UNIVERSIDADE ESTADUAL DA PARAÍBA
CAMPUS I
CENTRO DE CIÊNCIAS E TECNOLOGIA
CURSO DE LICENCIATURA EM MATEMÁTICA

ANALISANDO OS HOMOMORFISMOS DE $\mathbb{Z}_m$ EM $\mathbb{Z}_n$

JAMERSON GUSTAVO LAURENTINO SANTOS

CAMPINA GRANDE
2018

JAMERSON GUSTAVO LAURENTINO SANTOS

ANALISANDO OS HOMOMORFISMOS DE $\mathbb{Z}_m$ EM $\mathbb{Z}_n$

Trabalho de Conclusão de Curso apresentado ao Departamento de Matemática da Universidade Estadual da Paraíba em cumprimento às exigências para obtenção do título de Licenciado em Matemática.

Orientadora: Prof[a]. Dr[a]. Emanuela Régia de Sousa Coelho

CAMPINA GRANDE

2018

S237a Santos, Jamerson Gustavo Laurentino.
Analisando os homomorfismos de Zm em Zn [manuscrito] / Jamerson Gustavo Laurentino Santos. - 2018.
41 p.
Digitado.
Trabalho de Conclusão de Curso (Graduação em Matemática) - Universidade Estadual da Paraíba, Centro de Ciências e Tecnologia , 2018.
"Orientação : Profa. Dra. Emanuela Régia de Sousa Coelho , Coordenação do Curso de Matemática - CCT."
1. Teoria dos números. 2. Homomorfismo. 3. Teoria de grupos. I. Título
21. ed. CDD 512.72

Elaborada por Giulianne M. Pereira - CRB - 15/714 BC/UEPB

JAMERSON GUSTAVO LAURENTINO SANTOS

ANALISANDO OS HOMOMORFISMOS DE $\mathbb{Z}_m$ EM $\mathbb{Z}_n$

Trabalho de Conclusão de Curso apresentado ao Departamento de Matemática da Universidade Estadual da Paraíba em cumprimento as exigências para obtenção do título de Licenciado em Matemática.

Aprovado em: 03/12/2018.

BANCA EXAMINADORA

Profa. Dra. Emanuela Régia de Sousa Coelho (Orientadora)
Universidade Estadual da Paraíba (UEPB)

Prof. Dr. Israel Burití Galvão
Universidade Estadual da Paraíba (UEPB)

Prof. Mc. José Ginaldo de Souza Farias
Universidade Estadual da Paraíba (UEPB - Campus VII)

Dedicatória

À minha querida família,
DEDICO.

Agradecimentos

Agradeço primeiramente a Deus pela minha vida, caso contrário eu não estaria aqui realizando tal conquista. Agradeço aos meus familiares, em especial à minha mãe Geovana Laurentino que infelizmente não está mais entre nós, mas sempre fez de tudo para que eu pudesse chegar até aqui. Ao meu pai, Cristiano Alves, que também teve sua parcela de contribuição. As minhas irmãs, Ketyane Laurentino e Kelyane Laurentino, pelo auxílio durante a realização deste. Não podendo esquecer da minha noiva, Nayara Diniz, pelo apoio e incentivo nos dias de maior dificuldade.

Agradeço a todos os meus amigos e colegas que estiveram presentes durante minha graduação, por todos os momentos descontraídos que serviram para minimizar a pressão e a responsabilidade do curso. Para não correr o risco de esquecer alguém optei por não mencionar vossos nomes. Todavia o apreço é o mesmo por todos, além do mais, quem esteve comigo saberá da minha gratidão para com eles.

Agradeço a toda equipe do departamento de matemática da UEPB, a todos os professores em que tive o prazer de ser aluno, pois foram muito importantes para a minha formação, sou grato por todos os ensinamentos e em especial a minha orientadora Emanuela Régia pelo apoio grandioso para realização deste trabalho.

Resumo

O presente trabalho tem como objetivo realizar um estudo sobre homomorfismo entre os grupos $\mathbb{Z}_m$ e $\mathbb{Z}_n$, com m,n $\in \mathbb{Z}$. Especificamente, apresentamos a quantidade de homomorfismos existentes entre esses dois grupos, a partir da ordem deles. Para isso utilizaremos alguns dos principais conceitos e resultados da teoria elementar dos números, da teoria de grupos, subgrupos e grupos ciclícos.

Palavras-chave: Teoria dos Números. Homomorfismo. Teoria de grupos.

Abstract

The present work aims to perform a study on homomorphism between the groups of $\mathbb{Z}_m$ in $\mathbb{Z}_n$. Specifically, we present the amount of homomorphisms existing between these two groups, from their order. To do this, we will use some of the main concepts and results of elementary theory of numbers, group theory, subgroups and cyclic groups.

Keywords: Theory of Numbers. Homomorphism. Group Theory.

Sumário

Introdução

A palavra álgebra é derivada da palavra árabe al-jabr. Ainda que originalmente *álgebra* se refira a equações, a palavra hoje tem um significado amplo e uma definição requer um enfoque em duas fases: (1) álgebra elementar e (2) álgebra abstrata. A álgebra elementar é o estudo das equações e métodos de resolvê-las. A álgebra abstrata é o estudo das estruturas matemáticas tais como grupos, anéis e corpos. É exatamente nessa segunda fase que o nosso tema, homomorfismo de grupos, é encontrado.

Sejam $(G_1, *)$ e $(G_2, .)$ dois grupos. Uma função $f : G_1 \to G_2$ chama-se homomorfismo de G_1 em $G2$ quando:

$$f(a * b) = f(a).f(b) \text{ para todo } a, b \in G_1.$$

No presente trabalho iremos apresentar o resultado de homomorfismo de grupos que afirma que o número de homomorfismos de grupos de $\mathbb{Z}_m$ em $\mathbb{Z}_n$ é igual ao $\text{mdc}(m, n)$, em que $\mathbb{Z}_n$ é o conjunto das classes de equivalência módulo n, $n \in \mathbb{N}$, $n > 1$. Para provar esse resultado, seguimos o que foi feito por Joseph A. Gallan e James Van Buskirk. [7].

Esse trabalho está organizado da seguinte maneira: No Capítulo 1, apresentamos um pouco da evolução da Teoria de Grupos, a partir de [9]; No Capítulo 2, apresentaremos conceitos e resultados que irão nos auxiliar para a prova do resultado do Teorema principal do nosso trabalho: trataremos do estudo de teoria dos números, grupos, subgrupos, grupos cíclicos e homomorfismo de grupos. Todos os resultados apresentados nesse capítulo podem ser encontrados em livros clássicos de Álgebra Abstrata e Teoria dos Números, mas nossa abordagem segue os referenciados nesse texto. Na última parte, Capítulo 3, apresentaremos a prova do teorema citado anteriormente e algumas consequências diretas do mesmo.

Capítulo 1

Contexto Histórico da Teoria de Grupos

Conhecer um pouco do histórico de evolução de determinado assunto é um bom caminho para tentar entender como aqueles que foram pioneiros enveredaram por certa direção. Pensando nisso, neste primeiro capítulo apresentamos um pouco da evolução da Teoria de Grupos, seguindo o que foi feito por Kleiner em [9].

1.1 Principais fontes

Nesse tópico delinearemos três fontes principais na evolução da teoria dos grupos. A primeira fonte (álgebra clássica) levou à teoria dos grupos de permutação; a segunda (teoria dos números) levou à teoria dos grupos abelianos; a terceira (geometria) levou à teoria dos grupos de transformação.

(I) - Algebra Clássica (J. L. Lagrange, 1770)

Em 1770, Lagrange escreveu em seu livro *"Reflexions sur la resolution algebrique des equations"* problemas que diziam respeito às equações polinomiais. Havia questões teóricas que lidavam com a existência e a natureza das raízes (por exemplo: Todas as equações têm uma raiz? Quantas raízes existem? Elas são reais, complexas, positivas, negativas?) E questões práticas relacionadas a métodos para encontrar as raízes. No último caso, haviam métodos exatos e métodos aproximados.

Um dos principais problemas para os dois séculos seguintes foi a solução algébrica do quântico. Esta foi a tarefa que Lagrange estabeleceu para si mesmo em seu artigo. No

texto, Lagrange analisa os vários métodos conhecidos (criados por F. Viete, R.Descartes, L. Euler e E. Bezout) para resolver equações cúbicas e quárticas. Ele mostra que a característica comum desses métodos é a redução de tais equações em equações auxiliares - as chamadas equações de resolução. Estas últimas possuiam graus menores que as equações originais.

O trabalho de Lagrange foi um marco, apesar de ele não ter conseguido resolver o problema da solvibilidade algébrica do quântico. Foi a primeira vez que foi feita uma associação entre as soluções de uma equação polinomial e as permutações de suas raízes. De fato, o estudo das permutações das raízes de uma equação foi um dos fundamentos da teoria geral de equações algébricas de Lagrange.

(II) - Teoria dos números (C. F. Gauss, 1801)

Gauss resumiu e unificou grande parte da teoria dos números em 1801 nos *Disquisitiones Arithmeticae*. O trabalho também sugeriu novas direções que mantiveram os matemáticos ocupados por todo o século. Pode-se dizer que os Disquisitiones Arithmeticae iniciaram a teoria de grupos abelianos infinitos. De fato, Gauss estabeleceu muitas das propriedades significativas desses grupos sem usar qualquer terminologia da teoria dos grupos. Os grupos aparecem em quatro formas diferentes. O grupo aditivo de inteiros módulo m; o grupo multiplicativo de inteiros relativamente primos a m módulo m; o grupo de classes de equivalência de formas quadráticas binárias e o grupo de enésimas raízes de unidade.

Por exemplo, considerando os inteiros diferentes de zero módulo p (p um primo), Gauss mostra que eles são todos potências de um único elemento; isto é, que o grupo $\mathbb{Z}^p$, de tais inteiros, é cíclico. Além disso, determina o número de geradores desse grupo (ele mostra que é igual a $\varphi(p-1)$, onde φ é a função de Euler). Dado qualquer elemento de $\mathbb{Z}^p$, ele define a ordem do elemento (sem usar a terminologia) e mostra que a ordem de um elemento é um divisor de $p-1$. Em seguida, ele mostra que se t é um inteiro positivo que divide $p-1$, então existe um elemento em $\mathbb{Z}^p$ cuja ordem é essencialmente o inverso do teorema de Lagrange para grupos cíclicos.

Embora os argumentos nos Disquisitiones Arithmeticae sejam bastante gerais, cada um dos vários tipos de grupos que ele considera é tratado separadamente.

(III) - Geometria (F. Klein, 1872)

Agora, vamos nos referir a palestra de Klein que ele proferiu em 1872, intitulada

A Comparative Review of Recent Researches in Geometry. Essa palestra tinha como objetivo a classificação da geometria como o estudo de invariantes sob vários grupos de transformações. Aqui aparecem grupos como o grupo projetivo, o grupo de movimentos rígidos, o grupo de semelhanças, o grupo hiperbólico, os grupos elípticos, bem como as geometrias associadas a eles.

O foco da geometria mudou para um estudo das próprias transformações. Assim, o estudo das relações geométricas das figuras tornou-se o estudo das transformações associadas. Vários tipos de transformações (por exemplo: colineações, transformações circulares, transformações inversas, afinidades) tornaram-se objetos de estudos especializados. Posteriormente, as conexões lógicas entre as transformações foram investigadas, e isso levou ao problema de classificar as transformações e, eventualmente, a síntese teórica da geometria de grupo de Klein. O uso de grupos de Klein na geometria foi o estágio final em trazer ordem à geometria. Um estágio intermediário foi a fundação da primeira grande teoria de classificação em geometria, começando em 1850, a Teoria Invariante de Cayley-Sylvester. Aqui o objetivo era estudar invariantes de formas sob transformações de suas variáveis.

1.2 Expansão dos desenvolvimentos na Teoria de Grupos

A teoria dos grupos evoluiu a partir de várias fontes diferentes, dando origem a várias teorias concretas. Essas teorias se desenvolveram de formas independentes. Algumas por mais de cem anos (começando em 1770) antes de convergirem (início da década de 1880) dentro do conceito de grupo abstrato. A teoria abstrata de grupos surgiu e se consolidou nos próximos quarenta anos. No final desse período, (por volta de 1920), pode-se discernir a divergência da teoria dos grupos em várias "teorias"distintas. Vamos citar alguns desses avanços e novas direções na teoria dos grupos, começando na década de 1920:

(i) Teoria dos grupos finitos - O principal problema aqui, já formulado por Cayley (1870) e estudado por Jordan e Hblder, era encontrar todos os grupos finitos de uma determinada ordem. O problema se mostrou muito difícil e os matemáticos recorreram a casos especiais (sugeridos especialmente pela teoria de Galois): encontrar todos os grupos simples ou todos os solucionáveis (cf. o teorema de Feit-Thompson de 1963 e a classificação de todos os grupos finitos simples em 1981).

(ii) Extensões de certos resultados da teoria dos grupos finitos para grupos infinitos com condições de finitude- Por exemplo a Prova, de J. Schmidt, em 1928, do teorema de Remak-Krull-Schmidt.

(iii) Apresentações em grupo (Teoria do Grupo Combinatório)- Iniciada por von Dyck em 1882, e continuada no século XX por M. Dehn, H. Tietze, J. Nielsen, E. Artin, 0. Schreier, et al. Para uma conta completa.

(iv) Teoria dos grupos abelianos infinitos- (H. Priufer, R.Baer, H. Ulm et al.-1920 a 1930).

(v) A teoria das extensões de grupo de Schreier (1926) - levando depois à cohomologia dos grupos.

(vi) Grupos algébricos - (A. Borel, C. Chevalley et al.-1940).

(vii) Grupos topológicos - incluindo a extensão da teoria de representação de grupos a grupos contínuos (Schreier, E. Cartan, L. Pontrjagin, I. Gelfand, J. von Neumann et ai., 1920 e 1930).

Capítulo 2

Preliminares

Neste capítulo serão apresentadas definições e resultados necessários na demonstração do teorema principal do trabalho.

2.1 Teoria dos números

O resultado principal deste trabalho trata de analisar os homomorfismos existentes entre os grupos $(\mathbb{Z}_m,+)$ e $(\mathbb{Z}_n,+)$. Por isto, nesta seção, apresentamos o conjunto $\mathbb{Z}_n$, que é, em verdade, um conjunto de classes de equivalência e é estudado através da teoria dos números, parte da matemática que se dedica ao estudo dos números inteiros.

Começaremos nosso texto apresentando o conceito da relação de equivalência.

Definição 2.1. *(Relação de Equivalência) Dizemos que uma relação R sobre um conjunto A é de equivalência quando ela é:*

i) *Reflexiva, ou seja, aRa, para todo $a \in A$;*

ii) *simétrica, ou seja, se aRb, então bRa, para todo $a, b \in A$;*

iii) *Transitiva, isto é, se aRb e bRc então aRc, para todo $a, b, c \in A$.*

Quando R é uma relação de equivalência em um conjunto A e a $\in$ A, o conjunto $\overline{a}$ é composto por todos $x \in$ A tal que x se relaciona com a , ou seja,

$$\overline{a} = \{x \in A; xRa\}.$$

Observação 2.1. *Segue da definição de relação de equivalência sobre um conjunto A que:*

- $A = \cup_{a \in A} \overline{a}$.

- *Uma e somente uma das situações acontece, para* $a, b \in A$*:*

$$\overline{a} = \overline{b} \text{ } ou \text{ } \overline{a} \cap \overline{b} = \emptyset.$$

Para o desenvolvimento do nosso trabalho, iremos utilizar uma relação de equivalência em especial, chamada de congruência módulo n.

Ou seja, R dá origem a uma partição de A.

Definição 2.2. *(Divisibilidade) Dizemos que a divide b, em símbolos* $a|b$*, se existir um número c, com* $c \in \mathbb{Z}$*, tal que:*

$$b = a \cdot c$$

Definição 2.3. *Sejam* $a, b, n \in \mathbb{Z}$ *e n>1. Dizemos que a é congruente a b módulo n se* $n|(a-b)$*, ou seja,*

$$a \equiv b(\text{mod } n) \Leftrightarrow n|(a-b)$$

Exemplo 2.1. $5 \equiv 2(\text{mod } 3)$ e $-1 \equiv 13(\text{mod } 7)$.

Solução: Por definição, temos que

$$5 \equiv 2(\text{mod } 3) \Leftrightarrow 3|(5-2) \Leftrightarrow 5-2 = 3k, \text{ para algum } k \in \mathbb{Z}.$$

Como $5 - 2 = 3 = 3.1$, então $5 \equiv 2(\text{mod } 3)$. Também temos

$$-1 \equiv 13(\text{mod } 7),$$

pois $-1 - 13 = -14$.

Proposição 2.1. *A congruência módulo n(* $\equiv (\text{mod } n)$*) é uma relação de equivalência.*

Prova. Para provarmos que a congruência modúlo n é uma relação de equivalência, temos que mostrar que ela é reflexiva, simétrica e transitiva.

Reflexiva: Para qualquer a $\in \mathbb{Z}$, temos que

$$a - a = 0 = 0 \cdot n,$$

isto é, a$\equiv a(\text{mod } n)$. Portanto $\equiv (\text{mod } n)$ é reflexiva.

Simétrica: Para todo a, b $\in \mathbb{Z}$, se $a \equiv b(\text{mod } n)$, então $a - b = c \cdot n$, para algum c $\in \mathbb{Z}$, e, assim,

$$b - a = -(a-b) = (-c) \cdot n$$

Logo, $b \equiv a(\text{mod } n)$, o que implica que a relação é simétrica.

Transitiva: Sejam a,b,c $\in \mathbb{Z}$, tais que $a \equiv b(\text{mod } n)$ e $b \equiv c(\text{mod } n)$, então $a - b = e \cdot n$

e $b - c = f \cdot n$, para algum $e, f \in \mathbb{Z}$. Logo,

$$a - c = a - b + b - c = e \cdot n + f \cdot n = (e + f) \cdot n$$

Portanto, $a \equiv c(\text{mod n})$, o que implica que a relação é transitiva.

Logo, temos que tal relação é de equivalência.

Definição 2.4. *Seja A um subconjunto não vazio de $\mathbb{Z}$. Dizemos que A é limitado inferiormente quando existe $x_0 \in \mathbb{Z}$ tal que $x_0 \leqslant x$, para todo $x \in A$.*

Axioma 2.1 ((Principio da boa ordenação - PBO))**.** *Todo subconjunto não vazio e limitado inferiormente A de $\mathbb{Z}$ possui um menor elemento.*

Observação 2.2. *Temos que se $md|rd$, então $m|r$, com $m, d, r \in \mathbb{Z}$.*

De fato, por definição, se $md|rd$, então existe um inteiro j tal que

$$rd = mdj \Leftrightarrow r = mj$$

ou seja, temos que $m|r$.

Teorema 2.1. *(Bezout) Para quaisquer números naturais a e b, existe $d = \text{mdc}(a, b)$. Além disso, existem $x_0, y_0 \in \mathbb{Z}$, tais que*

$$d = ax_0 + by_0.$$

Prova. A prova encontra-se em [6], página 99.

Definição 2.5. *Dois números a e b, são ditos relativamente primo quando o* $\text{mdc}(a, b) = 1$

Como consequência do Teorema anterior, temos o seguinte corolário.

Corolário 2.1. *Os inteiros a e b são relativamente primos se, e somente se, existem $x, y \in \mathbb{Z}$ tais que $1 = ax + by$.*

2.1.1 Os $\mathbb{Z}_n$

Definição 2.6. *Seja n um inteiro positivo, para cada $a \in \mathbb{Z}$, denotamos a classe de equivalência de a módulo n por*

$$\overline{a} := \{b \in \mathbb{Z}; b \equiv a(\text{mod } n)\}.$$

Chamamos de $\mathbb{Z}_n$ ao conjunto das classes de equivalência módulo n, $n \in \mathbb{N}$, $n > 1$. Portanto,

$$\mathbb{Z}_n = \{\overline{a}; a \in \mathbb{Z}\}.$$

Exemplo 2.2. Na congruência módulo 4, temos:

- $\overline{0} = \{a \in \mathbb{Z}; a \equiv 0(\text{mod } 4)\ \} = \{a = 4.k, k \in \mathbb{Z}\} = \{..., -4, 0, 4, 8, ...\}$;
- $\overline{1} = \{a \in \mathbb{Z}; a \equiv 1(\text{mod } 4)\} = \{a = 4.k + 1, k \in \mathbb{Z}\} = \{..., -3, 1, 5, 9, ...\}$;
- $\overline{2} = \{a \in \mathbb{Z}; a \equiv 2(\text{mod } 4)\} = \{a = 4.k + 2, k \in \mathbb{Z}\}\} = \{..., -2, 2, 6, 10, ...\}$;
- $\overline{3} = \{a \in \mathbb{Z}; a \equiv 3(\text{mod } 4)\} = \{a = 4.k + 3, k \in \mathbb{Z}\} = \{..., -1, 3, 7, 11, ...\}$.

Sejam $n \in \mathbb{Z}$, $n > 1$ e $\overline{a} \in \mathbb{Z}_n$. Então, aplicando o algoritmo da divisão temos que

$$\text{existem } q, r \in \mathbb{Z} \text{ tais que } a = q.n + r \text{ e } 0 \leq r < n.$$

Logo, $a - r = q.n$, o que implica em $a \equiv r(\text{mod n})$ e portanto, $\overline{a} = \overline{r}$, $0 \leqslant r < n$. Sendo assim, temos que $\mathbb{Z}_n = \{\overline{0}, \overline{1}, ..., \overline{n-1}\}$.

Observe que $\overline{a} = \overline{r}$, em que r é o resto da divisão de a por n, assim $\mathbb{Z}_n$ é também chamado de classe de restos.

Então, comparando com o exemplo anterior, temos que

$$\mathbb{Z}_4 = \{\overline{0}, \overline{1}, \overline{2}, \overline{3}\}.$$

Propriedades da congruência $\equiv (\text{mod } n)$

Teorema 2.2. *Dados $a, b, c, d \in \mathbb{Z}$, temos que se $a \equiv b(\text{mod } n)$ e $c \equiv d(\text{mod } n)$, então:*

$$(a + c) \equiv (b + d)(\text{mod } n) \quad e\ ac \equiv bd(\text{mod } n).$$

Prova. Por hipótese, temos que $a \equiv b(\text{mod } n)$ e $c \equiv d(\text{mod } n)$, então:

$$a = b + kn \text{ e } c = d + ln$$

para certos $k, l \in \mathbb{Z}$.

Somando tais igualdades, temos:

$$a + c = b + d + (k + l)n,$$

o que implica, $(a + c) \equiv (b + d)(\text{mod } n)$.

Analogamente, fazendo o produto das igualdades, temos:

$$ac = (b + kn)(d + ln) = bd + kdn + bln + kn^2l = bd + n(kd + bl + kln).$$

Fazendo $j = (kd + bl + kln) \in \mathbb{Z}$, temos $ac = bd + jn$, ou seja,

$$ac \equiv bd (\text{mod } n)$$

Definição 2.7. *Seja $n \in \mathbb{N}$, $n > 1$. Definimos as operações de soma e produto em $\mathbb{Z}_n$, respectivamente, por $+ : \mathbb{Z}_n \times \mathbb{Z}_n \to \mathbb{Z}_n$ e $\cdot : \mathbb{Z}_n \times \mathbb{Z}_n \to \mathbb{Z}_n$ onde*

$$\overline{a} + \overline{b} = \overline{a + b}$$

e

$$\overline{a} \cdot \overline{b} = \overline{a \cdot b}.$$

Observação 2.3. *Observe que a soma e o produto em $\mathbb{Z}_n$ estão bem definidos.*

De fato, para verificar que essas operações estão bem definidas, temos que provar que para todo $a, b, c, d \in \mathbb{Z}$, com $\overline{a} = \overline{c}$ e $\overline{b} = \overline{d}$ em $\mathbb{Z}_n$, então:

$$\overline{a + b} = \overline{c + d} \text{ e } \overline{a \cdot b} = \overline{c \cdot d}$$

Para isso, como $\overline{a} = \overline{c}$ e $\overline{b} = \overline{d}$, então $a \equiv c (\text{mod } n)$ e $b \equiv d (\text{mod } n)$. Pelo Teorema 2.2, temos que $a + b \equiv c + d (\text{mod } n)$ e $ab \equiv cd (\text{mod } n)$, ou seja,

$$\overline{a + b} = \overline{c + d} \text{ e } \overline{a \cdot b} = \overline{c \cdot d}$$

logo,

$$\overline{a} + \overline{b} = \overline{c} + \overline{d} \text{ e } \overline{a} \cdot \overline{b} = \overline{c} \cdot \overline{d}$$

o que prova a boa definição.

Propriedades das operações dos $\mathbb{Z}_n$

Proposição 2.2. *Sejam $\overline{a}, \overline{b}, \overline{c} \in \mathbb{Z}_n$, então*

i) $\overline{a} + \overline{b} = \overline{b} + \overline{a}$ *e* $\overline{a} \cdot \overline{b} = \overline{b} \cdot \overline{a}$ *(comutatividade);*

ii) $\overline{a} + (\overline{b} + \overline{c}) = (\overline{a} + \overline{b}) + \overline{c}$ *e* $\overline{a} \cdot (\overline{b} \cdot \overline{c} = (\overline{a} \cdot \overline{b}).\overline{c}$ *(associatividade);*

iii) $\overline{a} \cdot (\overline{b} + \overline{c}) = \overline{a} \cdot \overline{b} + \overline{a} \cdot \overline{c}$ *(distributividade);*

iv) $\overline{a} + \overline{0} = \overline{a}$ *(neutro da adição);*

v) $\overline{a} \cdot \overline{1} = \overline{a}$ *(neutro da multiplicação);*

vi) $\overline{a} \cdot \overline{0} = \overline{0}$ *(elemento absolvente da multiplicação);*

vii) $\overline{a} + \overline{n - a} = \overline{0}$ *(inverso aditivo).*

Prova. i) Sejam $\overline{a}, \overline{b} \in \mathbb{Z}_n$, por definição das operações temos:

$$\overline{a} + \overline{b} = \overline{a + b} = \overline{b + a} = \overline{b} + \overline{a}.$$

De forma análoga, provamos a comutatividade para multiplicação.

ii) Temos que

$$\overline{a} + (\overline{b} + \overline{c}) = \overline{a} + \overline{b + c} = \overline{a + b + c} = (\overline{a + b}) + \overline{c} = (\overline{a} + \overline{b}) + \overline{c}.$$

De forma análoga,provamos a associatividade para multiplicação.

iii) Note que,

$$\overline{a} \cdot (\overline{b} + \overline{c}) = \overline{a} \cdot (\overline{b + c}) = \overline{a \cdot (b + c)} = \overline{a \cdot b + a \cdot c} = \overline{a \cdot b} + \overline{a \cdot c}$$

iv) Temos que mostrar a existência um $\overline{e} \in \mathbb{Z}_n$ tal que $\overline{a} + \overline{e} = \overline{a}$. Para isso usaremos a definição das operações de $\mathbb{Z}_n$, assim , se

$$\overline{a} + \overline{e} = \overline{a}$$

então,

$$\overline{a + e} = \overline{a}.$$

Porém, isso acontece se e for múltiplo de n, pois

$$\overline{a + e} = \overline{a} \Leftrightarrow a + e \equiv a(\text{mod}n \Leftrightarrow a + e - a = k \cdot n, k \in \mathbb{Z} \Leftrightarrow e = k \cdot n, k \in \mathbb{Z}.$$

Nesse caso, a classe dele é igual a classe do zero, portanto,

$$\overline{e} = \overline{0}.$$

Logo $\overline{0}$ é o neutro da adição de $\mathbb{Z}_n$.

v) Temos que mostrar a existência de uma classe de equivalência $\overline{x} \in \mathbb{Z}_n$ tal que

$$\overline{a} \cdot \overline{x} = \overline{a}$$

Usaremos novamente a definição das operações de $\mathbb{Z}_n$, logo se

$$\overline{a} \cdot \overline{x} = \overline{a}$$

então,

$$\overline{a \cdot x} = \overline{a}$$

Isso acontece sempre que $x - 1$ é múltiplo de n, pois

$$\overline{ax} = \overline{a} \Leftrightarrow ax - a = k \cdot n, k \in \mathbb{Z} \Leftrightarrow a(x-1) = k \cdot n, k \in \mathbb{Z}.$$

Nesse caso, a classe dele é a mesma do 1 , ou seja,

$$\overline{x} = \overline{1}$$

Sendo assim, $\overline{1}$ é o neutro da multiplicação dos $\mathbb{Z}_n$.

vi)Temos que para todo $\overline{a} \in \mathbb{Z}_n$,

$$\overline{a} \cdot \overline{0} = \overline{a \cdot 0} = \overline{0}.$$

vii) Temos que

$$\overline{a} + \overline{x} = \overline{0} \Leftrightarrow \overline{a + x} = \overline{0}$$

Porém, $a + x \in \overline{0} \Leftrightarrow a + x = n.k$, para algum $k \in \mathbb{Z}$, ou seja,

$$x = nk - a.$$

Como os representantes das classes podem ser tomados no conjunto $\{0, 1, \cdots, n-1\}$, então podemos tomar $k = 1$, daí

$$x = n \cdot 1 - a = n - a$$

Portanto,

$$\overline{x} = \overline{n - a} \in \mathbb{Z}_n$$

é o inverso aditivo de $\overline{a}$.

2.1.2 A função φ de Euler

Definição 2.8. *Seja $n \in \mathbb{N}$. O número $\varphi(n)$ é definido como sendo*

$$\varphi(n) = \#\{k \in \mathbb{N}; 1 \leq k \leq n, \text{mdc}(k,n) = 1\}.$$

A função $\varphi : \mathbb{N} \to \mathbb{N}$ com $n \to \varphi(n)$ chama-se função de Euler.

Exemplo 2.3. a) Temos que $\varphi(12) = 4$, pois o conjunto de números relativamente primos a 12 $\{1, 5, 7, 11\}$.

b) Note que os números $1, 2, 4, 5, 7$ e 8 são relativamente primos a 9, portanto temos que $\varphi(9) = 6$.

Proposição 2.3. *Para todo $n \in \mathbb{N}$, temos:*

$$\sum_{d|n} \varphi(d) = n$$

Prova. Para todo divisor d de n consideramos o seguinte conjunto:

$$S_d = \{k; 1 \leq k \leq n, \text{mdc}(k,n) = d\}.$$

Primeiro, mostremos que $S_d \neq \emptyset$. Para isso, note que, se d divide n, então d é um número tal que $1 \leq d \leq n$ e, nesse caso, $\text{mdc}(d,n) = d$, pois d não possui divisores maiores que ele mesmo. Portanto, d pertence a S_d.

Temos $S_d \cap S_{d'} = \emptyset$ se d e d' são divisores distintos. Temos que:

$$\bigcup_{d|n} S_d = \{1, 2, ..., n\},$$

pois, se $k \in \{1, 2, \cdots, n\}$, então $k \in S_d$ quando $d = \text{mdc}(k,n)$. Assim,

$$n = \#\{1, 2, 3, ..., n\} = \#\left(\bigcup_{d|n} S_d\right) = \sum_{d|n} \#S_d.$$

Temos que

$$k \in S_d \Leftrightarrow \text{mdc}(k,n) = d \Leftrightarrow \text{mdc}\left(\frac{k}{d}, \frac{n}{d}\right) = 1.$$

Segue

$$\#S_d = \#\{l; 1 \leq l \leq \frac{n}{d} \text{ e } \text{mdc}(l, n/d) = 1\},$$

isto é,

$$\#S_d = \varphi\left(\frac{n}{d}\right).$$

Assim,

$$\sum_{d|n} \#S_d = \sum_{d|n} \varphi\left(\frac{n}{d}\right) = \sum_{d|n} \varphi(d),$$

a última igualdade segue do fato de

$$\left\{\frac{n}{d}; d \text{ divide } n\right\} = \{d'; d' \text{ divide } n\}.$$

Portanto, como afirmado

$$n = \sum_{d|n} \varphi(d).$$

2.2 Grupos

Como pretendemos estudar os homomorfismos de grupos existentes entre $\mathbb{Z}_m$ e $\mathbb{Z}_n$, nessa seção iremos apresentar a teoria de grupos e alguns dos resultados principais a serem utilizados. A teoria de grupos é importante em varias aréas da matemática. Por exemplo, na topologia algébrica, grupos são usados para descrever os invariantes de espaços topológicos; Em equações diferenciais e variedades o conceito de grupo de Lie é muito importante; A teoria de Galois, que é origem histórica do conceito de grupo, procura descrever as simetrias das equações satisfeitas pelas soluções de uma equação polinomial e Grupos de Permutação e o conceito de ação de um grupo são utilizados na ánalise combinatória para simplificar a contagem dos elementos. Na física, a teoria de grupo se faz presente para descrever as simetrias que as leis da Física devem obedecer. Em Química, grupos são utilizados para classificar estruturas cristalinas e a simetrias das moléculas.

Definição 2.9 (Operação binária)**.** *Seja C um conjunto não vazio. Uma função $f : C \times C \to C$ chama-se operação binária sobre C.*

Exemplo 2.4. A função $f : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$ dada por $f(a, b) = 2a \cdot b$ é uma operação sobre $\mathbb{N}$, onde $\cdot$ denota a operação de multiplicação usual.

Definição 2.10. *Seja G um conjunto não vazio munido com a operação binária $\star$. Di-*

zemos que G é um grupo se satisfizer as seguintes condições:

i) $\star$ *é associativa, ou seja,*

$$a \star (b \star c) = (a \star b) \star c \text{ para todo } a,\ b,\ c \in G;$$

ii) *Existe um elemento neutro para* $\star$*, ou seja,*

$$\exists\ e \in G \text{ tal que } a \star e = e \star a = a, \text{ para todo } a \in G;$$

iii) *Todo elemento em G possui inverso em relação a* $\star$*, ou seja,*

$$\text{para todo } a \in G,\ \exists\ a' \in G \text{ tal que } a \star a' = e = a' \star a.$$

O elemento a' inverso de a será denotado por a^{-1}.

Indicaremos um grupo G munido da operação $\star$ pela notação: $(G, \star)$.

Además, se

$$a \star b = b \star a, \text{ para todo } a, b \in G,$$

G é dito ser um grupo abeliano ou comutativo.

Exemplo 2.5. Para cada $n \in \mathbb{N}$, $n > 1$, o conjunto $\mathbb{Z}_n$ dotado da operação de adição é um grupo abeliano. Da Proposição 2.2, temos que a soma em $\mathbb{Z}_n$ é associativa, comutativa e além disso $\overline{0}$ é o elemento neutro e $\overline{n-a}$ é o inverso de $\overline{a}$, para todo $\overline{a} \in \mathbb{Z}_n$. Logo $\mathbb{Z}_n$ munido da operação de adição é um grupo abeliano e é denotado $(\mathbb{Z}_n, +)$.

Exemplo 2.6. O conjunto $\mathbb{Z}_n$ dotado da operação de multiplicação não é um grupo, pois $\overline{0}$ não possui inverso, visto que $\overline{1}$ é neutro, mas

$$\text{não existe } \overline{a} \in \mathbb{Z}_n \text{ tal que } \overline{0} \cdot \overline{a} = \overline{1}$$

Observação 2.4. *Dos exemplos anteriores, sempre que nos referirmos ao grupo $\mathbb{Z}_n$, estaremos pensando no conjunto $\mathbb{Z}_n$ munido da operação de adição de classes usual.*

Exemplo 2.7. O conjunto $\mathbb{R}$ munido da operação de adição é um grupo. De fato, sabemos que a adição em $\mathbb{R}$ é associativa, como também o número 0 é o neutro aditivo dos reais e dado $a \in \mathbb{R}$ temos que $-a$ é o inverso de a e $-a \in \mathbb{R}$. Analogamente, provamos que o conjunto $\mathbb{Z}$ munido com a operação de adição também é grupo.

Exemplo 2.8. Temos que o conjunto $\mathbb{R}^*$ munido com a operação de multiplicação é um grupo. De fato, o produto em $\mathbb{R}$ é associativo e sabemos que o número 1 é o neutro multiplicativo dos reais e dado $a \in \mathbb{R}^*$, $\frac{1}{a}$ é o inverso de a e $\frac{1}{a} \in \mathbb{R}^*$. Logo, $(\mathbb{R}^*, \cdot)$ é um grupo.

Definição 2.11 (Ordem de um grupo)**.** *Seja G um grupo munido da operação $\star$. Dizemos que $(G,\star)$ é finito quando o conjunto G possuir um número finito de elementos. Neste caso, chamamos de ordem o número de elementos de G. Caso G não seja finito, dizemos*

que (G,⋆) é de ordem infinita. Denotamos a ordem de G por | G |.

Exemplo 2.9. Temos que $| \mathbb{Z}_n | = n$ e o grupo $(\mathbb{Z}, +)$ é de ordem infinita.

2.2.1 Subgrupos

Definição 2.12. *Seja G um grupo. Um subconjunto não vazio H de G é um subgrupo de G quando, munido com a operação de G, também é um grupo. Para indicar que H é um subgrupo de G, usaremos a seguinte notação: $H < G$.*

Exemplo 2.10. Seja $G = \mathbb{Z}_4$. $H = \{\overline{0}, \overline{2}\}$ é um subgrupo de G. De fato, note que a soma é bem definida em H e como a soma em $\mathbb{Z}_n$ é associativa, então em H a soma é associativa, pois H é um subconjunto de $\mathbb{Z}_n$ para $n = 4$. Note também que $\overline{0} \in H$ e sabemos que $\overline{0}$ é o neutro de $\mathbb{Z}_n$, ademais temos que todos os elementos de H possuem seus inversos em H, pois o inverso de $\overline{0}$ é o próprio e o inverso de $\overline{2}$ também é o próprio. Logo, H também é um grupo, portanto por definição $H < G$.

Exemplo 2.11. Como $G = \mathbb{C}$ é um grupo multiplicativo(pois é associativo, contém neutro (o elemento 1) e o elemento a de G possui inverso($\frac{1}{a}$)). Temos que $H = \{1, -1, i, -i\}$ é um subgrupo de G. Observemos, primeiramente, que H é um subconjunto de G, sendo assim o produto em H é associativo. Por outro lado, o neutro multiplicativo dos complexos é o número 1 e $1 \in H$. Também note que o inverso de todos os elementos de H pertecem a H(1 é inverso dele mesmo, assim como -1 é inverso dele próprio; i e $-i$ são inversos um do outro). Portanto, H também é um grupo munido com a mesma operação de G, logo $H < G$

Teorema 2.3. *Seja H um subconjunto não vazio de um grupo G. Então, $H < G$ se, e somente se, uma das condições é satisfeita:*

i) *$h_1.h_2$ e $h_1^{-1} \in H$, para todo $h_1, h_2 \in H$.*

ii) *$h_1.h_2^{-1} \in H$, para todo h_1,$h_2 \in H$.*

Prova. Se H é um subgrupo de G, então H também é um grupo, por definição as condições são satisfeitas. Do mesmo modo, suponhamos que H satisfaz (i), logo, para todo $h \in H$, temos $h_1^{-1} \in H$. Assim $e = h.h^{-1} \in H$. O fato de $h_1.h_2 \in H$, para todo h_1,$h_2 \in H$ garante a boa definição da operação e a associatividade em G garante a associatividade em H. Por conseguinte, $H < G$. Finalmente se h satisfaz (ii) então dados h_1,$h_2 \in H$,

$$e = h_2.h_2^{-1} \in H$$

logo,

$$h_2^{-1} = e.h_2^{-1} \in H,$$

assim,

$$h_1 h_2 = h_1 (h_2^{-1})^{-1} \in H$$

e, por (i), $H < G$.

Exemplo 2.12. Sejam $H = \{0, 1\}$ e $G = (\mathbb{Z}, +)$. Temos que H não é subgrupo de G. Pelo teorema temos que para todo h_1,$h_2 \in H$, $h_1.h_2$ e $h^{-1} \in H$. Porém "+" não é uma operação em H. Logo, H não é um grupo e portanto não é subgrupo de G.

2.2.2 Grupos cíclicos

Definição 2.13. *Sejam G um grupo e $a \in G$. Definimos a potência de a por um número inteiro $n \in \mathbb{Z}$, denotado por a^n, como sendo*

$$a^n = \begin{cases} e, \ \textit{se } n = 0, \\ \underbrace{a \cdot a \cdot a \cdots a}_{n \ \textit{vezes}}, \ \textit{se } n > 0, \\ \underbrace{a^{-1} \cdot a^{-1} \cdot a^{-1} \cdots a^{-1}}_{-n \ \textit{vezes}}, \ \textit{se } n < 0. \end{cases}$$

Considere G um grupo e $a \in G$. Agora seja H o conjunto de todas as potências de a, ou seja,

$$H = \{a^n : n \in \mathbb{Z}\}.$$

Quando a operação for aditiva, H é o conjunto dos múltiplos de a, isto é,

$$H = \{n.a : n \in \mathbb{Z}\}.$$

Mostraremos que $H < G$. Sejam h_1,$h_2 \in H$. Como h_1,h_2 são potências de a, temos $h_1 = a^{n_1}$ e $h_2 = a^{n_2}$, para algum $n_1, n_2 \in \mathbb{Z}$. Assim:

$$h_1.h_2^{-1} = a^{n_1}.\frac{1}{a^{n_2}} = a^{n_1}.a^{-n_2} = a^{n_1 - n_2}$$

Tome $n_1 - n_2 = m \in \mathbb{Z}$ e temos que $h_1.h_2^{-1} = a^m$, logo, pertence a H e portanto $H < G$.

Nessas condições H é chamado subgrupo cíclico gerado por a, no qual denotaremos

$$H = \langle a \rangle.$$

Também dizemos que a é um gerador de H.

Exemplo 2.13. No grupo multiplicativo $G = \{1, -1, i, -i\}$ temos que, $i^0 = 1$, $i^1 = i$, $i^2 = -1$, $i^3 = i$. Assim $\langle i \rangle = \{1, -1, i, -i\} = G$.

Definição 2.14. *Um grupo G é dito cíclico quando existir um $a \in G$ tal que*

$$G = \langle a \rangle$$

Observação 2.5. *Da definição, segue que se $G = \langle a \rangle$:*

i) *$a^n = e$, para algum $n \in \mathbb{N}$.*

ii) *$a^n \neq e$ para todo $n \in \mathbb{N}$, neste caso G é de ordem infinita.*

Exemplo 2.14. Para $G = \mathbb{Z}_8$, temos que $\overline{1}, \overline{3}, \overline{5}$ e $\overline{8}$ são geradores de G.

Solução. Note que,

- $\langle \overline{1} \rangle = \{n\overline{1}; n \in \mathbb{Z}\} = \{\overline{n}; n \in \mathbb{Z}\} = G$
- $\langle \overline{3} \rangle = \{\overline{3n}; n \in \mathbb{Z}\} = \{\overline{3}, \overline{6}, \overline{1}, \overline{4}, \overline{7}, \overline{2}, \overline{5}, \overline{0}\} = G$.
- $\langle \overline{5} \rangle = \{\overline{5n}; n \in \mathbb{Z}\} = \{\overline{5}, \overline{2}, \overline{7}, \overline{4}, \overline{1}, \overline{6}, \overline{3}, \overline{0}\} = G$.
- $\langle \overline{7} \rangle = \{\overline{7n}; n \in \mathbb{Z}\} = \{\overline{7}, \overline{6}, \overline{5}, \overline{4}, \overline{3}, \overline{2}, \overline{1}, \overline{0}\} = G$.

Exemplo 2.15. Seja $n \in \mathbb{N}$, $n > 2$. O grupo $\mathbb{Z}_n$ é cíclico, pois

$$\mathbb{Z}_n = \langle \overline{1} \rangle.$$

Teorema 2.4. *Todo subgrupo de um grupo cíclico é cíclico.*

Prova. Sejam $G = \langle a \rangle$ e H um subgrupo de G. Para $H = \{e\}$, tem-se $H = \langle e \rangle$. Se $H \neq \{e\}$, então existe $b \in H$, com $b \neq e$. Como $b \in G$, $b = a^t$ para algum $t \in \mathbb{Z}^*$. Mas sendo $H < G$,$a^{-t} \in H$. Por isso,

$$X = \{n \in N : a^n \in H\} \neq \emptyset$$

Pelo PBO, (Axioma 2.1) X possui um menor elemento. Seja m=min X

Mostremos que $H = \langle a^m \rangle$.

Como $a^m \in H$, então $\langle a^m \rangle \subset H$. Consideremos, pois $h \in H$. Como $H < G$, então

$h = a^n$, para algum $n \in \mathbb{Z}$. Pelo algoritmo da divisão, existem $q, r \in \mathbb{Z}$, tais que

$$n = mq + r, \text{ com } 0 \leq r < m.$$

Logo $a^n = a^{mq+r} = a^{mq}.a^r$, ou seja,

$$a^r = a^n.(a^m)^{-q}$$

Como $a^m \in H$, segue que $(a^m)^{-q} \in$ H. Além disso, sendo a^n e $(a^m)^{-q}$ elementos de H, temos que $a^n.(a^m)^{-q} \in H$, portanto, $a^r \in$ H. Porém, desde que $m = minX$, devemos necessariamente ter $r = 0$. Logo, $n = mq$ e

$$h = a^n = (a^m)^q \in \langle a^m \rangle.$$

isto é, $H \subset \langle a^m \rangle$ e sendo assim, $H = \langle a^m \rangle$.

Definição 2.15. *Chamaremos de ordem de um elemento de um grupo a, ao menor inteiro positivo m tal que $a^m = e$ e denotaremos $o(a)$. Quando não existir m nessas condições, dizemos que ordem de a é infinita.*

Proposição 2.4. *Seja G um grupo.*

i) *Dado $a \in G$, $a \neq e$, tem-se que:*

$$o(a) = 2 \Leftrightarrow a = a^{-1}$$

ii) *$o(a) = o(a^{-1})$, para todo $a \in G$.*

iii) *Se $o(a) = 2$, para todo $a \in G \setminus \{e\}$, então G é abeliano.*

iv) *Se $o(a) = n.m$, então $o(a^m) = n$.*

Prova. i) Se o$(a) = 2$, então, por definição,

$$a^2 = e,$$

ou seja,

$$a.a = e \Leftrightarrow a.a.a^{-1} = a^{-1} \Leftrightarrow a = a^{-1}.$$

Por outro lado, se $a = a^{-1}$, temos

$$a.a = a.a^{-1} \Rightarrow a^2 = e$$

ii) Se $a \in G$, tem ordem finita, então existe $n \in \mathbb{N}$ tal que $a^n = e$. Porém,

$$a^n = e \Rightarrow a^{n-1} \cdot a \cdot a^{-1} = a^{-1} \cdot e = \underbrace{a^{-1} \cdot a^{-1} \cdot ... \cdot a^{-1}}_{n-vezes} = (a^{-1})^n$$

Por menor $m \in \mathbb{N}$ satisfazendo $a^m = e$ é o menor que satisfaz $(a^{-1})^m = e$. Logo o(a) =o(a^{-1}).

iii) Temos que o$(a) = 2$ para todo $a \in G \setminus \{e\}$. Logo por (i), temos que:

$$a = a^{-1}, \text{ para todo } a \in G.$$

Agora sejam $a, b \in G$, temos que $a \cdot b \in G$. Desse modo

$$a \cdot b = (ab)^{-1} = b^{-1} \cdot a^{-1} = b \cdot a$$

Portanto, G é abeliano.

iv) Assuma que o$(a) = n \cdot m$. Então,

$$\text{o}(a) = n \cdot m \Rightarrow a^{n \cdot m} = e \Rightarrow (a^m)^n = e.$$

Resta-nos mostrar que n é o menor inteiro satisfazendo $(a^m)^n = e$. Se $r \in \mathbb{N}$ e $r < n$ é tal que $(a^m)^r = e$, então:

$$a^{mr} = e \text{ e } mr < mn,$$

o que contradiz o fato de $m \cdot n$ ser a ordem de a. Logo o$(a^m) = n$.

Teorema 2.5. *Sejam G um grupo e $a \in G$.*

i) Se $a^n = e$ para algum $n \in \mathbb{N}$, então $o(a)$ divide n;

ii) Se o$(a) = m$, $k \in \mathbb{N}$ e r é o resto da divisão de k por m, então $a^k = a^r$.

iii) o$(a) = m$ se, e somente se, $\langle a \rangle$ tem ordem m.

Prova. i) Como $a^n = e$, então a é de ordem finita. Consideramos, pois, a ordem de a é igual a m. Pelo algoritmo da divisão existem $q, r \in \mathbb{Z}$ tais que $n = m.q + r$ com $0 \leq r < m$. Portanto,

$$e = a^n = a^{mq+r} = (a^m)^q.a^r = e^q.a^r \Rightarrow a^r = e$$

Pela minimidade de m, temos que $r = 0$ e assim $n = m.q$, o que significa que $m|n$.

ii) Basta notar que para cada $k \in \mathbb{Z}$, $k = m.q + r$ com $q, r \in \mathbb{Z}$ e $0 \leq r < m$, o que acarreta em $a^k = a^r$.

iii) Se $o(a) = m$, segue que os elementos $e, a, \cdots, a^{m-1}$ são todos diferentes. O que é verdadeiro, pois se $a^i = a^j$ para alguns $0 \leq i < j \leq m - 1$, então $a^{j-i} = e$ e $j - i < m$, o que é uma contradição. Agora seja $H = \langle a \rangle$. Por (ii), sabemos que dado $k \in \mathbb{Z}$, $a^k = a^r$,

sendo $r \in \{0, 1, ..., m-1\}$. Por isso,

$$H = \langle a \rangle = \{a^k; k \in \mathbb{Z}\} = \{a^r; r = 0, 1, ..., m-1\}$$

tem ordem m.

Por outro lado, suponhamos que H tem ordem m. Isso nos diz que as potências a^i,com $i \in \mathbb{Z}$, não podem ser todas diferentes. Logo, existem $i, j \in \mathbb{Z}$, com $i < j$, de maneira que $a^i = a^j$, isto é, a^{j-i}=e, o que implica que a tem ordem finita, digamos que $o(a) = m$. Assim, como dito anteriormente, os elementos $e, a, ..., a^{m-1}$ são todos diferentes. Logo, por (ii)

$$H = \langle a \rangle = \{a^r : r = 0, 1, ..., m-1\} = \{e, a, ..., a^{m-1}\}$$

Ou seja, $\langle a \rangle$ tem ordem m.

Teorema 2.6. *Seja $G = \langle a \rangle$ um grupo cíclico finito de ordem n. Então para cada divisor d de n, existe um único subgrupo H de G cuja ordem é d.*

Prova. Se $d = 1$ ou $d = n$, então basta considerarmos $H = \{e\}$ ou $H = G$. Suponhamos que 1< $d < n$ e seja $m \in \mathbb{N}$, tal que $n = m \cdot d$. Pelo item (iv) da Proposição 2.4, o elemento $b = a^m$ tem ordem d e, por isso, $H = \langle b \rangle$ é um subgrupo de G de ordem d.

Mostremos agora a unicidade de H. Seja K um subgrupo de G de ordem d. Pelo Teorema 2.4, K é cíclico gerado por um elemento da forma $c = a^r$. Logo, como a ordem de c é d,

$$e = c^d = a^{rd}.$$

Assim, pelo item (i) do Teorema 2.5, n divide rd, ou seja, $n = md|rd$. Com isso, da Observação 2.2, temos $m|r$, digamos que $r = m\alpha$, $\alpha \in \mathbb{Z}$. Portanto, para $x \in K = \langle a^r \rangle$, existe $s \in \mathbb{Z}$ tal que

$$x = (a^r)^s = a^{rs} = a^{m\alpha s} = (a^m)^{\alpha s} \in \langle a^m \rangle = H,$$

de maneira que $K \subset H$. Mas, como H e K, tem ordem d, temos que $K = H$.

Agora com os conhecimentos que temos acerca de grupos cíclicos e a função φ de Euler, iremos apresentar um teorema e um corolário que nos serão úteis para demonstração do teorema principal do nosso estudo.

Teorema 2.7. *Seja $G = \langle a \rangle$ um grupo cíclico finito de ordem n. Dado $t \in \mathbb{Z}$, o elemento*

a^t gera G se, e somente se, $\text{mdc}(t, n) = 1$.

Prova. Suponha que a^t gera G. Como $a \in G$, por definição, existe $r \in \mathbb{Z}$ tal que

$$a = (a^t)^r = a^{tr}$$

Donde,

$$a^{tr-1} = e$$

Assim, do Teorema 2.5,

$$n|(tr - 1)$$

ou seja,

$$tr \equiv 1(\text{mod}n).$$

Daí, existe $\lambda \in \mathbb{Z}$ tal que

$$1 = tr + \lambda n$$

o que implica, pelo Corolário 2.1 que $\text{mdc}(t, n) = 1$.

Reciprocamente, suponha $\text{mdc}(t, n) = 1$, do Corolário 2.1, existem $r, \lambda \in \mathbb{Z}$ tais que

$$1 = tr + \lambda n$$

Portanto,

$$a^1 = a^{tr+\lambda n} = a^{tr}a^{\lambda n} = a^{tr}(a^n)^\lambda = a^{tr}$$

Como $\langle a \rangle = G$ e $a \in \langle a^t \rangle$, temos que $G = \langle a \rangle \subset \langle a^t \rangle$, donde $\langle a^t \rangle = G$, como queríamos.

Como consequência do teorema acima, temos o seguinte corolário:

Corolário 2.2. *Se G é um grupo cíclico finito de ordem n, então G tem $\varphi(n)$ geradores.*

Apresentaremos agora as definições das classes laterais que será de grande importância para a demonstração do Teorema de Lagrange que virá a seguir.

Sejam G um grupo e H um subgrupo de G. Defina a relação

$$a \equiv_E b(\text{mod}H) \iff a^{-1}b \in H.$$

A relação anterior é de equivalência sobre G. Ademais, suas classes de equivalência são

dadas por

$$\overline{a} = \{ah; h \in H\} = aH, \ \ a \in G.$$

a qual chamaremos de classe lateral á esquerda de H em G determinada por a.

A relação $a \equiv_D b(\text{mod } H)$ sobre G dada, para quaisquer $a, b \in G$, por

$$a \equiv_D b(modH) \iff ab^{-1} \in H.$$

é de equivalência. Ademais, suas classes de equivalência são dadas por

$$\overline{a} = \{ha; h \in H\} = Ha, \ \ a \in G.$$

e chamaremos classe lateral á direita de H em G determinada por a.

Teorema 2.8 (Teorema de Lagrange)**.** *Sejam G um grupo finito e H um subgrupo de G. Então,*

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

em que $(G : H) = \#\{aH; a \in G\}$.

Ou seja, a ordem de H divide a ordem de G.

Prova. Como G é finito, então $(G : H)$ também é. Tomando $(G : H) = r$. Consideremos então H_E=$\{a_1H, a_2H, ..., a_rH\}$. Da Observação 2.1, temos que H_E é uma partição de G, ou seja,

$$G = a_1H \cup a_2H \cup ... \cup a_rH.$$

e mais ainda, $a_iH \cap a_jH = \emptyset$ para $i \neq j$. Desse modo, observando que a cardinalidade de cada classe em $|a : H|$ é igual a ordem de H, obtemos que

$$|G| = \underbrace{|H| + |H| + ... + |H|}_{r \ vezes} = |H|.r$$

ou seja, $|G| = |H|.(G : H)$.

O famoso Teorema de Lagrange será útil para a demonstração do teorema principal do nosso estudo.

Antes de começarmos a falar sobre homomorfismo de grupo, apresentaremos dois conceitos que serão de suma importância para a sessão seguinte.

Definição 2.16 (Subrupos Normais)**.** *Seja G um grupo. Chamamos um subgrupo H de*

G de normal quando:

$$ghg^{-1} \in H, \text{ para todo } g \in G \text{ e para todo } h \in H.$$

Denotaremos como: $H \triangleleft G$.

Observação 2.6. *Segue da definição de Subgrupos Normais que*

$$H \triangleleft G \iff aH = Ha, \text{ para todo } a \in G.$$

Isso nos leva a definir,

$$G/H = \{aH; a \in G\} = \{Ha; a \in G\}.$$

Mostraremos a seguir o teorema que nos leva a definição de grupo quociente.

Teorema 2.9. *Sejam (G,·) um grupo e H um subgrupo normal de G. Então,*

$$\begin{array}{rccc} \cdot : & G/H \times G/H & \longrightarrow & G/H \\ & (xH, yH) & \to & (xH)(yH) = xyH \end{array}$$

define uma operação binária sobre G/H e além disso, G/H é um grupo com tal operação.

Prova. Para provarmos que '$\cdot$' é uma operação binária sobre G/H, mostraremos que o resultado não depende do representante das classes, ou seja, se $x_1H = x_2H$ e $y_1H = y_2H$, com $x_1, x_2, y_1, y_2 \in$ G, então

$$x_1H.y_1H = x_2H.y_2H$$

Para $x_1H = x_2H$ e $y_1H = y_2H$, temos:

$$x_1 \equiv_E x_2 \text{ e } y_1 \equiv_E y_2 \Leftrightarrow x_1^{-1}x_2 = h_1 \in H \text{ e } y_1^{-1}y_2 = h_2 \in H.$$

Portanto,

$$y_1^{-1}x_1^{-1}x_2y_2 = y_1^{-1}h_2y_2$$

pois $x_1^{-1}x_2 = h_1$ e como $y_1^{-1} = h_2.y_2^{-1}$, então

$$y_1^{-1}x_1^{-1}x_2y_2 = h_2y_2^{-1}h_1y_2.$$

Como $H \triangleleft G$, então $y_2^{-1}h_1y_2$=$h_3 \in H$. Assim,

$$y_1^{-1}x_1^{-1}x_2y_2 = h_2h_3 \in H$$

donde,

$$(x_1y_1)^{-1}(x_2y_2) \in H$$

e consequentemente,

$$x_1y_1H = x_2y_2H,$$

Assim, $x_1H.y_1H = x_2H.y_2H$. Como consequência '$\cdot$' é uma operação binária sobre G/H.

Agora iremos mostrar que G/H é um grupo. Para isso considere $xH, yH, zH \in G/H$. Desse modo, como temos que a operação em G é associativa,

$$xH.(yH.zH) = (y.z)H = x(yz)H = (xy)zH = (xyH).zH = (xH.yH).zH,$$

isto é, a operação é associativa. Temos também:

$$(xH).(eH) = (xH) = (eH).(xH)$$

isto é, temos $eH = H$ é o elemento neutro da operação. Por fim, nos resta mostrar que cada elemento de G/H possui um inverso. Para isso, com relação a essa operação observemos que, se $x \in G$, então

$$(xH).(x^{-1}H) = e.H = (x^{-1}H).(xH) = H.$$

Logo,

$$x^{-1}H = (xH)^{-1}.$$

Portanto, $(G/H, \cdot)$ é um grupo e é chamado de grupo quociente de G por H.

2.3 Homomorfismos de grupos

Definição 2.17. *Sejam $(G, \star_1)$ e $(P, \star_2)$ dois grupos e $f : G \to P$ uma aplicação. f é chamada de homomorfismo do grupos G em P quando:*

$$f(a \star_1 b) = f(a) \star_2 f(b), \text{ para todo } a,b \in G.$$

Exemplo 2.16. Seja $f : \mathbb{R} \times \mathbb{R} \to \mathbb{R}^*$ dada por $f(x, y) = 2^{x-y}$. f é um homomorfismo.

Com efeito, sejam $(a,b),(c,d) \in \mathbb{R}\times\mathbb{R}$, temos que

$$f((a,b)+(c,d)) = f(a+c,b+d) = 2^{a+c-(b+d)} = 2^{(a-b)+(c-d)} = 2^{a-b}.2^{c-d} = f(a,b).f(c,d)$$

Logo, f é um homomorfismo de $\mathbb{R}\times\mathbb{R}$ em $\mathbb{R}^*$.

Exemplo 2.17. Seja $g:\mathbb{Z}\to\mathbb{Z}$ dada por $g(x) = x+2$ para todo $x\in\mathbb{Z}$. Notemos que g não é um homomorfismo. Pois, sendo $x,y\in\mathbb{Z}$, temos que

$$g(x+y) = x+y+2 \neq (x+2)+(y+2) = g(x)+g(y)$$

Portanto g não é um homomorfismo.

Exemplo 2.18. Se $(G_1,*)$ e $(G_2,\star)$ são grupos e

$$\begin{array}{rccc} f: & G_1 & \to & G_2 \\ & x & \mapsto & e_2 \end{array}$$

Então, f é sempre um homomorfismo.De fato, sejam $x,y\in G$, temos que:

$$f(x*y) = e_2 = e_2\star e_2 = f(x)\star f(y).$$

Logo, f é um homomorfismo.

Proposição 2.5. *Seja $f: G\to P$ um homomorfismo de grupos. Então:*

i) $f(e_1) = e_2$

ii) $f(a^{-1}) = f(a)^{-1}$, *para todo* $a\in G$.

iii) A imagem de f, denotado $Im(f)$, é um subgrupo de P.

Prova. i) Como $e_1 = e_1\cdot e_1$, então

$$f(e_1) = f(e_1\cdot e_1) = f(e_1)\cdot f(e_1)$$

Operando $(f(e_1))^{-1}$ em ambos os lados da igualdade, temos:

$$f(e_1)\cdot(f(e_1))^{-1} = f(e_1)\cdot f(e_1)\cdot(f(e_1))^{-1}$$

Portanto,

$$e_2 = f(e_1)$$

Logo $f(e_1) = e_2$.

ii) Para qualquer $a \in G$, $a.a^{-1} = e_1$. Portanto

$$f(a)f(a^{-1}) = f(a \cdot a^{-1}) = f(e_1) = e_2$$

ou seja, $f(a) \cdot f(a^{-1})$=e_2, assim,

$$f(a^{-1}) = f(a)^{-1}.$$

iii) Sendo $f(e_1) = e_2$, então $Im(f) \neq \emptyset$. Agora, sejam $x, y \in Im(f)$, existem $a, b \in G$, tais que $f(a) = x$ e $f(b) = y$. Por isso,

$$x \cdot y^{-1} = f(a) \cdot f(b)^{-1} = f(a) \cdot f(b^{-1}) = f(a \cdot b^{-1}$$

Portanto, $x \cdot y^{-1} \in Im(f)$, o que implica, pelo Teorema 2.3, que $Im(f) < P$.

Definição 2.18 (Isomorfismo de grupos)**.** *Um homomorfismo de grupos de G em P que seja bijetor é chamado de isomorfismo de grupos.*

Teorema 2.10. *Sejam G e P grupos com neutros e e e_1 respectivamente e $f : G \to P$ um homomorfismo. Então:*

i) $N(t) = \{g \in G : f(g) = e_1\}$ é um subgrupo normal de G que é chamado do núcleo do homomorfismo e ainda

$$f \text{ é injetiva } \Leftrightarrow N(f) = \{e\}.$$

ii) Existe um isomorfismo entre $G/N(f)$ e Imf.

Prova. i) Note que

- $e \in N(f)$ pois $f(e) = e_1$.
- Se g_1 e $g_2 \in N(f)$, então

$$f(g_1 \cdot g_2) = f(g_1).f(g_2) = e_1.e_1 = e_1$$

  Logo. g_1 $g_2 \in N(f)$;
- Se $g \in N(f)$, então

$$f(g^{-1}) = (f(g))^{-1} = e_1^{-1} = e_1.$$

  Logo, $g^{-1} \in N(f)$.

Agora, se $z \in N(f)$ e $g \in G$, temos:

$$f(g^{-1}.z.g) = f(g^{-1}).f(z).f(g) = (f(g))^{-1}.e_1.f(g) = e_1.$$

Portanto $g^{-1}.z.g \in N(f)$, para todo $z \in N(f)$ e $g \in G$. Logo $N(f)$ é um subgrupo normal de G.

ii) Seja $\overline{G} = G/N(f)$ e $N = N(f) \triangleleft G$. Vamos definir

$$\overline{f} : \overline{G} \to Im(f)$$
$$\overline{g} \mapsto f(g)$$

Primeiro, iremos ver que $\overline{f}$ está bem definida, pois,

$$\overline{g} = \overline{h} \Leftrightarrow gh^{-1} \in N(f) \Leftrightarrow f(gh^{-1}) = e_1 \Leftrightarrow f(g) = f(h).$$

Ademais, $Im(\overline{f}) = Im(f)$, pois $f(\overline{g}) = f(g)$, para $g \in G$ e portanto a função é sobrejetora.

Se $\overline{x}$ e $\overline{y} \in \overline{G}$, temos:

$$\overline{f}(\overline{x} \cdot \overline{y}) = \overline{f}(\overline{xy}) = f(xy) = f(x).f(y) = \overline{f}(\overline{x})\overline{f}(\overline{y})$$

Perceba ainda que

$$\overline{f}(\overline{x}) = e_1 \Leftrightarrow f(x) = e_1 \Leftrightarrow x \in N \Leftrightarrow \overline{x} = \overline{e}.$$

Portanto, $N(\overline{f}) = \{\overline{e}\}$ e assim $\overline{f}$ é injetora. O que nos mostra que $\overline{f}$ é um isomorfismo de $\overline{G}$ sobre a imagem de f.

Corolário 2.3. *Seja G um grupo finito e $f : G_1 \to G_2$ um homomorfismo de grupos. Então $|Im(f)|$ é um divisor de $|G_1|$*

Prova. Observemos que, do Teorema 2.10,

$$G_1/N(f) \text{ é isomorfo a } Im(f)$$

isso implica, por existir uma bijeção entre os conjuntos, que

$$|G_1/N(f)| = |Im(f)|.$$

Como, do Teorema de Lagrange,

$$|G_1/N(f)| = \#(G_1 : N(f)) = \frac{|G_1|}{|N(f)|}$$

portanto,

$$|G_1| = |N(f)||Im(f)|, \text{ e } |Im(f)| \text{ divide } |G_1|.$$

Capítulo 3

Homomorfismos de $\mathbb{Z}_m$ em $\mathbb{Z}_n$

Tudo que vimos até o presente momento no nosso estudo teve como propósito nos dar base para conseguirmos demonstrar o seguinte teorema, que envolve o número de homomorfismos de grupos de $\mathbb{Z}_m$ em $\mathbb{Z}_n$.

Teorema 3.1. *O número de homomorfismos entre os grupos $\mathbb{Z}_m$ e $\mathbb{Z}_n$ é* $\text{mdc}(m, n)$.

Prova. Seja $f : \mathbb{Z}_m \to \mathbb{Z}_n$ um homomorfismo. É importante observar que sempre existe, ao menos um homomorfismo de G_1 em G_2, para quaisquer grupos dados, graças ao Exemplo 2.18.

Pelo Corolário 2.3, observemos que a ordem da imagem de f divide m, pois $m = |\mathbb{Z}_m|$.

Por outro lado, $Im(f) < \mathbb{Z}_n$, pela Proposição 2.5, item (iii), e pelo Teorema de Lagrange, visto que $n = |\mathbb{Z}_n|$, a ordem da imagem divide n.

Seja $k = |Im(f)|$, pelo exposto acima, k é um divisor de $\text{mdc}(m, n)$. Além disso, como k é um divisor de n, pelo Teorema 2.6, $\mathbb{Z}_n$ tem um subgrupo único de ordem k e tal subgrupo, pelo Corolário 2.2, tem $\varphi(k)$ geradores.

Como f é homomorfismo, temos:

$$f(\overline{a}) = \underbrace{f(\overline{1} + \overline{1} + ... + \overline{1})}_{a-vezes} = a.f(\overline{1}), \forall \overline{a} \in \mathbb{Z}_m.$$

Portanto, para determinar f é suficiente mapear $\overline{1}$ para o gerador de um subgrupo H de $\mathbb{Z}_n$ que, como vimos, tem $\varphi(k)$ geradores.

Assim, a quantidade de homomorfismos de $\mathbb{Z}_m$ em $\mathbb{Z}_n$ é exatamente

$$\sum_{k|mdc(m,n)} \varphi(k).$$

Por outro lado, segue da Proposição 2.3 que

$$\sum_{k|mdc(m,n)} \varphi(k) = \text{mdc}(m,n)$$

Logo, o número de homomorfismo de $\mathbb{Z}_m$ em $\mathbb{Z}_n$ é igual ao $\text{mdc}(m,n)$.

3.1 Consequências imediatas

1) Se m e n forem números primos entre si, então pelo Teorema 3.1 temos apenas um homomorfismo de $\mathbb{Z}_m$ em $\mathbb{Z}_n$. E, pelo Exemplo 2.18, temos que tal homomorfismo é:

$$\begin{array}{rccc} f: & \mathbb{Z}_m & \to & \mathbb{Z}_n \\ & \overline{a} & \to & f(\overline{a}) = \overline{0} \end{array}$$

2) Se $m = 2k, k \in \mathbb{N}$, então:

$$f : \mathbb{Z}_m \to \mathbb{Z}_2$$

é homomorfismo, se e somente se,

$$f(\overline{a}) = \overline{0}, \text{ para todo } \overline{a} \in \mathbb{Z}_m$$

isto é,

$$Im(f) = \{\overline{0}\}$$

ou,

$$f(\overline{2r+1}) = \overline{1} \text{ e } f(\overline{2r}) = \overline{0} \text{ para todo } r$$

e, nesse caso,

$$Im(f) = \mathbb{Z}_2.$$

Considerações Finais

O estudo de homomorfismo de grupos de $\mathbb{Z}_m$ em $\mathbb{Z}_n$ nos propiciou um rico itinerário que englobou desde os conceitos de teoria dos números até a parte da álgebra que estuda os grupos. Embora o que vimos até aqui não seja nada inédito na matemática, esse estudo nos mostrou um resultado interessante sobre homomorfismo de grupos, especificamente os homomorfismos de $\mathbb{Z}_m$ em $\mathbb{Z}_n$. O teorema que é base para desse trabalho de conclusão de curso não é visto no componente curricular no qual os conteúdos vistos aqui são ministrados e seria interessante que tal teorema e suas aplicações fossem incorporados na grade curricular de tal componente.

Referências Bibliográficas

[1] BOURBAKI, N.**Elements d'Histoire des Mathematiques**. Hermann, 1969.

[2] CHANDLER, B.; MAGNUS W.;**The History of Combinatorial Group Theory**: A Case Study in the History of Ideas. Springer-Verlag, 1982.

[3] GAUSS, C.F.**Disquisitiones Arithmeticae**.Lipsiae. 1801;

[4] GORENSTEIN, D.**Finite Simple Groups**: An Introduction to Their Classification. Plenum Press. 1982.

[5] KLEIN, F.**A Comparative Review of Recent Researches in Geometry**. 1872;

[6] GONÇALVES, ADILSON.**Introdução a álgebra**. 5.ed. Rio de Janeiro: IMPA, 2012;

[7] JOSEPH, A. GALLAN; JAMES VAN BUSKIRK.**The number of homomorphisms from $\mathbb{Z}_m$ into $\mathbb{Z}_n$**.Mathematical Association of America.Disponivel em: <http://www.jstor.org/stable/2322360>

[8] LAGRANGE, J.L. **Reflexions sur la resolution algebrique des equations**. 1770;

[9] KLEINER, ISRAEL.**The Evolution of Group Theory: A Brief Survey**. Taylor E Francis, Ltd. on behalf of the Mathematical Association of America. Disponível em: < https://www.jstor.org/stable/2690312>

[10] MAIER, RUDOLF R.**Teoria dos números. Texto de aula**. Brasilia. 2005;

[11] NASCIMENTO, MAURI CUNHA DO; FEITOSA, HÉRCULES DE ARAUJO. **Elementos da Teoria dos Números**. São Paulo. 2013.

[12] TARWATER , J.; WHITE, J. T. HALL, C ; MOORE, M. E.**American Mathematical Heritage**: Algebra and Applied Mathematics. Texas Tech. Press, 1981.

[13] TARWATER , J.; WHITE, J. T; MILLER, J. D. **The rise of modem algebra to 1936**. in Men and Institutions in American Mathematics, Texas Tech. Press, 1976, pp. 41-63.

[14] **The Classification of Finite Simple Groups**. Plenum Press, 1983.

[15] VIEIRA, VANDEBERG LOPES.**Álgebra abstrata para licenciatura**. Campina Grande: EDUEPB, 2013;

[16] VIEIRA, VANDEBERG LOPES.**Um curso Básico em Teoria dos Números**. Campina Grande: EDUEPB, 2015;