Universidade Federal de Mato Grosso
Instituto de Ciências Exatas e da Terra
Departamento de Matemática

Sobre Grupos Abelianos Finitamente Gerados

André Luiz Pereira Zotti
Mestrado Profissional em Matemática: PROFMAT/SBM

Orientadora: **Profª. Dra. Eunice Cândida Pereira Rodrigues**

Trabalho financiado pela Capes

Cuiabá - MT
26 de abril de 2017

Sobre Grupos Abelianos Finitamente Gerados

Este exemplar corresponde à redação final da dissertação, devidamente corrigida e defendida por André Luiz Pereira Zotti e aprovada pela comissão julgadora.

Cuiabá, 26 de abril de 2017.

Profª. Dra. Eunice Cândida Pereira Rodrigues
Orientadora

Banca examinadora:

Prof. Dra. Eunice Cândida Pereira Rodrigues
Prof. Dra. Ivonildes Ribeiro Martins Dias
Prof. Dr. Clayton Eduardo Lente da Silva

Dissertação apresentada ao curso de Mestrado Profissional em Matemática – PROFMAT, da Universidade Federal de Mato Grosso, como requisito parcial para obtenção do título **de Mestre em Matemática**.

Dados Internacionais de Catalogação na Fonte.

Z89s Zotti, André Luiz Pereira.
Sobre Grupos Abelianos Finitamente Gerados / André Luiz Pereira Zotti. -- 2017
xi, 42 f. ; 30 cm.

Orientadora: Eunice Cândida Pereira Rodrigues.
Dissertação (mestrado profissional) - Universidade Federal de Mato Grosso, Instituto de Ciências Exatas e da Terra, Programa de Pós-Graduação em Matemática, Cuiabá, 2017.
Inclui bibliografia.

1. Proposta pedagógica. 2. Ensino de matemática. 3. Grupos abelianos. I. Título.

Ficha catalográfica elaborada automaticamente de acordo com os dados fornecidos pelo(a) autor(a).

Dissertação de Mestrado defendida em 31 de março de 2017 e aprovada pela banca examinadora composta pelos Professores Doutores

---

Prof[a]. Dra. Eunice Cândida Pereira Rodrigues

Prof[a]. Dra. Ivonildes Ribeiro Martins Dias

Prof. Dr. Clayton Eduardo Lente da Silva

Aos estudiosos da Matemática que anseiam em contribuir para a melhoria da educação, relembro a frase atribuída a Pitágoras: Não é livre quem não consegue ter domínio sobre si mesmo.

Agradecimentos

A Deus pela vida. A minha família pelo amor, apoio e pela compreensão nestes últimos dois anos, em especial aos meus pais Antônio e Sônia pela educação dada a mim, meus irmãos Pedro e Ticciana pelo carinho , à minha filha Bianca que é a luz do meu caminho ,à minha esposa Leonice pela paciência nos momentos difíceis. Agradeço ainda aos meus professores, especialmente a minha orientadora Professora Eunice, pelas contribuições e pela experiência partilhada no desenvolvimento deste trabalho. Gostaria de agradecer aos amigos Candido, Dalcimar, Marcos Terra e Rorger pelos momentos compartilhados nas idas e vindas de Cuiabá, bem como pela amizade construída. Os meus agradecimentos também a CAPES (Coordenação de Aperfeiçoamento de Pessoal de Nível Superior) pela concessão da bolsa durante todo o período de realização deste mestrado. Finalmente os meus agradecimentos aos profissionais da Escola Estadual Dom Aquino Correa bem como aos colegas da Escola Municipal Anfilófio de Souza Campos pelos dois anos de paciência e colaboração. Muito obrigado a todos.

"O processo de explicação do fracasso escolar tem sido uma busca de culpados .... Os educadores, todos nós, precisamos não encontrar culpados mas encontrar as formas eficientes de ensino e aprendizagem em nossa sociedade. "

Resumo

Em Matemática, Teoria dos Grupos é o ramo que estuda as estruturas algébricas chamadas de grupos. Os métodos da teoria dos grupos influenciaram fortemente vários ramos da Álgebra. Na análise combinatória, a noção de grupo e de permutação de um grupo é frequentemente utilizado para simplificar a contagem de um conjunto de objetos. A compreensão da teoria de grupos é fundamental na Física, onde é utilizada para descrever as simetrias que as leis da Física devem obedecer. Em Química, grupos são utilizados para classificar estruturas cristalinas e as simetrias das moléculas. Diante do exposto, neste trabalho faz -se um estudo envolvendo conceitos e propriedades da Teoria dos Grupos, com foco em grupos abelianos finitamente gerados. Após apresentado a teoria envolvendo os citados grupos, propõem-se algumas atividades didáticas para serem trabalhadas com os discentes do ensino médio. Tais atividades enfatizam algumas propriedades abordadas no ensino médio. O suporte teórico está alicerçado em autores como (GARCIA, 2003), (GONÇALVES, 2008) e (FRALEIGH, 2000).

Palavras chave: Ensino de matemática, Proposta pedagógica, Grupos abelianos.

Abstract

The Group Theory is a branch of Mathematics which studies Algebraic Structures called Group. The methods of Group Theory have strongly influenced various branches of algebra. In Combinatorial Analysis the notion of permutation group from a group is a commonly used to simplify the counting of Objects Set. The Group Theory understanding is key role in Physics. It is used to describe symmetries which Physical Laws must obey. In Chemistry, groups are used to classify crystalline structures and molecules symmetry. In view of what has been exposed here, the objective of the present work was to realize a study on concepts and properties of Group Theory with special reference to Generated finitely abelian Groups. After theories on groups referred above it was proposed some didactic activities to be developed by high school students. Such activities emphasized some properties discussed in high school. The theoretical background was based in following authors (GARCIA, 2003), (GONÇALVES, 2008) and (FRALEIGH, 2000).

Keywords: Mathematics Teaching, Pedagogical Proposal, Abelian Groups.

Sumário

Lista de Figuras

Introdução

Em nossa sociedade, o conhecimento matemático é necessário em grande diversidade de situações, seja no apoio a outras áreas do conhecimento, como instrumento para lidar com situações da vida cotidiana, ou ainda, como forma de desenvolver habilidades de pensamento. Os Parâmetros Curriculares Nacionais do Ensino Médio, (MEC (2002)), sinalizam que a Matemática deve ser compreendida como uma parcela de conhecimento humano essencial a formação de todos os jovens, a qual contribui na construção de uma visão de mundo, para ler e interpretar a realidade e para desenvolver capacidades que deles serão exigidas ao longo da vida social e profissional. Além disso, relatam que aprender matemática no ensino médio deve ir além da memorização dos resultados dessa ciência e que a aquisição de conhecimento matemático deve estar vinculado ao domínio de um saber pensar matemático. O professor tem importância fundamental no processo de oportunizar uma melhor aprendizagem aos discentes do ensino médio, mostrando por exemplo, as demonstrações de algumas propriedades inseridas na Álgebra, Geometria, Matemática Financeira, etc. No caso da Álgebra, apesar de conter um certo formalismo em sua linguagem e necessitar da utilização de procedimentos não muito simples, exigindo um maior grau de abstração, é importante lembrar que a forma do professor trabalhar conteúdos matemáticos deve abranger também a linguagem formal. Por exemplo, para os alunos torna-se mais fácil, memorizar que menos com menos é mais do que entender a justificativa algébrica do porque $-(-x) = x$ para $\forall \in \mathbb{R}$.

Diante da abordagem supracitada, o foco neste trabalho é fazer um estudo sobre alguns conceitos e resultados da Teoria de Grupos, especificamente sobre os grupos abelianos finitamente gerados, visando no final deste, apresentar sugestões aos docentes do ensino médio para que os mesmos possam ter um olhar não apenas informal ao trabalharem às demonstrações de algumas propriedades que são imprescindíveis no ensino aprendizagem. Para atingirmos o objetivo proposto, organizamos este trabalho como segue.

No primeiro capítulo introduzimos conceitos e resultados que fazem parte da literatura usual da Teoria de Grupos e que serão necessários para o desenvolvimento de nosso trabalho.

Na segunda parte fizemos uma abordagem sobre uma apresentação de grupo, enfatizando a definição de palavra, gerador, relação e relatores.

No terceiro capítulo, abordamos o conceito de grupos abelianos livres e alguns resultados, e por fim enunciamos, demonstramos e aplicamos o Teorema Fundamental para Grupos Abelianos Finitamente Gerados.

Já no último capítulo, apresentamos algumas atividades, com intuito de que sirvam como propostas para o ensino da Matemática básica.

Capítulo 1

Preliminares

Neste capítulo, mencionaremos alguns conceitos e propriedades da Teoria dos Números[1] e da Teoria de Grupos[2] importantes para o desenvolvimento dos capítulos subsequentes. Omitiremos às demonstrações de quase todos os resultados que podem ser encontradas em Fraleigh (2003); Garcia e Lequain (2003); Hefez (2011).

1.1 Relação de equivalência

Nesta seção faremos uma breve revisão, introduzindo a noção de produto cartesiano e de relação de equivalência bem como apresentaremos alguns exemplos e contra-exemplos envolvendo os referidos conceitos. Vale ressaltar que relação de equivalência é fundamental para os matemáticos entenderem certas classes de objetos. Como por exemplo, temos a congruência, que será explicitada na seção 1.4.

Definição 1.1.1 *Dados dois conjuntos X e Y, é chamado de relação de X em Y todo subconjunto S do produto cartesiano $X \times Y$.*

Exemplo 1.1.1 *Considerando X o conjunto dos números inteiros e Y o conjunto dos números naturais, então o conjunto $S = (x, y) \in \mathbb{Z} \times \mathbb{N}/x^2 + y^2 = 25\}$ é uma relação de $\mathbb{Z}$ em $\mathbb{N}$, onde os elementos são: $S = \{(-5, 0), (-4, 3), (-3, 4), (0, 5), (3, 4), (4, 3), (5, 0)\}$. Graficamente, percebemos que este produto cartesiano possui pontos da circunferência de centro O (0, 0) e raio 5, dada pela equação de circunferência $x^2 + y^2 = 25$. A relação S de X em Y consiste em 7 pontos sobre ela.*

Vale ressaltar que podemos definir uma relação S de um conjunto X nele mesmo. Neste caso, dizemos que S é uma relação sobre X.

Uma relação S sobre X pode ser uma relação de equivalência, conforme segue.

[1] É o ramo da Matemática que estuda propriedades dos números em geral, e em particular dos números inteiros.

[2] É o ramo da Matemática que estuda as estruturas algébricas chamadas de grupos.

Definição 1.1.2 *Dizemos que a relação S sobre X é uma relação de equivalência em X, se ela cumpre as seguintes condições:*

i)$(x, x) \in S$*, para todo* $x \in X$*;*

ii) Se x *e* y *são elementos de* X *tais que* $(x, y) \in S$*, então* $(y, x) \in S$*;*

iii) Se x*,* y *e* z *são elementos de* X *tais que* $(x, y) \in S$ *e* $(y, z) \in S$*, então* $(x, z) \in S$*.*

Portanto, para que uma relação seja de equivalência, ela tem que satisfazer as propriedades denominadas reflexiva, simétrica e transitiva, respectivamente.

Exemplo 1.1.2 *Seja S uma relação sobre X, sendo $X = \{$triângulos que possuem a mesma área $K\}$. A relação S é de equivalência. De fato, se o triângulo a tem área K é claro que ele possui a mesma área que ele mesmo, isto é, aSa, $\forall a \in K$. Com o triângulo a tendo a mesma área do triângulo b, então o triângulo b tem a mesma área do triângulo a, ou seja, aSb e bSa. Neste caso, verificamos que em S vale a propriedade simétrica. Sabendo que o triângulo a possui a mesma área que o triângulo b, se b possuir a mesma área que o triângulo c, então o triângulo a possui a mesma área que o triângulo c, especificamente tem-se que, aSb e bSc então aSc, ou seja, vale a propriedade transitiva. Como a relação S é reflexiva, simétrica e transitiva, então S é uma relação de equivalência sobre X.*

Exemplo 1.1.3 *Seja X o conjunto que reúne todos os parentes de uma família, até terceiro grau e S a relação de irmãos de X. Se a pertence ao conjunto X, então a não é irmão do próprio a. Sabendo que a é irmão de b, logo b é irmão de a, tomando a irmão de b e b irmão de c, podemos ter a irmão de c, todavia pensando no caso de c ser o próprio a, então a não pode ser irmão de a. Logo S não é uma relação de equivalência em A.*

Exemplo 1.1.4 *A seguir verificaremos se a relação $S = \{(x, y) \in \mathbb{Z} \times \mathbb{Z} \ / \ x - y$ é par $\}$ é de equivalência, isto é, se a relação cumpri as propriedades reflexiva, simétrica e transitiva. Vejamos:*

i) Para qualquer $x \in \mathbb{Z}$, temos que x se relaciona com x, ou seja, $x - x = 0$, e 0 é um número par, daí temos que S é reflexiva;

ii) Suponhamos que $(x, y) \in S$ para $x, y \in \mathbb{Z}$, então $x - y$ é par, como o oposto de qualquer inteiro também é par então $-(x - y)$ é par e consequentemente $y - x$ é par, portanto $(y, x) \in S$, ou seja S é simétrica;

iii) Suponhamos que $(x, y) \in S$ e $(y, z) \in S$ para $x, y, z \in \mathbb{Z}$, assim temos que $x-y$ e $y-z$ são pares, como a soma de dois números pares é par, então $(x-y)+(y-z) = x - z$ é um número par, portanto $(x, z) \in S$, o que mostra que S é transitiva. Logo S é uma relação de equivalência sobre $\mathbb{Z}$.

Exemplo 1.1.5 *Considerando agora a relação dada por $S = \{(x, y) \in \mathbb{Z}^* \times \mathbb{Z}^* / mdc(x, y) = 1\}$, verificamos que esta relação é simétrica, mas não é reflexiva pois, $mdc(6, 6) =$*

$6 \neq 1$. *Além disso não é transitiva, porque* $mdc(16, 21) = 1 emdc(21, 26) = 1$, *porém* $mdc(16, 26) = 2 \neq 1$. *Portanto concluímos que S não é uma relação de equivalência.*

Observe que na relação dada no Exemplo 1.1.4, isto é, S = $\{(x, y) \in \mathbb{Z} \times \mathbb{Z} / x - y$ é par $\}$ podemos encontrar todos os x de $\mathbb{Z}$ que se relacionam com 5, isto é, $xS5$. Especificamente, podemos obter $x \in \mathbb{Z}$ tal que $x - 5 = 2k, k \in \mathbb{Z}$. Portanto, x pertence ao conjunto $\{\ldots -5, -3, -1, 1, 3, 5, \ldots\}$. O citado conjunto é denotado por $\overline{x}$, denominado classe de equivalência de x segundo a relação S.

1.2 Classe de equivalência

Definição 1.2.1 *Dada uma relação de equivalência S sobre um conjunto X, chamamos de classe de equivalência de* $a \in X$ *segundo a relação S, que denotamos* $\overline{a}$, *o conjunto* $\{x \in X / xSa\}$.

Definição 1.2.2 *O conjunto formado por todas as classes de equivalência módulo S, é chamado de conjunto quociente de X por S e denotamos por* X/S.

Exemplo 1.2.1 *Vimos que* $S = \{(x, y) \in \mathbb{Z} \times \mathbb{Z} / x - y$ *é par* $\}$ *é uma relação de equivalência sobre* $\mathbb{Z}$ *(Exemplo 3). Assim, inicialmente para todo* $x \in \mathbb{Z}$, *existe* $\overline{x} \in \mathbb{Z}/S$. *Em particular, para* $x = 0$ *temos que* $\overline{0} = \{\ldots, -2, 0, 2, 4, \ldots\}$. *Além disso, para* $x = 2$ *segue que* $\overline{2} = \{\ldots, -2, 0, 2, 4, \ldots\}$.

Após os cálculos das classes $\overline{0}$ e $\overline{2}$ podemos concluir que $\forall x \in \mathbb{Z}$, tal que x é par, segue $\overline{x} = \overline{0}$. Ainda no citado exemplo podemos encontrar as classes $\overline{1}, \overline{3}$, ou seja, $\overline{1} = \{\ldots, -5, -3, -1, 1, 3, 5, \ldots\}$ e $\overline{3} = \{\ldots, -5, -3, -1, 1, 3, 5, \ldots\}$.

De modo geral, se $x \in \mathbb{Z}$ é ímpar, segue que $\overline{x} = \overline{1}$. Desta forma, temos que o conjunto de todas as classes de equivalência em $\mathbb{Z}$ terá apenas dois conjuntos distintos, $\overline{0}$ e $\overline{1}$. Assim, o conjunto quociente de $\mathbb{Z}$ por S, é dado por $\mathbb{Z}/S = \{\overline{0}, \overline{1}\}$. O teorema a seguir estabelece condições para que duas classes de equivalência sejam iguais. Omitiremos a demonstração do mesmo, a qual poderá ser encontrada em [2].

Teorema 1.2.1 *Seja S uma relação sobre X e* $a, b \in X$. *Então as seguintes proposições são equivalentes:*

i) $(a, b) \in S$;
ii) $a \in \overline{b}$;
iii) $b \in \overline{a}$;
iv) $\overline{a} = \overline{b}$.

1.3 Partição de um conjunto

Definição 1.3.1 *Seja X um conjunto não vazio. Diz-se que uma classe P de subconjuntos não vazios de X é uma partição de X se:*

i) Dois membros quaisquer de P são iguais ou são disjuntos;

ii) A união dos membros de P é igual a X.

Exemplo 1.3.1 *Seja $P = \{(-\infty, 3), [3, 4), [4, 5], (5, \infty)\}$ é uma partição de $\mathbb{R}$, pois os seus membros são dois a dois disjuntos e, além disso, a união deles é igual a $\mathbb{R}$.*

A seguir apresentaremos dois teoremas que relacionam conjunto quociente e partição. As suas demonstrações podem ser encontradas em [2].

Teorema 1.3.1 *Se S é uma relação de equivalência sobre X, então o conjunto quociente X/S é uma partição de X.*

Teorema 1.3.2 *Se P é uma partição de X, então existe uma relação S de equivalência sobre X de modo que $X/S = P$.*

1.4 Relação de congruência módulo m

A teoria das congruências é um vasto campo da Matemática, inserido na Teoria dos Números. Abrange propriedades e teoremas cujo entendimento e aplicabilidade variam dos níveis mais básicos aos mais avançados.

Em Matemática a aritmética modular (chamada também de aritmética do relógio) é um sistema de aritmética para inteiros, onde os números voltam, quando atingem um certo valor, o módulo. O matemático Euler foi o pioneiro na abordagem de congruência por volta de 1750, quando ele introduziu a ideia de congruência módulo um número $m \in \mathbb{N}$ com $m > 1$. Vale ressaltar que a aritmética modular foi desenvolvida posteriormente por Carl Friedrich Gauss em seu livro Disquisitiones Arithmeticae, publicado em 1801.

Definição 1.4.1 *Sejam a e b dois números inteiros e m um número inteiro positivo maior que 1. Dizemos que a e b são congruentes módulo m se o m divide a diferença $a - b$. Quando os inteiros a e b são congruentes módulo m, escrevemos:*

$$a \equiv b \; mod \; m.$$

Exemplo 1.4.1 *Veja que $21 \equiv 13$ mod 2 pois, $2|(21 - 13)$ e 21 não é congruente a 13 mod3, pois 3 não divide $(21 - 13)$. Dizer que $m|(a - b)$ é equivalente a dizer que os restos da divisão de a por m e b por m são iguais.*

Exemplo 1.4.2 *Um exemplo envolvendo o nosso cotidiano, refere-se aos relógios analógicos que trata-se de um caso de uma congruência módulo* 12*. Note que* 13 *horas é congruente a* 1 *hora, no módulo* 12*. Ambos divididos por* 12*, deixam resto* 1 *e que* 17 *horas é congruente a* 5 *horas, módulo* 12*. Tanto* 17*, como* 5*, divididos por* 12*, deixam resto* 5*, e assim, sucessivamente.*

$$1 \equiv 13 \equiv 25 \; mod \; 12$$
$$5 \equiv 17 \equiv 29 \; mod \; 12$$

Assim, as horas marcadas num relógio analógico constituem também um caso clássico de congruência, nesse caso com módulo 12*.*

A congruência módulo m é uma relação de equivalência em $\mathbb{Z}$.

De fato, considere $S = \{(a, b) \in \mathbb{Z} \times \mathbb{Z}/a \equiv b \; mod \; m\}$. Então S é uma relação de equivalência sobre $\mathbb{Z}$. Uma vez que:

i) Temos a $\equiv a \; mod \; m$, pois $m|(a - a) = 0$. Portanto é reflexiva;

ii) Se $a \equiv b \; mod \; m$, então $b \equiv a \; mod \; m$, pois, como m $|(a - b)$ então m divide o oposto, e daí $m|(b - a)$. Logo vale a propriedade simétrica;

iii) Se $a \equiv b \; mod \; m$ e $b \equiv c \; mod \; m$, então $a \equiv c \; mod \; m$, pois como $m|(a - b)$ e $m|(b - c)$, então m divide a soma, daí $m|[(a - b) + (b - c)]$, assim $m|(a - c)$, portanto S é transitiva.

Logo, pela Definição 2, S é uma relação de equivalência sobre $\mathbb{Z}$.

Definição 1.4.2 *A relação de congruência módulo m sobre $\mathbb{Z}$ determina um conjunto quociente $\mathbb{Z}/S$ que é indicado por $\mathbb{Z}_m$, ou seja, $\mathbb{Z}_m$ é o conjunto de todas as classes de equivalência sobre S.*

A seguir mostraremos que em $\mathbb{Z}_m$ existem exatamente m elementos distintos.

Proposição 1.4.1 *O conjunto $\mathbb{Z}_m$ tem exatamente m elementos, isto é,*

$$\mathbb{Z}_m = \{\overline{0}, \overline{1}, \overline{2}, \overline{3}, \ldots, \overline{m-1}\}.$$

Prova 1.4.1 *Dado $a \in \mathbb{Z}$, efetuamos a divisão euclidiana de a por m. Sendo q o quociente e r o resto dessa divisão, temos: $a = mq + r$, como $0 \leq r < m$ logo, $a - r = mq$, isto é, $a \equiv r \; mod \; m$, ou ainda, $\overline{a} = \overline{r}$. Como $r \in \{0, 1, 2, 3, \ldots, m - 1\}$, temos que $\overline{a} \in \mathbb{Z}_m \Rightarrow \overline{a} \in \{\overline{0}, \overline{1}, \overline{2}, \overline{3}, \ldots, \overline{m-1}\}$. Suponhamos agora que existam duas classes iguais em $\{\overline{0}, \overline{1}, \overline{2}, \overline{3}, \ldots, \overline{m-1}\}$, isto é:*
$\overline{r} = \overline{s}$ com $0 \leq r < s < m$. Neste caso, temos: $\overline{r} = \overline{s} \Rightarrow r \equiv s \; mod \; m \Rightarrow m|(s - r)$. Como $0 < s - r < m$, então isto é impossível. Logo, o número de elementos de $\mathbb{Z}_m$ é exatamente m.

1.5 Operações em $\mathbb{Z}_m$

Vimos que uma aplicação da aritmética modular está relacionado com os ponteiros do relógio, no qual o dia é dividido em dois períodos de 12 horas cada. Por exemplo, se agora são 7 horas, então quantas horas serão daqui 8 horas ? A adição usual sugere que o tempo futuro deveria ser $7+8=15$, mas esta é a resposta errada por que o relógio "volta pra trás" a cada 12 horas, não existe 15 horas no relógio de ponteiro. Da mesma forma, se o relógio começa em $12:00$ (meio dia) e passam 21 horas , então a hora será $9:00$ do dia seguinte, em vez de $33:00$. Como o número de horas começa de novo depois que atinge 12, essa aritmética é chamada aritmética módulo 12. E 12 é congruente não só a 12 mesmo, mas também a 0, assim a hora chamada $12:00$ pode também ser chamada $0:00$, pois $0 \equiv 12 \ mod \ 12$.

Definição 1.5.1 *Sejam $\overline{x}$ e $\overline{y}$ elementos do conjunto $\mathbb{Z}_m$, assim a operação $\overline{x}+\overline{y}$, chamada adição módulo m , é o resto da divisão $x+y$ por m, ou seja $\overline{x}+\overline{y}=\overline{x+y}$.*

Exemplo 1.5.1 *Sejam $\overline{3},\ \overline{4}\ \in \mathbb{Z}_5$ então $\overline{3}+\overline{4}$ é um elemento em $\mathbb{Z}_5$, o qual é igual a $\overline{7}=\overline{2}$.*

A tabela abaixo, chamada de tábua da adição módulo 5, mostra a soma de todos elementos de $\mathbb{Z}_5$. Na referida tabela iremos omitir as barras dos elementos de $\mathbb{Z}_5$, para não sobrecarregá-la.

+	0	1	2	3	4
0	0	1	2	3	4
1	1	2	3	4	0
2	2	3	4	0	1
3	3	4	0	1	2
4	4	0	1	2	3

Tabela1.1: Adição em $\mathbb{Z}_5$

Definição 1.5.2 *Sejam $\overline{x}$ e $\overline{y}$ elementos do conjunto $\mathbb{Z}_m$, a operação $\overline{x}.\overline{y}$, chamada de multiplicação módulo m, é o resto da divisão $x.y$ por m, ou seja, $\overline{x}.\overline{y}=\overline{x.y}$.*

Exemplo 1.5.2 *Veja que $\overline{3}.\overline{2}$, é um elemento de $\mathbb{Z}_4$, sendo $\overline{6}=\overline{2}$, pois a divisão de 6 por 4 deixa resto 2.*

Assim, construindo a tábua da multiplicação módulo 4, com omissão das barras, obtemos:

.	0	1	2	3
0	0	0	0	0
1	0	1	2	3
2	0	2	0	2
3	0	3	2	1

Tabela1.2: Multiplicação em $\mathbb{Z}_4$

Um fato a observar é que nem todos os elementos de $\mathbb{Z}_m^*$, possui inverso. Um exemplo pode ser visto em $\mathbb{Z}_4^* = \{\overline{1}, \overline{2}, \overline{3}\}$, pois $\overline{2} \in \mathbb{Z}_4^*$,no entanto $\overline{2}$ não tem inverso em $\mathbb{Z}_4^*$.

A seguir exibiremos um resultado que estabelece condições para que $\overline{a} \in \mathbb{Z}$ seja invertível.

Proposição 1.5.1 *Sejam a e m inteiros, com $m \geq 2$. Então:*
i) $\overline{a}$ é elemento invertível de $\mathbb{Z}_m^*$ se, e somente se a e m são primos entre si, ou seja, se, e somente se $mdc(a, m) = 1$.
ii) Se a e m são primos entre si, existem inteiros r e s satisfazendo $ra + sm = 1$. Nesse caso, o inverso de $\overline{a}$ em $\mathbb{Z}_m^*$ é dado por $\overline{a}^{-1} = \overline{r}$.

Prova 1.5.1 *Suponhamos que $\overline{a}$ é invertível em $\mathbb{Z}_m^*$. Então existe $\overline{b} \in \mathbb{Z}_m^*$, com $b \in \mathbb{Z}$, satisfazendo $\overline{a}.\overline{b} = \overline{1}$. Daí, temos que $\overline{ab} = \overline{1}$ e pelo Teorema 1 segue que $ab \equiv 1 mod m \Rightarrow ab - 1 = mq$, para algum inteiro q. Logo $ab - mq = 1$ e portanto $mdc(a, m) = 1$, ou seja, a e m são primos entre si.*

Reciprocamente, se a e m são primos entre si, então $ra + sm = 1$ para certos inteiros r e s. Daí, $\overline{ra + sm} = \overline{1} \Rightarrow \overline{ra} + \overline{sm} = 1 \Rightarrow \overline{r}.\overline{a} + \overline{s}.\overline{m} = \overline{1}$. Como $\overline{m} = \overline{0}$, chegamos a $\overline{r}.\overline{a} = \overline{1}$, e portanto a é invertível, já que a multiplicação em $\mathbb{Z}_m$ é comutativa. Sendo assim, provamos simultaneamente as duas propriedades enunciadas.

Exemplo 1.5.3 *Note que em $\mathbb{Z}_7^*$ os elementos $\overline{3}$ e $\overline{5}$ são invertíveis (Proposição 2, item i). Além disso, como $\overline{3}.\overline{5} = \overline{5}.\overline{3} = \overline{1}$ então $\overline{3}$ é o inverso de $\overline{5}$ e vice versa.*

Vale ressaltar, por exemplo, que em $\mathbb{Z}_4^* = \{\overline{1}, \overline{2}, \overline{3}\}$ o elemento $\overline{2} \in \mathbb{Z}_4^*$ não tem inverso no referido conjunto.

A seguir apresentaremos uma função que nos auxilia na obtenção dos elementos inversíveis em $\mathbb{Z}_m^*$.

1.6 Função φ de Euler e a congruência módulo m

A função representada por φ(m) é na Teoria dos Números, definida para um número natural x como sendo igual à quantidade de números menores ou igual a x coprimos com respeito a ele.

Definição 1.6.1 *Dado $m \in \mathbb{N}$, designaremos $\varphi(m)$ a quantidade de números naturais entre 0 e $m - 1$ que são primos com m. Isto define uma importante função, chamada de função φ de Euler:*

$$\varphi : \mathbb{N} \to \mathbb{N} \text{ tal que } \varphi(m) = \{n \in \mathbb{N} / (m, n) = 1 \;\; 1 \leq n < m\}.$$

Exemplo 1.6.1 *Veja que* $\varphi(8) = 4$ *uma vez que* $1, 3, 5$ *e* 7 *são co-primos de* 8*. Um outro exemplo,* $\varphi(1) = 1$ *pois* $mdc(1, 1) = 1$*.*

A função $\varphi(m)$ é importante principalmente porque fornece o tamanho do grupo multiplicativo de inteiros módulo m.

Corolário 1.6.1 *Pela definição, temos que* $\varphi(m) \leq m - 1$*, além disso:*
i) $\varphi(m) = m - 1$ *se, e somente se, m é primo;*
ii) Se $m = pq$*, com p e q primos, então* $\varphi(m) = \varphi(pq) = \varphi(p).\ \varphi(q) = (p - 1)(q - 1)$*;*
iii) Se $n = p^k$*, isto é, se n é potência de um primo p, então* $\varphi(n) = \varphi(p^k) = p^k - p^{k-1}$*.*

Exemplo 1.6.2 *Pautado no corolário anterior, segue:*
i) $\varphi(7) = 6 = 7 - 1$*;*
ii) $\varphi(21) = 12 = 2.6 = \varphi(3).\varphi(7)$*;*
iii) $\varphi(8) = 4 = 8 - 4 = 2^3 - 2^{3-1}$*.*

Teorema 1.6.1 *(Euler): Sejam* $m,\ a \in \mathbb{N}$ *com* $m > 1$ *e* $mdc(a, m) = 1$*. Então,*

$$a^{\varphi(m)} \equiv 1\ mod\ m \tag{1.1}$$

O Teorema de Euler pode ser usado para determinar o inverso de alguns elementos $\overline{a} \in \mathbb{Z}_m^*$, pois da Equação 3.1.6 segue que

$$a^{-1} \equiv a^{\varphi(m)-1} mod\ m. \tag{1.2}$$

Exemplo 1.6.3 *Por meio da Equação1.2 temos que o inverso de* $\overline{7} \in \mathbb{Z}_{10}^*$ *pode ser obtido da seguinte maneira:*

$$7^{-1} \equiv 7^{\varphi(10)-1} \equiv 7^{4-1} \equiv 7^3 \equiv 343 \equiv 3\ mod\ 10,$$

ou seja, $\overline{7}^{-1} = \overline{3}$*. De fato,* $\overline{7}.\overline{3} = \overline{3}.\overline{7} = \overline{21} = \overline{1}$*.*

1.7 Grupos

O conceito de grupo, definido abaixo, emergiu do estudo de equações de polinômios, com Évariste Galois na década de 1830. Após contribuições vindas de outros ramos da Matemática, como Teoria dos Números e Geometria, a noção de grupo foi generalizada e se estabeleceu firmemente por volta de 1870. A Teoria dos Grupos moderna

é uma área muito ativa de pesquisa que estuda os grupos em si mesmos. Além das propriedades abstratas, matemáticos estudam as diferentes maneiras em que um grupo pode ser expresso concretamente, tanto de um ponto de vista teórico quanto prático e computacional. Em particular, uma teoria ricamente desenvolvida é a dos grupos finitos, que culminou com a monumental classificação dos grupos simples finitos, completada em 1983.

Definição 1.7.1 *Seja G um conjunto não vazio e*

$$\begin{aligned} * : G &\longrightarrow G \\ (x, y) &\longmapsto x * y \end{aligned}$$

uma operação em G.
Dizemos que G é um grupo em relação a operação $*$ se, e somente se, são verificadas as propriedades $i)$, $ii)$, $iii)$ abaixo:
$i)$ $a * (b * c) = (a * b) * c, \forall\ a,\ b,\ c\ \in G$; (Propriedade associativa)
$ii)$ $\exists\ e\ \in\ G$ tal que $a * e = e * a = a$, $\forall a \in\ G$; (Existência do elemento neutro)
$iii)$ $\forall\ a\ \in\ G$, $\exists\ b\ \in G$ tal que $a * b = b * a = e$; (Existência do simétrico)
Se para um grupo $(G, *)$verifica-se também a propriedade.
$iv)$ $a * b = b * a, \forall a, b \in G$. (Comutativa)
Dizemos que o grupo $(G, *)$ é um grupo abeliano.

O elemento neutro e o simétrico são únicos conforme proposições a seguir.

Proposição 1.7.1 *(Unicidade do elemento neutro).Numa operação binária associativa, o elemento neutro de cada elemento, caso exista, é único.*

Prova 1.7.1 *Suponha que $a * b$ define uma operação binária e temos dois elementos neutros e_1 e e_2. Então temos que $e_2 = e_1 * e_2$ por que e_1 é o elemento neutro, mas $e_2 * e_1 = e_1$ por que e_2 é o elemento neutro. Com $e_2 = e_1 * e_2 = e_2 * e_1 = e_1$, logo $e_1 = e_2$. Assim, não pode haver mais de um elemento neutro.*

Proposição 1.7.2 *(Unicidade do elemento inverso). Numa operação binária associativa o elemento inverso de cada elemento, caso exista, é único.*

Prova 1.7.2 *Suponha que $a * b$ define uma operação binária associativa, com e sendo o elemento neutro. Se b e b'são elementos inversos de a, temos que $b * a = e$ e $a * b' = e$. Assim, $b = b * e = b * (a * b') = (b * a) * b' = e * b' = b'$. Assim, não pode haver mais de um elemento inverso.*

Exemplo 1.7.1 *O conjunto de simetrias do triângulo equilátero, denotado por S_Δ, com a operação de composição é um exemplo de grupo, haja vista que seus elementos são o elemento neutro $R_0 = id$, que corresponde a não rodar nada ou girar um número qualquer de voltas, outro elemento seria uma rotação de 120^0 ($R_{\frac{2\pi}{3}}$) ou 120^0 mais um*

número de voltas, o terceiro elemento é uma rotação de 240^0 ($R_{\frac{4\pi}{3}}$) ou duas rotações de 120^0 que resulta em uma rotação de 240^0, mais um número de voltas. O quarto elemento R_1 é encontrado se fixarmos o primeiro vértice do triângulo efetuando uma translação em que o vértice 2 ocupe a posição do vértice 3 e o vértice 3 assume a posição do vértice 2, o quinto e o sexto elementos são encontrados de forma análoga que correspondem a fixar os vértices 2 e 3 efetuando também uma translação, que denotamos por R_2 e R_3 respectivamente. Note que o elemento neutro pertence ao conjunto G, para cada elemento de G existe um único inverso, e os elementos com os seus respectivos inversos são: neutro com seu inverso sendo o próprio neutro, o inverso de girar 120^0 é girar 240^0 e vice versa, os inversos de R_1, R_2, R_3 são eles mesmos. Uma vez que fixar o vértice 1 e efetuar novamente uma translação, faz com que retornemos na posição inicial. Vale também a propriedade associativa.

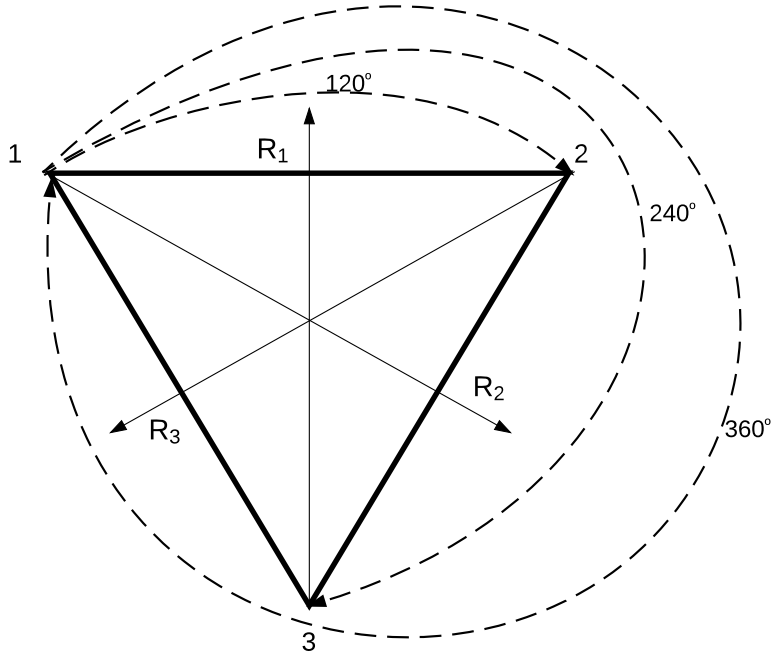

Figura 1.1: Simetria no triângulo equilátero

O grupo supracitado não é abeliano, pois $R_1 o R_2 = R_{2\pi/3} \neq R_2 o R_1 = R_{4\pi/3}$.

Exemplo 1.7.2 *O conjunto dos números inteiros módulo m, com a operação de adição, é um grupo abeliano, representado por* $(\mathbb{Z}_m, +)$.

Em um grupo G existem subconjuntos, não vazios, que também possuem estruturas de grupo, conforme segue.

1.8 Subgrupos

Na Teoria de Grupos, algumas vezes fica muito complicado estudar todas as características de um dado grupo, então podemos estudar e mostrar situações em subgrupos e compreender, em muitos casos, qual o comportamento do grupo maior.

Definição 1.8.1 *Seja $(G, *)$ um grupo. Dizemos que um subconjunto não vazio, $H \subset G$ é um subgrupo de G se, e somente se,*

i) $\forall a, b \in H \Rightarrow a * b \in H$;

ii)$(H, *)$ *também é um grupo.*

Teorema 1.8.1 *Seja H um subconjunto não vazio de um grupo G. Então H é um subgrupo de G se, e somente se, as duas condições seguintes são satisfeitas:*

i) $h_1 * h_2 \in H, \forall h_1,\ h_2 \in H$;

ii) $h^{-1} \in H, \forall h \in H$.

Subgrupos podem ser caracterizados da seguinte forma.

Exemplo 1.8.1 *Usando $G = S_\Delta$, como no Exemplo 14, então $H = \{id, R_{2\pi/3}, R_{4\pi/3}\}$ é um subgrupo de G.*

Exemplo 1.8.2 *O conjunto dos inteiros módulo 4, $\mathbb{Z}_4 = \{\ \overline{0},\ \overline{1},\ \overline{2},\ \overline{3}\ \}$, com a operação adição, possui o subconjunto $H = \{\ \overline{0},\ \overline{2}\ \}$ de $\mathbb{Z}_4$ que é um subgrupo de G.*

Exemplo 1.8.3 *O conjunto dos números inteiros, representados por $\mathbb{Z}$,possui os subgrupos $2\,\mathbb{Z}$, $3\,\mathbb{Z}$, tendo a interseção $6\,\mathbb{Z}$ como subgrupo. Em geral os subgrupos de $\mathbb{Z}$ são da forma $n\,\mathbb{Z}$, $n \in \mathbb{Z}$. Pode ser mostrado que os referidos subgrupos são únicos.*

Existe subgrupo de um dado grupo G que é obtido a partir de um elemento do grupo, isto é, os elementos deste subgrupo podem ser escritos como potências ou múltiplos deste elemento.

1.9 Potências e múltiplos

Definição 1.9.1 *Em um grupo multiplicativo $(G, .)$(grupo em que a operação é a multiplicação que será denotado por . e o simétrico do elemento a será denotado por a^{-1}) com elemento neutro e, dados $x \in G$ e $n \in \mathbb{Z}$, definimos a potência x^n da seguinte forma:*

$$x^n = \begin{cases} x^{n-1}.x, & se\ n \geq 1 \\ e, & se\ n = 0 \\ (x^-1)^n, & se\ n < 0 \end{cases}$$

Pela definição $x^0 = \text{e}$, $x^n = \underbrace{x.x.x.\ldots.x}_{n}$, com n fatores, se $n > 0$ e $x^{-n} = x^{-1}.x^{-1}.x^{-1}.\ \ldots\ .x^{-1}$ com n fatores, se $\text{n} < 0$.

Definição 1.9.2 *Em um grupo aditivo (G, +) (grupo em que a operação é a adição que será denotado por + e o simétrico do elemento a será denotado por $-a$) com elemento neutro 0, dados $x \in G$ e $n \in \mathbb{Z}$, definimos o múltiplo nx da seguinte forma:*

$$nx = \begin{cases} (n-1)x + x, & se\ n \geq 1 \\ 0, & se\ n = 0 \\ (-n)(-x), & se\ n < 0 \end{cases}$$

Pela definição 0x = 0, nx = $\underbrace{x + x + x + \ldots + x}_{n}$, com n parcelas, se $\text{n} > 0$ e
-nx = (-x) + (-x) +(-x) +...+(-x), com n parcelas, se $\text{n} < 0$.

1.10 Grupos cíclicos

1.10.1 Grupo gerado por um elemento

Seja x um elemento de um grupo multiplicativo $(G, .)$. O subgrupo gerado por a, denotado por $< a >$, é o conjunto de todas as potências de expoente inteiro de a:

$$< a >= \{a^n | n \in \mathbb{Z}\} = \{\ldots, a^{-3}, a^{-2}, a^{-1}, 0, a, a^2, a^3, \ldots\}.$$

Se (G, +) for um grupo aditivo e b ∈ G, então $< b >$ é o conjunto de todos os múltiplos de b,

$$< b >= \{\ nb | n \in \mathbb{Z}\ \} = \{\ \ldots\ , -3b, -2b, -b, e, b, 2b, 3b,\ \ldots\ \}.$$

Exemplo 1.10.1 *Considere $G = S_\Delta$ e $R_{2\pi/3} \in S_\Delta$. Temos que $< R_{2\pi/3} >= \{id,\ R_{2\pi/3},\ R_{4\pi/3}\}$.*

1.10.2 Grupos cíclicos

Um grupo G é denominado cíclico se existir $a \in G$ tal que $G =< a >$. Neste caso, todos os elementos de G são potências (ou múltiplos) de a que é denominado gerador de G.

Exemplo 1.10.2 *O grupo dos números inteiros, com a operação de adição dado por $(\mathbb{Z}, +)$ é um grupo cíclico porque todo inteiro é múltiplo de 1, ou seja, $\mathbb{Z} =< 1 >$. Um grupo cíclico pode ter mais de um gerador. Note que neste caso temos também $\mathbb{Z} =< -1 >$.*

Exemplo 1.10.3 *O grupo cíclico* $(\mathbb{Z}_5^*, .)$ *é gerado por* $\overline{2}$ *porque* $< \overline{2} >= \{ \overline{2}^0, \overline{2}^1, \overline{2}^2, \overline{2}^3 \} = \{ \overline{1}, \overline{2}, \overline{4}, \overline{3} \} = (\mathbb{Z}_5^*, .)$.

Visto que um grupo pode ter mais que um gerador e em particular se a é o gerador de um grupo e b é o inverso de a, então b também é um gerador do grupo, observe os exemplos.

Exemplo 1.10.4 *Seja o grupo formado pelos elementos* $\{ 1, -1, i, -i \}$, *com a multiplicação usual de complexos. Tem-se um grupo cíclico gerado pelo elemento i, bem como o seu inverso -i que também é um gerador, basta ver que* $< -i > = G$.

Exemplo 1.10.5 *O grupo* $(\mathbb{Z}_7^*, .)$ *possui os geradores* $\overline{3}$ *e o* $\overline{5}$, *uma vez que* $< \overline{3} >= \{ \overline{3}^0, \overline{3}^1, \overline{3}^2, \overline{3}^3, \overline{3}^4, \overline{3}^5, \overline{3}^6 \} = \{ \overline{1}, \overline{2}, \overline{3}, \overline{4}, \overline{5}, \overline{6} \}$ *e como* $\overline{5}$ *é o inverso de* $\overline{3}$, *logo* $\overline{5}$ *também é um gerador de* $(\mathbb{Z}_7, .)$.

Proposição 1.10.1 *Seja a um elemento de um grupo G. Então se* $a^m = e$ *para certo* $m \geq 1$ *e* $\{ e, a, a^2, \ldots, a^{m-1} \}$ *forem distintos, então* $< a > \subset \{ e, a, a^2, \ldots, a^{m-1} \}$ *e, nesse caso,* $a^m = a^p$, *se, e somente se,* $m|p$ *(m divide p).*

Prova 1.10.1 *É imediato que* $< a > \subset \{e, a^1, a^2, \ldots, a^{m-1}\}$ *Veja que se* $k \geq 0$, *a divisão euclidiana nos fornece* $k = qm + r$ *com* $q, r \in \mathbb{Z}$ *e* $0 \leq r < m$, *onde* $a^k = a^{qm}a^r$. *Portanto,* $< a > \subset \{ e, a, a^2, \ldots, a^{m-1} \}$.
Se $a^n = a^p$ *então* $a^{n-p} = e$, *e portanto, pelo mesmo argumento,* $n - p = qm + r$, *com* $0 \leq |r| < m$, *e obtemos* $a^r = e$, *donde* $r = 0$, *ou seja,* $m|n - p$. *Isso termina a prova da proposição.*

Quando um elemento a satisfaz *a* condição *ii*), da Proposição 5, dizemos que m é a ordem de a e denotado por $\theta(a) = m$.

Exemplo 1.10.6 *Dado o grupo de simetria do triângulo equilátero,* S_Δ, *que não é um grupo cíclico, mas possui o subgrupo* $G = \{id, R_{2\pi/3}, R_{4\pi/3} \}$, *que é cíclico e gerado por* $R_{\frac{2\pi}{3}}$, *ou seja* $\theta(R_{2\pi/3}) = 3$.

Exemplo 1.10.7 *O conjunto dos números inteiros, com a operação usual de adição, é um grupo cíclico infinito:* $\mathbb{Z} = \{\ldots, -2, -1, 0, 1, 2, \ldots\}$. *Ele pode ser gerado por a = 1 ou a = -1.*

1.11 Produto direto

Seja $\{G_i\}_{1 \leq i \leq n}$ uma família não vazia de grupos multiplicativos e seja $G = G_1 \times G_2 \times \ldots \times Gn$ o produto cartesiano dos conjuntos $G_1, G_2, \ldots, G_n$. Sejam $(g_1, g_2, \ldots, g_n)$ e $(h_1, h_2, \ldots, h_n)$ dois elementos quaisquer de G e definamos em G a seguinte operação:

$$(g_1,\ g_2,\ \ldots,\ g_n).\ (h_1,\ h_2,\ \ldots,\ h_n) = (g_1h_1,\ g_2h_2,\ \ldots,\ g_nh_n).$$

Desta forma, G munido desta operação é um grupo chamado produto direto da família $\{\ G_i\ \}_{1\leq i\leq n}$. De fato, para todo $g_i\ \in\ G_i$ existe $g_i^{-1}\ \in G_i$, para todo i $\in\ \{\ 1,\ 2,\ \ldots,\ n\}$, pois G_i é um grupo. Logo, se $(g_1,\ g_2,\ \ldots,\ g_n)$ é um elemento qualquer de G, o seu inverso é um elemento de G e é dado por:

$$(g_1,\ g_2,\ \ldots,\ g_n)^{-1} = (g_1^{-1},\ g_2^{-1},\ \ldots, g_n^{-1})\ \in G.$$

Da mesma forma, se g_i e h_i são dois elementos quaisquer de G_i, então $g_ih_i^{-1}\ \in\ G_i,\ \forall\ i\ \in\ \{\ 1,\ 2,\ \ldots\ ,n\ \}$. Logo, se $(\ g_1,\ g_2,\ \ldots,\ g_n)$ e $(h_1,\ h_2,\ \ldots,\ h_n)$ são dois elementos quaisquer de G então:

$$(g_1,\ g_2,\ \ldots,\ g_n).(h_1,\ h_2,\ \ldots,\ h_n)^{-1} = (g_1,\ g_2,\ \ldots,\ g_n).(h_1^{-1},\ h_2^{-1},\ \ldots,\ h_n^{-1}) =$$
$$(g_1h_1^{-1},\ g_2h_2^{-1},\ \ldots,\ g_nh_n^{-1})\ \in G.$$

A propriedade associativa é evidente em G. Portanto, G é um grupo. Além disso, o elemento neutro de g é $(e_1,\ e_2,\ \ldots,\ e_n)$, onde e_i é o elemento neutro de $G_i,\ \forall\ i\ \in\ \{\ 1,\ 2,\ \ldots,\ n\}$.Portanto, com a operação definida acima G é um grupo.

Afirmamos que $G = G_1\ \times\ G_2\ \times\ \ldots\ \times\ G_n$ é abeliano se, e somente se, G_i é abeliano, $\forall\ i\ \in\ \{\ 1,\ 2,\ \ldots,\ n\}$. De fato, se G é abeliano então para quaisquer dois elementos $(g_1,\ g_2,\ \ldots,\ g_n)$, $(h_1,\ h_2,\ \ldots,\ h_n)$ de G temos

$$(g_1,\ g_2,\ \ldots,\ g_n\ ).\ (h_1,\ h_2,\ \ldots,\ h_n) = (h_1,\ h_2,\ \ldots,\ h_n).\ (g_1,\ g_2,\ \ldots,\ g_n),$$

se, e somente se,

$$(g_1h_1,\ g_2h_2,\ \ldots,\ g_nh_n) = (h_1g_1,\ h_2g_2,\ \ldots,\ h_ng_n),\ \forall\ i\ \in\ \{\ 1,\ 2,\ \ldots,\ n\}$$

Assim, G_i é abeliano, $\forall\ i\ \ \in\ \ \{\ 1,\ 2,\ \ldots,\ n\ \}$. Por outro lado, se G_i é abeliano $\forall\ i \in\ \{\ 1,\ 2,\ \ldots,\ n\ \}$ então $g_ih_i = h_ig_i$. Assim,

$$(g_1,\ g_2,\ \ldots,\ g_n).\ (h_1,\ h_2,\ \ldots,\ h_n) = (g_1h_1,\ g_2h_2,\ \ldots,\ g_nh_n) =$$
$$(h_1g_1,\ h_2g_2,\ \ldots,\ h_ng_n) = (h_1, h_2,\ \ldots,\ h_n).(g_1,\ g_2,\ \ldots,\ g_n).$$

Portanto G é abeliano.

Exemplo 1.11.1 *Considere* $G_1 = \mathbb{Z}_2 = \{\ \overline{0},\ \overline{1}\ \}$ *e* $G_2 = \mathbb{Z}_3 = \{\ \overline{0},\ \overline{1},\ \overline{2}\ \}$. *Assim, omitindo as barras dos elementos de* G_1 *e* G_2, *temos* $\mathbb{Z}_2\ \times\ \mathbb{Z}_3 = \{\ (0,0),\ (0,1),\ (0,2),\ (1,0),\ (1,1),\ (1,2)\ \}$.

1.12 Classes laterais

Se H é um subgrupo de um grupo G e $x \in$ G, o subconjunto de G, dado por $H_x = \{\ hx :\ h\ \in\ H\}$ é chamado de classe lateral à direita de H em G. Analogamente, definimos classe lateral á esquerda de H em G. Quando o conjunto das classes laterais á direita ou á esquerda de H em G for finito, dizemos que H é um subgrupo de índice finito em G, e o número de classes laterais disjuntas é chamado o índice de H em G e denotado por $|G : H|$. Se G for escrito com notação aditiva, uma classe lateral de H em G se escreve: $H + x = \{h + x : h \in H\}$. Como Hx é uma classe lateral de H em G, dizemos que x é um representante da classe lateral Hx. É claro que se $x' = h'x$ para certo $h' \in$ H, então $Hx' = Hx$, e portanto x' é outro representante da mesma classe lateral Hx. A razão é que as classes laterais são classes de equivalência com a seguinte relação de equivalência em G, $x \approx y$ se, e somente se $xy^{-1} \in H$. Para melhor compreensão dos conceitos acima mencionados, vejamos o seguinte exemplo:

Exemplo 1.12.1 *Vimos no Exemplo 19 que $H = \{\ \overline{0},\ \overline{2}\ \}$ é subgrupo de $\mathbb{Z}_4$. Desta forma, podemos calcular as classes laterais de H em $\mathbb{Z}_4$. Obtendo as classes laterais á direita e á esquerda de H em $\mathbb{Z}_4$, respectivamente.*

Exemplo 1.12.2 *Vimos no Exemplo 1.8.2 que $H = \{\ \overline{0},\ \overline{2}\ \}$ é subgrupo de $\mathbb{Z}_4$. Desta forma, podemos calcular as classes laterais de H em $\mathbb{Z}_4$. Obtendo as classes laterais à direita e à esquerda de H em $\mathbb{Z}_4$, respectivamente.*
$i) H + \overline{0} = \{\overline{h} + \overline{0}, \overline{h} \in H\} = \{\overline{0}, \overline{2}\}$
$ii) H + \overline{1} = \{\overline{h} + \overline{1}, \overline{h} \in H\} = \{\overline{1}, \overline{3}\}$
$iii) H + \overline{2} = \{\overline{h} + \overline{2}, \overline{h} \in H\} = \{\overline{0}, \overline{2}\}$
$iv) H + \overline{3} = \{\overline{h} + \overline{3}, \overline{h} \in H\} = \{\overline{1}, \overline{3}\}$
$v) \overline{0} + H = \{\overline{0} + \overline{h}, \overline{h} \in H\} = \{\overline{0}, \overline{2}\}$
$vi) \overline{1} + H = \{\overline{1} + \overline{h}, \overline{h} \in H\} = \{\overline{1}, \overline{3}\}$
$vii) \overline{2} + H = \{\overline{2} + \overline{h}, \overline{h} \in H\} = \{\overline{0}, \overline{2}\}$
$viii) \overline{3} + H = \{\overline{3} + \overline{h}, \overline{h} \in H\} = \{\overline{1}, \overline{3}\}$

Exemplo 1.12.3 *Seja $G = \mathbb{Z}$ o grupo aditivo dos números inteiros e $H = < 2 >$ o subgrupo dos números pares. Temos duas classes laterais distintas: $H+0 = \{\ldots, -2, 0, 2, \ldots\}$ e $H + 1 = \{\ldots, -3, -1, 1, 3, \ldots\}$ e portanto $|G : H| = 2$.*

Se D e E representam respectivamente o conjunto das classes laterais á direita e á esquerda de H em G. Pode ser mostrado que a função $f : D \longrightarrow$ E dada por $Hx \longrightarrow x^{-1}H$ estabelece uma bijeção entre os dois conjuntos, de modo que a definição de índice independe de tomarmos classes laterais á direita ou á esquerda. Para mais detalhes veja [2].

1.13 Subgrupo normal

Sendo (G, $*$) um grupo, um subgrupo H de G é denominado normal, se para todo elemento x de G tivermos $x * H = H * x$. Denotaremos H normal em G por $H \triangleleft G$.

Exemplo 1.13.1 *Seja $G = \mathbb{Z}_4$ e $H = \{\overline{0}, \overline{2}\}$. Veja que H é normal em G (Conforme Exemplo* 1.12.2*).*

Se H é um subgrupo de um grupo G, é usual denotarmos o conjunto das classes laterais de H em G por G/H.

1.14 Grupo quociente

Dado H $\triangleleft$ G, o conjunto de todas as classes laterais módulo H é um grupo com a operação definida por $(aH) * (bH) = (abH),\ \forall a,\ b \in G$ e é denominado grupo quociente de H em G que denotamos por G/H.

Se H é um subgrupo normal de G, então o quociente G/H admite uma estrutura de grupo, chamada de grupo quociente.

Exemplo 1.14.1 *Seja $4\mathbb{Z} = \{0, \mp 4, \mp 8, \ldots\}$ o subgrupo de $\mathbb{Z}$ dos múltiplos inteiros de 4. Vamos construir o grupo quociente $\mathbb{Z}/4\mathbb{Z}$. Consideramos as classes laterais de $4\mathbb{Z}$ em $\mathbb{Z}$:*

$$\begin{aligned} 0 + 4\mathbb{Z} &= \{\ldots, -4, 0, 4, 8, \ldots\} \\ 1 + 4\mathbb{Z} &= \{\ldots, -3, 1, 5, 9, \ldots\} \\ 2 + 4\mathbb{Z} &= \{\ldots, -2, 2, 6, 10, \ldots\} \\ 3 + 4\mathbb{Z} &= \{\ldots, -1, 3, 7, 11, \ldots\} \end{aligned}$$

O teorema abaixo, cuja demonstração pode ser encontrada em [2], auxilia a demonstração do Teorema de Lagrange que é uma ferramenta de grande utilidade para a Teoria de Grupo.

Os exemplos anteriores levantam questões como : Quando é que $aH = bH$? Quantos elementos têm em comum aH e Hb ? O seguinte Teorema ajuda a esclarecer.

Teorema 1.14.1 *Seja G um grupo, $H \leq G$ e $a,\ b \in G$. Então:*

i) $a \in aH$;

ii) $aH = H$ se e só se $a \in H$;

iii) $aH = bH$ ou $aH \cap bH = \oslash$;

iv) $aH = bH$ se e só se $a^{-1}b \in H$;

v) $\#aH = \#bH$;

vi) $aH = Ha$ se, e só se, $H = aHa^{-1}$;

vii) aH é um subgrupo de G se, e só se a, $\in H$.

Teorema 1.14.2 *(Lagrange) Se G é um grupo finito e H é um subgrupo de G, então:*

$$| G | = | H | . |G : H|.$$

Prova 1.14.1 *Sejam a_1H, a_2H, ..., a_rH as classes laterais à esquerda de H em G. Como cada elemento de G pertence a alguma classe lateral esquerda de H (do Teorema anterior), tem-se:*

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

Como esta união é disjunta do Teorema anterior, tem-se:

$$|G| = \#a_1H + \#a_2H + \ldots + \#a_rH.$$

Usando agora v do Teorema anterior, tem-se : $| a_iH | = | H |$, para qualquer i, logo $| G | = r | H |$.

O Teorema de Lagrange tem diversas consequências, dentre as quais:

Corolário 1.14.1 *A ordem de um elemento de um grupo finito divide a ordem do grupo.*

Corolário 1.14.2 *Todo grupo de ordem prima é cíclico.*

1.15 Homomorfismo

Em Álgebra abstrata, um homomorfismo, que será definido abaixo, é uma aplicação que preserva a estrutura entre duas estruturas algébricas, como por exemplo grupos. A palavra homomorfismo vem da língua grega, haja vista que homos significa mesmo e morphe significa formato.

Definição 1.15.1 *Sejam $(G, .)$ e $(J, *)$ dois grupos. Uma função $f : G \longrightarrow J$ satisfazendo $f(a.b) = f(a) * f(b)$, para todos os a, $b \in G$ é dito um homomorfismo de grupos.*

Se f é um homomorfismo bijetor, então dizemos que f é um isomorfismo entre G e J e escrevemos $G \cong J$, é possível verificar que a função inversa $f^{-1} : J \longrightarrow G$ também é um homomorfismo de grupos.

Exemplo 1.15.1 *A função logaritmo $f : R^+ \longrightarrow R$ dada por $f(x) = log(x)$ é uma bijeção, como $log(x.y) = log(x) + log(y)$, os grupos $(R^+, .)$ e $(R, +)$ são isomorfos. Note que a sua função inversa exponencial dada por $exp(x)$, é igualmente um isomorfismo.*

Exemplo 1.15.2 *Não podemos estabelecer um isomorfismo entre $\mathbb{Z}_4$ e $\mathbb{Z}_2 \times \mathbb{Z}_2$, uma vez que em $\mathbb{Z}_4$ temos um elemento de ordem 4 e em $\mathbb{Z}_2 \times \mathbb{Z}_2$ todos os elementos tem ordem 2. Em outras palavras, os referidos grupos não possuem a mesma estrutura, isto é, não são isomorfos.*

Para que seja candidata a isomorfismo de $\mathbb{Z}_4$ em $\mathbb{Z}_2 \times \mathbb{Z}_2$, necessariamente deveríamos ter apenas o zero no primeiro conjunto para obter o zero no outro conjunto .

Isto é,
$f(0) = (0,0)$
$f(1) = (1,1)$
$f(2) = f(1+1) = f(1) + f(1) = (1,1) + (1,1) = (0,0)$
$f(3) = f(1+2) = f(1) + f(2) = (1,1) + (0,0) = (1,1)$.

Isto mostra que f não é injetora, pois $f(0) = f(2)$ e $f(1) = f(3)$, e nem sobrejetora , com $Im(f) = \{(0,0),(1,1)\}$ e portanto não há nenhum isomorfismo de ($\mathbb{Z}_4$, +) em $\mathbb{Z}_2 \times \mathbb{Z}_2$.

Exemplo 1.15.3 *Sejam os grupos ($\mathbb{Z}_6 = \{\overline{0}, \overline{1}, \overline{2}, \overline{3}, \overline{4}, \overline{5}\}$ e $\mathbb{Z}_2 \times \mathbb{Z}_3 = \{(\overline{0}, \overline{0}$),*
($\overline{1}, \overline{1}$), $(\overline{0}, \overline{2}), (\overline{1}, \overline{0}), (\overline{0}, \overline{1}), (\overline{1}, \overline{2})\}$. Podemos estabelecer um isomorfismo entre os citados grupos da seguinte forma:

$$
\begin{aligned}
&(\overline{0}, \overline{0}) \longmapsto \overline{0} \\
&(\overline{1}, \overline{1}) \longmapsto \overline{1} \\
&(\overline{0}, \overline{2}) \longmapsto \overline{2} \\
&(\overline{1}, \overline{0}) \longmapsto \overline{3} \\
&(\overline{0}, \overline{1}) \longmapsto \overline{4} \\
&(\overline{1}, \overline{2}) \longmapsto \overline{5}
\end{aligned}
$$

Exemplo 1.15.4 *O grupo (Z_6, +) = { $\overline{0}$, $\overline{1}$, $\overline{2}$, $\overline{3}$, $\overline{4}$, $\overline{5}$ } não é isomorfo a S_Δ, uma vez que o grupo S_Δ não é cíclico.*

Teorema 1.15.1 *($1^{\underline{o}}$ Teorema do Homomorfismo) Sejam G e J grupos com identidades e_1 e e_2, respectivamente e $\varphi : G \longrightarrow J$ um homomorfismo.*
Então:
i) Im $\varphi = \varphi(G) = \{ \varphi (g) / g \in G \}$ é um subgrupo de J;
ii) Ker $\varphi = \{ g \in G / \varphi (g) = e_1 \}$ é um subgrupo normal de G, denominado kernel do homomorfismo φ;
iii) $\dfrac{G}{Ker\varphi} \cong Im\ \varphi$.

Exemplo 1.15.5 *Seja $\varphi : \mathbb{Z} \longrightarrow \mathbb{Z}_m$ um homomorfismo definido por $\varphi(g) = \overline{g}$. Então, pelo Teorema* 1.15.1*, segue:*
i)$\varphi(\mathbb{Z}) = \mathbb{Z}_m$;
ii)$Ker\varphi = \{mq,\ q \in \mathbb{Z}\} = m\mathbb{Z}$;
iii)$\dfrac{\mathbb{Z}}{Ker\varphi} \cong \mathbb{Z}_m$.

Teorema 1.15.2 *O grupo $\mathbb{Z}_m \times \mathbb{Z}_n$ é isomorfo a $\mathbb{Z}_{mn}$, se, e somente se, m e n são relativamente primos, isto é, o máximo divisor comum entre eles é 1.*

Corolário 1.15.1 *O grupo* $\prod_{i=1}^{n} \mathbb{Z}_{m_i}$ *é cíclico e isomorfo a* $\mathbb{Z}_{m_1.m_2} \ldots m_n$*, se, e somente se, os números* m_i *para* $i = 1, 2, 3, \ldots, n$ *são tais que o máximo divisor comum de quaisquer dois deles é 1.*

Exemplo 1.15.6 *O corolário anterior nos diz que se n é escrito como produto de potências de números primos distintos, ou seja,* $n = p_1^{n1}.p_2^{n2} \ldots p_r^{nr}$*, então* $\mathbb{Z}_n$ *é isomorfo a* $\mathbb{Z}_{{p_1}^{n_1}} \times \mathbb{Z}_{{p_2}^{n_2}} \times \mathbb{Z}_{{p_r}^{n_r}}$.

1.16 Grupos de permutações

Exemplo 1.16.1 *Podemos pensar em uma fila com 3 pessoas, então para a primeira posição existem 3 possibilidades, para a segunda posição existem 2 possibilidades, e para a última posição temos 1 possibilidade.*

Uma permutação de um conjunto A a uma função bijetiva α que leva A em A, ou seja, α : A $\longrightarrow$ A. Um grupo de permutações de um conjunto A é um conjunto de permutações de A que, com a operação de composição, forma um grupo. Quando B = $\{1, 2, 3, \ldots, n\}$, indicaremos uma permutação τ de B pela notação matricial:

$$\begin{pmatrix} 1 & 2 & 3 & \ldots & n \\ \tau(1) & \tau(2) & \tau(3) & \ldots & \tau(n) \end{pmatrix}$$

Com esta notação, a permutação idêntica de B denotamos por I_B que representa a matriz.

$$\begin{pmatrix} 1 & 2 & 3 & \ldots & n \\ 1 & 2 & 3 & \ldots & n \end{pmatrix}$$

O número total de permutações de um conjunto finito B com n elementos é igual ao produto dos n primeiros inteiros positivos, ou seja, 1 . 2 . 3 . . . . .n = n!

Denotaremos os conjuntos das permutações do conjunto B, contendo n elementos, como S_B ou S_n.

Exemplo 1.16.2 *Quando* $G = S_3$*, então os elementos de* S_3 *são:*

$$\begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}.$$

1.17 Permutação inversa

Definição 1.17.1 *Seja $B = \{$ 1, 2, 3, ..., n$\}$, e γ uma permutação de B, então a inversa de γ será a permutação $\gamma^{-1} =$*

$$\begin{pmatrix} \gamma(1) & \gamma(2) & \gamma(3) & \dots & \gamma(n) \\ 1 & 2 & 3 & \dots & n \end{pmatrix} = \begin{pmatrix} \gamma^{-1}(1) & \gamma^{-1}(2) & \gamma^{-1}(3) & \dots & \gamma^{-1}(n) \\ 1 & 2 & 3 & \dots & n \end{pmatrix}$$

Exemplo 1.17.1 *Se o conjunto $B = \{1, 2, 3, 4, 5\}$, então uma permutação de B é $\varphi =$*

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 4 & 3 & 1 & 5 & 2 \end{pmatrix}$$

A permutação inversa de φ é a aplicação bijetora $\varphi^{-1} =$

$$\begin{pmatrix} 4 & 3 & 1 & 5 & 2 \\ 1 & 2 & 3 & 4 & 5 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 5 & 2 & 1 & 4 \end{pmatrix}$$

.

Exemplo 1.17.2 *Se o conjunto $B = \{1, 2, 3, 4\}$, considere as permutações:*

$$\varphi = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 1 & 4 \end{pmatrix} e \, \Psi \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 1 & 2 \end{pmatrix}$$

.

As aplicações compostas $\varphi \; o \; \Psi$: B $\longrightarrow$ B e $\Psi \; o \; \varphi$ B $\longrightarrow$ B são bijetoras e, portanto, também são permutações de B. Temos:

$$\varphi o \Psi = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 1 & 4 \end{pmatrix} o \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 1 & 2 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 4 & 2 & 3 \end{pmatrix}$$

$$\Psi o \varphi = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 1 & 2 \end{pmatrix} o \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 1 & 4 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 1 & 3 & 2 \end{pmatrix}$$

. Veja que $\varphi \; o \; \Psi \neq \Psi \; o \; \varphi$.

1.18 Notação de ciclo

As matrizes são convenientes para descrever permutações. Mas há um modo mais simples que é a notação de ciclos. Um ciclo pode ser pensado como uma série de tranposições de estado que acaba por retornar ao estado inicial.

Exemplo 1.18.1 *Considere a permutação:*

$$\begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 2 & 4 & 1 \end{pmatrix}$$

Voltando a pensar nas filas das pessoas, esta permutação faz o seguinte: A pessoa que estava na posição 1 vai para a posição 3, a pessoa que estava na posição 3 vai para a posição 4, a pessoa que estava na posição 4 vai para a posição 1, a pessoa que estava na posição 2 vai continuar na posição 2. Repare no modo como as pessoas 1, 3 e 4 transitam em círculo. Podemos representar o trânsito das pessoas da seguinte forma $\sigma : 1 \longmapsto 3 \longmapsto 4 \longmapsto 1$*, significando que a pessoa da posição 1 vai para a posição 3, que a pessoa da posição 3 vai para a posição 4, a pessoa da posição 4 vai para a posição 1 e a pessoa da posição 2 continua na posição 2. Melhor ainda, podemos simplesmente escrever* σ *: (1 3 4), significando a mesma coisa. Esta é chamada de notação de ciclos de* σ*.*

Na notação de ciclos os n elementos entre parênteses formam um n-ciclo. Da mesma forma que as matrizes, os 3-ciclos (1 3 4), (3 4 1), (4 1 3) são iguais. E convenientemente, começamos um ciclo pelo menor elemento. Assim escrevendo a permutação

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 1 & 3 & 5 & 6 & 4 \end{pmatrix} = (12)(456)$$

Logo esta permutação consiste em um 2-ciclo e um 3-ciclo.

1.19 Grupo das permutações de um conjunto

Os elementos do conjunto das permutações S_n possuem algumas caracterizações, as quais seguem.

Definição 1.19.1 *Seja* $B = \{1, 2, 3, \ldots, n\}$*. Uma permutação* α *de* S_n *é chamado de r-ciclo se existem elementos distintos* a_1*,* a_2*,* a_3*,...,* $a_r \in \{1, 2, 3, \ldots, n\}$ *tais que* $\alpha(a_1) = a_2$*,* $\alpha(a_2) = a_3$*, ...* $\alpha(a_{r-1}) = a_r$*,* $\alpha(a_r) = a_1$*.*

Proposição 1.19.1 *Todo elemento de* S_n *é produto de transposições, isto é,* S_n *é gerado por transposições. O conjunto das permutações de* S_n *tem estrutura de grupo, como mostra o teorema abaixo.*

Teorema 1.19.1 *Seja B um conjunto não vazio e* $S_n = \{\tau : B \longrightarrow B / \tau$ *é bijetora* $\}$*, então:*

i) (S_B*, o) é um grupo, onde o é a operação composição.*

ii) Se $\#(B) > 2$*, então (*S_B*, o) não é abeliano.*

Prova 1.19.1 *Temos que i é imediato, pois dados* τ_1, τ_2, $\tau_3 \in S_B$, *valem:*

a) $\tau_1 o \tau_2 \in S_B, \forall \tau_1, \tau_2 \in S_B$*(fechamento);*

b) $(\tau_1 \ o \ \tau_2) \ o \ \tau_3 = \tau_1 \ o \ (\tau_2 \ o \ \tau_3)$ *(associativa);*

c) $\tau_1 \ o \ I_B = I_B \ o \ \tau_1$ *(existência do elemento neutro, denotado por* I_B*);*

d) $\tau_1 \ o \ \tau_1^{-1} = \tau_1^{-1} \ o \ \tau_1 = I_B$ *(com* τ_1^{-1} *sendo o inverso de* τ_1 *).*

Para o item ii) temos que se o conjunto B tem mais de dois elementos, o grupo (S_B, o) *não é abeliano. Como* $\#(B) > 2$*, sendo B a união dos conjuntos disjuntos dada por* $B = \{b_1, b_2, b_3\} \cup B'$*. Considere as permutações* τ *e* $\rho \in S_B$*, assim definidas:* $\tau(b_1) = b_2, \tau(b_2) = b_3, \tau(b_3) = b_1, \ \tau(x) = x \forall x \in B´, \ \rho(b_1) = b_2, \rho(b_2) = b_1, \rho(b_3) = b_3, \rho(x) = x \forall x \ in \ B´$*.*

Temos que: $\tau o \rho(b_1) = \tau(\rho(b_1)) = \tau(b_2) = b_3$ *e ainda* $(\rho\tau)(b_1) = \rho(\tau_1)) = \rho(b_2) = b_1$*. Portanto,* $\rho\tau \neq \tau o \rho$*, isto mostra que o grupo* (S_B, o) *não é abeliano.*

Consideremos o grupo $S_3 = \{$ id, (1 2), (1 3), (2 3), (1 2 3), (1 3 2)$\}$. Sejam
$\alpha = (1\ 2\ 3)$ e $\beta = (1\ 2)$, temos: $\alpha^2 = (1\ 2\ 3)(1\ 2\ 3) = (1\ 3\ 2)$, $\alpha^3 = (1\ 3\ 2)(1\ 2\ 3) =$ id, $\beta^2 = (1\ 2)(1\ 2) =$ id, $\beta\alpha = (1\ 2\ 3)(1\ 2) = (1\ 3)$, $\alpha\beta = (1\ 2)(1\ 2\ 3) = (2\ 3)$, $\alpha^2\beta = (1\ 3\ 2)(1\ 2) = (2\ 3)$.

Observe acima que α e β geram o grupo S_3, isto é, que todos os elementos do grupo são produtos finitos de fatores iguais a α e β. Dadas duas permutações é possível operá-las, isto é, suponhamos que o conjunto a ser permutado seja $\{1, 2, 3, 4, 5\}$. Desejamos fazer $\sigma = (1\ 2\ 4)(3\ 5)$ seguido de $\tau = (1\ 3\ 5)(2\ 4)$, que é, obter a composição dessas permutações, ou seja, τ o σ . Basta seguir, cada elemento do conjunto e ver onde ele irá parar. Por exemplo, σ leva 1 no 2 e τ leva 2 no 4, logo 1 vai no 4. Em seguida , σ leva 2 no 4 e τ leva 4 no 2, logo o 2 não se move. E ainda, σ leva o 4 no 1 e τ leva o 1 no 3, então 4 vai no 3. Assim σ leva 3 no 5 e τ leva 5 no 1 logo o 3 vai no 1. Fechando temos ainda que o 5 vai no 3 e o 3 vai no 5, logo o 5 não se move. Portanto $\tau o \sigma = (135)(24) o (124)(35) = (143)$.

1.20 Permutações pares e ímpares

Definição 1.20.1 *Seja* σ *uma permutação. Se* σ *pode ser fatorada com um número par de transposições, então dizemos que* σ *é uma permutação par. Se* σ *pode ser fatorada com um número ímpar de transposições, então ela é chamada permutação ímpar. Em geral, a fatoração de uma permutação em transposições não é única.*

A composição de permutações pares resulta numa permutação par. A composição de permutações ímpares e a composição de uma permutação par com uma permutação ímpar resultam em uma permutação ímpar.

Proposição 1.20.1 *Se* A_n *é o conjunto de todas as permutações pares em* S_n *então* A_n *é um subgrupo de* S_n*.*

Prova 1.20.1 *De fato, A_n é um subgrupo de S_n, pois temos que, dados $\alpha, \gamma \in A_n$, $\alpha o \gamma \in A_n$. Além disso, se $\alpha \in A_n \Rightarrow \alpha^{-1} \in A_n$. A_n é denominado grupo alternado de grau n.*

Pode ser mostrado que a quantidade de elementos de A_n é $\dfrac{n!}{2}$.

Exemplo 1.20.1 *Seja o grupo S_4 de permutações com 24 elementos. Então o grupo das permutações pares, A_4, tem $\dfrac{n!}{2} = \dfrac{4!}{2} = \dfrac{4.3.2.1}{2} = 12$ elementos, a saber: $A_4 =$ { id; (1 2)(3 4), (1 4)(2 3), (1 3)(2 4), (1 3 4), (1 4 3), (1 2 3), (1 3 2), (2 3 4), (2 4 3), (1 2 4) e (1 4 2) }.*

Capítulo 2

Uma abordagem sobre apresentação de grupos

No capítulo supracitado explicitaremos alguns conceitos e resultados presentes na teoria de apresentação de grupos. Tal explanação estará alicerçado em Magnus et al. (2004).

2.1 Apresentação de grupos

Podemos descrever um grupo em termos de um conjunto de geradores e de relações. Por exemplo, um grupo cíclico de ordem 12 pode ser apresentado por um único elemento b (gerador) e a relação $b^{12} = 1$.

Já o grupo de Klein [6] pode ser apresentado por dois geradores a e b com relações $a^2 = e$, $b^2 = e$, $ab = ba$.

O conjunto constituído de geradores e relações tais que todos os elementos podem ser originadas, é denominado apresentação de grupo. Para melhor compreensão do que vem a ser uma apresentação de grupo, no sentido mais geral, explicitaremos alguns resultados e conceitos, que de certa forma, generalizam as relações algébricas presentes nos exemplos anteriores.

2.2 Palavra

Definição 2.2.1 *Sejam a, b, c, ... símbolos distintos e os novos símbolos formados* a^{-1}, b^{-1}, c^{-1}, ... *Uma palavra nos símbolos a, b, c, ... é uma sequência finita dada por:*

$$f_1, f_2, \ldots, f_{n-1}, f_n, \tag{2.1}$$

[6] É o grupo de 4 elementos isomorfo a $(\mathbb{Z}_2 \times \mathbb{Z}_2, +)$.

onde cada f_v *;* $v \in \{ 1, \ldots, n \}$ *é um dos símbolos a, b, c, ...* a^{-1}, b^{-1}, c^{-1}.

É comum usarmos a Equação 2.1 da forma:

$$f_1 f_2 \ldots f_{n-1} f_n. \tag{2.2}$$

Uma palavra W nos símbolos a, b, c, ... será denotada por W (a, b, c, ...).

Exemplo 2.2.1 *Uma palavra nos símbolos a, b, c, ... dada por* $a^3 b a^{-1} c^{-1}$ *será denotada por W(a, b, c) =* $a^3 b a^{-1} c^{-1}$.

Observação 2.2.1 *O comprimento de uma palavra W, denotado por L(W), é um inteiro n. Assim, na palavra W(a, b, c) =* $a^4 b a^{-2} c^{-2}$*, temos que L(W) = 9.*

Observação 2.2.2 *Por conveniência introduziremos a palavra vazia de comprimento zero e a denotamos por 1.*

Observação 2.2.3 *Vale ressaltar que a palavra W(a, b, c) =* $a^{-2} a^2 b^{-1} b c^3 c^{-3}$ *tem comprimento 12 e não zero.*

Finalizamos esta seção dizendo que é comum abreviar um bloco de n símbolos consecutivos de a^{-1}, da forma $a^{-1}.a^{-1}.\ldots.a^{-1}$ por a^{-n}. Por exemplo, a palavra W (a, b, c) = $a^3b^2b^{-1}a^{-2}c^{-1}$ coincide com a palavra $aaabbb^{-1}a^{-1}a^{-1}c^{-1}$, porém é diferente da palavra $aaaba^{-1}a^{-1}a^{-1}c^{-1}$.

2.3 Palavra inversa

A inversa de uma palavra W, não vazia dada pela Equação **??** é a palavra

$$f_n^{-1} f_{n-1}^{-1} \ldots f_2^{-1} f_1^{-1}. \tag{2.3}$$

A inversa da palavra vazia é ela mesma.

Exemplo 2.3.1 *Se considerarmos* $W_1(a, b, c) = aa^{-1}c$, $W_2(a, b, c) = aaba^{-1}b^{-1}b^{-1}b$, $W_3(a, b, c) = 1$, *então* ${W_1}^{-1}(a, b, c) = c^{-1}aa^{-1}$, ${W_2}^{-1}(a, b, c) = b^{-1}bbab^{-1}a^{-1}a^{-1}$ *e* ${W_3}^{-1}(a, b, c) = 1$.

No exemplo acima, veja que $L(W_1) = L({W_1}^{-1})$, $L(W_2) = L({W_2}^{-1})$ e $L(W_3) = L({W_3}^{-1})$. Na realidade essas igualdades não são válidas apenas para estes casos particulares. Especificamente se W é uma palavra dada pela Equação 2.2, então podemos mostrar que $L(W) = L(W^{-1})$ e $(W^{-1})^{-1} = W$.

2.4 O produto de duas ou mais palavras

Se W é a palavra $f_1\ f_2 \ldots f_n$ e U é a palavra $g_1\ g_2 \ldots g_s$, então definimos o produto das palavras W e U por justaposição das palavras, ou seja, $f_1\ f_2 \ldots f_n\ g_1\ g_2 \ldots g_s$.

Exemplo 2.4.1 *Se W_1 (a, b, c) = $aa^{-1}c$ e W_2 (a, b, c) = $c^{-1}b$ então, $W_1 W_2$=$aa^{-1}cc^{-1}b$ e além disso, L($W_1 W_2$) = 5 = L(W_1)+L(W_2). Temos ainda que, $(W_1 W_2)^{-1}$ $b^{-1}cc^{-1}aa^{-1}$ = ${W_2}^{-1}{W_1}^{-1}$.*

Proposição 2.4.1 *Para duas palavras W (a, b, c, ...) e V (a, b, c, ...), segue que: $(WV)^{-1}$= V^{-1} W^{-1} e L(WV) = L(W) + L(V).*

2.5 Geradores

Definição 2.5.1 *Quando todo elemento $g \in G$ é obtido a partir de seus elementos a, b, c,..., então dizemos que a, b, c,... são geradores de G.*

Exemplo 2.5.1 *Dado $G = S_3$, com a = (1 2 3) e b = (1 2), então os elementos de S_3 são descritos pelas seguintes palavras W_0(a, b) = 1 , W_1(a, b) = a, W_2(a, b) = a^2, W_3(a, b) = b, W_4(a, b) = ab, W_5(a, b) = ba. Em suma, a e b são os geradores do grupo G.*

2.6 Relator e relação

A palavra $R(a, b, c, \ldots)$ que define a identidade 1 em G é chamada de relator. Intuitivamente um relator é apenas um auxiliar para ocorrer a relação que leva um elemento do grupo ao elemento neutro. No Exemplo 2.5.1, a^3 e b^2 são relatores, uma vez que $a^3 = 1$ e $b^2 = 1$.

A equação $R(a, b, c, \ldots) = S(a, b, c, \ldots)$ é chamada uma relação se a palavra RS^{-1} é um relator, equivalentemente, se R e S definem o mesmo elemento em G.

Em qualquer grupo a palavra vazia e as palavras aa^{-1}, $a^{-1}a$, bb^{-1}, $b^{-1}b$, cc^{-1}, $c^{-1}c$, ..., são sempre relatores, eles são chamados de relatores triviais.

2.7 Apresentação

Supondo que P, Q, R são relatores quaisquer de G. Dizemos que uma palavra é originada de P, Q, R, ..., se as seguintes condições, aplicadas com um número finito de vezes, transforma W na palavra vazia:

i) Inserção de uma das palavras P, P^{-1}, Q, Q^{-1}, R, R^{-1}, ... ou dos relatores triviais entre quaisquer dois símbolos consecutivos de W, antes de W, ou depois de W.

ii) Eliminando de uma das palavras P, P^{-1}, Q, Q^{-1}, R, R^{-1}, ..., ou dos relatores triviais, se ela forma um bloco consecutivo de símbolos em W.

Exemplo 2.7.1 *A palavra* $ab(aa)^{-1}ab$ *é originada da palavra abab.*

Claro que se W é uma palavra originada dos relatores P, Q, R, ..., então W é um relator de si mesmo.

Se qualquer relator é originado dos relatores P, Q, R, ..., então P, Q, R, ..., definem um conjunto de relatores ou um conjunto completo de relatores para o grupo G com os geradores a, b, c, ... Se P, Q, R é um conjunto de relatores definidos para o grupo G sobre os geradores a, b, c, ..., dizemos que < a, b, c, .../ P(a, b, c, ...); R(a, b, c, ...); ... > é uma **apresentação** de um grupo G e escrevemos G = < a, b, c, ...,P, Q, R, ... >.

Dizemos que a referida apresentação é finitamente gerada (finitamente relatada) se o número de geradores (relações definidas) é finito. Se uma apresentação é finitamente gerada e finitamente relatada, dizemos que a apresentação é finita.

Exemplo 2.7.2 *Seja G um grupo tal que* $G = < a, b \ / \ a^2 = 1, b^2 = 1, ab = ba >$. *Então, G tem uma apresentação finita.*

Dado o conjunto de símbolos a, b, c, ..., e um conjunto (possivelmente vazio) de palavras P, Q, R, ..., em a, b, c, ..., então podemos mostrar que existe um único grupo (a menos de isomorfismo) com a apresentação < a, b, c, .../ P, Q, R, ... >.

A afirmação acima na realidade está descrita em [15] sob a forma de um Teorema, no qual existem outros conceitos envolvidos e que, no momento, estudá-los não são convenientes (devido a sua complexidade). Para melhor compreensão desta afirmação seguem os exemplos.

Exemplo 2.7.3 *O grupo G com a apresentação* $< a \ / \ a^6 = 1 >$ *é tal que* $G \cong \mathbb{Z}_6$. *Especificamente, a menos de um isomorfismo, só existe um grupo de ordem 6, e cíclico.*

Exemplo 2.7.4 *Dado* $G = < a, b/a^3 = 1, b^2 = 1, ab = ba^2 >$, *e considerando que em* S_3 *existem dois elementos, a saber* $(123)e(12)$ *com ordem 3 e 2, respectivamente e ainda que (1 2 3)(1 2) = (1 2)(1 3 2), então, a menos de um isomorfismo, só existe um grupo não abeliano de ordem 6, isto é, o* S_3.

Exemplo 2.7.5 *O grupo G com a apresentação* $< a/a^4 = 1 >$ *é tal que* $G \cong \mathbb{Z}_4$. *Especificamente, a menos de um isomorfismo, só existe um grupo de ordem 4 e cíclico.*

Exemplo 2.7.6 *O grupo* $G =< a, b/a^2 = 1, b^2 = 1, ab = ba >$ *é tal que* $G \cong \mathbb{Z}_2 \times \mathbb{Z}_2$, *ou seja, a menos de um isomorfismo só existe um grupo de ordem 4 abeliano e não cíclico.*

Capítulo 3

Grupos abelianos finitamente gerados

Neste capítulo usaremos a notação aditiva, pois todos os grupos que consideraremos são abelianos. Iniciaremos este fazendo uma abordagem sobre grupos abelianos livres, com o intuito de enunciarmos, demonstrarmos e aplicarmos o Teorema Fundamental para Grupos Abelianos Finitamente Gerados, nosso suporte teórico esta alicerçado em Fraleigh (2003).

3.1 Grupos abelianos livres

Revisaremos a noção de um conjunto de geradores para um grupo G e grupo finitamente gerado. Além disso, conforme mencionamos acima trataremos de grupo abeliano finitamente gerado com a notação aditiva, ou seja:
i) 0 para a identidade, + para a operação;
ii) $nx = \underbrace{x + x + x + \ldots + x}_{n}$,com n parcelas, se $n \in \mathbb{Z}^*$ e $x \in G$ e $-nx = (-x) + (-x) + (-x) + \ldots + (-x)$, com n parcelas;
iii) $0x = 0$ para o primeiro zero em $\mathbb{Z}$ e o segundo em G.

Continuaremos usando o símbolo $\times$ para o produto direto de grupos (Conforme 1.11).

Para reforçar os conceitos acima mencionados, segue:

Exemplo 3.1.1 *O conjunto* $\{(1,0),(0,1)\}$ *é constituído de geradores para o grupo* $\mathbb{Z} \times \mathbb{Z}$ *já que* $(n,m) = n(1,0) + m(0,1)$ *para qualquer* (n,m) *em* $\mathbb{Z} \times \mathbb{Z}$. *Este conjunto de geradores tem a propriedade que cada elemento pode ser unicamente expressado na forma* $n(1,0) + m(0,1)$. *Isto é, os coeficientes* m *e* n *são únicos.*

Teorema 3.1.1 *Seja X é um conjunto de um grupo abeliano $G \neq \{0\}$. As seguintes condições em X são equivalentes:*
i) Cada elemento não nulo $a \in G$ pode ser expressado unicamente na forma $a = n_1x_1 + n_2x_2 + \ldots + n_rx_r$, com $n_i \neq 0$, em $\mathbb{Z}$ e elementos distintos x_i em X.
ii) X gera G, e $n_1x_1 + n_2x_2 + \ldots + n_rx_r = 0$ para $n_i \in \mathbb{Z}$ e elementos distintos x_i em X, se, e somente se, cada n_i for nulo, ou seja, $n_1 = n_2 = \ldots = n_r = 0$.

Prova 3.1.1 *Suponha a condição i) verdadeira. Como $G \neq \{0\}$, temos que $X \neq \{0\}$. Segue de i) que $0 \notin X$, pois se $x_i = 0$ e $x_j \neq 0$, então $x_j = x_i + x_j$, o qual contradiz a unicidade da expressão de x_j. De i), X gera G, e $n_1x_1 + n_2x_2 + \ldots + n_rx_r = 0$ se $n_1 = n_2 = \ldots = n_r = 0$. Supondo que $n_1x_1 + n_2x_2 + \ldots + n_rx_r = 0$ com algum $n_i \neq 0$; estando os termos restantes com coeficientes zero e reescrevendo n_i, podemos assumir todos os $n_i \neq 0$. Então:*

$$x_1 = x_1 + (n_1x_1 + n_2x_2 + \ldots + n_rx_r) = (n+1)x_1 + (n_2x_2 + n_2x_2 + \ldots + n_rx_r),$$

o qual escreve $x_1 \neq 0$ de duas formas, contradizendo o item i) que afirma existir um único modo para escrever cada elemento. Assim a condição i) implica a condição ii).
Mostraremos agora que a condição ii) implica a condição i). Seja $a \in G$ como X gera G, podemos escrever a da seguinte forma $a = n_1x_1 + n_2x_2 + \ldots + n_rx_r$. Suponha que exista outra forma para escrever a em termo de X. Usando os coeficientes não nulos das duas expressões, podemos assumir que eles envolvem os mesmos elementos em X e são da forma:

$$a = n_1x_1 + n_2x_2 + \ldots + n_rx_r = 0$$

$$a = m_1x_1 + m_2x_2 + \ldots + m_rx_r = 0$$

Subtraindo as equações acima, obtemos:

$$a = (n_1 - m_1)x_1 + (n_2 - m_2)x_2 + \ldots + (n_r - m_r)x_r = 0,$$

assim $n_i - m_j = 0$ pala condição ii), e $n_i = m_i$ para $i \in \{$ 1, 2, ..., r $\}$. Desta forma os coeficientes são únicos.

Definição 3.1.1 *(Grupo Abeliano Livre) Um grupo abeliano G tendo um conjunto de geradores X (não vazio) satisfazendo as condições descritas no Teorema* 3.1.1 *é um grupo abeliano livre, e X é uma base para G*

Exemplo 3.1.2 *O grupo $\mathbb{Z} \times \mathbb{Z}$ é abeliano livre e $\{(1,0),(0,1)\}$ é uma base. De forma análoga temos que $\{(1,0,0),(0,1,0),(0,0,1)\}$ é uma base para o grupo abeliano $\mathbb{Z}\times\mathbb{Z}\times\mathbb{Z}$. Assim, produtos direto finito do grupo $\mathbb{Z}$ com ele mesmo são grupos abelianos livres.*

Exemplo 3.1.3 *O grupo $\mathbb{Z}_m$ não é abeliano livre, pois $mx = 0$ para qualquer $x \in \mathbb{Z}_m$ e $m \neq 0$, o que contradiz a condição ii) do Teorema* 3.1.1.

Teorema 3.1.2 *Se $G \neq \{0\}$ é um grupo abeliano livre com uma base de r elementos, então G é isomorfo a $\mathbb{Z} \times \mathbb{Z} \times \mathbb{Z} \times \ldots \times \mathbb{Z}$ para r fatores.*

Prova 3.1.2 *Suponha que o grupo abeliano livre G tem uma base finito$X = \{x_1, x_2, \ldots x_r\}$. Se $a \in G$ e $a \neq 0$, então, pelo Teorema* 3.1.1*, a tem uma única expressão da forma:*

$$a = n_1x_1 + n_2x_2 + \ldots + n_rx_r \text{ para } ni \in \mathbb{Z}.$$

Considere a seguinte aplicação:

$$\phi : G \to \mathbb{Z} \times \mathbb{Z} \times \ldots \times \mathbb{Z} \text{ com r fatores, definida por}$$

$\phi(a) = (n_1, n_2, \ldots, n_r)$ *e* $\phi(0) = (0, 0, \ldots, 0)$. *Assim ϕ é um isomorfismo.*

Teorema 3.1.3 *Se $G \neq \{0\}$ é um grupo abeliano livre com uma base finita. Então qualquer base de G é finita, e todas as bases tem o mesmo número de elementos.*

Prova 3.1.3 *Se G tem uma base $\{x_1, x_2, \ldots, x_r\}$. Então, G é isomorfo a $\mathbb{Z} \times \mathbb{Z} \times \ldots \times \mathbb{Z}$ para r fatores (Teorema* 3.1.2*). Seja $2G = \{2g/g \in G\}$. Pode ser verificado que $2G$ é um subgrupo de G. Como $G \cong \mathbb{Z} \times \mathbb{Z} \times \ldots \times \mathbb{Z}$) para r fatores, então temos,*

$$G/2G \cong (\mathbb{Z} \times \mathbb{Z} \times \ldots \times \mathbb{Z})/(2\mathbb{Z} \times 2\mathbb{Z} \times \ldots \times 2\mathbb{Z}) \cong \mathbb{Z}_2 \times \mathbb{Z}_2 \times \ldots \times \mathbb{Z}_2,$$

para r fatores. Assim $|G/2G| = 2^r$, e neste caso o número de elementos de qualquer base finita X é $r = log_2^{|G/2g|}$. Portanto qualquer duas bases finitas tem o mesmo número de elementos.
Agora mostraremos que G não pode ter uma base infinita. Seja Y uma base qualquer de G, e seja $\{y_1, y_2, \ldots, y_s\}$ elementos distintos em Y. Seja H um subgrupo de G gerado por $\{y_1, y_2, \ldots, y_s\}$ e seja K um subgrupo de G gerado pelos elementos restantes de Y. Então $G \cong H \times K$, com $G/2G \cong (H \times K) / (2H \times 2K) \cong (H/2K) \times (k/2K)$.
Como $|H/2H| = 2^s$ temos que $|G/2G| \geq 2^s$. Como $|G/2G| = 2^r$ segue que $s \leq r$. Então Y não pode ser um conjunto infinito, pois teríamos $s > r$.

Definição 3.1.2 *Se G é um grupo abeliano livre, o posto de G é o número de elementos em uma base de G. Além disso, todas as bases tem o mesmo número de elementos.*

Exemplo 3.1.4 *Uma base para $\mathbb{Z} \times \mathbb{Z}$ é $\{(1, 0), (0, 1)\}$, com posto 2. Veja que $\{(1, 1), (0, 1)\}$ é outra base para o referido grupo, também com posto 2.*

Teorema 3.1.4 *Se G é um grupo abeliano finitamente gerado com conjunto de geradores $\{a_1, a_2, \ldots, a_n\}$. Seja:*

$$\phi : \mathbb{Z} \times \mathbb{Z} \times \ldots \times \mathbb{Z} \to G, \text{ com } n \text{ fatores,}$$

sendo definida por $\phi(h_1, h_2, \ldots, h_n) = h_1a_1.h_2a_2.\ldots.h_na_n$. *Então* ϕ *é um homomorfismo sobre G.*

Prova 3.1.4 *Sejam* $(h_1, h_2, \ldots, h_n)$ *e* $(k_1, k_2, \ldots, k_n)$ *elementos de* $\mathbb{Z} \times \mathbb{Z} \times \ldots \times \mathbb{Z} \to G$. *Então* $\phi[(h_1, h_2, \ldots, h_n) + (k_1, k_2, \ldots, k_n)] = \phi(h_1 + k_1, h_2 + k_2, \ldots h_n + k_n)$
$= (h_1 + k_1)a_1 + (h_2 + k_2)a_2 + \ldots + (h_n + k_n)a_n$
$= h_1a_1 + k_1a_1 + h_2a_2 + k_2a_2 + \ldots + h_na_n + k_na_n$
$= (h_1a_1 + k_1a_1) + (h_2a_2 + k_2a_2) + \ldots + (h_na_n + k_na_n)$
$= (h_1a_1 + h_2a_2 + \ldots + h_na_n) + (k_1a_1 + k_2a_2 + \ldots + k_na_n)$
$=\phi\ (k_1, k_2, \ldots, k_n\ ) + \phi\ (\ h_1, h_2, \ldots, h_n\ )$.
Desde que $\{a_1, a_2, \ldots, a_n\}$ *geram G, segue que* ϕ *é um homomorfismo sobrejetor.*

Teorema 3.1.5 *Se* $X = \{x_1, x_2, \ldots, x_r\}$ *é uma base para um grupo abeliano livre G e t* $\in \mathbb{Z}$, *então para* $i \neq j$, *o conjunto*

$$Y = \{x_1, x_2, \ldots, x_{j-1}, tx_i, x_j, x_{j+1} \ldots, x_r\}$$

é também uma base para G.

Prova 3.1.5 *Desde que* $x_j = (-t)x_i + (1)(x_j + tx_i)$, *temos que* x_j *pode ser retirado de Y, o qual também gera G.*
De fato, supondo que:

$$n_1x_1 + \ldots + n_{j-1}x_{j-1} + n_jx_j + n_itx_i + n_{j+1}x_{j+1} + \ldots + n_rx_r = 0.$$

então

$$n_1x_1 + \ldots + (n_in_jt)x_i + \ldots + n_jx_j + \ldots + n_rx_r = 0,$$

e sendo X uma base, segue $n_1 = \ldots = n_in_jt = \ldots = n_r = 0$.
De $n_j = 0$ *e de* $n_in_jt = 0$, *segue que* $n_i = 0$ *e também* $n_1 = n_2 = \ldots n_j = \ldots n_r = 0$, *e a condição ii) do Teorema* 3.1.1 *é satisfeita. Assim Y é uma base para G.*

Exemplo 3.1.5 *Uma base para* $\mathbb{Z} \times \mathbb{Z}$ *é* $\{(1, 0), (0, 1)\}$. *Outra base é* $\{(1, 0), (4, 1)\}$ *e (4, 1) é da forma 4 (1, 0) + (0, 1) = (4, 1). Contudo* $\{(3, 0), (0, 1)\}$ *não é uma base. Por exemplo, não podemos expressar (2,0) na forma* $n_1(3, 0) + n_2(0, 1)$ *com n e m* $\in \mathbb{Z}$. *Aqui (3,0)= (1,0)+ 2(1,0).*

Um grupo abeliano livre de posto finito pode ter muitas bases. Mostraremos que se K é um subgrupo de G, então K também é abeliano livre com posto dele não excedendo o posto de G.

Teorema 3.1.6 *Seja $G \neq \{0\}$ um grupo abeliano livre de posto finito n, e seja K é um subgrupo não nulo de G. Então K é um grupo abeliano livre de posto $s \leq n$. Além disso, se existe uma base $\{x_1, x_2, \ldots, x_n\}$ de G e inteiros positivos $d_1, d_2, \ldots, d_s$, onde d_i divide d_{i+1} para i = 1, ..., s-1, no qual $\{d_1x_1, d_2x_2, \ldots, d_sx_s\}$ é uma base de K.*

Prova 3.1.6 *Suponha que $Y = \{y_1, \ldots, y_n\}$ seja uma base de G. Todos os elementos em K podem ser expressos da forma $k_1y_1 + k_2y_2 + \ldots + k_ny_n$, onde alguns $|k_i|$ não são nulos. Entre todas as bases de G, selecione uma base Y_1 tal que o mínimo sendo um valor não nulo $|k_i|$, assim todos os elementos de K são escritos em termos dos elementos da base em Y_1.*
Substituindo os elementos de Y_1 se necessário, podemos assumir que existe $w_1 \in K$ tal que

$$w_1 = d_1y_1 + k_2y_2 + \ldots + K_ny_n,$$

onde $d_1 > 0$ e d_1 é o menor coeficiente para alcançar toda a descrição pretendida.
Usando o algoritmo da divisão, escrevemos $k_j = d_1q_j + r_j$, onde $0 \leq r_j < d_1$ para j = 2, 3, ... , n. Então:

$$w_1 = d_1(y_1 + q_2y_2 + \ldots + q_ny_n)$$

Agora seja $x_1 = y_1 + q_2y_2 + ... + q_ny_n$. Pelo Teorema 3.1.5 *, $\{x_1, y_2, \ldots, y_n\}$ é também uma base para G.*
Da Equação 3.1.6 *e da escolha do coeficiente minimal em Y_1, vemos que $r_1 = r_2 = \ldots = r_n = 0$. Assim, $d_1x_1 \in K$.*

Considere agora uma base para G da forma $\{x_1, y_2, \ldots, y_n\}$. Cada elemento K pode ser expresso na forma:

$$h_1x_1 + k_2y_2 + \ldots + k_ny_n,$$

Como $d_1x_1 \in K$, podemos subtrair um múltiplo adequado de d_1x_1 e então usando a minimalidade de d_1 vemos que h_1 é um múltiplo de d_1, e $k_2y_2 + \ldots + k_ny_n \in K$. Dentre todas as bases $\{x_1, y_2, \ldots, y_n\}$ escolhemos uma base Y_2 tal que conduz a um mesmo $k_i \neq 0$de magnitude minimal.

Neste caso, k é gerado por d_1x_1.

Renumerando os elementos de Y_2 podemos assumir que existe $w_2 \in k$ tal que

$$w_2 = d_2y_2 + \ldots + k_ny_n,$$

onde $d_2 < 0$ e d_2 é o elemento minimal descrito acima. Desta forma, como fizemos acima, podemos modificar a base de $Y_2 = \{x_1, y_2, \ldots, y_n\}$ para a base $\{x_1, x_2, y_3 \ldots, y_n\}$ para G onde $d_1x_1 \in K$ e $d_2x_2 \in K$. Escrevendo $d_2 = d_1q + r$ para $0 \leq r < d_1$, vemos que $\{x_1 + qx_2, x_2, y_3, \ldots, y_n\}$ é uma base para G, e $d_1x_1 + d_2x_2 = d_1(x_1 + qx_2) + rx_2 \in k$. Pela escolha do elemento minimal d_1, temos que $r = 0$ e assim d_1 divide d_2.

Agora, consideremos todas as bases da forma $\{x_1, x_2, y_3 \ldots, x_n\}$ *para* G *examine os elementos de* k *da forma* $k_3y_3, \ldots, k_ny_n$.

Continuaremos o processo a fim de obtermos a base $\{x_1, x_2, \ldots, x_n, y_{s+1}, \ldots, y_n\}$ *onde somente o elemento de* K *da forma* $k_{s+1}y_{s+1} + \ldots + k_ny_n$ *é zero, isto é, todos os* k_i *são nulos. Então seja* $x_{s+1} = y_{s+1}, \ldots, x_n = y_n$ *e assim obtemos uma base para* G*, como queríamos demonstrar.*

3.2 Grupos Abelianos Finitamente Gerados

O nosso próximo passo é enunciar, demonstrar e aplicar o Teorema Fundamental para Grupos Abelianos Finitamente Gerados.

Teorema 3.2.1 *Qualquer grupo abeliano finitamente gerado é isomorfo ao grupo da forma* $\mathbb{Z}_{d_1} \times \mathbb{Z}_{d_2} \times \ldots \times \mathbb{Z}_{d_r} \times \mathbb{Z} \times \ldots \times \mathbb{Z}$*, de onde cada* d_i *divide* d_{i+1} *para* $i = 1, \ldots, r_{-1}$.

Prova 3.2.1 *Por conveniência usaremos as notações* $\mathbb{Z}/1\mathbb{Z} = \mathbb{Z}/\mathbb{Z} \cong \mathbb{Z}_1 = \{0\}$.

Seja G *um grupo abeliano gerado por* n *elementos e considere o grupo abeliano livre de posto* n *como* $F = \mathbb{Z} \times \mathbb{Z} \times \ldots \times \mathbb{Z}$.

Do Teorema 3.1.4 *segue que* $\varphi : F \to G$ *é um homomorfismo.*

Seja K *o kernel desse homomorfismo. Então, pelo Teorema* 3.1.6*, existe uma base de* F *da forma* $\{x_1, ..., x_n\}$ *onde* $\{d_1x_1, d_2x_2, \ldots, d_sx_s\}$ *é uma base para* K *e* d_i *divide* d_{i+1} *para* $i = 1, \ldots, s-1$.

Logo, pelo Teorema 1.15.1 *temos que* $F/K \cong Im\ \varphi$

$$Mas\ F/K = (\mathbb{Z} \times \mathbb{Z} \times \ldots \times \mathbb{Z})/(d_1\mathbb{Z} \times d_2\mathbb{Z} \times \ldots \times d_1\mathbb{Z} \times 0 \times \ldots \times 0) \cong$$
$$\mathbb{Z}d_1 \times \mathbb{Z}d_2 \times \ldots \times \mathbb{Z}d_s \times \mathbb{Z} \times \mathbb{Z} \times \mathbb{Z} \times \ldots \times \mathbb{Z}.$$

Corolário 3.2.1 *Todo grupo abeliano finitamente gerado* $G = < x_1, \ldots, x_n >$ *tem uma apresentação da forma*

$$G \cong \left\langle y_1, \ldots, y_{m+s} / y_i^{d_i}, 1 \leq i \leq m, x_iy_j = x_jy_i, 1 \leq i < j \leq m+s \right\rangle,$$

onde $d_i \geq 2$ *e* d_i/d_{i+1} *, i = 1, 2, ... m-1.*

Exemplo 3.2.1 *Seja* G *um grupo abeliano de ordem 360. Primeiramente vamos expressar 360 na forma* $2^3.3^2.5$*. Assim pelo teorema 3.1.6 e corolário* 1.15.1*, temos que:*
$G_1 = \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2\mathbb{Z}_3 \times \mathbb{Z}_3 \times \mathbb{Z}_5$
$G_2 = \mathbb{Z}_2 \times \mathbb{Z}_4 \times \mathbb{Z}_3 \times \mathbb{Z}_3 \times \mathbb{Z}_5$
$G_3 = \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2\mathbb{Z}_9 \times \mathbb{Z}_5$
$G_4 = \mathbb{Z}_2 \times \mathbb{Z}_4 \times \mathbb{Z}_9 \times \mathbb{Z}_5$
$G_5 = \mathbb{Z}_8 \times \mathbb{Z}_3 \times \mathbb{Z}_3 \times \mathbb{Z}_5$
$G_6 = \mathbb{Z}_8 \times \mathbb{Z}_9 \times \mathbb{Z}_5$
portanto existem seis diferentes grupos (a menos de isomorfismo) de ordem 360.

Capítulo 4

Proposta

Este capítulo esta alicerçado em Noronha (2014).

4.1 Por que (-a).(-b) = ab?

Atualmente, os números negativos são comuns no dia a dia. Estando presentes nas medidas de temperaturas, altitudes, deslocamentos, calendário, fuso horário, questões de natureza contábil. Mas nem sempre foi assim. Os números negativos tem a origem incerta, existem registros de obras envolvendo tais números, pelos chineses, 200 a.C., mas somente no século XVII é que os matemáticos passaram a usar os negativos com desembaraço. O próprio nome desses números nos mostram o quanto eles foram vistos com desconfiança, pois números negativos representa negação, ou seja, não número. O ensino dos números negativos é um grande desafio para nós professores, pois a não compreensão do conceito de números negativos, faz com que o aluno crie outras dificuldades. Segundo Borba(2009), a aprendizagem dos números inteiros relativos é importante à compreensão de outros conceitos matemáticos e para a resolução de diversos problemas como os que envolvem álgebra, funções e o cálculo de quantidades. Constata-se então, que a não compreensão dos números inteiros, além de dificultar a aprendizagem de outros conceitos, prejudica também a resolução de situações que envolvem as operações nesse conjunto, como a multiplicação e a divisão. Uma dificuldade que temos, em relação aos números negativos, é repassar aos alunos a famosa regra de sinal da multiplicação, pois muitas vezes esta regra é imposta aos alunos, sem justificativas. O aluno por sua vez, apenas memoriza tal regra, o que torna sem sentido as operações com números negativos. Alguns livros didáticos trazem ilustrações para justificarem a regra de sinais, estas ilustrações são bons artifícios didáticos, mas que na maioria das vezes, tornam-se regras de memorização. Apresentaremos abaixo algumas dessas ilustrações:

i) Considere (+) sendo amigo e (-) sendo inimigo. Assim:

O amigo de meu amigo é meu amigo, ou seja (+).(+)=(+);

O amigo de meu inimigo é meu inimigo, ou seja (+).(-)=(-);

O inimigo de meu amigo é meu inimigo, ou seja (-).(+)=(-);
O inimigo de meu inimigo é meu amigo, ou seja (-).(-)=(+).
ii) Considere um ganho representado por um número positivo e a perda por um número negativo, considere ainda o tempo no futuro por um número positivo e no passado por um número negativo, assim:
iii)Se uma pessoa perde 5 reais por dia, então daqui 3 dias terá perdido 15 reais, ou seja (-5).(+3)= -15;
iv)Se uma pessoa perde 5 reais por dia, então há 3 dias estava com 15 reais a mais, ou seja (-5).(-3)= +15.
v) Considere a sequência: $3.(-2) = -6; 2.(-2) = -4; 1.(-2) = -2; 0.(-2) = 0$. Continuando a sequência teremos, $-1.(-2) = 2; -2.(-2) = 4$.
Iremos apresentar agora, uma maneira algébrica que responde a pergunta que foi colocada como título desta seção, porque (-a).(-b) = ab? Consequentemente, justificar a regra de sinal da multiplicação.
Pois bem, vimos no Capítulo 1 que $(\mathbb{Z}, +)$ é um grupo abeliano e que, mesmo $(\mathbb{Z}, .)$ não sendo grupo, verificam-se algumas propriedades:
i) Existência do elemento neutro, que é o número 1;
ii) Além disso a multiplicação é distributiva em relação à adição, ou seja, $a.(b + c) = ab + ac, a, b, c \in \mathbb{Z}$.

As citadas propriedades são importantes para mostrarmos que: $(-a).(-b) = ab$. De fato, inicialmente mostraremos que $a.0 = 0, \forall$ a $\in \mathbb{Z}$.

Considere a um número inteiro qualquer, assim $a + a.0 = a.1 + a.0 = a(1 + 0) = a.1 = a = a + 0$, portanto $a + a.0 = a + 0$ e fazendo o cancelamento, temos que $a.0 = 0$. Agora podemos mostrar que $(-1).a = -a$ para todos número inteiro a.

Considere a um número inteiro qualquer, assim $a + (-1).a = 1.a + (-1)a = [1 + (-1)].a = 0.a = 0$. Assim a e $(-1)a$ são simétricos, pois $a + (-1).a = 0$, ou seja, $(-1)a = -aea = -[(-1)a]$. Em particular, fazemos $a = -1$, temos que $(-1).(-1) = -(-1) = 1$, generalizando, temos $(-a).(-b) = (-1).a.(-1).b = (-1).(-1).ab = 1.ab = ab$.

Com isso terminamos a demonstração e concluímos que o produto de dois números inteiros negativos é sempre um número inteiro positivo. Alguns professores podem achar que esta demonstração é muito abstrata para apresentar aos seus alunos, mas se o professor partir de casos particulares, conseguirá fazer com que o aluno compreenda tal demonstração.

4.2 A Criptografia e o conjunto $\mathbf{Z}_m$

Na criptografia, o processo de converter um texto original para um texto cifrado é chamado de codificação ou cifragem, e o processo de reverter é chamado de decodificação ou decifragem.

Definição 4.2.1 *Sejam P o conjunto de todas as possíveis mensagens unitárias u do texto original e C todas as possíveis mensagens unitárias c do texto cifrado, assim a correspondência biunívoca*

$$f: P \to C \text{ tal que } f(u) = c \text{ é o processo de codificação. E a correspondência biunívoca}$$
$$f^{-1} : C \to P \text{ tal que } f^{-1}(c) = u$$

é o processo de decodificação. Qualquer uma dessa bijeções de P sobre C recebe o nome de Criptossistemas.

Normalmente substituímos as letras do alfabeto usado por números inteiros 0, 1, 2, ... para tornar mais agradável a construção do criptossistema f. As barras dos elementos de $\mathbb{Z}_m$ serão omitidas ao longo do texto, para não carregar o mesmo. Fazendo a correspondência identidade entre o alfabeto $\{A, B, C, \ldots X, Y, Z\}$ e o conjunto dos números inteiros $\mathbb{Z}_{27} = \{0, 1, 2, 3, \ldots, 26\}$ chegamos:

A	B	C	...	K	...	Z
↕	↕	↕	↕	↕	↕	↕
0	1	2	...	10	...	26

Teorema 4.2.1 *Sejam $m \in \mathbb{N}$ e a, $b \in \mathbb{Z}_m$ fixados. Se $mdc(a, m) = 1$, então a função $f : \mathbb{Z}_m \to \mathbb{Z}_m$ dada por $f(x) = ax + b$ é um criptossistema.*

Prova 4.2.1 *Como $mdc(a, m) = 1$ temos que existe $a^{-1} \in Z_m^*$ tal que $a.a^{-1} = 1$. Assim $f^{-1}(x) = a^{-1}x + b^{-1}$ onde $b^{-1} = -ba^{-1}$, é tal que f o $f^{-1} = f^{-1}$ o $f = I\mathbb{Z}_m$, isto é, f^{-1} é a função inversa de f.*

O criptossistema f(x) = ax+b é chamado de transformação afim, onde o par (a, b) é chamado de chave de codificação. Quando m = 27, a = 1 e b $\in \mathbb{Z}_{27}$ o criptossistema f(x) = x + b temos as famosas Cifras de César. Apresentaremos agora um exemplo de criptossistemas, codificaremos o texto original PROFMAT, com a chave de codificação (2, 4). Primeiramente faremos a correspondência numérica.

P	R	O	F	M	A	T
↕	↕	↕	↕	↕	↕	↕
15	17	14	5	12	0	19

Agora passaremos a codificar o texto original usando a função f(x) = 2 x + 4, onde x representa o correspondente numérico da mensagem original e $f(x)$ representa o correspondente numérico da mensagem codificada. Daí:

$f(15) = 2.15 + 4 = 34 \equiv 7 \; mod \; 27$;

$f(17) = 2.17 + 4 = 38 \equiv 11 \; mod \; 27$;

$f(14) = 2.14 + 4 = 32 \equiv 5 \; mod 27$;

$f(5) = 2.5 + 4 = 14$;

$f(12) = 2.12 + 4 = 28 \equiv 1 \; mod \; 27$;

$f(0) = 2.0 + 4 = 4$;
$f(19) = 2.19 + 4 = 42 \equiv 15\ mod\ 27$.

Fazendo novamente a correspondência numérica, temos:

7	11	5	14	1	4	15
↕	↕	↕	↕	↕	↕	↕
H	L	F	O	B	E	P

Portanto o texto original PROFMAT cifrado com a chave (2, 4) é HLFOBEP Iremos agora decodificar esta mensagem HLFOBEP. Primeiro calculamos a inversa da função f(x) = 2x + 4 que é a função f^{-1}(x) = 2^{-1} - 4.f^{-1}. Daí calculando os inversos temos:

$$2^{-1} \equiv 2^{\varphi(27)-1} \equiv 2^{\varphi(1)}.7 \equiv 14 mod 27;\ \text{-}4.2^{-1} \equiv \text{-}4.14 \equiv 23.14 \equiv 322 \equiv 25 mod 27$$

Assim $f^{-1}(x) = 14x + 25$ e fazendo:
$f^{-1}(7) = 14.7 + 25 = 123 \equiv 15\ mod\ 27$
$f^{-1}(11) = 14.11 + 25 = 179 \equiv 17\ mod\ 27$
$f^{-1}(5) = 14.5 + 25 = 95 \equiv 14\ mod\ 27$
$f^{-1}(14) = 14.14 + 25 = 221 \equiv 5\ mod\ 27$
$f^{-1}(1) = 14.1 + 25 = 39 \equiv 12\ mod\ 27$
$f^{-1}(4) = 14.4 + 25 = 81 \equiv 0\ mod\ 27$
$f^{-1}(15) = 14.15 + 25 = 235 \equiv 19\ mod\ 27$
Portanto após decodificar o texto cifrado, chegamos em 15 17 14 5 12 0 27 que fazendo a relação numérica chegamos, no texto original PROFMAT.

Capítulo 5

Conclusão

Motivado por práticas educacionais não significativas para os alunos, tornando as aulas de matemática, especificamente as aulas de Álgebra, ainda mais complicadas, levando o aluno a decorar regras que não contribuem adequadamente para a formação do jovem, construímos este trabalho com o objetivo de ser um material de apoio, indicando um caminho para o ensino de matemática utilizando algumas propostas. Para atingir este objetivo, recomendamos que o professor enfatize o quarto capítulo, todavia os iniciantes ao estudo da teoria de grupos podem usar os capítulos anteriores para fornecer suporte teórico para outras propostas e ou até mesmo para um estudo mais aprofundado acerca da teoria de grupos podendo contribuir para uma aprendizagem mais significativa.

Assim ao planejar uma aula o professor poderá escolher uma destas propostas ou formular outra proposta para fortalecer a aprendizagem , escolhe-se qual a habilidade a ser atingida, e uma estratégia para atingi-las, e a partir, de aplicações na realidade do aluno ou que desperte curiosidade no mesmo.

Com um professor preocupado em buscar caminhos que facilitarão a aprendizagem de Matemática, teremos melhores condições para desmistificar o conceito de ciência inerte no ensino de Matemática, que necessita apenas de memorização de procedimentos e fórmulas. Também, colocará os alunos como sujeito ativo do processo de ensino e aprendizagem. Fazendo da Matemática uma construção humana, e que deve ser compreendida como uma parcela de conhecimento humano essencial a formação de todos os jovens, a qual contribui na construção de uma visão de mundo, para ler e interpretar a realidade e para desenvolver capacidades que deles serão exigidas ao longo da vida social e profissional. O professor tem importância fundamental no processo de oportunizar uma melhor aprendizagem aos discentes do ensino médio, mostrando por exemplo, as demonstrações de algumas propriedades inseridas na Álgebra, Geometria, Matemática Financeira, etc.

No caso da Álgebra, apesar de conter um certo formalismo em sua linguagem e necessitar da utilização de procedimentos não muito simples, exigindo um maior grau de abstração, é importante lembrar que a forma do professor trabalhar conteúdos matemáticos deve abranger também a linguagem formal. Por exemplo, para os alunos torna-

se mais fácil, memorizar que menos com menos é mais do que entender a justificativa algébrica do porque $-(-x) = x$ para $\forall \in \mathbb{R}$ e a última proposta que é uma atividade de criptografia que pode até se aplicada de forma lúdica, onde os alunos criarão um código criptográfico para se comunicarem e assim poderão estudar criptografia de uma forma significativa.

Referências Bibliográficas

Borba, R. (2009). *O que pode influenciar a compreensão de conceitos: o caso dos números relativos*. Borba, R. e Guimarães, G. A pesquisa em Educação Matemática: repercussões na sala de aula, São Paulo: Cortez.

Domingues, H. H. e Iezzi, G. (2003). *Álgebra moderna*. Atual.

Fgueiredo, L. M. S. (2006). *Números primos e criptografia de chave pública*. Rio de Janeiro: Universidade Federal Fluminense.

Fraleigh, J. B. (2003). *A first course in abstract algebra*. Pearson Education India.

Garcia, A. e Lequain, Y. (1988). *Algebra: um curso de introduçao*. IMPA.

Garcia, A. e Lequain, Y. (2003). *Elementos de álgebra*. Instituto de Matemática Pura e Aplicada.

Gonçalves, A. (2006). *Introdução a Álgebra, ed*. IMPA., 5ªed, Rio de Janeiro.

Hefez, A. (2011). *Elementos de Aritmética, 2ª*. Edição. Rio de Janeiro, SBM.

Lima, E. L. (2006). *Meu professor de matemática: e outras histórias*. Sociedade Brasileira de Matemática.

Magnus, W., Karrass, A., e Solitar, D. (2004). *Combinatorial group theory: Presentations of groups in terms of generators and relations*. Courier Corporation.

Noronha, V. R. A. d. (2014). *Grupos e algumas aplicação*. Universidade Federal de Mato Grosso.

Santos, J. P. d. O. (2010). *Introdução à teoria dos números*. Instituto de Matemática Pura e Aplicada.

Silva, V. V. (2003). *Números: Construções e propriedades*. Cegraf-UFG. Goiânia-Go.

Singh, S. (2007). *O livro dos códigos tradução de Jorge Calife*. Rio de Janeiro: Record.