Universidade Federal de Santa Catarina
Licenciatura em Matemática

Introdução à teoria de grupos

André Fornerolli Machado

Orientadora: Profa. Virgínia Silva Rodrigues

Florianópolis
Agosto de 2012

Esta Monografia foi julgada adequada como TRABALHO DE CONCLUSÃO DE CURSO no Curso de Matemática - Habilitação Licenciatura, e aprovada em sua forma final pela Banca Examinadora designada pela Portaria nº / CCM /

Prof. Nereu Estanislau Burin
Professor da disciplina

Banca Examinadora:

Orientadora : Profa. Virgínia Silva Rodrigues

Luciano Bedin

Luiz Augusto Saeger

Agradecimentos

À Deus.

Aos professores da banca que se dispuseram a ler este trabalho.

À todos os professores do curso que, de uma maneira ou de outra, contribuíram para que eu chegasse aqui. Principalmente à professora Virgínia que orientou este trabalho com muita responsabilidade, empenho e incentivo. Obrigada pela dedicação e pelos ensinamentos.

À minha família que sempre me apoiou em todos os momentos.

Índice

Introdução

Entre 1500 e 1515, o matemático italiano Scipione del Ferro descobriu um procedimento para resolver a equação cúbica $x^3 + px = q$ $(p, q > 0)$.

> [...] Del Ferro mostrou que a equação é resolúvel por radicais. A solução de Del Ferro colocou o seguinte desafio para os algebristas: será que toda equação algébrica é resolúvel por radicais?
>
> [...] As pesquisas visando responder a essa questão se arrastaram por mais de dois séculos e meio, frustraram alguns dos grandes matemáticos desse período e contribuíram decisivamente para a criação do conceito de grupo.
>
> [...] Com o tempo, verificou-se que a idéia de grupo era um instrumento da mais alta importância para a organização e o estudo de muitas partes da matemática. Em nível mais elementar, um exemplo é a teoria das simetrias, muito importante para a cristalografia e a química, por exemplo. Essencialmente, os grupos podem ser usados para retratar simetrias geométricas: a cada figura associa-se um grupo, grupo esse que caracteriza e retrata a simetria da figura.

Nesse trabalho, o leitor vai conhecer os principais conceitos, propriedades e resultados da teoria de grupos que, como dito anteriormente, servirá de base para os mais variados ramos da matemática. Apresentamos uma disposição geral de nosso trabalho.

No capítulo 1, estudamos os conceitos de grupos e subgrupos, bem como suas principais propriedades. Apresentamos alguns exemplos, a fim de fixar melhor os conceitos estudados.

No capítulo 2, estudamos classes laterais e fornecemos exemplos das mesmas, mostrando inclusive que podemos ter classes laterais à esquerda que não são classes

laterais à direita e vice-versa. De posse do conceito de classe lateral à direita (à esquerda), apresentamos os conceitos de subgrupos normais e de grupos quocientes que são importantes para o estudo de grupos. Os principais motivos para estudarmos grupos quocientes é para obtermos outros grupos a partir de um grupo dado, assim como, para identificarmos um grupo mais simples e fácil de trabalharmos com outro mais complexo, via isomorfismo de grupos. Mais uma vez apresentamos exemplos para fixação.

No capítulo 3, estudamos os conceitos de homomorfismo e isomorfismo, bem como resultados importantes desses conceitos que serão de extrema utilidade para os conceitos apresentados no capítulo 4. Uma importante aplicação de isomorfismo de grupos é o teorema de Cayley que afirma que todo grupo G é isomorfo a um subgrupo do grupo das permutações de G.

Finalmente, no capítulo 4, estudamos o teorema do homomorfismo, um dos principais senão o mais importante dos teoremas vistos na teoria de grupos. Apresentamos também seus corolários a fim de aprofundarmos o estudo e aplicarmos o dito teorema.

Capítulo 1

Grupos

Nesse capítulo, o objetivo principal é apresentar definições, propriedades e exemplos de grupos.

1.1 Definição e exemplos

Seja G um conjunto não vazio onde está definida uma operação entre pares de G, denotada por

$$\begin{array}{rccc} * : & G \times G & \to & G \\ & (x, y) & \mapsto & x * y. \end{array}$$

Dizemos que o par $(G, *)$ é um grupo se são válidas as seguintes propriedades:

G_1) $a * (b * c) = (a * b) * c \ \forall \ a, b, c \in G$, ou seja, a operação $*$ é associativa;

G_2) $\exists e \in G$ tal que $a * e = e * a = a$, $\forall \ a \in G$, dizemos que e é o elemento neutro para a operação $*$;

G_3) $\forall \ a \in G$, $\exists b \in G$ tal que $a * b = b * a = e$, o elemento $b \in G$ é chamado simétrico para a em relação a operação $*$.

Se ocorre $a * b = b * a$, $\forall \ a, b \in G$, dizemos que o grupo $(G, *)$ é um *grupo comutativo* ou *abeliano* (em honra ao matemático norueguês N.H. Abel - 1802-1829).

A fim de simplificar notações usamos G ao invés de $(G, *)$ para denotar um grupo. Usamos também $a \cdot b = ab$, em vez de $a * b$, para representar o resultado de a operado com b. Disso, fica claro que estamos usando notação multiplicativa. Nesse contexto, o elemento b tal que $ab = ba = e$ é chamado inverso de a e o

denotamos por $b = a^{-1}$ e G é dito um grupo multiplicativo, $(G, \cdot)$.

Definição 1.1. *Seja G um grupo multiplicativo. Se $a \in G$ e $m \in \mathbb{Z}$, a potência m-ésima de a de expoente m, é o elemento de G denotado por a^m e definido da seguinte maneira:*

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

Proposição 1.2. *Propriedades imediatas de um grupo. Seja $(G, \cdot)$ um grupo.*

(i) *O elemento neutro é único;*

(ii) *Para cada $a \in G$, existe único $b \in G$ tal que $ab = ba = e$, ou seja, o elemento inverso é único;*

(iii) $a^m a^n = a^{m+n}$, $\forall a \in G$, $\forall\ m, n \in \mathbb{Z}$;

(iv) $(a^m)^n = a^{mn}$, $\forall a \in G$, $\forall\ m, n \in \mathbb{Z}$;

(v) $(ab)^{-1} = b^{-1}a^{-1}$.

Demonstração. (i) Sejam $e_1, e_2 \in G$ elementos neutros de G. Logo, $e_1 = e_1 e_2 = e_2$.

(ii) Sejam b_1, $b_2 \in G$ tais que $ab_1 = b_1 a = e$ e $ab_2 = b_2 a = e$. Segue que $b_1 = eb_1 = (b_2 a)b_1 = b_2(ab_1) = b_2$ e portanto, $b_1 = b_2$.

(iii) Demonstramos primeiro para o caso particular: $n \geq 0$ e $m + n \geq 0$. O raciocínio será por indução sobre n.

Se $n = 0$, então $a^m a^n = a^m a^0 = a^m e = a^m = a^{m+0} = a^{m+n}$. Portanto, a propriedade é verdadeira quando $n = 0$.

Seja $r \geq 0$ e suponhamos que, para qualquer inteiro m tal que $m + r \geq 0$, se tenha $a^{m+r} = a^m a^r$. Então $a^m a^{r+1} \overset{(*)}{=} a^m(a^r a) = (a^m a^r)a \overset{(**)}{=} a^{m+r}a \overset{(*)}{=} a^{(m+r)+1}$. Em $(*)$ usamos definição de potência e em $(**)$ usamos a hipótese de indução.

Para o caso geral, sejam m e n inteiros quaiquer. Tomemos um número inteiro $p > 0$ tal que $p + n > 0$ e $p + m + n > 0$, o que obviamente sempre é possível, pois $\mathbb{Z}$ é ilimitado superiormente. Isso posto, observemos primeiro que, devido à definição, $a^p a^{-p} = a^p (a^p)^{-1} = e$. Então

$$\begin{array}{rclcl} a^{m+n} & = & a^{m+n}(a^p a^{-p}) & = & (a^{m+n}a^p)a^{-p} \\ & = & a^{(m+n)+p}a^{-p} & = & a^{m+(n+p)}a^{-p} \\ & = & (a^m a^{n+p})a^{-p} & = & [a^m(a^n a^p)]a^{-p} \\ & = & [(a^m a^n)a^p]a^{-p} & = & (a^m a^n)(a^p a^{-p}) \\ & = & (a^m a^n)e & = & a^m a^n. \end{array}$$

(iv) Demonstramos primeiro para o caso particular: $n \geq 0$ e $mn \geq 0$. O raciocínio será por indução sobre n.

Se $n = 0$, então $(a^m)^n = (a^m)^0 = e = a^0 = a^{m0} = a^{mn}$. Portanto, a propriedade é verdadeira quando $n = 0$. Seja $r \geq 0$ e suponhamos que, para qualquer inteiro m tal que $mr \geq 0$, se tenha $a^{mr} = (a^m)^r$. Então $(a^m)^{r+1} = (a^m)^r(a^m)^1 \overset{(*)}{=} a^{mr}a^m \overset{(**)}{=} a^{mr+m} = a^{m(r+1)}$, em $(*)$ usamos a hipótese de indução e em $(**)$ usamos (iii).

Agora suponhamos $n < 0$. Então $(a^m)^n \overset{(*)}{=} [(a^m)^{-n}]^{-1} = (a^{-mn})^{-1} \overset{(**)}{=} a^{mn}$, usamos em $(*)$ a definição de potência e em $(**)$ a definição de inverso.

(v) Temos que $(ab)(b^{-1}a^{-1}) = ((ab)b^{-1})a^{-1} = (a(bb^{-1}))a^{-1} = (ae)a^{-1} = aa^{-1} = e$. Também, $(b^{-1}a^{-1})(ab) = b^{-1}(a^{-1}(ab)) = b^{-1}((a^{-1}a)b) = b^{-1}(eb) = b^{-1}b = e$. Logo, $(ab)^{-1} = b^{-1}a^{-1}$. □

Exemplo 1.3. Seja S um conjunto não vazio e seja

$$G = \{f : S \to S : f \text{ bijetora}\}.$$

Consideremos $\circ$ a operação composição de funções, e definimos

$$\begin{array}{rccc} * : & G \times G & \to & G \\ & (g, f) & \mapsto & g \circ f \end{array}$$

então $(G, \circ)$ é claramente um grupo tendo I como elemento neutro. Esse grupo é chamado de *grupo das permutações do conjunto* S e denotamos por $S(G)$.

Se $S = \{1, 2, \cdots, n\}$ denotaremos esse grupo por S_n, e temos que o número de elementos de S_n é exatamente $n!$.

Agora vamos mostrar que os grupos S_n, $n \geq 3$, são exemplos de grupos não abelianos.

De fato, sejam f, $g \in S_n$ definidas como segue:

$$f : \{1, 2, 3, \cdots, n\} \to \{1, 2, 3, \cdots, n\}$$

$f(1) = 2$, $f(2) = 1$, $f(x) = x$ $\forall x$, $3 \leq x \leq n$ e

$$g : \{1, 2, 3, \cdots, n\} \to \{1, 2, 3, \cdots, n\}$$

$g(1) = 2$, $g(2) = 3$, $g(3) = 1$, $g(x) = x$ $\forall x$, $4 \leq x \leq n$.

Ora, como

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

temos que $g \circ f \neq f \circ g$.

Exemplo 1.4. Grupo aditivo de classe de restos $(\mathbb{Z}_n, +)$, $n \geq 2$.

Lembremos que, para qualquer inteiro $n \geq 2$, o conjunto das classes de resto módulo n, ou seja, $\mathbb{Z}_n = \{\bar{0}, \bar{1}, \bar{2}, \cdots, \overline{n-1}\}$ é o conjunto quociente de $\mathbb{Z}$ pela relação de equivalência congruência módulo n. A adição é definida por: $\bar{a} + \bar{b} = \overline{a+b}$.

Não é difícil ver que esta operação é associativa e comutativa e, além disso, tem $\bar{0}$ como elemento neutro e $\forall \bar{a} \in \mathbb{Z}_n, \exists\, \overline{n-a} \in \mathbb{Z}_n$ tal que $\bar{a} + \overline{n-a} = \overline{a+n-a} = \overline{n} = \bar{0}$. Portanto, $(\mathbb{Z}_n, +)$ é um grupo comutativo.

Exemplo 1.5. Grupo dos elementos invertíveis de $\mathbb{Z}_n$ - $(U(\mathbb{Z}_n), \cdot)$.

Se considerarmos primeiramente o conjunto $\mathbb{Z}_6$ com a operação multiplicativa, vemos facilmente que $\bar{0}, \bar{2}, \bar{3}, \bar{4}$ não possuem inverso em $\mathbb{Z}_6$ e portanto, $(\mathbb{Z}_6, \cdot)$ não é um grupo. Agora se excluirmos estes elementos, ficamos com o conjunto $U(\mathbb{Z}_6) = \{\bar{1}, \bar{5}\}$ cujos elementos são invertíveis em $\mathbb{Z}_6$, pois $\bar{1}\bar{1} = \bar{1}$, o que implica $\bar{1}^{-1} = \bar{1}$ e $\bar{5}\bar{5} = \overline{25} = \bar{1}$, o que implica que $\bar{5}^{-1} = \bar{5}$. Este é o grupo dos elementos invertíveis de $\mathbb{Z}_6$.

Mas como descobrir quais são os elemento invertíveis de $\mathbb{Z}_n$? Mostramos a seguinte afirmação: $\bar{x} \in \mathbb{Z}_n$é invertível $\Leftrightarrow MDC(x, n) = 1$

($\Rightarrow$) Temos por hipótese que $\bar{x}$ é invertível. Assim, $\exists\, \bar{y} \in \mathbb{Z}_n$ tal que $\bar{x}\bar{y} = \bar{1}$, ou seja, $\overline{xy} = \bar{1}$. Portanto, $n|xy - 1$ e $xy - 1 = nq$ para algum $q \in \mathbb{Z}$.

Logo, $xy + n(-q) = 1$, o que implica, $MDC(x, n) = 1$.

($\Leftarrow$) Temos por hipótese que o $MDC(x, n) = 1$. Daí, $na_0 + xb_0 = 1$, para convenientes inteiros a_0 e b_0 (identidade de Bezout). Temos que $1 - xb_0 = na_0$ e isso implica que $n|1 - xb_0$, isto é, $\overline{xb_0} = \bar{1} \Rightarrow \bar{x}\overline{b_0} = \bar{1}$ e $\bar{x}$ é invertível.

Exemplo 1.6. Grupo das simetrias do triângulo equilátero, D_3.

Para caracterizar geometricamente as simetrias do triângulo equilátero, indiquemos seus vértices consecutivamente por $1, 2, 3$ e consideremos as seguintes retas pelo baricentro O do triângulo: x, pelo vértice 1, y pelo vértice 2, e z, pelo vértice 3. Denotando-se por R_0, R_1 e R_2 as rotações de $0, 2\pi/3$ e $4\pi/3$ radianos em torno de O no sentido anti-horário e por X, Y e Z, respectivamente, as reflexões espaciais de π radianos em torno das retas x, y e z. Mostremos que o conjunto $\{R_0, R_1, R_2, X, Y, Z\}$ com a composição de transformações é um grupo não abeliano.

$\circ$	R_0	R_1	R_2	X	Y	Z
R_0	R_0	R_1	R_2	X	Y	Z
R_1	R_1	R_2	R_0	Z	X	Y
R_2	R_2	R_0	R_1	Y	Z	X
X	X	Z	Y	R_0	R_2	R_1
Y	Y	X	Z	R_1	R_0	R_2
Z	Z	Y	X	R_2	R_1	R_0

Por meio da tábua acima verificamos o fechamento, que R_0 é o elemento neutro e que $R_0^{-1} = R_0$, $R_1^{-1} = R_2$, $R_2^{-1} = R_1$, $X^{-1} = X$, $Y^{-1} = Y$ e $Z^{-1} = Z$. Vale a associatividade por se tratar de composição de transformações, então efetivamente se trata de um grupo. Denotamos esse grupo por $D_3 = \{R_0, R_1, R_2, X, Y, Z\}$. Como $XY = R_2 \neq R_1 = YX$, o grupo não é abeliano. Por outro lado, observando-se que $R_1^2 = R_1 \circ R_1 = R_2$, $X \circ R_1 = Z$ e $X \circ R_1^2 = Y$, então $D_3 = \{R_1^0, R_1, R_1^2, X, X \circ R_1, X \circ R_1^2\}$.

1.2 Subgrupos

Nessa seção, definimos o conceito de subgrupos, apresentamos algumas definições equivalentes e alguns exemplos.

Definição 1.7. *Sejam G um grupo e H um subconjunto não vazio de G. Dizemos que H é um subgrupo de G se H for ele próprio um grupo com a mesma operação de G.*

Se H for um subgrupo de G denotamos isso por $H \leq G$.

Antes da próxima proposição, observamos que se H é um subgrupo de G, e_H é o elemento neutro de H e e_G é o elemento neutro de G, então $e_H = e_G$. Isso acontece, pois para todo $x \in H$, existem x_H^{-1} (o inverso de x em H) e x_G^{-1} (o inverso de x em G) tais que $xx_H^{-1} = x_H^{-1}x = e_H$ e $xx_G^{-1} = x_G^{-1}x = e_G$. Assim,

$$e_H = e_H e_G = e_H(xx_G^{-1}) = (e_H x)x_G^{-1} = xx_G^{-1} = e_G.$$

Donde, $e_H = e_G$.

Aproveitamos a oportunidade para mostrarmos que para todo $x \in H$, $x_H^{-1} = x_G^{-1}$. De fato, $x_H^{-1} = e_H x_H^{-1} \overset{(*)}{=} (x_G^{-1}x)x_H^{-1} = x_G^{-1}(xx_H^{-1}) = x_G^{-1}e_H \overset{(*)}{=} x_G^{-1}$, em que as igualdades $(*)$ e $(**)$ são devidas ao fato de que $e_H = e_G$.

Proposição 1.8. *Sejam G um grupo e H um subconjunto de G. As seguintes condições são equivalentes:*

(a) *H é um subgrupo de G;*

(b) (i) *$e \in H$;*

(ii) *$\forall a,\ b \in H$ tem-se $ab \in H$;*

(iii) *$\forall a \in H$ tem-se $a^{-1} \in H$;*

(c) *$H \neq \emptyset$ e $\forall a,\ b \in H$ tem-se $ab^{-1} \in H$.*

Demonstração. (a) $\Rightarrow$ (b) Segue imediatamente da definição de subgrupo.

(b) $\Rightarrow$ (c) Primeiramente, se $e \in H$ então $H \neq \emptyset$ e se $b \in H$ então $b^{-1} \in H$ por (iii).

Assim, se $a,\ b \in H$ temos que $a,\ b^{-1} \in H$ e por (ii) segue $ab^{-1} \in H$ como queríamos demonstrar.

(c) $\Rightarrow$ (a) Sendo $H \neq \emptyset$, $\exists\, h \in H$. Daí, $e = hh^{-1} \in H$. Dado $x \in H$ e como $e \in H$, segue que $x^{-1} = ex^{-1} \in H$. Finalmente, dados $x, y \in H$, sabemos que $y^{-1} \in H$ e portanto, $xy = x(y^{-1})^{-1} \in H$. Como a associatividade é herdada de G, segue que H é um subgrupo de G. □

Exemplo 1.9. Seja G um grupo. Então

$$Z(G) = \{a \in G : ax = xa\ \forall x \in G\}$$

é um subgrupo de G. $Z(G)$ é denominado *centro do grupo* G. Além disso, $Z(G)$ é um subgrupo abeliano do grupo G.

De fato, $e \in Z(G)$ pois $xe = ex = x$, $\forall x \in G$. Dados $a, b \in Z(G)$, $(ab)x = a(bx) = a(xb) = (ax)b = (xa)b = x(ab)$, $\forall x \in G$. Logo, $ab \in Z(G)$. Também, se $a \in Z(G)$, então $ax = xa$, $\forall x \in G$. Daí, $a^{-1}(ax) = a^{-1}(xa) \Rightarrow x = (a^{-1}x)a \Rightarrow xa^{-1} = (a^{-1}x)aa^{-1} = a^{-1}x$, ou seja, $xa^{-1} = a^{-1}x$, $\forall x \in G$ e portanto, $a^{-1} \in Z(G)$.

Finalmente, $Z(G)$ é comutativo, pois para qualquer $x, y \in Z(G)$, trivialmente, $xy = yx$.

Exemplo 1.10. Sejam G um grupo e $x \in G$. Se $n \in \mathbb{Z}$ já sabemos que

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

Se denotarmos $< x >= \{x^m : m \in \mathbb{Z}\} \subset G$ então como $x^0 = e$, $(x^m)^{-1} = x^{-m}$ e $x^m x^n = x^{m+n}$ (propriedades (iii) e (iv) de grupos) segue que $< x >$ é um grupo chamado *subgrupo cíclico* gerado pelo elemento $x \in G$.

No caso em que $G =< x >$, G é dito grupo cíclico gerado pelo elemento x.

Em notação aditiva

$$< x >= \{nx : n \in \mathbb{Z}\}$$

o grupo cíclico gerado por x e

$$nx = \begin{cases} e & se \quad n = 0 \\ ((n-1)x) + x & se \quad n > 0 \\ -((-n)x) & se \quad n < 0. \end{cases}$$

Proposição 1.11. *Todo grupo cíclico é abeliano.*

Demonstração. Seja G um grupo cíclico. Então $G =< x >= \{x^m : m \in \mathbb{Z}\}$. Sejam $x', y' \in G$. Então $x' = x^m$ e $y' = x^n$. Pela propriedade (iii) de grupos, temos que $x^m x^n = x^{m+n}$ e portanto, $x^{m+n} = x^{n+m} = x^n x^m$. Logo, todo grupo cíclico é abeliano. □

Exemplo 1.12. O grupo aditivo das classes de restos $(\mathbb{Z}_n, +)$, $n \geq 2$, é um grupo cíclico gerado por $\bar{1}$, pois $\forall\, \bar{x} \in \mathbb{Z}_n$, $\bar{x} = x\bar{1} = \bar{1} + \bar{1} + \cdots + \bar{1}$ n vezes.

Exemplo 1.13. Seja $G = \{R_0, R_1, R_2\}$ com a operação composição de funções,

o grupo das rotações planas do triângulo equilátero. Temos que G é cíclico gerado por R_1, pois $R_1^2 = R_2$ e $R_1^3 = R_2 \circ R_1 = R_0$.

Exemplo 1.14. Considerando $u = cos\frac{2\pi}{n} + isen\frac{2\pi}{n}$, o conjunto $\{1, u, u^2, \cdots, u^{n-1}\}$, para $n \geq 1$ é um grupo cíclico gerado por u. Tal grupo é conhecido como o grupo das raízes n-ésimas da unidade.

Notemos que $u^n = (cos\frac{2\pi}{n} + isen\frac{2\pi}{n})^n = cos2\pi + isen2\pi = 1$. Consequentemente, para qualquer $k \in \mathbb{Z}$, pela divisão de k por n, segue que existem $q, r \in \mathbb{Z}$ tais que $k = nq + r$ com $0 \leq r \leq n-1$. Assim, $u^k = (u^n)^q\, u^r$ e com isso, $u^k = u^r$ com $0 \leq r \leq n-1$ para todo $k \in \mathbb{Z}$, ficando claro que o grupo das raízes n-ésimas da unidade é gerado por u.

Capítulo 2

Classes laterais e grupos quociente

Nesse capítulo, introduzimos os conceitos de classes laterais à direita e à esquerda. Fixado um subgrupo H de um grupo G, o fato de que classe lateral à esquerda e à direita de H em G para certos elementos de G podem ser distintas, traz a necessidade da definição de subgrupos normais. Tais subgrupos possibilitam a construção de grupos quocientes.

2.1 Classes laterais

Proposição 2.1. *Sejam G um grupo e $x, y \in G$. Seja H um subgrupo de G. Dizemos que $x \equiv y \,(\mathrm{mod} H) \Leftrightarrow xy^{-1} \in H$. Então $\equiv (\mathrm{mod} H)$ é uma relação de equivalência no conjunto G.*

Demonstração. Sejam $x, y, z \in G$. Então
(i) $x \equiv x \pmod{H}$ $\forall x \in G$ pois $e = xx^{-1} \in H$.
(ii) Se $x \equiv y \pmod{H}$ então $y \equiv x \pmod{H}$, pois se $xy^{-1} \in H$ então $yx^{-1} = (xy^{-1})^{-1} \in H$.
(iii) Se $x \equiv y \pmod{H}$ e $y \equiv z \pmod{H}$ então $x \equiv z \pmod{H}$, pois

$$xy^{-1} \in H \text{ e } yz^{-1} \in H \Rightarrow xz^{-1} = (xy^{-1})(yz^{-1}) \in H.$$

e isto demonstra a proposição. □

Consideremos agora um elemento qualquer $x \in G$, sua classe de equivalência é definida como

$$\bar{x} = \{y \in G : y \equiv x (\mathrm{mod} H)\}.$$

Assim, $y \in \bar{x} \Leftrightarrow y \equiv x \pmod{H} \Leftrightarrow yx^{-1} = h \in H$, para algum $h \in H \Leftrightarrow y = hx$ para algum $h \in H$. Logo, $Hx = \{hx : h \in H\} = \bar{x}$ e a chamamos *classe lateral à direita de H em G determinada por x*. Alertamos o leitor para o fato de que podemos usar ambas as notações, ou seja, Hx ou $\bar{x}$.

Analogamente à Proposição 2.1, podemos definir a relação de equivalência $x \equiv y \pmod{H} \Leftrightarrow x^{-1}y \in H$.

Nesse caso $xH = \{xh : h \in H\}$ é chamada *classe lateral à esquerda de H em G determinada por x*.

Proposição 2.2. *Sejam $x, y \in H$. Então $Hx = Hy$ se, e somente se, $xy^{-1} \in H$. Analogamente, $xH = yH$ se, e somente se, $x^{-1}y \in H$.*

Demonstração. ($\Rightarrow$) Suponhamos $Hx = Hy$. Sendo assim, $x \in Hy$ e isso implica que $x \equiv y \pmod{H}$ que, por sua vez, implica que $xy^{-1} \in H$.

($\Leftarrow$) Suponhamos que $xy^{-1} \in H$. Seja $z \in Hx$. Então $z = hx$ para algum $h \in H$ e daí, $zy^{-1} = hxy^{-1} \in H$. Logo, $z \in Hy$ e $Hx \subseteq Hy$. Analogamente, $Hy \subseteq Hx$ e portanto, $Hy = Hx$. □

Calculamos abaixo algumas classes laterais e o leitor observará casos em que classes laterais à direita e classes laterais à esquerda podem ser distintas e podem ser iguais. Certamente, se o grupo é abeliano, para quaisquer elementos do grupo, suas classes laterais à direita e à esquerda coincidem, independentemente do subgrupo em questão.

Exemplo 2.3. No grupo multiplicativo $G = \{1, -1, i, -i\}$ das raízes quárticas da unidade, consideramos o subgrupo $H = \{1, -1\}$. As classes laterais à esquerda e à direita, nesse caso são:

$$\begin{gathered} 1H = \{1, -1\} = H1 \\ (-1)H = \{-1, 1\} = H(-1) \\ iH = \{i, -i\} = Hi \\ (-i)H = \{-i, i\} = H(-i). \end{gathered}$$

Portanto, temos duas classes laterais à direita (que também são classes laterais à esquerda), a saber, $H1$ e Hi (respectivamente $1H$ e iH).

Exemplo 2.4. No grupo das simetrias do triângulo, $D_3 = \{R_0, R_1, R_2, X, Y, Z\} = \{R_0, R_1, R_1^2, X, X \circ R_1, X \circ R_1^2\}$, consideramos o subconjunto $H = \{R_0, X\}$. Não é difícil observar que H é subgrupo de D_3. Agora, vejamos as classes laterais determinadas por Z:

$$Z \circ H = \{Z, R_2\}$$
$$H \circ Z = \{Z, R_1\}$$

Vemos neste caso que a classe lateral à esquerda e à direita determinadas por Z são diferentes.

Ao observarmos os exemplos acima, percebemos que há casos em que as classes laterais à esquerda e à direita são diferentes e em outros casos elas são iguais. Nosso foco daqui para frente será nos casos em que elas são iguais. Porém, antes disso, mostramos alguns resultados envolvendo classes laterais como, por exemplo, o Teorema de Lagrange.

Proposição 2.5. *Sejam G grupo e H um subgrupo de G. Então, para quaisquer $x, y \in G$, existe uma bijeção entre Hx e Hy e também entre H e Hx.*

$$\begin{array}{rccc} \varphi: & Hx & \to & Hy \\ & hx & \mapsto & hy \end{array}$$

Demonstração. Primeiro mostramos que φ é injetora. Suponhamos $\varphi(hx) = \varphi(h'x)$. Então $hy = h'y \Rightarrow hyy^{-1} = h'yy^{-1} \Rightarrow h = h' \Rightarrow hx = h'x$.

Agora mostremos que φ é sobrejetora. Seja $z \in Hy$. Então $z = hy$ para algum $h \in H$ e daí, $hx \in Hx$ e $\varphi(hx) = hy = z$. Logo, Hx e Hy possuem a mesma cardinalidade.

Além disso, seja

$$\begin{array}{rccc} \varphi: & H & \to & Hx \\ & h & \mapsto & hx \end{array}$$

Temos que φ é claramente sobrejetora. Por outro lado, se $\varphi(h_1) = \varphi(h_2)$ então $h_1x = h_2x$ e isso implica que $h_1 = h_2$ e daí, φ é injetora. □

Proposição 2.6. *Sejam G um grupo e H um subgrupo de G. Então existe uma bijeção entre o conjunto das classes laterais à direita e o conjunto da classes laterais à esquerda.*

$$\begin{array}{rccc} \varphi: & \{Hx : x \in G\} & \to & \{xH : x \in G\} \\ & Hx & \mapsto & x^{-1}H \end{array}$$

Demonstração. Primeiro mostramos que φ está bem definida (não depende do representante). De fato, se $Hx = Hy$, isto implica que $xy^{-1} \in H$ pela Proposição 2.2. Como $(x^{-1})^{-1}y^{-1} = xy^{-1} \in H$ segue, novamente pela Proposição 2.2 que, $x^{-1}H = y^{-1}H$ e portanto, $\varphi(Hx) = \varphi(Hy)$.

Agora, mostremos que φ é bijetora. Temos que φ é injetora, pois se $\varphi(Hx) = \varphi(Hy)$ então $x^{-1}H = y^{-1}H$ e daí, $(x^{-1})^{-1}y^{-1} = xy^{-1} \in H$, ou seja, $Hx = Hy$.

Por último, mostremos que φ é sobrejetora. Seja $z \in \{xH : x \in G\}$. Então $z = yH$, para algum $y \in G$. Claramente $Hy^{-1} \in \{Hx : x \in G\}$ e portanto, $\varphi(Hy^{-1}) = (y^{-1})^{-1}H = yH = z$. □

Antes de provarmos o conhecido teorema de Lagrange, consideremos G um grupo finito, chamamos *ordem de* G ao número de elementos do grupo G e notamos por $|G|$.

Teorema 2.7. *(Teorema de Lagrange) Se G é um grupo finito e H é um subgrupo de G então o número de elementos de H é um divisor do número de elementos de G.*

Demonstração. Definindo em G a relação de equivalência $\equiv \pmod{H}$ e sendo G um grupo finito segue imediatamente que o conjunto das classes laterais à direita (e à esquerda) de H em G é finito. Seja n o número de classes laterais à direita de G. Assim,

$$G = Hx_1 \cup Hx_2 \cup \cdots \cup Hx_n$$

(união disjunta) e portanto, segue que

$$|G| = |Hx_1| + |Hx_2| + \cdots + |Hx_n|.$$

Pela Proposição 2.5, $G = n|H|$ e assim, $|H|$ é um divisor de $|G|$. □

Com a notação acima, mas no caso particular em que H é normal em G (estudamos normalidade na próxima seção), temos que $n = |G/H|$ é a ordem do grupo quociente G/H e, por Lagrange, $G = |G/H||H|$.

Corolário 2.8. *Todo grupo finito de ordem prima é cíclico.*

Demonstração. Seja G um grupo tal que $|G| = p$ onde p é um número primo. Como $p \geq 2$, existe $x \in G$, $x \neq e$. Então $< x >$ é um subgrupo de G contendo o conjunto $\{e, x\}$. Assim, pelo Teorema de Lagrange, $| < x > |$ é um divisor de $|G| = p$ e como $| < x > | > 1$, segue que $| < x > | = p$ e isso nos diz que $G =< x >$. □

Corolário 2.9. *Se G é um grupo tal que $|G| \leq 5$ então G é abeliano.*

Demonstração. Se $|G| = 1$ então $G = \{e\}$. Se $|G| = 2$, 3 ou 5 e como esses são números primos segue, pelo corolário acima, que G é cíclico e portanto abeliano. Para $|G| = 4$ temos dois casos. Primeiro caso, se $\exists\, x \neq e$, $x \in G$ tal que $< x >= G$ então G é cíclico e portanto abeliano. No segundo caso, $\forall\, x \in G$, $x \neq e$, temos $< x >\neq G$. Ora, pelo teorema de Lagrange, segue imediatamente que $| < x > | = 2$. Assim, $x^2 = e$, $\forall\, x \in G$ e, nesse caso G é abeliano, veja observação abaixo. □

Observação: Se $x^2 = e$, $\forall\, x \in G$ então G é abeliano. Sendo $x^2 = e$, segue que $x = x^{-1}$, $\forall\, x \in G$. Assim $xy = (xy)^{-1} = y^{-1}x^{-1} = yx$. Logo, G é abeliano.

2.2 Subgrupos normais

O objetivo de se estudar normalidade é exatamente o fato de querermos obter grupos quocientes e, para tanto, será necessário introduzir uma operação num conjunto quociente e tal operação só estará bem definida se o subgrupo em questão for normal no grupo dado.

Definição 2.10. *Seja G um grupo. Dizemos que um subgrupo H de G é normal em G se $gH = Hg\,, \forall g \in G$.*

Trivialmente $\{e\}$ e G são normais em G e são chamados subgrupos normais triviais de G. Usamos a notação $H \lhd G$ para dizermos que H é um subgrupo normal em G.

Um resultado direto desta definição é que se G é abeliano, então todo subgrupo de G é normal. De fato, seja H um subgrupo de G. Seja $x \in gH$. Então $x = gh$, para algum $h \in H$. Mas G é abeliano, então $x = hg \in Hg$. Sendo assim, $gH \subseteq Hg$. Analogamente, $Hg \subseteq gH$.

Observe que o subgrupo H do Exemplo 2.3 é normal em G (G é abeliano), mas o subgrupo H do Exemplo 2.4 não o é.

Podemos definir a normalidade equivalentemente como segue. Seja G um grupo e seja H um subgrupo de G. Se $g \in G$ definimos a função φ_g (*conjugação pelo elemento* $g \in G$) por

$$\begin{array}{rccccc} \varphi_g: & G & \to & G & & \\ & x & \mapsto & \varphi_g(x) & = & g^{-1}xg. \end{array}$$

Observemos que $\varphi_g(H) = \{\varphi_g(h) : h \in H\} = \{g^{-1}hg : h \in H\} = g^{-1}Hg$. Notemos que $g^{-1}Hg$ é também um subgrupo de G, pois

(i) $e = g^{-1}eg \in g^{-1}Hg$;
(ii) Dados $g^{-1}h_1g$ e $g^{-1}h_2g$ em $g^{-1}Hg$, temos que $g^{-1}h_1gg^{-1}h_2g = g^{-1}h_1h_2g \in g^{-1}Hg$;
(iii) Dado $g^{-1}hg \in g^{-1}Hg$, temos que $(g^{-1}hg)^{-1} = g^{-1}h^{-1}g \in g^{-1}Hg$.

Assim, a função conjugação transforma subgrupos de G em subgrupos de G.

Definição 2.11. *Seja G um grupo. Dizemos que um subgrupo H de G é normal (ou invariante por conjugação) em G se $\varphi_g(H) \subseteq H$, $\forall\, g \in G$.*

Proposição 2.12. *(Equivalência das definições de normalidade). Sejam G um grupo e H um subgrupo de G. Então $H \triangleleft G$ se, e somente se, $g^{-1}Hg \subseteq H$, $\forall\, g \in G$.*

Demonstração. ($\Rightarrow$) Como $H \triangleleft G$, temos que $Hg = gH$, $\forall\, g \in G$. Sejam $g \in G$ e $x \in g^{-1}Hg$. Então $x = g^{-1}hg$, para algum $h \in H$. Mas $hg \in Hg = gH$ e daí, $hg = gh'$, para algum $h' \in H$. Logo, $x = g^{-1}gh' = eh' = h' \in H$ e portanto, $g^{-1}Hg \subseteq H$.

($\Leftarrow$) Temos que $g^{-1}Hg \subseteq H$, $\forall\, g \in G$. Devemos mostrar que $Hg = gH$, $\forall\, g \in G$. Seja $x \in Hg$. Então $x = hg$ para algum $h \in H$. Mas $x = (gg^{-1})hg = g(g^{-1}hg) = gh' \in gH$, onde $h' = g^{-1}hg \in H$. Assim, $x \in gH$, ou seja, $Hg \subseteq gH$. Analogamente, $gH \subseteq Hg$. □

Agora, mostramos algumas propriedades de subgrupos normais.

Proposição 2.13. *Seja G um grupo. Então são válidas.*

(i) *Se $N_1, N_2 \triangleleft G$ então $N_1 \cap N_2 \triangleleft G$.*

(ii) *Se H é um subgrupo de G e $N \triangleleft G$ então $HN = \{hn : h \in H,\, n \in N\}$ é um subgrupo de G.*

(iii) *Se $N_1, N_2 \triangleleft G$ então $N_1N_2 \triangleleft G$.*

(iv) *Se H é um subgrupo de G e $N \triangleleft G$ então $H \cap N \triangleleft H$.*

Demonstração. (i) Sejam $x \in N_1 \cap N_2$ e $g \in G$. Então $x \in N_1$ e $x \in N_2$. Assim, $g^{-1}xg \in g^{-1}N_1g \subseteq N_1$ e $g^{-1}xg \in g^{-1}N_2g \subseteq N_2$, ou seja, $g^{-1}xg \in N_1 \cap N_2$. Assim, $g^{-1}(N_1 \cap N_2)g \subseteq N_1 \cap N_2$, $\forall\, g \in G$.

(ii) Sejam H subgrupo de G e $N \triangleleft G$. Vamos provar que $L = HN = \{hn : h \in H, n \in N\}$ é um subgrupo de G. De fato, $e = ee \in HN$. Sejam $h_1n_1, h_2n_2 \in L$. Então $h_1n_1h_2n_2 = h_1(h_2h_2^{-1})n_1h_2n_2 = (h_1h_2)(h_2^{-1}n_1h_2)n_2$. Se denotarmos $h = h_1h_2$, $n = (h_2^{-1}n_1h_2)n_2$, teremos $h \in H$ e $n \in N$ (pois $N \triangleleft G$) e assim,

$$(h_1n_1)(h_2n_2) = hn \in L = HN.$$

Se $x = hn \in L$ então $x^{-1} = n^{-1}h^{-1} = h^{-1}(hn^{-1}h^{-1})$. Mas $h^{-1} \in H$ e $hn^{-1}h^{-1} \in (h^{-1})^{-1}Nh^{-1} \subseteq N$ e portanto, $x^{-1} \in L = HN$ e isso demonstra o item (ii).

(iii) Basta observarmos que $\forall\, g \in G$, temos $g^{-1}(N_1N_2)g = (g^{-1}N_1g)(g^{-1}N_2g)$ e como $g^{-1}N_1g \subseteq N_1$ e $g^{-1}N_2g \subseteq N_2$, $\forall\, g \in G$, segue que $g^{-1}(N_1N_2)g \subseteq N_1N_2$ $\forall\, g \in G$.

(iv) Sejam $x \in H \cap N$ e $h \in H$. Então $x \in N$ e $h^{-1}xh \in h^{-1}Nh \subseteq N$. Como $x, h \in H$ segue imediatamente que $h^{-1}xh \in H \cap N$ $\forall\, h \in H$. Logo, $H \cap N \triangleleft H$. □

Exemplo 2.14. $Z(G)$ é um subgrupo normal de G. De fato, mostremos que $g^{-1}Z(G)g \subseteq Z(G)$, $\forall\, g \in G$. Sejam $g \in G$, $x \in Z(G)$ e $y \in G$. Então

$$(g^{-1}xg)y = xg^{-1}gy = xyg^{-1}g = yxg^{-1}g = y(g^{-1}xg).$$

2.3 Grupos quocientes

Agora definimos grupo quociente. Sejam G um grupo e H um subgrupo de G. Sabemos que para $x, y \in G$, $x \equiv y \pmod{H} \Leftrightarrow xy^{-1} \in H$ define uma relação de equivalência em G.

O conjunto $G/H = \{\bar{g} : g \in G\}$ é o conjunto quociente de G por essa relação de equivalência onde $\bar{g} = Hg = \{hg : h \in H\}$ é a classe de equivalência módulo H tendo g como representante.

Se H é um subgrupo normal em G, podemos introduzir de modo natural uma operação no conjunto das classes G/H de modo que G/H seja um grupo com esta operação. Este grupo receberá o nome de *grupo quociente de G por H*.

Teorema 2.15. *Sejam G um grupo e H um subgrupo normal em G. Então, $\forall\, x, y \in G$, $\bar{x}\bar{y} = \overline{xy}$ define uma operação no conjunto das classes G/H e mais ainda G/H é um grupo com essa operação.*

Demonstração. Para demonstrarmos que $\bar{x}\bar{y} = \overline{xy}$ define uma operação em G/H temos que provar que a definição acima não depende da escolha dos representantes das classes. De fato, se $\bar{x} = \bar{a}$ e $\bar{y} = \bar{b}$ provaremos que $\bar{x}\bar{y} = \bar{a}\bar{b}$, isto é, $\overline{xy} = \overline{ab}$.

Para isso é suficiente provarmos que $Hxy = Hab$, ou equivalentemente $(xy)(ab)^{-1} \in H$. Mas $xy(ab)^{-1} = xyb^{-1}a^{-1}$ e $\bar{x} = \bar{a}$ e $\bar{y} = \bar{b}$ nos diz que $xa^{-1} \in H$ e $yb^{-1} \in H$.

Se $xa^{-1} = h_1 \in H$ e $yb^{-1} = h_2 \in H$, então $(xy)(ab)^{-1} = xh_2a^{-1} = (h_1a)h_2a^{-1} = h_1(ah_2a^{-1})$ e como $h_1 \in H$ e $ah_2a^{-1} = (a^{-1})^{-1}h_2a^{-1} \in H$ segue imediatamente que $(xy)(ab)^{-1} \in H$ e a definição não depende da escolha dos representantes.

Agora, vejamos que G/H é um grupo.

(i) $\bar{x}(\bar{y}\bar{z}) = \bar{x}(\overline{yz}) = \overline{x(yz)} = \overline{(xy)z} = \overline{(xy)}\bar{z} = (\bar{x}\bar{y})\bar{z}$, $\forall\, \bar{x}, \bar{y}, \bar{z} \in G/H$.

(ii) Se e é o elemento neutro de G, então $\bar{e} = He = H$ é o elemento identidade de G/H, pois $\bar{e}\bar{x} = \overline{ex} = \bar{x} = \overline{xe} = \bar{x}\bar{e}$, $\forall\, \bar{x} \in G/H$.

(iii) Se $\bar{x} \in G/H$ então $\overline{x^{-1}}\bar{x} = \bar{x}\overline{x^{-1}} = \bar{e}$.

Assim $\overline{G} = G/H$ é um grupo com a operação definida pela regra $\bar{x}\bar{y} = \overline{xy}$, $\forall\, \bar{x}, \bar{y} \in \overline{G}$. □

Proposição 2.16. *Sejam G um grupo e $N \triangleleft G$. Então são válidas as afirmações.*
(i) *Se G é abeliano então $\overline{G} = G/N$ é abeliano.*
(ii) *Se G é cíclico então $\overline{G} = G/N$ é cíclico.*

Demonstração. (i) Sejam $\bar{x}, \bar{y} \in \overline{G} = G/N$. Então

$$\bar{x}\bar{y} = \overline{xy} = \overline{yx} = \bar{y}\bar{x}.$$

(ii) Se $G =< x >= \{x^m : m \in \mathbb{Z}\}$ então $\forall\, \bar{y} \in \overline{G}$ temos que $y \in G =< x >$ e assim $y = x^m$, para algum $m \in \mathbb{Z}$ e daí, segue que

$$\bar{y} = \overline{x^m} = \bar{x}^m \in < \bar{x} >= \{\bar{x}^r : r \in \mathbb{Z}\}.$$

Logo, $\overline{G} =< \bar{x} >$ como queríamos demonstrar. □

Capítulo 3

Homomorfismo e isomorfismo de grupos

Nesse capítulo, definimos homomorfismo e isomorfismo de grupos e apresentamos as principais propriedades relacionadas ao tema.

3.1 Homomorfismo

Sejam G_1 e G_2 grupos. Para facilitar a escrita, usamos notação multiplicativa para ambos grupos.

Definição 3.1. *Um homomorfismo de G_1 em G_2 é uma $f : G_1 \to G_2$ tal que, para quaisquer $x, y \in G_1$ vale*

$$f(xy) = f(x)f(y).$$

No caso particular em que $G_1 = G_2 = G$ e f é um homomorfismo, chamamos f um *endomorfismo* de G.

Proposição 3.2. *Sejam G_1 e G_2 grupos, $f : G_1 \to G_2$ um homomorfismo de grupos e e_1 e e_2 elementos neutros de G_1 e G_2, respectivamente. São válidas as seguintes propriedades.*

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

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

(iii) *A imagem de f, $Im(f) = f(G_1) = \{f(x) : x \in G_1\}$, é um subgrupo de G_2.*

(iv) *O núcleo de f, $Ker(f)$, definido como $Ker(f) = \{x \in G_1 : f(x) = e_2\}$ é um subgrupo normal de G_1.*

(v) *f é injetora se, e somente se, $Ker(f) = \{e_1\}$.*

(vi) *Seja $g : G_2 \to G_3$ homomorfismos de grupos. Então $g \circ f : G_1 \to G_3$ é um homomorfismo de grupos.*

Demonstração. (i) Temos que $f(e_1) = f(e_1e_1) = f(e_1)f(e_1)$, ou seja, $f(e_1) = f(e_1)f(e_1)$ e multiplicando-se ambos os lados dessa igualdade por $f(e_1)^{-1}$, segue que, $e_2 = f(e_1)$.

(ii) Usamos o item acima. Temos que $f(a)f(a^{-1}) = f(aa^{-1}) = f(e_1) = e_2$ e analogamente, $f(a^{-1})f(a) = e_2$ e isso implica que $f(a^{-1}) = (f(a))^{-1}$ (definição de elemento inverso).

(iii) Como $e_2 = f(e_1) \in Im(f)$, segue que $Im(f) \neq \emptyset$. Agora, sejam $c, d \in Im(f)$. Então $c = f(a)$ e $d = f(b)$, para convenientes elementos $a, b \in G_1$. Logo, $cd^{-1} = f(a)(f(b))^{-1} = f(a)f(b^{-1}) = f(ab^{-1})$. Como $ab^{-1} \in G_1$, então $cd^{-1} \in Im(f)$. Sendo assim, $Im(f)$ é um subgrupo de G_2.

(iv) Primeiro mostremos que $Ker(f)$ é um subgrupo de G_1. Como $f(e_1) = e_2$, então $e_1 \in Ker(f)$ e portanto, $Ker(f) \neq \emptyset$. Por outro lado, se $a, b \in Ker(f)$, então $f(a) = f(b) = e_2$ e daí,

$$f(ab^{-1}) = f(a)f(b^{-1}) = f(a)(f(b))^{-1} = e_2e_2^{-1} = e_2.$$

Isso demonstra que $ab^{-1} \in Ker(f)$ e portanto, $Ker(f)$ é um subgrupo de G_1.

Agora, para mostrarmos que $Ker(f) \triangleleft G_1$ basta mostrar que $x^{-1}Ker(f)x \subseteq Ker(f)\ \forall\, x \in G_1$, ou seja, $f(x^{-1}Ker(f)x) = e_2$. Seja $y \in Ker(f)$. Então

$$f(x^{-1}yx) = f(x^{-1})f(y)f(x) = f(x^{-1})e_2f(x) = f(x^{-1}x)e_2 = f(e_1)e_2 = e_2e_2 = e_2.$$

Logo, $x^{-1}Ker(f)x \subseteq Ker(f)$ e portanto $Ker(f) \triangleleft G_1$.

(v) ($\Rightarrow$) Seja $a \in Ker(f)$. Mostremos que necessariamente $a = e_1$. De fato, como $a \in Ker(f)$, então $f(a) = e_2$. Mas sabemos que $f(e_1) = e_2$ e sendo f é injetora, segue que $a = e_1$.

($\Leftarrow$) Sejam $x, y \in G$ elementos tais que $f(x) = f(y)$. Multiplicando-se cada membro dessa igualdade por $(f(y))^{-1}$, obtém-se $f(x)(f(y))^{-1} = e_2$. Mas $e_2 = f(x)(f(y))^{-1} = f(x)f(y^{-1}) = f(xy^{-1})$. Portanto, $xy^{-1} \in Ker(f) = \{e_1\}$. Então $xy^{-1} = e_1$ e assim, $x = y$. Donde, f é injetora, como queríamos demonstrar.

(vi) Sejam $x, y \in G_1$. Temos que $(g \circ f)(xy) = g(f(xy)) = g(f(x)f(y)) = g(f(x))g(f(y)) = (g \circ f)(x)(g \circ f)(y)$. □

Exemplo 3.3. Homomorfismo trivial. Sejam G_1 e G_2 grupos.

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

Sejam $x, y \in G_1$. Então

$$f(xy) = e_2 = e_2 e_2 = f(x)f(y).$$

Logo, f é um homomorfismo.

Exemplo 3.4. A identidade I é um homomorfismo. Seja G um grupo. Então

$$\begin{array}{rccc} I: & G & \to & G \\ & g & \mapsto & g \end{array}$$

é claramente um homomorfismo. Basta observarmos que dados quaisquer $g_1, g_2 \in G$ temos que $I(g_1 g_2) = g_1 g_2 = I(g_1)I(g_2)$.

Exemplo 3.5. Inclusão canônica. Sejam G um grupo e H um subgrupo de G.

$$\begin{array}{rccc} \iota: & H & \to & G \\ & h & \mapsto & h \end{array}$$

Sejam $h_1, h_2 \in H$. Então

$$\iota(h_1 h_2) = h_1 h_2 = \iota(h_1)\iota(h_2).$$

Logo, ι é um homomorfismo.

Exemplo 3.6. Projeção canônica. Sejam G um grupo, $N \triangleleft G$ e $\overline{G} = G/N$ o grupo quociente de G por N. Então

$$\begin{array}{rccccc} \pi: & G & \to & \overline{G} & & \\ & x & \mapsto & \pi(x) & = & \bar{x} \end{array}$$

é um homomorfismo sobrejetor. De fato, $\pi(xy) = \overline{xy} = \bar{x}\bar{y} = \pi(x)\pi(y)\ \forall\, x, y \in G$. Também, $Ker(\pi) = \{x \in G : \pi(x) = \bar{e}\} = N$, pois $\pi(x) = \bar{e}$ se, e somente se, $\bar{x} = \bar{e}$ se, e somente se, $x \in N$.

Exemplo 3.7. Sejam G um grupo e $g \in G$ fixo. A função φ_g (conjugação pelo elemento $g \in G$)

$$\begin{array}{rccc} \varphi_g: & G & \to & G \\ & x & \mapsto & g^{-1}xg \end{array}$$

é um homomorfismo. De fato, sejam $x, y \in G$. Então

$$\varphi_g(xy) = g^{-1}xyg = (g^{-1}xg)(g^{-1}yg) = \varphi_g(x)\varphi_g(y).$$

Agora, vejamos alguns exemplos envolvendo núcleo de um homomorfismo.

Exemplo 3.8. Seja $f : \mathbb{Z} \to \mathbb{C}^*$ definida por $f(m) = i^m$ para todo $m \in \mathbb{Z}$. É fato que f é um homomorfismo, pois $f(m+n) = i^{m+n} = i^m i^n = f(m)f(n)$.

Sendo $Ker(f) = \{m \in \mathbb{Z} : f(m) = 1\}$. Assim, se $m \in Ker(f)$, então $i^m = 1$ e por um simples cálculo, concluímos que o conjunto das soluções dessa equação, ou seja, o núcleo de f, é

$$Ker(f) = \{\cdots, -8, -4, 0, 4, 8, \cdots\}$$

Exemplo 3.9. Consideremos a função $f : \mathbb{C}^* \to \mathbb{R}_+^*$ definida por $f(z) = |z|$ onde $|z|$ representa o módulo de $z \in \mathbb{C}^*$. É claro que f é um homomorfismo de grupos, pois $f(z_1 z_2) = |z_1 z_2| = |z_1||z_2| = f(z_1)f(z_2)$.

Sendo $Ker(f) = \{z \in \mathbb{C}^* : f(z) = 1\}$, então para determinarmos o núcleo de f, temos que encontrar as soluções de $|z| = 1$, ou seja, o núcleo é formado por todos os números complexos de módulo igual a 1 que são exatamente os pontos de $\mathbb{R}^2$ situados na circunferência de centro na origem e raio 1.

3.2 Isomorfismo

Agora, estamos interessados nos casos em que um homomorfismo é bijetor, pois a partir desse fato, poderemos dizer, por exemplo, que dois grupos são ou não isomorfos. Um dos resultados principais envolvendo isomorfismo será visto no último capítulo desse trabalho.

Definição 3.10. *Sejam G_1 e G_2 grupos. Dizemos que G_1 e G_2 são isomorfos se existe um homomorfismo $\varphi : G_1 \to G_2$ bijetor.*

Notamos $G_1 \cong G_2$ para dizermos que os grupos G_1 e G_2 são isomorfos. No caso em que $G_1 = G_2 = G$ e $\varphi : G \to G$ é um isomorfismo, chamamos φ um automorfismo de G.

Exemplo 3.11. A identidade $I : G \to G$ é um automorfismo, pois como já vimos, a identidade é um homomorfismo e é claramente bijetora. Sendo assim, I é um automorfismo.

Exemplo 3.12. A função φ_g (conjugação pelo elemento $g \in G$) é um isomorfismo. Vimos anteriormnte que a mesma é um homomorfismo. Devemos então mostrar que φ_g é bijetora.

Mostremos que $Ker(\varphi_g) = \{e\}$. De fato, seja $a \in Ker(\varphi_g)$. Então $\varphi_g(a) = e$ e assim, $\varphi_g(a) = e = \varphi_g(e)$ e isso implica que $g^{-1}ag = g^{-1}eg = e$, donde $a = e$.

Finalmente, mostremos que φ_g é sobrejetora. Seja $y \in G$. Consideremos $x = gyg^{-1}$ que, claramente, pertence a G. Logo, $\varphi_g(x) = g^{-1}xg = g^{-1}gyg^{-1}g = y$ e isso demonstra o que queríamos.

Exemplo 3.13. Seja S_3 o grupo das permutações do conjunto $S = \{1, 2, 3\}$. Escrevemos um elemento $h \in S_3$ do seguinte modo

$$h = \begin{pmatrix} 1 & 2 & 3 \\ h(1) & h(2) & h(3) \end{pmatrix}.$$

O grupo S_3 possui os seguintes elementos

$$f_0 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix} \quad ; \quad f = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} \quad ; \quad f^2 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}$$

$$g = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} \; ; \; gf = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} \; ; \; gf^2 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}.$$

Lembramos que o grupo das simetrias do triângulo equilátero é dado por $D_3 = \{R_0, R_1, R_2, X, Y, Z\}$. Construímos um isomorfismo entre D_3 e S_3.

Suponhamos $\varphi : D_3 \to S_3$ um homomorfismo, então necessariamente, $\varphi(R_0) = f_0$ e escolhemos $\varphi(R_1) = f$. Segue portanto que, $\varphi(R_2) = \varphi(R_1^2) = \varphi(R_1 \circ R_1) = \varphi(R_1) \circ \varphi(R_1) = f \circ f = f^2$. Agora escolhendo $\varphi(X) = g$ temos $\varphi(Y) = \varphi(X \circ R_1^2) = \varphi(X) \circ \varphi(R_1^2) = gf^2$ e $\varphi(Z) = \varphi(X \circ R_1) = \varphi(X) \circ \varphi(R_1) = gf$.

Por construção $\varphi : D_3 \to S_3$ é bijetor e não é difícil ver que, assim definida, φ é um homomorfismo e portanto, um isomorfismo.

Apresentamos agora dois resultados que serão úteis como aplicação do teorema do homomorfismo, feito no próximo capítulo.

Seja G um grupo. Definimos

$$Aut(G) = \{f : G \to G : f \text{ é isomorfismo}\}.$$

Proposição 3.14. *Se G é um grupo então $(Aut(G), \circ)$ é um grupo, no qual $\circ$ é a operação composição de funções.*

Demonstração. Sabemos que a composição de homomorfismo é um homomorfismo, veja Proposição 3.2 (vi). Por outro lado, a composição de funções bijetoras é

bijetora. Logo, $f \circ g \in Aut(G)$, $\forall\, f, g \in Aut(G)$, ou seja, a operação $\circ$ é fechada. A composição de funções é associativa (fato sabido) e, além disso, a identidade em G, $I \in Aut(G)$ é o elemento neutro, pois $I \circ f = f \circ I = f$, $\forall\, f \in Aut(G)$.

Seja $f \in Aut(G)$. Mostremos que $f^{-1} \in Aut(G)$. Sabemos que f^{-1} é bijetora. Só resta ver que f^{-1} é um homomorfismo. De fato,

$$f^{-1}(xy) = f^{-1}(f(x')f(y')) = f^{-1}(f(x'y')) = (f^{-1} \circ f)(x'y') = x'y' = f^{-1}(x)f^{-1}(y)$$

em que $x = f(x')$ e $y = f(y')$ e por isso $f^{-1}(x) = x'$ e $f^{-1}(y) = y'$. Logo, $(Aut(G), \circ)$ é um grupo. □

Agora definimos

$$Inn(G) = \{\varphi_g : G \to G : \varphi_g(x) = g^{-1}xg, \forall x, g \in G\}.$$

Este é o conjunto das conjugações por todos os elementos de G. Abaixo é mostrado que $Inn(G)$ é um subgrupo e portanto, um grupo, chamado *grupo dos automorfismos internos de* G.

Proposição 3.15. *Se G é um grupo então $Inn(G) \triangleleft Aut(G)$.*

Demonstração. Primeiramente, se $g_1, g_2 \in G$, então $\varphi_{g_1} \circ \varphi_{g_2} = \varphi_{g_2 g_1}$. De fato,

$$\varphi_{g_2g_1}(x) = (g_2g_1)^{-1}x(g_2g_1) = g_1^{-1}(g_2^{-1}xg_2)g_1 = \varphi_{g_1}(g_2^{-1}xg_2) = (\varphi_{g_1} \circ \varphi_{g_2})(x)\, \forall\, x \in G.$$

Assim, $Inn(G)$ é um subconjunto fechado em relação à composição de funções. Como $I = \varphi_e \in Inn(G)$ e $(\varphi_g)^{-1} = \varphi_{g^{-1}} \in Inn(G)\, \forall g \in G$ (pois $\varphi_{g^{-1}} \circ \varphi_g = \varphi_e = I = \varphi_g \circ \varphi_{g^{-1}}$), segue imediatamente que $Inn(G)$ é um subgrupo de G.

Agora, sejam $g \in G$ e $f \in Aut(G)$. Então

$$(f^{-1} \circ \varphi_g \circ f)(x) = f^{-1}(g^{-1}f(x)g) = (f^{-1}(g))^{-1}xf^{-1}(g) = \varphi_{f^{-1}(g)}(x),\ \forall\, x \in G,$$

ou seja, $f^{-1} \circ \varphi_g \circ f = \varphi_{f^{-1}(g)} \in Inn(G)$, $\forall\, f \in Aut(G)$ e $\forall\, g \in G$. □

3.3 Teorema de Cayley

Como já vimos, a natureza dos grupos varia amplamente. Há grupos de números, grupos de permutações, grupos de matrizes, entre outros. O objetivo central desta seção é mostrar que há um certo elo entre eles, uma vez que cada grupo será isomorfo a um subgrupo do grupo das permutações desse grupo.

Definição 3.16. *Seja G um grupo. Para cada $a \in G$, a aplicação*

$$\delta_a : G \to G$$

tal que $\delta_a(x) = ax$, para qualquer $x \in G$, será chamada translação à esquerda definida por a. De maneira análoga é definida translação à direita.

No caso de G ser um grupo aditivo, a translação à esquerda definida por um elemento $a \in G$ é definida como $\delta_a(x) = a + x$.

Nas considerações a seguir, é indiferente usarmos translações à esquerda ou à direita, efetivamente as primeiras serão usadas.

Proposição 3.17. *Toda translação por elementos de um grupo G é uma bijeção, ou seja, é uma permutação dos elementos de G.*

Demonstração. Sejam $a \in G$ e δ_a uma translação de G. Suponhamos $\delta_a(x) = \delta_a(y)$. Então $ax = ay$ e portanto, $x = y$, pois $a^{-1}ax = a^{-1}ay$ e isso implica que $x = y$. Donde, δ_a é injetora. Para mostrar que é sobrejetora, dado um elemento qualquer $y \in G$, deve ser possível encontrar $x \in G$ tal que $ax = y$. Consideremos $x = a^{-1}y \in G$ e daí, $\delta_a(x) = a(a^{-1}y) = y$. Então δ_a é sobrejetora. □

Adotando a notação $T(G)$ para indicar o conjunto das translações em G e lembrando que $S(G)$ é a notação adotada para o conjunto das permutações dos elementos de G, então essa proposição nos diz que $T(G) \subseteq S(G)$.

Proposição 3.18. *Seja δ_a uma translação de um grupo G. Então são válidas as afirmações.*
(i) *A composição de translações é uma operação sobre $T(G)$.*
(ii) *A inversa da translação δ_a é a translação $\delta_{a^{-1}}$.*
(iii) *$T(G)$ é um subgrupo do grupo $S(G)$.*

Demonstração. (i) Sejam δ_a e δ_b translações de G. Então, $\forall x \in G$,

$$(\delta_a \circ \delta_b)(x) = \delta_a(\delta_b(x)) = \delta_a(bx) = a(bx) = (ab)x = \delta_{ab}(x)$$

o que mostra que $\delta_a \circ \delta_b = \delta_{ab}$.

(ii) Como δ_a é bijetora, procede falar em aplicação inversa nesse caso. O

enunciado já aponta como "candidata", a translação $\delta_{a^{-1}}$. Daqui para a frente é apenas questão de verificação. Temos

$$(\delta_a \circ \delta_{a^{-1}})(x) = \delta_a(\delta_{a^{-1}}(x)) = \delta_a(a^{-1}x) = a(a^{-1}x) = (aa^{-1})x = x = I(x),$$

então $\delta_a \circ \delta_{a^{-1}} = I$.

Da mesma forma se prova que $\delta_{a^{-1}} \circ \delta_a = I$. Portanto, $\delta_{a^{-1}}$ é a inversa de δ_a, isto é, $(\delta_a)^{-1} = \delta_{a^{-1}}$.

(iii) Sejam δ_a e $\delta_b \in T(G)$. Então

$$\delta_a \circ (\delta_b)^{-1} = \delta_a \circ (\delta_{b^{-1}}) = \delta_{ab^{-1}}.$$

Donde, $\delta_a \circ (\delta_b)^{-1} \in T(G)$ e portanto, $T(G)$ é um subgrupo de $S(G)$. □

Teorema 3.19. *(Teorema de Cayley) Se G é um grupo, então a aplicação*

$$\begin{array}{rccc} f: & G & \to & T(G) \\ & a & \mapsto & \delta_a \end{array}$$

é um isomorfismo de grupos.

Demonstração. Sejam $a, b \in G$ tais que $f(a) = f(b)$. Então $\delta_a = \delta_b$ e portanto, $\delta_a(x) = \delta_b(x)$, para todo $x \in G$. Temos que $ax = bx$, $\forall x \in G$. Em particular, para $x = e$, segue que $ae = be$, ou seja, $a = b$. Logo, que f é injetora.

Seja $\psi \in T(G)$. Então $\psi(x) = ax$ para todo $x \in G$ e para $a \in G$ fixo (definição de translação). Assim, $f(a) = \delta_a$ e para todo $x \in G$, temos que $\delta_a(x) = ax = \psi(x)$ e daí, $\psi = \delta_a$. Portanto, f é sobrejetora.

Para quaisquer $a, b \in G$,

$$f(ab) = \delta_{ab} = \delta_a \circ \delta_b = f(a) \circ f(b)$$

e portanto, f é um homomorfismo de grupos. □

O teorema de Cayley mostra que efetivamente todo grupo G é isomorfo ao subgrupo $T(G)$ do grupo das permutações dos elementos de G.

Exemplo 3.20. Consideremos o grupo aditivo $\mathbb{Z}_3$ das classes de resto módulo 3. Para facilitar a notação, não colocamos os traços sobre os elementos de $\mathbb{Z}_3$. Portanto, $\mathbb{Z}_3 = \{0, 1, 2\}$ e a operação considerada é claramente a adição módulo 3. A tábua do grupo, sem os traços, fica assim

$+$	0	1	2
0	0	1	2
1	1	2	0
2	2	0	1

Assim, a translação à esquerda definida por a, ou seja, a aplicação δ_a que associa a cada x do grupo o elemento $a + x$, será denotada por

$$\delta_a = \begin{pmatrix} 0 & 1 & 2 \\ a+0 & a+1 & a+2 \end{pmatrix}.$$

Portanto, as translações são

$$\delta_0 = \begin{pmatrix} 0 & 1 & 2 \\ 0 & 1 & 2 \end{pmatrix}$$

$$\delta_1 = \begin{pmatrix} 0 & 1 & 2 \\ 1 & 2 & 0 \end{pmatrix}$$

$$\delta_2 = \begin{pmatrix} 0 & 1 & 2 \\ 2 & 0 & 1 \end{pmatrix}.$$

Pelo teorema de Cayley, $T(\mathbb{Z}_3) = \{\delta_0, \delta_1, \delta_2\}$ é isomorfo ao grupo $\mathbb{Z}_3$. De fato $\delta_1^2 = \delta_2$, $\delta_2^2 = \delta_1$ e $\delta_1\delta_2 = \delta_0$.

Capítulo 4

Teorema do homomorfismo e suas aplicações

Agora, demonstramos um dos principais teoremas básicos da teoria de grupos que possui diversas aplicações tanto na álgebra como em outras áreas da matemática.

4.1 Teorema do homomorfismo

Teorema 4.1. *Sejam G_1 e G_2 grupos e $\varphi : G_1 \to G_2$ um homomorfismo de grupos. Então $G_1/Ker(\varphi) \cong Im(\varphi)$.*

Demonstração. Definimos

$$\begin{array}{rccc} \overline{\varphi}: & G_1/Ker(\varphi) & \longrightarrow & Im(\varphi) \\ & \overline{g} & \longmapsto & \overline{\varphi}(\overline{g}) = \varphi(g). \end{array}$$

Mostremos que $\overline{\varphi}$ está bem definida, ou seja, suponhamos que $\overline{g} = \overline{g'}$. Então $gg^{'-1} \in Ker(\varphi)$ e daí, $\varphi(gg^{'-1}) = e_2$. Logo, $\varphi(g)\varphi(g^{'-1}) = e_2$ e isso nos diz que $\varphi(g)\varphi(g^{'})^{-1} = e_2 \Leftrightarrow \varphi(g) = \varphi(g^{'}) \Leftrightarrow \overline{\varphi}(\overline{g}) = \overline{\varphi}(\overline{g^{'}})$.

Também, $\overline{\varphi}$ é um homomorfismo de grupos. De fato, $\overline{\varphi}(\overline{g}\overline{g^{'}}) = \overline{\varphi}(\overline{gg^{'}}) = \varphi(gg^{'}) \overset{(*)}{=} \varphi(g)\varphi(g^{'}) = \overline{\varphi}(\overline{g})\overline{\varphi}(\overline{g^{'}})$, a igualdade $(*)$ ocorre, pois φ é um homomorfismo de grupos.

Agora, para encerrar a demonstração devemos mostrar que $\overline{\varphi}$ é bijetora.

Temos $Im(\overline{\varphi}) = \{\overline{\varphi}(\overline{g}) : \overline{g} \in G_1/Ker(\varphi)\} = \{\varphi(g) : g \in G_1\} = Im(\varphi)$, ou seja, $\overline{\varphi}$ é sobrejetora.

Finalmente, mostremos que $\overline{\varphi}$ é injetora. Suponhamos que $\overline{\varphi}(\overline{g}) = e_2$ e portanto, $\varphi(g) = e_2$. Logo, $g \in Ker(\varphi)$ e isso nos diz que $\overline{g} = \overline{e_1}$ e assim, $\overline{\varphi}$ é injetora. □

4.2 Aplicações do teorema do homomorfismo

Apresentamos nessa seção algumas aplicações importantes que, na verdade, são corolários do teorema acima. As mesmas são bastante usadas na teoria geral de grupos.

Corolário 4.2. *Sejam G_1 e G_2 grupos finitos e $\psi : G_1 \to G_2$ um homomorfismo de grupos. Então*
(i) *$|Im(\psi)|$ é um divisor de $|G_1|$;*
(ii) *Se G_1 é um p-grupo então $\psi(G_1) = Im(\psi)$ é também um p-grupo.*

Demonstração. (i) Pelo teorema do homomorfismo, $G_1/Ker(\psi)$ é isomorfo à $Im(\psi)$. Como G_1 é finito, segue que $G_1/Ker(\psi)$ também o é, e portanto, $Im(\psi)$ é um subgrupo finito de G_2. Pelo teorema de Lagrange, $|G_1| = |Ker(\psi)||G_1/Ker(\psi)| = |Ker(\psi)||Im(\psi)|$ e isso implica que $|Im(\psi)|$ divide $|G_1|$.

(ii) Se G é um p-grupo, isto é, $|G|$ é uma potência do primo p, e como $|Im(\psi)|$ é um divisor de $|G| = p^m$, $m > 1$, segue imediatamente que, $|Im(\psi)| = p^s$, $s \leq m$, por causa do Teorema Fundamental da Aritmética. □

Corolário 4.3. *Sejam G um grupo e $Z(G)$ o centro do grupo G. Então $Inn(G) \cong G/Z(G)$.*

Demonstração. Definimos

$$\begin{array}{rccc} \varphi: & G & \to & Inn(G) \\ & g & \mapsto & \varphi(g) = \varphi_{g^{-1}}. \end{array}$$

Temos que φ é um homomorfismo, pois para quaisquer $g, h \in G$, segue que $\varphi(gh) = \varphi_{(gh)^{-1}}$. Para todo $x \in G$, vem que

$$\begin{array}{rcl} \varphi(gh)(x) & = & \varphi_{(gh)^{-1}}(x) = ((gh)^{-1})^{-1}x(gh)^{-1} = g(hxh^{-1})g^{-1} \\ & = & g((h^{-1})^{-1}xh^{-1})g^{-1} = (g^{-1})^{-1}(\varphi_{h^{-1}}(x))g = \varphi_{g^{-1}}((\varphi_{h^{-1}})(x)) \\ & = & (\varphi_{g^{-1}} \circ \varphi_{h^{-1}})(x) = (\varphi(g) \circ \varphi(h))(x). \end{array}$$

Assim, $\varphi(gh) = \varphi(g) \circ \varphi(h)$, $\forall\, g, h \in G$.

Temos que $Im(\varphi) = \{\varphi(g) : g \in G\} = \{\varphi_{g^{-1}} : g \in G\} = Inn(G)$ e φ é sobrejetora.

Para finalizar a demonstração, devemos mostrar que $Ker(\varphi) = Z(G)$. Temos que

$$Ker(\varphi) = \{g \in G : \varphi(g) = I\} = \{g \in G : \varphi_{g^{-1}} = I\},$$

ou seja, para todo $x \in G$, $\varphi_{g^{-1}}(x) = I(x) = x \Leftrightarrow (g^{-1})^{-1}xg^{-1} = x \Leftrightarrow gxg^{-1} = x \Leftrightarrow gx = xg$, e isso nos diz que $g \in Ker(\varphi) \Leftrightarrow g \in Z(G)$. Assim, $Ker(\varphi) = Z(G)$ e, pelo teorema do homomorfismo, $Inn(G) \cong G/Z(G)$. □

Conclusão

Esse trabalho possibilitou o conhecimento sobre assuntos que infelizmente não vi em minha graduação. Sou aluno do currículo antigo e ele não contempla a disciplina de Álgebra II, disciplina essa que tem em sua ementa o conteúdo abordado nesse trabalho. Por esse motivo e por ter sido muito interessante minhas aulas na disciplina de Álgebra I, escolhi como tema deste trabalho a teoria de grupos.

Através desse trabalho pude ver que os grupos possuem estruturas extraordinárias com uma infinidade de utilidades nos mais variados ramos da matemática. Ainda vi que a disciplina de Álgebra pode ser mais explorada no curso de licenciatura para que possamos ter contato com assuntos mais sofisticados que enriquecem nossa formação.

Considero esse projeto a atividade mais importante que realizei durante o curso, pois pude estudar durante um ano um único tema e aprofundá-lo o tanto quanto foi possível nesse período. Percebo ao terminar tal trabalho, que ainda há muito a ser estudado sobre grupos, suas propriedades e aplicações e, por isso, convido a quem ler o mesmo a continuar a pesquisar sobre o assunto.

Finalmente, espero que esse possa ser útil a outras pessoas como um material de estudo e/ou consulta.

Referências Bibliográficas

[1] Gonçalves, A., *Introdução à Álgebra*, Projeto Euclides, IMPA, Rio de Janeiro (2001).

[2] Lequain, Y. e Garcia, A., *Elementos de Álgebra*, Projeto Euclides, IMPA, Rio de Janeiro (2003).

[3] Domingues, H. H. e Iezzi, G., *Álgebra Moderna*, volume único, 4ª edição reformada, São Paulo (2003).