Universidade Estadual da Paraíba
Centro de Ciências e Tecnologia
Departamento de Matemática

Grupos Alternados

Ana Flávia de Brito Lira

Trabalho de Conclusão de Curso

Orientador: **Prof. Dr. Vandenberg Lopes Vieira**

Banca Examinadora:
Prof. Dr. Vandenberg Lopes Vieira - DM/UEPB
Prof. Dr. Juarez Dantas de Souza - DM/UEPB
Prof. José Elias da Silva - DM/UEPB

Trabalho de Conclusão de Curso apresentado na Universidade Estadual da Paraíba, como parte dos requisitos exigidos para a obtenção do título de Licenciado em Matemática.

05 de Agosto 2013
Campina Grande - PB

FICHA CATALOGRÁFICA ELABORADA PELA BIBLIOTECA CENTRAL – UEPB

L768g Lira, Ana Flávia de Brito.
Grupos alternados [manuscrito] / Ana Flávia de Brito Lira. – 2013.
67 f.

Digitado.
Trabalho de Conclusão de Curso (Graduação em Matemática) – Universidade Estadual da Paraíba, Centro de Ciências e Tecnologia, 2013.
"Orientação: Prof. Dr. Vandenberg Lopes Vieira, Departamento de Matemática".

1. Teoria Básica dos Grupos. 2. Teoria de Galois. 3. Grupo Alternado. I. Título.

21. ed. CDD 512.5

ANA FLÁVIA DE BRITO LIRA

GRUPOS ALTERNADOS

Trabalho de conclusão de Curso apresentado na Universidade Estadual da Paraíba, como parte dos requisitos exigidos para obtenção do Título de Licenciado em Matemática.

BANCA EXAMINADORA

Prof. Dr. Vandenberg Lopes Vieira
Departamento de Matemática – CCT/UEPB
Orientador

Prof. Dr. Juarez Dantas de Souza
Departamento de Matemática – CCT/UEPB
Examinador

José Elias da Silva

Prof. José Elias da Silva
Departamento de Matemática – CCT/UEPB
Examinador

Campina Grande, 06 de Agosto de 2013

À minha família

DEDICO

Agradecimentos

Primeiramente a Deus, o qual me concedeu saúde e sabedoria para concluir mais essa etapa da minha vida.

A todos os meus familiares, em especial aos meus pais Verônica Leal e José Vital Lira, minha avó Maria do Carmo Leal, meus irmãos, Francielli, Flávio e Cicero, que sempre me incentivaram e apoiaram. Também a minha prima Ana Cláudia e seu esposo Clélio, por me acolherem tão bem em sua casa.

Aos meus professores do ensino básico, fundamental, médio, e superior, que participaram e tem uma grande importância em minha formação. Em especial aos professores Aldo Trajano Lourêdo e ao meu orientador Vandenberg Lopes Vieira, a quem tenho grande admiração.

Aos meus amigos e amigas, que estavam presentes em minha caminhada.

Resumo

Neste trabalho apresentamos alguns resultados sobre os grupos alternados A_n, que são subgrupos de grupos de permutações S_n. Os grupos A_n formam uma classe importante de grupos finitos, sendo um base para o desenvolvimento de elementos da Teoria de Galois. São apresentados como estudo inicial elementos da Teoria Básica dos Grupos, tais como grupo, homomorfismo, ciclo, órbita e permutação pares e permutação ímpar.

Palavras-chave: Grupo, Permutação, Grupo Alternado.

Sumário

Capítulo 1

Introdução

O que hoje conhecemos por grupos, foi estudado até o fim do século XVIII e no inicio do século XIX, ainda assim, somente no decorrer do século XIX é que a noção de grupo abstrato foi introduzida e, surgiu como um ramo da matemática "pura", ligado ao problema de encontrar raízes de equações algébricas por radicais, por E. Galois e outros matemáticos.

A idéia de grupo faz parte de um agrupamento de objetos matemáticos que possuem características similares. Ou seja, a função desse agrupamento é organizar estes objetos em classe de maneira que todos eles satisfaçam as mesmas propriedades. A teoria dos grupos aparece em muitas áreas da matemática e tem numerosas aplicações em outras ciências. Grupos estão por trás de muitas estruturas algébricas, como corpos e espaços vetoriais, e é uma ferramenta bastante útil para o estudo de simetrias. Por estas razões e entre outras, a teoria de grupos é uma área importante da matemática moderna.

Galois foi praticamente o primeiro a usar a noção de grupos para estudar a solubilidade das equações. Uma equação solúvel por radicais é uma equação para a qual é possível determinar suas raízes pelo processo que envolve apenas operações ordinárias de aritmética, juntamente com a extração de n-raízes. Por isso, equações algébricas de grau até quatro são solúveis por radicais. Entretanto, isso não é válido em geral para uma equação algébrica de grau $n \geq 5$. Prova-se usando o conceito de grupos entre outros que, em geral, uma equação algébrica de quinto grau não é solúvel por radicais, ou seja, não há fórmulas para determinar as raízes de uma equação arbitrária de grau

$n \geq 5$.

O estudo de equações algébricas é realizado pela Teoria de Galois. Essa teoria é a interação entre polinômios e as estruturas algébricas de grupos e corpos. Galois associou um grupo a cada polinômio e usou propriedades desse grupo para dar, para qualquer polinômio, condições para que a equação algébrica associada seja solúvel por radicais. Na realidade, Galois mostrou que uma equação algébrica é solúvel por radicais se, e somente se, o grupo de automorfismo associado à equação é solúvel. Talvez essa teoria constitua em uma das mais importantes aplicações da teoria dos grupos e seja um dos mais belos ramos da matemática, pois sintetiza resultados clássicos da teoria dos grupos e da teoria dos corpos, de modo a fornecer uma resposta completa ao problema da solubilidade de polinômios por radicais.

O estudo de equação algébrica solúvel por radicais está associado com o estudo de grupos solúveis. Esse é o principal elo entre a teoria dos grupos e essas equações. Por outro lado, o estudo de grupos solúveis é feito através do grupo alternado A_n que um subgrupo de S_n de índice dois e, portanto, de ordem $\frac{n!}{2}$.

Neste trabalho será abordado os grupos de permutações S_n tendo como foco principal o grupo alternado A_n. De inicio teremos um breve relato da história das equações algébricas sóluveis por radicais, que implicou no surgimento da teoria dos grupos. Em seguida iremos descrever sobre a teoria abstrata de grupos destacando: subgrupos, grupos cíclicos, ordem de um elemento de um grupo, classes laterais e o teorema de lagrange, homomorfismo de grupos, subgrupos normais e grupos quocientes, grupos de permutações. conceitos estes que são imprescindíveis para o estudo de A_n. Por fim abordaremos os conceitos de ciclos, órbitas e os grupos alternados que é o foco principal deste trabalho.

Capítulo 2

Breve relato histórico das equações algébricas solúveis por radicais

Neste tópico abordaremos a história do problema da resolução de equações algébricas, desde os antigos egípcios, destacando a busca pelas soluções por radicais de equações algébricas de grau n. Fazendo uma pequena abordagem das principais idéias sobre o tema e seus personagens, até alcançar o trabalho de Evariste Galois (1811-1832).

A procura por métodos para resolver problemas de determinação de incógnitas (isto é, encontrar as soluções algébricas de uma equação) sempre foi de interesse geral para todos os povos desde a antiguidade. Os primeiros registros podem ser encontrados tanto nas tabuletas de argila da suméria quanto nos papiros egípcios, onde encontramos problemas matemáticos que lidam com a resolução de equações. No Papiro Rhind, por exemplo, documento egípcio que data aproximadamente do ano 1650 a.C. e no qual o escriba conta que está copiando material que provém do ano 2000 a.C., encontramos problemas sobre distribuição de mercadorias que conduzem a equações relativamente simples, que hoje conhecemos como equações do 1° grau. Descobrimos também que os antigos babilônios sabiam resolver completamente equações de segundo grau (veja, por exemplo o Capítulo 3 de [1]).

A equação quadrática começou a ser manuseada, apesar de percebermos as manifestações destas por estudiosos de civilizações bem antigas, com Al-Khwarizmi (790-850 d.C), que deu uma classificação a tipos diferentes de equações quadráticas (embora,

somente exemplos numéricos de cada um). Os diferentes tipos de exemplos, que apresentou Al-Khwarizmi, não tiveram como solução o valor zero, nem números negativos. Ele apresenta um método para resolver cada uma destas equações. Essencialmente é a fórmula quadrática familiar, ele resolve um exemplo numérico em cada caso. Basicamente a prova para cada exemplo foi geométrica e consistia em uma "completação de quadrado".

Somente no século XII as equações quadráticas foram postas na forma como hoje conhecemos, graças à contribuição de Baskhara (matemático hindu) que a escrevera em versos.

As equações do terceiro e quarto graus tiveram suas fórmulas estabelecidas no século XVI pela escola italiana representada por S. del Ferro (1465-1526), N. Tartaglia (1500-1557), G. Cardano (1501-1576) e L. Ferrari (1522-1565), entre outros. Deve-se a del Ferro a resolução da equação cúbica (ele manteve o seu método em segredo), mais tarde também resolvida independentemente por N. Tartaglia. Tudo isso se deu até 1545, ano em que G. Cardano a publicou, com as devidas referências a del Ferro e Tartaglia, em seu livro "Ars Magna", juntamente com a fórmula da equação quártica, esta última estabelecida "a seu pedido"por seu discípulo L. Ferrari.

Um único método para resolver as equações dos primeiros quatro graus foi proposto por Leonard Euler em 1732. Ele sempre supôs que qualquer equação algébrica de grau n poderia admitir uma redução de seu grau para n -1, como acontece de fato com as equações de segundo, terceiro e quarto graus. Então propôs, para as raízes da equação de grau n, a forma

$$x = \sqrt[n]{A_1} + \sqrt[n]{A_2} + ... + \sqrt[n]{A_{n_{-1}}},$$

onde o A_i são as raízes do chamado resolvente da equação (expressão construída em função das raízes da equação dada), embora nunca tenha feito os cálculos para $n = 5$.

Uma vez que tinham sido encontrados os métodos de resolver as equações gerais de 1^o grau, quadráticas, cúbicas e quárticas, foi natural aparecer o problema de se resolver a equação geral quíntica. O famoso matemático francês Joseph-Louis Lagrange (1736-1813) em seu trabalho "Refleções sob a solução de equações algébricas"publicado em

1770-1771, criticamente examina todas as soluções das equações de segundo, terceiro e quarto grau conhecidas até sua época e demonstrou que seu êxito sempre se baseia em propriedades que não cumprem equações de quinto grau e graus superiores. Apesar de seus persistentes esforços, o problema de encontrar solução por radicais para equações de graus maiores que quatro permaneceu sem solução e constituía, em palavras do mesmo Lagrange:

" *Um desafio para a mente humana . . .* "

Foi Ruffini quem primeiro desfez a convicção dos estudiosos de álgebra quando demonstrou em 1799 a não existência de um resolvente que reduzisse o grau de equações de grau 5. Logo, também demonstrou indiretamente que as equações de quinto e maiores graus, não eram solúveis por radicais. Estes resultados estão contidos numa longa memória intitulada "Teoria generale delle equazioni". A primeira prova convincente da impossibilidade de resolução da equação quíntica foi estabelecida, no início do século XIX, pelo matemático norueguês N. H. Abel (1802-1829).

A resposta a este problema que dava fim a todo este assunto das equações deu-se ao brilhante matemático francês Evariste Galois (1811-1832). A vida de E. Galois foi curta e trágica, nascido perto de Paris em 1811, sempre foi um jovem rebelde, reprovado nas provas da escola e que brigava constantemente com seus professores, não conseguiu dedicar muito tempo de sua vida à matemática já que morreu à idade de 21 anos e nos dois últimos anos de sua vida viu-se em volta do torvelino da política na época da revolução de 1830, sendo encarcerado por amenaçar públicamente a vida do rei, o reacionário Luís Felipe.

Depois da cárcere seguiu uma briga de saias o que custou sua vida. Apesar do curto tempo de sua vida, Galois fez descobertas bastante avançadas para seu tempo em muitos ramos da matemática, em particular, deu a solução ao problema que ficava pendente na teoria das equações algébricas em um pequeno manuscrito titulado: "Memória sob as condições para resolver as equações por radicais", que fora escrito em trinta e uma páginas quase indecifráveis escritas durante a noite antes do duelo em que foi morto. E. Galois (1811-1832), caracterizou as equações com grau arbitrário n, que

são solúveis por radicais por meio de uma propriedade de certo grupo de permutações de suas raízes, atualmente denominado: O grupo de Galois. Pode-se dizer que exatamente aí nasce a teoria dos grupos. A partir desse resultado, conclui-se que a equação geral de grau $n \geq 5$ não pode ser resolvida por radicais.

Capítulo 3

Conceitos preliminares

Neste capitulo, destacaremos o conceito de grupos e de outros relacionados, que serão imprescindíveis no nosso estudo. Abordaremos conceitos de grupos, subgrupos, grupos cíclicos, ordem de elemento de um grupo, classes laterais e o Teorema de Lagrange, homomorfismo de grupos, subgrupos normais e grupo quociente e grupo de permutações. Procurando exemplificar e demonstrar os principais resultados de cada seção. Teremos um olhar especial neste capitulo para os grupos de permutações S_n, já que é de fundamental importancia para o foco principal do nosso trabalho o grupo alternado A_n.

3.1 Definição e Exemplos de Grupos

Nesta seção vamos iniciar o estudo de grupos, destacando algumas propriedades e exemplos, de modo a fixar as principais idéias apresentadas.

Definição 3.1.1 *Sejam G um conjunto não vazio e $\star$ uma operação em G. Dizemos que G munido desta operação é um* ***grupo*** *quando as propriedades seguintes são satisfeitas:*

($\mathcal{G}_1$) *A operação é associativa, isto é,*

$$a \star (b \star c) = (a \star b) \star c, \quad \forall\ a, b, c \in G.$$

($\mathcal{G}_2$) *Existe elemento neutro para* $\star$*, isto é,*

$$\exists\ e \in G \ \ tal\ que\ \ a \star e = e \star a = a, \quad \forall\ a \in G.$$

($\mathcal{G}_3$) *Todo elemento em* G *é invertível em relação à operação* $\star$*, isto é,*

$$\forall\ a \in G, \quad \exists\ a' \in G \ \ tal\ que\ \ a \star a' = a' \star a = e.$$

O grupo G assim definido será indicado por $(G, \star)$. Às vezes, para simplificar a notação, o indicaremos simplesmente por G. Isto naturalmente exige que não haja dúvida quanto à operação considerada sobre G.

Chama-se frequentemente a operação $\star$ de **produto**. Entretanto, isto não tem a princípio relação com os produtos que conhecemos sobre os conjuntos numéricos clássicos. Usa-se $a \cdot b$ ou ab (notação multiplicativa) ao invés de $a \star b$. Neste caso, diz-se que o grupo G é **multiplicativo**. Em geral, isso será considerado no desenvolvimento dos resultados sobre grupos, devendo-se apenas a uma questão de praticidade, pois tais resultados independem da notação usada para indicar a operação considerada em G. Especificamente, vamos considerar exemplos de grupos com operações indicadas por $+$, — os **grupos aditivos**.

Definição 3.1.2 *Um grupo* $(G, \star)$ *é* ***comutativo*** *ou* ***abeliano*** *quando*

$$a \star b = b \star a, \quad \forall\ a, b \in G,$$

ou seja, quando a operação em G *for comutativa.*

Exemplo 3.1.3 Com as operações usuais de adição, temos que

$$(\mathbb{Z}, +)\,, \ \ (\mathbb{Q}, +)\,, \ \ (\mathbb{R}, +) \ \ \text{e} \ \ (\mathbb{C}, +)$$

são exemplos clássicos de grupos abelianos. ♣

Exemplo 3.1.4 O conjunto $\mathbb{Z}_n = \left\{\overline{0},\ \overline{1},\ \overline{2}, \ldots, \overline{n-1}\right\}$ é um grupo abeliano sob a operação $\overline{a} + \overline{b} = \overline{a+b}, \quad \forall\ \overline{a}, \overline{b} \in \mathbb{Z}_n$.

Solução: *Inicialmente, ressaltamos que, de acordo com os resultados sobre a relação de congruência módulo n, mostra-se que*

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

define uma operação sobre $\mathbb{Z}_n$. Agora, dados $\overline{a}, \overline{b}, \overline{c} \in \mathbb{Z}_n$, temos que,

$$\begin{aligned} \overline{a} + \left(\overline{b} + \overline{c}\right) &= \overline{a} + \overline{b+c} \\ &= \overline{a + (b+c)} \\ &= \overline{(a+b) + c} \\ &= \overline{a+b} + \overline{c} \\ &= \left(\overline{a} + \overline{b}\right) + \overline{c} \end{aligned}$$

O elemento $\overline{0} \in \mathbb{Z}_n$ é tal que

$$\overline{a} + \overline{0} = \overline{a+0} = \overline{a} = \overline{0+a},$$

ou seja, $\overline{0}$ é o elemento neutro da operação. Por fim,

$$\overline{a} + \overline{n-a} = \overline{n} = \overline{0},$$

de modo que $\overline{n-a}$ é inverso aditivo de $\overline{a}$. Isso mostra que $(\mathbb{Z}_n, +)$ é um grupo, que é abeliano, pois

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

♣

Exemplo 3.1.5 O conjunto $G = M_{n\times m}(\mathbb{R})$ de todas as matrizes reais de ordem $n \times m$ é um grupo abeliano sob a adição usual. De fato,

a) $X + (Y + Z) = (X + Y) + Z, \quad \forall\ X, Y, Z \in G.$

b) $X + \mathbf{0} = \mathbf{0} + X, \quad \forall\ X \in G,$ em que

$$\mathbf{0} = \begin{pmatrix} 0 & \dots & 0 \\ \vdots & \dots & \vdots \\ 0 & \dots & 0 \end{pmatrix} \quad \text{(a matriz nula).}$$

c) Para

$$X = \begin{pmatrix} a_{11} & \dots & a_{1m} \\ \vdots & \dots & \vdots \\ a_{n1} & \dots & a_{nm} \end{pmatrix} \in G,$$

a matriz

$$Y = \begin{pmatrix} -a_{11} & \dots & -a_{1m} \\ \vdots & \dots & \vdots \\ -a_{n1} & \dots & -a_{nm} \end{pmatrix}$$

é tal que $X+Y = Y+X = \mathbf{0}$. Isso mostra que G é um grupo. A comutatividade da adição em G é imediata. ♣

Exemplo 3.1.6 Consideremos o conjunto $G = M_n(\mathbb{R})$ de todas as matrizes reais de ordem n. Sabe-se que o produto usual de matrizes é associativo, ou seja, dadas as matrizes $X, Y, Z \in G$,

$$X \cdot (Y \cdot Z) = (X \cdot Y) \cdot Z.$$

Além disso, a matriz identidade de ordem n,

$$I_n = \begin{pmatrix} 1 & 0 & \dots & 0 \\ 0 & 1 & \dots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \dots & 1 \end{pmatrix},$$

é o elemento neutro do produto, pois

$$X \cdot I_n = I_n \cdot X = X, \quad \forall\ X \in G.$$

Agora, como $\mathbf{0} \in G$ (a matriz nula de ordem n) e para tal não existe $Y \in G$, com $\mathbf{0} \cdot Y = I_n$, então $G = M_n(\mathbb{R})$ não é um grupo. Aliás, dado $X \in G$, existe $Y \in G$ tal que $X \cdot Y = I_n$ se, e somente se, $\det X \neq 0$. ♣

Exemplo 3.1.7 No exemplo anterior, observamos que em $G = M_n(\mathbb{R})$, pois a propriedade da existência de inverso não é satisfeita. No entanto, o conjunto

$$GL_n(\mathbb{R}) = \{X \in M_n(\mathbb{R}) : \det X \neq 0\} \subset G$$

é um grupo multiplicativo. De fato, pelo que foi exposto antes, é suficiente mostrar que $GL_n(\mathbb{R})$ é fechado sob o produto (já usando o fato que $I_n \in G$). Se $X, Y \in GL_n(\mathbb{R})$,

então $\det X \neq 0$ e $\det Y \neq 0$; como o determinante do produto de duas matrizes é o produto de seus determinantes, então $\det(X \cdot Y) = \det X \cdot \det Y \neq 0$, ou seja, $X \cdot Y \in GL_n(\mathbb{R})$. Logo, $GL_n(\mathbb{R})$ é fechado sob o produto e, assim, é um grupo. Chama-se $GL_n(\mathbb{R})$ **grupo linear de grau** n **sobre** $\mathbb{R}$. Nota-se que, para $n > 1$, o grupo $GL_n(\mathbb{R})$ não é abeliano. Similarmente, tem-se os grupos lineares $GL_n(\mathbb{Q})$ e $GL_n(\mathbb{C})$. ♣

Exemplo 3.1.8 O conjunto $G = \mathbb{R}^*$ munido da operação " $\star$ " definida por $a \star b = \frac{a}{b}$ não é um grupo, pois a operação não associativa. De fato, para $a = 4$, $b = 3$ e $c = 2$, temos

$$(4 \star 2) \star 3 = \frac{4}{2} \star 3 = \frac{2}{3}$$

e

$$4 \star (2 \star 3) = 4 \star \frac{2}{3} = 6,$$

isto é, $(4 \star 2) \star 3 \neq 4 \star (2 \star 3)$. ♣

Proposição 3.1.9 *Seja $(G, \star)$ um grupo. Então, as leis do cancelamento à esquerda e à direita são válidas em G, isto é, dados $a, b, c \in G$,*

$$a \star b = a \star c \;\Rightarrow\; b = c \;\; e \;\; b \star a = c \star a \;\Rightarrow\; b = c.$$

Demonstração: Como existe $a_1 \in G$ tal que $a_1 \star a = e = a \star a_1$, temos

$$\begin{aligned} a \star b = a \star c \;&\Rightarrow\; a_1 \star (a \star b) = a_1 \star (a \star c) && \text{(operando à esquerda com } a_1) \\ &\Rightarrow\; (a_1 \star a) \star b = (a_1 \star a) \star c && \text{(pois } \star \text{ é associativa)} \\ &\Rightarrow\; e \star b = e \star c && \text{(pois } a_1 \star a = e), \end{aligned}$$

isto é, $b = c$. Da mesma forma, mostra-se que $b \star a = c \star a$ implica em $b = c$. ■

Proposição 3.1.10 *Seja $(G, \star)$ um grupo. Dados $a, b \in G$, as equações lineares $a \star x = b$ e $x \star a = b$ têm únicas soluções em G.*

Demonstração: Vamos mostrar a existência e unicidade de solução apenas para equação $a \star x = b$; o outro caso é tratado similarmente. Seja $a_1 \in G$, com $a_1 \star a = e$.

Logo, o elemento $x_0 = a_1 \star b \in G$ é tal que

$$a \star (a_1 \star b) = (a \star a_1) \star b = e \star b = b,$$

isto é, x_0 é uma solução de $a \star x = b$. Suponhamos agora que $y_0 \in G$ seja outra solução. Por isso, $a \star x_0 = b$ e $a \star y_0 = b$, ou seja, $a \star x_0 = a \star y_0$. Logo, pela Proposição (3.1.9), temos $x_0 = y_0$, mostrando a unicidade de solução. ■

Proposição 3.1.11 *Seja $(G, \star)$ um grupo. Então,*

(1) *Existe único elemento $e \in G$ tal que*

$$e \star a = a \star e = a, \quad \forall\ a \in G.$$

(2) *Para cada $a \in G$, existe único $a' \in G$ tal que*

$$a' \star a = a \star a' = e.$$

Por isso, em um grupo $(G, \star)$, o elemento neutro da operação e o inverso de cada elemento em G são únicos. Chama-se o elemento neutro de " $\star$ " a **identidade** de G. Quanto ao inverso a' de a, denotaremos de modo específico por a^{-1} ou $-a$, conforme a operação em G seja multiplicativa ou aditiva, respectivamente. Por exemplo, para o grupo $(\mathbb{Z}, +)$, o inverso de $a = 3$ é $-a = -3$ $(3 + (-3) = 0 = e)$; e para o grupo $(\mathbb{R}^*, \cdot)$, o inverso de $a = 3$ é $a^{-1} = 3^{-1} = \frac{1}{3}$ $(3 \cdot 3^{-1} = 1 = e)$.

Observação 3.1.12 *No decorrer de todo texto, a identidade de um grupo G será indica por e. Além disso, se $\{G_i\}_{i \in \Lambda}$ é uma família de grupos, então e_i indicará a identidade do grupo G_i.*

Observação 3.1.13 *Em decorrência da Proposição (3.1.10), temos que um elemento $e \in G$ é a identidade do grupo $(G, \star)$ quando $e \star a = a$ para algum $a \in G$. Similarmente, para verificar que $a' \in G$ é o inverso de $a \in G$, basta mostrar que $a' \star a = e$ ou $a \star a' = e$.*

Proposição 3.1.14 *Seja G um grupo abeliano e " $\cdot$ " uma operação em G. Então,*

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

(2) $(a \cdot b)^{-1} = b^{-1} \cdot a^{-1}, \quad \forall a, b \in G.$

Demonstração: (1) Dado $a \in G$, um elemento $b \in G$ é, por definição, o inverso de a ou vice-versa, quando

$$a \cdot b = b \cdot a = e.$$

Como $a \cdot a^{-1} = a^{-1} \cdot a = e$, então $a = (a^{-1})^{-1}$.

(2) Vamos mostrar que

$$(a \cdot b) \cdot (b^{-1} \cdot a^{-1}) = (b^{-1} \cdot a^{-1}) \cdot (a \cdot b) = e. \tag{3.1}$$

Usando a propriedade associativa da operação em G, pode-se omitir os parêntesis em (3.1), de modo que

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

e

$$\begin{aligned} (b^{-1} \cdot a^{-1}) \cdot (a \cdot b) &= b^{-1} \cdot a^{-1} \cdot a \cdot b &= b^{-1} \cdot e \cdot b \\ &&= e. \end{aligned}$$

Por conseguinte, $(a \cdot b)^{-1} = b^{-1} \cdot a^{-1}$. ■

O resultado do item (2) da Proposição (3.1.14) pode ser generalizado da seguinte forma: para $a_1, a_2, \ldots, a_n \in G$,

$$(a_1 \cdot a_2 \cdots a_n)^{-1} = a_n^{-1} \cdot a_{n-1}^{-1} \cdots a_2^{-1} \cdot a_1^{-1}.$$

De fato, por indução, para $n = 2$ (o caso $n = 1$ é direto), temos $(a_1 \cdot a_2)^{-1} = a_2^{-1} \cdot a_1^{-1}$. Supondo o resultado válido para $n \geq 2$,

$$\begin{aligned} (a_1 \cdot a_2 \cdots a_n \cdot a_{n+1})^{-1} &= ((a_1 \cdot a_2 \cdots a_n) \cdot a_{n+1})^{-1} \\ &= a_{n+1}^{-1} \cdot (a_1 \cdot a_2 \cdots a_n)^{-1} \\ &= a_{n+1}^{-1} \cdot a_n^{-1} \cdot a_{n-1}^{-1} \cdots a_2^{-1} \cdot a_1^{-1}. \end{aligned}$$

3.2 Subgrupos

Consideremos agora o conceito de subgrupo de um grupo com suas propriedades. Esses subgrupos são subconjuntos especiais de um grupo G, no sentido da definição seguinte.

Definição 3.2.1 *Sejam $(G, \star)$ um grupo e H um subconjunto não vazio de G. Dizemos que H é **subgrupo** de G se, e somente se, H munido da operação induzida de G é também um grupo.*

Um subgrupo H de um grupo G será sempre indicado em símbolos como sendo,

$$H < G.$$

Observação 3.2.2 *O elemento neutro de H será indicado por e_H e é o mesmo advindo do grupo G, ou seja,*

$$e_H = e.$$

Dado um elemento $h \in H$. O inverso deste, é o mesmo tanto em H quanto em G.

Exemplo 3.2.3 Seja G um grupo qualquer. Para ele, de imediato se verifica a existência de dois subgrupos. O primeiro é seu elemento neutro $\{e\}$ e o segundo é o próprio G. Estes subgrupos são chamados de subgrupos triviais de G. ♣

Exemplo 3.2.4 Com a soma usual, temos:

$$\mathbb{Z} < \mathbb{Q} < \mathbb{R} < \mathbb{C}$$

E com a multiplicação,

$$\mathbb{Q}^* < \mathbb{R}^* < \mathbb{C}^*.$$

Esses são exemplos clássicos. ♣

Antes de mais exemplos, vamos estabelecer um critério para verificar quando um subconjunto $H \subset G$ é um subgrupo de G.

Proposição 3.2.5 *Sejam $(G, \cdot)$ um grupo e H um subconjunto não vazio de G. Então, H é subgrupo de G se, e somente se, uma das seguintes condições é verdadeira:*

(1) $h_1 \cdot h_2 \in H \quad e \quad h_1^{-1} \in H, \quad \forall\ h_1, h_2 \in H.$

(2) $h_1 \cdot h_2^{-1} \in H, \quad \forall\ h_1, h_2 \in H.$

Mais exemplos

Exemplo 3.2.6 O subconjunto

$$H = \left\{ \begin{pmatrix} a & b \\ c & -a \end{pmatrix} \in M_2(\mathbb{R}) \right\}$$

é subgrupo do grupo aditivo $G = M_2(\mathbb{R})$. De fato, consideremos $A, B \in H$, digamos

$$A = \begin{pmatrix} a & b \\ c & -a \end{pmatrix} \quad \text{e} \quad B = \begin{pmatrix} r & s \\ t & -r \end{pmatrix}.$$

Assim,

$$A + B = \begin{pmatrix} a & b \\ c & -a \end{pmatrix} + \begin{pmatrix} r & s \\ t & -r \end{pmatrix} = \begin{pmatrix} a+r & b+s \\ c+t & -(a+r) \end{pmatrix} \in H$$

e

$$-A = \begin{pmatrix} -a & -b \\ -c & +a \end{pmatrix} \in H.$$

Por isso, H é subgrupo de G. ♣

Exemplo 3.2.7 O subconjunto $H = \{A \in GL_n(\mathbb{R});\ \det A = 2\}$ não é subgrupo de $(GL_n(\mathbb{R}), \cdot)$. De fato, tomando $A, B \in H$, motiva que

$$\det A = 2 \quad \text{e} \quad \det B = 2.$$

Mas

$$\det(AB) = \det A \cdot \det B = 2 \cdot 2 = 4 \Rightarrow \det(AB) \notin H.$$

Logo, H não é subgrupo de $(GL_n(\mathbb{R}), \cdot)$. ♣

Exemplo 3.2.8 Considerando o grupo aditivo $\mathbb{Z}_8 = \{\bar{0},\ \bar{1},\ \bar{2},\ \bar{3},\ \bar{4},\ \bar{5},\ \bar{6},\ \bar{7}\}$, vamos verificar quais dos subconjuntos abaixo são subgrupos de $\mathbb{Z}_8$.

$$H_1 = \{\bar{0},\ \bar{1}\},\ H_2 = \{\bar{0},\ \bar{4}\}.$$

Solução: *Para H_1, temos que $\bar{1} \in H_1$ e $\bar{1} + \bar{1} = \bar{2} \notin H_1$.*

Logo, H_1 não é subgrupo de $\mathbb{Z}_8$.

Com $H_2 = \{\bar{0},\ \bar{4}\}$, $\bar{4} + \bar{4} = \bar{0} \in \mathbb{Z}_8$.

Portanto, H_1 é subgrupo de $\mathbb{Z}_8$. ♣

3.3 Grupos Cíclicos

Nesta seção destacaremos a classe dos grupos cíclicos. Esses grupos são essenciais para o estudo de grupos. Como exemplos de tais grupos, destacam-se os grupos $(\mathbb{Z}, +)$ e $(\mathbb{Z}_n, +)$. Estes são os exemplos mais importantes; isso se deve ao fato de que qualquer grupo cíclico é equivalente a $(\mathbb{Z}, +)$ ou $(\mathbb{Z}_n, +)$ para algum n. Quando dizemos que dois grupos são *equivalentes,* queremos dizer que eles possuem as mesmas propriedades algébricas.

Começaremos com a seguinte:

Definição 3.3.1 *Seja $(G, \cdot)$ um grupo. Dados $a \in G$ e $n \in \mathbb{Z}$, define-se a n-ésima potência de a, em símbolos a^n, da seguinte forma:*

$$a^n = \begin{cases} e & se \quad n = 0, \\ a^{n-1} \cdot a & se \quad n > 0, \\ (a^{-n})^{-1} & se \quad n < 0. \end{cases}$$

De acordo com a definição, dado $n \in \mathbb{N}$,

$$a^n = a \cdot a \cdot \cdots \cdot a \quad (n \text{ fatores})$$

e

$$a^{-n} = a^{-1} \cdot a^{-1} \cdot \cdots \cdot a^{-1} \quad (n \text{ fatores}).$$

Se a operação em G for aditiva, então define-se múltiplo de a, $n \cdot a$, ao invés de potência de a. Assim,

$$n \cdot a = \begin{cases} e & \text{se} \quad n = 0, \\ (n-1)a + a & \text{se} \quad n > 0, \\ (-n)(-a) & \text{se} \quad n < 0. \end{cases}$$

Da mesma forma, para $n \in \mathbb{N}$,

$$n \cdot a = a + a + \cdots + a \quad (n \text{ parcelas})$$

e

$$n \cdot (-a) = (-a) + (-a) + \cdots + (-a) \quad (n \text{ parcelas})$$

Exemplo 3.3.2 No grupo multiplicativo $(\mathbb{Q}^*, \cdot)$, $(\frac{1}{2})$

$$\left(\tfrac{1}{2}\right)^3 = \left(\tfrac{1}{2}\right)^2 \cdot \tfrac{1}{2} = \tfrac{1}{8} \quad \text{e} \quad \left(\tfrac{1}{2}\right)^{-3} = \left(\left(\tfrac{1}{2}\right)^3\right)^{-1} = 8$$

Já para os grupos aditivos $(\mathbb{Z}, +)$ e $(\mathbb{Z}_6, +)$,

$$2 \cdot 3 = 3 + 3 = 6 \quad \text{e} \quad (-2) \cdot 3 = 2 \cdot (-3) = -6$$

e

$$4 \cdot \overline{2} = \overline{2} + \overline{2} + \overline{2} + \overline{2} = \overline{2} \quad \text{e} \quad (-3) \cdot \overline{2} = 3 \cdot \left(-\overline{2}\right) = 3 \cdot \overline{4} = \overline{0}.$$

♣

Proposição 3.3.3 *Seja G um grupo. Dado $a \in G$ e n, $m \in \mathbb{Z}$, então*

(1) $a^n \cdot a^m = a^{n+m}$.

(2) $(a^n)^m = a^{nm}$.

Consideremos um grupo $(G, \cdot)$. Dado $a \in G$, o subconjunto H dado por

$$H = \{a^n : n \in \mathbb{Z}\} \tag{3.2}$$

vamos mostrar que $H < G$. Inicialmente temos que, $H \neq \emptyset$, pois $e = a^0 \in H$. Agora, sejam $h_1, h_2 \in H$, digamos $h_1 = a^{n_1}$ e $h_2 = a^{n_2}$, n_1, $n_2 \in \mathbb{Z}$, temos que

$$h_1 \cdot h_2 = a^{n_1} \cdot a^{n_2} = a^{n_1+n_2} \in H.$$

Agora,

$$h_1^{-1} = (a^{n_1})^{-1} = a^{-n_1} \in H.$$

Por isso, $H < G$. O subgrupo H em (3.2) chama-se **subgrupo cíclico** gerado por a. Diz-se também que a é um gerador de H. Em símbolos,

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

Às vezes pode ocorrer que $H = G$.

Isso nos leva à definição:

Definição 3.3.4 *Um grupo G é dito* ***cíclico*** *quando existir $a \in G$ de maneira que*

$$G = \langle a \rangle .$$

Observação 3.3.5 *Para um grupo cíclico $G = \langle a \rangle$ há duas possibilidades:*

(a) *$a^n = e$ para algum $n \in \mathbb{N}$. Neste caso, G tem ordem finita. Ou,*

(b) *$a^n \neq e$ para todo $n \in \mathbb{N}$. Neste caso, todas as potências de a são distintas e G tem ordem infinita.*

Exemplo 3.3.6 Se $G = \{e\}$, então $G = \langle e \rangle$, ou seja, G é cíclico. ♣

Exemplo 3.3.7 Para cada $n \in \mathbb{N}$, o grupo $(\mathbb{Z}_n, +)$ é cíclico. De fato, dado $\overline{a} \in \mathbb{Z}_n$,

$$\overline{a} = \overline{1 + 1 + \cdots + 1} = \overline{1} + \overline{1} + \cdots + \overline{1}. \quad (a \text{ vezes})$$

Desse modo,

$$\overline{a} = a \cdot \overline{1} \Rightarrow \overline{a} \in \left\langle \overline{1} \right\rangle .$$

Isso mostra que $\mathbb{Z}_n \subset \left\langle \overline{1} \right\rangle$, e como $\left\langle \overline{1} \right\rangle \subset \mathbb{Z}_n$, então $\left\langle \overline{1} \right\rangle = \mathbb{Z}_n$. ♣

Exemplo 3.3.8 Vamos verificar se o grupo $\mathbb{Z}_2 \times \mathbb{Z}_2$ é cíclico.

Solução: *Sabemos que:*

$$\mathbb{Z}_2 \times \mathbb{Z}_2 = \{(\bar{0}, \bar{0}), (\bar{0}, \bar{1}), (\bar{1}, \bar{0}), (\bar{1}, \bar{1})\} .$$

Vamos determinar os subgrupos gerados pelos elementos de $\mathbb{Z}_2 \times \mathbb{Z}_2$.

$$\alpha_1 = (\bar{0}, \bar{1}), \ 2\alpha_1 = \alpha_1 + \alpha_1 = (\bar{0}, \bar{1}) + (\bar{0}, \bar{1}) = (\bar{0}, \bar{0}) = e$$

Logo

$$\langle \alpha_1 \rangle = \langle (\bar{0}, \bar{1}) \rangle = \{(\bar{0}, \bar{0}), (\bar{0}, \bar{1})\}$$

Para,

$$\alpha_2 = (\bar{1}, \bar{0}), \ 2\alpha_2 = \alpha_2 + \alpha_2 = (\bar{1}, \bar{0}) + (\bar{1}, \bar{0}) = (\bar{0}, \bar{0}) = e$$

Assim,

$$\langle \alpha_2 \rangle = \langle (\bar{1}, \bar{0}) \rangle = \{ (\bar{0}, \bar{0}), (\bar{1}, \bar{0}) \}$$

Da mesma forma, com $\alpha_3 = (\bar{1}, \bar{1})$*,*

$$\langle \alpha_3 \rangle = \langle (\bar{1}, \bar{1}) \rangle = \{ (\bar{0}, \bar{0}), (\bar{1}, \bar{1}) \}$$

Logo, $\mathbb{Z}_2 \times \mathbb{Z}_2$ *não é ciclico. Este é um exemplo clássico de um grupo abeliano que não é cíclico.* ♣

Proposição 3.3.9 *Todo grupo cíclico é abeliano.*

Demonstração: Seja G um grupo cíclico. Digamos $G = \langle a \rangle$, e $x, y \in G$. Logo,

$$x = a^{n_1} \text{ e } y = a^{n_2},\ n_1, n_2 \in \mathbb{Z}$$

Dessa forma,

$$x \cdot y = a^{n_1} \cdot a^{n_2} = a^{n_1+n_2} = a^{n_2+n_1} = a^{n_2} \cdot a^{n_1} = y \cdot x.$$

Logo, G é abeliano. ■

3.4 Ordem de um elemento de um grupo

Consideremos agora o conceito de ordem de um elemento de um grupo, que será de grande importancia para o decorrer de nosso trabalho, uma vez que seus resultados serão imprescindiveis para o estudo de importantes teoremas, como é o caso do teorema de Lagrange.

Definição 3.4.1 *Sejam* G *um grupo e* $a \in G$*. Se existe* $n \in \mathbb{N}$ *tal que* $a^n = e$*, diz-se que o elemento* a *tem* ***ordem finita*** *(ou é de ordem finita). Neste caso, o menor inteiro positvo* m *tal que* $a^m = e$ *chama-se* ***ordem*** *de* a*, a qual denotaremos por* $O(a)$*. Caso não exista nenhum* $n \in \mathbb{N}$ *satisfazendo* $a^n = e$*, então o elemento* a *é dito ser de* ***ordem infinita****.*

Em um grupo G, tem-se sempre

$$O(a) = 1 \Leftrightarrow a = e.$$

Exemplo 3.4.2 No grupo multiplicativo $G = \{1, -1, i, -i\}$, $O(-1) = 2$, pois $-1^2 = 1 = e$. Além disso, $O(i) = O(-i) = 4$. ♣

Proposição 3.4.3 *Seja G um grupo. Dado $a \in G$ e $a \neq e$, então*

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

(2) $O(a) = O(a^{-1})$.

(3) Se $O(a) = 2, \quad \forall\ a \in G - \{e\}$, então G é abeliano.

Teorema 3.4.4 *Sejam G um grupo e $a \in G$.*

(1) *Se $a^n = e$ para algum $n \in \mathbb{N}$, então $O(a)$ divide n.*

(2) *Se $O(a) = m$, então para qualquer $k \in \mathbb{Z}$, $a^k = a^r$, sendo r o resto da divisão de k por m.*

(3) *$O(a) = m$ se, e somente se, $\langle a \rangle$ tem ordem m.*

O teorema a seguir é uma reciproca do teorema de Lagrange para grupos cíclicos finitos.

Teorema 3.4.5 *Seja $G = \langle a \rangle$ um grupo cíclico finito de ordem n. Então para cada divisor de $\mathbb{N}$ de n,existe único subgrupo H de G tal que*

$$|H| = d$$

Exemplo 3.4.6 Consideremos o grupo $\mathbb{Z}_8 = \{\bar{0},\ \bar{1},\ \bar{2},\ \bar{3},\ \bar{4},\ \bar{5},\ \bar{6},\ \bar{7}\}$. Sabemos que $\mathbb{Z}_8 = \langle \bar{1} \rangle = \langle \bar{3} \rangle = \langle \bar{5} \rangle = \langle \bar{7} \rangle$. Vamos escolher $a = \bar{1}$. Como $d = 4$ divide $|\mathbb{Z}_8| = 8$, vamos determinar o subgrupo H de $\mathbb{Z}_8$ com ordem 4. Temos,

$$n = 8 \ \ e \ \ 8 = 4 \cdot 2 \Rightarrow m = 2.$$

Logo, H é dado por:

$$H = \langle 2 \cdot \bar{1} \rangle = \langle \bar{2} \rangle \Rightarrow H = \langle \bar{2} \rangle .$$

Aqui, $O(2) = |H| = 4$. Assim,

$$\langle \bar{2} \rangle = \{\bar{0},\ \bar{2},\ 2 \cdot \bar{2},\ 3 \cdot \bar{2}\} = \{\bar{0},\ \bar{2},\ \bar{4},\ \bar{6}\} .$$

♣

3.5 Classes laterais e o teorema de lagrange

Nesta seção trataremos do teorema de Lagrange que é o principal resultado sobre grupos finitos. Para tanto, é necessário o estudo das classes laterais que são classes de equivalência, obtidas de relações de equivalência convenientemente construídas.

Consideremos um grupo G e H um subgrupo de G. Sobre G seja $(\equiv_E (\mathrm{mod}\, H)$ a relação dada para qualquer $x, y \in G$, por

$$x \ \equiv_E y \ \Leftrightarrow x^{-1} \cdot y \ \in \ H$$

Mostraremos que $\equiv_E$ é de equivalência.

Consideremos $a, b, c \in G$.

($\equiv_E$ **é reflexiva)** Como $a^{-1}a = e \in H$, então $a \equiv_E a(\mathrm{mod}\, H)$, ou seja, $\equiv_E$ é reflexiva.

($\equiv_E$ **é simétrica)** Se $a \equiv_E b(\mathrm{mod}\, H)$, então $a^{-1}b \in H$. Mas,

$$a^{-1}b \in H \Rightarrow (a^{-1}b)^{-1} \in H \Rightarrow b^{-1}a \in H \Rightarrow b \equiv_E a(\mathrm{mod}\, H),$$

de modo que $\equiv_E (\mathrm{mod}\, H)$ é simétrica.

($\equiv_E$ **é transitiva)** Se $a \equiv_E b(\mathrm{mod}\, H)$ e $b \equiv_E c(\mathrm{mod}\, H)$, então $a^{-1}b = h_1 \in H$ e $b^{-1}c = h_2 \in H$. Como $H < G$,

$$(a^{-1}b)\left(b^{-1}c\right) = h_1h_2 \in H \Rightarrow a^{-1}c \in H \Rightarrow a \equiv_E c(\mathrm{mod}\, H).$$

Assim, $\equiv_E (\mathrm{mod}\, H)$ é transitiva e, por isso, é de equivalência. ■

Proposição 3.5.1 *Sejam G um grupo e H um subgrupo de G então, dado $x \in G$, sua classe de equivalência é dada por $\bar{x}$ segundo à relação $\equiv_E$.*

$$\bar{x} = \{xh : h \ \in H\} .$$

Demonstração: Dado $y \in \bar{x}$, temos

$$y \in \bar{x} \Leftrightarrow y \equiv_E x \Leftrightarrow y^{-1}x \ \in H.$$

Logo,

$$y^{-1}x = hx^{-1} \Rightarrow y = xh^{-1} \ \in \ \{xh : h \in H\}$$

isto é, $\bar{x} \subset \{xh : h \ \in H\}$.

Por outro lado, seja $y \in \{xh : h \ \in H\}$. Logo,

$$y = xh, \ h \in H.$$

Assim,

$$x^{-1}y = h \Rightarrow x \equiv_E y \Rightarrow y \in \bar{x}.$$

Por isso, $\{xh : h \in H\} \subset \bar{x}$.

Daí, $\bar{x} = \{xh : h \in H\}$. ■

Observação 3.5.2 *A classe de equivalência de $x \in G$ segundo $\equiv_E$ chama-se classe lateral à esquerda de H determinada por x, ou simplismente classe lateral de x à esquerda, caso não haja dúvida quanto ao subgrupo H. Além disso, vamos denotar $\bar{x}$ por xH, ou seja,*

$$xH = \{xh : h \in H\}.$$

Da mesma forma prova-se que a relação $\equiv_D$ sobre G dada por,

$$x \equiv_D y \Leftrightarrow x \cdot y^{-1} \in H, \quad \forall \ x, y \in G,$$

é de equivalência. Além disso, a classe de equivalência de $x \in G$ segundo $\equiv_D$ é

$$\bar{x} = \{hx : h \in H\}.$$

Assim denotaremos por $H - x$, ou seja,

$$Hx = \{hx : h \in H\}.$$

E chamaremos classe lateral de x à direita.

Decorrem duas coisas importantes: Primeiramente,

$$\bigcup_{x\in G} x \cdot H = G. \tag{3.3}$$

e

$$x \cdot H \cap y \cdot H = \emptyset. \tag{3.4}$$

Os resultados de (3.3) e (3.4) são válidos também para as classes laterais à direita.

Além disso:

1) Se G for abeliano, então dado $x \in G$,

$$xH = \{xh : h \in H\} = \{hx : h \in H\} = Hx.$$

2) O próprio H é tanto uma classe lateral à esquerda quanto à dieita, pois

$$eH = \{eh : h \in H\} = \{h : h \in H\} = H = He.$$

3) Dado $x \in G$,

$$\begin{aligned} xH = H &\Leftrightarrow xh = eH \\ &\Leftrightarrow x \equiv_E e \Leftrightarrow x^{-1}e \in H \\ &\Leftrightarrow x^{-1} \in H \Leftrightarrow x \in H. \end{aligned}$$

Ou seja,

$$xH = H \Leftrightarrow x \in H.$$

Da mesma forma

$$Hx = H \Leftrightarrow x \in H.$$

Exemplo 3.5.3 Considere o grupo aditivo $\mathbb{Z}_6$ e o subgrupo $H = \{\bar{0}, \bar{3}\}$, determinemos as classes laterais.

Solução: *Sendo G abeliano, segue que*

$$x + H = H + x, \quad \forall\, x \in G.$$

Como $\bar{0}, \bar{3} \in H$, então

$$\bar{0} + H = H = \bar{3} + H.$$

Agora,

$$\bar{1} + H = \{\bar{1} + \bar{0}, \bar{1} + \bar{3}\} = \{\bar{1}, \bar{4}\} = \bar{4} + H.$$

$$\bar{2} + H = \{\bar{2} + \bar{0}, \bar{2} + \bar{3}\} = \{\bar{2}, \bar{5}\} = \bar{5} + H.$$

Logo

$$H,\ \bar{1} + H,\ \bar{2} + H.$$

são as únicas únicas classes laterais à esquerda(à direita). ♣

Exemplo 3.5.4 Sejam $G = (\mathbb{Z}, +)$ e $H = 3\mathbb{Z} = \{3k : k \in \mathbb{Z}\}$. Como G é abeliano, então o conjunto H_E é igual a H_D. Sendo G infinito, vamos considerar um elemento arbitrário $n \in \mathbb{Z}$ e analisar as possíveis classes $n + 3\mathbb{Z}$. Não há mais nada natural do que fazer uso do Algoritmo da Divisão e considerar os resultados sobre classes laterais (de equivalência) vistos até aqui. Por esse algoritmo, existem $q, r \in \mathbb{Z}$ tais que

$$n = 3q + r \quad \text{com} \quad r \in \{0, 1, 2\}.$$

Dessa forma,

$$n - r = 3q \in H \Leftrightarrow n \equiv_E r.$$

Portanto, sendo $\equiv_E$ uma relação de equivalência sobre G, tem-se

$$n + 3\mathbb{Z} = r + 3\mathbb{Z}.$$

Mas, como $r = 0$, $r = 1$ ou $r = 2$, então $0 + 3\mathbb{Z} = 3\mathbb{Z}$, $1 + 3\mathbb{Z} = \{1 + 3\lambda : \lambda \in \mathbb{Z}\}$ e $2 + 3\mathbb{Z} = \{2 + 3\lambda : \lambda \in \mathbb{Z}\}$ são as únicas classes à esquerda (à direita) de H. Consequentemente, $H_E = H_D = \{3\mathbb{Z}, 1 + 3\mathbb{Z}, 2 + 3\mathbb{Z}\}$. ♣

Proposição 3.5.5 *Os conjuntos H_E e H_D tem o mesmo número de elementos (mesma cardinalidade).*

Demonstração: Basta notar que a aplicação

$$\begin{array}{rccc} \varphi: & H_E & \longrightarrow & H_D \\ & x \cdot H & \longmapsto & H \cdot x^{-1}. \end{array}$$

é uma bijeção. ■

Proposição 3.5.6 *Sejam G um grupo e H um subgrupo de G. Então cada classe lateral à esquerda(à direita) tem a mesma cardinalidade de H.*

O Teorema de Lagrange é a base da teoria dos grupos finitos. Mais antes desse teorema, vamos considerar o conceito de índice de um subgrupo.

A cardinadidade do conjunto H_E (que é a mesma do conjunto H_D como vimos na proposição (3.5.5), chama-se índice de H em G, e denota-se por

$$(G : H).$$

Considerando $H = \{\bar{0},\ \bar{3}\}$ e $G = \mathbb{Z}_6$, então

$$H_E = \{H,\ \{\bar{1},\ \bar{4}\},\ \{\bar{2},\ \bar{5}\}\}.$$

Logo,

$$(G : H) = 3$$

Nota-se que:

$$6 = 2 \cdot 3 \Rightarrow |G|\ = |H|\ \cdot (G : H).$$

Teorema 3.5.7 (Teorema de Lagrange) *Sejam G um grupo finito e H um subgrupo de G. Então a ordem de H divide a ordem de G. Especicamente,*

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

Demonstração: Consideremos $|G| = n$. Sendo G finito, então H_E também é finito. Façamos então

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

Como H_E é uma partição de G, então:

$$G = \bigcup_{x \in G} xH \tag{3.5}$$

Considere $H_E = \{x_1H,\ x_2H, ...,\ x_rH\ \}$. Reescrevendo (3.5), temos:

$$G = \bigcup_{k=1}^{r} x_kH,$$

ou seja,

$$G = x_1H \ \cup \ x_2H \ \cup \ ... \ \cup \ x_rH.$$

Por isso, pela proposição 3.5.6,

$$\begin{aligned} |G| \ &= \ |H| \ + |H| \ + \ ... \ + |H| \\ |G| \ &= r \cdot |H|. \end{aligned}$$

Logo,

$$|G| \ = |H| \ \cdot (G : H) \, .$$

■

Corolário 3.5.8 *Sejam G um grupo finito e $x \in G$. Então, $O(x)$ divide a ordem de $|G|$. Em particular,*

$$x^{|G|} = e.$$

Corolário 3.5.9 *Todo grupo G de ordem prima é cíclico.*

Corolário 3.5.10 *Todo grupo de ordem menor ou igual a cinco é abeliano.*

3.6 Homomorfismos de grupos

Neste tópico destacamos as principais propriedades de homomorfismo de grupos que serão usadas no decorrer do trabalho. Apresentamos exemplos de isomorfismos de grupos, que são homomorfismos bijetivos. Destacando também o núcleo e imagem de um homomorfismo.

Definição 3.6.1 *Considere os grupos $(G_1, \star)$ e $(G_2, \cdot)$. Uma função $f : G_1 \longrightarrow G_2$ é dita* ***homomorfismo*** *quando a seguinte condição é satisfeita:*

$$f\left(a \star b\right) = f\left(a\right) \cdot f\left(b\right), \quad \forall \ a, b \in G_1.$$

Pelo método de indução finita, podemos mostrar que:

$$f\left(a_1 \star a_2 \star \cdots \star a_n\right) = f\left(a_1\right) \cdot f\left(a_2\right) \cdot \ldots \cdot f\left(a_n\right), \quad \forall a_1, \ a_2, \ \ldots, \ a_n \in G_1.$$

Exemplo 3.6.2 Sejam G_1 e G_2 dois grupos quaisquer. A função $f : G_1 \longrightarrow G_2$ dada por $f(x) = e_2, \quad \forall\ x \in G_1$é um homomorfismo, chamado homomorfismo trivial. ♣

Exemplo 3.6.3 Seja G um grupo qualquer. A aplicação $Id\ G(x) = x, \quad \forall\ x \in G$ é um homomorfismo, chamado de homomorfismo identidade. ♣

Exemplo 3.6.4 Considere os grupos $G_1 = (\mathbb{Z}, +)$ e $G_2 = (\mathbb{Z} \times \mathbb{Z}, +)$. Mostre que a aplicação

$$\begin{array}{rccc} f: & \mathbb{Z} & \longrightarrow & \mathbb{Z} \times \mathbb{Z} \\ & f(x) & = & (x, 0), \quad \forall\ x \in \mathbb{Z}. \end{array}$$

É um homomorfismo.

Solução: *Sejam x, $y \in \mathbb{Z}$. Então,*

$$f(x + y) = (x + y, 0) = (x, 0) + (y, 0) = f(x) + f(y).$$

Logo f é um homomorfismo. ♣

Exemplo 3.6.5 Considere os grupos $G_1 = (\mathbb{R}_+, \cdot)$ e $G_2 = (\mathbb{R}, +)$. Mostre que a aplicação

$$\begin{array}{rccc} h: & \mathbb{R}_+ & \longrightarrow & \mathbb{R} \\ & x & \longmapsto & \log x \end{array}$$

é um homomorfismo.

Solução: *Consideremos $x, y \in \mathbb{R}_+$. Assim,*

$$h(x \cdot y) = \log x \cdot y = \log x + \log y = h(x) + h(y)$$

O que mostra que h é homomorfismo. ♣

Exemplo 3.6.6 Sejam $G_1 = (\mathbb{Z}, +)$ e $G_2 = (\mathbb{R}, +)$. Verifique se função $g : \mathbb{Z} \longrightarrow \mathbb{R}$ dada por

$$f(x) = x + 2.$$

É um homomorfismo.

Solução: *Ora, se* $x, y \in \mathbb{Z}$*, então*

$$f(x+y) = x + y + 2.$$

Por outro lado,

$$f(x) + f(y) = x + y + 4.$$

Ou seja,

$$f(x+y) \neq f(x) + f(y).$$

Logo, g não é homomorfismo. ♣

Proposição 3.6.7 *Sejam* G_1 *e* G_2 *grupos multiplicativos e* $f : G_1 \longrightarrow G_2$ *um homomorfismo de grupos. Assim, considerando* e_1 *o elemento neutro de* G_1 *e* e_2 *o de* G_2*, vale que*

(1) $f(e_1) = e_2$.

(2) $f(x^{-1}) = f(x)^{-1}, \forall\ x \in G_1$.

Demonstração: Vamos demonstrar apenas o item (1). Sabemos que $e_1 = e_1 \cdot e_1$. Logo,

$$\begin{array}{rcl} e_1 = e_1 \cdot e_1 \Rightarrow f(e_1) = f(e_1 \cdot e_1) = f(e_1) \cdot f(e_1) \\ \Rightarrow f(e_1) = f(e_1 \cdot e_1) \\ \Rightarrow f(e_1) = e_2 \end{array}$$

■

3.6.1 Núcleo e imagem de um homomorfismo

Consideraremos agora os conceitos de núcleo e imagem de um homomorfismo, conceitos estes que serão imprescindiveis para o estudo do principal resultado dessa seção que é o Teorema Fundamental dos Homomorfismos.

Seja $f : G_1 \longrightarrow G_2$ um homomorfismo de grupos. O núcleo desse homomorfismo denotado por $N(f)$ ou $Ker(f)$ é o seguinte conjunto

$$N(f) = \{x \in G_1;\ f(x) = e_2\}.$$

Vale ressaltar que como $f(e_1) = e_2$, então $e_1 \in N(f)$. Portanto, ao menos o elemento neutro de G_1 pertence ao núcleo de f.

Definição 3.6.8 *Seja $f : G_1 \longrightarrow G_2$ um homomorfismo de grupos. A imagem desse homomorfismo denotada por* $\mathrm{Im}(f)$ *é o seguinte conjunto*

$$\mathrm{Im}(f) = \{f(x) \in G_2;\ x \in G_1\}.$$

Exemplo 3.6.9 Vamos determinar o núcleo e a imagem do homomorfismo $f : \mathbb{R}_+ \longrightarrow \mathbb{R}$ definido por $f(x) = \log x$. *(conferir exemplo (3.6.5)).*

Solução: *Dado $x \in \mathbb{R}_+$, temos*

$$x \in N(f) \Leftrightarrow f(x) = e_2 \Leftrightarrow \log x = 0 \Leftrightarrow x = 1$$

Portanto,

$$N(f) = \{x \in G;\ f(x) = e_2\} = \{1\} = \{e_1\}$$

Além disso, consideremos $y \in \mathbb{R}$ de modo a verificar se existe para ele, $x \in \mathbb{R}_+$ de modo que $f(x) = y$. Temos,

$$f(x) = y \Leftrightarrow \log x = y \Leftrightarrow x = 10^y \in \mathbb{R}_+$$

Logo,

$$f(10^y) = y, \quad \forall y \in \mathbb{Z}.$$

implicando que

$$\mathrm{Im}(f) = \{f(x) \in \mathbb{R};\ x \in \mathbb{R}_+\} = \mathbb{R}$$

♣

Exemplo 3.6.10 Considere os grupos $G_1 = (\mathbb{R}^2, +)$ e $G_2 = (\mathbb{R}, +)$. Verifique se a função $g : \mathbb{R}^2 \longrightarrow \mathbb{R}$ definida por $g(x, y) = x$ é um homomorfismo, caso seja determine $N(g)$ e $\mathrm{Im}(g)$.

Solução: *Observe que* $g(0,0) = 0 = e_2$. *Agora, sejam* $\alpha_1 = (x_1, y_1)$ *e* $\alpha_2 = (x_2, y_2)$ *pontos em* $\mathbb{R}^2$, *temos*

$$g(\alpha_1 + \alpha_2) = g(x_1 + x_2, y_1 + y_2) = x_1 + x_2 = g(x_1, y_1) + g(x_2, y_2) =$$
$$= g(\alpha_1) + g(\alpha_2)$$

Logo g *é um homomorfismo. Determinemos agora* $N(g)$ *e* $\mathrm{Im}(g)$. *Consideremos* $\alpha = (x, y) \in \mathbb{R}^2$. *Dado*

$$\alpha \in N(g) \Leftrightarrow g(\alpha) = e_2 \Leftrightarrow g(x, y) = 0 \Leftrightarrow x = 0$$

Logo,

$$N(g) = \{\alpha \in \mathbb{R}^2 : \ x = 0\} = \{(0, y) : \ y \in \mathbb{R}\}$$

Agora, dado $b \in \mathbb{R}$, $b \in \mathrm{Im}(g)$ *se, e somente se, existe* $(x, y) \in \mathbb{R}^2$ *tal que*

$$g(x, y) = b \Leftrightarrow x = b$$

Por isso, $g(b, y) = b$,*qualquer que seja o* $y \in \mathbb{R}$. *Desse modo,*

$$\mathrm{Im}(g) = \mathbb{R}.$$

♣

Proposição 3.6.11 *Seja* $f : G_1 \longrightarrow G_2$ *um homomorfismo de grupos. Então são válidas as seguintes:*

(1) $N(f) < G_1$ (O núcleo é um subgrupo de G_1).

(2) $\mathrm{Im}(f) < G_2$ (A imagem é um subgrupo de G_2).

(3) f é injetora se, e seomente se, $N(f) = \{e_1\}$.

Demonstração: Vamos demonstrar o item (3). Como $f(e_1) = e_2$, então $N(f) \neq \emptyset$.

Suponhamos que $N(f) = \{e_1\}$, e sejam $x_1, x_2 \in G_1$ tais que $f(x_1) = f(x_2)$. Logo,

$$\begin{aligned} f(x_1) = f(x_2) &\Rightarrow f(x_1)f(x_2)^{-1} = e_2 \quad \text{(operando à esquerda com } f(x_2)^{-1}) \\ &\Rightarrow f(x_1)f(x_2^{-1}) = e_2 \quad \text{(pois } f(x_2)^{-1} = f(x_2^{-1})) \\ &\Rightarrow f(x_1x_2^{-1}) = e_2. \quad \text{(pois } f \text{ é homomorfismo)} \end{aligned}$$

Mas, $f(x_1x_2^{-1}) = e_2$ implica em $x_1x_2^{-1} \in N(f) = \{e_1\}$, de modo que $x_1x_2^{-1} = e_1$, ou seja, $x_1 = x_2$. Portanto, f é injetora. Reciprocamente, dado $x \in G_1$,

$$x \in N(f) \Leftrightarrow f(x) = e_2 = f(e_1).$$

Mas, como por hipótese f é injetora, $f(x) = f(e_1)$ nos diz que $x = e_1$ e, assim, $N(f) = \{e_1\}$. ■

3.6.2 Isomorfismo de Grupos

Apresentamos agora exemplos de isomorfismos de grupos, que são homomorfismos bijetivos, destacando o principal teorema sobre os homomorfismos.

Um homomorfismo $\varphi : G_1 \longrightarrow G_2$ bijetivo é chamado de **isomorfismo**. Em particular, um isomorfismo de G_1. Verifica-se que se $\varphi : G_1 \longrightarrow G_2$ é um isomorfismo, então $\varphi^{-1} : G_2 \longrightarrow G_1$ também é um isomorfismo. Por isso dois grupos G_1 e G_2 são ditos isomorfos. em símbolos,

$$G_1 \simeq G_2.$$

Quando existe um isomorfismo entre eles.

Dois grupos isomorfos são conciderados essencialmente os mesmos, isto com relação as suas propriedades algébricas. Neste caso, se $\varphi : G_1 \longrightarrow G_2$ é um isomorfismo, então o elemento $x \in G_1$ tem as mesmas propriedades do elemento $\varphi(x)$, ou seja, x é identificado com $\varphi(x)$, em símbolos,

$$x \leftrightarrow \varphi(x).$$

Por exemplo, se $G_1 = \langle a \rangle$ e $\varphi : G_1 \longrightarrow G_2$ é um isomorfismo, então G_2, também é cíclico. Além disso,

$$G_2 = \langle \varphi(a) \rangle.$$

Exemplo 3.6.12 Dados os grupos $G_1 = (\mathbb{R}_+, \cdot)$ e $G_2 = (\mathbb{R}, +)$. Verifique se a aplicação

$$\begin{array}{rccc} \varphi: & \mathbb{R}_+^* & \longrightarrow & \mathbb{R} \\ & x & \longmapsto & \log x \end{array}$$

é um isomorfismo.

Solução: *No exemplo (*3.6.5*), vimos que*

$$\varphi(x \cdot y) = \varphi(x) + \varphi(y), \quad \forall\ x,\ y \in \mathbb{R}_+.$$

*E do exemplo (*3.6.9*), sabemos que*

$$N(\varphi) = \{1\},$$

ou seja, φ é injetora. Por fim, dado $y \in \mathbb{R}$, verifiquemos se existe $x \in \mathbb{R}_+^*$, tal que $\varphi(x) = y$. Ora,

$$\varphi(x) = y \Leftrightarrow \log x = y \Leftrightarrow x = 10^y \in \mathbb{R}_+^*.$$

Isso mostra que φ é sobrejetora e, portanto, φ é um isomorfismo, ou seja,

$$\mathbb{R}_+^* \simeq \mathbb{R}.$$

♣

O teorema a seguir é o principal teorema sobre os homomorfismos.

Teorema 3.6.13 (Teorema Fundamental dos Homomorfismos) *Seja $f : G_1 \longrightarrow G_2$ um homomorfismo de grupo. Então,*

$$\frac{G_1}{N(f)} \simeq \mathrm{Im}\,(f).$$

Exemplo 3.6.14 Para cada $n \in \mathbb{N}$, mostrar que

$$\frac{\mathbb{Z}}{n\mathbb{Z}} \simeq \mathbb{Z}_n.$$

Solução: *Consideremos a função $f : \mathbb{Z} \to \mathbb{Z}_n$ dada por $f(m) = \overline{m}$, para todo $m \in \mathbb{Z}$. Dados, $m_1, m_2 \in \mathbb{Z}$,*

$$f(m_1 + m_2) = \overline{m_1 + m_2} = \overline{m_1} + \overline{m_2} = f(m_1) + f(m_2),$$

de modo que f é um homomorfismo. Claramente, f é sobrejetora. Determinemos agora o núcleo de f. Para $m \in \mathbb{Z}$,

$$\begin{aligned} m \in N(f) &\Leftrightarrow f(m) = \overline{0} \\ &\Leftrightarrow \overline{m} = \overline{0} \\ &\Leftrightarrow m = kn, \end{aligned}$$

para algum $k \in \mathbb{Z}$. *Desse modo,* $N(f) = n \cdot \mathbb{Z}$ *e, pelo Teorema* (3.6.13),

$$\mathbb{Z}/n\mathbb{Z} \simeq \mathbb{Z}_n.$$

♣

3.7 Subgrupos normais e Grupos Quocientes

Subgrupos normais são exemplos importantes de subgrupos. Destacaremos suas principais propriedades de modo a estudar os grupos quocientes G/H. Pois se H é um subgrupo normal de G, então é possível dotar o conjunto quociente G/H de G por H com a estrutura de grupo, o qual chama-se grupo quociente de G por H.

Definição 3.7.1 *Consideremos o subgrupo* H *de um grupo* G. *Diz-se que* H *é subgrupo normal em símbolos* $H \rhd G$, *quando*

$$g \cdot h \cdot g^{-1} \in H \quad \forall g \in G \ \ e \ \ \forall h \in H$$

ou

$$g^{-1} \cdot h \cdot g \in H \quad \forall g \in G \ \text{ e } \ \forall h \in H$$

Exemplo 3.7.2 Para qualquer grupo G, $H = \{e\}$ e $H = G$ são subgrupos normais de G. ♣

Exemplo 3.7.3 Todo subgrupo H de um grupo abeliano é normal.

De fato, para $g \in G$ *e* $h \in H$,

$$g \cdot h \cdot g^{-1} = g \cdot g^{-1} \cdot h = e \cdot h = h \in H$$

Assim,para os grupos $(\mathbb{Z}, +) < (\mathbb{Q}, +) < (\mathbb{R}, +)$, *temos:* $\mathbb{Z} \rhd \mathbb{Q} \rhd \mathbb{R}$. ♣

Teorema 3.7.4 *Seja* H *um subgrupo de um grupo* G. *Então as seguintes afirmações são equivalentes:*

(1) $H \rhd G$;

(2) $gHg^{-1} = H, \quad \forall g \in G$;

(3) $g \cdot H = H \cdot g, \quad \forall g \in G$.

Teorema 3.7.5 *Seja H um subgrupo normal de um grupo G. Então a aplicação*

$$\begin{aligned} \cdot : \ G/H \times G/H &\to G/H \\ (xH, yH) &\mapsto xy \cdot H. \end{aligned}$$

Define-se uma operação sobre o conjunto G/H. Além disso, $(G/H, \cdot)$ é um grupo, o qual chamado grupo quociente de G por H.

Demonstração: Para verificarmos que " $\cdot$ " é uma operação sobre G/H, precisamos mostrar que o resultado independem dos representantes[1] das classes. Especificamente, se $x_1H = x_2H$ e $y_1H = y_2H$, com $x_1, x_2, y_1, y_2 \in G$, então

$$x_1H \cdot y_1H = x_2H \cdot y_2H.$$

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

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

Portanto,

$$\begin{aligned} y_1^{-1}x_1^{-1}x_2y_2 &= y_1^{-1}h_1y_2 \qquad (\text{pois} \quad x_1^{-1}x_2 = h_1) \\ &= h_2y_2^{-1}h_1y_2. \quad (\text{pois} \quad y_1^{-1} = h_2y_2^{-1}) \end{aligned}$$

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

$$\begin{aligned} y_1^{-1}x_1^{-1}x_2y_2 &= h_2h_3 \in H \\ &\Leftrightarrow (x_1y_1)^{-1}(x_2y_2) \in H \\ &\Leftrightarrow x_1y_1H = x_2y_2H, \end{aligned}$$

ou seja, $x_1H \cdot y_1H = x_2H \cdot y_2H$. Por conseguinte, " $\cdot$ " é uma operação sobre G/H. Consideremos agora xH, $yH, zH \in G/H$. Desse modo, como a operação em G é asso-

[1] Isso se faz necessário, uma vez que uma classe lateral pode ter mais do que um representante, ou seja, $g_1, g_2 \in G$, $g_1 \neq g_2$ com $g_1H = g_2H$.

ciativa,

$$\begin{aligned} xH \cdot (yH \cdot zH) &= xH \cdot (yz)H \\ &= x(yz)H \\ &= (xy)zH \\ &= xyH \cdot zH \\ &= (xH \cdot yH) \cdot zH, \end{aligned}$$

ou seja, " $\cdot$ " é associativa. Agora, como

$$xH \cdot H = xH \cdot eH = xeH = xH,$$

então H é o elemento neutro da operação em G/H . Para finalizar,

$$xH \cdot x^{-1}H = xx^{-1}H = eH = H$$

e

$$x^{-1}H \cdot xH = x^{-1}xH = eH = H.$$

Por isso, $x^{-1}H$ é o inverso de xH em G/H. Concluímos que $(G/H, \cdot)$ é um grupo. ■

Exemplo 3.7.6 Consideremos o grupo multiplicativo $G = \{1, -1, i, -i\}$. O conjunto $H = \{1, -1\}$ é um subgrupo de G. Além disso, como G é abeliano, então, $H \rhd G$. Por isso, G/H é um grupo. Vamos descrever os elementos de G/H. Como $1, -1 \in H$, então

$$1H = (-1)H = H$$

Agora,

$$iH = \{i1,\ i(-1)\} = \{i,\ -i\} = (-i)H$$

Desse modo,

$$G/H = \{H,\ \{i, -i\}\} = \{H, iH\}$$

Neste grupo, temos:

$$HiH = 1Hih = 1iH = iH$$

e

$$iHiH = iiH = (-1)H = H \Rightarrow O(iH) = 2$$

♣

Proposição 3.7.7 *Sejam G um grupo e H um subgrupo normal de G. Então,*

(1) Se G for abeliano, então G/H também é abeliano.

(2) Se G for cíclico, então G/H também é cíclico.

3.8 Grupo de Permutações

Faremos aqui um estudo mais detalhado de grupos de permutações de um conjunto não-vazio X. Nesta direção, o caso de interesse principal é quando $X = \{1, 2, 3, 4, ..., n\}$. Isso nos conduzirá ao grupo simétrico de grau n, S_n.

Sejam A um conjunto não vazio e $S(A)$ o conjunto de todas as permutações de A, ou seja

$$S(A) = \{f : A \to A \text{ tal que } f \text{ é bijetora}\}$$

Vamos mostrar que $S(A)$ sob a composição de funções é um grupo. É claro que $S(A) \neq \emptyset$, pois

$$\begin{array}{rccc} id_A: & A & \to & A \\ & x & \mapsto & x \end{array}$$

é uma bijeção.

Mostraremos primeiramente que $S(A)$ é fechado sob "$\circ$". Consideremos $f, g \in S(A)$. Daí,

$$f : A \to A \text{ e } g : A \to A.$$

Dados $x, y \in A$,

Ora,

$$\begin{array}{rcccccc} (f \circ g)(x) & = & (f \circ g)(y) & \Rightarrow & f(g(x)) & = & f(g(y)) \\ & & & \Rightarrow & g(x) & = & g(y) \\ & & & \Rightarrow & x & = & y, \end{array}$$

ou seja, $f \circ g$ é f injetora. Agora, dado $z \in A$, então como f é sobrejetora, existe $x_1 \in A$ tal que $f(x_1) = z$. Por outro lado, como $x_1 \in A$ e g é sobrejetora existe $x_2 \in A$

com $g(x_2) = x_1$. Por isso,

$$(f)(x_1) = z \Rightarrow f(g(x_2)) = z \Rightarrow (f \circ g)(x_2) = z$$

Daí, $f \circ g$ é sobrejetora e portanto é bijetora. Isso mostra que "$\circ$" é uma operção sobre $S(A)$.

Sabemos que "$\circ$" é associativa, também

$$\begin{array}{rccc} id_A: & A & \to & A \\ & x & \mapsto & x \end{array}$$

É tal que

$$(f \circ id_A)(x) = f(id_A(x)) = f(x), \quad \forall f \in S(A) \ e\forall \ x \in A$$

Da mesma forma,

$$(id_A \circ f)(x) = id_A(f(x)) = f(x), \quad \forall f \in S(A) \ e\forall \ x \in A$$

Portanto, id_A é o neutro da operação.

Sabe-se que uma função é bijetora se, e somente se, admite inversa. Como cada $f \in S(A)$é uma bijeção, tem-se que existe $f^{-1} \in S(A)$ tal que

$$f \circ f^{-1} = f^{-1} \circ f = id_A$$

Portanto, $(S(A), \circ)$ é um grupo, o qual chama-se **grupo de permutações** de A. ■

Em geral $S(A)$ é não abeliano.

Em particular quando A for finito, digamos $A = \{1, 2, 3, ..., n\}$,então denota-se $S\{A\}$ por S_n.

Pela análise combinatória, mostra-se que S_n tem $n!$ elementos.

Em geral, uma permutação $\alpha \in S_n$ é indicada por

$$\alpha = \begin{pmatrix} 1 & 2 & 3 & ... & n \\ a_1 & a_2 & a_3 & ... & a_n \end{pmatrix}$$

Em que $\alpha(1) = a_1$, $\alpha(2) = a_2, ..., \alpha(n) = a_n$

A notação é mais prática quando os cálculos são de $\alpha \circ \beta = \alpha \cdot \beta \in S_n$.

Nota-se que S_n é abeliano se, e somente se, $n = 1$ ou $n = 2$.

Exemplo 3.8.1 Vamos determinar S_3. Neste caso, $A = \{1, 2, 3\}$. Assim, os elementos de S_3, são:

$$\alpha_1 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}, \ \alpha_2 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}, \ \alpha_3 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}$$

$$\alpha_4 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}, \ \alpha_5 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}, \ \alpha_6 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}$$

Logo,

$$S_3 = \{\alpha_1, \alpha_2, \alpha_3, \alpha_4, \alpha_5, \alpha_6\}$$

Consideremos algumas decomposições

$$\alpha_2 \cdot \alpha_3 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} = \alpha_6$$

$$\alpha_3 \cdot \alpha_2 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} = \alpha_5$$

Observe que $\alpha_2 \cdot \alpha_3 \neq \alpha_3 \cdot \alpha_2$

$$\alpha_4 \cdot \alpha_5 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} = \alpha_3$$

E assim por diante. ♣

Capítulo 4

Os Grupos Alternados

Para mencionar os conceitos inerentes a estruturas algébricas mais específicas precisamos nos reter aos conceitos preliminares vistos até agora, já que vários de seus resultados podem ser ampliados a fim de ajudar no estudo o da teoria dos Grupos Alternados. Na seção anterior, destacamos a importância dos grupos de permutações e que em particular, quando um grupo G for finito, então G é identificado como subgrupo de S_n. Neste Capítulo, vamos considerar mais uma vez os grupos S_n, mas focalizando um tipo especial de subgrupos, os grupos das permutações pares ou grupos alternados.

4.1 Ciclos e órbitas

Consideramos aqui os conceitos de ciclos, órbitas e de transposição, destacando os principais teoremas relacionados.

Entre as permutações dos grupos S_n, destacam-se de modo especial, as denominadas ciclos, definidas como segue.

Definição 4.1.1 *Uma permutação $\alpha \in S_n$ chama-se* ***ciclo de comprimento*** **r** *ou* **r-*ciclo*** *quando existem $a_1, a_2, ..., a_r \in I_n$ tais que*

$$\alpha(a_1) = a_2, \alpha(a_2) = a_3, ..., \alpha(a_{r-1}) = a_r, \alpha(a_r) = a_1$$

e

$$\alpha(i) = i, \quad \forall i \in I_n - \{a_1, a_2, ..., a_r\}$$

Em particular, um 2-ciclo chama-se ***transposição****.*

Em geral, denota-se um r-ciclo α por

$$\alpha = (a_1 a_2 ... a_r)$$

Qualquer elemento a_i pode ser considerado como ponto inicial do r-ciclo; por isso, existem r maneiras para representar $\alpha = (a_1 a_2 ... a_r)$, ou seja,

$$\alpha = (a_1 a_2 ... a_r) = (a_2 a_3 ... a_r a_1) = ... = (a_r a_1 a_2 ... a_{r-1}) .$$

Exemplo 4.1.2 Em S_n, o único 1-ciclo(o ciclo trivial) é a identidade $\alpha = e$, a qual representa-se por $\alpha = (1)$ ou por $\alpha = (a)$ com $a \in I_n$. ♣

Exemplo 4.1.3 No grupo S_5, a permutação

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

é tal que $\alpha(1) = 3$, $\alpha(3) = 5$, $\alpha(5) = 4$, $\alpha(4) = 1$ *e* $\alpha(2) = 2$. Por isso, $\alpha = (1354)$; ou seja, α é um 4-ciclo. Nota-se que

$$\alpha = (4135) = (5413) = (3541)$$

♣

Exemplo 4.1.4 A permutação

$$\alpha = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 5 & 4 & 3 & 1 \end{pmatrix} \in S_5$$

não é um r-ciclo qualquer que seja r. Isto porque α é o produto de dois ciclos $\mu_1 = (125)$ e $\mu_2 = (34)$. Vale ressaltar que o produto de dois ciclos não é necessariamente um ciclo. ♣

Definição 4.1.5 *Se $\alpha \in S_n$ e $i \in I_n$, diz-se que α move i quando $\alpha(i) \neq i$; e diz-se que α fixa i quando $\alpha(i) = i$.*

Nota-se que na representação $\alpha = (a_1 a_2 ... a_r)$, se omitem os inteiros $i \in I_n$ que são fixados por α.

Exemplo 4.1.6 Em S_5, a permutação $\alpha = (125)$ move os inteiros $i = 1$, $i = 2$ e $i = 5$; e fixa $i = 3$ e $i = 4$. ♣

Proposição 4.1.7 *Um r-ciclo em S_n tem ordem r.*

Demonstração: Seja $\alpha = (a_1 a_2 ... a_r)$ um r-ciclo; vamos mostrar que $\alpha^r = e$ e $\alpha^k \neq e$ e para $0 < k < r$. Notemos que como $\alpha(a_1) = a_2$ e $\alpha(a_2) = a_3$, então $\alpha^2(a_1) = a_3$, $\alpha^3(a_1) = a_4$, e assim por diante. Por isso,

$$\alpha^2(a_1) = a_3, \alpha^3(a_1) = a_4, ..., \alpha^{r-1}(a_1) = a_r.$$

Sendo $\alpha(a_r) = a_1$, então

$$\alpha^{r-1}(a_1) = a_r \Longrightarrow \alpha^r(a_1) = \alpha(a_r) = a_1,$$

ou seja, $\alpha^r(a_1) = a_1$; para o inteiro a_2,

$$a_2 = \alpha(a_1) \Longrightarrow \alpha^r(a_2) = \alpha^{r+1}(a_1) = \alpha(\alpha^r(a_1)) = \alpha(a_1) = a_2,$$

de maneira que $\alpha^r(a_2) = a_2$. Da mesma forma, prova-se que $\alpha^r(a_i) = a_i$ para $i = 3, ..., r$. Além disso, como α^r fixa os outro elementos de $I_n - \{a_1, a_2, ..., a_r\}$, pois assim o faz α,segue que α^r é a identidade. Por outro lado, nenhuma das permutações $\alpha, \alpha^2, ..., \alpha^{r-1}$ é igual a identidade, pois todas elas movem o elemento a_1. Portanto, a ordem de α é r. ■

Exemplo 4.1.8 O 4-ciclo $\alpha = (1235) \in S_6$ tem ordem quatro; o 5-ciclo $\beta = (13478) \in S_8$ tem ordem cinco. ♣

Proposição 4.1.9 *Se $\mu = (a_1 a_2 ... a_r) \in S_n$ é um r-ciclo, então $\mu^{-1} = (a_r a_{r-1} ... a_2 a_1)$.*

Definição 4.1.10 ***Definição 4.1.11*** *Dois ciclos $\alpha, \beta \in S_n$, digamos $\alpha = (a_1 a_2 ... a_r)$ e $\beta = (b_1 b_2 ... b_k)$, são ditos ciclos disjuntos quando nenhum elemento de $I_n = \{1, 2, ..., n\}$ é movido por ambos. Equivalentemente, quando*

$$\{a_1, a_2, ..., a_r\} \cap \{b_1, b_2, ..., b_k\} = \emptyset$$

Uma família de ciclos $\alpha_1, \alpha_2, ..., \alpha_t$ é disjunta quando α_1 e α_j são disjuntos, para quaisquer $i, j \in I_n$ com $i \neq j$.

Exemplo 4.1.12 Em S_5, os ciclos $\alpha = (13)$ e $\beta = (245)$ são disjuntos, pois $\{1,3\} \cap \{245\} = \emptyset$; Já os ciclos $\gamma = (1245)$ e $\mu = (1367)$ não são disjuntos, pois ambos movem o elemento $i = 1$, isto é, $1 \in \{1,2,4,5\} \cap \{1,3,6,7\}$. ♣

Proposição 4.1.13 *Se $\alpha, \beta \in S_n$ são ciclos disjuntos, então $\alpha\beta = \beta\alpha$.*

Demonstração: É suficiente mostrar que $(\alpha\beta)(i) = (\beta\alpha)(i)$ para todo $i \in I_n$.

Se $i \in I_n$ é fixado por α e β, então $(\alpha\beta)(i) = \alpha(\beta(i)) = \alpha(i) = i$; da mesma forma, $(\beta\alpha)(i) = \beta(\alpha(i)) = \beta(i) = i$. Portanto, para este caso, tem-se que $(\alpha\beta)(i) = (\beta\alpha)(i)$. Agora, se α move o elemento i, digamos $\alpha(i) = j \neq i$, então $\beta(i) = i$, pois α e β são disjuntos. Desse modo,

$$(\alpha\beta)(i) = \alpha(\beta(i)) = \alpha(i) = j$$

e

$$(\beta\alpha)(i) = \beta(\alpha(i)) = \beta(j) = j,$$

pois α move o elemento j, pois se $\alpha(j) = j$, então $\alpha(i) = \alpha(j)$ com $i \neq j$, o que contradiz o fato de α ser injetora. Portanto, $(\alpha\beta)(i) = (\beta\alpha)(i)$ da mesma forma mostra-se esta igualdade quando o elemento i é movido por β. Por conseguinte, $\alpha\beta = \beta\alpha$. ■

Definição 4.1.14 *Consideremos $\alpha \in S_n$, e sobre o conjunto I_n, vamos definir $\sim_a$ dada para quaisquer $i, j \in I_n$, por*

$$i \sim j \Leftrightarrow \exists k \in \mathbb{Z} \text{ tal que } j = \alpha^k(i).$$

A relação $\sim_a$ é de equivalência, e as classes de equivalência determinadas por ela chama-se as **α-órbitas**. Assim, se $i \in I_n$, a α-órbita que contém i é o conjunto

$$orb(i) = \left\{\alpha^k(i) : k \in \mathbb{Z}\right\}.$$

Exemplo 4.1.15 Seja $\alpha \in S_6$ dada por

$$\alpha = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 4 & 5 & 6 & 3 & 1 \end{pmatrix}$$

Temos que $\alpha(1) = 2$, $\alpha(2) = 4$, $\alpha(4) = 6$ e $\alpha(6) = 1$. Desse modo,

$$\alpha^2(1) = 4 \ \ e \ \ \alpha^3(1) = 6$$

Portanto, a órbita de $i = 1$ é $orb(1) = \{1, 2, 4, 6\}$. Da mesma forma, obtém-se as órbitas $orb(3) = \{3, 5\}$. Estas são as únicas órbitas de α, pois $orb(1) = orb(2) = orb(4) = orb(6)$; $orb(3) = orb(5)$, uma vez que as classes de equivalência constituem uma partição de I_6. ♣

Pelo que foi descrito até agora, se $\mu = (a_1 a_2 ... a_r)$ é um r-ciclo, então

$$\alpha(a_1) = a_2, \ \alpha^2(a_1) = a_3, \ ..., \ \alpha^{r-1}(a_1) = a_r.$$

Por isso, a órbita do elemento $i = a_1$ é o conjunto

$$orb(a_1) = \{a_1, a_2, ..., a_r\}$$

Assim, o r-ciclo $\mu = (a_1 a_2 ... a_r)$ pode ser escrito como

$$\mu = \left(a_1 \alpha(a_1) \alpha^2(a_1) ... \alpha^{r-1}(a_1)\right).$$

4.2 Fatoração em ciclos disjuntos

O resultado principal desta seção será apresentado no teorema (4.2.1), o qual afirma que toda permutação $\alpha \in S_n - \{e\}$ pode ser escrita como produto de ciclos disjuntos aos pares.

Teorema 4.2.1 *Toda permutação $\alpha \in S_n - \{e\}$ pode ser escrita como um produto de ciclos disjuntos aos pares. Além disso, esta fatoração é única, a menos da ordem dos fatores.*

Demonstração: Se $\alpha \in S_n$ for um ciclo, então o resultado segue de imediato. Caso contrário, consideremos $\beta_1, \beta_2, ..., \beta_k$ as distintas α-órbitas não-triviais de α, ou seja, as órbitas com mais de um elemento. Temos então que $\alpha(\beta_i) = \beta_i$ qualquer que seja $i = 1, ..., k$. Para cada $i - 1, ..., n$, definamos

$$\mu_i(j) = \begin{cases} \alpha(j) & \text{se} \quad j \in \beta_i, \\ j & \text{se} \quad j \notin \beta_i. \end{cases}$$

Claramente, μ_i é um ciclo, pois se $j \notin \beta_i$, então $\mu(j) = j$ e portanto, a μ_i-órbita de j é unitária, isto é, igual a $\{j\}$. Temos também que β_i é uma óbita de μ_i, pois μ_i e α coicidem em β_i; e como $\alpha(\beta_i) = \mu_i(\beta_i) = \beta_i$, α^m coincide com μ_i , para todo $m \in \mathbb{Z}$. Além de $\mu_1, \mu_2, ..., \mu_k$ serem ciclos disjuntos aos pares, vê-se claramente que

$$\alpha = \mu_1\mu_2...\mu_k.$$

Mostraremos agora a unicidade da fatoração. Suponhamos que

$$\alpha = \beta_1\beta_2...\beta_l.$$

Sendo $\beta_{i,s}$ ciclos não-triviais disjuntos aos pares. Para cada $i = 1, ..., l$, chamemos de C_i a órbita de β_i. Desse modo, $C_1, C_2, ..., C_l$ são as órbitas de $\alpha = \beta_1\beta_2...\beta_l$. Isto significa que $l = k$ e, reordenando se necessário, temos $C_1 = \beta_1, C_2 = \beta_2, ..., C_k = \beta_k$. Logo, $\mu_i = \beta_i$ para $i = 1, .., k$, pois $\mu_i(j) = \alpha(j) = \beta(j)$ para todo $j \in \beta_i$. ■

Corolário 4.2.2 *Toda permutação $\alpha \in S_n$ pode ser escrita como produto de transposições.*

Demonstração: De acordo co o teorema anterior, é suficiente mostrar que todo ciclo em S_n é um produto de transposições. Considerando, pois, o r-ciclo $\mu = (a_1a_2...a_r)$, vê-se facilmente que

$$\mu = (a_1a_r)(a_1a_{r-1})...(a_1a_2).$$

■

Exemplo 4.2.3 A permutação $\beta = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 3 & 4 & 1 & 2 & 6 & 5 \end{pmatrix} \in S_6$ podemos expressar como o produto de ciclos disjuntos. Iniciando com o elemento $i = 1$,

$$\beta(1) = 3, \beta(3) = 1.$$

Isso nos dá a órbita $\beta_1 = \{1, 3\}$ e o ciclo associado $\mu_1 = (13)$. Considerando um elemento $i \in I_6$ que não aparece em β_1, digamos $i = 2$, então

$$\beta(2) = 4, \beta(4) = 2.$$

de modo que $\beta_2 = \{2, 4\}$ é uma órbita de β e $\mu_2 = (24)$ é outro ciclo de β. Tomemos agora $i = 5$, que não aparece nos dois primeiros ciclos, isto é, $5 \notin \beta_1 \cup \beta_2$, temos

$$\beta(5) = 6, \beta(6) = 5.$$

ou seja, $\beta_3 = \{5, 6\}$ e $\mu_3 = (56)$ é também um ciclo de β. Como não há mais elementos em S_7 a ser considerado, pois

$$\beta_1 \cup \beta_2 \cup \beta_3 = S_6.$$

Concluímos que μ_1, μ_2 e μ_3 são os únicos ciclos de β. Portanto,

$$\beta = \mu_1\mu_2\mu_3 = (13)(24)(56).$$

♣

Exemplo 4.2.4 Notemos que a permutação $\alpha \in S_5$ dada por

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

é tal que $\alpha = (15)(234)$. Portanto, como produto de transposições,

$$\alpha = (15)(24)(23).$$

♣

Teorema 4.2.5 *Sejam $\mu_1, \mu_2, ..., \mu_k \in S_n$ ciclos disjuntos de comprimentos $r_1, r_2, ..., r_k$, respectivamente. Então a ordem da permutação $\alpha = \mu_1\mu_2...\mu_k$ é igual a $mmc\{r_1r_2...r_k\}$.*

Demonstração: Como $\mu_1, \mu_2, ..., \mu_k$ são ciclos disjuntos, então pela proposicão 5.1.13, $\mu_i\mu_j = \mu_j\mu_i$ quaisquer que sejam $i, j \in \{1, 2, ..., k\}$. Por isso,

$$\alpha^s = (\mu_1\mu_2...\mu_k)^s = \mu_1^s\mu_2^s...\mu_k^s, \quad \forall s \in \mathbb{Z}.$$

Assim, sendo $m = mmc\{r_1 r_2 ... r_k\}$, então para cada $i \in \{1, 2, ..., k\}$, existe $\lambda_i \in \mathbb{Z}$ tal que $m = \lambda_i r_i$. Portanto,

$$\mu_i^m = \mu_i^{\lambda_i r_i} = (\mu_i^{r_i})^{\lambda_i} = e,$$

pois a ordem de μ_i é r_i. Logo

$$\alpha^m = (\mu_1 \mu_2 ... \mu_k)^m = \mu_1^m \mu_2^m ... \mu_k^m = e.$$

Por outro lado, se $\alpha^t = e$, então

$$\alpha^t = e \Rightarrow (\mu_1 \mu_2 ... \mu_k)^t = e \Rightarrow \mu_1^t \mu_2^t ... \mu_k^t = e.$$

Mas, como $\mu_{i,s}$ são disjuntos,

$$\mu_1^t \mu_2^t ... \mu_k^t = e \Rightarrow \mu_i^t = e, \quad \forall i \in \{1, 2, ..., k\}.$$

Portanto a ordem de μ_i divide t, ou seja, r_i divide t. Agora, sendo $m = mmc\{r_1 r_2 ... r_k\}$, então m divide t, de modo que $m \leq t$. Portanto, a ordem de $\alpha = \mu_1 \mu_2 ... \mu_k$ é igual a $m = mmc\{r_1 r_2 ... r_k\}$. ■

Exemplo 4.2.6 Vamos determinar a ordem da permutação

$$\gamma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 3 & 5 & 8 & 7 & 1 & 4 & 6 & 2 \end{pmatrix}.$$

Como

$$\gamma = (13825)(476),$$

em que $\mu_1 = (13825)$ e $\mu_2 = (476)$ ciclos disjuntos de comprimentos 5 e 3, respectivamente, temos pelo teorema anterior, que a ordem de γ é $mmc\{3, 5\} = 15$. ♣

4.3 Permutações pares e ímpares

Essa seção é dedicada ao estudo do principal foco do nosso trabalho, o estudo do grupo alternado A_n. Consideramos teoremas importantes sobre A_n.

Definição 4.3.1 *Uma permutação $\alpha \in S_n$ é par se α pode ser escrita como um produto de um número par de transposições; e α é ímpar quando α pode ser escrita como um produto de um número ímpar de transposições.*

Exemplo 4.3.2 A permutação identidade $e \in S_n$ é par, pois $e = (12)(12)$. Observar-se que quando $n = 1$, então não se pode fatorar e desta forma; neste caso, define-se $e \in S_1$ como sendo uma permutação *par*. ♣

Exemplo 4.3.3 Em S_6, a permutação $\alpha = (1456)(215)$ pode ser escrita da seguinte forma:

$$\alpha = (16)(15)(14)(25)(21),$$

ou seja, α tem uma fatoração com cinco transposições, de maneira que α é ímpar. ♣

Exemplo 4.3.4 Consideremos

$$\beta = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 8 & 2 & 6 & 3 & 7 & 4 & 5 & 1 \end{pmatrix} \in S_8.$$

Notemos que β admite os ciclos $\mu_1 = (18)$, $\mu_2 = (364)$ e $\mu_3 = (57)$ em sua fatoração. Assim,

$$\beta = \mu_1\mu_2\mu_3 = (18)(364)(57) = (18)(34)(36)(57).$$

isto é, β tem uma fatoração com quatro transposições. Por isso, β é par. ♣

Proposição 4.3.5 *Um r-ciclo em S_n é uma permutação par se, e somente se, r é ímpar.*

Denotaremos por A_n o conjunto de todas as permutações pares de S_n. Se $\alpha, \beta \in S_n$, então é imediato verificar que $\alpha\beta$ também está em S_n. Desde que A_n é um subconjunto finito e fechado de S_n, tem-se que A_n é um subgrupo de S_n. O grupo A_n chama-se grupo alternado de grau n ou grupo de permutações pares.

Determinaremos a ordem de A_n. É claro que se $n = 1$, então a ordem de A_n é 1, pois $e \in S_1$ é uma permutação par, por convenção. Por isso, vamos supor que $n \geq 2$. Denotando o conjunto das permutações ímpares por B_n, consideremos a transposição $\alpha = (12)$ e aplicação

$$\begin{array}{rccc} f_a: & A_n & \to & B_n \\ & \beta & \mapsto & \alpha\beta. \end{array}$$

Imicialmente, notemos que f_α está bem definida, pois α é uma transposição, de maneira que $\alpha\beta \in B_n$. Agora, se $\beta_1, \beta_2 \in A_n$ com $f_\alpha(\beta_1) = f_\alpha(\beta_2)$, então

$$f_\alpha(\beta_1) = f_\alpha(\beta_2) \Rightarrow \alpha\beta_1 = \alpha\beta_2 \Rightarrow \beta_1 = \beta_2,$$

pois S_n é um grupo. Logo, f_α é injetora.

Por outro lado, dado $\theta \in B_n$, segue que $\alpha\theta$ é uma permutação par. Além disso, como $\alpha^2 = 2$, então

$$f_\alpha(\alpha\theta) = \alpha(\alpha\theta) = \alpha^2\theta = \theta,$$

ou seja, f_α é sobrejetora e, assim, f_α é bijetora. Desse modo, existe uma bijeção entre A_n e B_n tem a mesma cardinalidade. Além disso, como

$$S_n = A_n \cup B_n \text{ e } A_n \cap B_n = \emptyset,$$

então

$$|S_n| = |A_n| + |B_n| = 2|A_n| \Rightarrow |A_n| = \frac{n!}{2}.$$

Logo a ordem de A_n é $\frac{n!}{2}$.

Proposição 4.3.6 *Para $n \geq 2$, S_n cotém $\frac{n!}{2}$ permutações pares e $\frac{n!}{2}$ permutaçõs ímpares.*

Agora pelo Teorema de Lagrange,

$$|S_n| = |A_n| \cdot (S_n : A_n) \Rightarrow (S_n : A_n) = 2.$$

Por isso concluimos que A_n é um subgrupo normal de S_n.

Teorema 4.3.7 *Para $n \geq 2$, o grupo alternado A_n é um subgrupo normal de S_n de ordem $\frac{n!}{2}$.*

Para $n > 3$, o grupo A_n é não-abeliano. De fato, se $a_1, a_2, a_3, a_4 \in I_n$ são distintos, então

$$(a_1a_2a_3)(a_1a_2a_4) = (a_1a_3)(a_2a_4) \in A_n,$$

$$(a_1a_2a_4)(a_1a_2a_3) = (a_1a_4)(a_2a_3) \in A_n.$$

Logo, $(a_1a_2a_3)(a_1a_2a_4) \neq (a_1a_2a_4)(a_1a_2a_3)$.

Teorema 4.3.8 *Se $n \geq 3$, então A_n contém todos os 3-ciclos. Além disso, todo elemento em A_n é um produto de 3-ciclos.*

Demonstração: Se $\mu = (a_1 a_2 a_3)$ é um 3-ciclo, então

$$\mu = (a_1 a_2 a_3) = (a_1 a_3)(a_1 a_2) \in A_n.$$

Para outra parte, é suficiente mostrar que o produto de quaisquer duas transposições é um produto de 3-ciclos; isso porque um elemento de A_n é um produto de um número par de transposições. Sejam $\mu_1 = (a_1 a_2)$ e $\mu_2 = (a_3 a_4)$ transposições de S_n. Se μ_1 e μ_2 são disjuntas(este caso exclui $n = 3$), então

$$\mu_1 \mu_2 = (a_1 a_2)(a_3 a_4) = (a_1 a_2)(1)(a_3 a_4).$$

Mas, como $e = (1) = (a_2 a_3)(a_2 a_3)$, tem-se que

$$\mu_1 \mu_2 = (a_1 a_2)(a_2 a_3)(a_2 a_3)(a_3 a_4) = (a_2 a_3 a_1)(a_3 a_4 a_2).$$

Caso contrário (este exclui $n = 3$), consideremos $\mu_1 = (a_1 a_2)$ e $\mu_2 = (a_2 a_3)$; logo

$$\mu_1 \mu_2 = (a_1 a_2)(a_2 a_3) = (a_1 a_2 a_3).$$

Concluímos que toda permutação de A_n pode ser escrita como produto de 3-ciclos. ■

Exemplo 4.3.9 Vamos escrever a permutação

$$\beta = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 4 & 1 & 8 & 2 & 7 & 3 & 6 & 5 \end{pmatrix} \in S_8,$$

como produto de 3-ciclos. Primeiramente, notamos que

$$\alpha = (142)(38576).$$

Pela (4.3.5), $\mu_1 = (142)(38576)$ são permutações pares, pois μ_1 é um 3-ciclo e μ_2 é um 5-ciclo; por isso, $\alpha = \mu_1 \mu_2 \in A_n$. Agora, $\mu_2 = (38576) = (63)(37)(53)(38)$. Assim,

$$\mu_2 = (63)(37)(53)(38) = (637)(538).$$

Portanto,

$$\alpha = \mu_1 \mu_2 = (142)(637)(538).$$

♣

Definição 4.3.10 *A fatoração completa de uma permutação $\alpha \in S_n$ é a fatoração de α em ciclos disjuntos que contém exatamente um 1-ciclo(i) para cada i fixado por α.*

Exemplo 4.3.11 Se $\alpha = (124) \in S_5$, então sua fatoração completa é $\alpha = (124)(3)(5)$. Já $(34)(1)$ não é a fatoração completa de $\beta = (34) \in S_5$, pois além de $i = 1$, β fixa os elementos $i = 2$ e $i = 5$. Por isso, a fatoração completa de β é $\beta = (34)(1)(2)(5)$. ♣

Definição 4.3.12 *Duas permutações α e $\beta \in S_n$ tem a mesma estrutura de ciclos se suas fatorações completas em ciclos disjuntos tem o mesmo número de r-ciclo para cada r.*

Exemplo 4.3.13 Em S_9, as permutações

$$\alpha = (1253) \ \ e \ \ \beta = (2679)$$

tem a mesma estrutura de ciclos, uma vez que ambas são 4-ciclos. ♣

A demonstração do teorema a seguir não será feita aqui; contudo, ela é apresentada com detalhes na referência ([3]). Sua demonstração consiste em mostrar que dados $\alpha, \theta \in S_n$, se $(a_1 a_2 ... a_r)$ é um ciclo que aparece na fatoração de $\theta \in S_n$, então $(\alpha(a_1)\alpha(a_2)...\alpha(a_r))$ é um ciclo que aparece na fatoração de $\alpha\theta\alpha^{-1}$; desse modo, $\alpha\theta\alpha^{-1}$ e θ tem sempre a mesma estrutura de ciclo.

Teorema 4.3.14 *Se $\alpha, \theta \in S_n$, então $\alpha\theta\alpha^{-1}$ é a permutação obtida aplicando α aos elementos dos ciclos que aparecem na fatoração de θ.*

Exemplo 4.3.15 Dadas as permutações em S_6

$$\alpha = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 3 & 5 & 6 & 1 & 4 \end{pmatrix} \ \ e \ \ \theta = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 1 & 2 & 3 & 5 & 6 & 4 \end{pmatrix}.$$

Vamos determinar $\alpha\theta\alpha^{-1}$ usando o teorema anterior e pelo método tradicional.

Como $\theta = (456)$, então

$$\alpha\theta\alpha^{-1} = (\alpha(4)\alpha(5)\alpha(6)) = (614) = (146).$$

Agora, pelo método tradicional,

$$\alpha^{-1} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 5 & 1 & 2 & 6 & 3 & 4 \end{pmatrix}.$$

e

$$\begin{aligned} \alpha\theta\alpha^{-1} &= \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 3 & 5 & 6 & 1 & 4 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 1 & 2 & 3 & 5 & 6 & 4 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 5 & 1 & 2 & 6 & 3 & 4 \end{pmatrix} \\ &= \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 4 & 2 & 3 & 6 & 5 & 1 \end{pmatrix} = (146). \end{aligned}$$

♣

Capítulo 5

Conclusão

Apresentamos neste trabalho os grupos de permutações S_n, focalizando um tipo especial de subgrupos — os grupos das permutações pares ou grupos alternados. Para isso se fez necessário apresentarmos alguns dos principais resultados da Teoria dos Grupos. Dessa forma tivemos conclusões relevantes referentes à teoria dos grupos.

Bibliografia

[1] C.B, *História da Matemática*, (edição revista por U.C. Merzzbach), Edgar Blücher, São Paulo, 1996.

[2] Gonçalves, Adilson. *Introdução à Álgebra*. Rio de Janeiro: IMPA, 2008.

[3] Garcia, A. I; Lequain, Y. *Elementos de Álgebra*. 4. ed. Rio de Janeiro: Projeto Euclides, 2006.

[4] Herstein, I. N., *Abstract Algebra*. John Wiley & sons . Inc. 3rd ed. 1999.

[5] www.mat.ufg.br/bienal/2006/mini/teixeira.pdf/2006/dissertação de mestrado de César Ricardo P. Martins, orientação de Prof. Dr. Marcos Vieira Teixeira.