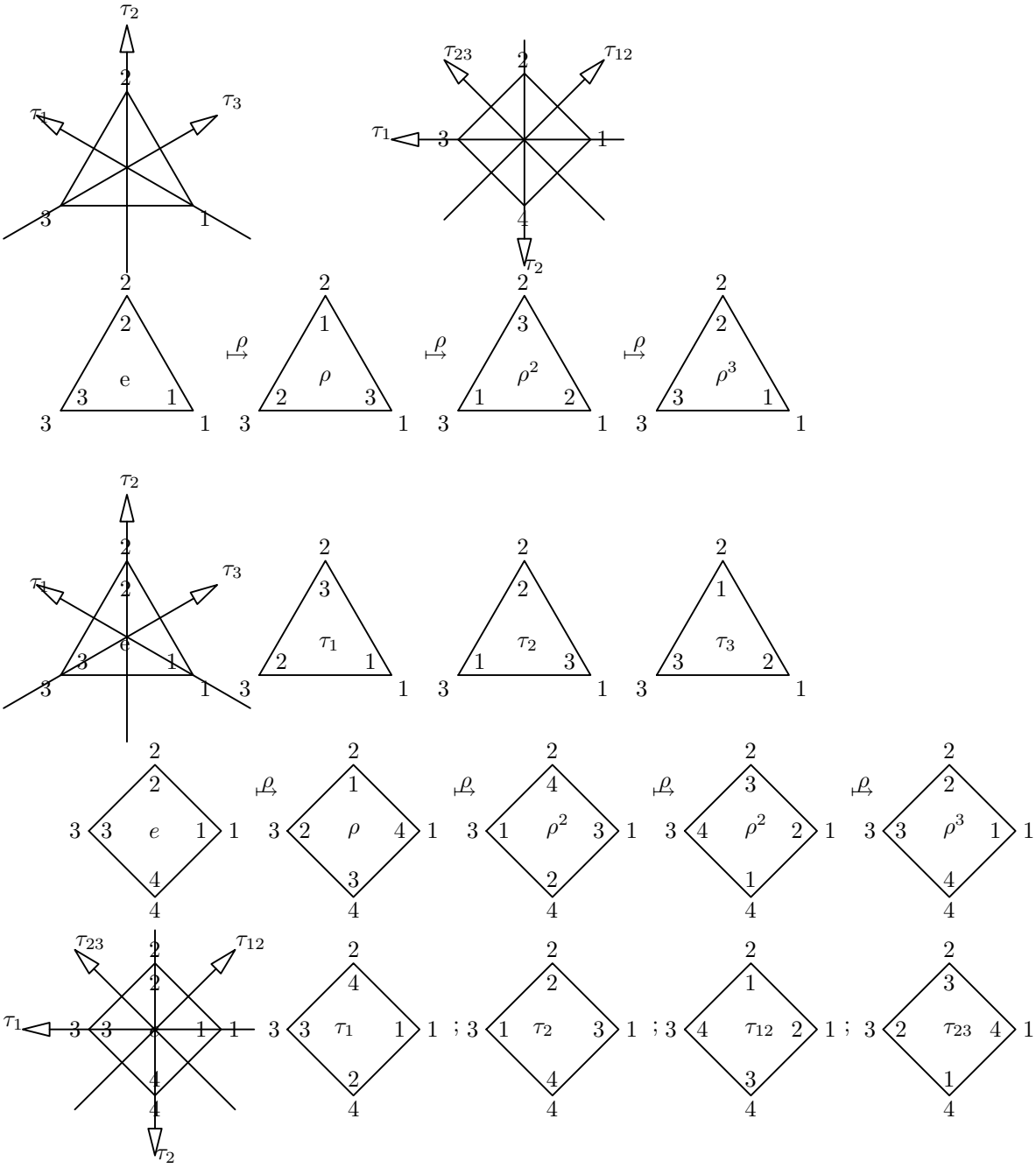


Preparação e Aplicação de Material Didático para Introdução à Álgebra Elementar em Cursos de Licenciatura

Autor Antônio Calixto de Souza Filho;

Sumário

Introdução

Segundo Benjamim Pierce a Matemática é a ciência que obtém conclusões necessárias. Esperamos contribuir com este texto para um primeiro estudo em álgebra, mais especificamente em teoria de grupos.

Uma reflexão sobre o que é necessário para estudar e compreender uma teoria matemática, ou uma teoria em geral, parece de fundamental importância quando o objetivo é introduzir elementos dessa teoria.

Na preparação deste material, que se propõe a um livro, procedemos norteados por este critério, mesmo que inicialmente seja necessário desenvolver um assunto essencialmente fundamental como a teoria de conjuntos.

Esperamos superar as dificuldades juntos e concluir nossa introdução à teoria de grupos com o consenso de sua necessidade.

Capítulo 1

Conjuntos, Relações e Funções: uma breve abordagem

A Matemática ... .

A noção de conjunto é considerada a partir de nossa intuição racional de agrupar objetos em geral. É um consenso que uma definição de conjunto iniciaria uma cadeia de novas definições, pois a cada definição dada, a palavra que estiver ligada ao sentido de conjunto deverá ser definida, e assim sucessivamente. Desse modo teríamos que parar em algum momento e aceitar esse termo como algo intuitivo e sem necessidade de definição, portanto consideramos já inicialmente a noção de conjunto com essa característica.

Estando de acordo com a noção intuitiva de conjunto, os objetos que formam o conjunto serão denotados como elementos do conjunto. Essa condição é representada pelo símbolo $\in$, indicando que um certo objeto é elemento do conjunto.

Dado um conjunto, podemos nomeá-lo de qualquer modo, mas, assim como nomeamos as pessoas, devemos dar nomes aos conjuntos que evitem algum tipo de confusão ou interpretação equivocada. Geralmente, o conjunto é representado através de uma lista de seus elementos, entre chaves e separados por vírgula.

Por exemplo $A = \{1, 2, 3, 4\}; ano = \{2004, 2005\}; V = \{a, e, i, o, u\}; Tipo = \{A, ano, V\}$. Assim dizemos que 1 é elemento de A e denotamos isso por $1 \in A$, como $2 \in A$, estes elementos ficam separados por vírgula. Finalmente, as chaves delimitam os conjuntos, e cada par $\{;\}$ determina um conjunto. Assim, segundo o exemplo anterior o conjunto Tipo é um conjunto de conjuntos, que também poderia ser representado por $Tipo = \{\{1, 2, 3, 4\}, \{2004, 2005\}, \{a, e, i, o, u\}\}$. Nesse caso, verificamos que 1 não é elemento do conjunto Tipo, pois não aparece no conjunto Tipo como elemento, isto é, separado por vírgula(s), e entre as chaves do conjunto Tipo. Um

modo simples de compreender isso é o seguinte, imagine que cada chave aberta inicie uma cor diferente desta chave, por exemplo, a primeira chave aberta no conjunto Tipo inicie a cor verde, sendo a própria chave de cor diferente de verde, e a segunda chave inicie a cor amarela, sendo esta segunda chave verde. No conjunto A, o número 1, $1 \in A$, seria verde, enquanto que no conjunto Tipo, esse número, $1 \notin Tipo$, seria amarelo. Ou seja, nessas condições um dado objeto é elemento de um conjunto somente se a cor que a chave inicia é mesma cor deste elemento, escolhida obviamente uma cor para cada chave aberta.

Ocorre que um conjunto pode ter muitos elementos! Por exemplo, seja *brasil* o conjunto de todos os brasileiros, ou X o conjunto de todos os brasileiros residentes no Brasil. Esses conjuntos certamente estão delimitados por chaves, mas com muitos elementos. O conjunto *brasil* é um conjunto maior ainda que X. Podemos representar um conjunto pela propriedade que seus elementos satisfazem, portanto $X = \{y$, tal que, $y \in$ brasil é residente no brasil$\}$. Observe que os elementos de X estão delimitados por chaves. Existem, ainda, conjuntos que são conhecidos apenas por seus nomes, como o conjunto dos números naturais, cujo símbolo é $\mathbb{N}$. Nesse caso $\mathbb{N} = \{0, 1, 2, 3, \cdots\}$. Estas são as formas mais clássicas de representação de um conjunto. Porém devemos utilizar modos precisos para representar os conjuntos, pois sem rigor podemos chegar a problemas conceituais ou mesmo erros.

Historicamente, o matemático Alemão Cantor, no século XIX, contribuiu com muito o que se conhece da teoria de conjuntos atualmente. Até aquele momento acreditávasse que dada uma propriedade P, os objetos que satisfizessem P formariam um conjunto. Por exemplo se a propriedade P fosse: X é um conjunto, então existiria o conjunto de todos os conjuntos, isto é, $\{X$,tal que, X é um conjunto$\}$ seria um conjunto? No início do século XX, no entanto, a teoria de conjuntos necessitou de um tratamento formal para que se evitasse contradições. Um fato importante, nesse sentido, foi o paradoxo de Russel, que contribuiu para esclarecer a nâo existência de conjuntos do tipo "o conjunto de todos os conjuntos", ou conjuntos obtidos a partir de uma dada propriedade. Esse paradoxo pode ser facilmente enunciado como segue:

Seja P a propriedade "$X \notin X$"e R a lista de objetos que satisfazem a propriedade P, isto é: $R = \{X$, tal que, $X \notin X\}$. Se consideramos que R é um conjunto, então temos o seguinte paradoxo: ocorre que $R \in R$ e $R \notin R$, simultaneamente! Um absurdo.

Tal construção é um paradoxo, no sentido que se R é um conjunto, para todo elemento X, ou ocorre que $X \in R$ ou $X \notin R$. Se dada a propriedade P acima e R a lista de objetos que satisfazem P, ou R é um conjunto ou R não é um conjunto. Caso suponhamos que R seja um conjunto, então tomamos $X = R$, isto é, podemos testar se R é, ou não, um elemento de R como conjunto. Então ocorre uma, e somente uma das seguintes condições:

(1) se $R \in R$, então R satisfaz a propriedade P, isto é $R \notin R$. Assim $R \in R$, por hipótese, e $R \notin R$ pela definição de R, portanto uma impossibilidade;

(2) se $R \notin R$, então R satisfaz a propriedade P, portanto $R \in R$, por força da definição de R, a mesma impossibilidade.

Desse modo, supor que R é um conjunto leva ao paradoxo que $R \in R$ e $R \notin R$. Daí este paradoxo mostra que nem toda lista de elementos, que satisfazem uma certa propriedade, define um conjunto. A seguir, apresentamos os axiomas da teoria de conjuntos; o Axioma da Separação deve ser confrontado com o paradoxo de Russel, de modo que se tenha uma idéia mais ampla do significado deste paradoxo. Por exemplo, a relação entre este paradoxo e a inexistência do conjunto de todos os conjuntos.

Tal construção levou essa área da matemática, que atualmente é conhecida por Fundamentos, a reformular a teoria de conjuntos. A axiomática, isto é, construção de uma teoria através de axiomas, foi o melhor resultado obtido nessa busca pela reformulação da teoria de conjuntos e os axiomas utilizados são os de Zermelo e Fraenkel e o Axioma da Escolha. Lembrando que axioma é uma regra fundamental, sem possibilidade ou necessidade de demonstração. Por exemplo os axiomas de Geometria.

1.1 Noção dos axiomas de Zermelo Frankel

Como apresentado, estamos supondo uma noção intuitiva de conjunto, cujo único símbolo é $\in$ (lê-se "é elemento"), que indica se um dado elemento está ou não no conjunto. Por motivo didático, apresentaremos ainda os símbolos $\subset$ e $\subseteq$, que indicam quando um conjunto tem os mesmos elementos de um outro conjunto, podendo ser iguais. Isto é, sejam A, B conjuntos; $A \subset B \Rightarrow \forall x \in A, x \in B$, que se lê: A é subconjunto de B se, e somente se, para todo x elemento do conjunto A, ocorre que x é elemento do conjunto B. O outro símbolo é utilizado, por exemplo para a condição $A \subseteq A$. Repetimos: somente o símbolo $\in$ é utilizado a priori, os demais podem ser definidos a partir dos axiomas abaixo. Apresentamos estas definições antes dos axiomas apenas para simplificar a compreensão.

Para os assuntos que estudaremos são suficientes os axiomas de 1 a 7, inicialmente apresentamos os axiomas e posteriormente exemplificamos e comentamos aqueles que utilizaremos com mais freqüência:

1. Axioma da Existência: existe um conjunto, denotado por $\emptyset$ para o qual qualquer elemento não está neste conjunto, isto é, $(\forall x), (x \notin \emptyset)$.

2. Axioma da Extensionalidade: Dados dois conjuntos A, B, se a condição $A = B$ ocorre, então $(\forall x \in A)(x \in B) \Rightarrow (\forall x \in B)(x \in A)$.

3. Axioma do Par: Dados dois conjuntos A, B, existe o conjunto $\{A, B\}$, o qual A e B são seus únicos elementos.

4. Axioma da União: Para qualquer conjunto A, existe o conjunto Y, tal que, os elementos de Y são exatamente os elementos dos elementos do conjunto A, isto é, $(\forall X \in A)(\forall y \in X)(y \in Y)$.

5. Axioma da Separação (ou Axioma do Subconjunto) Dado qualquer conjunto A e qualquer proposição $P(x)$, existe um subconjunto do conjunto A, que contém precisamente aqueles elementos para o qual $P(x)$ ocorre.

6. Axioma das Partes: Dado um conjunto A, existe o conjunto $\wp(A)$, cujos elementos de $\wp(A)$ são precisamente os subconjuntos de A.

7. Axioma do Infinito: Existe um conjunto A, tal que, $(\forall x \in A)(x \cup \{x\} \in A)$.

8. Axioma da Substituição: Dados um conjunto A e uma aplicação $P(x, y)$, existe um conjunto B, cujos elementos são precisamente a imagem do conjunto A.

9. Axioma da Regularidade: Para todo conjunto A, não vazio, $(\exists x \in A)(x \cap A = \emptyset)$.

10. Axioma da Escolha: Dado um conjunto A, de conjuntos não vazios e dois a dois disjuntos, existe um conjunto X (ou um conjunto escolha para A), que contém exatamente um elemento de cada membro do conjunto A, isto é, $(\forall A)(a, b \in A)(a, b \neq \emptyset)(a \cap b = \emptyset)(\exists X)(\forall a \in A)(\exists! u \in a)(u \in X)$.

A melhor forma de compreender os axiomas é exemplificar e estudar algumas propriedades, possíveis a partir da apresentação do axioma em particular. Acima estão apresentados todos os axiomas, como caráter informativo. Não é nossa intenção aqui estudar todos estes axiomas, porém apenas alguns deles, que devem auxiliar a compreensão da notação a ser seguida, bem como fundamentar algumas idéias que são essenciais à teoria de grupos e anéis.

1.1.1 Os Axiomas da Existência, Extensionalidade e do Par

O axioma $A1$ garante que existe um conjunto, com a propriedade que para qualquer elemento x não ocorre que x seja elemento deste conjunto, denominado de Conjunto Vazio. Podemos observar que o primeiro axioma garante que existe um conjunto sem elementos! Mas, esse mesmo axioma permite concluir que o conjunto vazio é único? Tal propriedade é possível de ser provada a partir de $A2$, o segundo axioma. Passamos então a consideração, também do axioma $A2$.

O axioma $A2$, elucida um problema bastante comum com conjuntos, que é a repetição de seus elementos. Por exemplo se, já avançados na teoria de conjuntos, aceitamos que além do conjunto vazio, existem outros conjuntos, fato que será garantido pelo $A3$, sejam $A = \{1, 2, 3\}$ e $B = \{1, 2, 1, 3, 2, 1\}$ dois conjuntos. Estes conjuntos são iguais? Essa questão, do ponto de vista lógico pode ter muitos desdobramentos, porém segundo o axioma $A2$, os conjuntos são iguais, pois $(\forall x \in A)(x \in B) \Rightarrow (\forall x \in B)(x \in A)$, ou seja, A é subconjunto de B e B é subconjunto de A, isto é, $A \subseteq B$ e $B \subseteq A$. Também podemos responder à questão sobre a unicidade (existência de um único objeto) do conjunto vazio. De fato! Se consideramos que o vazio não é único, é porque existe um conjunto vazio ϕ, tal que $\phi \neq \emptyset$, portanto segundo o axioma $A2$, um desses conjuntos deve possuir um elemento que não está no outro, mas isso não ocorre, pois ambos são conjuntos vazios e o $A1$ garante que tal conjunto não admite elementos, portanto $\phi = \emptyset$, logo a unicidade do conjunto vazio, sendo este o único conjunto que existe, segundo os axiomas $A1$ e $A2$

Há pouco, consideramos o conjunto $A = \{1, 2, 3\}$, embora, até este ponto, exista apenas o conjunto vazio; como podemos garantir que existe o conjunto A? Esse é o conteúdo dos axiomas $A3$ e $A4$, os axiomas do par e da união, respectivamente. Vejamos que o axioma $A3$ é um construtor de conjuntos. De fato, vamos mostrar que existem conjuntos unitários. Para isso considere a axioma $A1$, que garante que existe o conjunto vazio. No axioma $A3$, fazemos $A = B = \emptyset$, então segundo $A3$, existe o conjunto $C = \{\emptyset, \emptyset\}$, que pelo $A2$, é igual a $\{\emptyset\} \neq \emptyset$, pois $\emptyset \in C$, portanto C é não vazio, logo não é o conjunto vazio. Passamos a conhecer, segundo os axiomas dois conjuntos: o vazio e o unitário do vazio. Porém se utilizarmos o axioma $A3$ para o unitário do vazio, isto é $A = B = \{\emptyset\}$, obtemos o conjunto $\{\{\emptyset\}\}$ um conjunto unitário, porém diferente do unitário do vazio, isto é, pelo $A3$, $\{\emptyset\} \neq \{\{\emptyset\}\}$, pois como vimos $\emptyset$ é elemento do primeiro conjunto, $\{\emptyset\}$ é elemento do segundo conjunto e já mostramos que eles são diferentes, logo os conjuntos que os contêm são diferentes. Podemos construir conjuntos unitários, e como fizemos nos dois casos anteriores, sempre obteremos conjuntos unitários diferentes. O que mostra que existem infinitos conjuntos unitários distintos.

Se, ainda com o axioma $A3$, consideramos $A = \{\emptyset\}$ e $B = \{\{\emptyset\}\}$, então $C = \{\emptyset, \{\emptyset\}\}$ um conjunto com dois elementos. Assim, como existem infinitos conjuntos unitários, também podemos construir infinitos conjuntos de dois elementos, porém o axioma do par permite construir apenas os conjuntos unitários e os conjuntos com 2 elementos, pois como vimos, ou $A = B$, e $C = \{A, B\} = \{A, A\} = \{A\}$, ou $A \neq B$, e $C = \{A, B\}$ um conjunto com dois elementos. Para construir conjuntos com mais de 2 elementos, precisamos do axioma $A4$.

1.1.2 Os Axiomas da União e da Separação

A construção que daremos agora permite construir conjuntos finitos de tamanhos arbitrários. Inicialmente, contruimos um conjunto com 3 elementos, do seguinte modo:

- Tomemos o conjunto obtido segundo os axiomas $A1$ e $A2$, $C = \{\emptyset, \{\emptyset\}\}$ com dois elementos e o conjunto unitário $D = \{C\} = \{\{\emptyset, \{\emptyset\}\}\}$. Segundo o axioma 2 existe o conjunto $A = \{C, D\}$;
- Usamos o axioma $A4$, com o conjunto A obtido acima. Explicitando o conjunto temos: $A = \{\{\emptyset, \{\emptyset\}\}, \{\{\emptyset, \{\emptyset\}\}\}\}$. Assim existe o conjunto Y, cujos elementos são os elementos dos elementos, quando estes também são conjuntos, do conjunto A; os elementos de A são os conjuntos C e $\{C\}$, portanto o conjunto $Y = \{\emptyset, \{\emptyset\}, \{\emptyset, \{\emptyset\}\}\}$, com 3 elementos.
- Podemos interpretar a operação acima, feita a partir do axioma $A4$, do seguinte modo: $Y = C \cup \{C\} = \{y$, tal que, $y \in X$, sendo $X \in A\}$, ou seja a união dos elementos de A, como conjuntos, quando for este o caso.

Desse modo obtivemos o conjunto $\{\emptyset, \{\emptyset\}, \{\emptyset, \{\emptyset\}\}\}$, com 3 elementos. Podemos definir novos conjuntos do tipo A e obter assim conjuntos finitos com número de elementos arbitrários.

Definição 1.1.1. *Se A é um conjunto, $|A|$ denota o número de elementos de A, também denominado cardinalidade de A. Quando A for um conjunto finito, escreveremos $|A| < \infty$, caso contrário $|A| = \infty$.*

Mas de onde vem o conjunto $H = \{1, 2, 3\}$? Pois o que construimos foi o conjunto $Y = \{\emptyset, \{\emptyset\}, \{\emptyset, \{\emptyset\}\}\}$, $|Y| = 3$. O que fazemos, nesse caso, é identificar números com conjuntos e daí associar 1 ao conjunto $\{\emptyset\}$; 2 ao conjunto $\{\emptyset, \{\emptyset\}\}$ e 3 ao conjunto $\{\emptyset, \{\emptyset\}, \{\emptyset, \{\emptyset\}\}\}$. Assim identificados, com os axiomas $A3$ e $A4$, construimos o conjunto $\{\{\emptyset\}, \{\emptyset, \{\emptyset\}\}, \{\emptyset, \{\emptyset\}, \{\emptyset, \{\emptyset\}\}\}\}$ que é identificado com o conjunto $\{1, 2, 3\}$. Para o leitor interessado, essa identificação é a construção axiomática do conjunto dos números naturais, sendo o número 0 identificado com o conjunto vazio.

Observe, ainda, que o número natural identificado com o conjunto corresponde ao número de elementos desse conjunto, por exemplo, $|\emptyset| = 0$. Rigorosamente, dado um conjunto cujos elementos são conjuntos, contruir um outro conjunto, formado pelos naturais identificados com o número de elementos de cada conjunto, como feito acima, é possível a partir o axioma $A8$, o axioma da substituição, em que, por exemplo, dado o conjunto

$$A = \{\{\emptyset\}, \{\emptyset, \{\emptyset\}\}, \{\emptyset, \{\emptyset\}, \{\emptyset, \{\emptyset\}\}\}\},$$

e a aplicação que a cada elemento $X \in A$, associamos o número $y = |X|$, existe o conjunto formado pelos elementos y, que é o conjunto $\{1, 2, 3\}$; isto é, se A é um conjunto, $P(x, y) = y/y = |x|, \forall x \in A, \exists Y = \{y/P(x, y)\}$

O axioma $A5$ garante que, dado um conjunto qualquer A, existe um subconjunto de A que satisfaz uma dada propriedade $P(X)$. Devemos observar que, inicialmente, é garantido que A seja um conjunto. Essa hipótese é essencial, pois caso isso não seja verificado podemos obter paradoxos, como o de Russel.

Exemplo 1.1.2. *(1) Sejam $\mathbb{Z}$ o conjunto dos números inteiros e a propriedade $P(x) =$ "$\exists y \in \mathbb{Z}/x + y = 0$". O conjunto $\{z/P(z), z \in \mathbb{Z}\}$ é o próprio conjunto dos numeros inteiros;*

(2) Sejam $\mathbb{Z}$ o conjunto dos números inteiros e a propriedade $P(x) =$"o número x é positivo ou nulo"; neste caso existe o conjunto $\mathbb{N} = \{n$, tal que, ocorre $P(n), n \in \mathbb{Z}\}$ que é o conjunto dos números naturais;

(3) Sejam $\mathbb{R}$ o conjunto dos números reais e a propriedade $P(x) =$"o conjunto dos números da forma $\frac{p}{q}$, sendo $p, q \in \mathbb{Z}$ e $q \neq 0$"; pelo $A5$ existe o conjunto $frac = \{x/P(x), x \in \mathbb{R}\}$. Este pode ser obtido a partir do conjunto dos números inteiros, mas como $frac$ não é subconjunto de $\mathbb{Z}$, tal construção não é possível pelo axioma $A5$, o axioma que permite tal construção é o axioma $A8$. Veremos mais à frente que este conjunto não é o conjunto dos números racionais, veja [4]

(4) Sejam $\mathbb{Z}$ e a propriedade $P(x) =$ "$x \notin \{-1, 0, 1\}$ e os únicos divisores de x são ± 1 e $\pm x$"; segundo o axioma $A5$ existe o conjunto $\{p/P(p), p \in \mathbb{Z}\}$ conhecido como o conjunto dos números primos em $\mathbb{Z}$.

Um exemplo importante é quando, dados um conjunto C e a propriedade $P(X)$, os elementos do conjunto C não verificam a propriedade $P(X)$, ou seja o conjunto $\{x/P(x), x \in C\} = \emptyset$, que é um subconjunto de C, como demonstrado na proposição que segue.

Proposição 1.1.3. *Seja C um conjunto; $\emptyset \subseteq C$*

Demonstração. Se $C = \emptyset$, ocorre a igualdade. Sendo $\emptyset$ o conjunto vazio, pelo axioma $A1$, $\nexists x \in \emptyset$, portanto não ocorre a condição do conjunto $\emptyset$ possuir elemento que não esteja no conjunto C, logo a condição $\emptyset \nsubseteq C$ NÃO OCORRE, portanto $\emptyset \subseteq C$. □

Corolário 1.1.4. *Se A é um conjunto, então $A \subseteq A$.*

1.1.3 O Axioma das Partes

Vamos expor algumas considerações sobre o axioma $A6$, o axioma das partes, pela sua importância no contexto do assunto Relações e Funções, que são fundamentais para apresentação da

Teoria de Grupos. Os demais axiomas, embora importantes, não serão discutidos, por questões de prioridades em nossos objetivos. O leitor interessado pode consultar a referência [1], que aborda minuciosamente este assunto.

Como vimos, os axiomas são dedicados construtores de conjuntos e, teoricamente, garantem a existência de certos tipos deles. Segundo o axioma $A5$, dado um conjunto, podemos obter subconjuntos desse conjunto através de uma adequada propriedade $P(X)$. Mas como garantir que podemos determinar TODOS os subconjuntos de um conjunto dado? Este é o conteúdo do axioma $A6$, isto é, dado um conjunto A, existe o conjunto cujos elementos são precisamente os subconjuntos do conjunto A. De posse da proposição 1.1.3, o exemplo mais simples é o conjunto vazio: seja $A = \emptyset$, pela referida proposição $\emptyset \subseteq \emptyset$, e nenhum outro conjunto tem esta propriedade, porque é não-vazio. Assim o conjunto dos subconjuntos de $\emptyset$, denotado por $\wp(\emptyset) = \{\emptyset\}$.

Exemplo 1.1.5. *(1) Seja* $= \{1\}$ *o conjunto unitário do número* 1*. Pelo axioma* $A6$*, existe* $\wp(\{1\})$*; pela proposição 1.1.3,* $\emptyset$ *é subconjunto de* $\{1\}$*, pelo corolário dessa proposição, o próprio conjunto é subconjunto dele mesmo; sendo este conjunto unitário não existe nenhum outro subconjunto deste, portanto* $\wp(\{1\}) = \{\emptyset, \{1\}\}$

(2) Seja $A = \{x, y, z\}$*; se* $C \subseteq A$*, então os únicos elementos possíveis, supondo* $C \neq \emptyset$*, de* C *são* x, y, z*, portanto* C *é um conjunto unitário, ou de* 2 *elementos, ou o próprio conjunto* A*, logo,*

$$\wp(A) = \{\emptyset, \{x\}, \{y\}, \{z\}, \{x, y\}, \{x, z\}, \{y, z\}, \{x, y, z\}\};$$

(3) Se $A = \{\emptyset, \{\emptyset\}, \{\emptyset, \{\emptyset\}\}\}$*,* $|A| = 3$*, portanto identificando os elementos de* A*, com* x, y, z*, recaímos no caso anterior e podemos determinar* $\wp(A)$*.*

Dado um conjunto A, o axioma $A6$, garante a existência do conjunto $\wp(A)$. Se A é um conjunto finito, isto é, $|A| = n \in \mathbb{N}$, quantos elementos possui o conjunto $\wp(A)$? Se fizermos um estudo dos primeiros casos possíveis teremos:

$\lvert A\rvert$	$\lvert\wp(A)\rvert$	$2^{\lvert A\rvert}$
0	1	$1 = 2^0$
1	2	$2 = 2^1$
2	4	$4 = 2^2$
3	8	$8 = 2^3$
$\vdots$	$\vdots$	$\vdots$
n	2^n	2^n

A última linha da tabela acima é um resultado bastante conhecido, para o caso finito. Uma prova pode ser feita por indução finita. Comentamos rapidamente o esquema de uma prova por indução finita. Basicamente há dois tipos de prova por indução finita: o princípio de indução

finita e o princípio de indução finita completa. Uma discussão excelente pode ser encontrada na referência [7]. Observamos, ainda que o resultado acima também vale para o caso de conjuntos infinitos. Este assunto está além deste material, neste caso a prova do resultado é por indução transfinita.

A prova por indução ocorre pelo o seguinte esquema: devemos provar para o primeiro caso em que ocorre o resultado, este passo é denominado $P(n_0)$; supomos que seja válido o resultado para um número inteiro k, ou seja, assumimos válido, por hipótese, o fato que queremos provar para o inteiro k, esta é a hipótese de indução. Feito isso, consideramos o problema para o inteiro $k+1$ e devemos demonstrar que, sendo verdadeiro para k, o será para $k+1$, este é o passo de indução. Ou seja $P(k)$ é verdadeiro $\Rightarrow P(k+1)$ é verdadeiro.

Teorema 1.1.6. *Seja A um conjunto finito, o número de elementos do conjunto das partes de A, isto é, $|\wp(A)| = 2^{|A|}$*

Demonstração. Vamos provar por indução sobre a ordem de A. O primeiro caso é para um conjunto A, tal que, $|A| = 0$, isto é $A = \emptyset$, portanto, como vimos no exemplo, $|\wp(A)| = 1 = 2^0 = 2^{|A|} \therefore P(n_0)$ é verdadeira. Em seguida supomos que quando $|A| = k$, $|\wp(A)| = 2^k$. Vamos mostrar, que nessas condições, o resultado vale para $|A| = k+1$. De fato! Seja A um conjunto com $k+1$ elementos, digamos $A = \{a_1, a_2, \cdots, a_{k-1}, a_k, a_{k+1}\}$; podemos escrever o conjunto A de outro modo: $A = \{a_1, \cdots, a_k\} \cup \{a_{k+1}\} = B \cup \{a_{k+1}\}$, isto é, a união entre um conjunto B com k elementos, $|B| = k$, e um conjunto unitário, que resultará num conjunto de $k+1$ elementos, pois $a_{k+1} \notin B$; por hipótese de indução $|\wp(B)| = 2^k$, seja $Partes = \{X \cup \{a_{k+1}\}/X \in \wp(B)\}$, que existe segundo o axioma $A8$. Os conjuntos X tomados na união, são elementos das partes do conjunto B, portanto $a_{k+1} \notin X, \forall X \in \wp(B)$, então todos os elementos do conjunto $\wp(B)$ são diferentes dos elementos do conjunto $Partes$, isso significa que $B \cap Partes = \emptyset$, portanto $|\wp(B)| = |Partes|$. Afirmamos que $\wp(A) = \wp(B) \cup Partes$, de fato nesta união estão todos os subconjuntos de A que não contêm a_{k+1}, provenientes do conjunto B, e todos os subconjuntos de A que contêm a_{k+1}, provenientes do conjunto $Partes$, logo todos os subconjuntos de A estão nessa união, e portanto a igualdade dos conjuntos $\wp(A) = \wp(B) \cup Partes$. Finalmente! o número de elementos da união é exatamente a soma do número de elementos de cada componente dessa união, isto é, $|\wp(A)| = |\wp(B)| + |Partes|$, isso ocorre pela propriedade de interseção vazia, logo $|\wp(A)| = 2^k + 2^k = 2.2^k = 2^{k+1} = 2^{|A|}$, e provamos que o resultado vale para $k+1$, portanto está provado por indução finita que $|\wp(A)| = 2^{|A|}, \forall |A| = n \in \mathbb{N}$. □

Recomendamos ao leitor provar alguns detalhes dessa demonstração, como por exemplo a igualdade da união dos conjuntos, utilizando os axiomas. Nesse caso o axioma $A2$. Também sugerimos que o leitor aplique a construção da demonstração para conjuntos com 4 ou 5 elementos, utilizando o resultado dado no exemplo para um conjunto com 3 elementos.

O axioma das partes terá diversas aplicações no que estudaremos a seguir. Entre muitas de suas aplicações, estão algumas referentes às técnicas de contagem, por exemplo, já sabemos contar o número de subconjuntos de um conjunto com 10 elementos. O resultado é $2^{10} = 1024$ elementos, pois se A é um conjunto com 10 elementos, $|A| = 10$, daí pelo teorema anterior obtemos o resultado.

1.1.4 Números Binomiais

Um outro problema muito comum com conjuntos e subconjuntos é a contagem de subconjuntos com um numero fixo de elementos. Por exemplo, num conjunto com 10 elementos, há 1024 subconjuntos. Quantos deles são vazios? O leitor atento, rapidamente responde 1, pois sabe que existe um único conjunto vazio, pelos axiomas $A1, A2$. Também é imediato que há 10 conjuntos unitários, pois $|A| = 10$. Mas quantos subconjuntos de A existem com exatamente 2 elementos? Com 8 elementos? ... Enfim com k elementos, sendo $0 \leq k \leq 10$? Este problema clássico é conhecido por problema binomial. Abaixo enunciamos o problema binomial e indicamos uma referência onde pode ser encontrada uma demonstração do resultado.

Inicialmente definimos:

Definição 1.1.7. *Seja n um numero natural. Definimos $n! = n(n-1)!$ sendo que $0! \doteq 1$.*

Segundo a definição acima $1! = 1(1-1)! = 1.0! = 1.1 = 1$; $4! = 4.3! = 4.3.2! = 4.3.2.1! = 24$. Os números fatoriais são freqüentes em problemas de contagem, como observamos no seguinte lema.

Lema 1.1.8. *Seja A um conjunto com n elementos, isto é, $|A| = n$. Se X denota um subconjunto de A com exatamente k elementos, então o número de subconjuntos X é $\binom{n}{k} \doteq \frac{n!}{k!(n-k)!}$.*

Demonstração. ver [7] □

Exemplo 1.1.9. *(1) Dado o conjunto $\{0,1,2,3,4,5,6,7,8\}$, quantos subconjuntos com 3 elementos podem ser formados? Segundo o lema, o número de subconjuntos com 3 elementos é $\binom{9}{3} = \frac{9!}{3!(9-3)!} = \frac{9.8.7.6!}{3!6!} = \frac{9.8.7}{6} = 84$;*

(2) Em uma sala com 13 pessoas, quantas comissões de 5 pessoas podem ser formadas? Este problema equivale a determinar o número de subconjuntos com 5 elementos, de um conjunto com 13 elementos, verifique! Pelo lema, o número de comissões será $\binom{13}{5} = \frac{13!}{5!(13-5)!} = \frac{13.11.10.9.8!}{5!8!} = \frac{13.11.10.9}{120} = 1287$;

(3) Seja A um conjunto com 12 elementos, quantos subconjuntos têm mais de 4 elementos? Observe que a solução deve ser discutida. Poderíamos calcular os subconjuntos de

$5, 6 \cdots, 11, 12$ *elementos e somar tudo, mas podemos usar a idéia de complementar, isto é, o número total de subconjuntos é exatamente* $|\wp(A)| = 2^{12} = 4096$*; em seguida calculamos o número de subconjuntos com até 4 elementos, isto é,* $\binom{12}{0}+\binom{12}{1}+\binom{12}{2}+\binom{12}{3}+\binom{12}{4}=794$*, portanto o resultato é* $4096 - 794 = 3302$ *conjuntos são subconjuntos de A que têm mais de 4 elementos;*

(4) Um conjunto com n elementos tem 2^n *subconjuntos. Estes subconjuntos também podem ser obtidos somando o número de subconjuntos com* $0 \leq k \leq n$ *elementos, isto é:*

$$\binom{n}{0} + \binom{n}{1} + \binom{n}{2} + \cdots + \binom{n}{n-1} + \binom{n}{n} = 2^n = (1+1)^n$$

O axioma das partes também é central, para estudo de relações e funções, quando consideramos problemas de contagens para estes objetos. Isso já se evidencia com alguns problemas ligados ao produto cartesiano, que definimos na próxima seção, embora, uma leitura atenta irá indicar que estes problemas são equivalentes num contexto mais geral: as relações e as funções.

Sugerimos ao leitor textos complementares, pois há uma certa variação na linguagem e notação sobre este assunto. Lembramos que o texto apresentado é básico, recomendado como uma iniciação à teoria de conjuntos e motivação para adentrar em seu universo.

Exercícios 1.1.10. *(1) Para os conjuntos* $A = \{1, 2, 2\}, B = \{1, 2, 2, 3, 1\}, C = \{(1, 2), (2, 1)\}, D = \{1, 2, 2, 1\}, E = \{(1, 2)\}, F = \{1, 2\}, G = \{(1, 1)\}, H = \{(1, \{1\})\}, I = \{1, \{1\}\}, J = \{2, 1, 1, 2\}, K = \{1, 2, 3\}$*. Quais são iguais?*

(2) Seja $X = \{1, 2, 3\}$*. Determine os conjuntos*

- *(a)* $\wp(X)$*;*
- *(b)* $Partes = \{A \cup \{4\}/A \in \wp(X)\}$*;*
- *(c)* $\wp(X) \cup Partes$*;*
- *(d) Compare este último com o conjunto* $\wp(\{1, 2, 3, 4\})$*.*

(3) Para cada item a seguir determine os valores de x, y, z*, conforme o caso*

- **a.** $\{x - y, x + y + 3\} = \{2x + 3y + 2, x - 2y\}$
- **b.** $\{0, 2, 4, z\} \subseteq \{4, x, y\}$
- **c.** $\{1, x, y\} \subseteq \{0, 2, 4, z\}$

(4) Seja A um conjunto e $\wp(A)$ *o conjunto de todos os subconjuntos de A. Lembrando que se A e B são dois conjuntos,* $A \setminus B = \{a/a \in A, a \notin B\}$*. Dê exemplos de conjuntos A para os seguintes casos:*

- **a.** $\wp(A) = \{\emptyset, \{\emptyset\}, \{1\}, \{2\}, \{\emptyset, 1\}, \{\emptyset, 2\}, \{1, 2\}, \{\emptyset, 1, 2\}\}$*;*

b. $\{\{1\},\{1,-1\},\{\{1\},2,3\}\} \subset \wp(A)$. *Qual o menor valor possível para* $|A|$*?*

c. $A \setminus \wp(A) \neq A$;

d. $A \setminus \wp(A) = A \neq \emptyset$

e. $A \cap \wp(A) = \{\{1\},\{1,\emptyset\}\}$

(5) Seja A *um conjunto e* $|A| = n$*. Determine os possíveis valores de* $|\wp(A) \setminus A|$ *e* $|A \setminus \wp(A)|$

(6) Determine todos valores possíveis para x,y ou z, sabendo-se que $x, y, z \in \{-4,-1,0,1,3,4\}$ *e* $z + y + z = 0$

(7) Seja $X = \{-1,0,1,3,5,6,8\}$*. Determine:*

a. *Todos os subconjuntos de* X *que têm exatamente* 4 *elementos e cuja soma deles seja* 8 *ou* 12*;*

b. *O subconjunto de* X*, com* 5 *elementos, cuja soma entre os elementos seja a maior possível;*

c. *Os subconjuntos de* X *com* 5*, cujo produto entre seus as elementos seja nulo.*

(8) Seja X *um conjunto e* $\wp(X)$ *o conjunto das partes de* X*. Se* $A, B \in \wp(X)$*, prove as seguintes propriedades:*

a. $(A \cup B) \in \wp(X)$;

b. $(A \cap B) \in \wp(X)$;

c. $\Delta(A,B) \doteq (A \cup B) \setminus (A \cap B) \in \wp(X)$;

(9) Seja o nome PEDRO DE ALCANTARA MAGALHÃES.

a) *Determine o conjunto* NM*, formado pelas letras do nome acima.*

b) *Responda: o conjunto* $\{a,e,i,o,u\}$ *é um subconjunto de* NM*? Por que?*

c) *Qual o número de elementos de* NM *e de* $\wp(NM)$*?*

d) *Considere* $Q \subset \wp(NM)$*, cujos elementos* $X \in Q$*, sejam conjuntos de exatamente* 4 *elementos. Qual o número de elementos de* Q *e de* $\wp(Q)$*?*

e) *Considere* $T \subset \wp(NM)$*, cujos elementos* $X \in T$*, sejam conjuntos de exatamente* 3 *elementos. Determine* $|T|$*.*

1.2 Produto Cartesiano

Pelo axioma da extensionalidade, os conjuntos $\{1\}$ e $\{1,1\}$ são iguais. O mesmo ocorre com os conjuntos $\{1,2\}$ e $\{2,1\}$, neste caso, observamos que para um conjunto importa apenas seus

elementos, não a ordem que eles aparecem. Embora tal situação seja aparentemente ingênua, os conjuntos não parecem, num ponto de vista ainda mais ingênuo, ser eficientes para ordenar objetos, isto é, se quisermos interpretar um conjunto de modo semelhante a um número, ou seja o número 12 com o conjunto $\{1, 2\}$, tal identificação não fica bem definida pois $12 \neq 21$, embora $\{1, 2\} = \{2, 1\}$. Em breve poderemos dizer que os conjuntos não exibem, diretamente, uma hierarquia entre seus elementos. Anacronicamente, a situação que levantamos, isto é, uma boa notação para indicar ordem, posição ou hierarquia, foi definida no século XVI pelo pensador Renè Descartes, para representar sua idéia sobre o produto cartesiano. Uma considerável generalização geométrica foi possível a partir da idéia de par ordenado e sua associação com os pontos do espaço, definindo o que é conhecido hoje por plano cartesiano. Alguns séculos depois Gauss definiria o plano complexo, que além de associar pares ordenados aos pontos, permite definir operações algébricas entre estes elementos. Infelizmente, está longe de podermos discutir a revolução dessas idéias no mundo em geral; um texto sobre a história da Matemática pode contribuir neste sentido. Sugerimos o livro [**?**].

Iniciamos, portanto com a seguinte definição de par ordenado.

Definição 1.2.1. *Dizemos que* (x, y) *é um par ordenado se* $(x_1, x_2) = (y_1, y_2)$*, sempre que* $x_1 = y_1$ *e* $x_2 = y_2$

A definição de par ordenado pode estendida para uma n-upla ordenada, em que $n \in N^*$, e é comum simplesmente referir-se a uma n-upla, ficando subentendido a propriedade de ordem. Assim temos uma terna ordenada, 3-upla, uma quadra ordenada, 4-upla, entre várias.

O seguinte teorema foi inicialmente proposto pelo matemático polonês Kuratowsky, no início do século XX. Exibindo uma representação de conjunto para um *par ordenado*, isto é, Kuratowsky mostrou que é possível representar um par ordenado, e portanto estabelecer uma relação de ordem, utilizando-se apenas a representação de conjuntos.

Teorema 1.2.2 (Kuratowsky)**.** *Seja* (x, y) *um par ordenado. O conjunto* $\{\{x\},\{x,y\}\}$ *satisfaz as mesmas propriedades de* (x, y)*.*

De modo análogo podemos generalizar a representação de uma n-upla, utilizando apenas a notação de conjuntos.

Vamos definir produto cartesiano. Como motivação para esta definição apresentamos as seguintes questões. Se $A = \{x, y\} \subset B = \{1, 2, 3\}$, já vimos que A pode ser um subconjunto de B, com 1 elemento, caso $x = y$, ou 2 elementos se $x \neq y$. Mas o que dizer para o caso (x, y), tal que $x, y \in B$? Ou quais as possíveis ternas ordenadas (x, y, z), tal que, $x, y, z \in B = \{1, 2, 3\}$? A definição de produto cartesiano auxilia nesta questão, embora observamos que esta motivação, não necessariamente, esteja ligada à motivação original da definição de poduto cartesiano.

Definição 1.2.3. *Sejam A e B são dois conjuntos, o conjunto $A \times B = \{(a,b)/a \in A, b \in B\}$ é o produto cartesiano dos conjuntos A e B.*

A definição de produto cartesiano pode ser estendida para n-uplas, de modo análogo à definição anterior. A seguir exibimos alguns exemplos de produto cartesiano e sua generalização.

Exemplo 1.2.4. *(1) Se $A = B = \{1,2,3\}$, o produto cartesiano*
$A \times B = \{(1,1),(1,2),(1,3),(2,1),(2,2),(2,3),(3,1),(3,2),(3,3)\}$,
portanto observamos que há $3.3 = 9$ pares ordenados;

(2) Se $A = B = \mathbb{R}$,o conjunto dos números reais, então o produto cartesiano $A \times B$ define o plano cartesiano, representado por $\mathbb{R}^2$.

(3) Seja l um retângulo delimitado pelas retas $x = 1; x = 2; y = 1; y = 3$ do plano cartesiano. Sejam os conjuntos $X = \{x/1 \leq x \leq 2, x \in \mathbb{R}\}$ e $Y = \{y/1 \leq y \leq 3, y \in \mathbb{R}\}$. O produto cartesiano $A \times B$ define, como conjunto, o mesmo retângulo l;

(4) Sejam A, B, C conjuntos. Segundo a definição de produto cartesiano $D = A \times B$ é um conjunto, portanto $D \times C$ é o conjunto $T = \{(d,c)/d \in D, c \in C\}$. Se $x \in T$, $x = ((a,b),c), a \in A, b \in B, c \in C$. Este par ordenado tem as mesmas propriedades da terna (a,b,c), pois se $((a,b),c) = ((u,v),w) \Rightarrow (a,b) = (u,v)$ e $c = w$; da primeira igualdade, $a = u, b = v$, ou seja $(a,b,c) = (u,v,w)$. Assim os elementos de $(A \times B) \times C$ têm as mesmas propriedades das ternas (a,b,c), e podemos definir o produto cartesiano $A \times B \times C = \{(a,b,c)/a \in A, b \in B, c \in C\}$

(5) De modo análogo ao plano cartesiano, podemos definir o Espaço euclideano por $\mathbb{R} \times \mathbb{R} \times \mathbb{R} \doteq \mathbb{R}^3$

Seja A um conjunto. Lembrando que $|A|$ denota o número de elementos do conjunto A, então $|A \times B| = |A||B|$, o que sugere o nome "produto"cartesiano.

Exercícios 1.2.5. *(1) Para cada item a seguir determine os valores de x, y, z, conforme o caso*

(a) $(x - y, x + y + 3) = (2x + 3y + 2, x - 2y)$

(b) $(x + y + 3, x - y) = (2x + 3y + 2, x - 2y)$

(2) Seja $X = \{-1, 0, 1, 3, 5, 6, 8\}$ e $B = \wp(X) \times X$. Determine o subconjunto de B, isto é de elementos $(A, x), A \subset X, x \in X$, cujo $|A| = 5$, tal que o produto entre todos elementos de A e a segunda coordenada x, seja nulo.

(3) Prove o teorema de Kuratowsky;

(4) Generalize o teorema de Kuratowsky para uma n-upla;

(5) Mostre que se $|A| = m$ *e* $|B| = n$*, então* $|A \times B| = mn$*.*

(6) É verdade que $A \times B$ *é sempre diferente de* $B \times A$*, se* A *e* B *são diferentes?*

(7) Prove que $|A \times B| = |B \times A|$

1.3 Relações e Funções

O conceito de relação está diretamente ligado ao conceito de par ordenado, uma vez que podemos "relacionar"a primeira coordenada com a segunda coordenada, ou de modo geral para as n-uplas, relacionar as coordenadas umas com as outras, porém de um modo preciso. Como vimos no exemplo 4, as n-uplas podem, sempre, ser tratadas como pares ordenados, portanto o que apresentarmos para os pares ordenados, é análogo para as n-uplas.

Considere os conjuntos $A = \{-1, 1, 2, 7\}$, $B = \{1, 2, 5\}$ e $C = A \times B$, isto é,

$$C = \{(-1,1), (-1,2), (-1,5), (1,1), (1,2), (1,5), (2,1), (2,2), (2,5), (7,1), (7,2), (7,5)\},$$

o produto cartesiano entre A e B. Vamos considerar alguns subconjuntos do conjunto C e observar que podemos identificar estes subconjuntos com objetos ou propriedades conhecidas.

Por exemplo o conjunto $menor = \{(-1,1), (-1,2), (-1,5), (1,2), (1,5), (2,5)\}$ é um subconjunto de C, isto é $menor \subset C$, pois todos os elementos de $menor$ estão em C. Este mesmo conjunto pode ser determinado do seguinte modo: $menor = \{(a,b)/a \in A, b \in B, a < b\}$, ou seja $menor$ é o subconjunto do produto cartesiano $A \times B$, cuja primeira coordenada é menor que a segunda coordenada. Outro subconjunto de C é $reta = \{(-1,1), (1,2), (7,5)\}$, que também pode ser determinado do seguinte modo $\{(a,b)/a \in A, b \in B, a - 2b = -3\}$. Ou, da mesma forma, podemos obter subconjuntos de C, a partir de algum tipo de propriedade, por exemplo: $par = \{(a,b)/a \in A, b \in B, a$ é um numero par$\} = \{(2,1), (2,2), (2,5)\}$. Como vimos, teorema (1.1.6), $|C| = 4.3 = 12$ e portanto C possui $2^{12} = 4096$ subconjuntos, portanto ficaria extenso apresentar todas as possibilidades para este exemplo, bem como para conjuntos ainda maiores. Mas é importante ressaltar essa característica para o produto cartesiano entre os conjuntos. O que motiva a seguinte definição:

1.3.1 Relação

Definição 1.3.1. *Sejam* A *e* B *dois conjuntos não vazios. Definimos relação entre* A *e* B *a todo subconjunto de* $A \times B$*, o produto cartesiano de* A *e* B*. Se* R *é uma relação de* A *em* B*, denotamos isso por:* $R : A \to B$*, sendo* A *o domínio da relação e* B *o contra-domínio.*

Para conhecermos qual é a relação R, deve-se descrever a propriedade que relaciona os elementos do domínio, com os elementos do contra-domínio. A notação mais comum para esse fim é: $a \mapsto b$, sendo por convenção $a \in A$, $b \in B$, seguida da propriedade que o elemento b deve satisfazer, desse modo o par ordenado $(a, b) \in R$, pois $R \subset A \times B$. A seguir apresentamos alguns exemplos que elucidam essa notação.

Exemplo 1.3.2. *(1) Segundo o parágrafo anterior,* $menor : \{-1, 1, 2, 7\} \to \{1, 2, 5\}$*, que associa a todo elemento do domínio* $ain\{-1, 1, 2, 7\}$ *os elementos do contra-domínio* b*, tais que, a seja menor que* b*, isto é,* $a \mapsto b$*, tal que,* $a < b$*. Portanto* $(-1, 1) \in menor$*, porém* $(1, 1) \notin menor$*, pois não ocorre que* $1 < 1$*, ou seja, a relação menor não se verifica para o par* $(1, 1)$*;*

$$menor = \{(-1, 1), (-1, 2), (-1, 5), (1, 2), (1, 5), (2, 5)\};$$

(2) A relação $reta : \{-1, 1, 2, 7\} \to \{1, 2, 5\}$*,* $a \mapsto b/2b = a + 3$*. Neste caso,* $-1 \mapsto 2(1) = 2 = -1 + 3 \therefore (-1, 1) \in reta$*. Verificando a propriedade para todos os pares ordenados do produto cartesiano, obtemos* $reta = \{(-1, 1), (1, 2), (7, 5)\} \subset \{-1, 1, 2, 7\} \times \{1, 25\}$*, que é a relação dada;*

(3) A relação $t : \wp(\{x, y, z\}) \to \{-1, 0, 1, 2\}$*, tal que,* $X \mapsto |X|$*, isto é, o domínio é o conjunto* $\wp(\{x, y, z\}) = \{\emptyset, \{x\}, \{y\}, \{z\}, \{x, y\}, \{x, z\}, \{y, z\}, \{x, y, z\}\}$*, portanto* $\emptyset \mapsto 0; \{x\} \mapsto 1; \{y, z\} \mapsto 2$*, porém* $\{x, y, z\}$ *não está associado a qualquer elemento do contradomínio, pois* $3 \notin \{-1, 0, 1, 2\}$ *o contra-domínio. Desse modo, a relação é dada por* $t = \{(\emptyset, 0), (\{x\}, 1), (\{y\}, 1), (\{z\}, 1), (\{x, y\}, 2), (\{x, z\}, 2), (\{y, z\}, 2)\}$

(4) Seja $R : \mathbb{R} \to \{0, 1\}$*,* $x \mapsto 1$*, se* $x^2 < 0$*, ou seja a relação* R *associa* 1 *aos números reais cujo quadrado seja negativo. Mas o quadrado de qualquer número real é sempre positivo, logo nenhum elemento de* $\mathbb{R}$ *associa-se ao número* 1*, portanto não existem pares ordenados para essa relação, então* $R = \emptyset$*;*

(5) A relação $par : \mathbb{N} \mapsto \mathbb{N}/n \mapsto 2n$ *é o subconjunto* $par \subset \mathbb{N} \times \mathbb{N}$*,* $par = \{(n, 2n)/n \in \mathbb{N}\}$*.*

Sejam A, B dois conjuntos e $R : A \to B$ uma relação. Utilizaremos a seguinte notação: como vimos A é o domínio e B é o contra-domínio. Se $x \in A$ e $y \in B$ é tal que $(x, y) \in R$, então dizemos que y é imagem de x e denotamos isso por $R(x)$. O subconjunto do contra-domínio de todas as imagens de x, pela relação R, é denominado imagem de x e denotado por $R[x]$, isto é, $R[x] = \{y/(x, y) \in R\}$. Se $X \subseteq A$, $R[X] = \{y/(x, y) \in R, x \in X\}$ denominado conjunto imagem do subconjunto X, ou simplesmente imagem de X; podemos considerar a relação R restrita ao conjunto X, isso significa que a relação é calculada somente sobre o subconjunto X, que denotamos por $R|_X$. Desse modo $R[A]$ é denominado imagem da relação, ou simplesmente imagem. Assim, no exemplo (1) $menor(-1) = 1$, $menor(-1) = 2$; $menor[-1] = \{1, 2, 5\}$; $menor[1] = \{2, 5\}$; $menor(7)$ não existe no contra-domínio, portanto $menor[7] = \emptyset$; a imagem

da relação menor é o conjunto $\{1,2,5\}$, pois todos estes elementos estão associados a algum elemento do domínio. Nos exemplos seguintes temos: $reta[\{-1,1,2,7\}] = \{1,2,5\}; t[\wp(\{x,y,z\})] = \{0,1,2\}; R[\mathbb{R}] = \emptyset; par[\mathbb{N}] = \{0,2,\cdots,2n,...\}$, são os conjuntos imagens das relações indicadas. Podemos observar que, relativamente à imagem, nosso referencial é o domínio. Porém podemos tomar como referência o contra-domínio. Nesse caso, referimo-nos ao termo imagem inversa.

Seja $R : A \to B$, uma relação. Se $y \in B$, $R^{-1}[y] \doteq \{x/(x,y) \in R\}$ é denominado imagem inversa do elemento y, pela relação R. Analogamente, se $Y \subseteq B$, $R^{-1}[Y] = \{x/(x,y) \in R, y \in Y\}$. Retomando o exemplo 1,

$$menor^{-1}[2] = \{-1,1\}; menor^{-1}[\{1,2,5\}] = \{-1,1,2\}.$$

Seja $R : A \to B$ uma relação. Segundo a definição $R \subseteq A \times B$, isto é, $R \in \wp(A \times B)$ o conjunto de todos os subconjuntos de $A \times B$. Nessas condições, dados os conjuntos A e B, conhecemos TODAS as possíveis relações de A em B. Por exemplo, se $A = \{1,2\}$ e $B = \{-1,1\}$, existem 2^4 relações possíveis de A em B, pois $|A \times B| = 2.2 = 4$. Qualquer relação $R : A \to B$ é um subconjunto do produto cartesiano, isto é, $\forall R : A \to B, R \subseteq A \times B \therefore R \in \wp(A \times B)$; pelo teorema (1.1.6), $|\wp(A \times B)| = 2^{|A \times B|} = 2^4 = 16$. Este resultado é de fácil demonstração, bastando generalizar os argumentos anteriores.

Para os conjuntos A e B acima, seja $C = A \times B = \{(1,-1),(1,1),(2,-1),(2,1)\}$;

$$\wp(C) = \{\emptyset, \{(1,-1)\}, \cdots, \{(1,-1),(1,1),(2,-1)\}, \cdots, \{(1,-1),(1,1),(2,-1),(2,1)\}\},$$

cujos elementos são as relações de A em B. Assim o número de elementos possíveis para essas relações varia entre 0 e 4. Pelo teorema 1.1.8, podemos determinar o número de relações com exatamente $0 \leq k \leq |C|$ elementos, isto é $\binom{|C|}{k}$ relações têm exatamente k elementos.

Proposição 1.3.3. *Seja $R : A \to B$, uma relação. Tal que $|A| = m$ e $|B| = n$. Se $|R|$ denotar o número de relações de A em B, e $|R_k|$ a quantidade dessas relações, com exatamente k elementos, então:*

i.) $|R| = 2^{m.n}$;

2.) $|R_k| = \binom{m.n}{k}$.

Exercícios 1.3.4. *(1) Seja $R = \{(1,\{1,2\}),(\{-1\},1),(\{1\},\{1\}),((1,2),(-1,2))\}$, a relação $R : A \to B$, responda falso ou verdadeiro.*

a) *O conjunto A é o domínio da relação e $A \subset \{1,(1,2),2,\{1\},\{-1\}\}$;*

b) $R(1) \in \{1,2\}$;

c) $R(1) = \{1,2\}$;

d) $R[(1,2)] = \{(-1,2)\}$;

e) *O conjunto imagem da relação* R *é o conjunto* $\{1, \{1,2\}, \{1\}, (-1,2)\}$

(2) Seja $A = \{janeiro, fevereiro, março, abril, maio, junho, julho, agosto,$ $setembro, outubro, novembro, dezembro\}$ *e* $vg : A \to A; vg(x) = y$ *, quando o conjunto das vogais de* x *e o conjunto das vogais de* y *são iguais. Determine:*

a) *A imagem do elemento abril, isto é,* $vg(abril)$;

b) *A imagem inversa do elemento junho*

c) *O domínio, o contra-domínio, a relação* vg *e a imagem da relação*

d) $vg(junho) \bigcap vg(setembro)$

e) *Se* $vg : A \to A; vg(x) = y$*, quando o número de elementos do conjunto das vogais de* x *for igual ao número de elementos do conjunto das vogais de* y*, determine os itens anteriores para essa nova relação.*

(3) Seja X *um conjunto finito, tal que,* $|X| = n$*. Determine o número de relações possíveis de* X *em* $\wp(X)$ *e o número de relações possíveis de* $\wp(X)$ *em* X*. Dê exemplos de uma relação quando* $n = 4$ *e* $n = 5$*.*

(4) Sejam X *e* Y *dois conjuntos finitos não vazios, isto é,* $|X| = n$ *e* $|Y| = m$*, dois números naturais positivos.*

a) *Calcule o número de relações possíveis entre* X *e* Y*.*

b) *Para* $n = 5$ *e* $m = 4$*, determine exemplos de relações, em que a imagem de cada elemento tenha exatamente* 3 *elementos, e elementos distintos tenham imagens distintas.*

c) *Quantas relações, em que, cada elemento do domínio tenha exatamente 3 imagens sendo* $n = 5$ *e* $m = 4$*?*

d) *Quantas relações, do tipo do item b), são possíveis?*

(5) Sejam X *e* Y *dois conjuntos e* $R : X \to Y$ *uma relação. Explique, detalhadamente, os seguintes itens e exemplifique para* X *e* Y*, dois conjuntos escolhidos por você.*

a) $R(x), R[x], R[\{x\}], Im[\{x\}] e Im[x]$,$R$ *e* $Im(R)$ *quando* $x \in X$ *;*

b) $R[A]$ *e* $Im[A]$*, quando* $A \subseteq X$ *;*

c) $R^{-1}[Y], R^{-1}[\{Y\}]$ *quando* $y \in Y$

d) $R^{-1}[B]/B \subseteq Y$*.*

(6) Seja mod_n uma relação em $A \subset Z$, o conjunto dos números inteiros, que associa a cada inteiro i, o resto da divisão de i pelo número n, (por exemplo $mod_7(26) = 5$, pois $26 = 7.3 + 5$). Calcule a imagem da relação mod_n para os seguintes casos:

a) $n = 3$ *e* $A = \{1, 2, 3, 4, 5\}$

b) $n = 7$ *e* $A = \{-2, -1, 0, 1, 2, 3, 4\}$

c) $n = 10$ *e* $A = \{0, 1, ..., 23\}$, *o conjunto dos naturais entre*0 *e* 23*;*

d) $n = 4$ *e* $A = \{0, 1, 2, 3, 2001, 2002, 2003, 2004, 2005, 2006\}$

(7) Seja o conjunto $A = \{-1, 1, 2, -2\}$, e $subA : \wp(A) \to \wp(A)$, a relação que a todo elemento X do domínio associa os elementos Y do contra-domínio que têm o mesmo número de elementos, isto é, se $|X| = |Y|$, então, $(X, Y) \in subA$;

a) *Mostre que* $\{-1, 1\} \in \wp(A)$ *e determine* $subA[\{-1, 1\}]$ *, a imagem de* $\{-1, 1\}$*;*

b) *Mostre que* $\{1, 2, -2\} \in subA[\{1, 2, -2\}]$ *e calcule a imagem inversa desse elemento;*

c) *Se o conjunto A tiver 10 elementos, quantos elementos terá o conjunto imagem de um subconjunto de A com 6 elementos?*

(8) Seja $R : A \to B$, uma relação.

a) *Quantas relações R existem, se A tem 15 elementos e B tem 8 elementos?*

b) *Se* $A = \{1, 2, 3, 4, 5\}$ *e* $B = \{-1, 0, \{1\}, \{2\}\}$, *determine uma relação R com exatamente 6 elementos;*

c) *Se* $|A| = 5$ *e* $|B| = 4$ *, determine quantas relações existem com exatamente 6 elementos.*

(9) Seja $A = \{janeiro, fevereiro, março, abril, maio, junho, julho, agosto, setembro, outubro, novembro, dezembro\}$ e $vg : A \to A; vg(x) = y$, quando x e y têm as mesmas vogais, independentemente se repetem ou estão fora de ordem. Determine:

a) *A imagem do elemento abril;*

b) *A imagem inversa do elemento junho;*

c) $vg^{-1}[março] \cup vg^{-1}[maio]$*;*

d) *Prove que* $vg[junho] = vg^{-1}[outubro]$.

Como vimos, dados dois conjuntos A e B, podemos determinar as possíveis relações de um conjunto no outro. Dessas relações possíveis, existe um caso particular de especial importância, que denominamos de função. Vamos exemplificar, com uma situação física, uma dessas relações particulares: se o conjunto A representa o conjunto de todos os instantes em que uma partícula é observada e o conjunto B, a posição dessa particula e a relação $S : A \to B$, que a cada tempo t observado, $t \in A$ associa a posição $x \in B$ ocupada naquele instante, duas condições, do ponto de vista clássico, devem ocorrer.

i A cada instante $t \in A$, existe um elemento $p \in B$, correspondente à posição da partícula. Isto ocorre pois a particula não desaparece instantaneamente;

ii Cada instante t corresponde a uma única posição p, porque sabemos que um corpo não pode estar em dois lugares distintos ao mesmo tempo.

Uma relação com esta propriedade é o que será definido a seguir por função.

1.3.2 Função

Definição 1.3.5. *Sejam X e Y dois conjuntos e $f : X \to Y$ uma relação. Dizemos que a relação f é uma função se ocorrem as seguintes condições:*

(i) $\forall x \in X, \exists y \in Y / f(x) = y$ *[Lê-se: Para todo elemento do domínio, existe um elemento no contra-domínio que é sua imagem]. Esta condição denominamos de "existência"*

(ii) *O valor y da condição (i) é único. Esta condição denominamos de unicidade.*

As condições de existência e unicidade, que uma relação deve satisfazer para ser uma função, podem ser resumidas na seguinte expressão: $\forall x \in X \exists! y \in Y / f(x) = y$. O símbolo $\exists!$ significa: existe um único, portanto dizemos que f é uma função se para todo elemento do domínio existe um único elemento do contra-domínio que é sua imagem, isto é, $f(x) = y \in Y$.

Pelo fato de toda função ser uma relação, a notação utilizada para a relação é a mesma para as funções. Assim, se $f : X \to Y$ é uma função, o conjunto X é o domínio e Y o contra-domínio; se $x \in X$, $f(x) \in Y$ é a imagem de x pela função f. Pela definição de função o conjunto $f[x]$ será sempre unitário, portanto não é comum utilizar esta notação para um elemento, no contexto das funções. Se $A \subseteq X$, o conjunto $f[A] = \{f(x)/x \in A\}$ é denominado imagem do conjunto A. Quando $A = X$, o conjunto $f[X]$ será denominado imagem da função, nesse caso é comum referir-se a este conjunto por $Im(f)$. Se $y \in Y$, $f^{-1}[y] = \{x/f(x) = y\}$ é a imagem inversa de y, finalmente, se $B \in Y$ o conjunto $f^{-1}[B] = \{x/f(x) \in B\}$ é denominado imagem inversa do conjunto B.

É importante reforçar que uma função $f : A \to B$, é denominada de função f. Se $x \in A$, então há sentido escrever $f(x)$; e somente neste caso é possível tal representação. É comum em textos de matemática encontrarmos a representação $f(x)$, sem tal indicação, geralmente, por ficar subentendido que $x \in A$. Porém não devemos referirmo-nos a uma função pela representação $f(x)$, este termo, em verdade é um elemento do contra-domínio da função f, isto é, $f(x) \in B$. É comum escrevermos $f(x) =$"alguma sentença em x"e isto é feito para representar como a função f converte os elementos do domínio, em elementos do contra-domínio.

A seguir apresentamos alguns exemplos de função. Apresentamos algumas funções reais e lembramos que, para essa classe de funções, domínio é o maior subconjunto dos números reais para o qual a condição de existência e unicidade, de uma função f, esteja verificada, representamos este conjunto por $Dom(f)$.

Exemplo 1.3.6. *(1) A função $f : A \to A / f(a) = a$ denominada função identidade. Veremos no capítulo II a importância dessa função. A seguir os exemplos são de funções reais. Isso não impede que definamos essas funções em domínios quaisquer ou mesmo em conjuntos cujo domínio não seja igual ao contradomínio;*

(2) Sejam $a, b \in \mathbb{R}, a \neq 0$. A função $f : \mathbb{R} \to \mathbb{R} / f(x) = ax + b$ é a função linear. Se $b = 0$ é comum denominar a função $f(x) = ax$ de função afim. Se $a = 1, b = 0$ a função f é a função identidade em $\mathbb{R}$

(3) Sejam $a, b, c \in \mathbb{R}, a \neq 0$. A função $f : \mathbb{R} \to \mathbb{R} / f(x) = ax^2 + bx + c$ é a função quadrática, ou função de segundo grau;

(4) Sejam $a_i \in \mathbb{R}, i \in \mathbb{N}$ e $n \in \mathbb{N}$ um natural fixado, tal que, $a_n \neq 0$. A função $f : \mathbb{R} \to \mathbb{R}$, tal que

$$f(x) = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_2 x^2 + a_1 x + a_0 \doteq \sum_{1 \leq i \leq n} a_i x^i + a_0,$$

é a função polinomial de grau n;

(5) Sejam f,g duas funções polinomiais de graus m, n, respectivamente, e $O = \{x / x \in \mathbb{R}, g(x) = 0\}$ o conjunto de raízes da equação $g(x) = 0$. A função $Q : \mathbb{R} \setminus O \to \mathbb{R}$, tal que

$$Q(x) = \frac{f(x)}{g(x)},$$

é denominada função racional;

(6) Seja $a \in \mathbb{R}^+$. A função $f : \mathbb{R} \to \mathbb{R} / f(x) = a^x$ é a função exponencial.

(7) Seja $EXP = \{f : \mathbb{R} \to \mathbb{R}^+ / a \in \mathbb{R}^+, f(x) = a^x\}$ o conjunto de todas as funções exponenciais; $g : \mathbb{R}^+ \to EXP / g(a) = a^x$ é uma função.

(8) A função $\varphi : \mathbb{Z}^+ \to \mathbb{Z}^+ / n \mapsto |\{i,$ tal que, $1 \leq i \leq n - 1, mdc(n, i) = 1\}|$, isto é, $\varphi(n)$ representa a quantidade de números inteiros entre 1 e $(n - 1)$, que são relativamente primos com o número n. Esta função é conhecida por φ de Euler.

Inicialmente, observe que uma função f deve estar definida para um conjunto A, o domínio da função. Os exemplos acima, exceto os dois últimos, são parte de uma classe importante de funções: as funções elementares.

Podemos obter outras funções, de modo semelhante ao fato de podermos obter outros números a partir dos números naturais. Por exemplo seja $x \in \mathbb{R}$, dadas as funções reais g, h, tais que, $g(x) = -3x; h(x) = x + 7$, se $\forall z \in \mathbb{R}$, tomarmos $x = g(z) = -3z$ e em seguida calcularmos $h(x) = h(-3z) = -3z + 7 = h(g(z))$, portanto $\forall z \in Dom(g)$, tal que, $g(z) \in Dom(h)$, $h(g(z)) = -3z + 7$. Portanto definimos uma nova função denotada por $h \circ g$, repetimos, como observado anteriormante, que $h(g(z))$ não é uma função, porém um modo de expressar a função $h \circ g$ funcionalmente. A próxima definição trata desse caso.

Definição 1.3.7. *Sejam f, g funções, tal que, $f : A \to B; g : U \to V$, e $Im(f) \subseteq U$. Então podemos definir a função $g \circ f : A \to V / g \circ f(x) \doteq g(f(x))$.*

Exemplo 1.3.8. *(1) Seja A um conjunto não vazio, e $f, g : A \to A$, tal que $f(x) = x$ e $g(x) = 5x - 1$, Sendo $Im(f) \subseteq Dom(g)$, está definida a função $g \circ f$ e $g(f(x)) = g(x) = 5x - 1$; em particular $Im(g) \subseteq Dom(f)$, portanto também está definida a função $f \circ g$ e $f(g(x)) = f(5x - 1) = 5x - 1$. Observe que nesse exemplo $f \circ g = g \circ f$, o que não ocorre em geral;*

(2) Sejam as funções $f : \mathbb{R}^* \to \mathbb{R} / f(x) = \frac{1}{x}$, e $g : \mathbb{R} \to \mathbb{R} / g(x) = 5x - 15$. O conjunto $Im(g) = \mathbb{R} \nsubseteq \mathbb{R}^* = Dom(f)$, portanto a função $f \circ g$, não está definida, pois $f(g(x)) = f(5x - 15) = \frac{1}{5x-15}$ e $\nexists f(g(3))$, isto é, $f \circ g$ não satisfaz o critério de existência para $3 \in Dom(f \circ g)$. Porém $g \circ f$ está definida: $g(f(x)) = g(\frac{1}{x}) = \frac{5}{x} - 1$, pois $Dom(f) = \mathbb{R}^*$ e portanto $g \circ f$ é uma função.

(3) Sejam $f : \mathbb{R} \to \mathbb{R} / f(x) = \frac{3x-5}{2}$, e $g : \mathbb{R} \to \mathbb{R}, g(x) = 2^x$, as funções $f \circ g$ e $g \circ f$, estão definidas, sendo

$$f \circ g : \mathbb{R} \to \mathbb{R} / f(g(x)) = \frac{3(2^x) - 5}{2};$$

$$g \circ f : \mathbb{R} \to \mathbb{R} / g(f(x)) = 2^{(\frac{3x-5}{2})} = \sqrt{2^{3x-5}}$$

(4) Ainda considerando o exemplo anterior, estão definidas as funções

$$g \circ g : \mathbb{R} \to \mathbb{R} / g(g(x)) = 2^{2^x},$$

e $f \circ f$, esta última, se desejamos calcular $f(f(3))$, calculamos $f(3) = 2$, portanto $f(f(3)) = f(2) = \frac{1}{2}$. Funções do tipo $g \circ g$, também são denotadas por g^2; observe como esta função é explosiva!

Exercícios 1.3.9. *(1) Um edital para um contrato público contém 15 itens, a cada item do edital será atribuída uma nota n, na seguinte condição: $n \in \{1, 2, 3\}$, isto é, cada item pode ter uma nota valendo 1, 2 ou 3. Dessas 15 questões, 7 devem valer 1 pontos, 3 devem valer 2 e 5 devem valer 3 pontos. O edital permite que cada concorrente escolha a nota de cada item. Seja f a função, que representa um possível contrato:*

a) *Seja* $A = \{(x,1),(y,2),(z,3)/x \in \{3,5,7,10,11,13,14\}, y \in \{2,4,8\}, z \in \{1,6,9,12,15\}\}$, *escreva* A *e explique se ele representa uma possível função* f*?*

b) *Simule a proposta de* 3 *contratos diferentes, relativamente aos valores dos itens, isto é, determine* 3 *funções* f*;*

c) *Calcule o número possível de contratos distintos, que atenda às condições do edital?*

d) *Compare o valor do item c) com o número total de funções com domínio e contra-domínio iguais a função* f*. Justifique sua resposta.*

(2) Sejam X *e* Y *dois conjuntos e* $f : X \to Y$ *uma função. Responda os itens a seguir, ressaltando as diferenças com o exercício 5 da seção anterior*

a) $f(x), f[x], f[\{x\}], Im[\{x\}] e Im[x]$,$f$ *e* $Im(f)$ *quando* $x \in X$ *;*

b) $f[A]$ *e* $Im[A]$*, quando* $A \subseteq X$ *;*

c) $f^{-1}[Y], f^{-1}[\{Y\}]$ *quando* $y \in Y$

d) $f^{-1}[B]/B \subseteq Y$*.*

(3) Considere os conjuntos A*,* B*,* C *e* D*, tal que:* $A = \{1,2,3,4,5\}; B = \{-1,\{-1\},1,\{2\}\}; |C| =$ 12 *e* $D = A \times C$*, nessas condições:*

a) *Qual o número de elementos do conjunto* D*?*

b) *Determine o número de funções* $f : B \to D$ *;*

c) *Se* $R : A \to B$ *é uma relação, determine quantas relações* R *existem, com exatamente 6 elementos?*

d) *Dê exemplo de uma relação* $R : A \to B$*, com 5 elementos que seja uma função.*

(4) Seja $f : \{a,b,c,d,e,f\} \to \{a,b,c,d,e,f\}$*, uma função injetora. Seja* $ALFABETO$ *o conjunto de todas as letras do alfabeto* (26)*,* $PALAVRA$ *o conjunto de todas as "palavras"(justaposição de letras do alfabeto, com ou sem repetição) de até* 26 *letras, formadas pelas letras do alfabeto e* $g : \wp(ALFABETO) \to PALAVRA$*, a função que associa a cada subconjunto* $NOME \in \wp(ALFABETO)$*, a palavra formada pelas letras do conjuntos NOME, na ordem em que aparecem: da esquerda para a direita.*

a) *Dê* 5 *exemplos diferentes de função* f*;*

b) *Verifique se o conjunto* $Im(f)$ *é subconjunto de* $\wp(ALFABETO)$ *, caso afirmativo, calcule a função* g *, para os exemplos do item a).*

c) *Calcule quantas funções* f *e* g *pode-se definir.*

(5) Dê exemplos para as seguintes funções ou relações:

a) *uma função* f *entre os conjuntos* $\{1,2,3,4\}$ *e* $\{a,b,c,d,e\}$*, tal que* $|Im_f|$ *seja máximo;*

b) *uma função f entre os conjuntos $\{1,2,3,4\}$ e $\{a,b,c,d,e\}$, tal que $|Im_f| = 2$;*

c) *uma relação do conjunto Z sobre o conjunto Z que não verifique o critério de existência na definição de função;*

d) *uma relação do conjunto $\{1,2,3,4\}$ sobre R, que não verifique o critério de unicidade na definição de função.*

(6) Sejam $f : A \to B$ e $g : X \to Y$ duas funções.

a) *Em que condições podemos definir $f \circ g$;*

b) *Em que condições podemos definir $g \circ f$;*

c) *Em que condições podemos definir $f \circ g$ e $g \circ f$;*

d) *Exemplifique os itens acima.*

(7) Sejam $f, g : \{1,2,3\} \to \{1,2,3\}$. Se $f(1) = 2; f(2) = 3; f(3) = 1$ e $g(1) = 3, g(2) = 2; g(3) = 1$, Calcule as funções $f \circ g$; $g \circ f$; f^2 e g^2.

(8) Sejam $f : \mathbb{N} \to \mathbb{N}$ a função fatorial, $f(n) = n!$ e $g : \mathbb{Z} \to \mathbb{Z}^+$ a função que a cada número inteiro n, associa o maior fator primo de n, isto é $f(n) = p$ se p é o maior número primo que divide n.

a) *Calcule $f(4); g(100); g(800)$;*

b) *Explique se podemos definir a função $f \circ g$?*

c) *Explique se podemos definir a função $g \circ f$?*

d) *Calcule, quando possível: $f \circ g(16)$; $f \circ g(12)$; $g \circ f(12)$;*

e) *Mostre que se $g(n) = p$ então $g(f(n)) = p$.*

(9) Dê exemplos de relações que não sejam função. Apresente um exemplo que apenas falhe o critério e existência, e um outro que falhe apenas o critério de unicidade e um exemplo que falhe os dois critérios.

(10) Sejam X e Y dois conjuntos finitos não vazios, isto é, $|X| = n, |Y| = m \in \mathbb{N}^*$, inteiros positivos. Prove que o número de funções possíveis entre X e Y é dado por n^m.

(11) Mostre que dados $m, n \in \mathbb{N}^*$, então $m^n < 2^{mn}$ e $n^m < 2^{mn}$

1.3.3 Relação de Equivalência

Vamos apresentar alguns tipos importantes de relação e função, que aparecem naturalmente, tanto em teoria, quanto na natureza e atividades da vida. Iniciamos com o conceito de relação de equivalência, muito comum, como poderemos ver pelos exemplos.

Definição 1.3.10. *Seja A um conjunto e R uma relação em A, isto é $R : A \to A$. Dizemos que R é uma relação de equivalência se ocorrem as seguintes 3 propriedades:*

(i) *A propriedade reflexiva: $\forall a \in A, a \in R[a]$,*

(ii) *A propriedade simétrica: se $a \in R[b]$, então $b \in R[a]$*

(iii) *A propriedade transitiva: se $a \in R[b]$ e $b \in R[c]$, então $a \in R[c]$*

A imagem $R[a]$ é denominada classe de equivalência da relação.

A propriedade reflexiva garante que dentre as possíveis imagens para um elemento qualquer, a, do domínio, o próprio elemento é sua imagem, isto é, $R(a) = a$. Por exemplo a relação $M : \{1, 2, 3, 4\} \to \{1, 2, 3, 4\}$, tal que, $x \mapsto y$ se $x \leq y$.

A propriedade simétrica garante que dado um elemento x, se y está no conjunto imagem de x, então x está no conjunto imagem de y, isto é $R(x) = y \Rightarrow R(y) = x$. Por exemplo a relação acima não é transitiva, pois $M[2] = \{2, 3, 4\} \therefore M(2) = 4$, mas $M[4] = \{4\} \therefore M(4) = 4 \neq 2$. Um exemplo de relação simétrica é a relação $P : \{1, 2, 3, 4\} \mapsto \{1, 2, 3, 4\}$, $x \mapsto y$, se x e y têm a mesma paridade. Então $P(2) = 4$ pois são pares, e da mesma forma $P(4) = 2$. Esta relação também é reflexiva.

A propriedade transitiva permite relacionar dois elementos que tenham em comum o fato do primeiro ser a imagem de um certo elemento que, por sua vez, é a imagem do segundo elemento.

Exemplo 1.3.11. *(1) A relação em $\mathbb{Z}$, de paridade, $R : \mathbb{Z} \to \mathbb{Z}/R(i) = j$, se i, j são ambos pares, ou ímpares;*

(2) A relação em $\mathbb{Z}$, que fixado um número natural positivo n, associa ao número inteiro i, um número j, tal que $i - j$ seja um múltiplo de n, isto é, $\exists k \in \mathbb{Z}/i - j = kn$, observe que isso significa que o número $i - j$ é divisível por n e, geralmente, dizemos que n divide $i - j$. Essa relação é comum em Álgebra e tem várias notações e interpretações, vamos introduzindo essas notações ao longo dos capítulos, incialmente vamos denominá-la $mod_n : \mathbb{Z} \to \mathbb{Z}/mod_n(i) = j$, se n divide $i - j$, que também denotamos por $n|(i - j)$. Por exemplo $mod_6 : \mathbb{Z} \to \mathbb{Z}$, $mod_6(7) = 13$, pois $6|(13 - 7)$;

(3) A relação "dia"em "ano", o conjunto dos meses do ano, que associa a cada mês m, um mês, n, que tenha o mesmo número de dias de m, isto é, $dia : ano \to ano/dia(m) = n$ se m e n têm o mesmo número de dias, assim, $dia(fevereiro) = fevereiro$; $dia[abril] = \{abril, junho, setembro, novembro\}$

(4) A função identidade, isto é, $f : A \to A/f(x) = x$ é uma relação de equivalência. Deixamos ao leitor, como exercício, mostrar que é a única função com essa propriedade.

Os exemplos acima são de relações de equivalência, porém devemos provar quando uma dada relação é uma relação de equivalência. A seguir provamos que a relação mod_n é uma relação de equivalência.

Proposição 1.3.12. *Seja n um número inteiro positivo. A relação $mod_n : \mathbb{Z} \to \mathbb{Z}/i \mapsto j$ se n divide $i - j$, é uma relação de equivalência.*

Demonstração. Devemos provar que mod_n satisfaz as três propriedades da definição (1.3.10): *i.*) Reflexividade; $mod_n(i) = i$? Sim! Pois $i - i = 0$ e 0 é múltiplo de qualquer inteiro positivo, $0 = k0, \forall k\mathbb{Z}$; *ii.*) Simétrica; se $mod_n(i) = j \Rightarrow n$ divide $i - j \therefore \exists k \in \mathbb{Z}/i - j = kn \therefore j - i = (-k)n \Rightarrow n$ divide $j - i \therefore mod_n(j) = i$, provamos então que $mod_n(i) = j \Rightarrow mod_n(j) = i$, que é a propriedade simétrica; *iii.*) Transitividade; Se $i = mod_n(j)$ e $j = mod_n(k)$, então $i = mod_n(k)$? Ora n divide $i - j$ e n divide $j - k$, então existem inteiros x, y, tal que $i - j = xn$ e $j - k = yn$, somando as duas igualdades: $i - j + (j - k) = xn + yn = i - k = (x + y)n$, portanto $i - k$ é múltiplo de n, isto é, n divide $i - k \therefore i = mod_n(k)$. Assim provamos que mod_n, para n um inteiro positivo, é uma relação de equivalência. □

A relação de equivalência que acabamos de apresentar é comum em Teoria dos Números. Como dissemos, há muitas notações diferentes para essa relação, que nem sempre é apresentada como relação de equivalência, isso é o que ocorre no estudo de divisibilidade entre números inteiros: MDC, máximo divisor comum, MMC, mínimo múltiplo comum e no Teorema Fundamental da Aritmética. Mais à frente vamos retornar a essa idéia, utilizando também um conhecido teorema sobre divisibilidade: o Teorema da Divisão de Euclides.

Definição 1.3.13. *Seja A um conjunto. Uma partição* P *de A é um subconjunto do conjunto das partes de A,* $\mathrm{P} \subset \wp(A)$*, com a seguinte propriedade:*

(i) *Os elementos de* P *são dois a dois disjuntos, isto é,* $\forall B, C \in \mathrm{P}, B \cap C = \emptyset$

(ii) $A = \bigcup_{X \in \mathrm{P}} X$

Nessas condições temos um importante resultado:

Proposição 1.3.14. *Seja R uma relação em A. A relação R é uma relação de equivalência se, e somente se, existe uma partição* P *de A.*

Demonstração. Vamos provar para o caso finito $|A| < \infty$.Devemos provar duas coisas:

(1) ($\Rightarrow$) Se R é uma relação de equivalência em A então existe uma partição P de A;

(2) ($\Leftarrow$) Se existe uma partição P de A, então R é uma relação de equivalência em A.

($\Rightarrow$):seja $x \in A$ e $R[x]$ a imagem de x, tomemos $y \in A \backslash R[x]$; sendo R uma relação de equivalência $R[x] \cap R[y] = \emptyset$, tomando-se $z \in A \setminus (R[x] \cup R[y])$ o conjunto $R[z] \cap R[y] \cap R[x] = \emptyset$, repetindo-se este processo um número finito de vezes, no máximo $|A|$,o conjunto $\{R[x], R[y], \cdots, R[x_i]\}$ determina uma partição P de A: os conjuntos $R[x], R[y]$ são dois a dois disjuntos, por construção; $\forall a \in A, a \in R[A] = (R[x] \cup R[y] \cup \cdots \cup R[x_i])$, uma vez que R é relação de equivalência, isto é, $A = R[x] \dot{\cup} \cdots \dot{\cup} R[x_i]$, união de conjuntos dois a dois disjuntos $\therefore P = \{R[x], \cdots, R[x_i]\}$ define uma partição de A;

($\Leftarrow$): Seja $P \subset \wp(A)$ uma partição de A. Definimos a relação $R : A \to A/x \mapsto y$ se $x, y \in U$, para algum $U \in P$. Desse modo R é uma relação de equivalência, pois: $i.$) R é reflexiva: de fato! Como P é uma partição, $\forall x \in A, \exists U \in P / x \in U \therefore R(x) = x$; $ii.$) R é simétrica: pois se $x = R(y)$, então $\exists U \in P / x, y \in U \therefore R(y) = x$; $iii.$) R é transitiva, uma vez que se $x = R(y)$ e $y = R(z)$, então $x, y, z \in U$, para algum $U \in P$, portanto $x = R(z)$. □

A proposição anterior pode ser utilizada para representar, não somente de forma elegante, porém sintética, a imagem de uma dada relação de equivalência. Isto funciona, porque a toda relação de equivalência está associada uma partição, sendo os elementos da partição conjuntos disjuntos, podemos escolher, ver $A10$, um elemento, "representante", para cada conjunto da partição, que representa todos os elementos desse conjunto e, portanto, simplificar a representação da imagem da relação. Um exemplo clássico é a relação de paridade, que permite representar sua imagem: o conjunto dos números pares e o conjunto dos números ímpares, por dois de seus representantes, sejam 0 e 1. Para indicar que 0 está a representar o conjunto de todos os números pares é comum denotar essa representação por $\bar{0}$, em que $\bar{0} = \{2k / k \in \mathbb{Z}\}$. Portanto a relação do exemplo 2 mostra que $\mathbb{Z} = \bar{0} \cup \bar{1} \cup \cdots \cup \overline{n-1}$, uma representação finita, para um conjunto infinito.

Segundo o axioma $A8$, existe o conjunto,

$$frac = \{\frac{p}{q} / p, q \in \mathbb{Z}, q \neq 0\}.$$

Afirmamos que este conjunto não é o conjunto dos números racionais. De fato! isto é verdade, pois sabemos que os elementos $\frac{2}{3}, \frac{12}{18} \in frac$ e portanto $\frac{2}{3} \neq \frac{12}{18}$. Isto ocorre porque, segundo o axioma $A2$, se fossem iguais, então $2 = 12$ e $3 = 18$. A seguinte proposição justifica esse engano comum.

Proposição 1.3.15. *Seja o conjunto $frac = \{\frac{p}{q} / p, q \in \mathbb{Z}, q \neq 0\}$. A seguinte relação,*

$$Q : frac \to frac / \frac{p}{q} \mapsto \frac{u}{v} \text{ se } pv = qu$$

é uma relação de equivalência. Ademais, os elementos $\overline{\frac{p}{q}}$, tal que, $mdc(p, q) = 1, \forall p, q \in \mathbb{Z}^*$, juntamente com $\bar{0}$, são as classes de equivalência para essa relação.

Demonstração. Mostremos que estão satisfeitas as propriedades de relação de equivalência:

(1) Reflexiva: $Q(\frac{p}{q}) = \frac{p}{q}$ pois $pq = qp$;

(2) simétrica: Se $\frac{u}{v} = Q(\frac{p}{q})$, então $pv = qu$, sendo $qu = uq$ e $pv = vp$, então $uq = vp \therefore Q(\frac{u}{v}) = \frac{p}{q}$, ou seja Q é simétrica;

(3) Transitiva: Sejam $\frac{p}{q}, \frac{u}{v}, \frac{a}{b} \in frac$, tal que $\frac{u}{v} = Q(\frac{p}{q})$ e $\frac{p}{q} = Q(\frac{a}{b})$, então $pv = qu; aq = bp$ multiplicamos a segunda igualdade por v e obtemos $v(aq) = v(bp) = v(pb) = (vp)b = (pv)b$, substituindo $pv = qu$ naquela igualdade, obtemos $v(aq) = (qu)b$, sendo $q \neq 0$, podemos cancelar o número q em ambos os lados, então $va = ub \therefore av = bu \Rightarrow \frac{u}{v} = Q(\frac{a}{b})$

Para verificar que os elementos $\overline{\frac{p}{q}}$, tal que, $mdc(p, q) = 1, \forall p, q \in \mathbb{Z}^*$, são as classes de equivalência, é suficiente observar que estes conjuntos

$$\overline{\frac{p}{q}} = \{\frac{kp}{kq} / k \in \mathbb{Z}^*\},$$

juntamente com $\bar{0} = \{\frac{0}{k} / k \in \mathbb{Z}^*\}$, determinam uma partição de $\mathbb{Q}$. □

A relação de equivalência Q define os números racionais, e cada classe de equivalência de Q representa um número racional.

Exercícios 1.3.16. *(1) Seja A o conjunto dos meses do ano e vogal a relação que associa a cada elemento x de A, os meses que têm a mesma quantidade de consoantes, sem repetição. Mostre que essa relação é uma relação de equivalência, e determine a imagem de cada elemento. É verdade que para qualquer elemento, a sua imagem e a sua imagem inversa são sempre iguais?*

(2) Para o conjunto $A = \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10\}$, seja divisível a relação de A em A que a todo elemento $x \in A$ associa os números entre 0 e 10 que são divisíveis por x.

a) *Determine o domínio, o contra-domínio e o conjunto imagem dessa relação.*

b) *Determine divisível(2) e divisível$[7]$?*

c) *Determine divisível$^{-1}\{0\}$, isto é a imagem inversa do 0;*

d) *A relação divisível é uma relação de equivalência?*

(3) Seja a relação $R : \{1, 2, ..., 11, 12\} \to \{1, 2, ..., 11, 12\}; x \mapsto y$ se x e y têm o mesmo resto na divisão por 4.

a) *Determine $R(3)$ e $R[11]$;*

b) *Determine $R^{-1}[6]$;*

c) *Mostre que* $R[0] \cup R[1] \cup R[2] \cup R[3]$ *é uma partição do conjunto* $\{1, 2, ..., 11, 12\}$*;*

d) *R é uma relação de equivalência? Prove ou dê um contra-exemplo.*

(4) Seja R uma relação em X, isto é, entre X e Y = X. Dizemos que R é uma relação de equivalência se ocorrem 3 condições: 1. $R(x) = x$ *(pp reflexiva); 2. Se* $R(x) = y$ *então* $R(y) = x$ *(pp simétrica); 3. Se* $R(x) = y$ *e* $R(y) = z$*, então* $R(x) = z$ *(pp transitiva). Dê exemplos de relações de equivalência. Explique se é mais correto dizer* $R(x) = x$*, ou* $x \in R(x)$*? Reformule as outras duas condições com essa notação.*

(5) Seja R uma relação de equivalência em X, mostre que somente uma das seguintes condições ocorrem: $R(x)$=$R(y)$ *ou* $R(x) \bigcap \mathbb{R}(y) = \emptyset$*. Por exemplo a paridade é uma relação de equivalência para os números inteiros e* $R(1)$=$\{...-3, -1, 1, 3, 5, ...\}$ *e* $R(2)$=$\{..., -6, -4, -2, 0, 2, 4, ...\}$*, de modo que sempre ocorre a condição acima.*

(6) Sejam os conjuntos $P = \{\{0, 2, 4, 8\}, \{3, 6, 9\}, \{5, 1, 10\}, \{1, 7\}\}$ *e* $A = \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10\}$*. Responda:*

a) *O conjunto P define uma partição para o conjunto A?*

b) *Se a aplicação* $R : A \to A$*, definida por* $R(1) = \{1, 7\}; R(2) = \{0, 2, 4, 8\}; R(3) = \{3, 6, 9\}; R(5) = \{5, 10, 1\}$ *é uma relação de equivalência, calcule a imagem dos demais elementos do domínio.*

c) *É possível definir para este conjunto, uma relação de equivalência com 4 imagens distintas, porém com o mesmo número de elementos?*

(7) Seja X um conjunto, dizemos que P=$\{p_1, p_2, ..., p_i\}$ *é uma partição de X, se* $X = p_1 \bigcup p_2 \bigcup ...p_i$ *, ou seja, X é igual a união dos elementos de P. Essa partição é disjunta, quando a intersecção de cada dois conjuntos distintos da partição é vazia. Mostre que se R é uma relação de equivalência em X, então a imagem de R define uma partição disjunta de R.*

(8) Dê uma partição para o conjunto dos números inteiros, em que o conjunto P, a partição de X, tenha:

a 2 *elementos;*

b 3 *elementos;*

c *n elementos.*

(9) Seja $A = \{janeiro, fevereiro, março, abril, maio, junho, julho, agosto, //setembro, outubro, novembr$ *e* $vg : A \to A; vg(x) = y$ *, quando o conjunto das vogais de x e o conjunto das vogais de y são iguais. Mostre que vg é uma relação de equivalência. Se* $vgi : A \to A; vg(x) = y$*, quando o número de elementos do conjunto das vogais de x for igual ao número de elementos do conjunto das vogais de y, mostre que vgi é uma relação de equivalência.*

(10) Prove que se uma relação de equivalência é também uma função, então esta função é única. Nesse caso, qual deverá ser esta função?

(11) Seja $mod_6 : \{0,1,2,3,4,5,6,7,8\} \to \{0,1,2,3,4,5,6,7,8\}$ *a relação que associa* $n \mapsto m$ *se* $6 \mid n - m$*. Determine a relação* mod_6*, isto é, o conjunto imagem de cada elemento do domínio e prove que a relação é uma relação de equivalência.Determine as classes da relação.*

(12) Seja $mod_6 : \mathbb{Z} \to \mathbb{Z}$*, tal que,* $x \mapsto y$ *se* $6 \mid x - y$*. Mostre que* mod_6 *é uma relação de equivalência e quais as classes dessa relação.*

(13) Seja $resto : \mathbb{Z} \to \mathbb{Z}$*, tal que,* $resto(x) = y$ *se* x *e* y *têm o mesmo resto, quando são divididos por* 6*. Mostre que* $resto$ *é uma relação de equivalência. Verifique, ainda, que a relação* $resto$ *e a relação* mod_6 *definida anteriormente é a mesma relação.*

(14) Determine uma partição para o conjunto Z*, dos inteiros, com a relação* mod_n *, nos seguintes casos:*

a $n = 2$*;*

b $n = 3$*;*

c $n = 5$*;*

d $n = 12$*.*

(15) Seja mod_n *uma relação em* Z*, o conjunto dos números inteiros, que associa a cada inteiro* i*, o resto da divisão de* i *pelo número* n*. Mostre que* mod_n *é uma relação de equivalência para todo* n *inteiro positivo.*

(16) Seja α *um plano,* $X \subset \alpha$ *o conjunto de todas as retas do plano* α*. Seja* $P : X \to X$ *uma relação, tal que* $P(r) = s$ *se* $r//s$*, ou seja, as retas são paralelas. Mostre que* P *é uma relação de equivalência.*

(17) Seja α *um plano,* $X \subset \alpha$ *o conjunto de todas as retas do plano* α*. Seja* $P : X \to X$ *uma relação, tal que* $P(r) = s$ *se* $r \perp s$*, isto é, as retas são perpendiculares.* P *é uma relação de equivalência?*

(18) Seja $X = \{1,2,3,4\}$ *e* $\wp(X)$ *o conjunto das partes de* X*. Seja* $O : \wp(X) \to X$*,* $O(A) = B$ *somente quando* $|A| = |B|$*, ou seja, os conjuntos* A *e* B *têm a mesma quantidade de elementos. Prove que* O *é uma relação de equivalência. Em seguida determine as classes de equivalências de* O*.*

(19) Sejam os conjuntos $P = \{\{0,\{a,b\}\},\{-1,\{a,b\}\},\{-1,0\}\}$ *e* $A = \{-1,0,\{a,b\}\}$*.Responda:*

a) *O conjunto* P *define uma partição para o conjunto* A*?*

b) *Se a relação* $R : A \to A$, *definida por* $R[\{0\}] = \{-1, \{a, b\}\}; R[\{-1\}] = \{0, \{a, b\}\}$, *tal que* $\{(\{a, b\}, -1); (\{a, b\}, 0)\} \subset R$, *determine* $R[a, b]$;

c) *Explique se a relação do item b) é uma relação de equivalência?*

(20) Mostre que o conjunto de classes de equivalência de $\mathbb{Q}$ *são os elementos* $\overline{\frac{p}{q}}/mdc(p, q) = 1, \forall p, q \in \mathbb{Z}^*$ *e o* $\bar{0}$, *a classe dos números* $\frac{0}{q}/q \in \mathbb{Z}^*$.

1.3.4 Funções Injetoras, Sobrejetoras e Bijetoras

Para o que segue, vamos discutir três tipos de funções: as funções injetoras, as funções sobrejetoras e as funções injetoras e sobrejetoras, denominadas funções bijetoras.

Em geral, dada uma relação, é comum existirem propriedades que são preservadas pela relação. Em particular isso também ocorre para as funções. As funções injetoras são aquelas que preservam a propriedade de desigualdade para os elementos do domínio, isto é, elementos diferentes do domínio têm imagens diferentes no contra-domínio. Isto ocorre para qualquer função do tipo $f(x) = ax + b/a, b \in \mathbb{R}, a \neq 0$. Porém não ocorre para as funções de segundo grau. De fato! se $g : \{-1, 0, 1\} \to \{0, 1, 2, 3, 4\}$ é tal que, $g(x) = x^2$, $-1, 1$ são elementos do domínio e $-1 \neq 1$, mas $g(-1) = g(1) = 1$, isto é, as imagens não preservam, sempre, a desigualdade. Essa propriedade tem destaque pois para toda função injetora f, se y é um elemento da imagem, então o conjunto $f^{-1}[y]$ é unitário. No exemplo acima $g^{-1}[1] = \{-1, 1\}$.

Uma propriedade importante das funções injetoras é que se y é um elemento do contra-domínio, $|f^{-1}[y]| \in \{0, 1\}$. Desse modo, se $y \in Im(f)$, podemos associar a y um único elemento, que é sua imagem inversa. Isso permite, para uma função *injetora* $f : X \to Y$, definir a seguinte função $f^{-1} : Im(f) \to A$, que associa aos elementos do domínio, $y \in Im(f)$, o elemento $x \in X$, tal que, $f(x) = y$. A propriedade do conjunto $Im(f)$, garante o critério de existência para a imagem de y; a propriedade de injetividade da função f, garante a unicidade da imagem, e portanto f^{-1} é uma função. É uma verificação imediata, que a função assim obtida, tem a propriedade de seu contra-domínio ser igual a sua imagem, isto é $f^{-1}[Im(f)] = X$. As funções com essa propriedade, contra-domíno igual à imagem, são denominadas de funções sobrejetoras.

Vimos, acima, que se $f : X \to Y$ é uma função injetora, sempre é possível definir uma função a partir da imagem da f. Veremos mais à frente que esta função tem propriedades semelhantes a função f, por exemplo, ela também é injetora. No entanto, não é possível definir a função f^{-1} com o domínio igual ao contra-domínio da f. Isso somente será possível quando $Im(f) = Y$, isto é, quando a função f for sobrejetora. A função sobrejetora possui a seguinte propriedade: $\forall y \in Y, \exists x \in X / f(x) = y$. Uma função f que é injetora e sobrejetora é denominada função bijetora.

Apresentamos as seguintes definições para uma função f.

Definição 1.3.17. *Seja $f : X \to Y$ uma função.*

(i) *f é uma função injetora se $\forall x, z \in X, x \neq z \Rightarrow f(x) \neq f(z)$;*

(ii) *f é uma função sobrejetora se $f[X] = Y$*

(iii) *f é uma função bijetora se f é injetora e sobrejetora*

Uma propriedade fundamental para as funções bijetoras é a existência, para qualquer f bijetora, de uma função f^{-1}, tal que $f \circ f^{-1} = f^{-1} \circ f = Id$, sendo Id a função identidade, isto é, $\forall x \in Dom(Id), Id(x) = x$. A função f^{-1}, em geral, é denominada função inversa de f, e reciprocamente.

Exemplo 1.3.18. *(1) A função identidade, isto é, $f : A \to A / f(x) = x$ é uma função injetora, sobrejetora e portanto bijetora;*

(2) A função $f : \{1, 2, 3\} \to \mathbb{R} / f(x) = x^2 - x - 6$ é injetora, porém não sobrejetora;

(3) A função $f : [\frac{1}{2}, \infty[\to \mathbb{R} / f(x) = x^2 - x - 6$ é injetora, porém é não-sobrejetora, pois $-7 \in \mathbb{R}, \nexists x \in Dom(f) / f(x) = -7$;

(4) A função $f :]\frac{1}{2}, \infty[\to]\frac{-25}{4}, \infty[/ f(x) = x^2 - x - 6$, é injetora e sobrejetora, portanto é bijetora; sua inversa é a função

$$f^{-1} :]\frac{-25}{4}, \infty[\to]\frac{1}{2}, \infty[/ f(x) = \frac{1 - \sqrt{4x + 25}}{2};$$

(5) Lembrando que

$$|| : \mathbb{Z} \to \mathbb{Z} / |n| = \begin{cases} n, \text{ se } n \geq 0; \\ -n, \text{ se } n < 0 \end{cases},$$

é denominada função módulo. Essa função é não sobrejetora, uma vez que $2 \in \mathbb{Z}, \nexists x \in \mathbb{Z}, |x| = -2$; e é não injetora, pois $-1 \neq 1$ e $|-1| = |1|$;

(6) A função constante $f : \mathbb{R} \to \mathbb{R} / f(x) = 2$ é não injetora, pois $f(0) = f(1) = 2$, enquanto que $0 \neq 2$, isto é não preserva desigualdade; também não é sobrejetora, pois $Im(f) = \{2\}$

(7) A função

$$f : \mathbb{R} \to \mathbb{R} / f(x) = \begin{cases} x^2 - x - 6, \text{ se } x \in]-\infty, \frac{1}{2}[; \\ -4x - 6, \text{ se } x \in [\frac{1}{2}, \infty[\end{cases},$$

é injetora, porém não-sobrejetora, pois $-7 \in \mathbb{R}, \nexists x \in \mathbb{R} / f(x) = -7$. Isto ocorre, porque, -7 deve ser ou imagem da parábola, nesse caso $-7 = x^2 - x - 6 \therefore x^2 - x + 1 = 0$ e a raiz dessa equação não é real, pois $\Delta = -3 < 0$; ou -7 é imagem da reta, nesse caso $-7 = -4x - 6 \Rightarrow x = \frac{1}{4} \notin [\frac{1}{2}, \infty[$. Portanto -7 não é imagem da função f.

Apresentamos a seguir algumas técnicas de contagem para as funções injetoras, sobrejetoras e bijetoras. Vamo-nos deter no caso finito. Para o caso infinito apresentamos apenas um resultado.

Sejam X e Y dois conjuntos finitos. Assim como procedemos para as relações, calculando quantas relações podemos definir, fixados o domínio e o contradomínio de uma relação, podemos fazer o mesmo para as funções de X em Y. Sendo o conjunto X finito, podemos enumerar o conjunto $Im(f) = \{f(x_1), f(x_2), \cdots, f(x_{|X|})\}$. Não havendo restrições para a função f, $\forall x \in A, f(x) \in B$, podendo assumir, qualquer valor do conjunto Y. Se $|Y| = n$, cada imagem pode assumir n valores distintos, portanto fixados dois valores x, z, para cada um dos m possíveis valores de $f(x)$, podemos escolher outros m valores distintos de $f(x)$, em um total de $n * n$ funções distintas para x, z. Percorrendo-se todos os valores do domínio, teremos n^m funções distintas.

Se por um lado, $f : X \to Y$ é uma função injetora, deve ocorrer que $|X| \leq |Y|$. De fato! Sendo f injetora, há tantas imagens diferentes, quantos são os elementos de X, portanto $|X| = |Im(f)|$, como $Im(f) \subseteq Y \Rightarrow |Im(f)| \leq |Y|$, portanto $|X| \leq |Y|$. Por outro lado, se $f : X \to Y$ é sobrejetora, então $|X| \geq |Y|$, pois neste caso, $\forall y \in Y, \exists x \in X / f(x) = y$, isto é, a cada elemento do contra-domínio está associado, no mínimo, a um elemento do domínio. Desse modo se a função f é bijetora, pela injetividade ocorre $|X| \leq |Y|$ e, por conta da sobrejetividade, $|X| \geq |X|$, logo $|X| = |Y|$.

Ainda para o caso $|X|, |Y|$ finitos, podemos determinar o número de funções $f : X \to Y$, para os casos injetivo, sobrejetivo e bijetivo. Assim, se f é bijetora, $|X| = |Y| = n \in \mathbb{N}^*$. Podemos enumerar o conjunto imagem, $Im(f) = \{f(x_1), \cdots, f(x_n)\}$; $f(x_1) \in Y$, portanto há n possibilidades de escolha para definir a imagem de x_1, se escolhermos $f(x_1) = y \in Y$, devido à injetividade de f, a imagem para o próximo elemento $f(x_2) \in Y \setminus \{y\}$, portanto há $n-1$ possibilidades de escolha. Analogamente para os demais elementos da imagem, $f(x_k)$ terá $(n-k+1)$ possibilidades. Assim o número total de funções possíveis de serem definidas será $n.(n-1).\cdots.3.2.1 \doteq n!$. O princípio multiplicativo pode ser verificado por indução finita.

Se a função $f : X \to Y$ é injetora, a condição de cardinalidade para os conjuntos é $|X| = m \leq |Y| = n$, com um argumento semelhante ao anterior, o número possível de funções injetoras é $n.(n-1)\cdots.(n-m+1) = \frac{n!}{(n-m)!}$.

Se $f : X \to Y$ é sobrejetora, a condição de cardinalidade é $|X| = m \geq |Y| = n$. Para o caso $m = n$ o resultado é o mesmo do caso bijetivo, porém se $m > n$, o domínio tem mais elementos que a imagem, enquanto houver excesso de elementos, a imagem de cada elemento tem n possibilidades, a partir da condição de igualdade, o caso fica análogo à bijetividade. Portanto, o número de funções sobrejetoras é:

$$|Y|^{|X|-|Y|)}(|Y|)! = n^{(m-n)}.n!$$

Provamos o seguinte resultado:

Teorema 1.3.19. *Seja $f : A \to B$ uma relação, tal que, A, B são conjuntos finitos: $|A| = m$ e $|B| = n$.*

i. *Há 2^{mn} relações distintas;*

ii. *Há n^m funções;*

iii. *Há $\frac{n!}{(n-m)!}$ funções injetoras;*

iv. *Há $n^{(m-n)}.n!$ funções sobrejetoras;*

v. *Há $n!$ funções bijetoras.*

Exercícios 1.3.20.

Apresentamos algumas noções básicas, porém essenciais para um bom aproveitamente do que iremos estudar a seguir. Esperamos despertar o leitor, com este texto, para a importância, em matemática, de um tratamento rigoroso, e eventualmente formal, e utilização de uma linguagem precisa para apresentação de conceitos, idéias e demonstrações. Finalizamos o capítulo com o teorema de Cantor-Bernstein-Schröder, para funções sobre domínios infinitos, uma referência sobre a demonstração desse teorema pode ser encontrada no artigo [2]

Teorema 1.3.21. *(Teorema de Cantor-Bernstein-Schröder) Dados dois conjuntos X e Y, se existem duas funções $f : X \to Y, g : Y \to X$ injetoras, então X e Y têm a mesma cardinalidade.*

Este teorema permite estudar conjuntos de cardinalidade arbitrária. Uma importante aplicação deste teorema é apresentada a seguir, antes de apresentá-la, definimos os seguintes conceitos:

Definição 1.3.22. *Seja N um conjunto. Dizemos que que N é enumerável se existe uma bijeção entre N e $\mathbb{Z}$, o conjunto dos números inteiros. Um conjunto é não-enumerável se sua cardinalidade não é finita e não existe uma bijeção com o conjunto dos inteiros.*

Vimos que dados dois conjuntos, podemos definir o produto cartesiano entre eles. Ademais, podemos estender esta definição para qualquer número finito de conjuntos. A seguinte definição estende o produto cartesiano para um número não limitado de conjuntos.

Definição 1.3.23. *Dizemos que um conjunto $\mathbf{C}$ é o produto cartesiano enumerável de conjuntos, se existe um conjunto de índices I, enumerável e uma família de conjuntos $A_i/i \in I$, tal que,*

$$\mathbf{C} = A_m \times A_n \times \cdots \times A_k \times \cdots \doteq \prod_{i \in I} A_i.$$

Teorema 1.3.24. *Seja* **B** *o produto cartesiano enumerável do conjunto* $\{0,1\}$. *Existe uma bijeção entre os conjuntos* **B** *e* $\mathbb{R}$.

Corolário 1.3.25. *A cardinalidade dos números reais é não-enumerável, isto é,* $|\mathbb{R}| = 2^{\omega}$, *sendo* $\omega = |\mathbb{N}|$.

Sabemos que $\forall n \in \mathbb{N}, n < 2^n$, podemos provar isso por indução finita. Por indução transfinita, podemos provar que este resultado vale para qualquer cardinal, portanto $\omega < 2^{\omega}$. Sendo $\omega = |\mathbb{N}|$ e $|\mathbb{R}| = 2^{\omega}$, temos dois cardinais infinitos, porém não iguais! O primeiro cardinal é denominado *infinito enumerável* e o segundo *infinito não-enumerável*. A afirmação que não existe nenhum cardinal entre o infinito enumerável e o infinito não-enumerável é conhecida como hipótese do contínuo. Uma notação para estes cardinais é: $\omega \doteq \aleph_o$ e $2^{\omega} \doteq \aleph_1$, a primeira letra do alfabeto hebraico chamada Aleph. Existe uma conjectura sobre os cardinais infinitos: se $\aleph_0, \aleph_1, \aleph_2, \cdots$ é a seqüencia de cardinais infinitos consecutivos, então $2^{\aleph_i} = \aleph_{i+1}$. Esta conjectura é conhecida como hipótese generalizada do contínuo.

Embora não iremos estudar Ordinais e Cardinais, o teorema de *Cantor-Bernstein-Schröder* ilustra um fato essencial na teoria das funções, isto é, que não necessitamos, *a priori*, conhecer as funções do modo clássico-funcional, para afirmar ou refutar propriedades. As funções são entes mais abstratos, que devem satisfazer às condições de existência e unicidade em relação a dois conjuntos não vazios, como apresentado nos exemplos. Em demonstrações como este teorema, no entanto, geralmente, é necessário construir funções que representem as propriedades apontadas.

Procuramos dar ênfase à teoria de relações e funções, com enfoque na teoria de conjuntos, pela necessidade que temos, para o estudo em àlgebra abstrata, de construir estes objetos a partir de uma teoria elementar, básica e, dessa forma, rigorosa. Este material será utilizado para introdução à teoria de grupos, a partir do estudo das operações binárias, que exigem um conhecimento bem fundamentado dos fatos aqui expostos. A última seção, o teorema de Cantor-Schröder-Benrstein foi brevemente discutida, com o intuito de despertar no leitor a atenção para um tema essencialmente abstrato: a noção de infinito em Matemática.

Capítulo 2

Relações, Operações Binárias e Grupos

No capítulo anterior demos ênfase à caracterização axiomática da teoria de conjuntos. Essa abordagem, embora aparentemente árida, permite construir teorias a partir de conceitos elementares, apresentar idéias e demonstrações não triviais, que exigem algum nível de abstração e conhecimento matemático. Os axiomas, ou definições, são os primeiros passos para iniciar a *jornada abstrata* que a Álgebra propõe.

A escolha didática que fizemos, de partir dos axiomas, tem sido fruto de muita discussão sobre educação matemática. Acreditamos, que isso ocorra porque a iniciação nos axiomas seja freqüentemente adiada ou mesmo evitada, bem como apresente dificuldades inerentes a sua complexidade. Aqui fazemos um convite ao leitor para continuarmos nesse caminho.

Inicialmente definimos o conceito de relação binária e operação binária. Apresentamos algumas propriedades para as operações binárias e destacamos três delas para a definição de grupo. A partir daí, exemplificamos com alguns casos particulares, partimos às construções mais gerais, de modo a iniciarmos um curso introdutório à teoria de grupos em álgebra abstrata. A referência básica, [4] é o livro *Um primeiro curso em Àlgebra Abstrata*.

2.1 Relação Binária

No capítulo 1 definimos relação e ressaltamos a idéia de relacionar dois conjuntos, a partir de alguma relação. Podemos entender a relação binária como uma forma de relacionar pares de elementos de um mesmo conjunto, com os mesmos elementos do conjunto. Desse modo a cada par de elementos de um conjunto C, associamos os elementos de A, ou seja o domínio da relação binária é o produto cartesiano $A \times A$, e a imagem o conjunto A, o que nos referimos como relação

binária em A.

Definição 2.1.1. *Dizemos que R é uma relação binária em A se R é uma relação cujo domínio é o conjunto $A \times A$ e o contradomínio é o conjunto A, que indicamos por $R : A \times A \to A$.*

As relações binárias ocorrem naturalmente. Por exemplo, as 4 operações aritméticas, a soma: $3 + 4$ é a relação de adição, com o par $(3, 4)$, cujo resultado é o número inteiro 7, os exemplos a seguir complementam nossa compreensão.

Exemplo 2.1.2. *(1)* $+ : \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z} / + (m, n) \mapsto m + n$;

(2) $+\{-2, -1, 1, 3\} \times \{-2, -1, 1, 3\} \to \{-2, -1, 1, 3\} / (m, n) \mapsto m + n$

(3) $=: \mathbb{N} \times \mathbb{N} \to \mathbb{N} / = (m, n) \mapsto m = n$

(4) $entre : \{2, 5, 11, 14\} \times \{2, 5, 11, 14\} \to \{2, 5, 11, 14\} / entre(m, n) \mapsto x$, *tal que* $m < x < n$

(5) $\Delta : \wp(\{0, 1\}) \times \wp(\{0, 1\}) \to \wp(\{0, 1\})$, *que associa ao par de conjuntos* $(A, B) \mapsto (A \cup B) \setminus (A \cap B)$

A imagem de uma relação binária R em A é, como vimos para as relações, o subconjunto de A, cujos elementos estão associados aos pares ordenados do conjunto $A \times A$, definidos pela relação. A relação binária é portanto o conjunto dos pares $((a, b), c)$ tal que R(a,b)=c. Assim, no exemplo 2, a imagem da relação é o conjunto $Im(+) = \{-2, -1, 1\}$; e a relação o conjunto

$$+ = \{((-2, 1), -1), ((-2, 3), 1), ((-1, -1), -2), ((1, -2), -1), ((3, -2), 1)\},$$

de fato $+(3, -2) = 3 + (-2) = 1 \therefore ((3, -2), 1) \in +$, isto é, um elemento da relação binária $+$. Observe que $\nexists + (1, 3) \in +$, pois $+(1, 3) = 4 \notin \{-2, -1, 1, 3\}$. Por não haver ambigüidade, também denotamos os pares ordenados $((a, b), c)$ pelas ternas (a, b, c).

Uma apresentação esquemática dos pares ordenados de uma relação pode ser feita a partir da tabulação dos elementos do domínio, dispostos em linhas e colunas, em que cada elemento interno, z, da tabela representa a relação R sobre o par ordenado, (x, y), considerado, com o seguinte significado: $R(x, y) = z$ o elemento da tabela correspondente à linha de x e à coluna de y. Como representado a seguir: seja a relação $*$ em $A = \{\cdots, w, x, y, \cdots$, isto é, $* : A \times A \to A$. A tábua da relação $*$ é representada pela seguinte tabela:

$*$	$\cdots$	w	x	y	$\cdots$
$\vdots$					
w					
x				$z = R(x, y)$	
y					
$\vdots$					

.

Para a exemplo 2, a tabela da relação + é:

$+$	-2	-1	1	3
-2	$\nexists$	$\nexists$	-1	1
-1	$\nexists$	-2	$\nexists$	$\nexists$
1	-1	$\nexists$	$\nexists$	$\nexists$
3	1	-2	$\nexists$	$\nexists$

.

Em casos, como a relação do exemplo 4, podemos separar os elementos, quando não únicos, por vírgulas:

entre	2	5	11	14
2	$\nexists$	$\nexists$	5	$5, 11$
5	$\nexists$	$\nexists$	$\nexists$	11
11	$\nexists$	$\nexists$	$\nexists$	$\nexists$
14	$\nexists$	$\nexists$	$\nexists$	$\nexists$

.

Destacamos a relação binária do exemplo 5, pela importância das propriedades que ela satisfaz, discutidas a seguir.

Δ	$\emptyset$	$\{0\}$	$\{1\}$	$\{1, 0\}$
$\emptyset$	$\emptyset$	$\{0\}$	$\{1\}$	$\{1, 0\}$
$\{0\}$	$\{0\}$	$\emptyset$	$\{1, 0\}$	$\{1\}$
$\{1\}$	$\{1\}$	$\{1, 0\}$	$\emptyset$	$\{0\}$
$\{0, 1\}$	$\{0, 1\}$	$\{1\}$	$\{0\}$	$\emptyset$

.

A tábua da relação binária, para casos finitos, ou em que se possa reduzir ao caso finito, permite um cálculo rápido e preciso da relação. Os exemplos mostrados apresentam casos em que a relação binária pode não existir para alguns pares, exemplos 2 e 4, ou não é única, exemplo 4, isto é, não é uma *função*. Vamos, a partir desse ponto, a menos que seja explicitamente mencionado, considerar apenas as relações binárias que são função. Nesse caso denominamo-las ***operações binárias***.

Exercícios 2.1.3. *(1) Seja* $A = \{0, 1, 2, 3, 4, 5\}$ *e* $+ : A \times A \to A$ *a relação binária que a cada par* (i, j) *associa o número* $i + j$ *a soma usual.*

(2) Seja $A = \{0, 1, 2, 3, 4, 5\}$ *e* $+mod_3 : A \times A \to A$ *a relação binária que a cada par* (i, j) *associa o resto da divisão de* $i + j$ *por* 3*, sendo* $+$ *a soma usual.*

(3) Seja $A = \{0, 1\}$ *e* $* : A \times A \to A : (i, j) \mapsto ij$ *o produto usual.*

(4) Seja $A = \{-2, -1, 0, 1, 2\}$ *e* $* : A \times A \to A : (i, j) \mapsto i^j$*, como potência.*

(5) Seja $X = \{1, 2, \{1\}\}$*. Determine a imagem da relação binária:*

a) $\bigcup : \wp(X) \times \wp(X) \to \wp(X) : (A, B) \mapsto A \cup B$*;*

b) $\bigcap : \wp(X) \times \wp(X) \to \wp(X) : (A, B) \mapsto A \cap B$.

(6) Seja $F = \{x, x^2, x+2, x-2, 5x-3, x^2+4x+4, x^2-4x+4, 5x-1, \frac{x+3}{5}, \frac{x+1}{5}\}$ *um conjunto de funções. Determine a tábua da relação binária* $\circ : F \times F \to F : (u, v) \mapsto u \circ v$, *a composição de funções.*

(7) Seja $G = \{\{(a,a),(b,b),(c,c)\}, \{(a,b),(b,c),(c,a)\}, \{(a,c),(b,a),(c,b)\}\}$ *um conjunto de funções. Determine a tábua da relação binária* $\circ : G \times G \to G : (u, v) \mapsto u \circ v$.

(8) Determine a relação binária soma $: F \times F \to F : (u, v) \mapsto u + v$, *para* $F = \{1, x, x^2, 1 + x, 2x, x^2 + 1, x^2 + 2x, (x + 1)^2\}$, *um conjunto de funções.*

(9) Recordando que se A, B *são conjuntos,* $A \setminus B = \{x : x \in A, x \notin B\}$, *se* $X = \{1, 2, 3\}$ *determine a relação binária sobre* $\wp(X)$, *dada por:* $\Delta : \wp(X) \times \wp(X) \to \wp(X) : \Delta(A, B) = (A \cup B) \setminus (A \cap B)$.

(10) Para a conjunto $X = \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10\}$, *determine a tábua da relação binária* $mult : X \times X \to X$, *tal que,* $mult(i, j) = n$ *se* n *é múltiplo comum de* i *e de* j. *Lembrando que* n *é múltiplo de* i *se* $\exists k \in \mathbb{Z}$, *tal que,* $n = ki$.

(11) Para a conjunto $X = \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10\}$, *determine a tábua da relação binária* $mmc : X \times X \to X$, *tal que,* $mmc(i, j) = n$ *se* n *é o menor múltiplo comum de* i *e de* j.

(12) Seja $X = \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10\}$. *Determine a relação binária* $div : X \times X \to X$, $(i, j) \mapsto n$, *tal que* n *seja um divisor comum de* i *e* j.

(13) Seja $X = \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10\}$. *Determine a relação binária* $mdc : X \times X \to X$, $(i, j) \mapsto mdc(i, j)$, *o máximo divisor comum de* i *e* j

2.2 Operação Binária

Definição 2.2.1. *Seja* R *uma relação binária em* A. *Dizemos que* R *é uma operação binária, se a relação* R *é uma função.*

Exemplo 2.2.2. *(1) O exemplo 5, anterior, é uma operação binária;*

(2) Seja A *o conjunto dos restos da divisão por* 4, *isto é,* $A = \{0, 1, 2, 3\}$ *e* $+mod_4$ *a relação binária* $+mod_4 : A \times A \to A$, *definida por,* $+mod_4(i, j) = resto[(i + j), 4]$, *o resto de* $i + j$, *dividido por* 4; *sendo* $6 = 1 * 4 + 2$, *o resto da divisão de* 6 *por* 4 *é* 2, *logo* $+mod_4(2 + 4) =$

$resto(6,4) = 2$. *Podemos construir a tabela da operação* $+mod_4$ *sobre* A*:*

$+mod_4$	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

;

e verificarmos que os critérios de existência e unicidade estão atendidos, portanto a relação $+mod_4$ *é uma operação binária.*

(3) Analogamente a operação $*mod_4$ *sobre* $A = \{0,1,2,3\}$*, definida por:* $*mod_4 : A \times A \to A, *mod_4(i,j) = resto(ij,4)$*, o resto de i.j, o produto usual, por* 4 *é uma operação binária, como mostra a tábua da operação* $*mod_4$*:*

$*mod_4$	0	1	2	3
0	0	0	0	0
1	0	1	2	3
2	0	2	0	2
3	0	3	2	1

;

(4) A relação binária $+$ *sobre os inteiros é uma operação binária. De fato,* $+ : \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z}$*, que a todo para ordenado* $(i,j), i,j \in \mathbb{Z}$ *associa a soma* $i+j$*, satisfaz os critérios de existência e unicidade. Observe que não é possível escrever a tábua da operação* $+$*, pois o conjunto* $\mathbb{Z}$ *é infinito, embora garantimos que a soma de dois números inteiros é um número inteiro, pela propriedade do conjunto* $\mathbb{Z}$*.*

(5) Composição de funções: seja $A = \{f : \{1,2,3\} \to \{1,2,3\} / f$ *é bijetora*$\}$*. Como vimos no capítulo 1, há* $3! = 6$ *funções bijetoras sobre um conjunto com 3 elementos, logo* $|A| = 6$*, são elas:* $u(1) = 1, u(2) = 2, u(3) = 3, v(1) = 1, v(2) = 3, v(3) = 2, a(1) = 2, a(2) = 1, a(3) = 3, b(1) = 2, b(2) = 3, b(3) = 1, m(1) = 3, m(2) = 2, m(3) = 1, n(1) = 3, n(2) = 1, n(3) = 2$*. Isto é,* $A = \{u, v, a, b, f, g\}$ *seja* $\circ$ *a relação binária de composição de funções,* $\circ : A \times A \to A / \circ(f,g) = f \circ g$*, lembrando que,* $f \circ g(x) = f(g(x))$*, ou seja* $v \circ m(1) = v(m(1)) = v(3) = 2$*, então a função* $v \circ m \in \{a, b\}$*, pois ambas têm* 2 *como imagem de* 1*, porém* $v \circ m(2) = v(m(2)) = v(2) = 3$*, logo* $v \circ m = b$*, pois* 3 *é a imagem de* 2 *para a função* b*. Procedendo desse forma construímos a seguinte tábua:*

$\circ$	u	v	a	b	m	n
u	u	v	a	b	m	n
v	v	u	n	m	b	a
a	a	b	u	v	n	m
b	b	a	m	n	v	u
m	m	n	b	a	u	v
n	n	m	v	u	a	b

.

(6) Seja $i \in \mathbb{C}$, a unidade imaginária, isto é, $i^2 = -1$ e $A = \{-1, -i, 1, i\} \subset \mathbb{C}$. A relação binária do produto usual em A; $* : A \times A \to A / * (u, v) = uv$ é uma operação binária;

(7) Seja $m \in \mathbb{Z}$, $div(m) \doteq \{i / i \in \mathbb{Z}^+, i \text{ divide } m\}$, Se $m, n \in \mathbb{Z}^*$, definimos $mdc(n, m) =$máximo$(div(n) \cap div(m))$, máximo divisor comum, é uma operação binária em $\mathbb{Z}$

(8) Seja A um conjunto não vazio e $F(A)$ o conjunto de todas as funções em A, isto é, $F(A) = \{f : A \to A / f \text{ é uma função}\}$; a relação binária $\circ : F(A) \times F(A) \to F(A) / \circ (f, g) = f \circ g$ é uma operação binária;

(9) a relação $- : \mathbb{N} \times \mathbb{N} \to \mathbb{N} / -(i, j) = i - j$ não é uma operação binária, pois $-(1, 2) = -1 \notin \mathbb{N}$, portanto não verifica o critério de existência.

O exemplo 1 trata de uma idéia que discutimos rapidamente sobre divisibilidade entre números inteiros. Vimos que $a|b$ se $\exists k \in \mathbb{Z} / b = ka$, ou seja, b é múltiplo de a. Não ocorre, em geral, que um número divida o outro: um número maior, em módulo, nunca divide, no sentido da definição dada, um número menor, enquanto que a situação inversa pode, ou não ocorrer. Por exemplo, 5 não divide 23. Então surge a seguinte questão: dados dois inteiros m, n, qual o menor número inteiro não negativo r, tal que $n|(m - r)$, e este valor r sempre existe? A resposta a essa questão é o teorema da divisão de Euclides, que afirma:

Teorema 2.2.3. *Dados $m, n \in \mathbb{Z}$, existem $q, r \in \mathbb{Z}$, tal que $m = qn + r, 0 \leq r < |n|$.*

Vamos utilizar a notação resto(m, n), para indicar o valor r do teorema da divisão de Euclides. Ou seja, resto$(23, 5) = 3$. Este teorema permite a seguinte afirmação.

Proposição 2.2.4. *Seja $+$ e $*$ as operações binárias de adição e multiplicação no conjunto dos inteiros, n um número inteiro positivo e $A = \{0, 1, \cdots, n - 1\}$ o conjunto dos possíveis valores do resto da divisão de qualquer número inteiro m por n. Seja $\star \in \{+, *\}$, a relação binária*

$$\star mod_n : A \times A \to A / (i, j) \mapsto (i \star j) mod_n \doteq resto(i \star j, n).$$

Assim definida, $\star$ é uma operação binária.

Demonstração. Os critérios de existência e unicidade da relação estão garantidos pelo teorema da divisão de Euclides. □

O último exemplo, como vimos não é uma operação binária. As operações binárias têm papel fundamental para o assunto que segue. Apresentamos a seguir algumas definições para uma operação binária. **Tais definições serão discutidas somente para a condição de operação binária**, pois as hipóteses de existência e unicidade evitam possíveis casos patológicos, como observaremos adiante.

Exercícios 2.2.5. *(1) Verifique se a relação de união em $S = \wp(\{1,2,3\})$, isto é, $\bigcup : S \times S \to S : (X,Y) \mapsto X \cup Y$, é uma operação binária.*

(2) Seja $S = \{1,2,3,4,5,6\}$ e $*$ uma relação em S, tal que $*(i,j) = MDC(i,j)$. Verifique se $*$ é uma operação binária.

(3) Para o conjunto anterior, a relação $* : S \times S \to S, (i,j) = MMC(i,j)$ é operação binária?

(4) Para o conjunto $\{Z, *\}$, é verdade que $*(i,j) = MDC(i,j)$ é operação binária?

(5) Construa a tabela da relação binária $* : S \times S \to S$, sendo

$$S = \{ \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}, \quad \begin{bmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{bmatrix}, \quad \begin{bmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{bmatrix} \},$$

e $*(M,N) = MN$ o produto usual de matrizes. Esta relação é uma operação binária?

(6) Mostre que a operação de Multiplicação $* : \mathbb{R} \times \mathbb{R} \to \mathbb{R}, *(x,y) = xy$, o produto usual, é uma operação binária no conjunto dos números reais, porém isso não ocorre no conjunto dos números imaginários, lembrando que $I = \{xi$, tal que, $x \in \mathbb{R}$ e $i^2 = -1\}$ é o conjunto dos números imaginários.

(7) Seja A um conjunto numérico, e uma relação binária, em que, $\triangle(a,b) = (a+b)(a-b)$, denota o produto da soma pela diferença, da maneira usual.

a) *Verifique se quando o conjunto $A = \{-1,0,1\}$, $\triangle$ é uma operação binária;*

b) *Verifique se quando o conjunto $A = \{1,-1\}$, $\triangle$ é uma operação binária;*

c) *Dê exemplo de um conjunto A que seja infinito, e $\triangle$ não seja uma operação binária, nesse caso lembre-se de dar um contra-exemplo e dizer que critério está sendo falso.*

d) *Dê exemplo de um conjunto A que seja infinito, e $\triangle$ seja uma operação binária.*

e) *Qual o menor conjunto A possível, tal que,$\triangle$ seja uma operação binária.*

(8) Prove que a operação de Adição é uma operação binária sobre os números imaginários, isto é, $+ : I \times I \to I, +(x, y) = x + y$*?*

(9) Verifique que a operação de Adição é uma operação binária no conjuntos dos números complexos. Isso também é verdade para a operação de Multiplicação? Recorde que $\mathbb{C} = \{x + yi,$ *tal que,* $x, y \in \mathbb{R}$ *e* $i^2 = -1\}$ *é o conjunto dos números complexos.*

(10) Seja C *o conjunto das funções Reais, isto é,* $f \in \mathrm{C} \Rightarrow f : \mathbb{R} \to \mathbb{R}$ *é uma função. Mostre que a operação de composição de funções é uma operação binária.*

(11) Seja C *o conjunto das funções Reais. Se* $f, g \in \mathrm{C}$*, defina* $f + g$ *como sendo uma função real, tal que* $(f + g)(x) = f(x) + g(x)$*. Mostre que* $+$ *é uma operação binária.*

(12) Seja A *um conjunto numérico, e uma relação binária, em que,* $\triangle\ (a, b) = (a + b)(a - b)$ *, denota o produto da soma pela diferença, da maneira usual.*

a) *Verifique se quando o conjunto* $A = \{-1, 0, 1\}, \triangle$ *é uma operação binária;*

b) *Verifique se quando o conjunto* $A = \{1, -1\}, \triangle$ *é uma operação binária;*

c) *Dê exemplo de um conjunto* A *que seja infinito, e* $\triangle$ *não seja uma operação binária, nesse caso lembre-se de dar um contra-exemplo e dizer que critério está sendo falso.*

d) *Dê exemplo de um conjunto* A *que seja infinito, e* $\triangle$ *seja uma operação binária.*

e) *Qual o menor conjunto* A *possível, tal que,*$\triangle$ *seja uma operação binária.*

(13) Seja A *o conjunto dos restos da divisão por* 6*, isto é,* $A = \{0, 1, 2, 3, 4, 5\}$*. Defina uma relação binária* $+ : A \times A \to A$ *, que a todo par* $(m, n) \in A \times A$*, associa* $+(m, n) = mod_6(m + n)$ *(o resto da divisão do número inteiro* $m + n$ *por* 6*). Nestas condições responda:*

a) *Os valores de* $+(3, 5)$ *e* $+(2, 4)$*.*

b) *Monte a tabela da relação e verifique se trata-se de uma operação binária.*

c) *Verifique quais propriedades para a relação* $+$ *estão satisfeitas.*

d) *Determine o elemento neutro da relação* $+$*.*

e) *Determine os invertíveis do conjunto* A*, segundo a relação* $+$ *acima definida.*

(14) Repita o exercício anterior para a operação $*$*, definida por* $*(m, n) = mod_6(m.n)$*, sendo* $m.n$ *o produto usual entre os elementos.*

(15) Seja A *o conjunto dos restos por* 5*, sem o número* 0*, isto é,* $A = \{1, 2, 3, 4\}$*. Defina uma relação binária* $* : A \times A \to A$*, que a todo par* $(m, n) \in A \times A$*, associa* $*(m, n) = mod_5(m.n)$ *(o resto da divisão do número inteiro* $m.n$ *por* 5*). Nestas condições repita os itens do exercício* 17*.*

(16) Seja x um elemento com a seguinte propriedade: $2x = 0$. Mostre que a relação binária $+ : \{-x, 0, x\} \times \{-x, 0, x\} \to \{-x, 0, x\}$é uma operação binária.

(17) Seja o conjunto $A = \{f : \{1, 2\} \to \{1, 2\}\}$,tal que$f$ é bijetora.

a) *Determine o número de elementos do conjunto A e todos seus elementos;*

b) *Se $\circ : A \times A \to A$,tal que, $\circ(f, g) = f \circ g$ é uma relação binária, em que, denota-se $(f \circ g) = f(g(x))$, a composição de funções. Prove que a relação binária é uma operação binária*

c) *Refaça o exercício para $A = \{1, 2, 3\}$, $A = \{d, i, a\}, A = \{1, 2, 3, 4\}eA = \{r, o, m, a\}$*

2.3 Operações Binárias: algumas definições

Para as definições que seguem, estamos considerando R uma operação binária em A, isto é, $R : A \times A \to A$.

Muitas das operações aritméticas em matemáticas são binárias, isto é, são executadas para pares de números. Ocorre que fazemos operações do tipo $1 + 2 + 4$, que embora não aparentem são binárias. Mentalmente executamos um tipo de associatividade entre os fatores e procedemos assim até o resultado final. Um fato importante é que o resultado não depende da seqüência da associação, isto é, $(1 + 2) + 4 = 1 + (2 + 4)$. Definimos:

Definição 2.3.1. 2.3.1 Propriedade Associativa

Seja R uma operação binária em A. Dizemos que R satisfaz a propriedade associativa se dados $a, b, c \in A, R(a, R(b, c)) = R(R(a, b), c)$. Utilizando a notação $R(a, b) = a * b$ a propriedade associativa para R será: $a * (b * c) = (a * b) * c$

Se R satisfaz a propriedade associativa não há necessidade de hierarquia diante de uma operação com mais de 2 fatores, assim, $a*b*c = a*(b*a) = (a*b)*c$. As operações binárias de adição e multiplicação em números inteiros são por definição associativas. No entanto, a operação binária de subtração em $\mathbb{Z}, -(i, j) = i - j$, não é associativa, pois $-(-(1, 2), 3) = -(1 - 2, 3) = -(-1, 3) = -1 - 3 = -4$, enquanto que $-(1, -(2, 3)) = -(1, 2 - 3) = -(1, -1) = -1 - (-1) = 0$.

Mais geralmente, as operações usuais de soma + e produto . nos conjuntos numéricos: $\mathbb{N}, \mathbb{Z}, \mathbb{Q}, \mathbb{R}$ e $\mathbb{C}$ são associativas, por definição. O seguinte resultado é bastante útil para verificação se uma dada operação binária é associativa.

Lema 2.3.2. *Seja $*$ uma operação binária associativa em A. Se $X \subseteq A$ e $*$ restrita ao conjunto X é uma operação binária, então $* : X \times X \to X$ é uma operação binária associativa.*

Demonstração. Sejam $a, b, c \in X$, e $x = a * (b * c)$, como $*$ é operação binária $y = b * c \in X$, portanto $x = a * y \in X$. Analogamente $u = a * b \in X \therefore v = u * c = (a * b) * c \in X$. Como $*$ é operação binária em A, $X \subseteq A \Rightarrow a * (b * c) = (a * b) * c$, logo $*$ é operação binária em X. □

Desse modo a operação binária do produto usual em $\{-1, 1, -i, i\}$ é associativa, pois o produto . é associativo em $\mathbb{C}$ e $A \subset \mathbb{C}$. Observe que podemos provar a associatividade para esse conjunto fazendo todas as operações possíveis em A, nesse caso deveríamos verificar $4^3 = 64$ igualdades do tipo $a(bc) = (ab)c; a, b, c \in A$.

Exemplo 2.3.3. *(1) A operação binária, do exemplo 2.2.2.5, é associativa;*

(2) Seja $\div : \{1, -1, i, -i\} \times \{1, -1, i, -i\} \to \{1, -1, i, -i\} / \div (u, v) = \frac{u}{v}$, *lembrando que se* $u, v \in \mathbb{C}$, *então* $\frac{u}{v} = u\bar{v}$, *em que* $z = a + bi \Rightarrow \bar{z} = a - bi$, *podemos construir a tábua da relação* $\div$

$\div$	1	-1	i	$-i$
1	1	-1	$-i$	i
-1	-1	1	i	$-i$
i	i	$-i$	1	-1
$-i$	$-i$	i	-1	1

e verificar que $\div$ *é uma operação binária, que é NÂO-associativa. De fato!* $1 \div i \div -i$ *não está definido, pois, de um lado,* $(1 \div i) \div -i = -i \div -i = 1$, *por outro lado* $1 \div (i \div -i) = 1 \div -1 = -1$.

(3) A hipótese, do lema anterior, sobre operação binária associativa é assencial. Considere, por exemplo, a relação binária $-$, *a subtração, em* $\mathbb{Z}$. *Vimos que* $- : \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z}$ *é NÃO-associativa. No entanto o conjunto* $\{0\} \subset \mathbb{Z}$, *e* $- : \{0\} \times \{0\} \to \{0\}$ *é uma operação binária associativa.*

(4) A operação binária $\circ : F(A) \times F(A) \to F(A)$ *de composição de funções, sendo* $F(A)$ *o conjunto de todas as funções em A, é uma operação binária associativa;*

(5) A operação binária $\cap : \wp(A) \times \wp(A) \to \wp(A), (X, Y) \mapsto X \cap Y$, *a interseção dos subgrupos de A, é associativa.*

A próxima definição trata da propriedade comutativa, que é bastante comum em aritmética.

Exercícios 2.3.4. *(1) Seja* $*$ *uma relação em* $A = \{-1, 0, 1\}$, *que a cada par* $(x, y) \in A \times A$, *associa* $*(x, y) = x.y$, *o produto usual dos elementos. Determine a tabela da relação* $*$, *verificando se é uma operação binária. Quais propriedades são verificadas para essa relação?*

(2) *Seja X um conjunto que verifica a propriedade associativa para a relação binária $*$. Mostre que para $A \subseteq X$ a relação binária $* : A \times A \to A$ é associativa.*

(3) *Seja $*$ uma relação binária em A, um conjunto com 3 elementos, isto é $|A| = 3$. Para verificar se $*$ é uma relação binária associativa, quantas operações $*$ em A devem ser efetuadas. Exemplifique com o conjunto $A = \{1, \frac{-1+i\sqrt{3}}{2}, \frac{-1-i\sqrt{3}}{2}\}$, sendo i a unidade imaginária e $*$ o produto usual dos números complexos.*

(4) *Mostre que se $|A| = n$ e $*$ é relação binária em A, para verificarmos a condição de associatividade para $*$, devemos verificar n^3 igualdades.*

(5) *Seja $+mod(18)$ uma relação binária sobre o conjunto $\{0, 1, 2, ..., 16, 17\}$. Segundo a questão anterior, quantas igualdades devem ser verificadas para garantir que a relação binária é associativa? Como podemos utilizar a propriedade da questão 2, para simplificar os cálculos, sabendo-se que o conjunto dos números inteiros é associativo com a relação binária $+$ usual?*

(6) *Seja $-mod(18)$ a relação binária que associa ao par (x, y) o resto da divisão de $x-y$ por 18. Mostre que $-mod(18)$ em $A = \{0, 1, 2, ..., 17\}$ é operação binária, mas não é associativa.*

(7) *Seja $*$ uma operação binária que é não associativa em X. Se A é subconjunto de X, podemos, como na questão 2, dizer que $*$ não é associativa em A? (sugestão: estude o caso*

$$X = M_2(Z) = \{\begin{bmatrix} m & n \\ k & l \end{bmatrix}, m, n, k, l \in Z\} \text{ e } A = \{\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, \quad \begin{bmatrix} -1 & 0 \\ 0 & -1 \end{bmatrix}\},$$

e $*$ a operação binária do produto usual de matrizes.

2.3.2 Propriedade Comutativa

Definição 2.3.5. *Seja R um operação binária em A. Dizemos que R é comutativa se*

$$\forall a, b \in A, R(a, b) = R(b, a).$$

Se R é uma operação binária comutativa sobre um conjunto A finito, $R(a_i, a_j) = R(a_j, a_i)$, o termo à esquerda da igualdade corresponde à posição interna (i, j) da tábua da operação R, enquanto que o termo à direita da igualdade corresponde à posição (j, i), da mesma tábua. Portanto, como uma matriz, a parte interna da tábua da operação R, quando comutativa, é uma matriz simétrica. Os exemplos 2.2.2.4,2.3.3.5 são de uma operação comutativa, enquanto que os exemplos 2.3.3.2, 2.3.3.4 são de operações NÃO-comutativas. Embora a verificação para

a propriedade comutativa seja mais direta que para a associativa, temos um resultado análogo ao lema anterior.

As duas propriedades seguintes, juntamente com a propriedade associativa são importantes para todo o restante desse trabalho. São as propriedades de existência do elemento neutro e do elemento inverso, definidos como segue.

Exercícios 2.3.6.

2.3.3 Elemento Neutro

Definição 2.3.7. *Seja R uma operação binária em A, tal que, $\forall a \in A$ estejam satisfeitas as seguintes condições:*

(1) Existência do neutro à direita: $\exists d \in A / R(a, d) = a$

(2) Existência do neutro à esquerda: $\exists e \in A / R(e, a) = a$

A operação R admite elemento neutro se $d = e$, isto é, existe elemento neutro à direita, existe elemento neutro à esquerda e eles são iguais.

Em geral dizemos que 1 é o elemento neutro do produto e 0 o elemento neutro da adição, embora isso não seja, necessariamente, o que ocorre sempre. Veja exemplo a seguir.

Exemplo 2.3.8. *(1) Se A é um conjunto não vazio e $G = \{f : A \to A / f$ é bijetora $\}$, a operação binária $\circ : G \times G \to G / (f, g) \mapsto f \circ g$ admite elemento neutro, que denominamos I_A a função identidade em A, isto é, $I_A(x) = x$. Nessas condições $\forall f \in G, I_A \circ f(x) = I_A(f(x))$, como $f(x) \in A$, então $I_A(f(x)) = f(x) \Rightarrow I_A \circ f = f \therefore I_A$ é neutro à esquerda; analogamente, $\forall f \in G, f \circ I_A(x) = f(I_A(x)) = f(x)$, então $f \circ I_A = f \therefore I_A$ é neutro à direita, portanto I_A é o elemento neutro. Para as funções, a operação binária $\circ$ é semelhante à operação binária $*$ do produto usual entre números, nesse caso a função identidade, em A está relacionada com o número* 1.

(2) As matrizes $M_{n \times n}$ cujas entradas são números inteiros, que também denotamos por: $M_{n \times n} = (m_{i,j})_{i,j \in \{1,2,\cdots,n\}} / m_{i,j} \in \mathbb{Z}$ são denominadas $M(n, \mathbb{Z})$ matrizes quadradas de ordem n sobre o conjunto dos números inteiros. O produto usual, $*$, entre matrizes quadradas sobre $\mathbb{Z}$ é uma operação binária:

$$* : M(n, \mathbb{Z}) \times M(n, \mathbb{Z}) \to M(n, \mathbb{Z}) / (A, B) \mapsto A * B,$$

lembrando que $A * B = C$ é uma matriz quadrada de ordem n, tal que, $C = (c_{i,j})_{i,j \in \{1,2,\cdots,n\}}$ e cada entrada $c_{i,j} = \sum_{k \in \{1,\cdots,n\}} a_{i,k}.b_{k,j}$, sendo $a_{i,j}, b_{i,j}$ as entradas das matrizes A, B, res-

pectivamente. A operação binária $*$ possui elemento neutro, denominado $I_{n\times n} = (\delta_{i,j})$, a matriz identidade, sendo $\delta_{i,j} = 1$, quando $i = j$ e $\delta_{i,j} = 0$, quando $i \neq j$, com $1 \leq i, j \leq n$.

(3) O exemplo 2.3.3.2 tem apenas elemento neutro à direita, portanto não admite elemento neutro.

Se uma dada operação binária admite elemento neutro, este é único. Dada uma operação binária R, a existência do elemento neutro é essencial para a definição a seguir. Portanto, é importante, inicialmente, o reconhecimento do elemento neutro, para então prosseguir à identificação da propriedade:

2.3.4 Invertíveis

Definição 2.3.9. *Seja R uma operação binária em A e $e \in A$ o elemento neutro, tal que, para $u \in A$ estejam satisfeitas as seguintes condições:*

(1) Existência do inverso à direita: $\exists v \in A / R(u, v) = e$

(2) Existência do inverso à esquerda: $\exists w \in A / R(w, u) = e$

Dizemos que u tem a propriedade do inverso se $w = v$, isto é, v é o inverso de u.

Exemplo 2.3.10. *(1) A operação binária do exemplo 2.3.3.2, não admite a propriedade do inverso, pois não existe elemento neutro para a operação considerada. A operação binária do exemplo 2.3.3.4, embora admita elemento neutro, não admite a propriedade do inverso, pois existem funções, como as funções constantes, que não admitem inverso;*

(2) A operação binária $+ : \mathbb{Z}\times\mathbb{Z} \to \mathbb{Z}$, satisfaz a propriedade do inverso para qualquer inteiro i, pois todo número inteiro admite elemento oposto, isto é, $-i$, tal que $i + (-i) = 0$. Observe que nesse caso o elemento inverso, para a operação binária de adição, também é conhecido por elemento oposto.

(3) A operação binária $* : \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z}$, o produto usual, satisfaz a propriedade do inverso apenas para os elementos $\{-1, 1\}$. Embora esse resultado seja intuitivo, pois qualquer outro número inteiro, $n \neq 1$, por exemplo 2, não admite elemento inverso inteiro, isto é $2 * i = 2i \neq 1 \forall i \in \mathbb{Z}$, a prova desse resultado utiliza propriedades dos números inteiros que não trataremos aqui. Para leitura sobre este assunto, sugerimos a referência [7].

(4) Seja $A = \{0, 1, 2, 3, 4, 5\}$, para a operação binária

$$+mod_6 : A \times A \to A/(i, j) \mapsto resto(i + j, 6)$$

o inverso de 0 *é* 0*; o inverso de* 1 *é* 5*. Isso pode ser reconhecido facilmente pela tábua da operação binária:*

$+mod_6$	0	1	2	3	4	5
0	0	1	2	3	4	5
1	1	2	3	4	5	0
2	2	3	4	5	0	1
3	3	4	5	0	1	2
4	4	5	0	1	2	3
5	5	0	1	2	3	4

,

sendo suficiente verificar em qual posição interna da tábua ocorre o elemento neutro, os elementos da linha e da coluna cuja imagem, da operação binária, resulta no neutro é o inverso um do outro. Por exemplo, na posição ***interna*** *da terceira linha com a quinta coluna, ocorre o neutro* 0*, que corresponde a imagem do para* $(2, 4)$*, portanto, o inverso de* 2 *é* 4*, e vice-versa: confira!*

Encerramos as definições de operação binária que utilizaremos. Para a propriedade do inverso apresentamos a seguinte afirmação:

Proposição 2.3.11. *Seja* $*$ *uma operação binária em* A*, com elemento neutro* e*. As seguintes afirmações são verdadeiras:*

(1) O elemento neutro, e*, é único ;*

(2) O elemento neutro comuta com qualquer elemento de A*;*

(3) Se o inverso de u *é* v*, isto é,* $u^{-1} = v$*, então o inverso de* v *é* u*. Ou seja* $u^{-1} = v \Leftrightarrow v^{-1} = u$*;*

(4) se o inverso de u *é* v*, então eles comutam entre si.*

Se $*$ é uma operação binária em A, denotamos $\forall a, b \in A, *(a, b)$ por ab, isto é, $*(a, b) = ab$; em particular, quando $a = b, *(a, a) = aa$, que costumamos indicar por a^2, o quadrado de a. Vamos concluir esta seção com uma propriedade bastante comum para os números inteiros: a potenciação. A definição de potência, para a operação binária, é a mesma dada aos números inteiros, guardado um certo cuidado com a notação, por isso destacamos aqui essa propriedade.

Exercícios 2.3.12. *(1) Dê exemplo de uma operação binária que não seja associativa e uma operação binária que não tenha a propriedade de existência do elemento neutro.*

(2) Seja $A = \{0, 1, 2, 3, 4, 5, 6, 7, 8\}$ *, determine os elementos invertíveis de* A*, segundo as operações de* $+$ *e* $*$*, soma e produto, módulo* 9*.*

(3) Seja C *o conjunto das funções Reais, isto é,* $f \in \mathrm{C} \Rightarrow f : R \to \mathbb{R}$ *é uma função. Mostre que a operação de composição de funções é associativa, porém não comutativa. Mostre que a unidade de ,* c *com essa operação, é a função identidade.*

(4) Seja C *o conjunto das funções Reais. Se* $f, g \in \mathrm{C}$*, defina* $f + g$ *como sendo uma função real, tal que* $(f + g)(x) = f(x) + g(x)$*. Mostre que* $+$ *é uma operação binária associativa e comutativa, com elemento neutro, e que toda função real* f*, tem um oposto igual a* $-f$*.*

(5) Seja C *o conjunto das funções Reais. Seja* $\circ : \mathrm{C}\mathcal{O}\mathrm{C}$ $rightarrow\mathrm{C}$*a operação binária de composição. Qual a condição para que* $f\mathrm{C}$ *tenha inverso à direita, inverso à esquerda e inverso?*

2.3.5 Potenciação

Definição 2.3.13. *Seja* $*$ *uma operação binária em* A *e* $e \in A$ *o elemento neutro. Se* $a \in A$ *e* n *é um número inteiro não negativo, definimos* a^n*, sendo* a *denominado base e* n *denominado expoente, como segue:*

i. $a^0 \doteq e$*;*

ii. $a^n = *(a, a^{n-1}) = a * a^{n-1}$

iii. *Se* a^{-1}*, denota o inverso de* a*, então* $a^{-n} = (a^{-1})^n$*.*

A definição de potência, portanto, é recursiva, daí definirmos potência para números não negativos. Isso não impede que calculemos potências com expoentes inteiros, quando a base é um elemento invertível. A seguinte proposição é bastante útil:

Proposição 2.3.14. *Seja* $*$ *uma operação binária em* A *e* $a, b \in A$*, tal que, são invertiveis, isto é,* $\exists a^{-1}$ *o inverso de* a*.*

i. *Se* n *é um inteiro negativo, então* $a^n = (a^{-1})^{-n}$*;*

ii. $\forall m, n \in \mathbb{Z}$*,* $a^{m+n} = *(a^m, a^n) = a^m * a^n = a^n * a^m$

iii. $\forall m, n \in \mathbb{Z}$*,* $a^{mn} = (a^m)^n = (a^n)^m$

Exemplo 2.3.15. *(1) Seja* $+$ *a operação binária de adição em* A*. Então* $a^n = a + \cdots + a$*, uma soma com n-termos, logo* $a^n = na$*;*

(2) Seja G *o conjunto das funções bijetoras sobre* $A \neq \emptyset$ *e* $\circ$ *uma operação binária em* G*. Se* $A = \{1, 2, 3, 4, 5, 6\}$*, e* $f : A \to A / f(1) = 2, f(2) = 5, f(3) = 1, f(4) = 4, f(5) = 6, f(6) = 3$*, então:* $f^2 = f \circ f$ *é a função* $f^2(1) = f(f(1)) = f(2) = 5$*; calculando-se*

termo a termo, obtemos: $f^2(2) = 6, f^2(3) = 2, f^2(4) = 4, f^2(5) = 3, f^2(6) = 1$, *a função* f^n *será a composição n-vezes da função* f. *Se calcularmos* f^5 *a função obtida será a função identidade: vamos calcular* $f^5(1) = f^3(f^2(1)) = f^3(5) = f(f^2(5)) = f(3) = 1$, *isto é,* $f^5(1) = 1$, *repetindo-se esse cálculo concluímos que* $f^5(i) = i, 1 \leq i \leq 6$, *que é a função identidade. Vejamos que ainda para esse caso podemos calcular* f^{-3}, *pois sendo* f *bijetora, ela admite função inversa, que é o inverso da função* f. *Nesse caso* f^{-1} *é uma função bijetora, que para simplificar a notação vamos chamá-la de* $g = f^{-1}$, *desse modo* $f^{-3} = g^3$. *A função g pode ser obtida a partir de sua definição, isto é,* $g \circ f = I_A \therefore g(f(i)) = i$, *assim* $g(f(1)) = 1 = g(2); g(f(2)) = 2 = g(5)$, *repetindo-se essa idéia calculamos a função g nos demais valores, isto é,* $g(1) = 3; g(3) = 6; g(4) = 4; g(6) = 5$. *Daí calculamos* $g^3 = f^{-3}$;

(3) Seja $+mod_8$ *a operação binária em* $A = \{0, \cdots, 7\}$ *o conjunto de restos da divisão de um inteiro por* 8. *A potência* $6^7 = resto(6.7, 8) = resto(42, 8) = 2$.

Exercícios 2.3.16. *(1) Seja pot a relação binária em* $\{-1, 0, 1, 2\}$, *tal que* $pot(x, y) = x^y$, *x elevado a potência y.*

a) *Determine a tabela da relação binária;*

b) *Determine a relação binária pot, como subconjunto do produto cartesiano* $\{-1, 0, 1, 2\} \times \{-1, -, 1, 2\}$;

c) *Explique se pot é uma função, provando ou dando contra-exemplo.*

(2) Seja $- : Z \times Z \to Z / -(m, n) = m - n$ *uma relação binária.*

a) *A relação binária* $-$ *é uma operação binária?*

b) *Qual o elemento neutro da relação?*

c) *Quais os invertíveis da relação?*

d) *A relação binária é associativa? É comutativa?*

(3) Seja $- : \{0, 1\} \times \{0, 1\} \to \{0, 1\} / -(m, n) = (m, n) mod 2$, *isto é, o resto da divisão por* 2. *Verifique que é uma operação binária e estude suas propriedades.*

(4) Verifique para cada item, se a relação dada é uma relação binária. Caso afirmativo, verifique se é uma operação binária, caso negativo verifique se é uma função. Lembre-se que se afirmativo, devemos provar a afirmação, se negativo devemos exibir um exemplo onde falha o critério verificado.

a) $\bigcup : \wp(\{a, b, c\}) \times \wp(\{a, b, c\}) \to \wp(\{a, b, c\}); \bigcup(A, B) = A \bigcup B$

b) $* : \{1, \frac{-1+i\sqrt{3}}{2}, \frac{-1-i\sqrt{3}}{2\}}\} \times \{1, \frac{-1+I\sqrt{3}}{2}, \frac{-1-I\sqrt{3}}{2}\} \to \{1, \frac{-1+I\sqrt{3}}{2}, \frac{-1-I\sqrt{3}}{2}\} * (u, v) = uv$, *o produto usual, sendo* $\sqrt{-1} = i$, *a unidade imaginária;*

c) $\div : \{1, 2\} \times \{1, 2\} \to \{1, 2\}; \div(x, y) = x \div y$, *a divisão usual.*

(5) *Seja* $H = \{\frac{\sqrt{2}+i\sqrt{2}}{2}, (\frac{\sqrt{2}+i\sqrt{2}}{2})^2, (\frac{\sqrt{2}+i\sqrt{2}}{2})^3, (\frac{\sqrt{2}+i\sqrt{2}}{2})^4, (\frac{\sqrt{2}+i\sqrt{2}}{2})^5, (\frac{\sqrt{2}+i\sqrt{2}}{2})^6, (\frac{\sqrt{2}+i\sqrt{2}}{2})^7, (\frac{\sqrt{2}+i\sqrt{2}}{2})^8\}$ *, o conjunto das 8 primeiras potências de* $\frac{\sqrt{2}+i\sqrt{2}}{2}$*, sendo* $i^2 = -1$*, a unidade imaginária.*

a) *A relação* $* : H \times H \to H, (x, y) \mapsto x * y$ *, sendo* $x * y$ *o produto usual, é uma operação binária?*

b) *A relação* $+ : H \times H \to H, (x, y) \mapsto x + y$ *, sendo* $x + y$ *a soma usual, é uma operação binária?*

(6) *Seja A o conjunto dos restos da divisão por* 8*, isto é,* $A = \{0, 1, 2, 3, 4, 5, 6, 7\}$*. Defina uma relação binária* $* : A \times A \to A$*, que a todo para* $(m, n) \in A \times A$*, associa* $*(mn) = mod_8(mn)$*, o resto da divisão de* mn *por* 8*. Responda:*

a) *Os valores de* $*(3, 5)$ *e* $*(6, 7)$

b) *Monte a tabela e verifique se trata de uma operação binária;*

c) *Determine, caso exista, o neutro da relação* $*$*;*

d) *Determine, caso exista, os invertíveis do conjunto A, segundo a relação* $*$*;*

e) *O conjunto* $\{A, *\}$ *é um grupo.*

(7) *Determine para cada item o domínio, o contra-domínio, a relação e a imagem da relação:*

a) $\triangle : \wp(X) \times \wp(X) \to \wp(X)$
$\triangle(A, B) = (A \cup B) - (A \cap B)$

b) $R : \{-2, -1, 0, 1, 2\} \to \{0, 4\}; R(X) = \frac{(x^2-4)}{(x^2-1)}$

c) $* : \{1, -1, i, -i\} \times \{1, -1, i, -i\} \to \{1, -1, i, -i\}$ $(x, y) \mapsto y * x$ *, o produto usual, sendo* $\sqrt{-1} = i$ *, a unidade imaginária.*

d) $|.| : \{-1, 0, 1\} \to \{1, 2, 3, 4\}$*, que associa a todo elemento do domínio o seu módulo, isto é,*$|x| = x$ *se* x *é positivo ou nulo, e* $|x| = -x$ *se* x *é negativo.*

(8) *Seja A o conjunto dos restos da divisão por 8, isto é,*$A = \{0, 1, 2, 3, 4, 5, 6, 7\}$*. Defina uma relação binária* $* : A \times A \to A$ *, que a todo par* $(m, n) \in A \times A$*, associa* $(m, n) = mod_8(m * n)$*, o resto da divisão de* $m * n$*, o produto usual, por 8. Assim definido, responda:*

a) *Os valores de* $*(2, 7)$ *,* $*(5, 5)$ *e* $*(4, 6)$

b) *Monte a tabela da relação binária;*

Determine, utilize a tabela,$^{*-1}[0]$ *, a imagem inversa de 0;*

c) *Determine os pares* (x, y) *do domínio, para o qual* $*(x, y) = 1$*.*

d) *Determine o conjunto* $^{*-1}[0] \cup^{*-1} [1]$

(9) *Determine para cada item o domínio, o contra-domínio, o conjunto que define a relação, a imagem da relação e se a relação é uma função.*

a) *Seja* $X = \{1, \{1\}\}$ *e* $\triangle : \wp(X) \times \wp(X) \to \wp(X)$, *tal que,* $\triangle(A, B) = A \cup B$;

b) $R : \{-2, -1, 0, 1, 2, \} \to \{0, 4\}; R(x) = \frac{(x^2-4)}{(x^2-1)}$

c) $* : \{1, -1, i, -i\} \times \{1, -1, i, -i\} \to \{1, -1, i, -i\}$; $(x, y) \mapsto y * x$, *o produto usual, sendo* $\sqrt{-1} := i$, *a unidade imaginária.*

d) $pot : \{-1, 0, 1\} \times \{-1, 0, 1\} \to \{-1, 0, 1\}; pot(x, y) = x^y$.

(10) Seja $*$ *a relação binária em* $\{1, 2, 3, 4, 5\}$ *que associa ao par* (x, y) *o resto da divisão de* xy, *o produto usual, por 7, isto é,* $* : \{1, ..., 5\} \times \{1, ..., 5\} \to \{1, ..., 5\}; (x, y) \mapsto mod_7(xy)$

a) *Calcule* $*(3, 4)$ *e* $*(4, 4)$;

b) *Determine a tabela da operação binária;*

c) *Determine* $*^{-1}[5]$;

d) *É verdade que* $*(3, *(5, 6))$ *e* $*(*(3, 5), 6)$ *são iguais?*

(11) Seja $X : \{f : \{a, i, , p\} \to \{a, i, p\} / f$ *é bijetora*$\}$ *o conjunto das funções bijetoras sobre o conjunto* $\{a, i, p\}$.

a) *Determine o conjunto* X, *isto é, as funções sobre* $\{a, i, p\}$ *bijetoras;*

b) *Seja a relação binária*

$$\circ : X \times X \to X$$

$$\circ : (f, g) = f \circ g$$

de composição de funções, sendo $f \circ g(x) = f(g(x))$. *Determine a tábua da operação binária;*

c) *Se* $u, v \in X$, *é verdade que* $\circ(u, v) = \circ(v, u)$?

(12) Seja o conjunto $A = \{f : \{1, 2, 3\} \to \{1, 2, 3\},$ *tal que f é bijetora*$\}$.

a) *Determine o número de elementos do conjunto A*

b) *Determine todos os elementos do conjunto A*

c) *Se é uma relação binária, tal que,* $g \circ f(x) = g(f(x))$, *a composição de funções,prove que a relação binária é uma operação binária;*

d) *Monte a tabela da operação binária, determinando o elemento neutro, os invertíveis e se a operação binária é comutativa.*

(13) Determine para cada item o domínio, o contra-domínio, o conjunto que define a relação, a imagem da relação e se a relação é uma função.

a) *Seja* $X = \{1, \{1\}\}$ *Lembrando que* $X \backslash Y = \{x,$ *tal que,*$(x \in X) e (x \notin Y)\}$, *a relação* $\triangle : \wp(X) \times \wp(X) \to \wp(X)$, *em que* $\triangle(A, B) = (A \cup B) \backslash (A \cap B)$

b) $R : \{-2,-1,0,1,2,\} \to \{-1,0,4\}; R(x) = \frac{(x^2-4)}{(x^2-1)}$

c) $\div : \{1,-1,i,-i\} \times \{1,-1,i,-i\} \to \{1,-1,i,-i\}$; $(x,y) \mapsto \frac{x}{y}$, *a divisão usual, sendo* $i = \sqrt{-1}$, *a unidade imaginária.*

d) $pot : \{-1,1,2\} \times \{-1,1,2\} \to \{-1,1,2\}; pot(x,y) = x^y$.

2.4 Grupos

Estamos em condições de apresentar uma definição central para a teoria de grupos.

Definição 2.4.1. *Seja G um conjunto não vazio e $*$ um operação binária em G. O conjunto $\{G,*\}$ é denominado Grupo, se as seguintes condições são verificadas:*

i. *A operação binária $*$ é associativa;*

ii. *Existe elemento neutro;*

iii. *Todo elemento de G tem inverso, segundo a operação binária $*$. Nesse caso dizemos que G satisfaz a propriedade do inverso.*

Lembrando as propriedades que o grupo satisfaz, $*$ é associativa se $a*(b*c) = (a*b)*c$; existe elemento neutro se $\exists! e \in G / \forall g \in G, e*g = g*e = g$; G satisfaz a propriedade do inverso se $\forall g \in G, \exists h \in G / gh = hg = e$, nesse caso denotamos h, o inverso de g por g^{-1}.

Para os grupos finitos, a tábua da operação binária permite a verificação das duas últimas propriedades de grupo. A associatividade, quando não conhecemos a operação binária, deve ser provada abstratamente, ou elemento a elemento, como discutido na seção anterior. A seguir apresentamos exemplos de grupos, utilizando, para o caso finito, a tábua da operação binária.

Exemplo 2.4.2. *(1) Seja $G = \{-1,1\}$ e $* : G \times G \to G / (i,j) \mapsto ij$, o produto usual. O conjunto $\{G,*\}$ é um grupo. Segundo a tábua da relação binária:*

$*$	-1	1
-1	1	-1
1	-1	1

Verificamos que $*$ é uma operação binária; 1 é o elemento neutro; -1 é o inverso de -1, portanto G satisfaz a propriedade do inverso (PI). A propriedade associativa pode ser verificada diretamente, verificando 8 igualdades, ou utilizando o resultado do lema 2.3.2, isto é, o produto é associativo em $\mathbb{Z}$ e $G \subset \mathbb{Z}$. Logo $\{G,*\}$ é um grupo;

(2) Seja $G = \{-1,1\}$ e $+ : G \times G \to G / (i,j) \mapsto i+j$, a soma usual. O conjunto $\{G,+\}$ não é um grupo, pois $+(1,1) = 2 \notin G$, portanto $+$ não é operação binária em G, então $\{G,+\}$ não é um grupo;

(3) Seja $G = \{1, -1, i, -i\}$, *em que* $i = \sqrt{-1} \in \mathbb{C}$ *é a unidade imaginária, e* $* : G \times G \to G/(g,h) \mapsto gh$, *o produto usual. O conjunto* $\{G, *\}$ *é um grupo. Segundo a tábua da relação binária:*

$*$	1	-1	i	$-i$
1	1	-1	$-i$	i
-1	-1	1	$-i$	i
i	i	$-i$	-1	1
$-i$	$-i$	i	1	-1

.

Verificamos que $*$ *é uma operação binária;* 1 *é o elemento neutro; o inverso de* -1 *é* -1*; o inverso de* i *é* $-i$ *, portanto* G *satisfaz a propriedade do inverso (PI). A propriedade associativa, se verificada diretamente, exige o cálculo de* $4^3 = 64$ *igualdades!. Nesse caso, utilizamos o lema 2.3.2, isto é o produto é associativo em* $\mathbb{C}$ *e* $G \subset \mathbb{C}$. *Logo* $\{G, *\}$ *é um grupo;*

(4) Seja o conjunto $\mathbb{Z}$ *e* $+ : \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z}/(i,j) \mapsto i+j$. *O conjunto* $\{\mathbb{Z}, +\}$ *é um grupo. De fato,* $+$ *é operação binária em* $\mathbb{Z}$, *pois a soma de dois numeros inteiros é um número inteiro;* $+$ *em* $\mathbb{Z}$ *é associativa;* 0 *é o elemento neutro da adição; todo número inteiro* n *admite inverso, que é* $-n$, *o oposto. Portanto* $\{\mathbb{Z}, +\}$ *é um grupo, neste caso um grupo infinito, pois* $|Z|$ *é um conjunto infinito.*

(5) Seja $\mathbb{Q}^*$ *o conjunto dos números racionais e* $* : \mathbb{Q}^* \times \mathbb{Q}^* \to \mathbb{Q}^*/(\frac{p}{q}, \frac{u}{v}) \mapsto \frac{pu}{qu}$. *O conjunto* $\{\mathbb{Q}^*, *\}$ *é um grupo. Como no caso anterior, trata-se de um conjunto infinito, sem possibilidade de construção de tábua. Temos que utilizar as propriedades do conjunto dos números naturais: A relação binária é operação binária; o produto é associativo, o elemento neutro é a classe de equivalência do* 1, *isto é,* $\bar{1}$ *a classe de números do tipo* $\frac{p}{p}/p \in \mathbb{Z}^*$; *e para o inverso, tomando-se um elemento qualquer de* $\mathbb{Q}$, *por exemplo* $\overline{\frac{p}{q}}$ *a classe dos números* $\frac{kp}{kq}$ *com* $p, q, k \in \mathbb{Z}^*$, *o inverso dessa classe é a classe* $\overline{\frac{q}{p}}$. *Portanto* $\{\mathbb{Q}^*, *\}$ *é um grupo.*

(6) Seja A *um grupo finito e* $\Delta : \wp(A) \times \wp(A) \to \wp(A)$ *a operação binária* $\Delta(X,Y) = (X \cup Y) \setminus (X \cap Y)$, *denominada diferença simétrica. O conjunto* $\{\wp(A), \Delta\}$ *é um grupo.*

O próximo capítulo apresenta uma introdução à teoria de grupos, destacando algumas propriedades e definições, e apresentando exemplos de grupos que verifiquem tais propriedades e definições. O caráter introdutório do capítulo pode deixá-lo repetitivo em alguns conceitos e reduzido, ou mesmo incompleto, em algumas definições. Muitos termos técnicos da teoria, como Ação de Grupos ou Representações não serão mencionados a partir daqui. Algumas idéias, originadas numa teoria mais generalizada, serão simplificadas para podermos apresentar alguns resultados, compreendermos os exemplos e obter algumas conclusões, ou seja, fazermos algumas "contas".

Exercícios 2.4.3. *(1) Prove que o conjunto* $\{-1, 1, -i, i\}$ *é um grupo multiplicativo, com a operação binária* $*$*, o produto usual em* C*.*

(2) Sejam os conjunto A*,* B *e as operações definidas abaixo* $A = \{-1, 1, -i, i\}$ $* : A \times A \to A$ $(x, y) \mapsto xy$ $B = \{(-1, -1), (-1, 1), (1, -1), (1, 1)\}$ $\otimes : B \times B \to B$ $(u, v) \mapsto (u_1v_1, u_2v_2)$ *Mostre que os conjunto* $\{A*\}$,$\{B, \otimes\}$ *, são grupos, utilizando o fato que as operações são associativas;*

(3) Seja $\{G, *\}$ *um grupo.*

a) *Prove que o elemento neutro de* G *é único;*

b) *Se* $u, v \in G$ *e* v *é o inverso de* u*, isto é,* $u = v^{\{-1\}}$ *, mostre que* u *e* v *comutam;*

(4) Mostre que o conjunto dos números inteiros é um grupo aditivo, isto é, $\{Z, +\}$ *é um grupo.*

(5) Mostre que o conjuntos dos números racionais é um grupo aditivo, porém não é um grupo multiplicativo.

(6) Mostre que o conjunto dos números racionais sem o elemento 0*,* Q^**, é um grupo multiplicativo.*

(7) Prove que o conjunto dos números reais é um grupo aditivo.

(8) Prove que o conjunto dos números imaginários sem o 0*, não é um grupo multiplicativo.*

(9) Prove que o conjunto dos números complexos sem o 0*,* C^**, é um grupo multiplicativo.*

(10) Seja a operação binária $+$ *em* $\mathbb{Z}$*. Determine a unidade; para* $z \in \mathbb{Z}$*, determine o oposto de* z*.*

(11) Mostre que $\{\mathbb{Z}, +\}$ *é um grupo, porém* $\{Z, *\}$*, sendo a operação de multiplicação, não é um grupo.*

(12) Seja $2Z = \{2z/z \in \mathbb{Z}\}$ *isto é, o conjunto dos números pares. Mostre que* $\{2\mathbb{Z}, +\}$ *é um grupo infinito.*

(13) Seja $X = \{1, 2, 3\}$*, consideremos as seguintes funções bijetoras sobre* X*:* $e, f, g, u, w : X$ $rightarrow X$ *definidas abaixo:* $e(1) = 1, e(2) = 2, e(3) = 3; f(1) = 2, f(2) = 3, f(3) = 1; g(1) = 3, g(2) = 1, g(3) = 2;$ $u(1) = 2, u(2) = 1, u(3) = 3;$ $v(1) = 3, v(2) = 2, v(3) = 2; w(1) = 1, w(2) = 3, w(3) = 2$*. Responda os itens a seguir:*

a) *Seja* $S_3 = \{e, f, g, u, v, w\}$ *e* $\circ$ *a operação binária de composição de funções em* S_3*. Mostre que* $\{S_3, \circ\}$ *é um grupo finito.*

b) *Estude o grupo* S_3*, calculando a tábua da operação do grupo. Identifique a identidade do grupo.*

c) *O grupo S_3 satisfaz a propriedade comutativa?*

(14) Prove que o conjunto $2Z = \{n \in \mathbb{Z}/n$ é par $\}$ é um grupo infinito. Isso é verdade para p conjunto dos números ímpares?

(15) Seja $G = \{f, g, u\}$ um subconjunto do conjunto das funções bijetoras sobre $\{1, 2, 3, 4, 5, 6\}$. Determine a tábua do grupo $\{G, \circ\}$, cuja operação binária é a composição de funções, isto é $f \circ g(x) = f(g(x))$, sendo:$f(1) = 1, f(2) = 3, f(3) = 5, f(4) = 4, f(5) = 2, f(6) = 6; g(1) = 1, g(2) = 2, g(3) = 3, g(4) = 4, g(5) = 5, g(6) = 6; u(1) = 1, u(2) = 5, u(3) = 2, u(4) = 4, g(5) = 3, u(6) = 6$.

(16) Seja $*$ a relação binária sobre $A = \{0, 1, ..., 10, 11\}$ que associa a cada par (m, n) o resto do produto usual mn por 12. Determine as propriedades da relação binária: associatividade, comutatividade, elemento neutro e invertíveis. Explique se o conjunto $\{A, *\}$ é um grupo, justifique sua resposta.

(17) Seja $G = \{1, 3, 5, 9, 11, 13\}$ e $*mod_{14} : G \times G \to G$ a relação binária que associa ao par $(x, y) \mapsto mod_{14}xy$, o resto da divisão por 14 do produto usual xy.

a) *Mostre que $*mod_{14}$ é uma operação binária;*

b) *Prove que $\{G, *mod_1 4\}$ é um grupo, utilizando o fato que $*mod_1 4$ satisfaz a propriedade associativa em Z.*

(18) Seja x um elemento com a seguinte propriedade: $2x = 0$. Mostre que a relação binária $+ : \{-x, 0, x\} \times \{-x, 0, x\} \to \{-x, 0, x\}$é uma operação binária, mas o conjunto $A = \{-x, 0, x\}$ e a operação binária $+$, isto é $A, +$, não definem um grupo.

Capítulo 3

Introdução à Teoria de Grupos

No capítulo II apresentamos a definição de grupo, isto é um conjunto G associado a uma operação binária $*$ que satisfazem 3 condições: associatividade para a operação *; a existência de elemento neutro e a propriedade do inverso. Nessas condições o conjunto $\{G, *\}$ é denominado grupo. Quando não houver necessidade, referimos ao grupo apenas pelo conjunto G, e dizemos que G é um grupo.

A teoria de grupos foi tratada de modo puramente abstrato, a partir dos trabalhos de Galois sobre a solução das equações polinomiais por meio de radicais ...

Neste capítulo apresentamos algumas noções básicas de grupos. A teoria de grupos é uma área da Matemática, com muitos resultados importantes e questões em aberto. Como é comum em matemática, a teoria de grupos aparece naturalmente em Geometria, Topologia, Análise, Lógica e Fundamentos. Suas aplicações são também comuns, nas ciências em geral. Vamos discutir os grupos, de um ponto de vista abstrato. Iniciamos essa abordagem abstrata, estudando inicialmente alguns grupos finitos. No capítulo anterior finalizamos com exemplos de vários grupos, neste capítulo vamos começar construindo alguns grupos finitos.

3.1 Subgrupos e Subgrupos Cíclicos:Preliminares

Dado um grupo $\{G, *\}$, quando não houver ambigüidades, podemos refirmo-nos a este grupo, apenas pelo seu conjunto G, e denotar a condição $a * b$ simplesmente por ab. Assim como em teoria dos conjuntos, dado um conjunto C definimos os subconjuntos deste, para os grupos existe um análogo a essa definição.

Definição 3.1.1. *Seja $\{G, *\}$ um grupo, definimos como subgrupo de G, o subconjunto $H \subseteq G$, tal que, o conjunto $\{H, *\}$ seja um grupo, o qual denotamos por $H \leq G$ (Lê-se: H é subgrupo*

de G). Se $e \in G$ é o elemento neutro, os conjuntos $\{e\}$ e G, que são subgrupos de G, são denominados, respectivamente, de ***subgrupo trivial*** *e* ***subgrupo impróprio*** *de G. Os subgrupos não trivial ou impróprio de G são denominados* ***subgrupos próprios****.*

Uma conseqüência imediata da definição de subgrupo, é que se G é um grupo, o conjunto de subgrupos de G é não vazio, pois G admite os subgrupos não próprios. Oportunamente, estudaremos os grupos cujos únicos subgrupos sâo $\{e\}$ e G, mas para isso precisamos de mais teoria.

Os subgrupos de um grupo auxiliam no estudo do grupo, permitindo obter propriedades do grupo, a partir destes, embora isso não seja verdade em geral.

Para o caso de grupos finitos, uma forma rápida de verificar se um certo subconjunto de um grupo G é um subgrupo, é através da tábua da operação binária do grupo. A seguir citamos alguns exemplos de subgrupo.

Exemplo 3.1.2. *(1) Se G é um grupo com elemento neutro e, então G e $\{e\}$ são subgrupos de G.*

(2) Para o grupo aditivo dos números inteiros, $\{\mathbb{Z}, +\}$, o conjunto $\{0\}$ é o subgrupo trivial de $\mathbb{Z}$; o conjunto dos múltiplos de $n \in \mathbb{Z}^*$: $n\mathbb{Z} \doteq \{n(i)/i \in \mathbb{Z}\}$ é um subgrupo próprio de $\mathbb{Z}$;

(3) Seja $G = \{1, -1, i, -1\}, i \in \mathbb{C}$, o grupo multiplicativo $\{G, *\}$, sendo $*$ o produto usual em $\mathbb{C}$; o conjunto $H = \{1, -1\}$ com a operação de G, definine o subgrupo próprio $\{H, *\}$ do grupo G, indicado por $H < G$. No entanto, o conjunto $X = \{i, -i\}$ não é um subgrupo de G: por não ser um grupo multiplicativo, pois a operação binária $*$ em G, restrita ao conjunto X, não é operação binária, uma vez que $i(-i) = 1 \notin X$.

Para os grupos finitos, um recurso que auxilia na identificação de um subgrupo, nessa fase introdutória, é a construção da tábua para o conjunto considerado. Como mostrado a seguir para o último exemplo acima:

conjunto $\{1, -1\}$:

$*$	1	-1
1	1	-1
-1	-1	1

conjunto $\{i, -i\}$:

$*$	i	$-i$
i	-1	1
$-i$	1	-1

A primeira tábua é de uma grupo, a segunda não é tábua de uma operação binária, portanto $\{i, -i\}$ não é um grupo segundo o produto usual.

Uma característica da teoria de grupos é o fato de podermos definir propriedades para certos grupos, e a partir delas verificar quais grupos, ou condições destes, satisfazem tais propriedades.

Seja $\{G, *\}$ um grupo e $g \in G$. Sendo $*$ uma operação binária em G, as potências de g, segundo a definição 2.3.13, são elementos de G, isto é, $g^n \in G, \forall n \in \mathbb{Z}$. Então o conjunto

$\{g^n/n \in Z\}$ é um subconjunto de G. Se o grupo G é finito, então este conjunto, necessariamente, é finito. Portanto, a partir de um certo expoente de g, as potências $g^n, n \in \mathbb{Z}$ devem repetir-se. Pela definição 2.3.13, $g^0 = e$, daí podemos concluir que e o neutro de G, também é alguma potência de g. A seguinte proposição mostra que este conjunto é um subgrupo de G.

Proposição 3.1.3. *Seja $\{G, *\}$ um grupo finito e $g \in G$. O conjunto $H = \{g^n/n \in \mathbb{Z}\}$ é um subgrupo de G.*

Demonstração. Devemos provar que o conjunto $\{H, *\}$ é um grupo. Sendo $*$ a operação binária de G, então $\forall i, j \in \mathbb{Z}, g^i * g^j = g^{i+j} = g^n \in H$, logo $*$ é operação binária de H. Por definição $g^0 = e$, portanto H contém o neutro; $\forall g^n \in H, \exists g^{-n} \in H / g^n * g^{-n} = g^{-n} * g^n = e$, portanto H satisfaz a propriedade do inverso. A operação binária é associativa, pois $x, y, z \in H, \exists i, j, k \in \mathbb{Z} / x = g^i; y = g^j; z = g^k$, $x*(y*z) = g^i*(g^j*g^k) = g^i*g^{j+k} = g^{i+(j+k)} = g^{(i+j)+k} = (g^i * g^j) * g^k = (x * y) * z$: aqui utilizamos a propriedade que $\mathbb{Z}$ é associativo. Assim o conjunto H é um grupo, portanto $H \leq G$. □

Este resultado motiva a seguinte definição.

Definição 3.1.4. *Seja G um grupo e $g \in G$. O conjunto $\{g^n/n \in \mathbb{Z}\}$ é denominado subgrupo cíclico de G, gerado por g, que denotamos por $< g >$. Se $| < g > | < \infty$, definimos ordem de g como sendo o natural $| < g > |$, que denotamos por $o(g)$. Se $| < g > |$ é infinito, a ordem de g é infinita, isto é, $o(g) = \infty$.*

A definição de ordem de um elemento permite melhor compreender o significado de grupo cíclico. O seguinte resultado elucida o significado do conceito *ordem de um elemento.*

Proposição 3.1.5. *Seja G um grupo, tal que, $g \in G$ é um elemento de ordem finita. Se $g^n = e$, para algum inteiro n, então $o(g)|n$.*

Demonstração. Inicialmente, observamos que $o(g) = o(g^{-1})$, pois os conjuntos $< g > = < g^{-1} >$. Assim é suficiente provar para $n \in \mathbb{Z}^+$. Seja $o(g) = m$, pelo teorema da divisão, $n = qm + r, 0 \leq r < m$, das condições $g^m = e$, pois m é a ordem de g, e $g^n = e$, a hipótese: $e = g^n = g^{qm+r} = (g^m)^q g^r = g^r$, mas $e = g^r$, somente se $r = 0$, pois o conjunto $< g >$, das potências de g, tem m elementos e portanto as potências $g^r, 0 \leq r < m$ devem ser distintas. Uma vez que $g^0 \doteq e \Rightarrow r = 0$, logo $n = qm \therefore m|n$. □

Corolário 3.1.6. *Seja G um grupo com elemento neutro e. Se $g \in G$ é um elemento de ordem finita, então $o(g)$ é o menor inteiro positivo, tal que $g^{o(g)} = e$.*

Demonstração. Seja $n \in \mathbb{Z}^+$, tal que $g^n = e$, pela proposição anterior, $o(g)|n$, portanto $o(g) \leq n$, por força da divisibilidade. □

A idéia que utilizamos na proposição 3.1.5, para concluir que $r = 0$ é um recurso muito comum. Sugerimos que o leitor verifique detalhadamente este fato. A referência [7], seção 2.1 do capítulo Divisibilidade, elucida estas idéias.

Definição 3.1.7. *Seja G um grupo, tal que, $\exists g \in G$ e $G = \{g^n / n \in \mathbb{Z}\}$, então G é denominado Grupo Cíclico e g o gerador do grupo cíclico. Nestas condições denotamos $G =< g >$ o grupo cíclico gerado por g.*

Exemplo 3.1.8. *(1) Se $G = \{e\}$ é um grupo e $e \in G$ é o elemento neutro, $G =< e >$*

(2) Seja G o conjunto unitário $G = \{1\}$ e $*$ a operação de produto usual, $G =< 1 >$ Se $G = \{-1, 1\}$ é um grupo multiplicativo com dois elementos, $-1 \neq 1$, sendo $(-1)^2 = (-1)(-1) = 1$ então 1 é o neutro de G, portanto $o(-1) = 2$. Isto é, -1 é um elemento de ordem $2 \therefore G =< -1 >$;

(3) Seja $G = \{1, \frac{-1+i\sqrt{3}}{2}, \frac{-1-i\sqrt{3}}{2}\}$, em que i é a unidade imaginária. Sendo G um grupo multiplicativo, $(\frac{-1+i\sqrt{3}}{2})^2 = \frac{-1+i\sqrt{3}}{2}.\frac{-1+i\sqrt{3}}{2} = \frac{-1-i\sqrt{3}}{2} \neq 1$, portanto $o(\frac{-1+i\sqrt{3}}{2})$ não é 2. Calculando potência

$$(\frac{-1+i\sqrt{3}}{2})^3 = (\frac{-1+i\sqrt{3}}{2}).(\frac{-1+i\sqrt{3}}{2})^2 = (\frac{-1+i\sqrt{3}}{2})(\frac{-1-i\sqrt{3}}{2}) = 1 \therefore o(\frac{-1+i\sqrt{3}}{2}) = 3.$$

Analogamente, $o(\frac{-1-i\sqrt{3}}{2}) = 3$, uma possibilidade é $\therefore G =< \frac{-1+i\sqrt{3}}{2} >$

(4) Seja $G = \{0, 1, 2, 3\}$ e $* = +mod_4$ a operação de G, de modo que 0 é o elemento neutro, $2^2 = 4mod_4 = 0$, portanto $o(2) = 2$; $3^2 = 6mod_4 = 2; 3^3 = 3 * 3^2 = 3 * 2 = 5mod_4 = 1; 3^4 = 3 * 3^3 = 3 * 1 = 4mod_4 = 0$, portanto $o(3) = 4$. Analogamente, $o(1) = 4 \therefore G =< 1 >$;

(5) Seja $\mathbb{Z}$ o grupo aditivo dos números inteiros, 0 é o elemento neutro de $\mathbb{Z}$. Como vimos, $i^n = i + \cdots + i$, a soma de i n-vezes, logo $1^n = n, \forall n \in \mathbb{N}$, portanto $1^n = n \neq 0$, para todo inteiro positivo, portanto $1 \in \mathbb{Z}$ tem ordem infinita: $o(1) = \infty \therefore \mathbb{Z} =< 1 >$. Um argumento, análogo a este, mostra que $o(i) = \infty, \forall i \in \mathbb{Z} \setminus \{0\}$.

Exercícios 3.1.9. *(1) Sejam os conjunto A, B e as operações definidas abaixo $A = \{-1, 1, -i, i\}$*
$* : A \times A \to A$
$(x, y) \mapsto xy$ $B = \{(-1, -1), (-1, 1), (1, -1), (1, 1)\}$ $\otimes : B \times B \to B$
$(u, v) \mapsto (u_1v_1, u_2v_2)$

a) *Mostre que os conjunto $\{A*\}$,$\{B, \otimes\}$, são grupos, utilizando o fato que as operações são associativas;*

b) *Calcule a ordem de cada elemento;*

c) *Explique a estrutura de cada grupo: se é abeliano; se é cíclico; a ordem dos elementos, quantos subgrupos possui, entre outros.*

(2) Prove que se G é um grupo finito e $g \in G$, então $(g)^{|G|} = e$, a identidade de G, utilizando os seguintes fatos:

* $\forall g \in G, o(g) = K, 1 \leq K \leq |G|$;
* *Se $o(g) = k$, então $|G|$ é múltiplo de k.*

A seguir, apresentamos a construção de alguns grupos finitos. Observamos que a *construção* de um grupo finito, seja de 4 elementos, não significa um exemplo de um grupo de 4 elementos, porém qualquer grupo de 4 elementos. Como analogia, podemos pensar num exemplo de uma figura geométrica, um triângulo, que é diferente da construção do triângulo, possível, entre outras formas, a partir de seus três lados, quando estes satisfazem a desigualdade triangular. Ainda, utilizando a idéia geométrica do triângulo, sabemos que dados os ângulos internos do triângulo, podemos construir infinitos triângulos semelhantes, de tamanhos distintos ou não. Por exemplo o triângulo eqüilátero, existem infinitos triângulos eqüiláteros, porém são todos semelhantes. Para os grupos, utilizamos o termo isomorfos, em situações análogas a esta. A noção de isomorfismo é intrinseca à idéia de grupo, aparecendo constantemente a medida que avançamos com a teoria.

3.2 Grupos Finitos de Ordem $1, 2, 3$ e 4

Vamos tratar dos primeiros grupos finitos, lembrando que um grupo $\{G, *\}$, pode ser representado por G, de modo que, como conjunto, denominamos $|G|$ (leia-se ordem de G), como o tamanho do grupo, isto é, o número de elementos de G. Assim, inicialmente, vamos construir os grupos G de ordem: $1, 2, 3$ e 4. Para tal construção vamos fazer uso da tábua da operação de G. Obviamente, como estamos construindo grupos $\{G, *\}$, devemos satisfazer as propriedades da definição 2.4.1. Para tanto vamos provar o seguinte resultado, que auxilia na construção da tábua da operação binária $*$.

Teorema 3.2.1. *Seja $\{G, *\}$ um grupo de ordem n e T a matriz que representa a tabela interna da tábua da operação $*$, como apresentada na seção 2.1. Então o conjunto formado pelos elementos de cada linha **ou** cada coluna da matriz T deve ser igual a G*

Demonstração. Inicialmente ordenamos os elementos de $G = \{g_1, g_2, \cdots, g_n\}$. Seja H o conjunto formado pelas entradas da linha k da tabela T, isto é, $H = \{t_{k,i}/1 \leq i \leq n\}$, Sendo $*$ uma operação binária, então $H \subset G$. Basta provar que $G \subset H$. Suponha, por absurdo, $G \nsubseteq H$, então $|H| < n$, logo a linha k tem pelo menos um elemento repetido, isto é, duas entradas são iguais, logo $\exists m, n, 1 \leq m, n \leq n$, tal que $t_{k,m} = t_{k,n}$, estas entradas são o resultado da operação binária $*$, sobre os pares de elementos de G, em que, $t_{k,m} = g_k * g_m$ e $t_{k,n} = g_k * g_n$, portanto $g_k * g_m = g_k * g_n$. Como G é um grupo, existe o inverso do elemento $g_k = u$, multiplicamos a equação anterior à esquerda por u, isto é, $u * (g_k * g_m) = u * (g_k * g_n)$, sendo G um grupo, vale

a propriedade associativa, portanto $(u * g_k) * g_m = (u * g_k) * g_n$, sendo $u * g_k = e$, o elemento neutro, conluímos que $g_m = g_n$ e portanto, pelo $A2$, o grupo G tem **menos** de n elementos, um absurdo! Logo $G = H$. □

Corolário 3.2.2. *Nas condições do teorema, cada linha e cada coluna internas da tábua da operação $*$ não admite entradas repetidas.*

Nesta seção, em que construímos os grupos de ordem de 1 a 4, também introduzimos uma idéia central em Álgebra Abstrata, ligada as propriedades da operação binária, e portanto aos elementos do grupo. Em geral, estas propriedades são chamadas de propriedades estruturais, elas estão relacionadas à forma, ou estrutura, interna do grupo. Podemos citar, como propriedades estruturais, algumas definições apresentadas no capítulo anterior, como: $|G|$ a *ordem do grupo* e a *comutatividade*, também denominada *abeliana*. Outra propriedade estrutural é *ordem de um elemento*. As propriedades estruturais caracterizam completamente um grupo, isto é, elas definem com exatidão o grupo que as satisfaz e permite que possamos comparar os grupos entre si. Os grupos que apresentam as mesmas propriedades estruturais são denominados *GRUPOS ISOMORFOS*, isomorfo é uma palavra de origem grega que significa forma idêntica.

A teoria de grupos, entre outras coisas, desenvolve essa idéia de isomorfismo, de modo a conceituá-la precisamente. A partir daí, quando estudamos algum *problema* relativo aos grupos e determinamos um grupo que satisfaz às condições do problema, é comum referir-se a este grupo, como o grupo que resolve o *problema, a menos de isomorfismo*. Segundo a proposta dessa seção, portanto, vamos determinar os grupos de ordem 1 a 4, a menos de isomorfismos. Como dissemos, essa idéia será repetidamente usada e, vamos caminhar no sentido de torná-la mais precisa.

O último exemplo mostra um grupo com elementos de ordem infinita. Se G é um grupo finito, no entanto, qualquer elemento de G tem ordem finita, mais que isso, se $g \in G$, então $o(g) \leq |G|$. Isto decorre da propriedade da operação binária de G, pois o conjunto de todas as potências de g, até que ocorra o neutro, pode ter no máximo $|G|$ elementos. Se este conjunto tem exatamente $|G|$ elementos, é porque o neutro ocorreu exatamente para a última potência possível, que é $|G|$, portanto $g^{|G|} = e$, logo $o(g) = |G|$, se o conjunto tem menos de $|G|$ elementos, então para algum $n < |G|$, ocorreu que $g^n = e$ pela primeira vez, portanto $o(g) = n < |G|$. Daí todos os elementos têm ordem no máximo igual a $|G|$.

Veremos que o conceito de ordem de um elemento está diretamente ligado à ordem do grupo que contém este elemento.

Estamos em condições de determinar os grupos de ordem entre 1 e 3, a menos de isomorfismo. Para o que segue, podemos dizer que dois grupos são isomorfos se as tábuas de suas operações coincidem, pelo menos uma vez.

Proposição 3.2.3. *Seja $\{G, *\}$ um grupo finito. Existe, a menos de isomorfismo, exatamente um grupo, para $|G| \in \{1, 2, 3\}$*

Demonstração. (1) Se $|G| = 1$, como conjunto, G é unitário $\therefore G = \{g\}$. Sendo $*$ uma operação binária $g * g = g$. Sendo G um grupo, existe o elemento neutro, logo $g = e$. Portanto o único elemento de G é o neutro, que portanto é igual a seu inverso. A associatividade resulta também do fato de existir um único elemento. Daí, a menos de isomorfismo, existe um único grupo com 1 elemento, formado pelo neutro da operação binária do grupo.

(2) Se $|G| = 2 \Rightarrow G = \{g, h\}, g \neq h$. Pela existência do neutro, $e \in G$, portanto ou $g = e$ ou $h = e$. Seja $g = e$; $G = \{e, h\}$; $*$ é uma operação binária, portanto $h * h \in \{e, h\}$, se fizermos a tábua da operação binária $*$, pelo teorema 3.2.1, $h * h \neq h$, portanto $h * h = e$, nesse caso $o(h) = 2$. Assim G tem 2 elementos: um neutro e um elemento de ordem 2. Devemos provar, ainda, que ocorre a propriedade associativa: $a * (b * c) = (a * b) * c$? Uma vez que há somente 2 elementos, ou ocorre que $a = b$ ou $b = c$; se $a = b$, então $a * b = e$ logo $(a * b) * c = c$; ou $a = b = e$ então $a * (b * c) = c = a * (b * c)$, ou $a = b = h$ então $a * (b * c) = h * (h * c)$; ou $c = h \Rightarrow a * (b * c) = h \therefore a * (b * c) = c = (a * b) * c$, ou $c = e \Rightarrow a*(b*c) = h*(h*e) = h^2 = e = c = (a*b)*c$, portanto verifica a associatividade, logo é um grupo. Se trocarmos a escolha anterior para $h = e$, o mesmo aconteceria: o grupo teria um elemento neutro e um elemento de ordem 2. Portanto seria o mesmo grupo, a menos de isomorfismo.

(3) Se $|G| = 3$, como nos casos anteriores, segundo a propriedade do inverso,$e \in G$ o elemento neutro $\therefore G = \{e, a, b\}$ e devemos determinar, portanto, os outros 2 elementos de G. Podemos calcular a tábua da operação $*$, que pela propriedade do neutro determina a primeira linha e a primeira coluna, internas, da tábua:

$*$	e	a	b
e	e	a	b
a	a	x	y
b	b	z	w

$\Rightarrow$

$*$	e	a	b
e	e	a	b
a	a	b	e
b	b	e	a

Pelo teorema 3.2.1, $x \in \{e, b\}$, pois basta observar que tanto a linha, quanto a coluna, onde está x, também aparece a, como linha e coluna (internas!) não podem repetir elementos, os valores de x são somente aqueles. Se $x = e$, por um lado (o teorema 3.2.1), implica que $y = b$. Por outro lado (segundo a tábua), $y = ab = b$ então a é elemento neutro à esquerda, mas o neutro é único, então $a = e \therefore |G| = 2$, absurdo. Portanto $x = b$ e isso determina que $y = e$, utilizando o teorema 3.2.1, obtemos que $z = e; w = a$, e completamos a tábua da operação $*$, portanto $ab = ba = e \Rightarrow a = b^{-1}$, e vice-versa; $a^2 = b \Rightarrow a^3 = a*a^2 = a*b = e$,

o elemento a tem ordem 3, do mesmo modo, $b^2 = c \Rightarrow o(b) = 3$. A associatividade é verificada, pois o exemplo, 3, anterior, é de um grupo com 3 elementos, cuja operação do grupo é o produto usual, ora! os elementos desse grupo são números complexos, portanto são associativos, por definição. Como existe um único grupo, a menos de isomorfismo com 3 elementos e o conjunto acima tem as mesmas propriedades estruturais, também estes elementos associam, daí a tábua define um grupo. Portanto se $|G| = 3$, então os elementos diferentes do neutro têm ordem 3, sendo um o inverso do outro. Se tomarmos outro grupo, com 3 elementos, o mesmo ocorrerá, portanto existe um único grupo com 3 elementos, a menos de isomorfismo.

Assim os grupos de ordem 1,2 e 3 são únicos, a menos de isomorfismo. □

Corolário 3.2.4. *Os grupos de ordem* $1, 2$ *e* 3 *são cíclicos*

O resultado, deste corolário, não é verdadeiro para um grupo de 4 elementos. Isto porque, como veremos, existem 2 grupos com estruturas diferentes: em um deles não existe elemento com ordem 4.

A verificação da propriedade associativa pode ser bastante entediante, conforme vimos para um grupo com 2 elementos. A referência [4], indica uma maneira de provar associatividade, utilizando conjuntos numéricos os quais sabemos serem associativos, como fizemos para o caso $|G| = 3$. Assim, repetindo o que fizemos, podemos construir um grupo de ordem 3, com a operação $+mod_3$, que sabemos ser associativa para o conjunto $\{0, 1, 2\}$. Como provamos que existe um único conjunto $\{G, *\}$, com 3 elementos, a menos de isomorfismo, que verifica as propriedades de operação binária, elemento neutro e existência de inverso, então os conjuntos $\{G, *\}$ e $\{\{0, 1, 2\}, +mod_3\}$ são isomorfos, sendo este último associativo, então G é associativo. Para o que segue, verificamos associatividade dessa mesma forma.

Proposição 3.2.5. *Existem dois grupos* $\{G, *\}$ *com* 4 *elementos, isto é,* $|G| = 4$*, que não são isomorfos.*

Demonstração. Como na proposição anterior, $\exists e \in G$, elemento neutro. Então $G = \{e, a, b, c\}$. Podemos montar a tábua da operação binária $*$ e obter duas soluções não-isomorfas:

$*$	e	a	b	c
e	e	a	b	c
a	a	x	y	z
b	b	u	v	w
c	c	f	g	h

tábua I

$\Rightarrow$

$*$	e	a	b	c
e	e	a	b	c
a	a	e	c	b
b	b	c	e	a
c	c	b	a	e

tábua II

ou

$*$	e	a	b	c
e	e	a	b	c
a	a	e	c	b
b	b	c	a	e
c	c	b	e	a

tábua III

A primeira tábua mostra que $x, y, x, u, v, w, f, g, h \in G$. Mostremos que a segunda e terceira tabelas são as possíveis soluções para a primeira tábua.

(1) Pelo teorema 3.2.1 $x \in \{e, b, c\}$. Inicialmente considere que $x = e$, portanto $y \in \{b, c\}$, segundo a linha 2 e $y \neq b$ de acordo com a coluna 3, portanto $y = c$, assim $z = b$, e determinamos completamente a linha 2 da primeira tábua. Prosseguindo com essa tábua, pelo teorema 3.2.1, segundo a linha 3 e coluna 2, $u \in \{e, a, c\} \cap \{b, c\} = \{c\}$, portanto $u = c$. Analizando a linha 3 e a coluna 3, $v \in \{e, a\}$. Se $v = e \Rightarrow w = a$, e completamos a linha 3. O teorema 3.2.1 determina completamente a linha 4, e obtemos a segunda tábua.

(2) A terceira tábua, obtemos segundo a hipótese inicial de $x = e$ de modo que a situação é a mesma da segunda tábua, até a hipótese sobre v, que escolhemos $v = a$ e daí ocorrem as seguintes condições: $w = e; f = b; g = e; h = a$. As duas tábuas possíveis.

(3) Na segunda tábua, todo elemento, exceto o neutro, tem ordem 2, pois segundo essa tábua $a^2 = b^2 = c^2 = e$. No entanto, segundo a tábua III, $b^2 = a \Rightarrow b^3 = b * b^2 = b * a = c \therefore b^4 = b * b^3 = b * c = e$, logo essa tábua contém um elemento de ordem 4, portanto são NÃO-ISOMORFOS, os possíveis grupos da tábua II e III. Provaremos a seguir que as tábuas II e III são associativas, portanto definem um grupo. O grupo definido pela tábua II é o Grupo de Klein, enquanto que o outro é um Grupo Cíclico de ordem 4. Este último grupo contém 2 elementos de ordem 4, que são inversos um do outro e um elemento de ordem 2.

(4) Se consideramos, para a hipótese inicial que $x = b$, o mesmo processo leva a duas outras condições sobre v, e as tábuas mostram que em um deles todos elementos, diferente do neutro, têm ordem 2, enquanto que para a outra condição existirá um elemento de ordem 4. Este mesmo grupo, com um elemento de ordem 4, apresenta as mesma características do grupo ciclico de ordem 4 e portanto são isomorfos.

(5) Consideremos os grupos $\{H, +mod_4\}$, sendo $H = \{0, 1, 2, 3\}$ e $\{K, *\}$, o produto usual de matrizes, sendo

$$K = \{\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} 0 & -1 \\ -1 & 0 \end{pmatrix}\};$$
$$* : K \times K \to K/(A, B) \mapsto A * B.$$

O grupo K é isomorfo à tábua II e o grupo H é isomorfo à tábua III, portanto ambos são associativos. Mostramos assim, que existem, a menos de isomorfismo, 2 grupos de ordem 4. □

Exercícios 3.2.6. *(1) Seja $G = \{a, b\}$, $|G| = 2$. Mostre que se $\{G, *\}$ é um grupo, então $a * b = b$ e nesse caso a é a identidade do grupo, ou $a * b = a$ e nesse caso b é a identidade do grupo.*

(2) Seja $\{G, *\}$ um grupo e $|G| = 2$. Mostre que $\forall x \in G, x^2 = e$, sendo e a identidade de G.

(3) Dados os grupos $\{G, *\}$ *e* $\{H, \bullet\}$ *e as tábuas da operação binária:*

$*$	1	2	3	4
1	1	2	3	4
2	2	4	1	3
3	3	1	4	2
4	4	3	2	1

e

$\bullet$	1	2	3	4
1	1	2	3	4
2	2	1	4	3
3	3	4	1	2
4	4	3	2	1

Explique se os grupos têm as mesmas propriedades de ordem de elementos. Em seguida, identifique cada grupo como cíclico ou grupo de Klein. Se o caso cíclico ocorrer, exiba um de seus geradores

(4) Seja $\{G, *\}$ *um grupo. Construa a tábua da operação* $*$ *para os casos quando* G *possui* $1, 2, 3e4$ *elementos. Mostre que quando* $|G| = 1, 2, 3$ *a tábua é única, porém caso* $|G| = 4$*, existem duas tábuas possíveis.*

(5) Seja um grupo $G, g \in \mathcal{G}$*. Sex*$, y \in \mathcal{G}$*, então* $gx = gy \Leftrightarrow x = y$*.*

(6) Seja $\{G, *\}$ *um grupo. Prove que cada linha da tábua de multiplicação deve apresentar TODOS os elementos do grupo.*

(7) Para um grupo $\{G, *\}$*. Com* 3 *elementos, mostre que* $\forall x \in G, x^3 = e$*, sendo* e *a identidade de* G*.*

(8) Seja $G = \{a, b, c\}$ *tal que o conjunto* $\{G, *\}$ *é um grupo com três elementos. Monte a tabela do grupo e mostre que* G *contém dois elementos de ordem* 3*.*

(9) Dê exemplo de um grupo G*,*$|G| > 2$*, que todos os elementos, a menos da unidade, têm ordem* 2*.*

3.3 Noções Básicas da Teoria dos Grupos

Na seção anterior, discutimos a construção de alguns grupos finitos. Provamos que existem dois grupos de ordem 4, não isomorfos, sendo um deles o grupo de Klein e o outro o grupo cíclico. O primeiro nome é homenagem ao matemático Alemão, que provou esse resultado.

3.3.1 Subgrupos

Vimos que, para os grupos finitos, podemos verificar se um dado conjunto é um subgrupo, a partir da tábua da operação binária. No entanto, existem casos que tornam tal verificação, quando possível, exaustiva. Vamos prosseguir, com algumas definições e estudar alguns subconjuntos bastante comuns na teoria de grupos.

Definição 3.3.1. *Seja $\{G, *\}$, um grupo. Dizemos que G é um grupo abeliano se a operação binária $*$ é comutativa, isto é, $\forall f, g \in G, f * g = g * f$.*

Os grupos abelianos formam uma classe de grupos com características muito peculiares. Segundo alguns matemáticos, existem poucas propriedades com influência mais decisiva do que a comutatividade.

Os grupos cícllicos são sempre abelianos, isso é uma conseqüência direta da propriedade dos números inteiros. A prova desse fato é simples, muito semelhante ao argumento utilizado para provar a associatividade, no caso cíclico. A seguir apresentamos essa proposição e provamos o resultado, para melhor compreensão da teoria, ressaltamos que esse resultado é elementar.

Proposição 3.3.2. *Seja G um grupo cíclico. Então G é abeliano.*

Demonstração. Devemos provar que os elementos de G, comutam, ou seja, $\forall x, y \in G, xy = yx$. Sendo G cíclico, ele é gerado por algum elemento: $\exists g \in G, G =< g >$. Os elementos de G são, portanto potências do gerador, isto é,

$$\exists i, j \in \mathbb{Z}/x = g^i; y = g^j \therefore xy = g^i g^j = g^{i+j} = g^{j+i} = g^j g^i = yx,$$

portanto G é abeliano. □

Exercícios 3.3.3. *(1) Seja G o conjunto dos restos da divisão por 6, e o conjunto $\{G, *\}$, sendo $*$ a operação binária $+mod_6$, isto é, $*(x, y) = (x + y)mod_6$ o resto da divisão de $x + y$ por 6, a soma usual.*

a) *Sabendo-se que $+mod_6$ é associativa, prove que $\{G, *\}$ é um grupo;*

b) *Mostre que $\{G, *\}$ é um grupo cíclico;*

c) *Podemos afirmar que a operação $*$ é comutativa?*

(2) Seja $G = \{a, m, b, p, q\}$, um grupo de ordem 5, com as seguintes propriedades:$a^2 = m; m^2 = q; q^2 = a; a^{-1} = q$, isto é, o inverso de a é q.

a) *Determine o elemento neutro de G;*

b) *Determine o inverso de b;*

c) *Monte a tábua da operação binária de G, explicando seus passos;*

d) *Determine a ordem de cada elemento, a partir da tábua. Podemos afirmar que este grupo é cíclico?*

(3) Seja G um grupo, $x, y \in G$, tal que, $o(x)$=$o(y) = 2$, isto é, eles têm ordem 2, mostre que $xy = yx$, eles comutam.

(4) Seja $G = \{A, B, C, D, E, F\}$, e $\{G, *\}$ o grupo formado pelos elementos de G com a operação $*$ dada pelo produto dos elementos de G. São dadas

$*$	A	B	C	D	E	F
A	A	B		D		F
B		C		E		
C	C		B		D	
D	D	F			C	B
E	E			B		C
F	F	E		C	B	

a tábua do grupo e as matrizes do conjunto, determine:

a) *Complete a tábua do grupo;*

b) *Calcule B^3 e D^4 ;*

c) *Calcule a ordem de E;*

d) *Determine todos os elementos de ordem 2.*

(5) Seja $\{G, *\}$ um grupo com 4 elementos, $G = \{a, b, c, d\}$, segundo a operação $*$. Se a tábua do grupo é :

$*$	a	b	c	d
a	x	y	a	b
b	z	w	b	a
c	a	b	c	d
d	c	a	d	c

a) *Determine a unidade do grupo;*

b) *Calcule x, y, z, w e verifique se o grupo é comutativo ou não;*

c) *Determine a ordem dos elementos diferentes da unidade;*

d) *Encontre um subgrupo de G com exatamente 2 elementos.*

(6) Seja $P = \{1, 2, 4, 7, 8, 11, 13, 14\}$ e $*$ a operação do produto módulo 15.

a) *Mostre que $*(4, 7) = 13 = 7^3$;*

b *Mostre que $\{P, *\}$ é um grupo, sendo * a operação definida acima;*

c) *Utilize a tábua do grupo, ou calcule diretamente, a ordem dos elementos $2, 8, 14$ e 11 ;*

d) *Mostre que o conjunto $H = \{1, 2, 4, 8\}$ é um subgrupo de P.*

Os grupos de ordem até 5 são abelianos. O menor grupo não abeliano é o grupo das bijeções do conjunto $\{1, 2, 3\}$, também chamado de grupo das permutações de $1, 2, 3$, denotado por S_3. Os grupos não-abelianos são tão comuns, quanto os grupos abelianos, porém a propriedade comutativa permite obter resultados mais gerais. Um subconjunto importante, para um grupo G, é aquele formado pelos elementos do grupo que comutam entre si. Este conjunto é denominado centro de G.

Definição 3.3.4. *Seja $\{G, *\}$ um grupo. O subconjunto*

$$\{x \in G / g * x = x * g, \forall g \in G\}$$

é denominado centro de G, denotado por $\mathcal{Z}(G)$, os elementos de $\mathcal{Z}(G)$, são chamados de centrais.

Observe que se um elemento é central, tal elemento pode sempre ser colocado, juntamente com o sinal de $=$, no centro da igualdade.

Segundo a definição, se G é um grupo abeliano, então $G = \mathcal{Z}(G)$, pois todos os elementos de G comutam. Perguntamo-nos se o centro de um grupo é um subgrupo deste? Neste caso, nossa pergunta é bastante geral, pois não especifica o grupo considerado. Certamente $\mathcal{Z}(G)$ é o subgrupo não-próprio G, quando este é abeliano, mas resta analisar quando este não é abeliano. Podemos checar este subconjunto para o grupo S_3 e verificar que $\mathcal{Z}(S_3) = \{e\}$, sendo e o neutro do grupo, ou seja o $\mathcal{Z}(S_3)$ é o subgrupo trivial. O próximo teorema auxilia na resposta àquela questão.

Antes de enunciar o teorema, convém discutir a linguagem nele empregada. Quando dizemos que certas condições são equivalentes, estamos ressaltando o fato de poder afirmar a mesma coisa, através de condições, aparentemente distintas. O termo matemático para essa equivalência, entre outros, é a expressão "se, e somente se"($\Leftrightarrow$). Assim quando dizemos que A, B, C são equivalentes significa: $A \Leftrightarrow B \Leftrightarrow C$. A prova de uma equivalência, deve considerar, portanto as condições $\Rightarrow$ (necessidade); e $\Leftarrow$ (suficiência). Às vezes, em uma prova tipo $A \Rightarrow B$, pode ser mais conveniente provar $\sim B \Rightarrow \sim A$, em que $\sim A$ denota a negação da condição A. Um resultado, conhecido em Lógica, é que as duas implicações anteriores são equivalentes, assim provas (para a condição $A \Rightarrow B$) que levem à conclusão $\sim B \Rightarrow A$, são conhecidas por "provas por contradição", pois deveríamos concluir a necessidade para $\sim A$. A equivalência proposta a seguir $A \Leftrightarrow B \Leftrightarrow C$ será demonstrada do seguinte modo:$A \Rightarrow B; B \Leftrightarrow C; C \Rightarrow A$. É um resultado da Lógica de primeira ordem, via tautologias, que a essa demonstração equivale às condições $A \Leftrightarrow B \Leftrightarrow C$.

Teorema 3.3.5. *Seja $\{G, *\}$ um grupo e $H \subseteq G$, H um conjunto não vazio. As seguintes condições são equivalentes:*

(i) *$H \leq G$ (H é subgrupo de G)*

(ii) *$\forall a, b \in H \Rightarrow a * b \in H$ e $\forall a \in H \Rightarrow a^{-1} \in H$*

(iii) $\forall a, b \in H, a * b^{-1} \in H$

Demonstração. Devemos provar que $(i) \Leftrightarrow (ii) \Leftrightarrow (iii)$, faremos isso em 4 passos:

(1) $(i) \Rightarrow (ii)$, isto é, (i) é nossa hipótese, portanto estamos assumindo que $H \leq G$, devemos provar a tese (ii); se $a, b \in H$, sendo este um subgrupo (aqui estamos usando a hipótese), então $*$ é operação binária H, portanto $a * b \in H$, analogamente, se $a \in H$, sendo H um grupo, então $a^{-1} \in H$, pela propriedade do inverso.

(2) $(ii) \Rightarrow (iii)$: observe que a condição (ii) garante que para todo elemento de H, o inverso desse elemento também está em H; sejam $a, b \in H$, $(ii) \Rightarrow b^{-1} \in H \therefore a, b^{-1} \in H \therefore a * b^{-1} \in H$.

(3) $(iii) \Rightarrow (ii)$: inicialmente provemos que $e \in H$, o elemento neutro de G, sendo $H \neq \emptyset, \exists a \in H$, tomando-se $a = b$ na condição (III), $a, a \in H \Rightarrow a * a^{-1} = e \in H$ logo H contém o elemento neutro; sejam $e, a \in H, (iii) \Rightarrow e * a^{-1} = a^{-1} \in H \therefore a \in H \Rightarrow a^{-1} \in H$; então $a, b \in H, (iii) \Rightarrow b^{-1} \in H \therefore a, b^{-1} \in H, (iii) \Rightarrow a * (b^{-1})^{-1} = a * b \in H$, que são as condições de (ii). Este item e o anterior provaram que $(ii) \Leftrightarrow (iii)$ ocorre.

(4) $(iii) \Rightarrow (i)$: com a hipótese (iii), devemos provar que $H \leq G$. Sendo $H \subseteq G$, basta provar que H é um grupo. O item anterior mostrou que $\forall a, b \in H \Rightarrow a * b \in H$, logo $*$ é operação binária em H; no item anterior também provou-se que $(iii) \Rightarrow e \in H$, portanto H contém o elemento neutro; também mostrou-se que se $a \in H \Rightarrow a^{-1} \in H$, portanto H satisfaz a propriedade do inverso; sendo $H \subseteq G$ e $*$ operação binária associativa em G, que é operação binária em H, então pelo lema 2.3.2, $*$ é associativa em H. Como $\{H, *\}$ é um conjunto, em que $*$ é operação binária em H, e estão verificadas as propriedades: associatividade, existência do neutro e propriedade do inverso, o subconjunto $H \subseteq G$ é um grupo, portanto um subgrupo de G.

□

Podemos responder à questão anterior, positivamente, em forma de proposição.

Proposição 3.3.6. *Seja G um grupo e $\mathcal{Z}(G)$ o seu centro. Então $\mathcal{Z}(G) \leq G$.*

Demonstração. Inicialmente lembremos que $\mathcal{Z}(G) = \{x \in G / gx = xg, \forall g \in G\}$. Vamos provar que a condição (iii) do teorema 3.3.5 ocorre. Por hipótese, $\mathcal{Z}(G) \subseteq G$. Devemos garantir que $\mathcal{Z}(G)$ é não vazio; isso é verdade, pois $e \in G$ o neutro de G, é tal que $eg = ge, \forall g \in G \therefore e \in \mathcal{Z}(G) \Rightarrow \mathcal{Z}(G) \neq \emptyset$; provemos que $\forall a, b \in \mathcal{Z}(G) \Rightarrow ab^{-1} \in \mathcal{Z}(G)$, da hipótese $ag = ga$ e $bg = gb$, para todo $g \in G$; da condição $bg = gb$, multiplicamos à esquerda por b^{-1}, então $b^{-1}(bg) = b^{-1}(gb) = (b^{-1}b)g = (b^{-1}g)b \Rightarrow g = (b^{-1}g)b$, multiplicamo à direita por

b^{-1}, então $gb^{-1} = ((b^{-1}g)b)b^{-1} = (b^{-1}g)(bb^{-1}) = b^{-1}g$, portanto $b^{-1}g = gb^{-1}$; com esta três condições, temos o seguinte:$(ab^{-1})g = a(b^{-1}g) = a(gb^{-1}) = (ag)b^{-1} = (ga)b^{-1} = g(ab^{-1})$, portanto $ab^{-1} \in \mathcal{Z}(G)$, logo $\mathcal{Z}(G)$ satisfaz a condição (iii) do teorema e portanto é um subgrupo de G. □

O centralizador de um grupo, sendo um subgrupo, é ele próprio um grupo abeliano. Porém nem todo subgrupo abeliano de um grupo está contido no centralizador, veja por exemplo os subgrupos cíclicos do grupo S_3, são abelianos; no entanto $\mathcal{Z}(S_3) = \{e\}$.

Dado um elemento g de um grupo G, se $g \in \mathcal{Z}(G)$ então $\forall x \in G, gx = xg$. Neste caso dizemos que g é um elemento central. No entanto, se $g \notin \mathcal{Z}(G)$, com quais elementos de G este elemento comuta? O conjunto formado por estes elementos dá uma idéia do quanto g é não central. Além disso, o centralizador $\mathcal{Z}(G)$ é um subconjunto deste conjunto. Isso motiva a seguinte definição.

Definição 3.3.7. *Se G um grupo e $g \in G$ um elemento fixado. O conjunto $\{x \in G/xg = gx\}$ dos elementos do grupo que comutam com o elemento g, é denominado centralizador de g em G, denotado por $C_g(G)$.*

Para a proposição que segue, afirmamos que o centralizador de um elemento num grupo que o contém é um subgrupo deste; a prova é idêntica àquela apresentada para o centralizador. Para reforçar a idéia repetimos a demonstração, porém mais diretamente.

Proposição 3.3.8. *Seja G um grupo e $g \in G$ então $C_g(G) \leq G$, isto é, o centralizador de g em G é um subgrupo de G.*

Demonstração. Seja $e \in G$, o neutro, então $e \in C_g(G) \therefore C_g(G) \neq \emptyset$; sejam $a, b \in C_g(G) \Rightarrow bg = gb \therefore b^{-1}g = gb^{-1} \Rightarrow (ab^{-1})g = a(b^{-1}g) = a(gb^{-1}) = (ag)b^{-1} = g(ab^{-1})$, logo pelo teorema 3.3.5, item (iii), o conjunto $C_g(G) \subseteq G$ é um subgrupo de G, isto é, $C_g(G) \leq G$. □

Uma propriedade importante, para os elementos que comutam, é a distributividade da potência de seus fatores, lembrando que, dado um grupo G e $f, g \in G$, eles comutam se $fg = gf \therefore f \in Cg(G); g \in C_f(G)$. Veremos que o fato do centralizador ser um subgrupo simplifica a demonstração da próxima proposição.

Proposição 3.3.9. *Seja G um grupo e $f, g \in G$ dois elementos que comutam, isto é, $fg = gf$. Então $(fg)^n = f^n g^n = g^n f^n, \forall n \in \mathbb{Z}^+$.*

Demonstração. A prova é por indução finita; se $n = 1$, $(fg)^1 = fg = gf$, portanto $P(n_0)$ é verdadeira; supomos por hipótese de indução (HI) que seja verdadeiro para $k \in \mathbb{Z}^+$, isto é, $(fg)^k = f^k g^k = g^k f^k$. Vamos provar que o resultado é verdadeiro para $k + 1$:$(fg)^{k+1} \doteq$

$(fg)(fg)^k = (fg)(f^k g^k) = (fg)(g^k f^k)$, nestas duas últimas igualdades utilizamos a hipótese de indução. Segundo a associatividade: $(fg)(g^k f^k) = f(gg^k)f^k = fg^{k+1}f^k$, como observado há pouco, $fg = gf \Rightarrow g \in C_f(G)$, pela proposição 3.3.8, $C_f(G)$ é um subgrupo, portanto $g \in C_f(G) \Rightarrow g^{k+1} \in C_f(G)$, então $fg^{k+1}f^k = g^{k+1}ff^k = g^{k+1}f^{k+1}$; repetindo-se o procedimento inicial, de uma forma adequada: $(fg)(g^k f^k) = (gf)(f^k g^k) = gf^{k+1}g^k$, como $f \in C_g(G)$, concluímos

$$HI : (fg)^k = f^k g^k = g^k f^k \Rightarrow (fg)^{k+1} = f^{k+1}g^{k+1} = g^{k+1}f^{k+1},$$

portanto provamos por indução finita a proposição. □

Corolário 3.3.10. *Nas condições da proposição anterior,* $(fg)^m = f^m g^m = g^m f^m, \forall m \in \mathbb{Z}$.

Demonstração. Se $m = 0, \forall x \in G, x^0 \doteq e \in G$ o neutro de G, portanto um elemento central. Se $m < 0$, basta verificar que $fg = gf \Rightarrow f^{-1}g^{-1} = g^{-1}f^{-1}$, isso pode ser feito, multiplicando a igualdade, repetidas vezes, pelos inversos de seus fatores, mas vamos provar isso utilizando o fato que o $C_x(G)$ é um subgrupo; $fg = gf \Rightarrow f \in C_g(G) \Rightarrow f^{-1}g = gf^{-1} \Rightarrow g \in C_{f^{-1}}(G) \Rightarrow g^{-1}f^{-1} = f^{-1}g^{-1}$. Entao $(fg)^m = ((fg)^{-1})^{-m} = (g^{-1}f^{-1})^{-m}$ e $m < 0 \Rightarrow -m > 0$, pela proposição, substituindo $f^{-1} = u; g^{-1} = v; -m = n \therefore f^m = (f^{-1})^{-m} = u^n$ apenas por conveniência, $(uv)^n = u^n v^n = v^n u^n \Rightarrow (fg)^m = f^m g^m = g^m f^m$, $\forall m \in Z$. □

Vimos que dado um grupo G, se ocorre de $h \in \mathcal{Z}(G)$, então h comuta com todo elemento de G, em particular $gh = hg \therefore h \in C_g(G)$, portanto $\mathcal{Z}(G) \subseteq C_g(G), \forall g \in G$, vejamos que essa situação é mais geral ainda, pemitindo-se determinar o centro de G, a partir dos centralizadores dos elementos de G.

Proposição 3.3.11. *Seja G um grupo e $\mathcal{Z}(G)$ o centralizador de G. Para todo $g \in G$, denote $C_g(G)$ o centralizador de g em G. Então*

$$\mathcal{Z}(G) = \bigcap_{g \in G} C_g(G)$$

Demonstração. Seja $U = \bigcap_{g \in G} C_g(G)$; lembrando do axioma $A2$, axioma da extensionalidade, devemos mostrar que $\mathcal{Z}(G) \subseteq U$ e $U \subseteq \mathcal{Z}(G)$; a primeira inclusão é imediata, pois $x \in \mathcal{Z}(G)$ implica que x é central, logo centraliza todos os elementos de G, portanto $x \in U \Rightarrow \mathcal{Z}(G) \subseteq U$. Seja $x \in U \Rightarrow \forall g \in G, xg = gx \therefore g \in \mathcal{Z}(G) \therefore U \subseteq \mathcal{Z}(G)$. Assim $U = \mathcal{Z}(G)$. □

Na proposição acima, vimos que a interseção dos centralizadores dos elementos de um grupo, que são subgrupos, resultam também em um subgrupo. Este fato pode ser generalizado, ou seja, se H, K são subgrupos de G, então $H \cap K$ é um subgrupo de G. No entanto isso não é verdade para a união $H \cup K$, pois se $G = \{e, a, b, c / o(a) = o(b) = o(c) = 2\}$ o grupo de Klein,

$H =< a >; K =< b >$ são subgrupos de G, porém $L = H \cup K = \{e, a, b\}$ não é subgrupo de G, pois $a, b \in L$, mas $ab = c \notin G$, ou seja L não satisfaz as condições do teorema 3.3.5.

Proposição 3.3.12. *Seja G um grupo e $H, K \leq G$. Então $H \cap K \leq G$.*

Demonstração. A prova é imediata, a partir do teorema 3.3.5(iii). Sendo $H, K \leq G \Rightarrow e \in U; e \in K \therefore e \in H \cap K \therefore H \cap K \neq \emptyset$. Sejam $a, b \in H \cap K \Rightarrow a, b \in H; a, b \in K \therefore ab^{-1} \in H; ab^{-1} \in K \Rightarrow ab^{-1} \in H \cap K$, portanto $H \cap K$ é um subgupo de G. □

Existe um resultado importante para os subgrupos de um grupo finito, o teorema de Lagrange. Segundo o teorema, $H \leq G \Rightarrow |H| \mid |G|$, isto é, a ordem do subgrupo divide a ordem do grupo. No capítulo 1 discutimos a divisibilidade entre números inteiros, vamos recordar alguns pontos e definir certos conceitos, importantes para a compreensão do assunto subseqüente. A referência sobre este assunto é [7].

Exercícios 3.3.13. *(1) Determine os subgrupos do grupo $< i >$, sendo i a unidade imaginária, e do grupo de Klein.*

(2) Determine todos os subgrupos do grupo $G =< g >$, sendo g um elemento de ordem 8.

(3) Prove que se G é um grupo abeliano, cujo elemento neutro é e, o subconjunto de G, dado por $H = \{g \in G / g^2 = e\}$ é um subgrupo de G.

(4) Mostre que se G é um grupo finito cujo neutro é e, então $\forall g \in G, \exists n \in Z^+$, tal que,$g^n = e$

(5) Seja $\{G, *\}$ o grupo definido pelos elementos

$$G = \{1, 2, 3, 4, 6, 7, 8, 9, 11, 12, 13, 14, 16, 17, 18, 19, 21, 22, 23, 24\},$$

cuja operação $*(m, n) = (mn) mod_{25}$, o produto usual, módulo 25.

a) *Determine a ordem dos elementos 6 e 7;*

b) *Sabendo-se que $o(4) = 10$, mostre que G é um grupo cíclico gerado pelo 2, isto é, $G =< 2 >$;*

c) *Determine os subgrupos de G, que são gerados pelos elementos 6 e 7, isto é, $< 6 >$ e $< 7 >$;*

d) *Mostre que G admite um elemento de ordem 2, em seguida mostre qual é esse elemento.*

(6) Sejam A e B dois grupos com a seguinte tábua:

a) *Complete as tabelas para os elementos que faltam;*

b) *Determine f^3 e f^5;*

$\circ$	e	f	f^2	f^3	f^4	f^5
e		f	f^2	f^3		f^5
f	f	f^2	f^3			f^4
f^2	f^2	f^3	f^4	f^5		f
f^3					f	
f^4	f^4	f^5				
f^5			f	f^2	f^3	

c) *Lembrando que existem* 2 *grupos de ordem* 6*, explique se os grupos acima são os mesmos, mostrando se eles possuem as mesmas propriedades ou não.*

(7) Seja $G = \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11\}$ *e* $+$ *é a operação de soma módulo* 12*.*

a *Mostre que o subconjunto* $\{0, 3, 6, 9\}$ *é um subgrupo de* G*;*

b) *Calcule a ordem dos elementos* $4, 7, 6$ *e* 8*;*

c) G *contém algum subgrupo com* 2 *elementos? Qual?*

(8) Seja G *um grupo e* $\zeta(G) = \{g/g \in G, gx = xg, \forall x \in G\}$*.*

a) *Mostre que* $e \in \zeta(G)$ *, sendo o elemento neutro de* G*;*

b) $h \in \zeta(G) \Rightarrow h^{-1} \in \zeta(G)$*;*

c) $a, b \in \zeta(G) \Rightarrow ab \in \zeta(G)$

d) *Prove que* $\zeta(G)$ *é um grupo;*

e) *Prove que* $\zeta(G)$ *é um subgrupo de* G*, que é abeliano.*

eja G *um grupo e* $H = \{x \in g/g^{-1}xg = x \forall g \in G$*, um subconjunto de* G*.Mostre que* H *é um subconjunto de* G*.*

(9) Determine $\zeta(G)$ *para os seguintes grupos:*

a) *O grupo de Klein;*

b) *O grupo do exercício* 8*;*

c) *O grupo do exercício* 7*.*

(10) Para o exercício anterior, construa a tábua de $\zeta(G)$*, em cada caso.*

(11) Seja G *um grupo e* $C_G(x) = \{g/g \in G, gx = xg\}$*. Mostre que este conjunto é um grupo, portanto um subgrupo de* G*.*

(12) Para os grupos a seguir, determine o centralizador do elemento indicado:

a) $G = \{(-1,-1),(-1,1),(1,-1),(1,1)\}; x = (-1,1)$;

b) G=$\{\{(a,a),(i,i),(r,r)\}, \{(a,a),(i,r),(r,i)\}, \{(a,i),(i,a),(r,r)\}, \{(a,i),(i,r),(r,a)\}, \{(a,r),(i,i),(r,a)\}, \{(a,r),(i,a),(r,i)\}\}$;$x$=$\{(a,i),(i,a),(r,r)\}$;

c) $G = \{-i,-j,-k,-1,i,j,k,1/ij = k, jk = i, ki = j, i^2 = j^2 = k^2 = -1\}$; $x = k$.

(13) *Seja* $G = \{f : \{1,2,3,4,5,6\} \to \{1,2,3,4,5,6\}/f$ *é injetora*$\}$. *Sabendo-se que* $\{G, \circ\}$ *é um grupo, sendo* $\circ : G \times G \to G$ *a operação binária de composição de função, isto é,* $\circ(f,g) = f \circ g$ *e* $f \circ g(x) \doteq f(g(x))$ *, determine:*

a) *O elemento* $x = h \circ g$, *sabendo-se que* $h(1) = 3; h(2) = 1; h(3) = 5; h(4) = 4; h(5) = 2; h(6) = 6 e g(1) = 4; g(2) = 3; g(3) = 5; g(4) = 6; g(5) = 2; g(6) = 1$;

b) *Calcule as ordens de* h *e* x;

c) *Determine* h^{250}

d) *Determine o grupo cíclico* $< g >$

(14) *Prove que se* G *é um grupo abeliano, cujo elemento neutro é* e, *o subconjunto de* G, *dado por* $H = \{g \in G/g^2 = e\}$ *é um subgrupo de* G.

(15) *Mostre que se* G *é um grupo finito cujo elemento neutro é* e, *então* $\forall G \in G, \exists n \in Z^+$ *, tal que,*$g^n = e$

(16) *Sejam* H *e* K *dois subgrupos de* G. *Mostre que* $H \cap K$ *é um subgrupo de* G, *porém isso não é verdade para o conjunto* $H \cup K$, *sugestão: o grupo de Klein.*

(17) *Seja* H *um subgrupo de* G. *Seja* $R : G \to G$ *, uma relação, tal que* $R(a) = b \Leftrightarrow ab^{-1} \in H$. *Mostre que* R *é uma relação de equivalência.*

(18) *Seja* G *um grupo. Para* $g, h \in G$, *defina* $[g,h] = ghg^{-1}h^{-1}$. *Prove que* G *é um grupo abeliano se, e somente se,* $[g,h] = e$, $\forall g, h \in G$, *sendo* e *a unidade de* G.

(19) *Sejam* H *e* K *dois subgrupos de* G. *Prove que o conjunto* $H \cap K$ *é um subconjunto de* G, *que é um subgrupo, porém,* $H \cup K$ *nem sempre é um subgrupo. Nesse caso basta exibir um contra-exemplo, mostrando porque isso é falso.*

(20) *Seja* G *um grupo e* $H = \{x \in G/gx = gx, \forall g \in G\}$ *, um subconjunto de* G. *Prove que* H *é um subgrupo de* G. *No caso de* G *ser um grupo abeliano, o que podemos afirmar sobre* H*?*

(21) *Prove que se* g *e* h *são dois elementos de um grupo qualquer e* $o(g) = o(h) = o(gh) = 2$, *então eles comutam, isto é,* $gh = hg$.

3.3.2 Divisibilidade: Algumas Definições

Definição 3.3.14. *Sejam $i, j \in \mathbb{Z}$. Dizemos que i divide j, que denotamos por $i \mid j$, se $\exists k \in \mathbb{Z}/j = ki$, isto é se j é múltiplo de i.*

Se $n \in \mathbb{Z}$, seja $Div(n) = \{i \in \mathbb{Z}^+/i|n\}$ o conjunto dos divisores de n. Uma condição para que ocorra a divisibilidade é que $i \leq |n|$. Daí o conjunto $Div(n)$ sempre admite um elemento máximo, que é próprio $|n|$. Nas mesmas condições, seja $Mult(n) = \{k \in \mathbb{Z}^+/n|k\}$, pelo mesmo motivo, $\forall k \in Mult(n), |n| \leq k$, e o conjunto $Mult(n)$ sempre admite elemento mínimo, que é $|n|$. Estas condições permitem a seguinte definição.

Definição 3.3.15. *Sejam $m, n \in \mathbb{Z}$.*

(i) *Definimos $d = mdc(m, n) :=$máx$(Div(m) \cap Div(n))$;*

(ii) *Definimos $m = mmc(m, n) :=$mín$(Mult(m) \cap Multi(n)$,*

respectivamente, o máximo divisor comum, $mdc(m, n)$ e o mínimo múltiplo comum $mmc(m, n)$, entre m, n. Se $mdc(m, n) = 1$, m, n são relativamente primos.

Há uma interessante aplicação do *mmc* entre dois números, em teoria de grupos, quando dois elementos de ordem finita, digamos f, g, comutam. A demonstração que apresentamos utiliza um fato que ficará evidente após um resultado, que apresentamos mais à frente, sobre grupos cíclicos. Os resultados a seguir auxiliam na compreensão deste fato.

Sabemos que $12|48$, escrevendo $48 = 6 * 8$, então $12|6 * 8$, no entanto $12 \nmid 6$ ou $12 \nmid 8$; observe que $mdc(12, 6) = 6; mdc(12, 8) = 4$. Portanto se $i|mn$ nada se pode afirmar sobre as divisibilidades $i|m$ ou $i|n$. No entanto, se i é relativamente primo de um dos fatores, o teorema de Euclides garante que ocorre a divisibilidade de i com o outro fator.

Teorema 3.3.16 (Teorema de Euclides)**.** *Sejam m, n inteiros positivos se $i|mn$ e $mdc(i, n) = 1$, então $i|m$.*

Vamo-nos deter em aspectos particulares destas definições e resultados, úteis e importantes para o que segue. Um deles refere-se à divisibilidade entre dois números inteiros positivos. Se $m, n \in \mathbb{Z}$ e $m \nmid n$, $\exists k \in \mathbb{Z}/m|kn$, sendo $k = m$ um dos possíveis inteiros, por exemplo, $42 \nmid 144$, $6 = mdc(42, 144) \Rightarrow 6|42; 7 = \frac{42}{6} \therefore 7$ é o menor inteiro, tal que $42|7.144$. Nessas condições, interessa-nos qual o menor inteiro k.

Lema 3.3.17. *Sejam m, n números inteiros positivos. Se $m \leq n$ e $d = mdc(m, n)$, então $k = \frac{m}{d}$ é o menor inteiro positivo, tal que $m|kn$.*

Demonstração. Se $d = mdc(m,n)$, então d é um divisor de m,n; $d|m; d|n \Rightarrow m = m_1 d; n = n_1 d$ da condição $m|kn \Rightarrow m_1 d|kn_1 d \therefore m_1|kn_1$, sendo $mdc(m_1,n_1) = 1$, pelo teorema de Euclides, $m_1|k \therefore k = qm_1, q \in Z^*$, então $k = m_1 = \frac{m}{d}$ é o menor inteiro que satisfaz aquela condição. □

Lema 3.3.18. *Seja G um grupo e $g,h \in G$ dois elementos de ordem finita, tal que $gh = hg$. Se m é a ordem de gh, então $o(g) \mid m$.*

Demonstração. Sejam os grupos cíclicos $< g >$ e $< h >$, com elemento neutro e, tais que $< g > \cap < h >= \{e\}$; sendo m a ordem de $x = gh$, então $(gh)^m = e$, como $gh = hg$, pela proposição 3.3.9, $(gh)^m = g^m h^m = e$, como a única potência comum é o elemento neutro, então $g^m = h^m = e$, portanto pela proposição 3.1.5, então $o(g) \mid m$. Se $< x > \cap < y > \neq \{e\}$ □

Podemos, então, enunciar e demonstrar o seguinte resultado:

Proposição 3.3.19. *Seja G um grupo e $f,g \in G$, de ordens $o(f) = i; o(g) = j$ finitas. Se $fg = gf = x$, ou seja eles comutam entre si, então $o(x) = mmc(i,j)$.*

Demonstração. Seja $m = mmc(i,j)$, então m é o menor inteiro, tal que, $i|m$ e $j|m$, portanto, $m = i.i_1 = j.j_1$, daí, $x^m = (fg)^m$, pela proposição 3.3.9, como $fg = gf \Rightarrow (fg)^m = f^m g^m$, logo $x^m = f^m g^m = f^{ii_1} g^{jj_1} = (f^i)^{i_1} (g^j)^{j_1} = e$, assim $x^m = e$; pela proposição 3.1.5 então $o(x)|m$. Pela lema 3.3.18, $o(x)|i$, analogamente $o(x)|j$, pela minimalidade de m, sendo m o menor inteiro com essa propriedade, então $o(x) = m = mmc(i,j)$ □

Exercícios 3.3.20. *(1) Seja g um elemento de ordem 5, verifique que existem apenas 5 potências distintas de g.*

(2) Seja

$$m = \begin{bmatrix} 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix}$$

calcule a ordem multiplicativa de m e o grupo cíclico $< m >$.

(3) Para os elementos $0 \leq n \leq 18$, verifique quais são invertíveis pelo produto módulo 18. Em seguida calcule a ordem de cada elemento segundo essa operação.

(4) Sejam os elementos $1,5,7,11,13,17,19,23$. Verifique que estes são os únicos invertíveis pelo produto módulo 24. Em seguida, a ordem de cada elemento e o grupo cíclico gerado por este elemento.

(5) Prove que o grupo $\{0,1,2,...,n-1\}$, com a operação + módulo n é um grupo cíclico. Determine quais são os geradores desse grupo.

(6) Seja $H = \{0, 1, 2, 3, ..., n-1\}$ *e* $*$ *módulo* n *a operação de multiplicação de* H*. Prove que os invertíveis de* H*, segundo essa operação, são os números* $1 \leq u \leq n-1$*, tais que* $MDC(n, u) = 1$*.*

(7) Calcule a ordem dos invertíveis do exercício anterior, pela operação de produto, e prove que os elementos invertíveis do exercício anterior formam um grupo cíclico.

(8) Considere os números menores que 30*. Calcule o número de elementos invertíveis pela operação produto módulo* 30*?*

(9) Calcule a ordem do elemento 12*, segundo a operação* $+$ *módulo* 18*. Em seguida determine o grupo cíclico gerado por este elemento, segundo essa operação.*

(10) Calcule a ordem do elemento $7, 11$ *e* 23 *segundo a operação* $*$ *módulo* 30*.*

(11) Prove que se G *é um grupo cíclico e* x *é um elemento de* G*, então:*

a) *Existe* $g \in G$*, tal que,*$G =< g >$ *e* $x = g^j$

b) *o grupo cíclico gerado por* g *tem exatamente* $\frac{|G|}{MDC(|G|,j)}$ *elementos, isto é,* $| < x > | = \frac{|G|}{MDC(|G|,j)}$*.*

(12) Seja G *o grupo gerado por* 1*,* $G =< 1 >$*, segundo a operação* $+$ *módulo* 15*.*

a) *Calcule a ordem de* $x = 1^7$ *e* $y = 1^{12}$*;*

b) *Determine a potência* x^{212} *;*

c) *Calcule o inverso de* y*?*

(13) Mostre que os números 1, 2, 3, 4, 6, 7, 8, 9, 11, 12, 13, 14, 16, 17, 18, 19, 21, 22, 23, 24 são todos escritos como alguma potência de 2 *módulo* 25*.*

(14) Seja G *o grupo gerado por 1,* $G =< 1 >$*, segundo a operação* $+$ *módulo 36.*

a) *Calcule a ordem de* $x = 1^{10}$ *e* $y = 1^{16}$*;*

b) *Sabendo-se que* $o(g) = 12$ *e* $o(h) = 9$*, determine* $o(g^{314})$ *e* $o(h^{518})$

c) *Calcule os inversos de* x *e* y*?*

d) *Determine os valores possíveis para* g *e* h*.*

(15) Calcule a ordem de 18 no grupo cíclico gerado por 1, com a operação soma módulo 30. Determine $< 18 >$*, grupo cíclico gerado por 18, com essa operação. Existe algum número entre 0 e 29 cujo grupo cíclico tem o mesmo número de elementos do grupo* $< 18 >$*? Qual?*

(16) Dê exemplo de um grupo cíclico aditivo com 12 elementos, um grupo cíclico multiplicativo com 6 elementos e um grupo que não seja cíclico nem abeliano.

(17) Seja G o grupo formado pelos números naturais de 0 a 19, cuja operação do grupo seja $+$ módulo 20.

a) *Determine o grupo H, formado pelos invertíveis do conjunto G, segundo a operação $*$ módulo 20;*

b) *Prove se H é ou não cíclico;*

(18) Seja G o grupo formado pelos elementos $\{(1,1),(-1,-1),(1,-1),(-1,1)\}$, cuja operação $*$ do grupo é dada por: $*((i,j),(m,n)) = (im,jn)$, em que im e jn denotam o produto usual.

a) *Determine o elemento identidade de G, e calcule a ordem dos elementos de G;*

b) *Determine o subgrupo de G gerado pelo elemento $(-1,-1)$;*

c) *Mostre que G é o grupo de Klein.*

3.3.3 Grupos Cíclicos

Dado um grupo G, vimos que $\forall g \in G, < g > \leq G$, isto é, todo grupo cíclico, gerado pelos elementos de G, são subgrupos de G. Dentre os possíveis subgrupos de um dado grupo, os subgrupos que são cíclicos devem ocorrer com freqüência. Acrescente a este fato, a estrutura, relativamente simples, de um grupo cíclico. Estes fatores, por sim mesmos, motivam o estudo detalhado dos grupos cíclicos, que permitem obter resultados importantes para a teoria de grupos. O seguinte resultado, permite obter todos os subgrupos de um grupo cíclico.

Proposição 3.3.21. *Se G é um grupo cíclico finito, todo subgrupo de G é cíclico*

Demonstração. Seja $H \leq G$, sendo G cíclico $\exists g \in G / G =< g >$. Se H é o subgrupo trivial, $H = \{e\} \Rightarrow H =< e >$, portanto H é cíclico. Se H é um subgrupo próprio de G, $\forall h \in H \setminus \{e\} \subset G \Rightarrow \exists n, 0 \leq n < o(g) / h = g^n$, seja h a menor potência de g, nessas condições, então $H =< h >$. De fato! seja $h = g^k$, sendo k a menor potência de G para o qual $g^k \in H$, basta mostrar que qualquer elemento $x \in H$ é alguma potência de h, como $x \in G$, $x = g^n, 0 < n < |G|$, por hipótese $n \leq k$, portanto, pelo teorema da divisão de Euclides, $\exists q, r \in \mathbb{Z}, n = qk + r \Rightarrow x = g^n = g^{qk+r} = (g^k)^q g^r \Rightarrow g^r = (g^k)^{-q} x$, portanto $g^r \in H$, mas o teorema da divisão garante que $0 \leq r < k$, logo $r = 0$, pela minimalidade de k, pois apenas as potências maiores ou iguais a k, são elementos de H. Assim, como $r = 0 \Rightarrow x = (g^k)^q = h^q \therefore x$ é uma potência de $h \therefore H =< h >$, logo é um grupo cíclico. □

Segundo as definições e notações utilizadas, $|G|$ é a ordem do grupo: o número de elementos do conjunto G. Enquanto que $o(g)$ denota a ordem do elemento: o menor expoente positivo de g que é igual ao neutro do grupo. Se G é um grupo cíclico $\exists g \in G$, tal que, $G =< g >$.

Portanto, $o(g) = |G|$, isto é, a ordem do elemento g e a ordem do grupo G são iguais. Dizer que $< g >$ possui uma estrutura simples, significa, entre outras coisas, que todo elemento do grupo pode ser representado por uma potência do gerador g. Como vimos, propriedades como esta, permite obter resultados do tipo $< g >$ é um grupo abeliano, ou a proposição acima. A seguir vamos mostrar o teorema de Lagrange, para os grupos cíclicos finitos, utilizando, basicamente, esta propriedade estrutural. Para isso precisamos de mais alguns resultados.

Se G é um grupo finito, e $x \in G$, a ordem do subgrupo $< x >$ é a ordem do elemento x. Se supomos que esse grupo G é cíclico, a determinação da ordem de x depende somente da ordem do gerador de G e da potência que representa x em termos desse gerador, mais precisamente, temos o seguinte lema.

Lema 3.3.22. *Seja $< g >$ um grupo cíclico de ordem n. Se $x \in < g >$, tal que, $x = g^i$, então*

$$o(x) = \frac{n}{mdc(n,i)} \therefore o(x) \mid n.$$

Demonstração. Sendo $x = g^i$, duas condições excludentes ocorrem para a potência i: ou $i \mid n$ ou $i \nmid n$. Se ocorre que $i|n \Rightarrow \exists q \in \mathbb{Z}/n = qi$, afirmamos que, nessas condições, $o(x) = q$; primeiramente verificamos que $x^q = (g^i)^q = g^{iq} = g^{qi} = g^n = e$, pois $n = o(g)$, sendo $n = qi$, $q = \frac{n}{i}$ é o menor inteiro positivo para o qual $(x^i)^q = e$. Se ocorre a outra condição, isto é, $i \nmid n$, sendo $i < n$, pelo lema 3.3.17 se $d = mdc(i,n)$, $k = \frac{i}{d} \neq 1$ é o menor inteiro, tal que $i \mid kn$, portanto $kn = qi$, diante disso, afirmamos que $o(x) = q$, pois $x^q = (g^i)^q = g^{qi} = g^{kn} = (g^k)^n = e$, pois $g^k \in G$, $o(G) = n \therefore (g^k)^n = e$. Mostramos que $q = \frac{kn}{i} = \frac{n}{d} = \frac{n}{mdc(n,i)}$, e a minimalidade de k, garante que q é o menor inteiro, cujo $x^q = e$, portanto $o(x) = q$. Da relação obtida, $n = mdc(n,i)o(x) \therefore o(x) \mid n$ □

Corolário 3.3.23. *Se G é um grupo cíclico e $H \leq G$, então $|H| \;\big|\; |G|$*

Demonstração. Se $H \leq G$, pelo teorema 3.3.21, concluímos que o subgrupo H é cíclico, portanto, gerado por algum elemento $h \in G/H =< h >$, pelo lema anterior $o(h) \mid |G|$, sendo $o(h) = |H|$, concluímos que $|H| \;\big|\; |G|$. □

Como dissemos anteriormente, o corolário acima é válido para todo grupo finito e, mesmo para os grupos infinitos existe um resultado análogo. Este resultado é conhecido por Teorema de Lagrange. O corolário, que é o caso particular dos gupos cíclicos, permite-nos concluir a seguinte proposição, que mostra em quais condições um grupo cíclico não admite subgrupos não próprios, ou seja, os únicos subgrupos de G são $\{e\}$ e G, sendo e o neutro de G.

Teorema 3.3.24. *Seja G um grupo cíclico finito. Se $|G|$ é um número primo, então o grupo G admite somente os subgrupos não-próprios.*

Demonstração. Nas condições do teorema, seja G um grupo de ordem prima, cujo elemento neutro é e. Sendo G cíclico, se $g \in G \setminus \{e\}$, pelo lema anterior, $o(g) \mid |G|$, sendo $|G| = p$, um número primo, seus divisores são 1 ou p, mas $g \neq e$, portanto $o(g) = p = |G| \Rightarrow G$. Segundo a proposição 3.3.21, todo subgrupo $H \leq G$ é cíclico, portanto pelo corolário 3.3.23 $|H| \mid |G|$ e, pela primalidade de $|G|$, $|H| = |G| \therefore H = G$ ou $|H| = 1 \therefore H = \{e\}$, os grupos impróprio e trivial, respectivamente. □

Exercícios 3.3.25. *(1) Seja G o grupo de Klein, isto é, $G = \{e, a, b, c\}$, em que e é o elemento neutro e $o(a) = o(b) = o(c) = 2$. Prove que o grupo de Klein não é um grupo cíclico.*

(2) Seja $G = \{f, g, u, v, m, n\}$ o conjunto das funções bijetoras sobre $\{a, i, r\}$.

a) *Mostre que $G = \{\{(a,a),(i,i),(r,r)\},\{(a,a),(i,r),(r,i)\},\{(a,i),(i,a),(r,r)\},$ $\{(a,i),(i,r),(r,a)\},\{(a,r),(i,i),(r,a)\},\{(a,r),(i,a),(r,i)\}\}$;*

b) *Seja $\circ$:$G \times G \to G$, a relação binária de composição de funções. Construa a tábua da relação e explique se $\circ$ é uma operação binária?*

c) *Prove que $\{G, \circ\}$ é um grupo, sabendo-se que a operação binária de composição de funções é associativa;*

d) *Determine $|G|$ e explique se $\{G, \circ\}$ é abeliano.*

e) *G é um grupo cíclico?*

(3) Seja $G = \{0, 1, 2, 3, 4, 5\}$ e $+mod6 : G \times G \to G$, tal que, $+mod(i, j) = (i + J)mod6$, o resto da divisão de $i + j$ por 6.

a) *Construa a tábua da operação e explique se é operação binária*

b) *Mostre que $\{G, +mod6\}$ é um grupo;*

c) *Determine $|G|$ e verifique se é um grupo abeliano?*

d) *G é um grupo cíclico*

(4) Compare a estrutura de $\{G, +mod6\}$ e $\{G, \circ\}$, dos exercícios anteriores. item Prove que subgrupos de grupos cíclicos são cíclicos.

(5) Prove que todo grupo cíclico é abeliano. È verdade que todo grupo abeliano é cíclico? Se for o caso, dê um exemplo de um grupo que seja abeliano, porém não seja cíclico.

(6) Mostre que se um elemento g tem ordem 2, então, $g = g^{-1}$. Reciprocamente, se um elemento $g = g^{-1}$, então $o(g) = 2$.

(7) Seja g um elemento de ordem n, calcule g^{-1}, em função de g e n.

(8) Para o grupo S_3, determine a ordem de seus elementos.

(9) *Mostre que os grupos de ordem* $1; 2$ *e* 3 *são grupos cíclicos.*

(10) *Seja* g *um elemento de um grupo* G*. Se* $g^m = e$*, podemos afirmar que* $o(g) = m$*?*

(11) *Seja* $o(g) = n$ *e* $m|n$*, um divisor de* n*. Se* $n = km$*, mostre que se* $x = g^m$ *então* $x^k = e$*; se* $y = g^k$ *então* $y^m = e$*. Nesse caso, podemos afirmar que* $o(x) = k$ *e* $o(y) = m$*?*

(12) *Seja* $o(g) = n$*. Prove que* $x^n = e, \forall x \in < g >$*.*

(13) *Determine o grupo multiplicativo gerado pela unidade imaginária dos números complexos.*

(14) *Seja em* C*, o conjunto dos números complexos,*$x^5 = 1$*, a raiz quinta da unidade. Determine o grupo multiplicativo gerado por* x*.*

(15) *Mostre que* S_3 *não é um grupo cíclico.*

(16) *Verifique que* $Z, +$ *é um grupo cíclico gerado por* 1 *e infinito.*

(17) *Verifique que* $n\mathbb{Z} = nj, talque, j \in \mathbb{Z}$ *é um grupo aditivo. Mostre que o grupo cíclico aditivo gerado por* n *é igual ao grupo* $n\mathbb{Z}$*, isto é,* $n\mathbb{Z} = < n >, +$*.*

(18) *Seja* G *um grupo, tal que todo elemento de* G *tenha ordem* 2*. Mostre que* G *é um grupo abeliano.*

(19) *Mostre que se* G *é um grupo abeliano, então* $\forall g, h \in G$ *e* $n \in \mathbb{Z}, (gh)^n = g^n h^n$*.*

(20) *Seja* G *um grupo abeliano. Mostre que* $\forall g, h \in G$*, se* $o(g) = m$ *e* $o(h) = n$*, então* $o(gh) = MMC(m, n)$*, o mínimo múltiplo comum entre* m *e* n*.*

(21) *Seja* G *um grupo. É correto afirmar que se existem* $g, h \in G$*,* $o(g) = m$*,* $o(h) = n$ *e* $o(gh) > MMC(m, n)$*, então* G *não é um grupo abeliano?*

(22) *É verdade que para um grupo qualquer e elementos* g, h *do grupo,* $o(gh) = o(hg)$*?*

(23) *É verdade que para um grupo qualquer e elementos* g, h *do grupo,* $o(g) = m$*,* $o(h) = n$*,* $o(gh) \geq MMC(m, n)$*?*

(24) *Verifique para cada item, se a relação dada é uma relação binária. Caso afirmativo, verifique se é uma operação binária, caso negativo verifique se é uma função. Lembre-se que se afirmativo, devemos provar a afirmação, se negativo devemos exibir um exemplo onde falha o critério verificado.*

a) $\bigcup : \wp(\{a, b, c\}) \times \wp(\{a, b, c\}) \to \wp(\{a, b, c\}); \bigcup(A, B) = A \bigcup B$

b) $* : \{1, \frac{-1+i\sqrt{3}}{2}, \frac{-1-i\sqrt{3}}{2\}}\} \times \{1, \frac{-1+I\sqrt{3}}{2}, \frac{-1-I\sqrt{3}}{2}\} \to \{1, \frac{-1+I\sqrt{3}}{2}, \frac{-1-I\sqrt{3}}{2}\}$ $*(u, v) = uv$*, o produto usual, sendo* $\sqrt{-1} = i$ *, a unidade imaginária;*

c) $\div : \{1,2\} \times \{1,2\} \to \{1,2\}; \div(x,y) = x \div y$, *a divisão usual.*

(25) Seja G um grupo. Sabendo-se que $\forall g \in G, o(g) \mid |G|$, isto é, a ordem de qualquer elemento do grupo é um número que divide a ordem do G. Prove que se G é um grupo com 5 elementos, então:

a) *G é um grupo cíclico;*

b) *Os únicos subgrupos de G são $\{e\}$ e G, sendo e o elementos neutro do grupo.*

c) *Generalize este resultado para todo grupo cuja ordem é um número primo.*

(26) Seja $\{G, *\}$ o grupo definido pelos elementos

$$G = \{1,2,3,4,6,7,8,9,11,12,13,14,16,17,18,19,21,22,23,24\}$$

cuja operação $*(m,n) = (mn)mod_{25}$, o produto usual, módulo 25.

a) *Determine a ordem dos elementos 6 e 7;*

b) *Sabendo-se que $o(4) = 10$, mostre que G é um grupo cíclico gerado pelo 2, isto é, $G =< 2 >$;*

c) *Determine os subgrupos de G, que são gerados pelos elementos 6 e 7, isto é, $< 6 >$ e $< 7 >$;*

d) *Mostre que G admite um elemento de ordem 2, em seguida mostre qual é esse elemento.*

(27) Seja G o grupo de Klein, isto é, $G = \{e, a, b, c\}$, em que e é o elemento neutro e $o(a) = o(b) = o(c) = 2$. Prove que o grupo de Klein não é um grupo cíclico.

(28) (ou7ou8) Seja $G =< g >$, cuja ordem de g é 20. Se H é um subgrupo de G e $|H|$ denota a ordem de H, isto é, o número de elementos de H. Determine:

a) *Os possíveis valores de H;*

b) *Os elementos, como potências de g, de um subgrupo H de G, cuja ordem seja 4 e 10.*

(29) Prove que se $G =< g >$, então G é um grupo abeliano.

(30) Verifique que o grupo $G =< 4 >$ com a operação do produto módulo 25 é um grupo abeliano.

(31) Mostre que os números são todos escritos como alguma potência de 2 módulo 25.

(32) Calcule a ordem de 12 no grupo cíclico gerado por 1, com a operação soma módulo 30. Determine $< 12 >$, grupo cíclico gerado por 12, com essa operação.

(33) Dê exemplo de um grupo cíclico aditivo com 12 elementos, um grupo cíclico multiplicativo com 4 elementos e um grupo que não seja cíclico.

(34) Seja $G =< g >$, cuja ordem de g é 20. Se H é um subgrupo de G e $|H|$ denota a ordem de H, isto é, o número de elementos de H. Determine:

a) *Os possíveis valores de $|H|$;*

b) *Os elementos, como potências de g, de um subgrupo H de G, cuja ordem seja 4 e 10.*

(35) Prove que se $G =< g >$, então G é um grupo abeliano.

(36) Abaixo é dada a tábua do grupo $G = \{\{a, b, c, d, e, f, g, h, i, j, k, l\}, *\}$:

$*$	a	b	c	d	e	f	g	h	i	j	k	l
a	a	b	c	d	e	f	g	h	i	j	k	l
b	b	a	f	e	d	c	h	g	l	k	j	i
c	c	e	a	f	b	d	i	k	g	l	h	j
d	d	f	e	a	c	b	j	l	k	g	i	h
e	e	c	d	b	f	a	k	i	j	h	l	g
f	f	d	b	c	a	e	l	j	h	i	g	k
g	g	h	i	j	k	l	a	b	c	d	e	f
h	h	g	l	k	j	i	b	a	f	e	d	c
i	i	k	g	l	h	j	c	e	a	f	b	d
j	j	l	k	g	i	h	d	f	e	a	c	b
k	k	i	j	h	l	g	e	c	d	b	f	a
l	l	j	h	i	g	k	f	d	b	c	a	e

a) *Identifique o elemento neutro e determine a ordem de cada elemento;*

b) *Explique se este grupo é cíclico ou não;*

c) *Explique se existe um grupo cíclico de 4 elementos que seja subgrupo de G;*

d) *Determine um subgrupo de 4 elementos que não seja cíclico.*

(37) Verifique que o grupo $G =< 4 >$ com a operação do produto módulo 25 é um grupo abeliano.

(38) Mostre que os números são todos escritos como alguma potência de 2 módulo 25.

(39) Calcule a ordem de 12 no grupo cíclico gerado por 1, com a operação soma módulo 30. Determine $< 12 >$, grupo cíclico gerado por 12, com essa operação.

(40) Dê exemplo de um grupo cíclico aditivo com 12 elementos, um grupo cíclico multiplicativo com 4 elementos e um grupo que não seja cíclico.

(41) Seja G o grupo formado pelos números naturais de 0 a 23, cuja operação do grupo seja $+$ módulo 24.

a) *Determine o grupo H, formado pelos invertíveis do conjunto G, segundo a operação $*$ módulo 24;*

b) *Prove se H é ou não cíclico.*

(42) Seja G o grupo formado pelos elementos $\{(1,1),(-1,-1),(1,-1),(-1,1)\}$, cuja operação $*$ do grupo é dada por: $*((i,j),(m,n)) = (im,jn)$, em que im e jn denotam o produto usual.

a) *Determine o elemento identidade de G, e calcule a ordem dos elementos de G;*

b) *Determine o subgrupo de G gerado pelo elemento $(-1,-1)$;*

c) *Mostre que G não é um grupo cíclico.*

(43) Verifique que os elementos invertíveis da operação $*$ módulo 9formam um grupo. Em seguida calcule a ordem de cada elemento do grupo e mostre que é um grupo cíclico. Exiba um de seu geradores.

(44) Lembrando que se G é um grupo finito e $H \leq G$, então a ordem de H divide a ordem de G, determine 2 subgrupos, não triviais, do grupo $< \frac{\sqrt{2}+i\sqrt{2}}{2} >$, sendo $i^2 = -1$ a unidade imaginária, e todos os subgrupos do grupo de Klein, $G = \{1,a,b,c/a^2 = b^2 = c^2 = 1\}$

(45) Seja G o grupo formado pelos elementos $\{1,-1,i,-i,j,-j,k,-k\}$, tal que $ij = k; jk = i; ki = j; ji = -k, kj = -i; ik = -j$. Calcule as potências de i e monte a tábua do grupo, determinando a ordem de cada elemento do grupo e todos os subgrupos de G.

(46) Mostre que o menor grupo não cíclico é o grupo de Klein.

(47) Dê exemplo de um grupo cuja operação binária não seja comutativa.

(48) Mostre que se G é um grupo cíclico, então todo subgrupo de G é cíclico.

(49) Seja $\{G,*\}$ o grupo definido pelos elementos $G = \{0,1,2,3,4,6,7,8,9,11,12,13,14\}$ cuja operação $+(m,n) = (m+n)mod_{15}$, o produto usual, módulo 15.

a) *Determine a ordem dos elementos 6 e 7;*

b) *Mostre que G é um grupo cíclico gerado pelo 2, isto é, $G =< 2 >$;*

c) *Determine os subgrupos de G, que são gerados pelos elementos 6 e 7, isto é, $< 6 >$ e $< 7 >$;*

d) *Mostre que G não admite um elemento de ordem 2, mas admite um elemento de ordem 3. Em seguida determine esse elemento.*

(50) Seja $G =< g >$, cuja ordem de g é 24. Se H é um subgrupo de G e $|H|$ denota a ordem de H, isto é, o número de elementos de H. Determine:

a) *Os possíveis valores de H;*

b) *Os elementos, como potências de g, de um subgrupo H de G, cuja ordem seja 6.*

c) *Um subgrupo de G de ordem 4;*

d) *O grupo de Klein pode ser subgrupo de G? Justifique.*

(51) Seja G um grupo qualquer e $h \in G$. Prove que o conjunto $C(h) = \{g \in G / gh = hg\}$ é um subgrupo de G.

3.3.4 O Grupo das permutações e o Grupo dihedral

Um grupo de fundamental importância em teoria de grupos é o grupo de permutações, tanto abstratamente quanto pela riqueza de exemplos. Este último motivo, é uma conseqüência natural de uma propriedade do grupo de permutações, conhecida por Teorema de Cayley. Essencialmente, este teorema afirma que todo grupo finito é isomorfo a um subgrupo de algum grupo de permutações.

Nos exemplos anteriores, vimos que o conjunto das funções bijetoras sobre o conjunto $\{1, 2, 3\}$, com a operação de composição de funções, é um grupo. Este grupo é o grupo de permutações de 3 elementos, e qualquer função bijetora sobre o conjunto $\{1, 2, 3\}$ é uma permutação desse conjunto, tal função permuta estes elementos.

Definição 3.3.26. *Seja X um conjunto não vazio e $f : X \to X$ uma função em X. Dizemos que f é uma permutação de X se f é uma função injetora.*

A partir daqui vamos considerar permutações sobre conjuntos finitos X, cujos elementos são os $|X|$ primeiros inteiros positivos. A partir do conjunto X, podemos construir o conjuntos de todas as permutações de X que representamos por S_n, em que $n = |X|$ denota o número de elementos do conjunto. A seguinte definição deixa precisa esta idéia.

Definição 3.3.27. *Seja $X = \{1, 2, 3, \cdots, n\}$ o conjunto dos n números inteiros positivos e consecutivos, a partir de 1. Dada uma função $\alpha : X \to X$ bijetora, dizemos que α é uma permutação de X. Seja S_n o conjunto de todas as permutações sobre o conjunto X e $\circ : S_n \times S_n \to S_n$ a operação binária de composição de função. O conjunto $\{S_n, \circ\}$ é um grupo, denominado grupo das permutações dos n primeiros inteiros positivos.*

Proposição 3.3.28. *Seja n um inteiro positivo, S_n o conjunto de todas as permutações sobre o conjunto $X = \{1, 2, \cdots, n\}$ e $\circ : S_n \times S_n \to S_n$ a relação binária de composição de função. O conjunto $\{S_n, \circ\}$ é um grupo de ordem $n!$.*

Demonstração. Inicialmente devemos provar que a relação binária é uma operação binária. Isso decorre do fato que a composição de funções injetoras é uma função injetora, de fato, se

f, g são funções injetoras sobre X, então $f \circ g$ é uma função sobre X; basta provar que se $f(g(x)) = y$ e $f(g(z)) = y$ então $x = z$, da igualdade temos $f(g(x)) = f(g(z))$, sendo f uma função injetora, ela preserva igualdades, portanto $g(x) = g(z)$, sendo g injetora o mesmo ocorre, logo $x = z$, portanto $f \circ g$ é injetora e analogamente $g \circ f$ é injetora, portanto $f \circ g$ e $g \circ f$ são permutações de X, logo $f \circ g, g \circ f \in S_n$, isto é, $\circ$ é uma operação binária. Devemos provar que $\circ$ é associativa: ou seja $(f \circ g) \circ h = f \circ (g \circ h)$, este fato é geral para a composição de funções, vamos prová-lo para relembrar a propriedade associativa: seja $x \in X$, $(f \circ g) \circ h(x) \doteq (f \circ g)(h(x))$, $h(x) \in X \therefore h(x) = y \in X$, então $(f \circ g)(h(x)) = f \circ g(y) \doteq f(g(y)) = f(g(h(x)))$, por definição $g(h(x)) = g \circ h(x)$, se denominamos a função $g \circ h = \alpha$, teremos $g(h(x)) = \alpha(x)$, logo $f(g(h(x))) = f(\alpha(x)) \doteq f \circ \alpha(x) = f \circ (g \circ h)(x)$, logo $(f \circ g) \circ h(x) = f(g(h(x))) = f \circ (g \circ h)(x)$, $\forall x \in X$, logo $(f \circ g) \circ h = f \circ (g \circ h)$ e portanto ocorre a propriedade associativa. Como vimos a função Id_X, função identidade em X, é o neutro, segundo a operação binária de composição de funções, logo satisfaz a propriedade de existência do elemento neutro; toda função bijetora admite inverso segundo a operação de composição: a propriedade do inverso. Logo $\{S_n, \circ\}$ é um grupo, cuja ordem é $n!$, como visto no teorema 1.3.19. □

Exemplo 3.3.29. *(1) O grupo de permutações de* 1 *elemento é o conjunto unitário da função identidade* $e : \{1\} \to \{1\}$*, que é um grupo de ordem* 1

(2) O grupo de permutações de 2 *elementos é o conjunto das funções* $e, a : \{1, 2\} \to \{1, 2\}$*, sendo* e *a função identidade e* $a(1) = 2; a(2) = 1$*.*

(3) O grupo de permutações de 6 *elementos tem* $6! = 720$ *elementos, sendo* $e(1) = 1; e(2) = 2; ...; e(6) = 6$*, a função identidade, o neutro desse conjunto.*

A notação utilizada para o grupo de permutações S_n é porque este grupo também é denominado de grupo das simetrias de grau n. O grupo S_n é estudado no contexto da teoria de representação de grupos e muitos resultados importantes em teoria dos grupos são obtidos segundo o método de representação de grupos. Nossa abordagem aqui, restringe-se a algumas observações sobre este grupo, a notação utilizada e as operações, que a partir dessa notação ficam mais simples. Portanto, os conceitos de composição de funções são pré-requisito básico para estudo do S_n.

A ordem do grupo S_n, corresponde ao número de funções bijetoras sobre um conjunto com n elementos, portanto $S_n = n!$. Consideremos o grupo S_4, e $\alpha \in S_4$ a permutação: $\alpha(1) = 2; \alpha(2) = 1; \alpha(3) = 4; \alpha(4) = 3$, α é uma função bijetora sobre o conjunto $\{1, 2, 3, 4\}$. Se consideramos outra permutação $\beta \in S_4$, essa pemutação fica determinada de modo análogo ao de α, isto é, definindo para cada elemento do domínio a sua imagem, ou seja, $\beta(1) = 4; \beta(2) = 3; \beta(3) = 2; \beta(4) = 1$, e assim ocorre com qualquer elemento de S_n. O fato de, para um grupo de permutações, considerarmos funções sobre um mesmo domínio, permite notações mais simplificadas, de modo

que as permutações α, β são também denotadas por:

$$\alpha = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{pmatrix}; \beta = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 3 & 2 & 1 \end{pmatrix},$$

e dizemos, por exemplo, para permutação β, que 1 é levado em 4, 2 é levado em 3, e assim sucesivamente. Tal notação é econômica, pois permite identificar cada permutação com um único sinal de igualdade. No entanto, não somente a escrita é sintética, como também as operações entre as pemutações são simplificadas.

Sendo $\alpha, \beta \in S_4$, um grupo, $\alpha \circ \beta \in S_4$, seja tal permutação identificada por $\mu = \alpha \circ \beta$; de acordo com a definição de composição de funções, a função μ está determinada por $\mu(i) = \alpha(\beta(i))$, ou seja $\mu(1) = \alpha(\beta(1)) = \alpha(4) = 3$, esta mesma operação pode ser feita, segundo a notação anterior, por:

$$\alpha\beta = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 3 & 2 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 1 & 2 \end{pmatrix} \text{ pois fazemos: } \begin{array}{l} 1 \to 4 \to 3 \therefore 1 \to 3 \\ 2 \to 3 \to 4 \therefore 2 \to 4 \\ 3 \to 2 \to 1 \therefore 3 \to 1 \\ 4 \to 1 \to 2 \therefore 4 \to 2 \end{array};$$

e determinamos a permutação μ. Podemos observar que, quando calculamos pela definição $\mu(2) = \alpha(\beta(2)) = \alpha(1) = 4$, estamos realizando a seguinte seqüência de associações: $2 \to 1 \to 4$, que compõe a associação $2 \to 4$, que representa a imagem $\mu(2) = 4$. Devemos atentar que as associações são feitas partindo-se da última permutação, para a primeira, pois essa é a convenção a partir de nossa definição de composição de funções. O leitor interessado deve consultar outras notações de composição de funções, basicamente utilizadas em livros escritos em inglês.

Para a permutação $\alpha \in S_4$, é natural perguntarmo-nos qual é o inverso de α. No caso das pemutações, como função bijetora, seu inverso é dado diretamente pela definição de função inversa, isto é, $\alpha(i) = j \Leftrightarrow \alpha^{-1}(j) = i$. Utilizando a notação anterior, os inversos são obtidos diretamente:

$$\alpha = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{pmatrix} \Leftrightarrow \alpha^{-1} = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{pmatrix}; \tau = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 1 & 4 & 2 \end{pmatrix} \Leftrightarrow \tau^{-1} = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 4 & 1 & 3 \end{pmatrix}$$

A permutação α acima é igual a seu inverso, portanto $o(\alpha) = 2$. A seguir apresentamos alguns exemplos de produto, para cálculo da ordem de uma permutação

Exemplo 3.3.30. *(1) Se* $\alpha = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 4 & 5 & 1 & 3 \end{pmatrix}$ *é uma permutação de* S_5*, a ordem de* α *é calculada pelas potências:*

$$\alpha^2 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 4 & 5 & 1 & 3 \end{pmatrix}\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 4 & 5 & 1 & 3 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 4 & 1 & 3 & 2 & 5 \end{pmatrix};$$
$$\alpha^3 = \alpha^2\alpha = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 4 & 1 & 3 & 2 & 5 \end{pmatrix}\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 4 & 5 & 1 & 3 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 2 & 5 & 4 & 3 \end{pmatrix};$$
$$\alpha^4 = \alpha^3\alpha = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 2 & 5 & 4 & 3 \end{pmatrix}\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 4 & 5 & 1 & 3 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 4 & 3 & 1 & 5 \end{pmatrix};$$
$$\alpha^5 = \alpha^4\alpha = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 4 & 3 & 1 & 5 \end{pmatrix}\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 4 & 5 & 1 & 3 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 4 & 1 & 5 & 4 & 3 \end{pmatrix};$$
$$\alpha^6 = \alpha^5\alpha = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 4 & 1 & 5 & 2 & 3 \end{pmatrix}\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 4 & 5 & 1 & 3 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 2 & 3 & 4 & 5 \end{pmatrix} = e,$$

portanto $o(\alpha) = 6$*;*

(2) Se o produto dos elementos abaixo são pemutações do S_6*:*

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 3 & 4 & 5 & 6 & 1 & 2 \end{pmatrix}\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 3 & 4 & 5 & 6 & 1 \end{pmatrix}\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 5 & 1 & 6 & 2 & 4 & 3 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 4 & 3 & 5 & 1 & 6 \end{pmatrix}$$

(3) O grupo S_4*, é não abeliano, pois*

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

observamos que o primeiro produto fixa o número $3(3 \to 1 \to 3)$*, enquanto o segundo produto fixa o número* $1(1 \to 3 \to 1)$*.*

Exercícios 3.3.31.

3.3.5 Órbitas e O Ciclo de uma Permutação

O grupo S_n é uma fonte importante de exemplos para a teoria de grupos. Acima apresentamos uma notação que simplifica as operações do grupo, aqui nos referimos àquela notação por *notação funcional*. A seguir definimos o conceito de ciclo, que sintetiza mais ainda a notação de uma permutação. Embora essa notação seja natural, sua definição exige a seguinte proposição.

Lema 3.3.32. *Seja* $n \in \mathbb{Z}^+$ *e* S_n *o grupo de permutações dos* n *primeiros números inteiros positivos. Para qualquer permutação* $\alpha \in S_n$*, a relação*

$$C_\alpha : \{1, 2, \cdots, n-1, n\} \to \{1, 2, \cdots, n-1, n\}$$
$$C_\alpha(a) = b, \text{ se } \exists k \in \mathbb{Z}, |k| \leq o(\alpha) \text{ a ordem de } \alpha, \text{ tal que, } \alpha^k(a) = b.$$

É uma relação de equivalência.

Demonstração. Basta verificar que a relação C_α satisfaz as propriedades: 1) reflexiva, 2) simétrica e 3) transitiva. Assim ocorre, pois se $k = o(\alpha) \Rightarrow \alpha^k = I$ o neutro de S_n (a função identidade), portanto $\alpha^k(a) = a \therefore a \mapsto a$; se $a \mapsto b$, isto é, $\alpha^k(a) = b$, para algum inteiro k, tal que, $|k| \leq o(\alpha)$, sendo $\alpha \in S_n$, em que S_n é um grupo, existe o inverso de α e $\alpha^{-k}(b) = a \therefore b \mapsto a$, e a relação é simétrica; finalmente, seja $a \mapsto b$ e $b \mapsto c$, sejam $\alpha^k(a) = b; \alpha^l(b) = c$ então $c = \alpha^l(b) = \alpha^l(\alpha^k(a)) = \alpha^{l+k}(a)$, pelo teorema da divisão, $l + k = q(o(\alpha)) + r, 0 \leq r < o(\alpha)$, portanto $\alpha^r(a) = c \therefore a \mapsto c$, ocorre a transitividade, logo C_α é uma relação de equivalência. □

De acordo com a proposição 1.3.14, toda relação de equivalência em um conjunto A, define uma partição do conjunto A. Seja n um inteiro positivo; a relação de equivalência R_α, sendo α uma permutação de S_n, define portanto uma partição $P_\alpha \subset \wp(\{1, \cdots, n\})$. Ocorre que $P_\alpha = P_\beta$ não implica que $\alpha = \beta$, por exemplo, se $\alpha, \beta \in S_4$, tal que, $\alpha = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 2 & 4 & 1 \end{pmatrix}$ e $\beta = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 2 & 1 & 3 \end{pmatrix}$, $P_\alpha = \{\{1,3,4\},\{2\}\} = P_\beta = \{\{1,4,3\},\{2\}\}$, embora $\alpha(1) \neq \beta(1)$, isto é, $\alpha \neq \beta$.

A seguinte definição permite associar a cada permutação α, do grupo de simetrias dos n primeiros inteiros positivos, uma única representação a partir da partição P_α.

Definição 3.3.33. *Seja n um inteiro positivo e S_n o grupo de simetrias dos inteiros positivos menores ou iguais a n. Se $\alpha \in S_n$ é uma permutação e P_α a partição associada à relação de equivalência R_α, para qualquer inteiro $1 \leq i \leq n$, associamos o objeto*

$$\begin{pmatrix} i & \alpha(i) & \alpha^2(i) & \cdots & \alpha^k(i) \end{pmatrix},$$

uma matriz linha denominada órbita de i, sendo $k = |X| - 1$, tal que, $X \in P_\alpha$, e $i \in X$. A cada elemento $X \in P_\alpha$ e $i \in X$, associamos a órbita de i. A justaposição de todas as órbitas assim obtidas, uma e somente uma para cada elemento da partição, é denominada ciclo da pemutação α, isto é, se $P_\alpha = \{X_1, X_2, \cdots, X_m\}$, então

$$\begin{pmatrix} i_1 & \alpha(i_1) & \alpha^2(i_1) & \cdots & \alpha^k(i_1) \end{pmatrix}\begin{pmatrix} i_2 & \alpha(i_2) & \alpha^2(i_2) & \cdots & \alpha^k(i_2) \end{pmatrix}\cdots\begin{pmatrix} i_m & \alpha(i_m) & \alpha^2(i_m) & \cdots & \alpha^k(i_m) \end{pmatrix}$$

Observamos que esta definição, à primeira vista, possa parecer muito abstrata, no entanto os exemplos podem mostrar que se trata de uma representação natural de uma permutação. Além disso, como veremos a seguir, há uma simplificação tanto para denotar a pemutação, quanto para fazer operações com as mesmas. Sugerimos ao leitor, após familiarizar-se com a noção de ciclo, que retome a definição acima e, para algumas permutações, construa os ciclos associados a esta, segundo a definição.

Enfatizamos, no entanto, o caso quando, para uma permutação α e $X \in P_\alpha$, é um conjunto unitário, isto é, $|X| = 1$, então o ciclo correspondente à órbita dos elementos de X, tem apenas um elemento, digamos $x \in X$. Isso significa que este elemento fica fixado pela permutação α, isto

é, $\alpha(x) = x$. Assim, os elementos que estão fixados por uma dada permutação não aparecem nos ciclos, o que equivale a dizer que se um dado elemento não aparece nos ciclos de uma permutação, este elemento está fixado.

Vimos que à relação de equivalência, apresentada na proposição anterior, permutações distintas podem resultar em uma mesma partição. A definição acima, no entanto, garante que permutações distintas estão associadas a ciclos distintos, ou seja, existe unicidade na decomposição de uma permutação em ciclos, e portanto essa representação caracteriza a permutação, isto é, cada pemutação está associada a uma única representação em ciclos e uma representação em ciclos determina uma única permutação. A proposição seguinte testemunha este fato.

Proposição 3.3.34. *Seja α uma permutação do grupo S_n. Então, nas condições da definição 3.3.33*

$$\alpha = \begin{pmatrix} i_1 & \alpha(i_1) & \alpha^2(i_1) & \cdots & \alpha^k(i_1) \end{pmatrix} \begin{pmatrix} i_2 & \alpha(i_2) & \alpha^2(i_2) & \cdots & \alpha^k(i_2) \end{pmatrix} \cdots \begin{pmatrix} i_m & \alpha(i_m) & \alpha^2(i_m) & \cdots & \alpha^k(i_m) \end{pmatrix}.$$

A justaposição das órbitas da permutação α, que como conjuntos são disjuntos. E reciprocamente, dado um ciclo:

$$\begin{pmatrix} i_1 & i_2 & i_3 & \cdots & i_{k_1} \end{pmatrix} \cdots \begin{pmatrix} j_1 & j_2 & j_3 & \cdots & j_{k_m} \end{pmatrix}, x_y \in \mathbb{Z}^+.$$

Fica determinada uma única permutação α, nas condições da definição 3.3.34.

Demonstração. Seja $\alpha \in S_n$, de acordo com o lema 3.3.32, determinamos a partição P_α associada a relação de equivalência C_α, sendo n finito, $m = |P_\alpha| \leq n$, isto é, a partição tem no máximo n elementos. Para cada elemento $X \in P_\alpha$, determinamos a órbita de algum elemento $x \in X$. A Justaposição de todas essas órbitas é o ciclo da permutação α, vamos mostrar que todas as imagens de α estão representadas no ciclo da permutação, na forma $\alpha(j) = i$ com $1 \leq i, j \leq n$, sendo α uma função bijetora, o ciclo a determina univocamente. De fato! Seja $1 \leq i \leq n$, sendo i um elemento do domínio da relação C_α, $\exists A \in P_\alpha$, tal que $i \in A$, seja $a \in A$ e $\mathcal{O}(a)$ a órbita de a, então $i = \alpha^q(a)$ para algum $1 \leq q \leq |A| - 1$. Se $|A| = 1$, então i está fixado pela permutação $\alpha \therefore \alpha(i) = i$, senão $\alpha^{q-1}(a) = j$ tal que $1 \leq j \leq n$ $\therefore \alpha(j) = \alpha(\alpha^{q-1})(a) = \alpha^{1+q-1}(a) = \alpha^q(a) = i$, portanto α está representada no ciclo, para todo elemento de seu domínio, o que determina α de maneira única. Cada órbita do ciclo é formada pelos elementos de uma classe da relação de equivalência 3.3.32, que como conjuntos são disjuntos. Reciprocamente, dado um ciclo, seja n o maior inteiro não fixado pelo ciclo, isto é, o maior inteiro das órbitas do ciclo, definimos $\alpha : \{1, 2, \cdots, n\} \longrightarrow \{1, \cdots, n\}$ a seguinte aplicação: $\alpha(i) = i$ se i não aparece em alguma órbita do ciclo; $\alpha(i) = j$ se i aparece em uma das órbitas do ciclo, sendo j o elemento da órbita de i que aparece imediatamente à direita de i, ou o primeiro elemento da órbita de i, se i for o último elemento dessa órbita. A relação α é uma função: ocorre ou que i não aparece em qualquer das órbitas, ou cada i está em uma única órbita e aparece uma única vez, logo tem um único elemento à direita, ou na primeira

posição, dependendo do caso, esta mesma condição garante que α é injetora, portanto é uma permutação, ou seja $\alpha \in S_n$. □

A proposição acima garante que dada uma permutação α podemos representá-la segundo a definição anterior em forma de um ciclo, reciprocamente, o ciclo caracteriza uma permutação, isto é, dado um conjunto de órbitas disjuntas e justapostas, existe uma única permutação associada e este ciclo.

Exemplo 3.3.35. *(1) Se $e \in S_n$ é o elemento neutro, então o ciclo correspondente é*

$$e = \begin{pmatrix} 1 \end{pmatrix}\begin{pmatrix} 2 \end{pmatrix}\cdots\begin{pmatrix} n-1 \end{pmatrix}\begin{pmatrix} n \end{pmatrix}$$

ou seja todos os elementos estão fixados, nesse caso, como não há ambigüidade, a identidade não é expressa na forma de ciclos, sendo denotada simplesmente por e;

(2) Seja $\alpha \in S_3$, a permutação $\alpha(1) = 3; \alpha(2) = 2; \alpha(3) = 1$, então $\alpha = \begin{pmatrix} 1 & 3 \end{pmatrix}$

(3) Seja $\alpha \in S_8$, dada por $\alpha = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 1 & 7 & 5 & 6 & 2 & 8 & 3 & 4 \end{pmatrix}$, cujo ciclo é:

$$\alpha = \begin{pmatrix} 2 & 7 & 3 & 5 \end{pmatrix}\begin{pmatrix} 4 & 6 & 8 \end{pmatrix}$$

(4) Se $\alpha \in S_6$ é representada pelo ciclo $\alpha = \begin{pmatrix} 1 & 5 \end{pmatrix}\begin{pmatrix} 3 & 6 \end{pmatrix}$, então $\alpha(1) = 5; \alpha(2) = 2; \alpha(3) = 6; \alpha(4) = 4; \alpha(5) = 1; \alpha(6) = 3$ fica univocamente, de modo único, determinada;

(5) Se $\alpha \in S_5$ é o ciclo $\alpha = \begin{pmatrix} 1 & 5 & 3 & 4 & 2 \end{pmatrix}$, então $\alpha = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 5 & 1 & 4 & 2 & 3 \end{pmatrix}$

(6) Se $\alpha \in S_5$, o ciclo $\alpha = \begin{pmatrix} 4 & 2 & 1 & 5 & 3 \end{pmatrix}$, define a mesma permutação do exemplo anterior, pois, de acordo com a definição os ciclos são formados por órbitas, e cada órbita, como elemento de uma partição é fixada, unicamente, a partir dos elementos que a compõem. Observe que nos dois casos temos:

$$1 \mapsto 5; 5 \mapsto 3; 3 \mapsto 4; 4 \mapsto 2; 2 \mapsto 1$$

ciclicamente.

Teorema 3.3.36. *Se $\alpha, \beta \in S_n$ são ciclos disjuntos, isto é, os elementos que não estão fixados por α devem estar fixados por β e vice-versa, então $\alpha\beta = \beta\alpha$.*

Demonstração. Seja $1 \leq i \leq n$, devemos mostrar que $\alpha\beta(i) = \beta\alpha(i)$; se i está fixado por α e β, isto é $\alpha(i) = i = \beta(i)$, então $\alpha(\beta(i)) = \alpha(i) = i = \beta(\alpha(i))$; se i não é fixado por α, então $\alpha(i) = j \neq i$, j está na órbita de i, logo necessariamente j também não é fixado por α, como os ciclos são disjuntos i, j devem estar fixados por β, ou seja, $\beta(i) = i$ e $\beta(j) = j$, portanto

$\alpha(\beta(i)) = \alpha(i) = j$, e também $\beta(\alpha(i)) = \beta(j) = j$. Analogamente ocorre para o caso em que β não fixa i, portanto $\alpha(i) = i$ e a conclusão é a mesma. Sendo estas as únicas possibilidades $\forall i, 1 \leq i \leq n$, logo $\alpha\beta = \beta\alpha$ e os ciclos comutam. □

Corolário 3.3.37. *Se uma permutação α está escrita como um ciclo, cada órbita é disjunta, portanto comuta com as demais órbitas.*

Exemplo 3.3.38. *(1) Sejam os ciclos $\alpha = (138)(257)$ e $\beta = (46)$, então $\alpha\beta = (138)(257)(46) = (46)(138)(257) = \beta\alpha$*

(2) A pemutação $\alpha = (157)(2435)$ não é um ciclo, pois as órbitas não são disjuntas;

(3) a expressão $(123258)(746)$ não representa uma permutação, segundo as notações discutidas até aqui, pois o primeiro termo desta não é uma órbita;

(4) O ciclo $\alpha = (359)(12467)$ pode ser escrito de várias formas, entres elas: $\alpha = (12467)(359) = (46712)(359) = (935)(12467) = (46712)(935)$;

(5) as permutações $\alpha = (13456)(872)$ e $\beta = (45631)(872)$ são ciclos, porém distintos pois têm órbitas diferentes, em α a primeira órbita indica que $6 \mapsto 1$, enquanto em β uma das órbitas indica $6 \mapsto 3$, ou seja $\alpha(6) = 1 \neq 3 = \beta(6)$, portanto $\alpha \neq \beta$, embora como conjunto as órbitas sejam as mesmas.

(6) Se $\alpha = (135)(7248)$ e $\beta = (531)(2784)$, o produto

$$\alpha\beta = (135)(7248)(531)(2784) \neq \beta\alpha = (531)(2784)(135)(7248)$$

pois as órbitas permutadas não são disjuntas, embora

$$\alpha\beta = (135)(7248)(531)(2784) = (135)(531)(7248)((2784),$$

pois as órbitas que foram permutadas são disjuntas. Além disso, tanto $\alpha\beta$ quanto $\beta\alpha$ não são ciclos.

Nos exemplos (2) e (6), vimos permutações escritas como justaposição de órbitas, que não são ciclos, pois não ocorre de serem órbitas disjuntas. A diferença entre uma permutação escrita na forma de ciclo e os exemplos citados, é que dado um ciclo, a pemutação fica univocamente determinada, como visto na proposição 3.3.34, porém no exemplo (2) ocorre $1 \to 5$ e $3 \to 5$, que violaria a condição de injetividade da permutação. Veremos que neste caso trata-se do produto de dois ciclos, ou seja o produto de duas permutações, digamos $\lambda = (157)$ e $\mu = (2435)$. Como vimos, no final da seção anterior, podemos calcular o produto $\lambda\mu$ que é uma permutação, digamos $\sigma = \lambda\mu$, por exemplo na forma de composição de funções, isto é $\sigma(i) = \lambda\mu(i) = \lambda(\mu(i))$, assim $\sigma(3) = \lambda(\mu(3)) = \lambda(5) = 7$. Procedendo-se dessa forma e supondo que $\lambda, \mu, \sigma \in S_8$, determinamos $\sigma = (152437)$, verifique. A seguir discutimos a operação entre ciclos não disjuntos.

Se α e β são dois ciclos não disjuntos, devemos fazer as operações entre as órbitas que, como vimos na proposição 3.3.34, representam permutações e portanto podemos fazer o produto usual duas a duas, reduzindo cada par de órbitas em permutações, eventualmente sobrando uma órbita, quando o número de órbitas for ímpar, que por si mesma é uma permutação. Teremos o produto de permutações, que sendo uma permutação, pela proposição 3.3.34 é a justaposição de órbitas disjuntas, ou seja o resultado é um ciclo. Mas como garantir que isso sempre ocorre, isto é, dadas órbitas quaiquer podemos reduzi-las a órbitas disjuntas. Este é o conteúdo do seguinte teorema, que provamos a partir da seguinte proposição:

Proposição 3.3.39. *Dadas m órbitas, com $m > 1$, o produto destas órbitas é uma permutação do grupo das simetrias S_n.*

Demonstração. Vamos utilizar indução em m o número de órbitas. Se $m = 2$, o primeiro passo de indução, cada órbita, tomada como um ciclo, pode representar uma permutação de S_n, segundo a proposição 3.3.34, sendo suficiente tomar n como o maior inteiro não fixado pelas duas órbitas. Portanto o produto é uma permutação de S_n. Supomos por hipótese de indução que o teorema vale para k órbitas, isto é, o produto de k órbitas é uma permutação de S_n para algum inteiro positivo n. Devemos provar então que o teorema será válido para $k+1$ órbitas. De fato, dadas $k+1$ órbitas, seja β a permutação associada à última órbita, que é uma pemutação de S_l, sendo l o maior inteiro não fixado da órbita de β, teremos então o produto de k órbitas, com a órbita α, **por hipótese de indução** as k órbitas é uma permutação $\alpha \in S_n$, sendo n o maior inteiro não fixado pelas k primeiras órbitas. Assim $\alpha\beta \in S_j$, sendo $j = máx\{l, n\}$, é a permutação que representa o produto de $k+1$ órbitas, logo está **provado por indução finita** que o produto de m órbitas é uma permutação de S_n. □

Teorema 3.3.40. *Seja o produto de $m > 1$ órbitas*

$$\begin{pmatrix} i_1 & i_2 & i_3 & \cdots & i_{k_1} \end{pmatrix} \cdots \begin{pmatrix} j_1 & j_2 & j_3 & \cdots & j_{k_m} \end{pmatrix}, x_y \in \mathbb{Z}^+$$

Podemos sempre escrever este produto na forma de ciclos disjuntos.

Demonstração. Pela proposição anterior o produto de m órbitas é uma permutação $\alpha \in S_n$, para algum inteiro positivo n, pela proposição 3.3.34 α é escrito na forma de ciclo, que é a justaposição de órbitas disjuntas. □

A presente seção contribui tanto para o desenvolvimento teórico do grupo de simetrias, quanto à prática para o cálculo, entre outros, do produto de duas permutações. A proposição mostra que podemos ir reduzindo as órbitas a permutações e fazer o produto dessas permutações. No entanto a realiação dessas contas fica bastante tediosa e acaba por não utilizar a notação de ciclo que estamos discutindo. Uma vez que garantimos que o produto de ciclos, vistos como órbitas,

resulta sempre em um ciclo, ou órbitas disjuntas, temos garantias que podemos manter a notação de ciclo para essas operações. Lembrando que cada ciclo pode ser associado a uma permutação e que o produto de permutações é a composição destas como função, que segundo nossa definição inverte a ordem dos cálculos, isto é, se desejamos calcular $\alpha \circ \beta(i)$, inicialmente calculamos $\beta(i) = j$ e posteriormente calculamos $\alpha(j)$, ou seja há uma inversão da ordem em que aparece os termos da composição. Assim, se desejamos efetuar o produto de m, com $m > 1$, órbitas, podemos tratar cada órbita como se fosse um ciclo, teremos então m permutações associadas a cada ciclo, determinamos n o maior inteiro não fixado pelos ciclos e calculamos, para cada inteiro i, $1 \leq i \leq n$, a composição das permutações, iniciando pela última, até chegar à primeira permutação, isto é, se $\alpha_1 \cdots \alpha_m$ são as m permutações associadas a cada ciclo, para cada i, calculamos

$$\alpha_m(i) = i_m; \alpha_{m-1}(i_m) = i_{m-1} \cdots \alpha_1(i_2) = i_1 \therefore i \mapsto i_1,$$

isto é o ciclo equivalente ao produto dos m ciclos é tal que i e i_1 estão na mesma órbita e caso sejam distintos, i_1 deve estar imediatamente à direita de i. Este mesmo processo pode ser feito, utilizando diretamente os ciclos do seguinte modo:

$$i \mapsto i_m \mapsto i_{m-1} \mapsto \cdots \mapsto i_2 \mapsto i_1 \therefore i \mapsto i_1.$$

Fazemos isso para i, $1 \leq i \leq n$, obtendo o ciclo que representa o produto. Os exemplos a seguir mostram este processo.

Exemplo 3.3.41. *(1)* $(157)(2435)$*, fazemos os cálculos para* $1 \leq i \leq 7$*,* $\alpha_1 = (157)$*,* $\alpha_2 = (2435)$*,* 1 *está fixo em* α_2*, logo* $\alpha_2(1) = 1; \alpha_1(1) = 5 \therefore 1 \mapsto 5$*, poderíamos diretamente fazer* $1 \mapsto 1 \mapsto 5 \therefore 1 \mapsto 5$*, assim sucessivamente* $2 \mapsto 4 \mapsto 4 \therefore 2 \mapsto 4$*;* $3 \mapsto 5 \mapsto 7 \therefore 3 \mapsto 7$*; os demais são feitos de forma análoga e obtemos* $4 \mapsto 3$*;* $5 \mapsto 2$*;* $6 \mapsto 6$*;* $7 \mapsto 1$*. A partir daí contruímos as órbitas* $(1524371) = (152437)$ *observe que o último elemento de qualquer órbita está sempre associado ao primeiro elemento da órbita, por isso a penúltima igualdade não é necessária. Ou seja* $(157)(2435) = (152437)$

(2) $(13456)(872)(45631)(872)$*, devemos determinar as imagens de* $1 \leq i \leq 8$*. Assim*

$$\begin{aligned}
&1 \mapsto 1 \mapsto 4 \mapsto 4 \mapsto 5 \therefore 1 \mapsto 5;\\
&2 \mapsto 8 \mapsto 8 \mapsto 7 \mapsto 7 \therefore 2 \mapsto 7;\\
&3 \mapsto 3 \mapsto 1 \mapsto 1 \mapsto 3 \therefore 3 \mapsto 3;\\
&4 \mapsto 4 \mapsto 5 \mapsto 5 \mapsto 6 \therefore 4 \mapsto 6;\\
&5 \mapsto 5 \mapsto 6 \mapsto 6 \mapsto 1 \therefore 5 \mapsto 1;\\
&6 \mapsto 6 \mapsto 3 \mapsto 3 \mapsto 4 \therefore 6 \mapsto 4;\\
&7 \mapsto 2 \mapsto 2 \mapsto 8 \mapsto 8 \therefore 7 \mapsto 8;\\
&8 \mapsto 7 \mapsto 7 \mapsto 2 \mapsto 2 \therefore 8 \mapsto 2.
\end{aligned}$$

Observe que o ciclo correspondente fixa o número 3*, podemos determinar o ciclo* $(15)(278)(46)$*, isto é* $(13456)(872)(45631)(872) = (15)(278)(46)$*, que de fato é um ciclo;*

(3) O exemplo anterior, do produto de 4 *ciclos, não é um ciclo, pois as órbitas não são disjuntas. Podemos checar que os ciclos não comutam, isto é,* $(45631)(872)(13456)(872) = (278)(35)(46) \neq (15)(278)(46) = (13456)(872)(45631)(872)$*;*

(4) $(123)(346)(6214)(1542)(245)$*, devemos avaliar* 5 *permutações nos números* $1 \leq i \leq 6$*, ou seja* 30 *atribuições:*

$$1 \mapsto 1 \mapsto 5 \mapsto 5 \mapsto 5 \mapsto 5 \therefore 1 \mapsto 5;$$
$$2 \mapsto 4 \mapsto 2 \mapsto 1 \mapsto 1 \mapsto 2 \therefore 2 \mapsto 2;$$
$$3 \mapsto 3 \mapsto 3 \mapsto 3 \mapsto 4 \mapsto 4 \therefore 3 \mapsto 4;$$
$$4 \mapsto 5 \mapsto 4 \mapsto 6 \mapsto 3 \mapsto 1 \therefore 4 \mapsto 1;$$
$$5 \mapsto 2 \mapsto 1 \mapsto 4 \mapsto 6 \mapsto 6 \therefore 5 \mapsto 6.$$

Observe que, segundo a propriedade da permutação, já podemos prever que $6 \mapsto 3$*, de fato, verificamos que* $6 \mapsto 6 \mapsto 6 \mapsto 2 \mapsto 2 \mapsto 3 \therefore 6 \mapsto 3$*. Daí* $(123)(346)(6214)(1542)(245) = (15634)$*;*

(5) A notação de ciclo permite escrever uma permutação sem a necessidade de muitas igualdades, como no caso funcional ou como imagem de seu domínio. Então, no caso S_3*, em que* $f \in S_3$*,* $f(1) = 2; f(2) = 3, f(3) = 1$ *ou* $f = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$*, a notação de ciclo é* $f = (123)$*, portanto* $S_3 = \{e, (12), (13), (23), (123), (132)\}$*.*

Exercícios 3.3.42. *(1) Para os seguintes elementos e seus respectivos grupos, represente o elemento nas formas: funcional, em notação padrão (primeira linha:domínio;segunda linha:imagem), ou ciclo, conforme o caso:*

a) $\sigma \in S_8, \sigma(1) = 8; \sigma(2) = 6; \sigma(6) = 1; \sigma(8) = 2$ *e a identidade para os demais elementos, isto é,* $\sigma(x) = x, x\{1, 2, 6, 8\}$*;*

b) $\sigma \in S_5, \sigma = (12345); \tau \in S_7, \tau = (36)(415)$*;*

c)

$$\sigma = \begin{bmatrix} 123456789 \\ 481369257 \end{bmatrix} \quad ; \tau = \begin{bmatrix} 1234567 \\ 3517264 \end{bmatrix} \quad ; \mu = \begin{bmatrix} 12345 \\ 45123 \end{bmatrix}$$

(2) Sejam dados os seguintes elementos do grupo S_6*, o grupo de permutações de* 6 *elementos:*

$$\sigma = \begin{bmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 3 & 1 & 4 & 5 & 6 & 2 \end{bmatrix} \quad ; \tau = \begin{bmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 4 & 1 & 3 & 6 & 5 \end{bmatrix} \quad ; \mu = \begin{bmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 5 & 2 & 4 & 3 & 1 & 6 \end{bmatrix}$$

a) *Calcule os produtos* $\tau\sigma; \sigma\tau; \tau^2\sigma; \mu\sigma^2; \sigma^{-2}\tau; \sigma^{-1}\tau\sigma$

b) *Escreva os elementos acima, bem como os produtos obtidos na forma de ciclos;*

c) *Determine* $o(\sigma); o(\tau^2); o(\mu^{-1})$*;*

d) *Calcule as potências* $\sigma^{100}; \tau^{85}; \mu^{210}$*.*

.

(3) Sejam dados os seguintes elementos do grupo S_6, o grupo de permutações de 6 elementos:

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 5 & 3 & 4 & 1 & 6 & 2 \end{pmatrix}; \tau \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 5 & 6 & 1 & 3 & 4 & 2 \end{pmatrix}; \mu \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 6 & 5 & 3 & 2 & 4 & 1 \end{pmatrix}$$

a) *Calcule os produtos* $\tau\sigma, \sigma\tau, \tau^2\sigma, \mu\sigma^2, \sigma^{-2}\tau, \sigma^{-1}\tau\sigma$

b) *Escreva os elementos acima, bem como os produtos obtidos na forma de ciclos;*

c) *Determine* $o(\sigma); o(\tau^2); o(\mu^{-1})$ *;*

d) *Calcule as potências* $\sigma^{100}; \tau^{85}; \mu^{210}$.

(4) Sejam os elementos do S_7*:* $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 3 & 6 & 4 & 7 & 5 & 2 & 1 \end{pmatrix}, \mu = \sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 3 & 7 & 6 & 4 & 1 & 2 & 5 \end{pmatrix}$.
Determine:

a) *Os elementos* σ, μ *na forma de ciclos;*

b) *Calcule os produtos* $\sigma\mu$ *e* $\sigma\mu$ *e explique se* S_7 *é um grupo abeliano*

c) *A potência* μ^{137}

d) *O inverso de* σ*, isto é,* σ^{-1}.

(5) Sejam dados os seguintes elementos do grupo S_6, o grupo de permutações de 6 *elementos:*

$$\sigma = \begin{bmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 3 & 1 & 4 & 5 & 6 & 2 \end{bmatrix}; \quad \tau = \begin{bmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 4 & 1 & 3 & 6 & 5 \end{bmatrix}; \quad \mu = \begin{bmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 5 & 2 & 4 & 3 & 1 & 6 \end{bmatrix}$$

a) *Calcule os produtos* $\tau\sigma; \sigma\tau; \tau^2\sigma; \mu\sigma^2; \sigma^{-2}\tau; \sigma^{-1}\tau\sigma;$

b) *Escreva os elementos acima, bem como os produtos obtidos na forma de ciclos;*

c) *Determine* $o(\sigma); o(\tau^2); o(\mu^{-1});$

d) *Calcule as potências* $\sigma^{100}; \tau^{85}; \mu^{210}$.

Vamos discutir um subgrupo do grupo S_n, que tem tanto uma interpretação algébrica, quanto geométrica, denominado Grupo Diehdral.

3.3.6 Grupo Dihedral

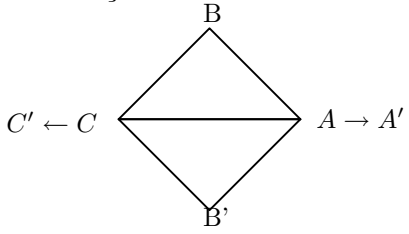
O grupo diehdral é um dos objetos matemáticos que, embora seja definido formalmente como um grupo, pode ser também compreendido geometricamente, não somente pela forma e posição de seus elementos, mas também segundo a operação binária definida sobre seu conjunto. Um aspecto importante é que todo grupo dihedral é subgrupo do grupo de permutações S_n, em que

$2n$ é exatamente a ordem do grupo dihedral, isto é, $2n$ representa o número de elementos do grupo dihedral. Inicialmente vamos discutir o grupo dihedral do ponto de vista geométrico, os elementos desse grupo, podem ser interpretados como operações geométricas. Posteriormente, discutimos a interpretação algébrica do grupo dihedral, que, entre outras, está relacionada com a potência de um número complexo.

Dado um objeto do plano cartesiano, por exemplo um segmento de reta com extremos A, B, podemos definir dois tipos de operação para esse objeto: uma translação ou uma rotação. Para o grupo dihedral interessa-nos a operação de rotação, e esta operação fica bem definida, isto é, sempre podemos aplicá-la sem ambigüidades, conhecendo-se o ângulo θ de rotação, o sentido da rotação: horário ou anti-horário e o ponto de referência para a rotação, ou centro de rotação. Por convenção o ângulo de rotação θ será medido a partir do eixo das abscissas, no sentido anti-horário e a partir da semi-reta que liga o ponto a ser rotacionado até a origem, ou seja a origem é o centro de rotação. Observe que neste caso não se define rotação para o ponto da origem, pois a semi-reta, neste caso, não está definida.

Por exemplo, seja a semi-reta definida pelos pontos $A \equiv (-1, 0); B \equiv (0, 1)$, a rotação $\theta = \frac{\pi}{2}$ do ponto A, transforma o ponto A num ponto $A' \equiv (1, 0)$ e o ponto B é transformado no ponto $B' \equiv (-1, 0)$. Isto ocorre pois estamos considerando a semi-reta AB, como um conjunto de pontos alinhados com seus extremos e portanto se o ponto A sofre uma rotação, todos os pontos de semi-reta, exceto a origem, sofrem a mesma rotação. Existem rotações não nulas, $\theta = (2n + 1)\pi, n \in \mathbb{Z}$, que permutam os pontos A e B, mas não alteram a figura original. Por figura original entendemos a figura plana inicial ou de referência.

Considere um triângulo de vértices A, B, C, centrado na origem, isto é, a origem é o circunscentro desse triângulo, o centro da circunferência que passa pelos vértices do triângulo. Sejam $A \equiv (1, 0); B \equiv (0, 1), C \equiv (-1, 0)$ os vértices de um triângulo retângulo em B, de catetos medindo $\sqrt{2}$ e hipotenusa 2, cuja origem é o circunscentro do triângulo, verifique! Seja uma rotação $\theta = \pi$ do ponto A. Considerando que o triângulo mantenha sua forma, os pontos se transformam da seguinte maneira: $A' \equiv (-1, 0); B' \equiv (0, -1); C' \equiv (1, 0)$, ou seja o triângulo retângulo ABC cujo vértice B encontrava-se acima da origem foi transformado no triângulo retângulo $A'B'C'$, cujo vértice B' é oposto ao vértice B, ou seja todo vértice do triângulo é transformado em seu oposto. Ainda neste caso, as únicas rotações, não nulas, que não alteram a figura original, isto é, o triângulo com o vértice oposto à hipotenusa sobre o eixo vertical e acima da origem, são para $\theta = 2n\pi, n \in \mathbb{Z}$, porém tais rotações mantêm os vértices sempre na mesma posição.



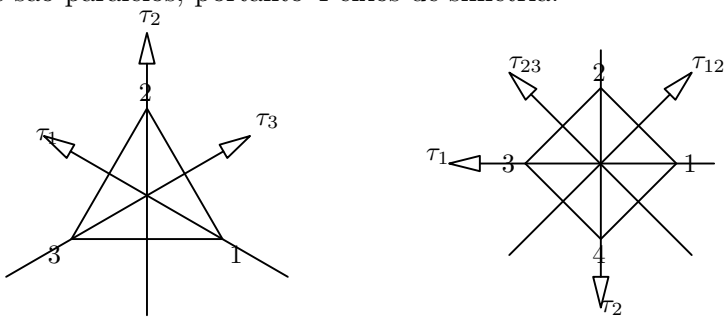
Temos dois exemplos de figuras planas, com uma diferença fundamental entre eles, o primeiro permuta pontos, sem alterar sua figura inicial, o segundo nunca permuta seus pontos, sem alterar a figura original. Estamos interessados no primeiro caso.

Perguntamo-nos, existe algum triângulo, cujo circuncentro seja a origem, para o qual existem rotações que permutem seus vértices, porém não altere sua figura original? Podemos verificar que todo triângulo eqüilátero tem esta propriedade e qualquer ângulo de rotação da forma $\theta = n\frac{\pi}{3}, n \in \mathbb{Z}$ e tal que $3 \nmid n$, permuta os vértices, sem mudar a figura original. Alguma reflexão e chegamos ao seguinte fato: Todo polígono regular tem a propriedade de existirem ângulos de rotação não nulos, que permutam os vértices e mantêm a figura original.

A rotação, portanto, é uma transformação no plano que para a classe dos polígonos, pode permutar os pontos de seus vértices sem alterar a figura original do polígono. Uma outra transformação que tem esta mesma propriedade, porém não é uma transformação no plano, é a reflexão.

A reflexão pode ser entendida como uma rotação, porém não exatamente em torno de um ponto, mas em torno de um eixo, denominado eixo de simetria, interessa-nos os eixos de simetria que estejam no mesmo plano da figura e quando nos referirmos a eixo de simetria estamos considerando somente aqueles que estão no mesmo plano da figura.

Por exemplo, o triângulo eqüilátero possui 3 eixos de simetria, definidos pelas retas que passam pelos seus vértices e os pontos médios de seus lados opostos. Para o quadrado, um polígono regular de 4 lados, os eixos de simetria são determinados pelas retas que passam pelos vértices oposto, isto é as duas diagonais, e pelas retas que passam pelos pontos médios dos lados que são paralelos, portanto 4 eixos de simetria.



Dada uma figura plana simétrica e um eixo de simetria s, existe uma transformação para os pontos da figura, que mantêm fixos todos os pontos do eixo de simetria s e permuta todo ponto da figura que é oposto em relação a este eixo de simetria, mantendo a figura original.

Exemplo 3.3.43. *(1) seja uma semi-reta centrada na origem e sobre o eixo das abscissas, de extremos A, B. O eixo das ordenadas, que passa pela origem é único eixo de simetria plano da figura e a transformação em relação a este eixo é idêntica à rotação de $\theta = \pi$. Sendo este o único caso em que rotação e reflexão, diferentes da identidade, são as mesmas*

transformações;

(2) Seja um triângulo eqüilátero de vértices A, B, C e M_A, M_B, M_C os pontos médios dos lados opostos aos vértices indicados. A reta que passa pelos pontos A, M_A é o eixo de simetria dos vértices B, C e a transformação correspondente fixa o vértice A e permuta o vértice B com o vértice C, de modo que $A' \equiv A$; $B' \equiv C$; $C' \equiv B$, e analogamente para os outros dois eixos de simetria.

A seguir definimos o que discutimos anteriormente, para prosseguir a definição de grupo diehdral.

Definição 3.3.44. *Dizemos que uma figura plana é um polígono regular, se a figura possui n vértices, com $n \geq 3$, e os seguimentos determinados pelos vértices adjacentes sejam todos congruentes. Dado um polígono regular, consideramos este centrado na origem. Definimos uma aplicação $\rho : \mathbb{R}^2 \longrightarrow \mathbb{R}^2$ que a cada vértice A do polígono, associa o ponto A' determinado pela rotação de A de um ângulo $\rho = \frac{2\pi}{n}$. Definimos uma aplicação $\tau_{xy} : \mathbb{R}^2 \longrightarrow \mathbb{R}^2$, sendo XY o eixo de simetria determinado pelos pontos X, Y do polígono, que a todo vértice A do polígono associa ou o próprio A se A é um ponto do eixo XY ou o ponto A', o oposto do ponto A em relação ao eixo de simetria XY.*

Uma verificação geométrica rápida mostra que a rotação ρ definida acima não altera a figura inicial do polígono, embora permute todos seus vértices, não fixando nenhum deles. Se aplicamos novamente a rotação, isto é, $\rho \circ \rho \doteq \rho^2$, o mesmo ocorre, e assim para qualquer potência ρ^k, com $1 \leq k < n$. Porém a potência ρ^n é a menor das potências de ρ que fixa todos os vértices, isto é, $\rho^n(A) = A$, para qualquer vértice do polígono, ou seja, ρ^n é a função identidade.

Analogamente, a aplicação determinada pela reflexão τ, para qualquer eixo de simetria do polígono regular, fixa, no máximo 2 vértices do polígono e permuta os demais, mantendo a figura inicial do polígono. Se aplicamos novamente a transformação τ, isto é, τ^2, os pontos fixos permanecem fixos, e os demais retornam à posição de origem, pois a operação de levar um ponto a seu oposto, sempre resulta no mesmo ponto quando aplicada 2 vezes. Neste caso, $\tau^2(A) = A$ ou seja a função identidade.

Estas observações levam as seguintes conclusões: tanto a aplicação ρ, quanto a aplicação τ, quando restritas ao conjunto de vértices de um polígono regular, permutam estes vértices, sem alterar a figura do polígono. Qualquer composição entre a rotação ρ, e suas potências, com as reflexões τ_{XY} permuta os vértices, sem alterar a figura do polígono. Como as únicas operações que permutam os vértices, sem alterar a figura de um polígono são as rotações e as reflexões, qualquer composição entre elas resulta numa reflexão ou em uma rotação. Isto pode ser enunciado em forma de proposição:

Proposição 3.3.45. *Dado um polígono regular de n vértices, existem no máximo n rotações distintas, que não alteram a figura do polígono e permutam seus vértices e no máximo n reflexões que, também, não alteram a forma do polígono e permutam seus vértices. Portanto há exatamente* $2n$ *transformações que não alteram a figura do polígono e permutam seus vértices.*

Demonstração. Para um polígono regular centrado na origem, a posição dos vértices fica determinada a partir de um vértice de referência. Cada vértice pode ser identificado com um número inteiro i, entre 1 e n, tomamos o vértice 1 como referência e o situamos no eixo positivo das abscissas, então cada vértice i determina um ângulo de $(i-1)\frac{2\pi}{n}$, entre a semireta definida pela origem e por este vértice. Se para algum vértice j aplicamos uma rotação $\theta = k\frac{2\pi}{n}$, com $1 \leq k < n$, então este vértice irá para a posição l, sendo l igual ao resto da divisão de $(j+k)$ por n, isto é, $l \neq j$ e $1 \leq l \leq n$, portanto a figura inicial do polígono não muda, e todos seus vértices são permutados, ocorre que tal rotação corresponde à rotação ρ^k, como existem n vértices, devem existir, no mínimo n rotações distintas, como as únicas rotações que mantêm a figura inicial deve ser algum múltiplo de $\frac{2\pi}{n}$, existem exatamente n dessas rotações. As reflexões, dependem de $n = 2k$ ou $n = 2k+1$, ou seja, se n é par ou ímpar. Se n é ímpar, cada eixo de simetria é determinado pela reta que liga um vértice ao ponto médio de seu lado oposto, como há n vértices, então há n reflexões, o único vértice fixado é aquele que está no eixo de simetria, portanto são funções distintas. Se o número de vértice é par, $n = 2k$, os eixos de simetria ou são retas determinadas pelos vértices opostos portanto k reflexões, ou retas determinadas pelos pontos médio dos lados opostos portanto k reflexões, num total de $2k = n$ reflexões. Como uma rotação permuta qualquer vértice, se f é alguma rotação $f(A) \neq A$, para todo vértice A, no caso de $n = 2k+1$ se g é uma reflexão, sempre ocorre que $g(A) = A$ para um único vértice, logo $f \neq g$. Se $n = 2k$, e g é uma reflexão que não fixa nenhum vértice, sempre ocorre que pelo menos dois vértices adjacentes são permutados, que são exatamente os vértices do lado cujo eixo de simetria passa pelo ponto médio, e portanto se fosse uma rotação, o ângulo deveria ser $\frac{2\pi}{n}$ o que implicaria que somente os vértices adjacentes seriam permutados, mas a reflexão permuta os vértices opostos pelo eixo de simetria, portanto $f \neq g$, então há $2n$ transformações que permutam vértices e mantêm a figura original. □

Corolário 3.3.46. *Seja* D_n *o conjunto de todas as rotações e reflexões de um polígono regular de n vértices, então a aplicação* $\circ : D_n \times D_n \longrightarrow D_n : (f,g) \mapsto f \circ g$ *é uma operação binária.*

Demonstração. A composição das transformações que permutam os vértices e mantêm a figura original, necessariamente deve manter a figura original. Pelo teorema há exatamente $2n$ dessas funções; como pela proposição $|D_n| = 2n$, o conjunto D_n é o conjunto de todas as transformações deste gênero, como $f \circ g$ mantém a figura original, então $f \circ g \in D_n$. □

Proposição 3.3.47. *Seja* ρ *a rotação de um polígono de n vértices de um ângulo* $\rho = \frac{2\pi}{n}$.

Então o conjunto das rotações do polígono, que não alteram a figura inicial, com a operação de composição de funções, determina um grupo cíclico de ordem n.

Demonstração. Segundo a proposição anterior, somente rotações de um ângulo que seja múltiplo de $\frac{2\pi}{n}$, não alteram a figura original. Portanto há n, dessas rotações. A transformação correspondente a n rotações corresponde a uma rotação de 2π, portanto cada vértice A é transformado nele mesmo, isto é, $\rho^n(A) = A \therefore \rho^n = I_d$ a função identidade, que é o elemento neutro da operação de composição de funções, logo $o(\rho) = n$, portanto $< \rho >$ é um grupo cíclico de ordem n. □

O teorema a seguir pemite-nos definir o grupo diehdral. Em seguida, vamos construir o grupo dihedral de menor ordem, isto é, o grupo de rotações e reflexões de um triângulo eqüilátero.

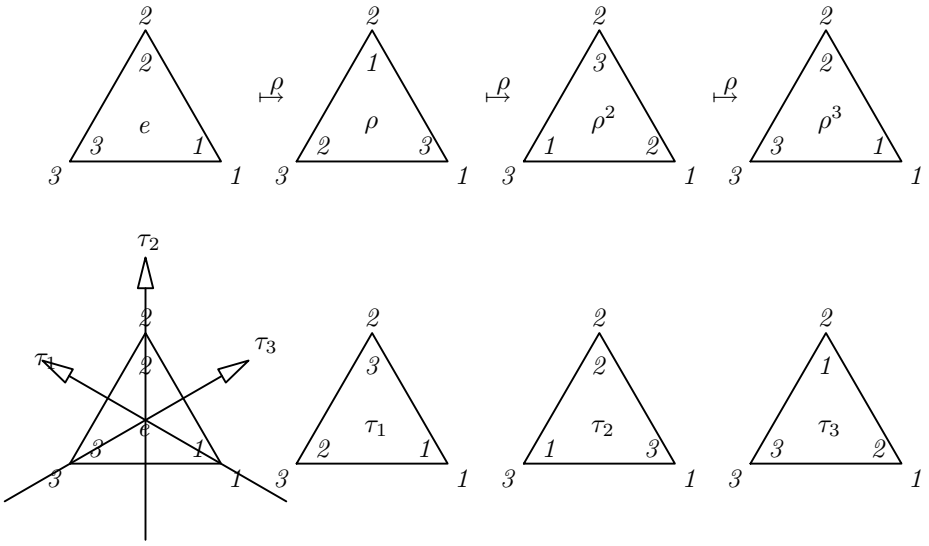
Teorema 3.3.48. *Sejam D_n o conjunto de todas as rotações e reflexões de um polígono regular de n vértices. O conjunto $\{D_n, \circ\}$ é um grupo de ordem $|D_n| = 2n$.*

Demonstração. A demonstração segue a forma padrão, mas já está quase tudo feito. Pelo corolário, a composição de funções sobre D_n é uma operação binária. A composição de funções é sempre associativa, portanto a operação binária é associativa. Existe o elemento neutro, que é a função identidade. Resta provar que todo elemento de $u \in D_n$ admite elemento inverso, de fato! Se u é uma rotação, então $u \in < \rho >$, portanto $u = \rho^k, 1 \leq k \leq n$, $u^{-1} = \rho^{n-k}$, logo u admite elemento inverso. Se u é uma reflexão, então u^2 é a identidade, portanto $u^{-1} = u$. Então o conjunto $\{D_n, \circ\}$ é um grupo. □

Definição 3.3.49. *Seja D_n o conjunto das rotações e reflexões de um polígono regular de n vértices. O grupo $\{D_n, \circ\}$ é denominado grupo diehdral.*

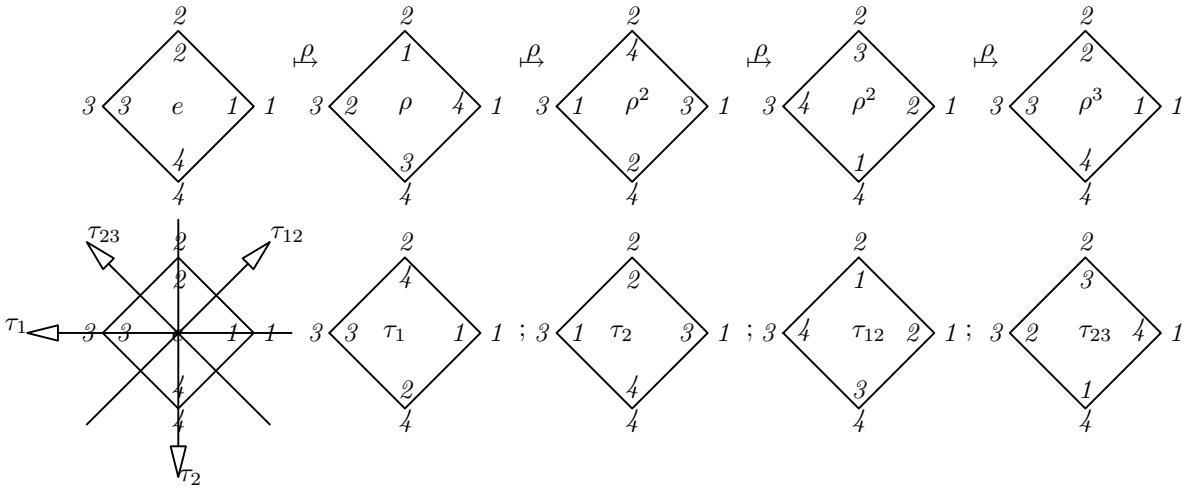
Exemplo 3.3.50. *(1) Inicialmente identificamos os vértices do triângulo com os números $1, 2, 3$, marcados no sentido anti-horário, com os vértice 1 e 2 no quarto e terceiro quadrantes, respectivamente, e o vértice 3 sobre o eixo das ordenadas, conforme figura abaixo. Segundo a definição a rotação $\rho = \frac{2\pi}{3}$. A seguir, marcamos, no interior e no exterior do triângulo, sua configuração inicial , correspondente à posição inicial dos vértices. Se aplicamos uma rotação ρ sobre o triângulo, $\rho(i) = j$ significa que a rotação moveu o vértice interno i do triângulo, indicado no interior do triângulo, para a posição j do plano, fixada e marcada externamente ao triângulo, como mostra a figura 3. Ou seja, $\rho(1) = 2; \rho(2) = 3; \rho(3) = 1$. Se aplicarmos outra rotação ρ, teremos $\rho^2(1) = 3; \rho^2(2) = 1; \rho^2(3) = 2$. Finalmente, $\rho^3(1) = 1; \rho^3(2) = (2); \rho^3(3) = 3$, estas são todas as rotações possíveis, mostrando que $o(\rho) = 3$. Para as reflexões há 3 eixos de simetria. A primeira reflexão denominamos τ_1, aquela que fixa o vértice 1, portanto $\tau_1(1) = 1; \tau_1(2) = 3; \tau_1(3) = 2$, segundo a mesma notação da rotação, isto é, $\tau(i) = j$ indica que o vértice interno i foi*

movido, pela reflexão τ para a posição fixa do vértice externo j. Outra reflexão fixa o vértice 2, seja esta τ_2, portanto $\tau_2(1) = 3$;$\tau_2(2) = 2$;$\tau_2(3) = 1$, a terceira reflexão será $\tau_3(1) = 2; \tau_3(2) = 1; \tau_3(3) = 3$. Podemos verificar que cada rotação: ρ, ρ^2 e ρ^3 e cada reflexão: τ_1, τ_2 e τ_3, são pemutações do S_3. Como ocorrem 6 permutações distintas, que são os elementos do grupo D_3, então $D_3 = S_3$, podemos então escrever cada rotação na forma de ciclo, portanto $\rho = (123); \rho^2 = (132); \rho^3 = e; \tau_1 = (23); \tau_2 = (13); \tau_3 = (12)$. Observe que, por exemplo, o ciclo (132), significa a o vértice interno 1 foi deslocado para a posição fixa do vértice externo 3; que o vértice interno 3 foi deslocado para a posição fixa do vértice externo 2, e que o vértice interno 2 foi deslocado para a posição fixa do vértice externo 1, como mostra a figura a seguir. Portanto $D_3 = \{e, (123), (132), (12), (13), (23)\}$ que é o grupo S_3.

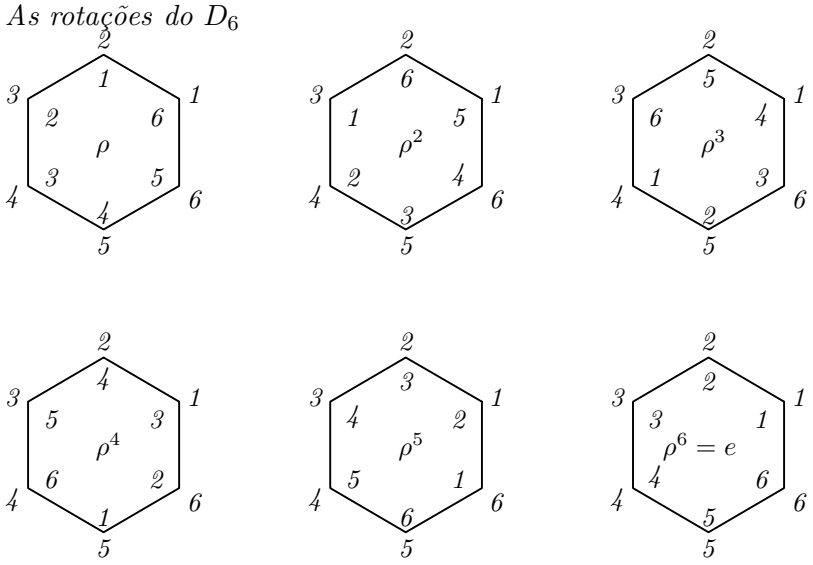


(2) Analogamente, construímos o grupo D_4, das reflexões do quadrado. Observe, que neste caso as reflexões τ_i, são definidas tanto pelos pontos médios dos lados opostos $\tau_{i,j}$, quanto pelos vértices opostos τ_i, veja as figuras desta secção. Assim

$$D_4 = \{e, \underbrace{(1234)}_{\rho}, \underbrace{(13)(24)}_{\rho^2}, \underbrace{(1432)}_{\rho^3}, \underbrace{(24)}_{\tau_1}, \underbrace{(13)}_{\tau_2}, \underbrace{(12)(34)}_{\tau_{12}}, \underbrace{(14)(23)}_{\tau_{23}}\}$$



(3) As rotações do D_6



$\rho = (123456)$

$\rho^2 = (135)(246)$

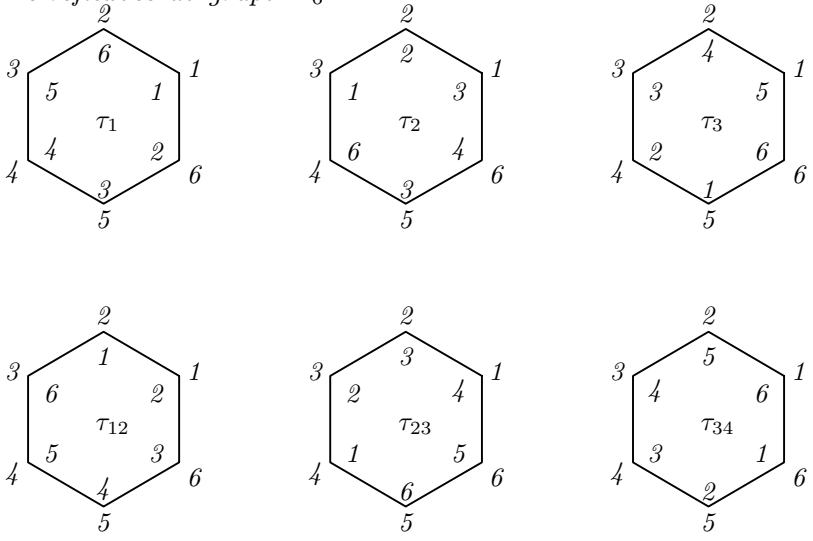
$\rho^3 = (14)(25)(36)$

$\rho^4 = (153)(264)$

$\rho^5 = (165432)$

$\rho^6 = e$

(4) As reflexões do grupo D_6



$\tau_1 = (26)(35)$

$\tau_2 = (13)(46)$

$\tau_3 = (24)(15)$

$\tau_{12} = (12)(36)(45)$

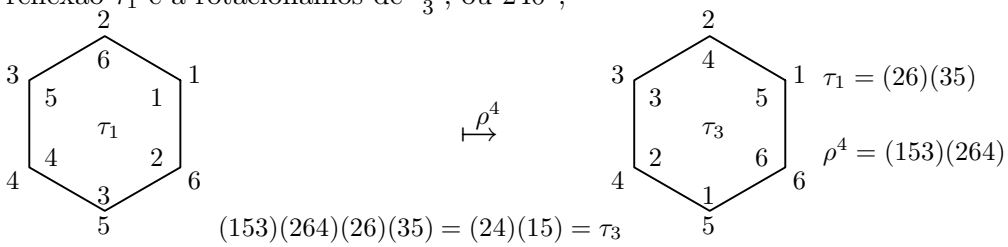
$\tau_{23} = (23)(14)(56)$

$\tau_{34} = (34)(25)(16)$

Se D_n é o grupo dihedral do n-ágono e $\rho = \frac{\pi}{n}$ uma rotação que preserva a configuração inicial, o grupo cíclico $< \rho >$ é subgrupo do grupo D_n. Considerando o plano complexo $\mathbb{C}$, geometricamente, este subgrupo representa as raízes da unidade, isto é, cada vértice do polígono é uma raiz da equação $z^n = 1$. No exemplo anterior o grupo $< \rho >$ representa, geometricamente, as soluções da equação $x^4 = 1$.

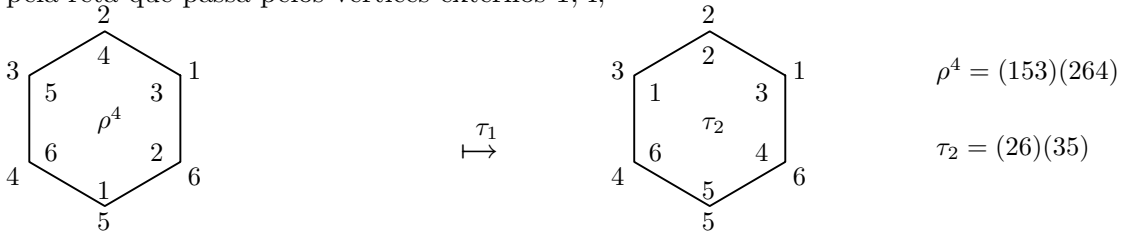
Os exemplos anteriores ilustram o significado geométrico do grupo dihedral. A operação entre os elementos do grupo dihedral, também tem uma interpretação geométrica. A seguir exemplificamos algumas das operações do grupo D_6, as reflexões e rotações de um hexagono regular. Sejam $\sigma, \mu \in D_6$, observe que $\sigma\mu$, segundo o conceito de composição de funções, significa que aplicamos a função σ, sobre $\mu(i), i \in \{1,2,3,4,5,6\}$, veremos que geometricamente, isto equivale a fixar a configuração equivalente à permutação μ e aplicar a rotação ou reflexão σ. Por exemplo $\sigma = (14)(25)(36)$ e $\mu = (246)(135)$, $\sigma\mu$ significa fixar a rotação μ e rotacioná-la de um ângulo de 180^0, representado pela rotação σ.

(1) $(153)(264)(26)(35)$ é a operação entre a rotação ρ^4 e a reflexão τ_1, ou seja, fixamos a reflexão τ_1 e a rotacionamos de $\frac{2\pi}{3}$, ou 240^0;



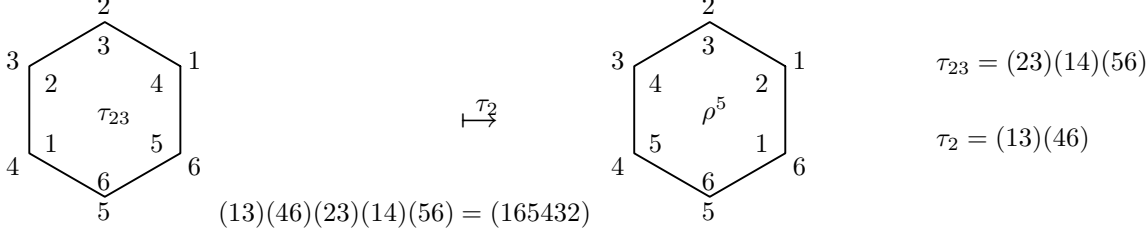
$$(153)(264)(26)(35) = (24)(15) = \tau_3$$

(2) $(26)(35)(153)(264)$, neste caso devemos fixar a rotação ρ^4 e aplicamos a reflexão τ_1, definida pela reta que passa pelos vértices externos $1, 4$;



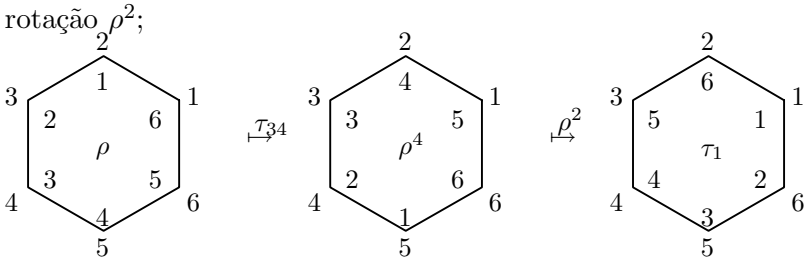
$$(26)(35)(153)(264) = (13)(46) = \tau_2$$

(3) $(13)(46)(23)(14)(56)$, fixa a reflexão τ_{23} e aplica-se a reflexão τ_2;



$$(13)(46)(23)(14)(56) = (165432)$$

(4) $\rho^2\tau_{34}\rho$, fixamos inicialmente a rotação ρ, aplicamos a reflexão τ_{34} e a este resultado a rotação ρ^2;



$$(135)(246)(34)(25)(16)(123456) = (26)(35)$$

Exercícios 3.3.51. *(1) Monte a tábua multiplicatica do grupo dihedral D_3*

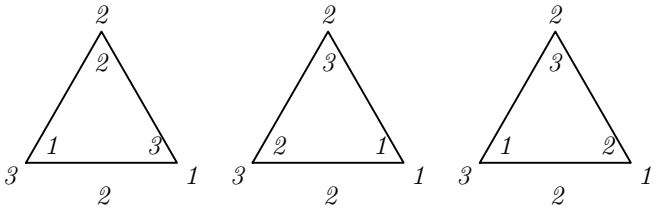
(2) Determine os grupos dihedrais:

a) *D_5;*

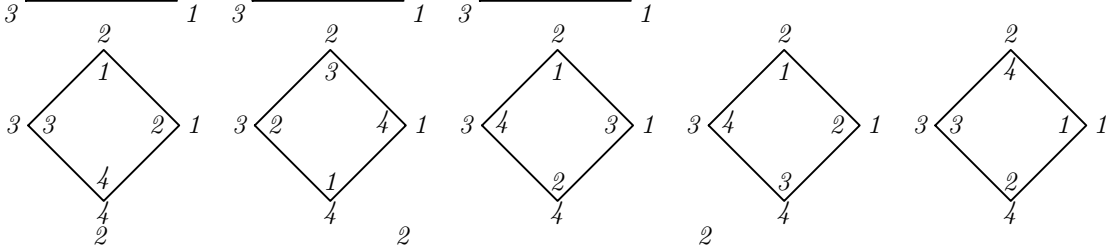
b) *D_6.*

(3) Para os polígonos regulares a seguir, verifique quais deles, segundo a notação apresentada, representa um elemento do grupo dihedral D_n. Se for o caso, determine o elemento na forma de ciclos e sua ordem.

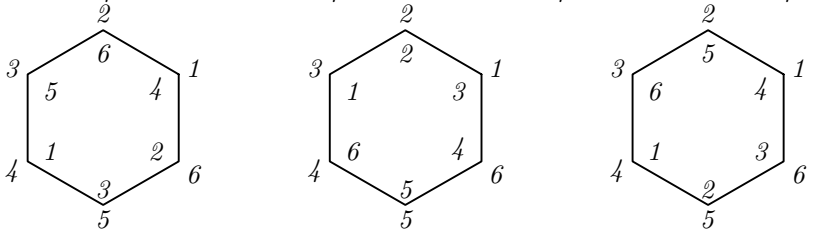
a)



b)



c)



(4) Sejam $\sigma, \tau \in D_n$ uma rotação e uma simentria, respectivamente. Prove que $\tau\sigma\tau = \sigma^{-1}$

(5) Seja $x \in \mathbb{C}$, para as condições a seguir, considere $G =< x >$, o grupo cíclico gerado por x. Determine $|G|$ e sua representação geométrica no plano:$x^3 = i$;$X^5 = -1$;$x^4 = -i$;$x^6 = 1$;

(6) Seja $A = \{1, \frac{1+i\sqrt{3}}{2}, \frac{-1-i\sqrt{3}}{2}\}$, sendo i a unidade imaginária. Responda:

a) *Se* $* : A \times A \to \mathcal{A}$ *é a relação binária do produto usual, isto é,* $*(x, y) = xy$*, faça a tabela da relação* $*$*, verificando se é uma operação binária;*

b) *Represente os elementos do conjunto A no Plano Complexo;*

c) *Represente os elementos do conjunto A na forma polar;*

d) *Mostre que* $x \in A \Rightarrow x^n \in A, \forall n \in Z$*. (sugestão: utilize a relação* $*$*).*

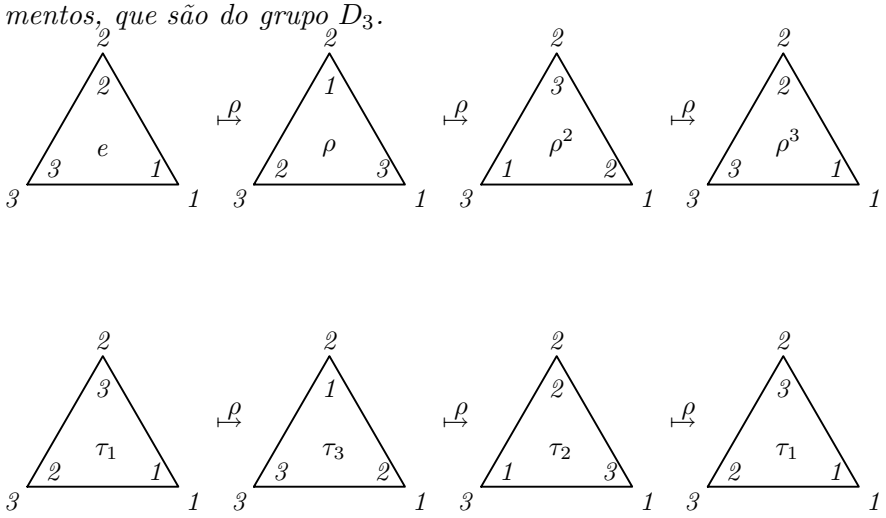
(7) Repita o exercício anterior, para o conjunto $A = \{1, \frac{1+i\sqrt{3}}{2}, \frac{-1+i\sqrt{3}}{2}, -1, \frac{-1-i\sqrt{3}}{2}, \frac{1-i\sqrt{3}}{2}\}$.

Definição 3.3.52. *Seja G um grupo. Se existem elementos* $\rho, \tau \in G$*, tal que, todo elemento de G é da forma* $\rho^i\tau^j, i, j \in \mathbb{Z}$*, então dizemos que G é gerado pelos elementos* ρ, τ *e representamos isso por* $G =< \rho, \tau >$*.*

Proposição 3.3.53. *Seja* ρ *a rotação de um polígono de* $n \leq 3$ *vértices e* τ *uma reflexão desse polígono, isto é,* $\rho, \tau \in D_n$*. Se* $o(\rho) = n$ *e* $\tau\rho\tau = \rho^{-1}$*, então* $D_n =< \rho, \tau >$*.*

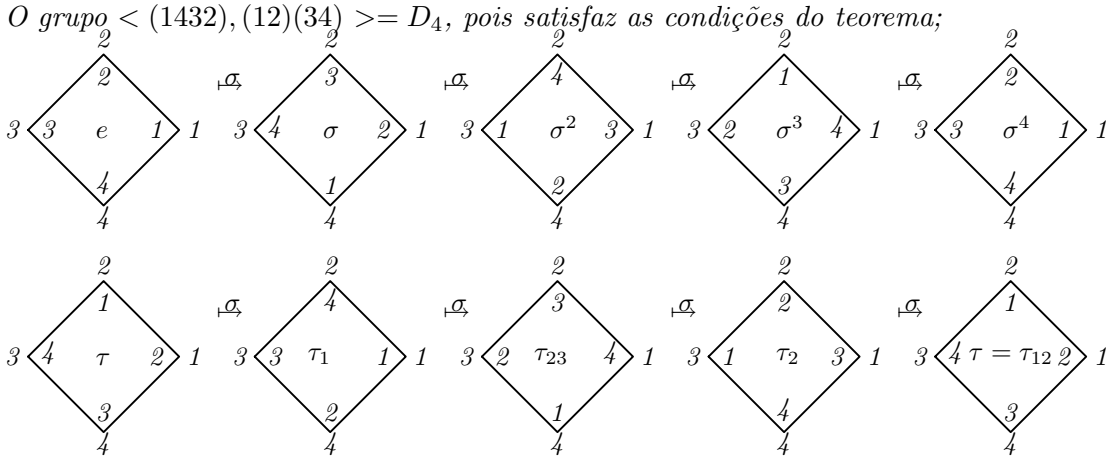
Demonstração. Sendo $o(\rho) = n$, $< \rho >$ é um grupo cíclico de ordem n. Obviamente $< \rho >$ é subgrupo de D_n. Para cada elemento do grupo $< \rho >$, isto é ρ^i, com $1 \leq i \leq n$, podemos aplicar a reflexão τ, de modo que $\tau_i = \rho^i \circ \tau \in D_n$. Afirmamos que $\tau_i \notin < \rho >$. Com efeito, $\tau_i^2 = \rho^i\tau\rho^i\tau = \rho^i \circ \rho^{-1} = e$, portanto $o(\tau_i) = 2$, mas os únicos elementos de ordem 2 de um grupo dihedral, quando n é ímpar, são as reflexões; caso n seja par, $n = 2k$, suponho que τ_i não seja uma reflexão, então $\tau_i = \rho^k = \rho \circ \tau \therefore \tau = \rho^{k-i}$, um absurdo, pois τ é reflexão por hipótese. Portanto τ_i é uma reflexão. Há n rotações distintas ρ^i, $1 \leq i \leq n$, portanto há n reflexões τ_i distintas, então $D_n \subset < \rho, \tau >$. Mas $< \rho, \tau > \doteq \{\rho^i\tau^j : i, j \in \mathbb{Z}\} \Rightarrow < \rho, \tau > \subseteq D_n$, pois D_n é um grupo, logo $D_n =< \rho, \tau >$. □

Exemplo 3.3.54. *(1) O grupo* $D_3 = \{e, (123), (132), (12), (13), (23)\}$*, seja* $\sigma = (132)$ *e* $\tau = (12)$*;* $< \sigma, \tau >= D_3$*, pois para as potências se* σ*, aplicamos a reflexão* τ*, obtendo* 6 *elementos, que são do grupo* D_3*.*



(2) O grupo $< (13)(24), (12)(34) >$*, não gera o grupo* D_4*, embora* $\sigma = (13)(24)$ *é uma rotação de* D_4 *e* $\mu = (12)(34)$ *uma reflexão do grupo, porém* $o(\sigma) = 2$*, enquanto que* $n = 4$*;*

(3) O grupo $< (1432), (12)(34) >= D_4$*, pois satisfaz as condições do teorema;*



Observe acima, que os elementos do grupo foram determinados geometricamente, aplicando-se a rotação $\sigma = (1432)$*, sucessivamente para a identidade (a primeira linha da figura), e sucessivamente para a reflexão* $\tau = (12)(34)$ *(a segunda linha da figura). Pela figura, podemos observar que a rotação* σ *gira a figura no sentido horário. Uma outra forma de determinar os elementos do grupo, seria calcular os produtos* $\sigma^i\tau^j, 1 \leq i \leq 4; 1 \leq j \leq 2$*, por exemplo* $\sigma\tau = (1432)(12)(34) = (24) = \tau_1$*; verifique, ainda, que geometricamente, calculamos este elemento na segunda linha da figura.*

(4) O grupo $< (12345), (123) >$ *não é o* D_5*, pois* (123) *não é uma reflexão deste grupo.*

Proposição 3.3.55. *Seja* n *um inteiro positivo,* $n \leq 3$*. Então* $D_n \leq S_n$*. Além disso somente ocorre a igualdade se* $n = 3$

Demonstração. Basta provar que $\exists \sigma, \mu \in S_n$, tal que $o(\sigma) = n$, $o(\mu) = 2$ e $\mu\sigma\mu = \sigma^{-1}$, pois nessas condições, pela proposição 3.3.53, $< \sigma, \mu >= D_n \therefore D_n \subseteq S_n$. Se n é da forma $2k + 1$, os ciclos

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & \cdots & n \end{pmatrix}; \mu = \begin{pmatrix} 2 & n \end{pmatrix}\begin{pmatrix} 3 & n-1 \end{pmatrix}\cdots\begin{pmatrix} \frac{n-1}{2} & \frac{n+1}{2} \end{pmatrix},$$

satisfazem as condições. Se $n = 2k$, para o ciclo σ, da condição anterior, e

$$\mu = \begin{pmatrix} 2 & n \end{pmatrix}\begin{pmatrix} 3 & n-1 \end{pmatrix}\cdots\begin{pmatrix} \frac{n}{2}-1 & \frac{n}{2}+1 \end{pmatrix}$$

isso também ocorre, portanto D_n é subgrupo de S_n. Sendo $|D_{2n}| = 2n$ e $|S_n| = n!$, os grupos $S_n = D_n$ somente se $2n = n!$, isto é $n = 3$. □

Exercícios 3.3.56. *(1) Mostre que os elementos* $\alpha = (13524), \beta = (23)(41)$ *geram um grupo dihedral, determinando qual a ordem desse grupo, seus elementos e um subgrupo não trivial deste grupo.*

(2) Mostre em que casos os elementos geram o grupo dihedral, e a ordem desse grupo.

a) $\rho = (123), \tau = (12)$

b) $\rho = (132), \tau = (23)$

c) $\rho = (53142), \tau = (42)(51)$

d) $\rho = (135)(246), \tau = (13)(46)$

e) $\rho = (165432), \tau = (26)(35)$

f) $\rho = (3572461), \tau(34)(25)(16)$

g) $\rho = (4132), \tau = (123)$

h) $\rho = (4132), \tau = (14)(32)$

(3) Determine todos os subgrupos dos grupos dihedrais: D_3, D_4, D_5, D_6.

3.4 Classes Laterais e O Teorema de Lagrange

Dado um grupo $\{G, *\}$, se $g \in G$, então $g * G \doteq \{g * h : h \in G\}$. Como vimos, no teorema 3.2.1, deve ocorrer que $g * G = G, \forall g \in G$. No entanto, se consideramos $H < G$, a condição $g * H = H$ deve ocorrer se, e somente se, $g \in H$. Dado um subgrupo H de um grupo G, os conjuntos gH têm um papel importante na teoria de grupos. Tais conjuntos, quando agrupados convenientemente, auxiliam na determinação de propriedades do grupo como: comutatividade, a ordem dos possíveis subgrupos de um grupo finito, a partição de um grupo infinito em um número finito de termos, entre outras propriedades.

Definição 3.4.1. *Seja G um grupo, H um subgrupo de G e $g \in G$. O conjunto*

$$gH = \{gh : h \in G\}$$

é denominado classe lateral à esquerda de H em G. Analogamente definimos o conjunto Hg pela classe lateral à direita de G. O conjunto $S_G(H) = \{gH : g \in G\}$ é o conjunto das classes laterais à esquerda de H em G e o conjunto $D_G(H) = \{Hg : g \in G\}$ é o conjunto das classes laterais à direita de H em G. Denotamos $\mathcal{C}_G(H)$ o conjunto das classes laterais de H em G, isto é,

$$\mathcal{C}_G(H) = D_G(H) \cup S_G(H).$$

Nas condições da definição anterior, dado $g \in G$, as classes laterais à esquerda e à direita podem ser distintas, porém são as mesmas se o grupo é abeliano, verifique! Por exemplo, o grupo S_3 apresenta classes laterais distintas para o subgrupo $H =< \sigma >, \sigma \in S_3, o(\sigma) = 2$. Se $H = \{e, (12)\}$ para o elemento $(13) \in S_3$, a classe lateral à esquerda $(13)H = \{(13)e, (13)(12)\} =$

$\{(13),(123)\}$, porém a classe lateal à direita $H(13) = \{e(13),(12)(13)\} = \{(13),(132)\}$, uma vez que os ciclos $(123) \neq (132)$, então $(13)H \neq H(13)$, isto é a classe lateral à direita e à esquerda de (13) em H são distintas.

Ocorre que mesmo os grupos não-abelianos, como S_3, podem apresentar, para um subgrupo H as mesmas classes laterais, à esquerda e à direita. Por exemplo, se $H =< \sigma >, \sigma \in S_3, o(\sigma) = 3$. Isto é, $H = \{e,(123),(132)\}$, basta verificar para os elementos $(12),(13),(32)$, pois os demais são elementos de H. Então $(12)H = \{(12)e,(12)(123),(12)(132)\} = \{(12),(13),(32)\}$ e $H(12) = \{e(12),(123)(12),(132)(12)\} = \{(12),(13),(32)\}$, portanto $(12)H = H(12)$, ocorrendo o mesmo para os demais elementos. Os subgrupos com esta propriedade são essenciais à teoria de grupos, pois permite que a estrutura do grupo seja conhecida a partir destes grupos. A próxima seção trata deste assunto.

A seguir vamos enunciar o teorema de Lagrange, que apresenta uma condição necessária para que um conjunto seja subgrupo de um grupo finito. A seguinte proposição auxilia na demonstração deste teorema.

Proposição 3.4.2. *Seja G um grupo e H um subgrupo finito de G. As classes laterais de H em G têm a mesma cardinalidade.*

Demonstração. Seja $g \in G$, $|gH| \leq |H|$, por conta da definição. Basta provar que $|H| \leq |gH|$. Suponha, por contradição que isso não ocorre, então $\exists h,k \in H, h \neq k$ tal que $gh = gk$, pela propriedade de G, $g^{-1} \in G \Rightarrow g^{-1}(gh) = g^{-1}(gk)$, logo $h = k$, absurdo! Portanto $|H| = |gH|$. Analogamente ocorre $|H| = |Hg|$. □

Esta proposição permite-nos construir a seguinte relação de equivalência.

Lema 3.4.3. *Seja G um grupo e H um subgrupo de G. A relação*

$$\begin{array}{rccll} L: & G & \to & G & \\ & g & \mapsto & h & \text{se } gh^{-1} \in H. \end{array}$$

É uma relação de equivalência, cuja imagem de cada elemento g é a classe lateral à direita Hh se, e somente se, $g \mapsto h$.

Demonstração. Basta verificar as propriedades: reflexiva, simétrica e transitiva. Reflexiva: $g \mapsto g$ pois $gg^{-1} = e \in H$. Simétrica: $g \mapsto h \Rightarrow gh^{-1} \in H$, sendo H um subgrupo, todo elemento de H é invertível, logo $(gh^{-1})^{-1} \in H$, mas $(gh^{-1})^{-1} = hg^{-1}$, portanto $h \mapsto g$ e a relação é simétrica. Transititva: se $g \mapsto h; h \mapsto k$, então gh^{-1} e hk^{-1} são elementos de H, sendo este um subgrupo, $gh^{-1}(hk^{-1}) = g(hh^{-1})k^{-1} = hk^{-1} \in H$, logo $g \mapsto k$ e a relação é simétrica. Logo L é uma relação de equivalência. Além disso, se por um lado, quando $g \mapsto h$, então $gh^{-1} \in H$, isto é, $\exists x \in H$, tal que, $gh^{-1} = x \Rightarrow g = xh \therefore g \in Hh$; por outro lado se

$g \in Hk$, para algum $k \in G$, então $L(g) = k$. Mas sendo L uma relação de equivalência, nessas condições, $k \in Hh$, portanto $L[g] = Hh$, isto é, a classe Hh é o conjunto imagem de g, para todo $h \in G$, tal que $L(g) = h$. Reciprocamente, se $L[g] = Hh$, ou seja, a imagem e g é a classe lateral Hh, sendo L uma relação de equivalência, $L(g) = g$, propriedade reflexiva, portanto $g \in Hh \therefore \exists x \in H, g = xh \therefore x = gh^{-1} \in H$, logo $L(g) = h$. □

Sabemos, pela proposição 1.3.14, que uma relação de equivalência sobre um conjunto G determina uma partição P deste conjunto, sendo os elementos da partição P as classes de equivalência da relação L, que são conjuntos disjuntos. Estes fatos, convenientemente encadeados demonstram o seguinte teorema.

Teorema 3.4.4 (Teorema de Lagrange)**.** *Seja G um grupo finito. Se H é um subgrupo de G, então $|H| \mid |G|$.(lê-se a ordem de H divide a ordem de G)*

Demonstração. Seja

$$\begin{array}{rccll} L: & G & \to & G & \\ & g & \mapsto & h & \text{se } gh^{-1} \in H, \end{array}$$

L é uma relação de equivalência, cujas classes de equivalência são as classes laterais de H. pela proposição $|Hh| = |H|$, se Hh, Hk são classes distintas, então $Hh \cap Hk = \emptyset$. Seja n o número de classes laterais de H em G, então o conjunto P das classes de equivalência coincide com o conjunto de classes laterais, $\bigcup_{Hh \in P} Hh = G$ é a união disjunta, logo $n = |P|$; $|G| = |\dot{\cup} Hh| = \sum |Hh| = n|H|$, pois as classes têm o mesmo número de elementos, logo $|G| = n|H|$ portanto $|H| \mid |G|$. □

Existe um resultado importante do teorema de Lagrange para grupos finitos de ordem prima:

Corolário 3.4.5. *Seja G um grupo de ordem prima, isto é, $|G| = p$ um número primo. Então G é um grupo cíclico, cujos únicos subgrupos de G são G e $\{e\}$.*

Demonstração. Seja $g \in G \setminus \{e\}$, o grupo cíclico $< g >$ é um subgrupo de G, não trivial, pois $g \in < g > \Rightarrow | < g > | \geq 2$. pelo teorema de lagrange $| < g > | \mid | < G > | \therefore | < g > | \in \{1, p\}$ mas $| < G > | \geq 2 \therefore | < g > | = p = |G|$; logo G é gerado por $g \in G$, portanto um grupo cíclico; $\forall g \in G, o(g) = p = |G|$, portanto se $H < G$, então $|H| \mid |G| \therefore |H| \in \{1, p\}$ ou $H = \{e\}$ ou $H = G$, logo todo subgrupo de G é trivial. □

Como vimos, todo grupo cíclico é abeliano, logo se G é um grupo e p é um número primo, então $|G| = p \Rightarrow G$ é um grupo abeliano.

Exemplo 3.4.6. *(1) O grupo S_3, cuja ordem é 6, não possui subgrupos de ordem 4, pois $4 \nmid 6$.*

(2) Seja S_n o grupo de n-permutações, dizemos que $\sigma \in S_n$ é uma permutação par, se $\prod_{1\leq i<j\leq n} \frac{\sigma(i)-\sigma(j)}{i-j}$, em que $\prod$ denota o produtório dos elementos, é um número positivo. Por exemplo, a permutação $\sigma = (1452) \in S_5$ é ímpar, pois

$$\prod \frac{\sigma(i)-\sigma(j)}{i-j} =$$
$$\frac{(\sigma(1)-\sigma(2))(\sigma(1)-\sigma(3))(\sigma(1)-\sigma(4))(\sigma(1)-\sigma(5))(\sigma(2)-\sigma(3))(\sigma(2)-\sigma(4))(\sigma(2)-\sigma(5))(\sigma(3)-\sigma(4))(\sigma(3)-\sigma(5))(\sigma(4)-\sigma(5))}{(1-2)(1-3)(1-4)(1-5)(2-3)(2-4)(2-5)(3-4)(3-5)(4-5)} =$$
$$\frac{(4-1)(4-3)(4-5)(4-2)(1-3)(1-5)(1-2)(3-5)(3-2)(5-2)}{(1-2)(1-3)(1-4)(1-5)(2-3)(2-4)(2-5)(3-4)(3-5)(4-5)} =$$
$$\frac{(1-2)(1-3)(-1+4)(1-5)(-2+3)(-2+4)(-2+5)(-3+4)(3-5)(4-5)}{(1-2)(1-3)(1-4)(1-5)(2-3)(2-4)(2-5)(3-4)(3-5)(4-5)} =$$
$$(-1)(-1)(-1)(-1)(-1) = -1 \therefore \sigma \text{ é ímpar.}$$

Definição 3.4.7. *Se $\sigma \in S_n$, definimos $sgn(\sigma) := \prod_{1\leq i<j\leq n} \frac{\sigma(i)-\sigma(j)}{i-j}$ o sinal de σ*

O subconjunto $A_n = \{\sigma \in S_n : \sigma \text{ é uma permutação par}\}$ de S_n é um subgrupo de S_n, denominado subgrupo alternado de S_n. Deixamos a prova dessa afirmação como exercício. A seguinte proposição mostra que o produto de duas permutações pares é uma permutação par.

Proposição 3.4.8. *Seja $X = \{1, 2, \cdots, n\}$ e $Sym(X) := S_n$. As seguintes proposições são verdadeiras:*

(1) Se $\alpha \in S_n$ e $\alpha[X] = \{\alpha(1), \alpha(2), \cdots, \alpha(n)\}$, então toda permutação $\pi \in S_n$ é uma permutação de $Sym(\alpha[X])$. Ademais a permutação π em S_n é a mesma em $Sym(\alpha[X])$.

(2) O sinal $sgn(\alpha)$ é invariante sobre o grupo de permutações de n símbolos.

(3) Se $\alpha, \beta \in S_n$ então $sgn(\alpha\beta) = sgn(\alpha)sgn(\beta)$.

Demonstração. (1) Sendo a permutação π uma função injetora sobre X, como conjunto $X = \alpha[X]$, logo π é uma permutação de $Sym(\alpha[X])$. Obviamente a permutação π permuta igualmente os elementos dos conjuntos $X = \alpha(X)$, logo é a mesma permutação.

(2) Seja Y um conjunto e $|X| = |Y| = n \neq 0$. Se $\alpha : X \to Y$ é injetora, então $\alpha \in Sym(X)$, pois para todo $y \in Y$, existe $x \in X$ tal que $y = \alpha(x)$. Pelo item anterior a permutação α de X é a mesma de α de Y, logo tem o mesmo sinal.

(3) Sejam $\alpha, \beta \in S_n$; $sgn(\alpha\beta) = \prod_{1\leq i<j\leq n} \frac{\alpha(\beta((i))-\alpha(\beta((j))}{i-j}$. Pelo item (1), α é permutação de $\beta[X]$, logo:

$$sgn_{\beta[X]}(\alpha) = \prod_{1\leq i<j\leq n} \frac{\alpha(\beta((i))-\alpha(\beta((j))}{\beta(i)-\beta(j)} = \prod_{1\leq i<j\leq n} (\frac{\alpha(\beta((i))-\alpha(\beta((j))}{i-j})sgn(\beta) \quad (\star),$$

pois $\beta(i)-\beta(j) = \frac{(i-j)(\beta(i)-\beta(j))}{(i-j)}$. Daí, usando o fato que, em um produtório $\prod_{i,j}((A(i,j)B(i,j)) = (\prod_{i,j}(A(i,j))(\prod_{i,j} B(i,j))$, quando $A(i,j)B(i,j) = B(i,j)A(i,j)$ e $sgn(\beta) = \frac{1}{sgn(\beta)}$, pois $sgn(\beta) \in \{1,-1\}$ obtemos $(\star)$. Pelo item (2), $sgn(\alpha) = sgn_X(\alpha) = sgn_{\beta[X]}(\alpha)$, então

$$sgn_{\beta[X]}(\alpha) = \prod_{1\leq i<j\leq n} (\frac{\alpha(\beta((i)) - \alpha(\beta((j))}{i-j})sgn(\beta) = sgn(\alpha\beta))sgn(\beta) = sgn(\alpha),$$

novamente $sgn(\beta) = \frac{1}{sgn(\beta)}$ logo $sgn(\alpha\beta) = sgn(\alpha)sgn(\beta)$.

□

Sendo $\sigma \in S_n$ uma permutação ou par ou ímpar, então a classe lateral σA_n ou é o próprio A_n, quando σ é par ou σA_n é um conjunto de permutações ímpares, se σ é ímpar. Logo há exatamente 2 classes laterais para A_n. Sendo $S_n = A_n \dot\cup \sigma A_n = |S_n| = n! = |A_n| + |A_n| \therefore |A_n| = \frac{n!}{2}$. Portanto o subgrupo $A_4 < S_4$ é um grupo de ordem, $|A_4| = \frac{4!}{2} = 12$. Embora $6 \mid 12 = |A_4|$, veremos adiante que A_4 não possui subgrupo de ordem 6, ou seja se $n \mid |G|$ não garantimos que exista um subgrupo $H < G$, cuja ordem seja n, $|H| = n$.

Exercícios 3.4.9. *(1) Seja $V = \{e, a, b, c\}$, o grupo de Klein. Determine a classe lateral do subgrupo gerado por a. Este subgrupo, $< a >$, é um subgrupo normal?*

(2) Dadas as pemutações abaixo, verifique se são permutações pares ou ímpares:

a) *a permutação $\sigma = (12374)$ de S_7;*

b) *a permutação $\sigma = (125)(643)$ de S_6;*

b) *a pemutação $\sigma = (13)(45)(28)$ de S_8.*

(3) Prove todo ciclo da forma (ij) de S_n, para $1 \leq i, j \leq n; i \neq j$ é uma permutação ímpar.

(4) Prove que todo ciclo é o produto de 2-ciclos;

(5) Prove que o produto de duas permutações de mesma paridade é par e o produto de duas permutações de paridades opostas é ímpar.

(6) Refaça o execício 2, utilizando a representação de 2-ciclos para os ciclos da pemutação.

(7) Prove que A_n é um subgrupo de S_n.

3.4.1 Subgrupos Normais

Seja G um grupo. Dado um subgrupo, $H < G$, as classes laterais à esquerda e a direita, podem ser distintas! Como vimos para o grupo S_3. Nesta seção, vamos descatacar os subgrupos os quais isso não ocorre.

Definição 3.4.10. *Seja G um grupo e $H < G$, tal que $\forall g \in G$, $gH = Hg$, o grupo H é denominado subgrupo normal de G e denotado por $H \lhd G$.*

Os grupos abelianos, que são comutativos, naturalmente, são plenos em subgrupos normais, como vemos na proposição:

Proposição 3.4.11. *Se G é um grupo abeliano, então todo subgrupo de G é normal.*

Uma clase importante de grupos é aquela formada dos grupos G os quais todo subgrupo $H < G$ não é normal. A definição a seguir refere-se a estes grupos.

Definição 3.4.12. *Seja G um grupo, tal que, para todo subgrupo próprio H de G, H não é um subgrupo normal. O grupo G é denominado grupo simples.*

A seguinte proposição mostra que existem infinitos subgrupos simples, bem como, apresenta uma classe importante destes.

Proposição 3.4.13. *Seja G um grupo finito. Se $|G| = p$, um número primo, então G é um grupo simples.*

Tanto os grupos normais, quanto os grupos simples, têm papel fundamental na teoria de grupos. Isto porque, dado um grupo finito G, podemos determinar os subgrupos

$$G \rhd N_1 \rhd N_2 \cdots N_n,$$

até que N_n seja um grupo simples. Tal construção é comum em teoria de grupos, mas não estudaremos este assunto. Vamo-nos deter a um aspecto muito peculiar dos subgrupos normais de um grupo, que permite definir uma operação binária $*$ para o conjunto $\mathcal{C}_G(H) = \{gH : g \in G\}$ das classes laterais de H tal que, o conjunto $\{\mathcal{C}_G(H), *\}$ seja um grupo. Neste caso o subgrupo H é um subgrupo normal de G.

A seguinte proposição é válida, mesmo para subgrupos H que não sejam normais. Veremos adiante que a operação binária abaixo definida, no entanto, somente admite elemento neutro, se o subgrupo H é um subgrupo normal de G.

Proposição 3.4.14. *Se $D_G(H)$ é o conjunto das classes laterais à direita de H em G,*

$$\begin{array}{rccc} * : & D_G(H) \times D_G(H) & \to & D_G(H) \\ & (Hg, Hh) & \mapsto & Hgh \end{array}$$

define uma operação binária associativa em $D_G(H)$.

Demonstração. Por conveniência, vamos denotar a operação $*(Hg, Hh) \doteq HgHh$. O fato de $*$ ser operação binária é imediato pois $gh \in G \therefore gh = \mu$, e $H\mu$ é uma classe lateral, logo $H\mu \in D_G(H)$. Além disso $*$ é associativa! Com efeito, $H\mu(HvHw) = H\mu(Hvw) = H\mu(vw) = H(\mu v)w = H(\mu v)Hw = (H\mu Hv)Hw$. Portanto um operação binária associativa. □

Uma verificação rotineira mostra que a operação binária definida acima não admite elemento neutro. De fato!, $*(Hg, H) = Hg.e = Hg$; seja $h \in H, h \neq e$, sabemos que $Hh = He = H$, nessas condições Hh é elemento neutro se $*(Hg, H) = Hg = *(Hg, Hh) = Hgh$; seja $x \in Hg$ então $x = yg, y \in H$, logo não necessariamente $x = zgh$, com $z \in H$, como mostra o seguinte contra-exemplo: Seja $H =< (12) >= \{e, (12)\}$ subgrupo de S_3 e a classe lateral $H(13) = \{(13), (132)\}$ e $*$ a operação binária definida anteriormente; $*(H(13), H) = H(13)$, $(12) \in H \therefore H(12) = H$, porém $*(H(13), H(12)) = H(13)(12) = H(123) = \{(123), (23)\}$, ou seja, embora $H = H(12)$ ocorre que $*(H(13), H) \neq *(H(13), H(12)$, portanto H não é elemento neutro.

A proposição seguinte mostra que o subgrupo H ser normal no grupo G é a condição para que a operação binária definida acima tenha um elemento neutro. Além disso, o conjunto $\mathcal{C}_G(H) = D_G(H)$ é um grupo, segundo esta operação binária.

Proposição 3.4.15. *Seja G um grupo e A um subgrupo normal em G. Se $\mathcal{C}_G(H)$ é conjunto das classes laterais de H em G, então $\{\mathcal{C}_G H, *\}$, tal que $*$ é a operaçao binária*

$$\begin{array}{rccc} * : & \mathcal{C}_G(H) \times x_G(H) & \rightarrow & \mathcal{C}_G(H) \\ : & (Hg, Hh) & \rightarrow & Hgh \end{array}$$

é um grupo.

Demonstração. Basta provar que a operação binária $*$ admite elemento neutro H e satisfaz a propriedade do inverso. Com efeito H é o elemento neutro, pois se $Hg \in \mathcal{C}_G(H), *(Hg, Hh) = Hgh$ basta provar que $Hgh = Hg, \forall h \in H$ ou seja $x \in Hgh \Rightarrow \exists y \in H$, tal que $x = y(gh)$ e $gh \in gH = Hg$, pois H é normal em G, logo $gh \in Hg \Rightarrow \exists z \in H$, tal que $gh = zg \therefore x = y(gh) = y(zg) = (yz)g$; mas $y, z \in H$ que é um subgrupo $\therefore yz = w \in H \therefore x = wg \in Hg \therefore *(Hg, Hh) = Hg, \forall h \in H \Rightarrow *(Hg, Hh) = *(Hg, H) = Hg$. Seja $Hg \in \mathcal{C}_G H$, então $*(Hg, Hg^{-1}) = *(Hg, Hu) = H, \forall u \in Hg^{-1}$. A primeira parte é imediata, pois $*(Hg, Hg^{-1}) = Hgg^{-1} = He = H; *(Hg, Hu) = Hgu$, mas $u \in g^{-1}H \therefore u = h^{-1}h, h \in H \therefore Hgu = Hg(g^{-1}h) = H(gg^{-1})h = Hh = H$, que é o elemento neutro, portanto os elementos de $\mathcal{C}_G(H)$ satisfazem a propriedade do inverso e o inverso da classe Hg é a classe Hg^{-1}. □

Exemplo 3.4.16. *Para o grupo $S_3 = \{e, (12), (13), (23), (123), (132)\}$ observe que o grupo H é um subgrupo normal: $H =< (123) >= \{e, (123), (132)\}$, portanto $*((132)H, (23)H) = (132)(23)H\ (13)H = *(H, (23)H) = (23)H = \{(23), (13), (12)\}$, que mostra que H pode ser o elemento neutro, bastando checar a outra possibilidade.*

Exercícios 3.4.17. *(1) Seja G um grupo abeliano. Mostre que todo subgrupo de G é um subgrupo normal.*

(2) Prove que todo subgrupo do grupo de Klein é normal.

(3) Prove que todo subgrupo de um grupo de ordem 5 é normal.

(4) Dê exemplo de um grupo de ordem 6, em que todos os subgrupos sejam normais e um grupo de ordem 6 para o qual existe algum subgrupo não normal.

(5) Mostre que se G é um grupo abeliano, então todo subgrupo de G é normal.

(6) Prove que se um grupo G é cíclico, todo subgrupo de G é normal.

(7) Seja $Q_8 = \{1, i, j, k, -1, -i, -j, -k / o(i) = o(j) = o(k) = 2, ij = k, jk = i, ki = j\}$. Mostre que esse conjunto é um grupo multiplicativo, em que todo subgrupo deste é um subgrupo normal, porém ele, Q_8, não é um grupo abeliano.

3.4.2 Grupos Quocientes

Definição 3.4.18. *Seja $\{G, ^*\}$ um grupo, $H < G$ e $\mathcal{C}_G(H)$ o conjunto das classes laterais de H em G, o conjunto $\{\mathcal{C}_G(H), *\}$ com $*$ a operação induzida de G, é um grupo, denominado grupo quociente de H em G, denotado por $\overline{G}$.*

O elemento $gH \in \mathcal{C}_G(H)$, geralmente é denotado por $\overline{g}$; se gH e $hH \in \mathcal{C}_G(H)$, o produto $gHhG \doteq ghH$ pode ser escrito segundo a notação: $\overline{g}.\overline{h} = \overline{gh}.H$ Ocorre que se $u \in gH$, então $gH = uH \therefore \overline{g} = \overline{u}$, reciprocamente, se $\overline{g} = \overline{u} \Rightarrow \overline{g}^{-1}\overline{u} = \overline{1} = \overline{g^{-1}u} \therefore \overline{g^{-1}u} = H$, logo $\overline{g^{-1}u} = \overline{g^{-1}}\overline{u} = \overline{1} \therefore \overline{g^{-1}}\overline{u} = H \therefore u \in gH$. Assim, as classes laterais podem ser, sem perda de geralidade, representadas por $\overline{g}$, sempre que $\overline{g} = gH = gH$.

Proposição 3.4.19. *Seja G um grupo, $H \lhd G$ e $\mathcal{C}_G(H)$ o grupo quociente de H em G. O conjunto $\{\overline{g} : \overline{g} = Hg\}$, com a operação $\overline{g}.\overline{h} = \overline{gh}$ define o grupo $\mathcal{C}_G(H)$.*

Exemplo:

(1) Se $G =< i >, H =< -1 >, i^2 = -1$ o grupo $\mathcal{C}_G(H) = \{\bar{1}, \bar{i}\}$

(2) Se $G = S_3, H =< x >, o(x) = 3$, o grupo $\mathcal{C}_G(H) = \{\bar{1}, \overline{(12)}\}$

(3) Se $G = S_4, H = A_4$ o grupo de permutação pares; o grupo $\mathcal{C}_G(H) = \{\bar{1}, \overline{(12)}\}$

(4) Se $G = \mathbb{Z}, H = 4\mathbb{Z}$; o grupo $\mathcal{C}_G(H) = \{\bar{0}, \bar{1}, \bar{2}, \bar{3}\}$

(5) Se $G = D_4, H =< \rho / o(\rho) = 4 >$; o grupo $\mathcal{C}_G(H) = \{\bar{1}, \overline{(12)}\}$

Segundo a notação $\overline{g} = gH$, é comum verificar se $h \in G$ é tal que $\overline{h} = \overline{g}$. Um modo de indicar $\overline{g} = \overline{h}$, relativamente ao grupo $H \lhd G$ é utilizar a notação $modH$ isto é, a condição $\overline{g} = \overline{h}$ é denotado por $g \equiv h\ modH$.

Proposição 3.4.20. *Seja G um grupo e $H \lhd G$; $g \equiv hmod(H) \Leftrightarrow gh^{-1} \in H$.*

Demonstração. Se $g \equiv h\ modH$, então $gH = hH$ se $u \in gH$ sendo H normal em G, $gH = Hg + hH = Hh \exists v \in Hg, u = vh \Rightarrow \therefore g \in hH\ \therefore g \in hH = Hh\ \therefore g = vh \Rightarrow gh^{-1} = v \in H$ □

Proposição 3.4.21. *Seja G um grupo e $H \lhd G$ se G é um grupo finito e G/H é o grupo quociente de G por H, então $|G/H| = k$, tal que $|G| = k.|H|$.*

Demonstração. Se$H < G$, a demonstração do teorema de lagrange mostra que $|\mathcal{C}_G(H)| = k$, tal que $|G| = k|H|$ com efeito, vimos que $G = \dot{\cup} gH \Rightarrow |G| = |gH| + \ldots + |hH| = k|H|, gH \in \mathcal{C}_G(H)$ sendo $k = |\mathcal{C}_G(H)|\ \therefore |G/H| = k$ □

Definição 3.4.22. *Seja G um grupo e H subgrupo de G. Se $|\mathcal{C}_G(H)| = k$, dizemos que k é o índice de H em G e denotamos isso por $[G : k]$. Observe que o subgrupo H não necessariamente é um subgrupo normal. No entanto se $H \lhd G$, então $[G : H]$ é a ordem do grupo quociente. A seguinte proposição afirma que todo subgrupo H de índice 2 em um grupo G, é um subgrupo normal.*

Proposição 3.4.23. *Seja G um grupo e H um subgrupo de G. Se $[G : H] = 2$, então $H \lhd G$.*

Demonstração. Se $[G : H] = 2$ então há 2 classes laterais à esquerda e 2 classes laterais à direita $\{gH, H\}$ são as classes laterais à esquerda e $\{Hg, H\}$ à direita. Como vimos $G = gH \cup H = Hg \cup H$; vamos provar que $gH = Hg$. Seja $x \in gH \Rightarrow x \notin H\ \therefore x \in Hg$, logo $gH \subseteq Hg$. Da mesma forma se $y \in gH \Rightarrow y \in gH\ gH \subseteq Hg\ \therefore gH = Hg$ logo H é um subgrupo normal. □

No capítulo I, vimos que dados os conjuntos A, G e H, podemos definir uma função$f : G \to H$. Se G e H são dois grupos, como conjuntos, a definição de f é a mesma. Porém: $f(g) = u; f(h) = v, gh = k\ f(g).f(h) = u.v$

Exercícios 3.4.24. *(1) Seja $\{\mathbb{Z}, +\}$ o grupo aditivo dos números inteiros.*

- **a)** *Prove que o conjunto dos múltiplos de 3, denotado por $3\mathbb{Z}$ é um subgrupo de $\mathbb{Z}$*
- **b)** *Determine as classes laterais de $3\mathbb{Z}$ à direita e à esquerda*
- **c)** *O subgrupo $3\mathbb{Z}$ é um subgrupo normal de $\mathbb{Z}$.*

(2) Seja D_4 o grupo dihedral do quadrado. Mostre que o conjunto das rotações forma um subgrupo cíclico. Determine as classes laterais desse subgrupo.

(3) Determine o grupo dihedral D_6, apresentando todos seus elementos, mostrando geometricamente cada elemento. Lembrando que D_6 é o grupo das simetrias e rotações de um hexano.

(4) Dizemos que um grupo é simples se os únicos subgrupos normais de G são os grupos triviais, isto é, $\{e\}$ e G. Prove que todo grupo finito de ordem prima é um grupo simples.

3.4.3 Homomorfismo e Isomorfismo de Grupos

Na seção anterior definimos para um grupo G e $H \lhd G$, o grupo quociente G/H cujos elementos são as classes laterais gH, $g \in G$. Apresentamos a notação $\bar{g} \stackrel{\circ}{=} gH$, que identifica uma classe lateral $gH = \{gh/h \in H\}$ que é um conjunto, a um simbolo $\bar{g}$. Esta notação,no entanto, é uma ($profunda$) representação com um nível de abstração elevado pois não somente associa o símbolo $\bar{g}$ ao conjunto gh, mas também elege um único símbolo, entre tantos outros possíveis do conjunto gH, para representa-lo. Ou seja, vimos que $\bar{g} = \bar{k} \Leftrightarrow k \in gH \Leftrightarrow g \in kH \Leftrightarrow gH = kH \Leftrightarrow gk{-}1 \in H \Leftrightarrow gk \in H$. Por exemplo a classe lateral...poderia ser representada por... Dizemos, no entanto, que $\bar{g}$ é uma representação natural para a classe gH. Por que sendo H um grupo e $\in H \therefore G.e \in gH$, ou seja, $g \in gH$ é a escolha mais $''natural''$ para representar a classe gH. Outro significado, profundo, para a representação de $\bar{g} = gH$ é uma independ encia do representante, isto é, não importa se a classe gH está representada por $\bar{g}$ ou $\bar{k}$, para $k \in gH$. Isso permite representar a operação binária $* : \mathcal{C}_G(H)x\mathcal{C}_G(H) \to \mathcal{C}_G(H)$ $(gH, kH) \mapsto gkH$ pelos representantes $(\bar{g}\bar{k}) = (\bar{gk})$, independentemente da escolha do representante. Vimos que $*$ é o $B \therefore$ é uma função, logo devemos garantir a unicidade da imagem de $(\bar{g}e\bar{k})$. Ou seja $(\bar{g}, \bar{k}) = \bar{gk} = \bar{u}\bar{v}$, desde que $\bar{u}$ e $\bar{g}$ representem a mesma classe, ou seja $u \equiv gmodH¿$ Tal conceito, em algebra abstrata, é essencial quando representamos muitos elementos por um único símbolo, $\bar{g}$, cujo símbolo g seja um daqueles, e portanto qualquer elementos. As relações definidas dessa forma, cuja propriedade de função é verificada, dizemos que $''$está bem definida$''$. A partir daqui faremos isso constante dessa propriedade e sempre que necessário mostraremos que isso de fato ocorre.

Proposição 3.4.25. *Seja G um grupo, $H \lhd G$ e $G/H = \{\bar{g}/g \in G\}$ o grupo quociente. A relação $\mathcal{C} : G \to G/H$ $g \mapsto \bar{g}$ é uma função bem definida.*

Demonstração. Basta provar que dados $g \neq u$, tal que, $\mathcal{C}(g) = \bar{g}$ e $\mathcal{C}(g) = \bar{u}$, então $\bar{g}\bar{u}$. A função $\mathcal{C} : G \to G/Ag \mapsto \bar{g}$ sendo $\bar{g} = gH$ é uma função muito particular, pois $\mathcal{C}(e) = \bar{e} = H$ significa que $e \mapsto H$ a identidade de G é relacionada à identidade de H. $\mathcal{C}(gh) = \bar{gh} \stackrel{\circ}{=} \bar{g}\bar{h} = \mathcal{C}(g).\mathcal{C}(H)$, ou seja a imagem do produto gh em G é o produto das imagens $\mathcal{C}(g)\mathcal{C}(h)$ em G/H. □

Definição 3.4.26. *Dados dois grupos $\{G, *\}$ e $\{k\circledast\}$ e $\mathcal{C} : G \to k$ uma função com as seguintes propridades:*

(1) $\mathcal{C}(e) = \in,,$ *sendo* $\in$ *o neutro de* k.

(2) $\mathcal{C}(gh) = \mathcal{C}(g) \circledast \mathcal{C}(h)$ *A função* $\mathcal{C}$ *é denominada homomorfismo e nessas condições os grupos* G *e* H *são homomorfos.*

É desafiador compreender o significado da definição acima. Tal condição, no entanto ocorre com frequência em teoria de grupos. A seguir apresentamos alguns que exibem propriedades surpreendentes para os homomorfismos. Uma delas está ligada às propriedades estruturais de um grupo como se é cíclico comutatividade, a simplicidade do grupo, os subgrupos, a ordem dos elementos, entre outras.

Exemplo 3.4.27. *(1) O homomorfismo trivial, isto é.* $\mathcal{C} : G \to k$ $g \mapsto ek$, *o neutro do grupo* k. *As propriedades:*

a) $\mathcal{C}(e) = k$

b) $\mathcal{C}(g.h) = \mathcal{C}(gh) = \mathcal{C}ek = ek.ek = \mathcal{C}(g).\mathcal{C}(h)$ *estão satisfeitos, então* $\mathcal{C}$ *é um homomorfismo.*

(2) O homomorfismo canônico $\mathcal{C} : G \to k$, *sendo* k *o grupo quociente* G/N, *em que* N *é um subgrupo normal* $\mathcal{C} : G \to G/N$ $g \mapsto gN$ *a classe lateral de* g.

a) $\mathcal{C}(e) = eN = N$ *que é o elemento neutro do grupo* G/N.

b) $\mathcal{C}(gh) = ghN = gN.hN = \mathcal{C}(g)\mathcal{C}(h) \therefore \mathcal{C}$ *é um homomorfismo.*

(3) O homomorfismo injetor entre os grupos aditivos $\mathbb{Z}$ *e* $\mathbb{R}$ $\mathcal{C} : \mathbb{Z} \to \mathbb{R}$ $m \mapsto m$

a) $\mathcal{C}(0) = 0$ *o neutro de* $\mathbb{R}$

b) $\mathcal{C}(mn) = m.n = \mathcal{C}(m).\mathcal{C}(n)$

(4) O homomorfismo entre o grupo multiplicativo $G = \{1, -1, i, -i\}$ *e o grupo* D_4 $\mathcal{C} : G \to D_4$ $i^n \mapsto p^n$

a) $\mathcal{C}(e) = \mathcal{C}(i^4) = p^4 = e$

b) $\mathcal{C}(xy) = \xi^m.i^n) = \mathcal{C}(i^{m+n}) = pm + n = p^m.p^n = \mathcal{C}(i^m).\mathcal{C}(i^n) = \mathcal{C}(x).\mathcal{C}(y)$

(5) $G = \{\mathbb{R}, +\}$ *e* $k = \{\mathbb{R}^*, \bullet\}$, *os grupos aditivos e multiplicativos* $\mathbb{R}$ *e* $\mathbb{R}^*$ *respectivamente.* $\mathcal{C} : \mathbb{R} \to \mathbb{R}^{ast}$ $x \mapsto z^x$ *é um homo.*

a) $\mathcal{C}(0) = z^0 = 1$ *neutro do produto em* $\mathbb{R}^3$

b) $\mathcal{C}(x + y) = z^{x+y} = z^x.z^y$.

(6) Se V *e* W *são espaços vetoriais de demensão finita, Ache os reais,* V *e* W *são grupos abelianos com a operação de adição.* $T : V \to W$, *uma transformação linear é um homomorfismo.*

a) $T(0) = 0$ *pois*

b) $T(v + w) = T(v) + T(w)$.

No capítulo I, estudamos uma relação muito comum, denominada função. A nomenclatura para as funções é semelhante, com exceção do conceito de núcleo de um homomorfismo, que é semelhante ao conceito de núcleo de uma (espaço vetorial) transformação linear, pois toda transformação linear é um homomorfismo dos grupos abelianos.

Definição 3.4.28. *Sejam Gek dois grupos e* $\mathcal{C} : G \to k$ *um homomorfismo. O conjunto* $\{g/g \in G$ *e* $\mathcal{C}(g) = ek\}$ *é denominado núcleo da homomorfismo.*

Uma propriedade importante para o núcleo de um homomorfismo é que, sendo o núcleo um subconjunto de G, podemos verificar que $(\mathcal{C})$ é um subgrupo de G, que além disso é um subgrupo normal de G. Está propriedade será essencial à teoria sobre homomorfismo, pois o grupo quociente $G/ker\mathcal{C}$ e a imagem do homomorfismo $\mathcal{C}$ serão iguais, a menos de homomorfismo, que vamos apresentar o conceito na próxima seção.

Proposição 3.4.29. *Sejam* G, K *dois grupos e* $\mathcal{C} : G \to k$ *um homomorfismo. Se* $ker\mathcal{C}$ *denotar o núcleo do homomorfismo, então:*

(1) $ker\mathcal{C}$ *é subgrupo de* G

Demonstração. Sendo $ker\mathcal{C} \subseteq G$, pelo teorema, ..., basta provar que $x, y \in ker\mathcal{C}$ então $xy^{-1} \in ker\mathcal{C}$. Com efeito$\mathcal{C}(xy^{-1} = \mathcal{C}(x).\mathcal{C}(y^{-1}) = ek.\mathcal{C}(Y^{-1})$. Afirmamos que $\mathcal{C}(^{-1}) \in ker\mathcal{C}$, pois $\mathcal{C}(e) \triangleq ek = \mathcal{C}(yy^{-1}) \therefore ek = \mathcal{C}(y).\mathcal{C}(y^{-1})y^{-1} \in ker\mathcal{C}$. Então $\mathcal{C}(xy^{-1}) = ek$, logo $xy^{-1} \in ker\mathcal{C}$, logo $ker\mathcal{C}$ é subgrupo de G. □

Exercícios 3.4.30.

3.4.4 Grupos Isomorfos

Exercícios 3.4.31.

Referências Bibliográficas

[1] F. Miráglia, *Axiomática da Teoria dos Conjuntos*, edusp,1990.

[2] F. Miráglia, *O teorema de Cantor-Bernstein, in Coleção Tópicos de Matemática Elementar*, IME-USP, 1987.

[3] A. Fazzio e K. Watari, *Introdução à Teoria de Grupos com aplicações em moléculas e sólidos*, Santa Maria, editoraufsm, 1998. (240P.)

[4] J. B. Fraleigh, *A First Course in Abtract Algebra*, 5ª edição, New York, Wesley Publishing Company, 1994. (556p)

[5] A. Garcia e Y. Lequain, *Álgebra: um curso de introdução*, Rio de Janeiro, Projeto Euclides-IMPA, 1988. (213p.)

[6] F. C. Polcino Milies, *A Gênese da Álgebra Abstrata, in Coleção Tópicos de Matemática Elementar*, IME-USP, 1987.

[7] F. C. Polcino Milies e S. P. Coelho, *Números uma introdução à Matemática*, 3ª edição, São Paulo, EDUSP, 2003. (341p.)

[8] D. J. S. Robinson, *A course in the Theory of Groups*, 2^{nd} edition, London, Springer, 1995. (499 p)