Z(x_\alpha)).$$

Para $x_\alpha \notin Z(G)$ temos $Z(x_\alpha) \subsetneq G$. Logo, por hipótese p^n não divide $|Z(x_\alpha)|$, e portanto p divide $(G : Z(x_\alpha))$. Como p divide $|G|$, obtemos então que p divide $|Z(G)|$. Como $Z(G)$ é um grupo abeliano existe um elemento $y \in Z(G)$ de ordem p . Como $y \in Z(G)$, é claro que $\langle y \rangle \triangleleft G$, de modo que podemos considerar o grupo quociente $G/\langle y \rangle$. Naturalmente, $|G/\langle y \rangle| < |G|$ e p^{n-1} divide $|G/\langle y \rangle|$. Logo, pela hipótese de indução, o grupo $G/\langle y \rangle$ possui um subgrupo K' de ordem p^{n-1} . Considere o homomorfismo canônico $\varphi : G \rightarrow G/\langle y \rangle$ e tome $K = \varphi^{-1}(K')$. Então K é um subgrupo de G e $|K| = |\ker(\varphi)||K'| = |\langle y \rangle||K'| = p^n$. $\square$

Corolário 7 (Generalização do Teorema de Cauchy). *Sejam G um grupo finito e p um número primo que divide $|G|$. Então existe um elemento $x \in G$ de ordem p .*

Corolário 8. *Seja G um grupo finito e seja p um número primo. Seja p^m a maior potência de p que divide $|G|$. Então existe um subgrupo de G de ordem p^m .*

Definição 23. *Sejam G um grupo finito, p um primo e p^m a maior potência de p que divide $|G|$. Os subgrupos de G que têm ordem p^m são chamados de p -subgrupos de Sylow de G .*

Se p é um número primo que não divide $|G|$, então e é o único p -subgrupo de Sylow de G .

Corolário 9. *Sejam G um grupo finito e p um número primo. Então $|G|$ é igual a uma potência de p se, e somente se, cada elemento do grupo G tem sua ordem igual a uma potência de p .*

Demonstração. Suponha que $|G| = p^t$ e seja $x \in G$, então a ordem de x é um divisor de p^t e, portanto, uma potência de p . Se $|G|$ não é uma potência de p , existe um número primo q tal que $q \neq p$ e q divide $|G|$; pelo Corolário 7, existe um elemento $x \in G$ de ordem q . $\square$

Definição 24. *Seja p um primo. Um grupo G (pode não ser finito) no qual todo elemento tem sua ordem igual a uma potência de p é chamado um p -grupo.*

Vimos que um p -subgrupo de Sylow de um grupo finito G , cuja ordem pode ser dividida pela maior potência de um número primo p^m , é um subgrupo de G de ordem p^m . É óbvio que se S é um p -subgrupo de Sylow de G e se $\rho \in \text{Aut}(G)$, então $\rho(S)$ é também um p -subgrupo de Sylow de G , pois ele tem p^m elementos. No caso particular de $\rho \in \mathcal{I}(G)$, isto é, se $\rho = \mathcal{I}_g$ para algum $g \in G$, então $\mathcal{I}_g(S) = gSg^{-1}$ é um p -subgrupo de Sylow de G . Então é possível verificar que, dado um primo p , todos os p -subgrupos de Sylow podem ser obtidos deste modo a partir de um deles, sendo todos os p -subgrupos de Sylow de G conjugados entre si.

Teorema 15 (2º Teorema de Sylow). *Sejam G um grupo finito, p um número primo e n_p o número de p -subgrupos de Sylow de G . Então:*

- Todos os p -subgrupos de Sylow de G são conjugados entre si. Em particular, um p -subgrupo de Sylow S de G é normal em G se, e somente se, S é o único p -subgrupo de Sylow de G .*
- Se P é um p -subgrupo de G , existe um p -subgrupo de Sylow S de G tal que $P \subseteq S$.*
- Se S é um p -subgrupo de Sylow, temos $n_p = (G : N_G(S))$.*

Demonstração. Para a demonstração deste teorema, usaremos o seguinte lema.

Lema 11. *Sejam G um grupo finito e p um número primo. Sejam S um p -subgrupo de Sylow de G e P um p -subgrupo qualquer de G . Então $P \cap N_G(S) = P \cap S$.*

DEMONSTRAÇÃO DO TEOREMA: Seja S um p -subgrupo de Sylow qualquer de G . Considere o conjunto $C = \{\text{conjugados de } S\} = \{gSg^{-1}; g \in G\}$. Por definição o conjunto C é a órbita de S na representação por conjugação $\mathcal{I} : G \rightarrow \mathcal{P}(D)$ onde denotamos $D = \{\text{subgrupos de } G\}$; portanto, pelo Teorema 13, temos

$$|C| = (G : N_G(S))$$

Para os itens a e b temos que mostrar que se P é um p -subgrupo qualquer de G , então o subgrupo P está contido num conjugado de S em G .

Consideremos a representação de P :

$$\begin{aligned}\mathcal{I} : P &\longrightarrow \mathcal{P}(C) \\ a &\longmapsto \mathcal{I}_a : C \rightarrow C \\ gSg^{-1} &\mapsto agSg^{-1}a^{-1}.\end{aligned}$$

Sejam $\mathfrak{D}_1, \dots, \mathfrak{D}_k$ as órbitas distintas dessa representação e para cada $\mathfrak{D}_i$ escolha um representante $S_i = g_i S g_i^{-1}$ dentro de $\mathfrak{D}_i$. É claro que $|C| = \sum_{i=1}^k |\mathfrak{D}_i|$; ademais, pelo Teorema 13, temos que $|\mathfrak{D}_i| = (P : E(S_i)) = (P : P \cap N_G(S_i))$ e, de acordo com o lema anterior, temos $(P : P \cap N_G(S_i)) = (P : P \cap S_i)$. Logo obtemos

$$|C| = \sum_{i=1}^k (P : P \cap S_i).$$

Das duas expressões obtidas para $|C|$, segue que

$$(G : N_G(S)) = \sum_{i=1}^k (P : P \cap S_i) \quad (*)$$

Cada parcela $(P : P \cap S_i)$ é igual a 1 ou a um múltiplo de p , pois P é um p -grupo. Em contrapartida, o primo p não divide $(G : S)$ pois S é um p -subgrupo de Sylow; portanto, $p \nmid (G : N_G(S))$. Em consequência disto, existe i tal que $p \nmid (P : P \cap S_i)$, logo $(P : P \cap S_i) = 1$ e portanto $P \subseteq S_i$.

Para o item c , pelo item a temos $\{p\text{-subgrupos de Sylow}\} = \{\text{conjugados de } S\}$, logo $n_p = (G : N_G(S))$. $\square$

Vimos que os p -subgrupos de Sylow são conjugados entre si, e o número n_p deles é igual $(G : N_G(S))$, sendo S um qualquer deles. As propriedades que veremos a seguir vão localizar o inteiro $(G : N_G(S))$ num pequeno conjunto de divisores de $|G|$.

Teorema 16 (3º Teorema de Sylow). *Sejam p um número primo e G um grupo finito de ordem $p^m b$, com $(p, b) = 1$. Seja n_p o número de p -subgrupos de Sylow de G . Então*

$$\begin{cases} n_p \text{ divide } b, \\ n_p \equiv 1 \text{ modulo } p. \end{cases}$$

Demonstração. Seja S um p -subgrupo de Sylow de G . Obviamente, temos que $(G : N_G(S))|(G : S) = b$. Consideraremos a expressão $(*)$ para $(G : N_G(S))$, estabelecida no decorrer da prova do Teorema 15. Tomando $P = S$ podemos obter $(G : N_G(S)) = \sum_{i=1}^k (S : S \cap S_i)$, onde $S_1, \dots, S_k$ representam distintamente as órbitas

$\mathcal{D}_1, \dots, \mathcal{D}_k$ da representação $\mathcal{I} : S \longrightarrow \mathcal{P}(C)$, sendo C o conjunto dos p -subgrupos de Sylow de G . Claramente podemos tomar $S_1 = S$, e assim temos

$$(G : N_G(S)) = (S : S \cap S) + \sum_{i=2}^k (S : S \cap S_i) \equiv 1 \mod p$$

Pelo Teorema 15 sabemos que $n_p = (G : N_G(S))$. Logo, temos os resultados desejados sobre n_p . □

CAPÍTULO 3

SOLUBILIDADE

Um dos conceitos mais antigos no estudo da teoria de grupos é o de grupos solúveis, que foi desenvolvido pelo famoso matemático Evariste Galois (1811-1832) ao estudar o problema de resolver equações algébricas polinomiais. Associando cada equação a um grupo, essas teriam solução se, e somente se, o grupo associado fosse solúvel.

Uma definição muito importante no estudo dos grupos solúveis é a definição do comutador de dois elementos de um grupo G .

3.1 Comutadores

Os grupos solúveis estão, de alguma forma, próximos dos grupos abelianos. Para mostrarmos isso, vamos inserir mais alguns conceitos no nosso estudo.

Definição 25. *Dados dois elementos x e y de um grupo G , o comutador de x e y é o elemento*

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

Um comutador de comprimento $n \geq 2$ é definido por

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

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

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

O grupo $G' = [G, G]$ é chamado subgrupo comutador ou subgrupo derivado de G .

É fácil mostrar que G' é um subgrupo normal de G . Iremos fazer essa demonstração daqui a pouco.

Depois de introduzirmos os conceitos acima, podemos definir a sequência de subgrupos a seguir:

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

Definição 26. O subgrupo $G^{(n)}$ definido acima é chamado o n -ésimo grupo derivado de G e a sequência $G = G^{(0)} \geq G^{(1)} \geq \dots \geq G^{(n)} \geq \dots$ chama-se a sequência derivada de G .

Existem algumas propriedades dos comutadores, as quais estão no seguinte lema.

Lema 12. 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 $\phi : G \rightarrow H$ é um homomorfismo de grupos, então $\phi([x, y]) = [\phi(x), \phi(y)]$.

No item (i) deste lema vemos que um grupo G é abeliano se, e somente se, $G' = 1$. Como em um grupo abeliano todos os elementos comutam uns com os outros, temos que $xy = yx$. Assim

$$x^{-1}y^{-1}xy = x^{-1}y^{-1}yx = x^{-1}x = 1.$$

O conhecimento de G' também nos mostra quando um grupo quociente é abeliano.

Lema 13. 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. Sejam x e y elementos de G . Denotaremos por $\bar{x}, \bar{y}$ duas classes em G/H . Um fato a ser notado é que $\bar{xy} = \bar{y}\bar{x} \Leftrightarrow [yx]^{-1}[xy] \in H$, isto é, se e somente se $[x, y] \in H \forall x, y \in G$, ou seja, $G' \subset H$. $\square$

Lema 14. *Sejam G um grupo e H e N subgrupos de G , então $[H, N] \subseteq N$ se, e somente se, $H \subseteq N_G(N)$. Particularmente, se N é normal em G , então $[H, N] \subseteq N$.*

Teorema 17. *Sejam G um grupo e H e N subgrupos normais em G , então $[H, N] \trianglelefteq G$.*

A próxima definição prova uma condição mais forte que a normalidade sobre um subgrupo derivado de G .

Definição 27. *Um subgrupo H de um grupo G diz-se um subgrupo característico se, $\phi(H) = H$ para todo automorfismo $\phi : G \rightarrow G$. Para indicar que H é um subgrupo característico de G escreveremos $H \text{ char } G$.*

Dizer que para todo automorfismo $\phi : G \rightarrow G$, $\phi(H) = H$ é equivalente a dizer que H é invariante por todos os automorfismos de G .

Todo subgrupo característico é um subgrupo normal, pois a conjugação por um elemento fixo g de G , $x \mapsto g^{-1}xg$ é um automorfismo de G . Além disso, se $\phi : G \rightarrow G$ é um automorfismo e H é um subgrupo característico de G , a restrição de ϕ a H é um automorfismo de H . Segue então que se $K \text{ char } H$ e $H \text{ char } G$, logo $K \text{ char } G$.

Proposição 10. *Seja $K \text{ char } H \triangleleft G$. Então $K \triangleleft G$.*

Demonstração. O nosso objetivo é mostrar que $\mathcal{I}_g(K) = K$, para todo $g \in G$. Seja $g \in G$ e $\mathcal{I}_g : G \rightarrow G$, $\mathcal{I}_g(x) = gxg^{-1}$. Vamos restringir $\mathcal{I}_g$ a H :

$$\begin{aligned} \mathcal{I}_g|_H : H &\longrightarrow G \\ h &\longmapsto ghg^{-1} \end{aligned}$$

A nossa hipótese é de que $H \triangleleft G$, então temos $\mathcal{I}_g|_H(H) = \mathcal{I}_g(H) = H$. Portanto $\mathcal{I}_g|_H$ é um automorfismo de H . Pela hipótese $K \text{ char } H$ e $\mathcal{I}_g|_H \in \text{Aut}(H)$, segue que

$$\mathcal{I}_g(K) = \mathcal{I}_g|_H(K) = K.$$

□

Proposição 11. *Seja $H \leq G$. 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. Como H' é o subgrupo gerado por todos os elementos da forma $[x, y]$ com $x, y \in H$, para provar a primeira afirmação basta mostrar que para todo automorfismo $\phi : G \rightarrow G$ tem-se que $\phi([x, y]) = [\phi(x), \phi(y)] \in H'$ e, como $H \text{ char } G$, segue imediatamente que $\phi([x, y]) \in H'$.

Em particular podemos tomar $H = G$ e como G é característico em G , pelo resultado G' é característico em G . Agora na proposição tomando $H = G'$ temos que $H' = G^{(2)}$ é característico em G , assim indutivamente $G^{(n)}$ é característico em G . □

Definição 28. Um subgrupo H de um grupo G é maximal com respeito à propriedade $\mathfrak{X}$ se H tem a propriedade $\mathfrak{X}$ e não há subgrupo de G maior com esta propriedade, ou seja, H é maximal $\mathfrak{X} \Leftrightarrow$ não há subgrupo N de G com a propriedade $\mathfrak{X}$ tal que $H < N < G$.

Analogamente, H é minimal $\mathfrak{X}$ se $H \neq 1$ e não há subgrupo K de G com a propriedade $\mathfrak{X}$ tal que $1 < K < H$.

A propriedade $\mathfrak{X}$ pode ser maximal ou minimal com relação à normalidade, à solubilidade, à nilpotência, entre outras.

Teorema 18.

1. H é um subgrupo normal maximal de G se, e somente se, G/H não possui subgrupos normais não triviais.
2. H é um subgrupo normal maximal de G se, e somente se, G/H é simples.
3. Em um grupo qualquer, um subgrupo normal minimal é caracteristicamente simples, ou seja, não possui subgrupos característicos próprios não triviais.

3.2 Grupos Solúveis

Definição 29. Um grupo G é dito solúvel se contém uma cadeia de subgrupos

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

tal que cada subgrupo G_{i-1} é normal em G_i e os grupos quocientes G_i/G_{i-1} , $1 \leq i \leq n$, são abelianos.

Uma cadeia de subgrupos com esta propriedade chama-se uma série subnormal abeliana de G e os quocientes respectivos chamam-se os fatores da série.

Não é imprescindível que os subgrupos G_i sejam normais em G , com $1 \leq i \leq n-1$. Quando ocorre que cada subgrupo G_i seja também normal em G , essa cadeia de subgrupos chama-se série normal abeliana de G .

Observação: Note que toda série normal é em particular uma série subnormal. No caso em que todos os fatores de uma série subnormal são simples a série é chamada *série de composição*.

Vamos citar alguns exemplos de grupos solúveis:

- Todo grupo abeliano é solúvel, onde podemos considerar uma série subnormal composta apenas pelo próprio grupo e o grupo trivial: $\{1\} \leq G$.
- O grupo S_3 é solúvel, mas não é abeliano. Se considerarmos o ciclo $\sigma = (1\ 2\ 3)$ então $H = \langle \sigma \rangle$ é cíclico de ordem 3 e $(G : H) = 2$, consequentemente $H \triangleleft S_3$. Podemos notar

que S_3/H é cíclico de ordem 2, e portanto abeliano. Logo, $\{1\} \leq H \leq G$ é uma série subnormal abeliana para S_3 .

O teorema a seguir trata de como a solubilidade pode ser caracterizada pela série derivada.

Teorema 19. *Um grupo G é solúvel se, e somente se, sua série derivada termina, ou seja, se existe um inteiro positivo n tal que $G^{(n)} = \{1\}$.*

Demonstração. Assumamos que existe um inteiro positivo n tal que $G^{(n)} = \{1\}$. Portanto, é evidente que

$$G^{(0)} \geq G^{(1)} \geq G^{(2)} \geq \dots \geq G^{(n)} = \{1\}$$

é uma série subnormal abeliana para G .

Vamos agora supor que G contém uma série subnormal abeliana

$$G = G_0 \geq G_1 \geq G_2 \geq \dots \geq G_n = \{1\}.$$

Já sabemos que todo quociente G_{i-1}/G_i , $0 \leq i \leq n-1$ é abeliano. Pelo Lema 13, sabemos que

$$G/G_1 \text{ abeliano} \Rightarrow G' \subset G^{(2)} \subset G'_1$$

deste fato e claramente pelo Lema 13, temos

$$G_1/G_2 \text{ abeliano} \Rightarrow G'_1 \subset G_2, \text{ ou seja, } G^{(2)} \subset G_2.$$

Indutivamente, podemos chegar que $G^{(i)} \subset G_i$.

□

Definição 30. *Sejam G um grupo e $N \triangleleft G$. Suponha que $N \simeq B$ e $G/N \simeq A$. Então dizemos que G é uma extensão de B por A .*

Observamos que A não é necessariamente um subgrupo de G .

Como exemplo, sejam A e B grupos cíclicos de ordem 2. Vamos obter duas extensões distintas de B por A .

- i) Consideremos $K = \{1, a, b, ab\}$ o grupo de Klein (todo elemento tem ordem 2). Temos que $|K| = 4$ e K não é cíclico. $N = \langle a \rangle = \{1, a\}$, donde $N \simeq B$, $N \triangleleft K$, $|K/N| = 2$, K/N é cíclico e $K/N \simeq A$. Logo K é extensão de B por A .
- ii) Consideremos C_4 o grupo cíclico de ordem 4: $C_4 = \{1, c, c^2, c^3\}$.

Temos: $N = \{1, c^2\}$ o subgrupo de C_4 cuja ordem é 2. Considere $N \simeq B$. Ainda, $N \triangleleft C_4$, $|C_4/N| = 2$, donde $C_4/N \simeq A$. Logo C_4 é uma extensão de B por A . Observe que em C_4 não existe outro subgrupo de ordem 2 além de N . Assim, não há um subgrupo $H \neq N$ tal que H seja isomorfo a A .

Lema 15. *Seja $H \triangleleft G$. Se H e G/H são solúveis, então G é solúvel.*

Proposição 12. *Todo p -grupo finito é solúvel.*

Demonstração. Seja G um p -grupo tal que $|G| = p^m$, $m \geq 1$. Vamos provar o resultado por indução sobre m . Se $m = 1$ então $|G| = p$ e G é abeliano, portanto solúvel. Agora, vamos considerar $m > 1$ e o resultado válido para um p -grupo J , tal que $|J| = p^k$, $m > k$.

No caso G abeliano, temos G solúvel. Já para G não abeliano, temos que $Z(G) \neq G$ e $Z(G) \neq 1$. Além disso, sabemos que $Z(G)$ é abeliano e $Z(G) \triangleleft G$, e assim podemos considerar $G/Z(G)$. Note que tais subgrupos são p -grupos cujas ordens são menores que p^m . Portanto, pela nossa hipótese de indução, ambos são solúveis. Assim, pelo Lema 15 temos que G é solúvel. $\square$

Proposição 13. *A classe dos grupos solúveis é fechada com respeito a*

- i) *Subgrupos;*
- ii) *Quocientes;*
- iii) *Extensão de seus membros.*

Demonstração. i) Sejam G solúvel e $H \leq G$. Consideremos uma série subnormal abeliana de G :

$$1 \leq H_1 \leq \dots \leq H_n = G$$

onde $H_i \triangleleft H_{i+1}$ e H_{i+1}/H_i é abeliano para todo i . Pelo Segundo Teorema do Isomorfismo

$$\frac{H \cap H_{i+1}}{H \cap H_i} \simeq \frac{(H \cap H_{i+1})H_i}{H_i} \leq \frac{H_{i+1}}{H_i}$$

que mostra que $\{H \cap H_i : i = 0, 1, \dots, n\}$ forma uma série subnormal abeliana de H , logo H é solúvel.

ii) Sejam G solúvel com a série dada anteriormente e $N \triangleleft G$. Aplicando o Segundo e o Terceiro Teorema do Isomorfismo temos,

$$\begin{aligned} \frac{H_{i+1}N/N}{H_iN/N} &\simeq \frac{H_{i+1}N}{N} && \text{3º Teorema do Isomorfismo} \\ &\simeq \frac{H_{i+1}}{H_{i+1} \cap (H_iN)} && \text{2º Teorema do Isomorfismo} \end{aligned}$$

O último é um quociente de H_{i+1}/H_i , pois pelo 3º Teorema do Isomorfismo

$$\frac{H_{i+1}}{H_{i+1} \cap (H_iN)} \simeq \frac{H_{i+1}/H_i}{(H_{i+1} \cap H_iN)/H_i}.$$

Logo, $\{H_i N/N : i = 0, 1, \dots, n\}$ forma uma série subnormal abeliana de G/N . Assim G/N é solúvel.

iii) Seja $N \triangleleft G$, N solúvel tal que G/N é solúvel. Consideremos as séries subnormais abelianas de N e G/N , respectivamente,

$$1 \leq N_1 \leq \dots \leq N_r = N$$

$$N \leq H_1 N/N \leq \dots \leq H_s N/N = G/N$$

Note que

$$1 \leq N_1 \leq \dots \leq N_r = N \leq H_1 N \leq \dots \leq H_s N = G$$

é uma série subnormal abeliana de G . □

Lema 16. *O produto de dois subgrupos normais solúveis é solúvel.*

Demonstração. Sejam $H, K \triangleleft G$, H, K solúveis. Sabemos do 2º Teorema do Isomorfismo que

$$\frac{HK}{K} \simeq \frac{H}{H \cap K}.$$

Como $H \cap K \triangleleft H$ e H é solúvel, temos que HK/K é solúvel (Quociente de solúvel é solúvel). Agora HK/K e K solúveis, implica HK solúvel (Extensão de solúvel é solúvel). □

Há uma cadeia subnormal muito interessante nos grupos solúveis finitos.

Proposição 14. *Um grupo solúvel finito G contém uma série subnormal abeliana cujos fatores são todos cíclicos de ordem prima.*

Demonstração. Usando indução sobre a ordem de G , verificamos que se $|G| = 1$ não há o que provar. Portanto, vamos supor que $|G| > 1$ com o resultado valendo para todos os grupos solúveis de ordem menor que n , que é a ordem de G . Se $|G|$ é um número primo, o resultado é trivial uma vez que $\{1\} \leq G$ é uma série subnormal abeliana para G . Mas se G é solúvel e não possui ordem de número primo, ele contém pelo menos um subgrupo normal H . Como a $|H|$ e $|G/H|$ são menores do que n , pela hipótese de indução, os dois grupos tem séries subnormais abelianas com fatores cíclicos.

Chamando $\overline{G} = G/H$, tomemos as séries

$$\begin{aligned} \{1\} &= H_0 \triangleleft H_1 \triangleleft \dots \triangleleft H_m = H \\ \{1\} &= \overline{G}_0 \triangleleft \overline{G}_1 \triangleleft \dots \triangleleft \overline{G}_n = \overline{G} \end{aligned}$$

que são subnormais abelianas, e possuem fatores cíclicos, para H e $\overline{G}$. Há subgrupos G_i de G que contém H tais que $G_i/H = \overline{G}_i$, e $G_{i-1} \triangleleft G_i$, $1 \leq i \leq n$. Uma vez que

$$\frac{\overline{G}_i}{\overline{G}_{i-1}} = \frac{G_i/H}{G_{i-1}/H} \simeq \frac{G_i}{G_{i-1}}$$

podemos ver que a série de subgrupos é uma série subnormal abeliana em G , com fatores cíclicos, onde

$$\{1\} = H_0 \triangleleft H_1 \triangleleft \dots \triangleleft H_m = H = G_0 \triangleleft G_1 \triangleleft \dots \triangleleft G_n = G.$$

□

Proposição 15. *Se G é um grupo finito, então todo subgrupo normal minimal solúvel é um p -grupo abeliano elementar, ou seja, todo elemento deste subgrupo tem ordem p .*

Demonstração. Sejam G finito e M subgrupo normal minimal solúvel de G . Como M é solúvel, $M^{(d)} = 1$ para algum d . Assim $M' \neq M$. Sendo M normal minimal, M não possui subgrupo característico não trivial (caracteristicamente simples). Como M' char M segue que $M' = 1$. Assim, M é abeliano. Seja P um p -Sylow subgrupo de M , como M é abeliano (todos subgrupos são normais), P é o único p -sylow subgrupo de M , logo P char M . Assim, P char M e $M \triangleleft G \Rightarrow P \triangleleft G$. Logo, pela minimalidade de M temos que $M = P$. Agora, notemos que $\{x \in M; x^p = 1\}$ é característico em M . Portanto, M é abeliano elementar. □

Corolário 10. *Se G é um grupo solúvel finito, então todo subgrupo normal minimal é abeliano elementar.*

Proposição 16. *Sejam G um grupo solúvel finito e H um subgrupo maximal. Então $(G : H)$ é uma potência de um primo.*

Demonstração. Usaremos indução sobre a ordem de G .

Se $|G| = 1$, não há o que fazer. Suponha então que $|G| \neq 1$ e que o resultado é verdadeiro para todos os grupos com ordens menores que $|G|$. Seja N um subgrupo normal minimal de G e seja H um maximal qualquer. Devemos avaliar dois casos:

i) $N \leq H$

Temos G/H é solúvel e de ordem menor do que $|G|$ e H/N é subgrupo maximal de G/N . Por hipótese de indução $(G/N : H/N) = p^m \simeq G/H$ (3º Teorema do Isomorfismo). Isto nos dá que $(G : H) = p^m$.

ii) $N \not\leq H$

Vimos que N normal minimal em G , N solúvel e G finito, implica que N é abeliano elementar. Assim, $|N| = p^k$. Temos que $G = NH$, pois $N \not\leq H$ e H é maximal. Logo, $(G : H) = (NH : H) = (N : H \cap N)$, que divide $|N|$ e, assim, é uma potência de p . □

Vamos apresentar agora uma coleção de resultados que garantem a solubilidade de alguns grupos de acordo com a sua ordem.

Teorema 20. *Valem os seguintes resultados:*

- (i) *Se p, q e r são primos, então todos os grupos de ordens $p^m, p^m q, p^2 q^2, pqr$ são solúveis.*
- (ii) *(Teorema de Burnside - 1904) Todo grupo de ordem $p^m q^n$, p e q primos, é solúvel.*
- (iii) *(W. Feit & J. Thompson - 1963) Todo grupo de ordem ímpar é solúvel.*

A demonstração do resultado (i) pode ser encontrada em [6].

CAPÍTULO 4

GRUPOS NILPOTENTES

Os grupos nilpotentes estão, de certa forma, entre os grupos abelianos e os grupos solúveis. No entanto, como veremos a seguir, as condições exigidas na definição de nilpotência são claramente mais exigentes do que aquelas que aparecem na definição de grupo solúvel.

Definição 31. Um grupo G diz-se nilpotente se ele contém uma série de subgrupos

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

tal que cada subgrupo G_{i-1} é normal em G e cada quociente G_i/G_{i-1} está contido no centro de G/G_{i-1} , $1 \leq i \leq n$. Essa série de subgrupos é chamada de uma série central de G .

Uma observação pertinente é que todo grupo nilpotente tem centro não trivial, pois pela definição $G_i/G_{i-1} \subset Z(G/G_{i-1}) \forall i$. Em particular, se tomarmos $i = 1$ tem-se

$$G_1/G_0 \subset Z(G/G_0) \quad (*)$$

mas $G_0 = \{1\}$, então $G_1/G_0 \approx G_1$ e $G/G_0 \approx G$, ou seja, reescrevendo $(*)$ fica $G_1 \subset Z(G)$. Mas se $G_1 = \{1\}$, logo $G_2 \subset Z(G)$. E isso acontece de forma sucessiva, até chegar em algum subgrupo de G não trivial. Esse subgrupo existe pois a série alcança G . Como exemplo dessa observação temos o S_3 , que já mostramos em outra seção ser um grupo solúvel, mas não é um nilpotente uma vez que o seu centro é trivial.

Note que com essa definição obviamente todo grupo abeliano é nilpotente, e todo grupo nilpotente é solúvel. Pois se cada $G_i/G_{i-1} \subset Z(G/G_{i-1})$ então, em particular, cada elemento de G_i/G_{i-1} comuta entre si, logo esses grupos quocientes são abelianos. Se o grupo é nilpotente cada subgrupo $G_{i-1} \triangleleft G$, consequentemente $G_i \triangleleft G_{i+1}$.

Explorando as ligações entre nilpotência e alguns comutadores, segue duas possíveis caracterizações dos grupos nilpotentes. Para tanto, estabelecemos uma nova série de subgrupos em G :

$$\gamma_1(G) = G, \gamma_2 = [G, G], \gamma_3 = [\gamma_2(G), G] \text{ e } \gamma_i(G) = [\gamma_{i-1}(G), G].$$

Obviamente temos que $\gamma_1(G) = G \triangleleft G$ e que $\gamma_2(G) = [\gamma_1(G), G] = [G, G] = G' \trianglelefteq G$. Seguindo por indução e usando o Teorema 17 é fácil ver $\gamma_n(G) \trianglelefteq G$ para todo $n \in \mathbb{N}$. Pelo fato de $\gamma_n(G) \trianglelefteq G$ podemos usar o Lema 14 para justificar que $\gamma_{n+1}(G) \subseteq \gamma_n(G)$ para todo $n \in \mathbb{N}$.

Definiremos uma outra série a ser levada em consideração, fundamentada no conceito de centro de um grupo. Designando $\zeta_0(G) = \{1\}$ e $\zeta_1(G) = Z(G)$. Considerando o grupo quociente $G/\zeta_1(G)$, é possível mostrar (usando o Teorema da Correspondência) que existe um subgrupo $\zeta_2(G)$ de G tal que $Z(G/\zeta_1(G)) = \zeta_2(G)/\zeta_1(G)$. Como $\zeta_2(G)/\zeta_1(G) = Z(G/\zeta_1(G)) \trianglelefteq G/\zeta_1(G)$ segue que $\zeta_2(G) \trianglelefteq G$. Nos referimos a $\zeta_2(G)$ como sendo o 2º centro de G . Ao considerarmos o grupo quociente $G/\zeta_2(G)$, temos que existe $\zeta_3(G)$ subgrupo normal em G tal que $Z(G/\zeta_2(G)) = \zeta_3(G)/\zeta_2(G)$. $\zeta_3(G)$ é referido como sendo o 3º centro de G . Seguindo indutivamente, uma vez já definido o subgrupo $\zeta_i(G)$, que é normal em G , definimos $\zeta_{i+1}(G)$ como sendo o subgrupo de normal de G , tal que $Z(G/\zeta_i(G)) = \zeta_{i+1}(G)/\zeta_i(G)$. O subgrupo $\zeta_i(G)$ é chamado de *i-ésimo centro* de G .

Definição 32. *As sequências de subgrupos*

$$\begin{aligned} \{1\} = \zeta_0(G) &\leq \zeta_1(G) \leq \dots \leq \zeta_n(G) \leq \dots \\ &e \\ G = \gamma_1(G) &\geq \gamma_2(G) \geq \dots \geq \gamma_n(G) \geq \dots \end{aligned}$$

chamam-se a série central superior e a série central inferior de G , respectivamente.

Os seguintes lemas nos mostram porque são denominadas assim. Estas séries também são chamadas de série central ascendente e série central descendente.

Lema 17. *Seja $\{1\} = A_0 \leq A_1 \leq \dots \leq A_n \dots$ uma série central de G (uma cadeia de subgrupos normais tal que $A_i/A_{i-1} \subset Z(G/A_{i-1})$ para todo i). Então $A_i \subset \zeta_i(G)$ para todo i .*

Demonstração. Usando indução em i , o resultado é trivial se $i = 0$. Tomemos como hipótese de indução que $A_i \subset \zeta_i(G)$. Dados $x \in A_{i+1}$ e $g \in G$, como $A_{i+1}/A_i \subset Z(G/A_i)$ temos que $[x, g] \in A_i \subset \zeta_i(G)$. Assim, pela definição de $\zeta_{i+1}(G)$ temos que $A_{i+1} \subset \zeta_{i+1}(G)$. $\square$

Lema 18. *Seja $\{1\} = A_0 \leq A_1 \leq \dots \leq A_n = G$ uma série central de G . Então $\gamma_i(G) \subset A_{n-i+1}$, para todo i .*

Demonstração. Usando indução em i , o resultado é trivial se $i = 0$. Tomemos como hipótese de indução que $\gamma_i(G) \subset A_{n-i+1}$. Como A_{n-i+1}/A_{n-i} está em $Z(G/A_{n-i})$, temos que $[A_{n-i+1}, G] \subset A_{n-i}$. Assim, $\gamma_{i+1} = [\gamma_i(G), G] \subset [A_{n-i+1}, G] \subset A_{n-i}$. $\square$

Os resultados a seguir destacam a importância dessas duas séries centrais na caracterização de nilpotência de um grupo.

Teorema 21. *Seja G um grupo. São equivalentes:*

- (i) G é nilpotente.
- (ii) Existe um inteiro positivo m tal que $\zeta_m(G) = G$.
- (iii) Existe um inteiro positivo n tal que $\gamma_n = \{1\}$.

A classe de nilpotência de um grupo nilpotente é o comprimento que as suas séries centrais superior e inferior têm. Pelos lemas 17 e 18 fica evidente que elas possuem o mesmo tamanho.

Definição 33. *Seja G um grupo nilpotente. Definimos a classe de nilpotência de G , denotada por $cl(G)$, como sendo*

$$cl(G) = \min\{n \in \mathbb{N} | \zeta_n(G) = G\} = \min\{m \in \mathbb{N} | \gamma_{m+1}(G) = \{1\}\}.$$

Podemos observar que os grupos abelianos têm classe de nilpotência igual a 1. Sendo G um grupo, é fato que G é abeliano se, e somente se, $\{1\} = G' = \gamma_2(G)$. Assim, $cl(G) = 1$.

Proposição 17. *Seja G um grupo nilpotente. Então valem:*

- (i) *Todo subgrupo de G é nilpotente e tem classe de nilpotência menor ou igual a $cl(G)$.*
- (ii) *Todo grupo quociente de G é nilpotente e tem classe de nilpotência menor ou igual a $cl(G)$.*

A proposição a seguir trata da nilpotência dos p -grupos finitos.

Proposição 18. *Todo p -grupo finito é nilpotente.*

Demonstração. Seja N um subgrupo normal próprio de G , logo G/N é um p -grupo não trivial. Uma vez que G/N é um p -grupo, o $Z(G/N)$ tem ordem divisível por p e assim existe $H \leq G$, com $N \subseteq H$, onde $H/N \leq Z(G/N)$ de ordem p . Como $H/N \subseteq Z(G/N)$, temos que $H/N \trianglelefteq G/N$, implicando que $H \trianglelefteq G$. Podemos também notar que $|H| = p|N|$.

Se $|G| = p$, não precisa ser feito nada. Suponhamos que $|G| = p^n$, com $n > 1$. Como $Z(G)$ tem ordem divisível por p , existe $N_1 \leq G$ tal que $N_1 \subseteq Z(G)$ e $|N_1| = p$. Por $N_1 \subseteq Z(G)$ temos que $N_1 \trianglelefteq G$. Logo, existe $N_2 \trianglelefteq G$, com $N_1 \subseteq N_2$ tal que $N_2/N_1 \subseteq Z(G/N_1)$ e $|N_2| = p|N_1|$. Se $N_2 = G$, vemos que a série $\{1\} = N_0 \leq N_1 \leq N_2 = G$ é uma série central de subgrupos de G , sendo G um grupo nilpotente. Se $N_2 \subsetneq G$ podemos encontrar um subgrupo $N_3 \trianglelefteq G$, tal que $N_2 \subseteq N_3$, $N_3/N_2 \subseteq Z(G/N_2)$ e $|N_3| = p|N_2|$, seguindo indutivamente pode-se concluir que existe um série central de subgrupos de G do tipo $\{1\} = N_0 \leq N_1 \leq N_2 \leq N_3 \leq \dots \leq N_k \leq N_{k+1} \leq \dots$ de forma que $|N_{k+1}| = p|N_k|$. Como $|G| = p^n$ e $|N_0| = 1$, temos que $N_n = G$, o que implica que G é nilpotente. $\square$

Proposição 19. *Produtos diretos finitos de grupos nilpotentes são também nilpotentes.*

Já vimos que o centro de um grupo nilpotente não é trivial. Veremos agora que ele na verdade intercepta todos os subgrupos normais do grupo.

Proposição 20. *Seja $H \neq \{1\}$ um subgrupo normal de um grupo nilpotente G . Então $H \cap Z(G) \neq \{1\}$*

Demonstração. Como $G = \zeta_n(G)$ para algum índice n , existe um índice i que é o menor inteiro positivo tal que $H \cap \zeta_i(G) \neq \{1\}$. Então $[H \cap \zeta_i(G), G] \subset H \cap \zeta_{i-1}(G) = \{1\}$ logo $H \cap \zeta_i(G) \subset H \cap Z(G)$. $\square$

Corolário 11. *Um subgrupo normal minimal de um grupo nilpotente está contido no centro.*

A proposição a seguir trata de uma importante propriedade para descrever a estrutura dos grupos nilpotentes.

Proposição 21. *Seja H um subgrupo próprio de um grupo nilpotente. Então $H \subsetneq N_G(H)$.*

Demonstração. Como $\{1\} = \zeta_0(G) \leq H \leq \zeta_n(G) = G$, existe um inteiro positivo i tal que $\zeta_i(G) \subset H$ e $\zeta_{i+1}(G) \not\subset H$. Escolhemos um elemento $x \in \zeta_{i+1}(G) \setminus H$ e um elemento arbitrário $h \in H$. Como $[\zeta_{i+1}(G), G] \subset \zeta_i(G)$ temos que existe um elemento $y \in \zeta_i(G) \subset H$ tal que $xhx^{-1} = hy \in H$, logo $xHx^{-1} \subset H$ e portanto $x \in N_G(H)$, o que mostra que $H \subsetneq N_G(H)$. $\square$

Definição 34. *Diz-se que um grupo G tem a propriedade do normalizador se todo subgrupo próprio de G está estritamente contido no seu normalizador.*

O corolário seguinte é uma consequência imediata dessa definição.

Corolário 12. *Todo subgrupo maximal de um grupo nilpotente é normal.*

Demonstração. Seja H um subgrupo maximal de G , sendo então um subgrupo próprio de G . Pela proposição 21, $H \subsetneq N_G(H)$ e segue da maximalidade de H que $N_G(H) = G$. Assim, $H \trianglelefteq G$. $\square$

4.1 Grupos Nilpotentes Finitos

Os resultados a seguir discorrem sobre a caracterização dos grupos nilpotentes finitos.

Já vimos que um subgrupo H de um grupo G diz-se *subnormal* se existe uma cadeia de subgrupos:

$$H = H_0 \leq H_1 \leq \dots \leq H_n = G$$

tal que $H_{i-1} \triangleleft H_i$, $1 \leq i \leq n$.

Por conseguinte, temos o corolário.

Corolário 13. *Seja G um grupo nilpotente finito. Então, todo subgrupo de G é subnormal.*

Demonstração. Seja H um subgrupo de G . Definimos $H_0 = H$, e indutivamente, $H_n = N_G(H_{n-1})$. Da proposição anterior segue que se $H_{n-1} \neq G$ então $|H_{n-1}| < |H_n|$. Como G é finito, deve existir um índice n tal que $H_n = G$. $\square$

Teorema 22. *Seja G um grupo finito. Então, as seguintes condições são equivalentes.*

- (i) G é nilpotente.
- (ii) G tem a propriedade do normalizador.
- (iii) Todo subgrupo de Sylow de G é normal em G .
- (iv) G é o produto direto dos seus subgrupos de Sylow.
- (v) Todo subgrupo de G é subnormal.
- (vi) Todo subgrupo maximal de G é normal.

Demonstração. Podemos começar provando que $(i) \Rightarrow (ii) \Rightarrow (iii) \Rightarrow (iv) \Rightarrow (i)$. Mas $(i) \Rightarrow (ii)$ foi demonstrado na proposição 21.

$(ii) \Rightarrow (iii)$ Seja P um p -subgrupo de Sylow de G e seja $H = N_G(P)$. Se $H \neq G$ então (ii) implica que $H \subsetneq N_G(H)$, mas se P é um p -subgrupo de Sylow de um grupo G o $N_G(N_G(P)) = N_G(P)$. Daí $H = N_G(H)$ e $H = G$, donde $P \triangleleft G$.

$(iii) \Rightarrow (iv)$ Se cada subgrupo de Sylow é normal, segue imediatamente que o seu produto é direto e igual a G .

$(iv) \Rightarrow (i)$ Como todo p -grupo é nilpotente, temos que produtos diretos finitos de grupos nilpotentes são também nilpotentes.

Agora demonstraremos que $(i) \Rightarrow (v) \Rightarrow (vi) \Rightarrow (i)$.

$(i) \Rightarrow (v)$ segue do Corolário 13. Se a condição (v) é verdadeira e H é maximal, é imediato que ele é normal ficando óbvio $(v) \Rightarrow (vi)$.

Para demonstrar que $(vi) \Rightarrow (i)$ provaremos que se a condição (vi) é verdadeira então todo subgrupo de Sylow de G é normal, o que mostra que G é nilpotente. De fato, seja P um subgrupo de Sylow de G . Se $N_G(P)$ é um subgrupo próprio de G , ele deve estar contido num subgrupo maximal H de G que, em virtude da hipótese (vi) é normal. Assim, $N_G(H) = G$ e isso contradiz o seguinte resultado: "Seja P um p -subgrupo de Sylow de um grupo G e seja H um outro subgrupo. Se $N_G(P) \subset H$ então $H = N_G(H)$ ". $\square$

Pode-se notar que o teorema que acabamos de ver demonstra que se G é um grupo nilpotente de ordem $|G| = p_1^{n_1} \cdots p_t^{n_t}$, aonde denotaremos por $S(p_i)$, $1 \leq i \leq t$ os p_i -subgrupos de Sylow, temos que $G = S(p_1) \times \cdots \times S(p_t)$. Esse resultado é uma generalização do seguinte teorema que se refere aos grupos abelianos.

Teorema 23. *Seja G um grupo finito abeliano de ordem $|G| = p_1^{n_1} \cdots p_t^{n_t}$. Então*

$$G = G(p_1) \times \cdots \times G(p_t).$$

REFERÊNCIAS BIBLIOGRÁFICAS

- [1] ASSIS, E. H. Sobre grupos solúveis finitos, 2015.
- [2] DOMINGUES, HYGINO H. E IEZZI, G. *Álgebra Moderna*, 4ª edição ed. 2003.
- [3] GARCIA, ARNALDO E LEQUAIN, Y. *Elementos de Álgebra*. 2018.
- [4] HERSTEIN, I. N. *Topics in Algebra*. 1964.
- [5] MILIES, C. P. Grupos nilpotentes: Uma introdução. *MATEMÁTICA UNIVERSITÁRIA* (2003).
- [6] ROBINSON, D. J. S. *A Course in the Theory of Groups*, 2ª edition ed. 1995.
- [7] SILVA, T. F. Nilpotência e p-nilpotência de grupos finitos, 2015.
- [8] SOUZA, J. A. Uma nota sobre a teoria dos grupos: da teoria de galois à teoria de gauge. *Revista Brasileira de História da Matemática* 12, 24 (out. 2020), 71–81.