Grupos Solúveis e Nilpotentes: Uma Introdução

Textuniversitários 6

César Polcino Milies

Grupos Solúveis e Nilpotentes: *Uma Introdução*

Editora Livraria da Física
São Paulo – 2020

1a. Edição

Editor: José Roberto Marinho
Projeto gráfico e diagramação: Thiago Augusto Silva Dourado
Capa: Fabrício Ribeiro

Texto em conformidade com as novas regras ortográficas do Acordo da Língua Portuguesa.

Dados Internacionais de Catalogação na Publicação (CIP)
(Câmara Brasileira do Livro, SP, Brasil)

Milies, César Polcino

Grupos solúveis e nilpotentes : uma introdução / César Polcino Milies. – São Paulo : Editora Livraria da Física, 2020. – (Série textuniversitários ; 6)

Bibliografia.
ISBN 978-85-7861-647-2

1. Matemática 2. Matemática - Filosofia I. Título. II. Série.

20-32848 CDD-510.1

Índices para catálogo sistemático:

1. Matemática : Filosofia 510.1

Iolanda Rodrigues Biode - Bibliotecária - CRB-8/10014

ISBN 978-85-7861-647-2

Impresso no Brasil
Printed in Brazil

LF EDITORIAL
Editora Livraria da Física
Tel./Fax: +55 11 3459-4327 / 3936-3413
www.livrariadafisica.com.br

Prefácio

Este livro tem por base notas que elaboramos inicialmante para um minicurso ministrado na I Bienal da Sociedade Brasileira de Matemática em 2002, em Belo Horizonte e que foram publicadas depois na revista *Matemática Universitária* [28]. Nosso objetivo era então o de iniciar alunos de final da graduação ou início do mestrado no estudo dos grupos nilpotentes. Trata-se de um assunto belíssimo que normalmente não é tratado neste nível.

Agora ampliamos consideravelmente o texto, adicionando material que nos pareceu relevante sobre grupos solúveis e tratando de mais alguns tópicos relacionados aos grupos nilpotentes. Os assuntos expostos nesta versão certamente não poderiam ser tratados num minicurso de apenas uma semana. Mesmo assim, é um texto relativamente breve no qual apenas "arranhamos a superfície" de um assunto deveras apaixonante.

No primeiro capítulo tratamos brevemente de tópicos que podem ser considerados pré-requisitos para os capítulos seguintes e que normalmente são incluídos em cursos básicos de álgebra. Por esse motivo a maioria dos resultados são enunciados sem demonstração, embora tenhamos tratado com mais cuidado dos aspectos mais relevantes. Em particular, o capítulo termina com uma exposição

do Teorema de Sylow que, este sim, é demonstrado cuidadosamente. A importância deste tópico será claramente aparente nos capítulos subsequentes onde eles reaparecem, com diferentes graus de generalidade, dependendo da classe de grupos estudada.

O segundo capítulo é dedicado aos grupos solúveis. Após apresentarmos resultados básicos sobre comutadores e os teoremas clássicos sobre esta família de grupos que normalmente constam de textos gerais de álgebra ou de Teoria de Galois, provamos que certos grupos, com uma dada ordem, são solúveis. Fazemos isto como motivação para mencionar o teorema $p^a q^b$ de Burnside e o Teorema de Feit-Thompson, que enunciamos sem demonstração. Na seção seguinte mencionamos ainda outro resultado importante, o Teorema de Schur-Zassenhaus, cuja demonstração também omitimos, mas que é natural o suficiente como para ser aceito pelo leitor — que seguramente irá estuda-lo detidamente se prosseguir seus estudos nesta direção. Na seção seguinte utilizamos este teorema para provar o Teorema de Philip Hall, uma extensão notável do Teorema de Sylow para o caso dos grupos solúveis finitos.

Finalmente, no terceiro capítulo tratamos dos grupos nipotentes. Na primeira seção apresentamos os resultados gerais sobre nilpotência; na seção seguinte tratamos dos grupos nipotentes finitos e de sua estrutura como produto direto dos seus subgrupos de Sylow. Logo a seguir estudamos uma classe de grupos muito particular; os grupos Hamiltonianos, *i.e.* os grupos não comutativos em que todo subgrupo é normal. Finalmente consideramos os grupos nilpotentes infinitos e concluímos nosso estudo com uma breve seção sobre o Número de Hirsch.

O texto contém muitas notas históricas, não como apêndices de capítulos mas como parte integrante do texto. Isto nos parece de suma importância. Achamos que conhecer por exemplo as circunstâncias em que um determinado conceito foi introduzido é essencial para a boa formação do leitor.

Agradecemos muito especialmente a nosso aluno, orientando e amigo Thiago Silva Dourado, que muito insistiu para que retomássemos as notas sobre grupos nilpotentes e as transformássemos num livro introdutório. Além disso, sua colaboração foi fundamental para a edição e formatação do texto original.

Sumário

1

Preliminares

1.1 Conceitos Básicos

Neste capítulo vamos tratar de algumas definições e resultados básicos da Teoria de Grupos, o assunto central deste livro, com o intuito de fixar notações e explicitar resultados que serão necessários adiante. A maioria das provas serão omitidas porque imaginamos o leitor com experiência suficiente. Incluiremos uma ou outra demonstração, aqui e ali, para não tornar o capítulo apenas uma enfadonha lista de resultados

Definição 1.1.1 Um *grupo* é um conjunto não vazio G com uma operação binária (que denotamos por $\cdot$) tal que, para todos $a, b, c \in G$, valem as seguintes propriedades:

(i) $(ab)\,c = a\,(bc)$.

(ii) Existe um elemento, que denotaremos por $1 \in R$, tal que $a1 = 1a = a$, para todo $a \in G$.

(iii) Para cada elemento $a \in G$ existe um elemento, que denotaremos por $a^{-1} \in G$, tal que $aa^{-1} = a^{-1}a = 1$.

Se, além disso, vale a seguinte propriedade:

$$ab = ba,$$

então diz-se que o grupo é *abeliano* ou *comutativo*.

Se o conjunto G é finito, então o número de of elementos de G diz-se a *ordem* de G e será denotado por $|G|$.

Os grupos formam uma importante categoria de objetos matemáticos e existem muitíssimos exemplos que provavelmente são familiares ao leitor. Como ilustração listamos alguns a seguir.

Exemplo 1.1.2 O conjunto $\mathbb{Z}$ dos números inteiros; o conjunto $\mathbb{Q}$ dos números racionais, o conjunto $\mathbb{R}$ dos números reais e o conjunto $\mathbb{C}$ dos números complexos, com a operação de soma, são exemplos de grupos e todos eles são abelianos.

Ainda, se denotamos por $\mathbb{Q}^*$, $\mathbb{R}^*$ e $\mathbb{C}^*$ os conjuntos obtidos dos anteriores *excluindo o elemento* 0, então estes conjuntos, com a operação de multiplicação usual em cada um deles, também são exemplos de grupos abelianos.

O conjunto $\mathbb{Z}^*$ dos números inteiros sem o 0, não é um grupo com a multiplicação pois nenhum inteiro, com exceção 1 e -1, tem inverso multiplicativo.

O conjunto $\mathbb{Z}_m = \left\{\overline{0}, \overline{1}, \ldots, \overline{m-1}\right\}$ dos inteiros módulo m, com a soma definida por $\overline{a+b} = \overline{a} + \overline{b}$ é um grupo abeliano. Ainda, definindo a multiplicação por $\overline{ab} = \overline{a}\overline{b}$ segue que $\mathbb{Z}_m^*$ é um grupo com a multiplicação se e somente se o módulo m é primo (veja o Exercício 3).

Exemplo 1.1.3 Seja K um corpo. Então o conjunto $\mathrm{GL}(n, K)$ de todas as matrizes $n \times n$ inversíveis com coeficientes em K, com a multiplicação usual de matrizes, é um grupo, que não é comutativo se $n > 1$. Este grupo chama-se *grupo linear das matrizes* $n \times n$ *sobre* K.

Exemplo 1.1.4 (Produto Direto Externo) Sejam $G_1, G_2, \ldots G_n$ grupos. Consideramos o conjunto:

$$G_1 \dot{\times} G_2 \dot{\times} \cdots \dot{\times} G_n = \{(a_1, a_2, \ldots, a_n) \mid a_i \in R_i, 1 \leq i \leq n\},$$

com multiplicação definida componente a componente:

$$(a_1, a_2, \ldots, a_n)(b_1, b_2, \ldots, b_n) = (a_1 b_1, a_2 b_2, \ldots, a_n b_n).$$

Este conjunto, com a operação acima, é um grupo chamado o *produto direto (externo)* dos grupos $G_1, G_2, \ldots G_n$. O produto direto é abeliano se e somente se cada fator direto G_i, $1 \leq i \leq n$, é abeliano.

Nosso próximo exemplo é de particular interesse. Historicamente este foi o primeiro exemplo de grupo a ser descoberto, por causa de suas aplicações na teoria das equações algébricas.

Exemplo 1.1.5 (Grupo Simétrico) Seja M um conjunto finito. Lembramos que uma função bijetora de M em si mesmo chama-se uma *permutação* de M. Claramente, a função identidade é uma permutação e tanto a composição de permutações quanto a inversa de uma permutação são permutações.

Logo, segue facilmente que o conjunto de todas as permutações de um conjunto M é um grupo em relação à operação de composição de funções. Ele é denotado usualmente por S_M e é chamado o *grupo simétrico de* M.

Se $M = \{1, 2, \ldots, n\}$ então S_M chama-se o *grupo simétrico de grau* n e é denotado por S_n. Dado um elemento $\psi \in S_n$, se denotamos $i_k = \psi(k)$, $1 \leq k \leq n$, podemos representar ψ na forma:

$$\psi = \begin{pmatrix} 1 & 2 & 3 & \cdots & n \\ i_1 & i_2 & i_3 & \cdots & i_n \end{pmatrix},$$

uma notação introduzida por A.L. Cauchy em 1845 [5, vol. 1, pp. 64-90]. Usando esta notação, podemos representar o inverso de ψ como

$$\psi^{-1} = \begin{pmatrix} i_1 & i_2 & i_3 & \cdots & i_n \\ 1 & 2 & 3 & \cdots & n \end{pmatrix}.$$

Dado, por exemplo,

$$\phi = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 5 & 2 & 4 & 1 \end{pmatrix} \quad \text{e} \quad \psi = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 1 & 4 & 5 & 3 \end{pmatrix},$$

temos que $\phi\,\psi\,(1) = \phi\,(2) = 5$. Computando as imagens dos outros números de maneira similar obtemos:

$$\phi\,\psi = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 5 & 3 & 4 & 1 & 2 \end{pmatrix}.$$

Também podemos computar, da mesma forma:

$$\psi\,\phi = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 4 & 3 & 1 & 5 & 2 \end{pmatrix}.$$

Este cálculo simples mostra que, em geral, os grupos simétricos não são comutativos.

Dada uma permutação $\psi \in S_n$, e um inteiro positivo k, $1 \leq k \leq n$, diz-se que ψ *move* k se $\psi\,(k) \neq k$ e, em caso contrário, diz-se que ψ *fixa* k.

A ordem do grupo simétrico de grau n é $n!$. De fato, um elemento de S_n estará determinado ao especificar as imagens de cada elemento do conjunto $1, 2, \ldots, n$ in M. Então, para contar os elementos de S_n será suficiente contar o número de escolhas possíveis para as imagens. Como a imagem de 1 pode ser qualquer um dos elementos de M, temos exatamente n escolhas possíveis para esta imagem. Uma vez que a imagem de 1 foi escolhida, para a imagem de 2 podemos escolher qualquer um dos elementos restantes de M, donde temos $n-1$ escolhas possíveis. Da mesma forma, vamos ter $n-2$ imagens possíveis para 3 e assim por diante. Segue que existem $n\,(n-1)\,(n-2)\cdots 2\cdot 1 = n!$ permutações diferentes de M. Naturalmente, esta demonstração não é muito rigorosa, mas pode ser facilmente formalizada usando indução.

Definição 1.1.6 Um conjunto não vazio H de um grupo G diz-se um *subgrupo* de G se é fechado sob a operação de G (*i.e.* para cada par de elementos $a, b \in H$, tem-se que $ab \in H$) e H, com a restrição da operação de G é, ele próprio, um grupo.

Há muitos exemplos familiares de subgrupos; por exemplo, $\mathbb{Q}^*$ é um subgrupo de $\mathbb{R}^*$ que, por sua vez, é um subgrupo de $\mathbb{C}^*$.

Para qualquer grupo multiplicativo G os subconjuntos $\{1\}$ e G são subgrupos de G chamados os subgrupos *triviais* de G.

Exemplo 1.1.7 (Subgrupos Cíclicos) Seja a um elemento de um grupo G. Dado um inteiro n definimos as *potências* de a por:

$$a^n = \begin{cases} \underbrace{aa\cdots a}_{n \text{ vezes}} & \text{se} \quad n > 0, \\ \underbrace{a^{-1}a^{-1}\cdots a^{-1}}_{|n| \text{ vezes}} & \text{se} \quad n < 0, \\ 1 & \text{se} \quad n = 0. \end{cases}$$

Como é fácil verificar que $a^m a^n = a^{m+n}$, segue imediatamente que o conjunto

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

é um subgrupo de G, que é chamado o *subgrupo cíclico de G gerado por a*.

Se este subgrupo é finito, então devem existir inteiros n e m tais que $a^n = a^m$. Então $a^{n-m} = a^{m-n} = 1$. O menor inteiro positivo n tal que $a^n = 1$ chama-se a *ordem de* a e será denotado por $o(a)$. Se $\langle a \rangle$ é infinito, diz-se que a é um elemento de *ordem infinita*.

Se existe um elemento a em G tal que $G = \langle a \rangle$, diz-se que G é um *grupo cíclico* e que a é um *gerador* de G. Note que $o(a) = |\langle a \rangle|$.

Exemplo 1.1.8 (Subgrupos Gerados por um Conjunto) Seja X um subconjunto não vazio de um grupo G. Define-se o *subgrupo gerado por* X como a interseção de todos os subgrupos de G que contém X. Note que esta família de subgrupos é não vazia, já que pelo menos o próprio G pertence a ela, e que a interseção desta família é, de fato, um subgrupo que contém X (veja o Exercício 8). Este subgrupo será denotado por $\langle X \rangle$.

Deixamos como exercício para o leitor a tarefa de provar que

$$\langle X \rangle = \{x_1^{\varepsilon_1} \cdots x_k^{\varepsilon_k} \mid x_i \in X,\, \varepsilon_i = \pm 1,\, k \geq 1\} \cup \{1\}\,.$$

Se $\langle X \rangle = G$, então diz-se que X é um *conjunto de geradores* de G. Se X é finito, então diz-se que G é um grupo *finitamente gerado*.

Para dar outros exemplos, introduzimos mais alguns grupos.

Definição 1.1.9 Dado um corpo K, definimos:

(i) $\mathrm{SL}(n, K) = \{A \in \mathrm{GL}(n, K) \mid \det(A) = 1\}$, o *grupo linear especial de grau* n *sobre* K.

(ii) $\mathrm{T}(n, K) = \{A = (a_{ij}) \in \mathrm{GL}(n, K) \mid a_{ij} = 0 \text{ se } i > j\}$, o *grupo triangular superior de grau* n *sobre* K.

(iii) $\mathrm{UT}(n, K) = \{A = (a_{ij}) \in \mathrm{T}(n, K) \mid a_{ii} = 1\}$, o *grupo unitriangular superior de grau* n *sobre* K.

Então, é claro que $\mathrm{SL}(n, K)$, $\mathrm{T}(n, K)$ e $\mathrm{UT}(n, K)$ são todos subgrupos de $\mathrm{GL}(n, K)$ e que $\mathrm{UT}(n, K)$ é um subgrupo de $\mathrm{SL}(n, K)$.

A seguinte caracterização dos subgrupos é direta.

Lema 1.1.10 *Um conjunto não vazio H de um grupo G é um subgrupo de G se, e somente se, para todo par de elementos $x, y \in H$ temos que $x^{-1}y \in H$.*

Definição 1.1.11 O *centro* de um grupo G é o subgrupo:

$$\mathcal{Z}(G) = \{a \in G \mid ax = xa, \forall x \in G\}.$$

Dado um subgrupo H de um grupo G, podemos usá-lo para definir uma *partição* de G; *i.e.* um cobertura de G por subconjuntos disjuntos.

Definição 1.1.12 Seja H um subgrupo de um grupo G. Dado um elemento $a \in G$, os subconjuntos da forma:

$$aH = \{ah \mid h \in H\},$$
$$Ha = \{ha \mid h \in H\},$$

chamam-se as *classes laterais à esquerda* e *à direita de* H, determinadas por a respectivamente.

As classes laterais tem algumas propriedades elementares, que damos em continuação.

Proposição 1.1.13 *Seja H um subgrupo de um grupo G e sejam a e b elementos arbitrários de G. Tem-se que:*

(i) Se $b \in aH$, então $bH = aH$.

(ii) Se $b \notin aH$, então $aH \cap bH = \emptyset$.

Demonstração: Suponha inicialmente que $b \in aH$. Então, existe um elemento $h_0 \in H$ tal que $b = ah_0$. Dado um elemento arbitrário $bh \in bH$ temos que $bh = ah_0h \in aH$. Isto mostra que $bH \subset aH$. Como também podemos escrever que $a = bh_0^{-1}$ um argumento similar mostra que a inclusão oposta também vale, provando a igualdade.

Finalmente, suponha que existe um elemento $c \in aH \cap bH$. Por *(i)*, temos que $cH = aH$ e também $cH = bH$, donde $aH = bH$, o que prova *(ii)*. □

Corolário 1.1.14 *Seja H um subgrupo de um grupo G. Dados elementos $a, b \in G$, tem-se que $b \in aH$ se e somente se $aH = bH$.*

Cada elemento de uma classe lateral diz-se um *representante* da classe. Um conjunto completo de representantes das classes laterais à esquerda (ou à direita) chama-se um *transversal* à esquerda (ou à direita) de H em G.

Note que a função definida para todos os elementos $h \in H$ por $h \mapsto ah$ é uma bijeção de H sobre aH donde, se H é finito aH também é e ambos conjuntos têm o mesmo número de elementos.

Claramente, uma afirmação análoga vale para classes laterais à direita.

Ainda, a função $aH \mapsto Ha^{-1}$ é uma bijeção do conjunto das classes laterais à esquerda de G determinadas por H sobre o conjunto das classes laterais à direita. Logo, se o número de classes laterais à esquerda determinadas por H é finito, o número de classes laterais à direita também é e ambos coincidem.

Definição 1.1.15 Seja H um subgrupo de um grupo G. Se o número de classes laterais à esquerda (ou à direita) de H em G é finito, então este número diz-se o *índice* de H em G e se denota por $[G : H]$.

Teorema 1.1.16 (Lagrange) *Seja H um subgrupo de um grupo finito G. Então, a ordem de H divide a ordem de G; mais precisamente, temos que*

$$|G| = [G : H]\,|H|\,.$$

Demonstração: Seja $k = [G : H]$. Note que a Proposição 1.1.13 acima mostra que se escolhemos um elemento a_i, $1 \leq i \leq k$, em cada uma das classes laterais determinadas por H, então podemos escrever G como uma união disjunta de classes laterais diferentes:

$$G = a_1H \sqcup a_2H \sqcup \cdots \sqcup a_kH.$$

Como $|a_iH| = |H|$, temos que $|G| = k\,|H| = [G:H]\,|H|$, como afirmado. □

Como consequência imediata temos o seguinte.

Corolário 1.1.17 *Seja a um elemento de um grupo finito G. Então $o(a)$ é um divisor de $|G|$.*

A classe dos subgrupos cujas classes laterais à esquerda e à direita coincidem é particularmente importante. Note que, para um elemento a e um subgrupo H de um grupo G, temos que $aH = Ha$ se e somente se $a^{-1}Ha = H$. Isto sugere a seguinte.

Definição 1.1.18 Seja H um subgrupo de um grupo G. Diz-se que H é *normal* em G, e escrevemos $H \lhd G$, se $a^{-1}Ha = H$ para todo $a \in G$.

Se $a^{-1}Ha \subset H$ *para todo* $a \in G$ então também o $H \subset aHa^{-1}$ para todo $a \in G$. Logo, para verificar que um subgrupo H é normal num grupo G, é suficiente verificar apenas que uma das inclusões vale, para cada elemento $a \in G$.

1.2 Homomorfismos e Grupos Quociente

Definição 1.2.1 Sejam G_1 e G_2 grupos. Uma função $f : G_1 \to G_2$ diz-se um *homomorfismo* se para todos $g, h \in G$ tem-se que

$$f(gh) = f(g)\,f(h).$$

Claramente, a função $f : G_1 \to G_2$ dada por $f(g) = 1$ para todo $g \in G$, é sempre um homomorfismo, chamado o *homomorfismo trivial*.

O leitor pode verificar facilmente que se $f : G_1 \to G_2$ é um homomorfismo, então $f(1) = 1$ e $f(g^{-1}) = f(g)^{-1}$ para todo $g \in G$.

Definição 1.2.2 Seja $f : G_1 \to G_2$ um homomorfismo. Então a *imagem* de f é o conjunto

$$\mathrm{Im}\,(f) = \{y \in G_2 \mid \text{existe } x \in G_1 \text{ com } f(x) = y\}.$$

O *núcleo* ou *kernel* de f é o conjunto

$$\mathrm{Ker}\,(f) = \{x \in G_1 \mid f(x) = 1\}.$$

É fácil verificar diretamente que $\mathrm{Im}\,(f)$ é um subgrupo de G_2 enquanto que $\mathrm{Ker}\,(f)$ é um subgrupo normal de G_1.

Definição 1.2.3 Um homomorfismo $f : G_1 \to G_2$ diz-se um *epimorfismo* se é sobrejetor; *i.e.*, se $\mathrm{Im}\,(f) = G_2$ e diz-se um *monomorfismo* se é injetor; *i.e.*, se $f(x) = f(y)$ implica $x = y$, para $x, y \in G_1$ ou, equivalentemente, se $\mathrm{Ker}\,(f) = \{1\}$ *(prove!)*. Finalmente, f diz-se um *isomorfismo* se é sobrejetor e também injetor.

Definição 1.2.4 Dados dois grupos G_1 e G_2, se existe um isomorfismo $f : G_1 \to G_2$ diz-se que G_1 e G_2 são *isomorfos*, o que é denotado por $G_1 \cong G_2$.

Definição 1.2.5 Um homomorfismo de G em si mesmo diz-se um *endomorfismo* e, se é um isomorfismo, então é chamado de *automorfismo* de G.

Exemplo 1.2.6 Seja a um elemento fixado de um grupo G. Definimos uma função $\sigma_a : G \to G$ por $\sigma_a(x) = a^{-1}xa$, para todo $x \in G$. Um elemento da forma $a^{-1}xa$ chama-se um *conjugado* de x por a e é frequentemente denotado abreviadamente na forma x^a. Note que

$$\begin{aligned}\sigma_a(xy) &= a^{-1}(xy)\,a = a^{-1}x\left(aa^{-1}\right)ya \\ &= \left(a^{-1}xa\right)\left(a^{-1}ya\right) = \sigma_a(x)\,\sigma_a(y).\end{aligned}$$