MATEMÁTICA UNIVERSITÁRIA
nº34 – junho 2003 – pp. 55–100

Grupos Nilpotentes:
Uma Introdução

C. Polcino Milies

1 Introdução

Os grupos nilpotentes constituem uma família muito importante de grupos e seu estudo nos pareceu particularmente adequado para um curso com o espírito proposto para a primeira Bienal de Matemática da SBM.

Além de se tratar de um tópico que não é usualmente aprofundado nos cursos regulares de graduação ou de pós-graduação, ele tem a vantagem de que é possível exibir belos teoremas de estrutura para os grupos nilpotentes finitos e finitamente gerados. Ainda, como estes grupos estão, de alguma forma, próximos dos grupos abelianos, isto nos dá a oportunidade de comparar os resultados, ver o que se mantém e o que se perde de informação sobre estrutura, quando passamos dos grupos abelianos aos nilpotentes.

As notas que aqui apresentamos são apenas uma introdução a este assunto fascinante. Mesmo assim, acreditamos ter coberto, da forma mais clara e didática que nos foi possível, uma série de temas nem sempre explícitos nos textos clássicos.

Há na literatura excelentes livros básicos sobre teoria de grupos, como os de M. Hall [7], J.J. Rotman [19], W.R. Scott [20] e D.J.S. Robinson [18]. Nós tomamos como base para o desenvolvimento destas notas a seção 1.5 de um texto que escrevemos (como pré-requisito para

assuntos mais avançados) em co-autoria com o Prof. S.K. Sehgal [16] e utilizamos, como referência complementar, o texto clássico de P. Hall [10].

Como sempre acreditamos que é muito importante para o futuro pesquisador compreender os processos que levaram à introdução de determinados conceitos ou à demonstração de certos teoremas, procuramos sempre que possível, incluir notas históricas ao longo do texto. Para isso usamos como referência um artigo de G.A. Miller [15] e o livro de B. Chandler e W. Magnus [3].

Nos dois capítulos iniciais fazemos uma breve resenha de resultados que serão úteis para o desenvolvimento do assunto. No primeiro capítulo demonstramos os teoremas de Sylow e enunciamos, sem demonstração, vários resultados importante sobre a estrutura dos grupos abelianos finitamente gerados. No segundo, tratamos dos grupos solúveis e do calculo de comutadores, que preparam o leitor para o capítulo final, onde tratamos do assunto central destas notas.

Na primeira seção do Capítulo III introduzimos as propriedades fundamentais da nilpotência e alguns exemplos particularmente interessantes. Na segunda seção descrevemos a estrutura dos grupos nilpotentes finitos e na seção final estudamos alguns resultados, talvez menos conhecidos, sobre a estrutura de grupos nilpotentes infinitos.

2 Preliminares

Neste capítulo vamos lembrar alguns resultados fundamentais da teoria dos grupos que serão mecionados mais adiante. Devido às obvias limitações de tempo e espaço, alguns destes serão enunciados sem demonstração. Apenas aqueles essenciais para o desenvolvimento do assuto central destas notas serão demonstrados cuidadosamente.

Na primeira seção tratamos dos teoremas de Sylow, que são de referência constante em qualquer curso sobre Teoria dos Grupos e na seção seguinte discutimos brevemente os teoremas de estrutura para grupos abelianos finitamente gerados. Uma das preocupações constantes na álgebra é obter, precisamente, teoremas de estrutura; isto é, descrever

como determinados objetos de estudo podem ser construídos a partir dos objetos mais simples da mesma categoria. No caso dos grupos abelianos finitamente gerados, isto pode ser feito de uma forma particularmente satisfatória. Incluimos aqui estes resultados para servirem de comparação com teoremas similares que iremos obter para os grupos nilpotentes e que são o principal objetivo do texto.

2.1 Ações, p-grupos e subgrupos de Sylow

O primeiro teorema da teoria abstrata dos grupos é devido a Arthur Cayley [2] e estabelece que todo grupo é isomorfo a um grupo de permutações [1]. Para demonstrar este teorema, se associa, a cada elemento a de um grupo G, a permutação $f_a \in S_G$ definida por $f_a(g) = ag$ para todo $g \in G$ e logo se prova que a aplicação $a \mapsto f_a$ é um monomorfismo de G no grupo das permutações $S_G = \{f : G \to G \mid f \text{ é uma bijeção}\}$.

Esta idéia pode ser formulada de uma forma mais geral.

Definição 2.1 *Sejam G um grupo e M um conjunto. Diz-se que G* **age em** *M* **via** *ϕ se existe um homomorfismo $\phi : G \to S_M$.*

Na demonstração do Teorema de Cayley descrita acima, está se utilizando uma açao de G em si mesmo. Um outro exemplo é o seguinte.

Exemplo 2.2

Seja $\{v_1, \ldots, v_n\}$ uma base de um espaçao vetorial V de dimensão finita sobre um corpo K. Como todo elemento $v \in V$ pode-se escrever de modo único como uma combinação linear $v = \sum_{i=1}^{n} k_i v_i, k_i \in K, 1 \leq i \leq n$, podemos definir uma ação do grupo S_n das permutações de n elementos em V da seguinte forma. Dado $\sigma \in S_n$, definimos $f_\sigma : V \to V$ por:

$$f_\sigma \left(\sum_{i=1}^{n} k_i v_i \right) = \sum_{i=1}^{n} k_i v_{\sigma(i)}.$$

Como f_σ aplica a base $\{v_1, \ldots, v_n\}$ sobre a base $\{v_{\sigma(1)}, \ldots, v_{\sigma(n)}\}$, segue que f_σ é bijetora, donde $f_\sigma \in S_V$, e um cálculo simples mostra

[1] O artigo de Cayley referido acima, escrito em 1854 é hoje considerado como o primeiro trabalho em teoria *abstrata* de grupos. Os resultados anteriores, de Lagrange, Galois, Ruffini e Cauchy foram obtidos no contexto particular dos grupos de permutações.

que a aplicação $\phi : S_n \to S_V$ dada por $\sigma \mapsto f_\sigma$ é um homomorfismo.

Dada uma ação $\phi : G \to S_M$ do grupo G num conjunto M, e elementos $g \in G, x \in M$, vamos denotar abreviadamente por gx a imagem de $x \in M$ pela aplicação $\phi(g) \in S_M$. Dados dois elementos $x, y \in M$ diz-se que x é **G-equivalente** a y se existe um elemento $g \in G$ tal que $gx = y$. É fácil verificar que esta é uma relação de equivalência. As classes de equivalência de M sob esta relação chamam-se as **órbitas** de M sob a ação de G.

Assim, dado um elemento $x \in M$, a órbita de x sob a ação de G é o conjunto:

$$Orb(x) \ = \ \{gx \mid g \in G\}.$$

O conjunto

$$G_x \ = \ \{g \in G \mid gx = x\}$$

é um subgrupo de G chamado o **estabilizador** de x.

Um elemento $x \in M$ diz-se um **ponto fixo** sob a ação de G se $Orb(x) = \{x\}$ ou, equivalentemente, se $G_x = G$. Note que um argumento de contagem mostra que, para um dado elemento $x \in M$ tem-se que

$$|Orb(x)| \ = \ \frac{|G|}{|G_x|} \ = \ (G : G_x). \tag{1}$$

Consideraremos agora uma ação muito importante de G em si mesmo. A cada elemento a de um grupo G associamos o *automorfismo interior induzido por* a; que é a aplicação $\sigma_a : G \to G$ dada por $\sigma_a(x) = axa^{-1}, \forall x \in G$. A órbita de um elemento $g \in G$ sob esta ação chama-se sua **classe de conjugação** e seu estabilizador chama-se o **centralizador de** g em G e estão dados por:

$$\mathcal{C}(g) \ = \ \{x^{-1}gx \mid x \in G\},$$

$$C_G(g) \ = \ \{x \in G \mid xg = gx\}.$$

Note que é muito fácil provar que $C_G(g)$ é um subgrupo de G.

Observamos também que dois elementos diferentes $x, y \in G$ definem o mesmo conjugado de g em G se e somente se $xgx^{-1} = ygy^{-1}$; i.e., se

$(x^{-1}y)g(x^{-1}y)^{-1} = g$ o que significa que $x^{-1}y \in C_G(g)$. Assim, temos que

$$|\mathcal{C}(g)| = |G|/|C_G(g)| = (G : C_G(g)). \tag{2}$$

O número de classes de conjugação de um grupo G chama-se o **número de classes** de G.

Seja $x_1, \ldots, x_t$ um conjunto completo de representantes das classes de conjugação e seja $n_i = |\mathcal{C}(x_i)| = (G : C_G(x_i))$. Como estas classes formam um recobrimento disjunto de G, temos a seguinte **equação das classes**:

$$|G| = n_1 + n_2 + \cdots + n_t. \tag{3}$$

Note que um elemento $x_i \in G$ é central se e somente se sua classe de conjugação $\mathcal{C}(x_i)$ consiste de um único elemento, de modo que o número de inteiros n_i que são iguais a 1 na equação 3 acima é precisamente igual a $|\mathcal{Z}(G)|$. Assim, também podemos escrever a equação 3 da seguinte forma.

$$|G| = |\mathcal{Z}(G)| + \sum_{n_i > 1} n_i. \tag{4}$$

Seja p um inteiro primo. Um grupo finito G diz-se um **p-grupo** se sua ordem é uma potência de p e um elemento $g \in G$ diz-se um p-elemento se $o(g)$ é uma potência de p. Note que, num p-grupo finito, todo elemento é um p-elemento. Se a ordem de um elemento *não é* divisível por p, então ele diz-se um **p'-elemento.**

O seguinte teorema é um resultado fundamental sobre p-grupos finitos.

Teorema 2.3 *Seja G um p-grupo finito não trivial. Então, $\mathcal{Z}(G) \neq \{1\}$.*

Demonstração. Seja $|G| = p^n$, para algum inteiro positivo n. Se $\mathcal{Z}(G) = \{1\}$, então só existe uma classe de conjugação de G que contém um único elemento. Logo, usando a notação acima, teríamos que $n_1 = 1$ e $n_i \neq 1$, $2 \leq i \leq t$. Como a fórmula 2 mostra que cada $n_i, 2 \leq i \leq t$, é divisível por p, a equação das classes mostra que $p^n = 1 + n_2 + \cdots + n_t = 1 + kp$, para algum inteiro k, uma contradição. □

Damos a seguir algumas aplicações deste resultado.

Corolário 2.4 *Seja p um inteiro primo. Então, todos os grupos de ordem p^2 são abelianos.*

Demonstração. Seja G um grupo de ordem p^2. Então, o Teorema 2.3 mostra que $|\mathcal{Z}(G)|$ é igual a p ou a p^2 e portanto $(G : \mathcal{Z}(G))$ é igual a p ou é igual a 1. Logo, o grupo quociente $G/\mathcal{Z}(G)$ é cíclico. Se $x\mathcal{Z}(G)$ é um gerador deste grupo, segue facilmente que $G = \langle x, \mathcal{Z}(G)\rangle$ e, como x comuta com cada elemento de $\mathcal{Z}(G)$, temos que G é abeliano. □

Proposição 2.5 *Seja G um p-grupo finito de ordem p^n. Então, existe uma cadeia de subgrupos normais de G*

$$1 = G_0 \subset G_1 \subset \cdots \subset G_t = G,$$

tal que cada quociente G_{i+1}/G_i é de ordem p e está contido no centro de G/G_i, $1 \leq i \leq t-1$.

Demonstração. Vamos provar nossa afirmação por indução em n. Se $n = 0$ a afirmação é trivialmente verdadeira. Assim, vamos supor agora que ela é válida para grupos de ordem p^{n-1} e seja G um grupo de ordem p^n. Como $\mathcal{Z}(G) \neq \{1\}$ podemos escolher um elemento $z \in \mathcal{Z}(G)$ de ordem p. Se denotamos $\overline{G} = G/\langle z\rangle$ temos que $|\overline{G}| = p^{n-1}$, de modo que o teorema vale para $\overline{G}$ e, pela hipótese de indução, existe uma cadeia de subgrupos normais de $\overline{G}$

$$1 = \overline{G_1} \subset \overline{G_2} \subset \cdots \subset \overline{G_t} = \overline{G},$$

tal que $\overline{G_{i+1}}/\overline{G_i}$ tem ordem p e está contido no centro de $\overline{G}/\overline{G_i}$, $1 \leq i \leq t-1$.

Todo subgrupo normal $\overline{G_i}$ de $\overline{G}$ é da forma $\overline{G_i} = G_i/\langle z\rangle$ onde G_i é um subgrupo normal de G que contém $\langle z\rangle$.

Segue do segundo teorema do isomorfismo que:

$$\frac{\overline{G_{i+1}}}{\overline{G_i}} \simeq \frac{G_{i+1}/\langle z\rangle}{G_i/\langle z\rangle} \simeq \frac{G_{i+1}}{G_i},$$

donde

$$1 = G_0 \subset G_1 = \mathcal{Z}(G) \subset \cdots \subset G_t = G,$$

é uma cadeia de subgrupos de G nas condições do enunciado. □

Seja G um grupo finito de ordem $|G| = p^n m$, onde p denota um inteiro primo e m um inteiro positivo não divisível por p. Segue então do Teorema de Lagrange que um p-subgrupo de G não pode ter ordem maior do que p^n. Assim, um subgrupo de ordem p^n, se existe, deve ser maximal no conjunto dos p-subgrupos de G.

Definição 2.6 *Seja G um grupo finito de ordem $|G| = p^n m$ onde $p \nmid m$. Um subgrupo de G de ordem p^n chama-se um* **p-subgrupo de Sylow** *de G.*

Em 1872 o matemático noruegûes Ludwig Sylow (1832-1918) provou que sempre existem p-subgrupos de ordem máxima num grupo finito [21], trabalhando ainda com grupos de permutações[2]. Ele prova, nesse contexto, todos os resultados que damos no teorema a seguir, menos a última condição sobre o número de subgrupos. Seu teorema foi estendido posteriormente por G. Frobenius [6] aos grupos abstratos, que também completou o resultado sobre o número destes subgrupos, tal como está enunciado na parte (*iii*) do Teorema 2.9. A prova que damos a seguir, que é hoje *standard*, é devida a H. Wielant [23].

Precisamos inicialmente de um lema técnico e de mais uma definição.

Lema 2.7 *Seja $a = p^n m$ um inteiro positivo, onde p é um inteiro primo e $p \nmid m$. Então, o coeficiente binomial $t = \binom{p^n m}{p^n}$ não é divisível por p.*

Demonstração. De fato, escrevemos

$$t = \binom{p^n m}{p^n} = \frac{p^n m(p^n m - 1)\cdots(p^n m - p^n + 1)}{1 \cdot 2 \cdots (p^n - 1)p^n}.$$

Considere o número racional $\alpha = (p^n m - i)/i$, onde i é tal que $1 \leq i \leq p^n$. Note que, se p^j divide i para algum inteiro positivo j então

[2] É interessante notar que é neste mesmo artigo que Sylow demonstrou que o centro de um p-grupo é não trivial e o obteve seu corolário: todo grupo de ordem p^2 é abeliano.

$j < n$ e p^j divide $(p^n m - i)$. Reciprocamente, se p^j divide $(p^n m - i)$ então $j < n$ e p^j divide i. Então, tanto o numerador como o denominador do racional $(p^n m - i)/i$, $1 \leq i \leq p^n$ envolvem a mesma potência de p e, portanto, p não divide $\alpha = (p^n m - i)/i$, $1 \leq i \leq p^n$. Conseqüentemente, também não divide t. □

Definição 2.8 *Dado um subgrupo H de um grupo G chama-se* **normalizador** *de H em G ao conjunto*

$$N_G(H) = \{g \in G \mid g^{-1}Hg = H\}.$$

Mostra-se facilmente que $N_G(H)$ é um subgrupo de G que é, precisamente, o maior subgrupo em que H é normal.

Teorema 2.9 (Sylow) *Seja G um grupo finito de ordem $|G| = p^n m$, onde p é um inteiro primo que não divide m. Então:*

(i) G sempre contém p-subgrupos de Sylow e todo p-subgrupo de G está contido num p-subgrupo de Sylow de G.

(ii) Todos os p-subgrupos de Sylow de G são conjugados em G.

(iii) Se n_p denota o número de p-subgrupos de Sylow de G, então

$$n_p \equiv 1 \ (mod\ p) \quad e \quad n_p | m.$$

Demonstração. Vamos provar primeiro que existem, de fato, p-subgrupos de Sylow em G. Seja M o conjunto de todos os subconjuntos de G que têm exatamente p^n elementos. Podemos definir uma ação de G em M por multiplicação à esquerda; i.e., dado um elemento $g \in G$ e um subconjunto $X \in M$, a ação de g em X é dada por $X \mapsto gX$.

Como o número de elementos de M é $t = \binom{p^n m}{p^n}$, pelo Lema 2.7, existe pelo menos uma órbita, que denotamos $Orb(X_0)$, cujo número de elementos não é um múltiplo de p. Ainda, como $|Orb(X_0)| = |G|/|G_{X_0}|$ e $|G| = p^n m$, segue que p^n divide $|G_{X_0}|$.

Por outro lado, dado um elemento $a \in X_0$, para cada elemento $g \in G_{X_0}$, temos que $ga \in X_0$, de modo que a aplicação $g \mapsto ga$ é uma função injetiva de G_{X_0} em X_0. Logo, $|G_{X_0}| \leq |X_0| = p^n$. Isto

mostra que $|G_{X_0}| = p^n$ e, portanto, este subgrupo é um p-subgrupo de Sylow de G.

Note que uma vez demonstrado que $|G_{X_0}| = p^n$ temos imediatamente que $|Orb(X_0)| = m$. Agora, seja P um subgrupo de G de ordem p^s com $s \leq n$. Fazemos P agir em $Orb(X_0)$ novamente por multiplicação à esquerda e sejam $m_1, \ldots, m_h$ o número de elementos em cada órbita sob esta ação. Então

$$m = m_1 + \cdots + m_h.$$

Como cada m_i é também uma potência de p e $p \nmid m$ segue que existe uma órbita que contém um único elemento. Se xG_{X_0} denota a única classe lateral desta órbita, temos que $PxG_{X_0} = xG_{X_0}$. Conseqüentemente $PxG_{X_0}x^{-1} = xG_{X_0}x^{-1}$ e assim, como $1 \in xG_{X_0}x^{-1}$, temos que $P \subset xG_{X_0}x^{-1}$. Como $xG_{X_0}x^{-1}$ é também um p-subgrupo de Sylow, isto completa a prova de (i).

Se, em particular, tomamos $s = n$, o argumento acima prova também (ii).

Finalmente, seja $\mathcal{T}$ o conjunto de todos os conjugados de G_{X_0} em G. Então, G_{X_0} age por conjugação em $\mathcal{T}$ e o número de elementos numa G_{X_0}-órbita de $\mathcal{T}$ é uma potência de p. Seja $n_1, \ldots, n_r$ o número de elementos em cada classe de conjugação sob esta ação. Então, a equação das classes, aplicada a este caso, dá:

$$n_p = |\mathcal{T}| = n_1 + \cdots + n_r.$$

Seja G_1 um elemento de $\mathcal{T}$ cuja órbita consiste de um único elemento. Isto significa que G_1 é normal em $\langle G_1, G_{X_0} \rangle$. Logo $\langle G_1, G_{X_0} \rangle = G_1 G_{X_0}$ que é um subgrupo de ordem $|G_1 G_{X_0}| = |G_1||G_{X_0}|/|G_1 \cap G_{X_0}|$ e este número é uma potência de p que não pode exceder $|G_{X_0}| = p^n$.

Como $G_{X_0} \subset G_1 G_{X_0}$ segue que $G_{X_0} = G_1 G_{X_0}$ e $G_{X_0} = G_1$. Isto mostra que só existe uma classe de conjugação que consiste de um único elemento. Logo, da equação das classes obtemos que

$$n_p \equiv 1 \pmod{p},$$

como queríamos demonstrar.

Finalmente, notamos que, de acordo com a parte (ii) do enunciado, se P é um dado p-subgrupo de Sylow de G, então o número n_p de todos os p-subgrupos de Sylow de G é igual ao número de conjugados de P em G. Como dois elementos diferentes $x, y \in G$ definem o mesmo conjugado de P se e somente se $e \equiv y$, $mod(N_G(P))$ temos que

$$n_p = (G : N_G(P)) = \frac{|G|}{|N_G(P)|}.$$

Como $P \subset N_G(P)$ temos que $|N_G(P)|$ é um múltiplo de p^n. Portanto, segue da equação acima que $n_p \mid m$. □

Concluímos esta seção com um resultado que será útil mais adiante.

Proposição 2.10 *Seja P um p-subgrupo de Sylow de um grupo G e seja H outro subgrupo. Se $N_G(P) \subset H$ então $H = N_G(H)$.*

Demonstração. Seja $x \in N_G(H)$. Como $P \subset H \lhd N_G(H)$, temos que $xPx^{-1} \subset H$. Como P e xPx^{-1} são p-subgrupos de Sylow de H, existe um elemento $h \in H$ tal que $xPx^{-1} = hPh^{-1}$ donde $h^{-1}x \in N_G(P) \subset H$. Segue que $x \in H$ e portanto $N_G(H) = H$. □

Como conseqüência imediata temos o seguinte.

Corolário 2.11 *Seja P um p-subgrupo de Sylow de um grupo G. Então $N_G(N_G(P)) = N_G(P)$.*

Exercícios

1. Prove que vale a recíproca do Teorema de Lagrange para p-grupos; i.e., mostre que se G é um grupo de ordem p^n, então G contém subgrupos de ordem p^k, para todo inteiro positivo $k \leq n$.

2. Seja G um grupo. Prove que se dois elementos pertencem à mesma classe de conjugação então seus centralizadores são conjugados em G.

3. Seja H um p-subgrupo de Sylow de um grupo G. Prove que H é o único p-subgrupo de Sylow de G contido em $N_G(H)$.

4. Seja H um subgrupo de um grupo G. Prove que o número de conjugados de H em G é $(G : N_G(H))$.

5. Prove que não existem grupos simples de ordem 28 ou 312.

6. Prove que todo grupo de ordem 15 é cíclico.

2.2 Grupos Abelianos

Nesta seção vamos discutir a estrutura dos grupos abelianos que são gerados por um conjunto finito de elementos. É uma prática freqüente utilizar a notação aditiva ao se tratar dos grupos abelianos mas, como no restante destas notas escreveremos sempre os grupos multiplicativamente, vamos manter essa notação também aqui.

Inicialmente, vamos estudar os grupos abelianos finitos e, para isso, começamos com algumas observações de caráter geral.

Seja g um elemento de um grupo arbitrário G de ordem $o(g) = mn$, onde $(m, n) = 1$. Então, podemos achar inteiros r, s tais que $rm+sn = 1$. Assim, temos que $g = g^{rm+sn} = g^{rm}g^{sn}$ e é fácil verificar que $o(g^{rm}) = n$ e $o(g^{sn}) = m$. Mais ainda, esta descomposição é única. Esta idéia pode ser estendida, por indução, a um número finito de divisores da ordem de um elemento.

Lema 2.12 *Seja g um elemento de ordem $o(g) = p_1^{n_1} \cdots p_t^{n_t}$ num grupo arbitrário G. Então, podemos escrever $g = g_1 \cdots g_t$ com $o(g_i) = p_i^{n_i}$, $1 \leq i \leq t$. Ainda, os elementos $g_1, \ldots, g_t$ estão determinados univocamente e são potências de g e assim, eles comutam entre si.*

Lembramos, da seção anterior, que um elemento cuja ordem é uma potência de um primo p diz-se um **p-elemento** . Por outro lado, se p não divide a ordem do elemento, então ele chama-se um **p'-elemento**.

No caso dos grupos abelianos, o lema anterior permite demonstrar o seguinte.

Teorema 2.13 *Seja G um grupo finito abeliano de ordem $|G| = p_1^{n_1} \cdots p_t^{n_t}$. Então*

$$G = G(p_1) \times \cdots \times G(p_t).$$

Definição 2.14 *Um grupo abeliano G diz-se* **abeliano elementar** *se existe um inteiro primo p tal que todos os elementos de G diferentes da unidade são de ordem p.*

É interessante notar que todo p-grupo abeliano elementar, que é finito, tem uma estrutura bem determinada.

Lema 2.15 *Seja G um p-grupo abeliano elementar finito. Então G pode ser escrito como o produto direto de um número finito de grupos cíclicos de ordem p.*

Para um grupo arbitrário G define-se o **expoente** de G como o menor inteiro positivo m tal que $g^m = 1$, para todo $g \in G$, se este número existe, e escreve-se que $exp(G) = m$. Note que G é um p-grupo abeliano elementar se e somente se $exp(G) = p$. Se G é um grupo abeliano qualquer, denotamos por G^p o subconjunto

$$G^p = \{g^p \mid g \in G\}.$$

que é um subgrupo de G.

Note que, se G é um grupo abeliano e $exp(G) = p^m$, então $exp(G^p) = p^{m-1}$.

Estas observações são utilizadas para demonstrar o seguinte:

Teorema 2.16 *Seja G um p-grupo abeliano finito. Então G pode ser escrito como o produto direto de p-subgrupos cíclicos. Esta decomposição é única no seguinte sentido. Se*

$$G = C_1 \times \cdots \times C_t = D_1 \times \cdots \times D_s$$

onde $C_i, D_j, 1 \leq i \leq t, 1 \leq j \leq s$, são p-grupos cílicos de ordens $p^{n_1} \geq \cdots \geq p^{n_t} > 1$ and $p^{m_1} \geq \cdots \geq p^{m_s} > 1$ respectivamente, então $t = s$ e $n_i = m_i, 1 \leq i \leq t$.

A partir deste resultado, pode-se provar a seguinte propriedade.

Proposição 2.17 *Seja G um grupo finito de ordem n. Então, para cada divisor d de n, o número de subgrupos cílicos de G de ordem d é igual ao número de quocientes cíclicos de G da mesma ordem.*

A seguir, passaremos a considerar grupos abelianos infinitos.

Seja G um grupo. Um elemento de G diz-se um **elemento de torção** se é de ordem finita. Num grupo abeliano, se dois elementos $g, h \in G$ são de torção, de ordens m e n respectivamente, então segue imediatamente que $(g^{-1}h)^{mn} = 1$, o que mostra que *o conjunto dos elementos de ordem finita, num grupo abeliano, forma um subgrupo.* Note que esta mesma observação implica que dado um inteiro primo p, o conjunto de elementos de G cuja ordem é uma potência de p também é um subgrupo de G.

Definição 2.18 *Seja G um grupo abeliano. Então, o subgrupo*

$$T(G) = \{g \in G \mid o(g) < \infty\}$$

chama-se o **subgrupo de torção** *de G e o subgrupo*

$$G(p) = \{g \in G \mid o(g) \text{ é uma potência de } p\}$$

chama-se a **componente p-primária** *de G.*

Se $T(G) = \{1\}$, então diz-se que G é um grupo **sem torção**.

Um grupo abeliano diz-se **abeliano livre** *se é um produto direto de grupos cíclicos infinitos. Se o número de fatores diretos é finito, então este número chama-se o* **posto**. *Em caso contrário, diz-se que o grupo é* **de posto infinito**.

É fácil ver que grupos abelianos livres são sem torção. Pelo contrário, grupos sem torção não são necessariamente livres, como pode-se ver considerando o grupo aditivo dos números racionais. Porém, vale o seguinte.

Teorema 2.19 *Um grupo abeliano G finitamente gerado, sem torção, é livre (logo, da forma $G \simeq C \times \cdots \times C$, onde C denota um grupo cíclico infinito e o número de fatores é o posto de G).*

Um primeiro passo para descrever a estrutura dos grupos abelianos finitamente gerados é separar a parte livre e a parte de torção.

Teorema 2.20 *Seja G um grupo abeliano finitamente gerado. Então $T(G)$ é finito, $G/T(G)$ é livre, de posto finito e*

$$G \simeq T(G) \times \frac{G}{T(G)}$$

Corolário 2.21 *Um subgrupo de um grupo abeliano finitamente gerado é finitamente gerado.*

Combinando o teorema acima com os Teoremas 2.13 e 2.16 podemos dar uma descrição completa destes grupos.

Teorema 2.22 *Seja G um grupo abeliano finitamente gerado. Então existem primos $p_1, \ldots, p_t$ tais que G pode-se escrever como um produto direto*

$$G = C_1(p_1) \times \cdots \times C_{s_1}(p_1) \times \cdots \times C_1(p_t) \times \cdots \times C_{s_t}(p_t) \times C \times \cdots \times C,$$

onde $C_j(p_i)$, $1 \leq i \leq s_i$ indica um grupo cíclico de ordem potência de p_i, $1 \leq i \leq t$ e C denota um grupo cíclico infinito. Os inteiros s_i, $1 \leq i \leq t$, as ordens dos subgrupos $C_j(p_i)$ e o número de fatores cíclicos infinitos estão univocamente determinados.

Exercícios

1. Determine, a menos de isomorfismos, todos os grupos abelianos de ordem 60.

2. Sejam G e H grupos abelianos finitamente gerados. Prove que $G \times G \simeq H \times H$ se e somente se $G \simeq H$.

3. Seja G, H e K grupos abelianos finitamente gerados. Prove que $G \times K \simeq H \times K$ se e somente se $G \simeq H$.

4. Prove que vale a recíproca do Teorema de Lagrange para grupos abelianos finitos.

5. Prove que todo grupo abeliano é isomorfo a um grupo quociente de um grupo abeliano livre.

3 Solubilidade

3.1 Comutadores

Neste capítulo e no seguinte, vamos estudar grupos que, de alguma forma, estão próximos dos grupos abelianos. Para isso, começamos por introduzir mais alguns conceitos.

Definição 3.1 *Dados dois elementos x, y de um grupo G, o* **comutador** *de x e y é o elemento*

$$(x, y) = x^{-1}y^{-1}xy \in G.$$

Mais geralmente, um **comutador de comprimento** $n \geq 2$ *define-se indutivamente por*

$$(x_1, \ldots, x_n) = ((x_1, \ldots, x_{n-1}), x_n).$$

Dados dois subconjuntos H *e* K *de um grupo* G*, denotaremos por* (H, K) *o* subgrupo *de* G *gerado pelo conjunto:*

$$\{(h, k) \mid h \in H,\ k \in K\}.$$

Em particular, o grupo $G' = (G, G)$ *chama-se* **subgrupo comutador** *ou* **subgrupo derivado** *de* G.

Indutivamente, podemos definir agora uma sequência de subgrupos da seguinte forma:

$$G^{(0)} = G.$$
$$G^{(1)} = (G^{(0)}, G^{(0)}) = G'.$$
$$G^{(n)} = (G^{(n-1)}, G^{(n-1)}).$$

Definição 3.2 *O subgrupo* $G^{(n)}$ *definido acima chama-se o* **n-ésimo grupo derivado** *de* G *e a sequência*

$$G = G^{(0)} \supset G^{(1)} \supset \cdots \supset G^{(n)} \supset \cdots$$

chama-se a **sequência derivada** *de* G.

O conceito de *comutador* de dois elementos aparece pela primeira vez em 1860, ainda no contexto dos grupos de permutações, na tese de C. Jordan (1838-1922) [12], embora ele não chegasse a levar adiante o desenvolvimento da teoria correspondente. Já o conceito de *grupo comutador* aparece na literatura perto do fim do século XIX; G.A. Miller [14] publicou pela primeira vez as propriedades principais destes grupos, embora estas aparentemente já eram conhecidas de R. Dedekind (1831-1916) que foi quem introduziu o uso do termo *comutador* em 1897 [4].

As seguintes propriedades dos comutadores são de demonstração simples, que deixamos a cargo do leitor.

Lema 3.3 *Sejam* x, y, z *e* t *elementos de um grupo* G*. Então*

(i) $(x,y) = 1$ *se e somente se* $xy = yx$.

(ii) $(x,y)^{-1} = (y,x)$.

(iii) $(x,y)^z = (x^z, y^z)$.

(iv) $(xy,z) = (x,z)^y(y,z) = (x,z)((x,z),y)(y,z)$.

(v) $(x,yz) = (x,z)(x,y)^z = (x,z)(x,y)((x,y),z)$.

(vi) $(x,y)z = z(x^z, y^z)$.

(vii) $(x^y,z) = (x,z)^{(x,y)}(x,y,z)$.

(viii) $(x^{yz},t) = (x^y,t)^{(x^y,z)}(x^y,z,t)$.

(ix) $(x,y,z) = (x,y)^{-1}(x,y)^z$.

(x) *Se* $\phi : G \to H$ *é um homomorfismo de grupos, então* $\phi((x,y)) = (\phi(x), \phi(y))$.

Note que a parte (i) do Lema 3.3 mostra imediatamente que um grupo G é abeliano se e somente se $G' = \{1\}$. Veremos, a seguir, que o conhecimento de G' também permite saber quando um quociente é abeliano.

Lema 3.4 *Seja H um subgrupo normal de um grupo G. Então, o grupo quociente G/H é abeliano se e sòmente se $G' \subset H$.*

Demonstração. Dados elementos $x, y \in G$, vamos denotar por $\overline{x}, \overline{y}$ as respectivas classes em G/H. Note que $\overline{xy} = \overline{yx}$ se e somente se $(yx)^{-1}(xy) \in H$; isto é, se e somente se $(x,y) \in H$ para todo $x, y \in G$ ou, equivalentemente, se e somente se $G' \subset H$. □

A propriedade (iii) do Lema 3.3 permite deduzir facilmente que G' é um subgrupo normal de G. Na verdade, será possível provar que G' verifica uma condição mais forte, que foi introduzida por G. Frobenius em 1895 [6] e que damos a seguir.

Definição 3.5 *Um subgrupo H de um grupo G diz-se um* **subgrupo característico** *se $\phi(H) = H$ para todo automorfismo $\phi : G \to G$. Para indicar que H é um subgrupo característico de G escreveremos H car G.*

Como a conjugação por um elemento fixo a de G, $x \mapsto a^{-1}xa$, é um automorfismo de G, segue que todo subgrupo característico é, em particular, um subgrupo normal. Note ainda que, se $\phi : G \to G$ é um automorfismo e H é um subgrupo característico de G, então a restrição de ϕ a H é um automorfismo de H. Desta observação segue facilmente que se K *car* H e H *car* G, então K *car* G.

Proposição 3.6 *Seja H um subgrupo de um grupo G. Se H é característico em G então H' também é característico em G. Em particular, $G^{(n)}$ é característico em G, para todo inteiro positivo n.*

Demonstração. Como H' é o subgrupo gerado por todos os elementos da forma (x, y) com $x, y \in H$, para provar a primeira afirmação bastará mostrar que para todo automorfismo $\phi : G \to G$ tem-se que $\phi((x, y)) \in H'$.

De fato, $\phi((x, y)) = (\phi(x), \phi(y))$ e, como H *car* G, segue imediatamente que $\phi((x, y)) \in H'$.

A segunda afirmação do enunciado segue agora trivialmente, da anterior. □

Concluímos esta seção com um resultado técnico.

Lema 3.7 *Sejam x e y elementos de um grupo G e seja $\mathcal{Z}(G)$ o centro de G. Se $|G/\mathcal{Z}(G)| = n$ então $(x, y)^{n+1} = (x, y^2)(x^y, y)^{n-1}$.*

Demonstração. Como estamos assumindo que $|G/\mathcal{Z}(G)| = n$, temos que $(x, y)^n \in \mathcal{Z}(G)$. Logo:

$$\begin{aligned}(x,y)^{n+1} &= x^{-1}y^{-1}xy(x,y)^n = x^{-1}y^{-1}x(x,y)^n y = \\ &= x^{-1}y^{-1}x(x^{-1}y^{-1}xy)(x,y)^{n-1}y \\ &= x^{-1}y^{-2}xy^2y^{-1}(x,y)^{n-1}y \\ &= (x,y^2)(x^y,y)^{n-1}.\end{aligned}$$

□

A importância dos conceitos de *comutadores sucessivos* e da *série derivada* foi enfatizada por P. Hall em 1933 num trabalho fundamental [8] ao qual voltaremos a nos referir no próximo capítulo, embora eles já tivessem sido estudados em conexão com a teoria de grupos solúveis,

como veremos na seção seguinte. Ele observa que estes são grupos característicos e destaca a importância deste conceito:

> "Nós fomos guiados pela idéia de que a estrutura de um grupo deve ser exibida, tanto quanto possível, pela interrelação dos seus *subgrupos característicos*. Um subgrupo é característico, de acordo a Frobenius, se é transformado em si mesmo por todo automorfismo do grupo; logo os subgrupos característicos representam o que poderíamos chamar realmente das qualidades *invariantes* da estrutura de grupo."

Os termos da série derivada pertencem, na verdade, à família ainda mais restrita dos subgrupos *totalmente invariantes* (veja os exercícios 3, 4 e 5 abaixo), que foi introduzida por Levi [17] também em 1933.

Exercícios

1. Sejam H, K, L subgrupos normais de uma grupo G. Prove que:
   (i) (H, K) é um subgrupo normal de $\langle H \cap K \rangle$.
   (ii) $(H, K) = (K, H)$.
   (iii) $K \lhd H$ se e somente se $(H, K) \subset K$.
   (iv) Se H, K, L são todos normais em G então $(H, KL) = (H, K)(H, L)$.
   (v) Se $H \subset L$ e são ambos normais em G então $K/H \subset \mathcal{Z}(G/H)$ se e somente se $(K, G) \subset H$.
   (vi) Se H e K são normais em G então (H, K) é normal em G.

2. (Lema dos três subgrupos) Sejam H, K, L subgrupos de um grupo G tais que $(H, K, L) = 1$ e $(L, H, K) = 1$. Prove que também $(K, L, H) = 1$.

3. Um subgrupo H de um grupo G diz-se *totalmente invariante* se $\phi(H) \subset H$ para todo homomorfismo $\phi : G \to G$. Prove que
   (i) Subgrupos totalmente invariantes são característicos e subgrupos característicos são normais.
   (ii) As relações "totalmente invariante" e "característico" são transitivas, mas "normal" não é transitiva, em geral.
   (iii) Sejam H e K subgrupos de um grupo G. Se H é característico em K e $K \lhd G$ então $H \lhd G$.

4. Sejam H e K subgrupos característicos (totalmente invariantes) de um grupo G. Prove que $H \cap K$ e $\langle H, K \rangle$ são subgrupos característicos (totalmente invariantes) de G.

5. Prove que os subgrupos da série derivada de um grupo G são subgrupos totalmente invariantes de G.

6. Seja H um subgrupo normal de um grupo G tal que $|H|$ e $(G : H)$ são relativamente primos. Prove que H é característico em G (Sugestão: Dado um automorfismo f de G considere a ordem do subgrupo $Hf(H)$).

3.2 Grupos solúveis

O conceito de grupo solúvel é um dos mais antigos na teoria de grupos. Foi introduzido por E. Galois quando estudava o problema de resolver equações algébricas mediante radicais. Ele associava um grupo a cada equação e mostrou que a equação é resolúvel mediante radicais se e somente se o grupo correspondente é solúvel, no sentido que definimos abaixo. A definição e as primeiras propriedades dos grupos solúveis servirão, em certo sentido, como introdução ao objeto do nosso estudo.

Informalmente, pode-se pensar nos grupos solúveis como "aproximadamente abelianos". Por exemplo, podemos considerar que um grupo G está "perto" de ser abeliano se ele contém um subgrupo normal H tal que tanto H quanto o quociente G/H são abelianos (um tal grupo diz-se *metabeliano*). Generalizando esta idéia podemos formular a seguinte.

Definição 3.8 *Um grupo G diz-se* **solúvel** *se contém uma cadeia de subgrupos:*

$$\{1\} = G_0 \subset G_1 \subset \cdots \subset G_n = G$$

tal que cada subgrupo G_{i-1} é normal em G_i e o grupo quociente G_i/G_{i-1}, $1 \leq i \leq n$, é abeliano.

Uma cadeia de subgrupos de G com esta propriedade chama-se uma **série subnormal abeliana** *de G e os quocientes respectivos chamam-se os* **fatores** *da série.*

Note que, como a normalidade não é necessariamente transitiva, os subgrupos G_i não precisam ser normais em G, $1 \leq i \leq n-1$.

Exemplo 3.9

- Todo grupo abeliano é solúvel.
- Os grupos S_3 e S_4 são solúveis. De fato. para ver que S_3 é solúvel basta observar que se consideramos o ciclo $\sigma = (1\ 2\ 3)$ então $H = \langle\sigma\rangle$ é cíclico de ordem 3 e $(G : H) = 2$, o que implica que H é normal em G. Ainda, S_3/H é cíclico de ordem 2; logo; $\{1\} \subset H \subset G$ é uma série subnormal abeliana para S_3.

  Em S_4 consideramos o subgrupo $H = \{1,\ (1\ 2)(3\ 4),\ (1\ 3)(2\ 4),\ (1\ 4)(2\ 3)\}$. É facil verificar que $H \lhd A_4$, de modo que $\{1\} \subset H \subset A_4 \subset S_4$ é uma série subnormal abeliana para S_4.
- Um resultado clássico mostra que S_n e A_n não são solúveis se $n \geq 5$.
- A Proposição 2.5 mostra que todo p-grupo finito é solúvel.

Damos, a seguir, uma caracterização da solubilidade em termos da sequência derivada.

Teorema 3.10 *Um grupo G é solúvel se e somente se sua série derivada termina; i.e., se existe um inteiro positivo n tal que $G^{(n)} = \{1\}$.*

Demonstração. Vamos assumir inicialmente que existe um inteiro positivo n tal que $G^{(n)} = \{1\}$. Então, obviamente,

$$G^{(0)} \supset G^{(1)} \supset G^{(2)} \supset \cdots \supset G^{(n)} = \{1\}$$

é uma série subnormal abeliana para G.

Reciprocamente, suponhamos que G contém uma série subnormal abeliana

$$G_0 \supset G_1 \supset G_2 \supset \cdots \supset G_n = \{1\}.$$

Como todo quociente G_i/G_{i-1}, $0 \leq i \leq n-1$, é abeliano, segue do Lema 3.4 e de um argumento de indução que $G^{(i)} \subset G_i, 1 \leq i \leq n$. Logo, temos em particular que $G^{(n)} = \{1\}$. □

O próximo resultado é de demonstração simples a partir da caracterização acima e o dexamos a cargo do leitor.

Lema 3.11 *Subgrupos e grupos quocientes de grupos solúveis são solúveis.*

Vale também a recíproca deste resultado.

Lema 3.12 *Seja H um subgrupo normal de um grupo G. Se ambos H e G/H são solúveis, então G é solúvel.*

Demonstração. Como G/H é solúvel, existe um inteiro positivo n tal que $(G/H)^{(n)} = 1$. Isto implica que $G^{(n)} \subset H$. Ainda, como H também é solúvel, existe um inteiro positivo m tal que $H^{(m)} = \{1\}$. Logo $G^{(mn)} = \{1\}$, donde G é solúvel. □

Se um grupo solúvel é finito, então ele contém uma cadeia subnormal abeliana muito especial.

Proposição 3.13 *Um grupo solúvel finito G contém uma série subnormal abeliana cujos fatores são todos cíclicos de ordem prima.*

Demonstração. Vamos demonstrar o resultado por indução na ordem de G. Se $|G| = 1$ não há nada a provar. Assim, suponhamos que $|G| = n > 1$ e que o resultado vale para todos os grupos solúveis de ordem menor que n. Notamos que, se $|G|$ é um número primo, então o resultado segue trivialmente pois $\{1\} \subset G$ é uma série subnormal abeliana para G.

Se G é solúvel, e não é de ordem prima, então ele contém pelo menos um subgupo normal H. Como tanto $|H|$ como $|G/H|$ são menores que n segue, da hipótese de indução, que ambos os grupos têm séries subnormais abelianas com fatores cíclicos.

Denotando $\overline{G} = G/H$, sejam

$$\{1\} = H_0 \triangleleft H_1 \triangleleft \cdots \triangleleft H_m = H$$

$$\{1\} = \overline{G}_0 \triangleleft \overline{G}_1 \triangleleft \cdots \triangleleft \overline{G}_n = \overline{G}$$

séries subnormais abelianas, com fatores cíclicos, para H e $\overline{G}$ respectivamente. Existem subgrupos G_i de G que contém H tais que $G_i/H = \overline{G}_i$, e $G_{i-1} \triangleleft G_i$, $1 \leq i \leq n$. Como

$$\frac{\overline{G}_i}{\overline{G}_{i-1}} = \frac{G_i/H}{G_{i-1}/H} \simeq \frac{G_i}{G_{i-1}},$$

vemos imediatamente que a série de subgrupos

$$\{1\} = H_0 \lhd H_1 \lhd \cdots \lhd H_m = H = G_0 \lhd G_1 \lhd \cdots \lhd G_n = G$$

é uma série subnormal abeliana para G, com fatores cíclicos. □

Exercícios

1. Dar uma demonstração do Lema 3.11 diretamente a partir da definição de solubilidade, sem usar a série derivada.

2. Um gupo diz-se *perfeito* se coincide com seu grupo derivado. Provar que todo grupo que não é solúvel contém um subgrupo característico $H \neq \{1\}$ que é perfeito.

3. Sejam H e K dois subgrupos normais de um grupo G. Prove que se ambos H e K são solúveis, então o subgrupo HK também o é.

4. Prove que todo grupo de ordem 12 é solúvel.

5. Sejam $p \neq q$ dois inteiros primos. Prove que todo grupo de ordem pq é solúvel.

6. Prove que se um grupo de torção é solúvel e finitamente gerado, então ele é finito.

4 Grupos Nilpotentes

4.1 Introdução

Neste capítulo, estudaremos uma classe de grupos que, de certa forma, "está entre" a classe dos grupos abelianos e a classe dos grupos solúveis e mostraremos que é possível obter resultados fortes sobre a sua estrutura.

Em 1897 apareceu o primeiro livro inteiramente dedicado à teoria abstrata de grupos, o *Theory of Groups of Finite Order* de W. Burnside [1], que é um verdadeiro marco na história desta teoria [3]. Nele aparece a prova da existência da série central de um p-grupo, tal como vimos no Teorema 2.5. Na p.166 Burnside mostra um recíproco parcial: ele prova

[3] Deve-se notar, porém, que no *Lehrbuch der Algebra* de H. Weber [22] a teoria dos grupos já é tratada de um ponto de vista abstrato.

que se um grupo finito admite uma sequência semelhante à achada para um p-grupo (isto é, se ele é nilpotente no sentido da Definição 4.1), então ele é produto direto de p-grupos.

Além de sua importância histórica por representar o início do estudo dos grupos nilpotentes, este teorema teve também uma influência indireta, porém importante, no desenvolvimento da teoria. Lemos, no livro de B. Chandler e W. Magnus [3]:

> "Sabemos, por uma carta de P. Hall, que ele veio a se interessar na teoria dos grupos pela leitura do livro de Burnside sobre a teoria de grupos de ordem finita. Este fato estabelece uma relação entre o trabalho de Burnside sobre grupos de ordem potência de um primo e o artigo de P. Hall [8] sobre o mesmo tópico. O título do artigo de Hall, *A contribution to the theory of groups of prime power order*, não revela o fato de que também representa um marco na história da teoria combinatória de grupos. Isto deve-se à seção sobre 'cálculo de comutadores' do artigo na qual Hall investiga sistematicamente as relações complicadas entre a composição associativa de dois elementos do grupo e a composição definida formando o seu comutador. O resultado é a primeira análise completa dos grupos da série central inferior (um termo cunhado por Hall) dos grupos livres e sua relação com outros subgrupos totalmente invariantes dos grupos livres"

Definição 4.1 *Um grupo G diz-se* **nilpotente** *se ele contém uma série de subgrupos*

$$\{1\} = G_0 \subset G_1 \subset \cdots \subset G_n = G$$

tal que cada subgrupo G_{i-1} é normal em G e cada quociente G_i/G_{i-1} está contido no centro de G/G_{i-1}, $1 \leq i \leq n$.

Uma tal série de subgrupos de G diz-se uma **série central** *de G.*

Uma vez que as condições na definição de nilpotência são obviamente mais restritivas que aquelas que aparecem na definição de solubilidade, resulta evidente que todo grupo nilpotente é, em particular, solúvel. Note também que a Proposição 2.5 mostra que os p-grupos finitos são

nilpotentes. Daremos uma demonstração diferente deste fato na Proposição 4.7.

Note que a definição acima implica que G_1 está contido no centro de G. Se $G_1 = \{1\}$ então G_2 está contido no centro, e assim sucessivamente. Como a série central acaba, resulta imediatamente que todo grupo nilpotente tem centro não trivial.

Exemplo 4.2

- Todo grupo abeliano é nilpotente e a Proposição 2.5 mostra que, na verdade, todo p-grupo finito é nilpotente.
- Vimos, no Exemplo 3.2, que S_3 é solúvel. Como o centro de S_3 é trivial, segue imediatamente que este é um exemplo de um grupo solúvel que *não é* nilpotente.

Vamos dar agora duas caracterizações alternativas da nilpotência. Como no estudo da solubilidade, exploraremos as conexões entre a nilpotência e certo tipo de comutadores.

Para isso, definimos uma nova série de subgrupos, indutivamente:

$$\gamma_1(G) = G, \ \gamma_2(G) = G' \ \text{ e } \ \gamma_i(G) = (\gamma_{i-1}(G), G).$$

Precisaremos ainda de uma outra série, que definimos também indutivamente, nos apoiando no conceito de *centro* de um grupo:

Denotamos $\zeta_0(G) = \{1\}$, $\zeta_1(G) = \mathcal{Z}(G)$ e definimos indutivamente $\zeta_i(G)$ como sendo o único subgrupo de G tal que $\zeta_i(G)/\zeta_{i-1}(G) = \mathcal{Z}(G/\zeta_{i-1}(G))$.

O subgrupo $\zeta_i(G)$ chama-se **i-ésimo centro** de G.

Definição 4.3 *As sequências de subgrupos*

$$\{1\} = \zeta_0(G) \subset \zeta_1(G) \subset \cdots \subset \zeta_n(G) \subset \cdots$$

e

$$G = \gamma_1(G) \supset \gamma_2(G) \supset \cdots \supset \gamma_n(G) \supset \cdots$$

chamam-se a **série central superior** *e a* **série central inferior** *de G respectivamente.*[4]

Claramente, estas são séries centrais. A razão pela qual são chamadas de "superior" e "inferior" ficará clara a partir dos próximos resultados.

Lema 4.4 *Seja*

$$\{1\} = A_0 \subset A_1 \subset \cdots \subset A_n \cdots$$

uma série central de G (i.e., uma cadeia de subgrupos normais tal que $A_i/A_{i-1} \subset \mathcal{Z}(G/A_{i-1})$ para todo i). Então $A_i \subset \zeta_i(G)$ para todo i.

Demonstração. Vamos provar nossa afirmação usando indução em i. Note que o resultado é trivialmente verdadeiro para $i = 1$. Assumimos então, como hipótese de indução, que $A_i \subset \zeta_i(G)$. Dados $x \in A_{i+1}$ e $g \in G$, como $A_{i+1}/A_i \subset \mathcal{Z}(G/A_i)$ temos que $x^{-1}g^{-1}xg \in A_i \subset \zeta_i(G)$. Logo, da definição de $\zeta_{i+1}(G)$ temos que $A_{i+1} \subset \zeta_{i+1}(G)$. □

Lema 4.5 *Seja*

$$\{1\} = A_0 \subset A_1 \subset \cdots \subset A_n = G$$

uma série central de G. Então $\gamma_i(G) \subset A_{n-i+1}$, para todo i.

Demonstração. Se $i = 1$ o resultado é obviamente verdadeiro. Suponhamos, por indução, que $\gamma_i(G) \subset A_{n-i+1}$. Como A_{n-i+1}/A_{n-i} está no centro de G/A_{n-i}, temos que $(A_{n-i+1}, G) \subset A_{n-i}$. Logo

$$\gamma_{i+1}(G) = (\gamma_i(G), G) \subset (A_{n-i+1}, G) \subset A_{n-i},$$

como queríamos demonstrar. □

Destes resultados segue imediatamente a seguinte caracterização dos grupos nilpotentes.

Teorema 4.6 *Seja G um grupo. São equivalentes:*

[4] As vezes, estas séries são chamadas de **série central ascendente** e **série central descendente** respectivamente, por razões óbvias.

(i) G *é nilpotente.*

(ii) Existe um inteiro positivo m *tal que* $\zeta_m(G) = G$.

(iii) Existe um inteiro positivo n *tal que* $\gamma_n(G) = \{1\}$.

Também deve resultar claro, a partir dos lemas acima, que se G é um grupo nilpotente, então as séries centrais superior e inferior de G têm o mesmo comprimento. Este número chama-se a **classe de nilpotência** de G.

A série central inferior foi introduzida por W.B. Fite [5] em conexão com o estudo de p-grupos, em 1906, mas sua importância para o estudo da nilpotência só foi reconhecida por P. Hall, no seu artigo fundamental de 1933 [8].

Damos agora uma prova alternativa da nilpotência dos p-grupos finitos.

Proposição 4.7 *Todo* p*-grupo finito é nilpotente.*

Demonstração. Sabemos, do Teorema 2.3, que o centro de um p-grupo finito é não trivial. Como todos os quocientes de G são também p-grupos, segue que $\zeta_{i-1}(G) \subsetneq \zeta_i(G)$ para todo inteiro positivo i. Como G é finito, temos que existe um inteiro n tal que $\zeta_n(G) = G$, logo G é nilpotente. □

Proposição 4.8 *Produtos diretos finitos de grupos nilpotentes são também nilpotentes.*

Deixamos a demonstração deste resultado como exercício. (Sugestão: note que, se $G = G_1 \times \cdots \times G_n$ então $\gamma_i(G) = \gamma_i(G_1) \times \cdots \times \gamma_i(G_n)$ para todo índice i.)

Agora estamos em condições de mostrar que o centro de um grupo nilpotente é razoavelmente grande: ele intercepta todos os subgrupos normais do grupo.

Proposição 4.9 *Seja* $H \neq \{1\}$ *um subgrupo normal de um grupo nilpotente* G. *Então* $H \cap \mathcal{Z}(G) \neq \{1\}$

Demonstração. Como $G = \zeta_n(G)$ para algum índice n, existe um índice i que é o menor inteiro positivo tal que $H \cap \zeta_i(G) \neq \{1\}$. Então $(H \cap \zeta_i(G), G) \subset H \cap \zeta_{i-1}(G) = \{1\}$ logo $H \cap \zeta_i(G) \subset H \cap Z(G)$. □

Corolário 4.10 *Um subgrupo normal minimal de um grupo nilpotente está contido no centro.*

Vamos demonstrar a seguir uma propriedade importante dos grupos nilpotentes, que será útil mais adiante, para descrever sua estrutura .

Proposição 4.11 *Seja H um subgrupo próprio de um grupo nilpotente. Então $H \subsetneq N_G(H)$.*

Demonstração. Como $\{1\} = \zeta_0(G) \subset H \subset \zeta_n(G) = G$, existe um inteiro positivo i tal que $\zeta_i(G) \subset H$ e $\zeta_{i+1}(G) \not\subset H$. Escolhemos um elemento $x \in \zeta_{i+1}(G) \setminus H$ e um elemento arbitrário $h \in H$. Como $(\zeta_{i+1}(G), G) \subset \zeta_i(G)$ temos que existe um elemento $y \in \zeta_i(G) \subset H$ tal que $xhx^{-1} = hy \in H$, logo $xHx^{-1} \subset H$ e portanto $x \in N_G(H)$, o que mostra que $H \subsetneq N_G(H)$. □

Definição 4.12 *Diz-se que um grupo G tem a* **propriedade do normalizador** *se todo subgrupo próprio de G está estritamente contido no seu normalizador.*

Assim, acabamos de provar que todo grupo nilpotente tem a propriedade do normalizador. Como consequência imediata temos o seguinte.

Corolário 4.13 *Todo subgrupo maximal de um grupo nilpotente é normal.*

Uma família de exemplos

Lembramos que um elemento x de um anel R diz-se **nilpotente** se existe um inteiro positivo n tal que $x^n = 0$. Um ideal J do anel R diz se um **ideal nilpotente** se existe um inteiro positivo n tal quer $J^n = 0$. O ideal J^n define-se como o ideal formado por todas as somas finitas de

produtos da forma $x_1x_2\ldots x_n$, com $x_i \in J$, $1 \leq i \leq n$, donde $J^n = 0$ se e somente se todos esses produtos são iguais a 0. O menor inteiro positivo n para o qual $J^n = 0$ chama-se o **índice de nilpotência** de R.

Dado um ideal bilateral nilpotente J, de índice n, num anel R. Definimos

$$G = 1 + J = \{1 + x \mid x \in J\}.$$

Observamos inicialmente que este conjunto é fechado em relação à multiplicação, pois dados $x, y \in J$ temos que

$$(1+x)(1+y) = 1 + x + y + xy, \quad \text{onde} \quad x + y + xy \in J.$$

Ainda, se $x \in J$ temos que $x^n = 0$ donde:

$$(1+x)\left(1 - x + x^2 - \cdots + (-1)^{n-1}x^{n-1}\right) = 1,$$

o que mostra que $1 + x$ é inversível, e seu inverso é

$$1 - x + x^2 - \cdots + (-1)^{n-1}x^{n-1} \in 1 + J.$$

As observações acima mostram que G é um grupo em relação à operação de multiplicação induzida por restrição da multiplicação de R.

Vamos mostrar que o grupo G assim definido é nilpotente. Para isso definimos indutivamente uma cadeia de subgrupos da seguinte forma:

$$G_0 = 1 + J, \quad G_1 = 1 + J^2, \quad \ldots \quad G_{i-1} = 1 + J^i, \quad \cdots$$

Note que $G_0 = G$ e que $G_{n-1} = 1$. Vamos mostrar que

$$1 = G_{n-1} \subset G_{n-2} \subset \cdots \subset G_0 = G$$

é uma série central para G.

De fato, como J é um ideal bilateral, segue facilmente que todos os ideais J^i são também bilaterais e, conseqüentemente, que os subgrupos G_i são normais em G, $0 \leq i \leq n-1$.

Afirmamos que para todo par de inteiros positivos i, j tem-se que

$$(G_i, G_j) \subset G_{i+j}.$$

De fato, dados $x \in J^i$ e $y \in J^j$ temos que:

$$\begin{aligned}(1+x,1+y) &= (1+x)^{-1}(1+y)^{-1}(1+x)(1+y)\\ &= ((1+y)(1+x))^{-1}(1+x)(1+y)\\ &= (1+y+x+yx)^{-1}(1+x+y+xy)\end{aligned}$$

Denotamos $y+x+yx=-u$ e $x+y+xy=-v$. Então $(1-u)^{-1} = 1+u+\cdots+u^{n-1}$ e

$$\begin{aligned}(1+x,1+y) &= (1+u+\cdots+u^{n-1})(1-v)\\ &= 1+u+\cdots+u^{n-1}-v-uv\cdots-u^{n-1}v\\ &= 1+(u-v)+u(u-v)+\cdots+u^{n-2}(u-v)\\ &= 1+(1+u+\cdots+u^{n-2})(u-v).\end{aligned}$$

Como $u-v=xy-yx$ temos que $u-v \in J^{i+j}$ donde $(1+x)(1+y) \in 1+J^{i+j}=G_{i+j}$, como tínhamos afirmado.

Note que, em particular, isto implica que

$$(G_{i-1},G) \subset G_i, \quad \text{donde} \quad \frac{G_{i-1}}{G_i} \subset \mathcal{Z}\left(\frac{G}{G_i}\right)$$

e segue que a série de subgrupos dada é uma série central para G.

Temos então que G é nilpotente e que sua classe de nilpotência é menor ou igual a $n-1$.

Um caso particularmente importante da situação acima é o seguinte. Seja K um anel comutativo, com unidade. Denotamos por $M_n(K)$ o anel das matrizes $n \times n$ com coeficientes em K e definimos

(i) $T(n,K) = \{A=(a_{ij}) \in M_n(K) \mid a_{ij}=0 \text{ se } i>j\}$, o **anel das matrices triangulares superiores de grau n sobre K.**

(ii) $J(n,K) = \{A=(a_{ij}) \in M_n(K) \mid a_{ij}=0 \text{ se } i>j\}$, o conjunto das matrizes $n \times n$ que têm zeros na diagonal principal e em toda posição abaixo dessa diagonal.

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

É muito fácil verificar que $J(n,K)$ é um ideal bilateral nilpotente do anel $T(n,K)$, cuja classe de nilpotência é n e que $UT(n,K) = 1 + J(n,K)$, donde $UT(n,K)$ é um grupo nilpotente de classe menor ou igual a $n-1$.

Se denotamos por $E_{i,j}$ a matriz que tem zeros em todas as posições, menos na posição i,j, onde o coeficiente é igual a 1, tem-se que:

$$(1 + E_{1,2}, 1 + E_{2,3}, \ldots, 1 + E_{n-1,n}) \;=\; 1 + E_{1,n} \;\neq\; 1,$$

o que mostra que a classe de nilpotência de $UT(n,K)$ é precisamente $n-1$.

Note que este exemplo mostra que *existem grupos de nilpotência de classe arbitrária.* Esta família de grupos pode ser usada para ilustrar outras situações interessantes de grupos nilpotentes. Veja o exercício 6 da seção 5.1.

5 Grupos nilpotentes finitos

Nossa intenção nesta seção é mostrar que existe, para os grupos nilpotentes finitos, um teorema de estrutura semelhante àquele que vale para grupos abelianos finitos.

Definição 5.1 *Diz-se que um grupo G tem a* **propriedade do normalizador** *se todo subgrupo próprio de G está estritamente contido no seu normalizador.*

Lembramos que um subgrupo H de um grupo G diz-se *subnormal* se existe uma cadeia de subgrupos:

$$H = H_0 \subset H_1 \subset \cdots \subset H_n = G$$

tal que $H_{i-1} \lhd H_i$, $1 \leq i \leq n$.

Como consequência da proposição acima temos o seguinte.

Corolário 5.2 *Seja G um grupo nilpotente finito. Então, todo subgrupo de G é subnormal.*

Demonstração. Seja H um subgrupo de G. Definimos $H_0 = H$ e, indutivamente, $H_n = N_G(H_{n-1})$. Da proposição anterior segue que se $H_{n-1} \neq G$ então $|H_{n-1}| < |H_n|$. Como G é finito, deve existir um índice n tal que $H_n = G$. □

Estamos agora em condições de dar um teorema de caracterização dos grupos nilpotentes finitos.

Teorema 5.3 *Seja G um grupo finito. Então, as seguintes condições são equivalentes.*

(i) *G é nilpotente.*

(ii) *G tem a propriedade do normalizador.*

(iii) *Todo subgrupo de Sylow de G é normal em G.*

(iv) *G é o produto direto dos seus subgrupos de Sylow.*

(v) *Todo subgrupo de G é subnormal.*

(vi) *Todo subgrupo maximal de G é normal.*

Demonstração. Vamos provar inicialmente que $(i) \Rightarrow (ii) \Rightarrow (iii) \Rightarrow (iv) \Rightarrow (i)$.

O fato de que $(i) \Rightarrow (ii)$ foi provado na Proposição 4.11.

$(ii) \Rightarrow (iii)$ Seja P um p-subgrupo de Sylow de G e seja $H = N_G(P)$. Se $H \neq G$ então (ii) implica que $H \subsetneq N_G(H)$, mas o Corolário 2.11 mostra que $H = N_G(H)$, logo deve ser $H = G$, donde $P \lhd G$.

$(iii) \Rightarrow (iv)$ Se cada subgrupo de Sylow é normal, segue imediatamente que o seu produto é direto e igual a G (verifique!).

$(iv) \Rightarrow (i)$ Como todo p-grupo é nilpotente, o resultado segue da Proposição 4.8.

Vamos mostrar agora que $(i) \Rightarrow (v) \Rightarrow (vi) \Rightarrow (i)$.

Novamente, o fato de que $(i) \Rightarrow (v)$ já foi provado na Proposição 5.2. Se vale (v) e H é maximal, segue imediatamente que ele deve ser normal, de modo que, claramente, $(v) \Rightarrow (vi)$.

Finalmente, para provar que $(vi) \Rightarrow (i)$ mostraremos que, se vale (vi), então todo subgrupo de Sylow de G é normal o que, como vimos acima, implica na nilpotência de G. De fato, seja P um subgrupo de Sylow de G. Se $N_G(P)$ é um subgrupo próprio de G, ele deve estar contido num subgrupo maximal H de G que, em virtude da hipótese (vi), é normal. Isto significa que $N_G(H) = G$, o que contradiz a Proposição 2.10. □

Note que o teorema acima mostra que se G é um grupo nilpotente de ordem $|G| = p_1^{n_1} \dots p_t^{n_t}$, denotando por $S(p_i)$, $1 \leq i \leq n$ os p_i-subgrupos de Sylow correspondentes, temos que

$$G = S(p_1) \times \cdots \times S(p_n).$$

Observe que este resultado é uma generalização do Teorema 2.13.

5.1 Grupos nilpotentes infinitos

Nesta seção procuraremos obter resultados sobre a estrutura dos grupos nilpotentes infinitos e estudaremos mais particularmente o caso em que os grupos em questão são finitamente gerados. Tentaremos mostrar que existe um certo paralelo entre estes resultados e aqueles que vimos para o caso dos grupos abelianos.

Proposição 5.4 *Seja $G = \langle a_1, \dots, a_r \rangle$ um grupo finitamente gerado. Então, o subgrupo $\gamma_i(G)$ é o fecho normal do subgrupo de G gerado por todos os comutadores da forma $(b_1, \dots, b_i)$ com $b_j \in \{a_1, \dots, a_r\}, 1 \leq j \leq i$; isto é, o subgrupo gerado por todos os possíveis conjugados desses comutadores.*

Demonstração. Vamos provar o enunciado por indução em i. Nossa afirmação é obviamente verdadeira se $i = 1$, de modo que vamos assumir, como hipótese de indução, que $\gamma_i(G)$ é o subgrupo

$$\gamma_i(G) = \langle (b_1, \dots, b_i)^g \mid b_j \in \{a_1, \dots, a_r\}, 1 \leq j \leq i,\ g \in G \rangle.$$

Então, consideramos

$$H = \langle (b_1, \ldots, b_{i+1})^g \mid b_j \in \{a_1, \ldots, a_r\}, 1 \leq j \leq i+1,\ g \in G \rangle.$$

Claramente $H \subset \gamma_{i+1}(G)$. Para provar a inclusão contrária, tendo em vista o Lema 3.3, será suficiente mostrar que $(\gamma_i(G), b_{i+1}) \subset H$, para qualquer elemento $b_{i+1} \in \{a_1, \ldots, a_r\}$. Mais uma vez, levando em consideração o Lema 3.3 e a hipótese de indução, é suficiente provar que

$$((b_1, \ldots, b_i)^g, b_{i+1}) \in H$$

para $b_j \in \{a_1, \ldots, a_r\}, 1 \leq j \leq i+1$ e $g \in G$ arbitrário. Note que a parte $(viii)$ do Lema 3.3 implica que é suficiente provar que

$$((b_1, \ldots, b_i)^a, b_{i+1}) \in H, \quad \text{com } a \in \{a_1, \ldots, a_r\}.$$

Finalmente, as partes (vii) e (ix) do mesmo lema mostram que

$$\begin{aligned} ((b_1, \ldots, b_i)^a, b_{i+1}) &= (b_1, \ldots, b_i, b_{i+1})^{(b_1, \ldots, b_i, a)} (b_1, \ldots, b_i, a, b_{i+1}) \\ &= (b_1, \ldots, b_i, b_{i+1})^{(b_1, \ldots, b_i, a)} (b_1, \ldots, b_i, a)^{-1} \\ &\qquad (b_1, \ldots, b_i, a)^{b_{i+1}} \end{aligned}$$

donde $((b_1, \ldots, b_i)^a, b_{i+1}) \in H$ como queríamos demonstrar. □

Proposição 5.5 *Seja $G = \langle a_1, \ldots, a_r \rangle$ um grupo finitamente gerado. Então, para cada índice $i \geq 1$, o fator $\gamma_i(G)/\gamma_{i+1}(G)$ é gerado pelo conjunto finito de elementos $(b_1, \ldots, b_i)\gamma_{i+1}(G)$, onde $b_j \in \{a_1 \ldots, a_r\}$.*

Demonstração. Os elementos de $\gamma_i(G)$ são produtos de elementos da forma $(b_1, \ldots, b_i)^g$ com $b_j \in \{a_1, \ldots, a_r\}, 1 \leq j \leq i,\ g \in G$. Logo, as respectivas classes destes elementos são geradores do quociente $\gamma_i(G)/\gamma_{i+1}(G)$. Como

$$\begin{aligned} (b_1, \ldots, b_i)^g &= (b_1, \ldots, b_i)(b_1, \ldots, b_i)^{-1} g^{-1} (b_1, \ldots, b_i) g \\ &= (b_1, \ldots, b_i)(b_1, \ldots, b_i, g) \end{aligned}$$

e como

$$(b_1, \ldots, b_i, g) \in \gamma_{i+1}(G),$$

temos que

$$(b_1, \ldots, b_i)^g \gamma_{i+1}(G) \;=\; (b_1, \ldots, b_i)\gamma_{i+1}(G).$$

Isto implica o resultado. □

Corolário 5.6 *Todo subgrupo de um grupo nilpotente finitamente gerado é finitamente gerado.*

Demonstração. Seja H um subgrupo de um grupo nilpotente finitamente gerado G com série central inferior

$$G = \gamma_1(G) \supset \gamma_2(G) \supset \cdots \supset \gamma_s(G) = \{1\}.$$

Seja $H_i \;=\; H \cap \gamma_i(G)$, $1 \leq i \leq s$. Então

$$H = H_1 \supset H_2 \supset \cdots \supset H_s = \{1\},$$

onde

$$\frac{H_i}{H_{i+1}} = \frac{H \cap \gamma_i(G)}{H \cap \gamma_{i+1}(G)}.$$

Note que a aplicação $\varphi : H_i/H_{i+1} \to \gamma_i(G)/\gamma_{i+1}(G)$ dada por $h(H \cap \gamma_{i+1}(G)) \mapsto h\gamma_{i+1}(G)$ está bem definida, pois independe do representante. Por outro lado, é fácil provar que ela é injetiva, de modo que H_i/H_{i+1} é isomorfo a um subgrupo de $\gamma_i(G)/\gamma_{i+1}(G)$, que é um grupo abeliano finitamente gerado. Logo H_i/H_{i+1} também é finitamente gerado, pelo Corolário 2.21, $1 \leq i \leq s-1$. Como cada fator da série

$$H = H_1 \supset H_2 \supset \cdots \supset H_s = \{1\},$$

é finitamente gerado, segue que o próprio H é finitamente gerado. □

Este resultado não é verdadeiro em geral. O leitor familiarizado com o conceito de grupo livre encontrará um contra-exemplo no exercício 11, no final desta seção.

Lema 5.7 (P. Hall [8]) *Seja G um grupo nilpotente.*

(i) Se $a \in \gamma_i(G)$ e $b \in G$ então $(a, b^n) \;\equiv\; (a, b)^n \;\; (mod\ \gamma_{i+2}(G))$.

(ii) Se G é gerado por um número finito de elementos de ordem finita, então os fatores $\gamma_i(G)/\gamma_{i+1}(G)$ são finitos, para todo $i \geq 1$.

Demonstração. (i) Segue, da parte (v) do Lema 3.3 que $(a, b^2) = (a, b)(a, b)(a, b, b)$. Como $(a, b, b) = ((a, b), b)$ e $(a, b) \in \gamma_{i+1}(G)$ é central módulo $\gamma_{i+2}(G)$, temos que $(a, b^2) \equiv (a, b)^2 \pmod{\gamma_{i+2}(G)}$.

Indutivamente, obtemos também que $(a, b^n) \equiv (a, b)^n \pmod{\gamma_{i+2}(G)}$, o que prova o enunciado.

(ii) Vamos provar esta afirmação por indução em i. Suponha que $G = \langle a_1, \ldots, a_r \rangle$, onde cada a_j tem ordem finita. Para $i = 1$ temos que $\gamma_1(G)/\gamma_2(G)$ é gerado pelas classes $a_j\gamma_2(G)$, $1 \leq j \leq r$ dos geradores de G, que obviamente são de ordem finita. Como $\gamma_1(G)/\gamma_2(G)$ é abeliano, também é finito.

Assim, suponhamos que $\gamma_i(G)/\gamma_{i+1}(G)$ é finito. O fator $\gamma_{i+1}(G)/\gamma_{i+2}(G)$ é gerado por elementos da forma $(b_1, \ldots, b_{i+1})\gamma_{i+2}(G)$ onde $b_j \in \{a_1, \ldots, a_r\}$. Seja $n = o(b_{i+1})$. Então, da parte (i), temos que

$$(b_1, \ldots, b_{i+1})^n \equiv (b_1, \ldots, b_{i+1}^n) \equiv 1 \ (mod \ \gamma_{i+2}(G)) .$$

Isto mostra que $\gamma_{i+1}(G)/\gamma_{i+2}(G)$ é um grupo abeliano, finitamente gerado por elementos de ordem finita e, portanto, é finito. □

Agora estamos em condições de provar que vale, para os grupos nilpotentes, um resultado análogo ao Teorema 2.20 demonstrado para grupos abelianos.

Teorema 5.8 *Seja G um grupo nilpotente. Então, temos que*

(i) O conjunto T de elementos de ordem finita de G é um subgrupo totalmente invariante.

(ii) O quociente G/T é sem torção.

(iii) Para cada inteiro primo p tal que G contém elementos de ordem p, existe um único p-subgrupo maximal T_p de T e T é o produto direto de todos estes subgrupos.

Demonstração. Sejam x, y dois elementos de ordem finita em G e seja $H = \langle x, y \rangle$. Então, na série central inferior

$$H = \gamma_1(H) \supset \gamma_2(H) \supset \cdots \supset \gamma_n(H) = \{1\}$$

todos os fatores são finitos pelo Lema 5.7. Logo, H é finito e, conseqüentemente, $xy \in H$ é um elemento de ordem finita, como queríamos demonstrar.

O fato de que T é totalmente invariante e G/T é sem torção segue de um cálculo imediato.

Para provar a nossa última afirmação vamos mostrar que o produto de dois p-elementos é novamente um p-elemento, o que implicará que T_p é um subgrupo. Assim, sejam $a, b \in G$ p-elementos. Como vimos acima, $\langle a, b\rangle$ é finito e, como é um subgrupo de G, ele é nilpotente. Pelo Teorema 5.3 sabemos que $\langle a, b\rangle$ é o produto direto dos seus subgrupos de Sylow e, como a e b pertencem ambos ao único p-subgrupo de Sylow de $\langle a, b\rangle$, segue que o seu produto também é um p-elemento.

O resto da nossa afirmação é de demonstração simples, que deixamos como exercício para o leitor. □

A seguir, vamos refinar estes resultados para o caso em que G, além de ser nilpotente, é finitamente gerado. Veremos que, nessa hipótese, será possível obter bem mais informação sobre a estrutura do grupo. Começamos com uma observação simples, que é uma conseqüência direta de resultados anteriores.

Corolário 5.9 *Seja G um grupo nilpotente, finitamente gerado. Então $T(G)$ é um grupo finito.*

Demonstração. De acordo com o Corolário 5.6, $T(G)$ é um grupo finitamente gerado e a parte (ii) do Lema 5.7 mostra diretamente que, nestas condições, ele é finito. □

Lema 5.10 *Seja G um grupo com série central superior*

$$\{1\} = \zeta_0(G) \subset \zeta_1(G) \subset \cdots \subset \zeta_n(G) \subset \cdots .$$

Se $\zeta_1(G) = \zeta(G)$, o centro de G, é sem torção, então cada fator $\zeta_{i+1}(G)/\zeta_i(G)$ é sem torção.

Demonstração. Mais uma vez, faremos indução em i. Note que a afirmação é verdadeira para $\zeta_1(G)/\zeta_0(G)$ por hipótese. Suponhamos então que os fatores

$$\zeta_1(G)/\zeta_0(G), \ldots, \zeta_i(G)/\zeta_{i-1}(G)$$

são livres de torção.

Queremos provar que $\zeta_{i+1}(G)/\zeta_i(G)$ também é sem torção. Suponhamos, por absurdo, que existem um elemento $x \in \zeta_{i+1}(G)$ e um inteiro positivo m tais que $x^m \in \zeta_i(G)$. Seja g um elemento arbitrário de G. Então $(g,x) \in \zeta_i(G)$ e, pela parte (iii) do Lema 3.3, temos que

$$(g,x)^m \equiv (g,x^m) \equiv 1 \pmod{\zeta_{i-1}(G)}.$$

Então, da hipótese de indução vem que

$$(g,x) \in \zeta_{i-1}(G), \quad \forall g \in G,$$

o que mostra que $x \in \zeta_i(G)$.

Já provamos que, se $x \in \zeta_{i+1}(G)$ é tal que $\overline{x}^m = 1$ em $\zeta_{i+1}(G)/\zeta_i(G)$, então $\overline{x} = 1$, donde $\zeta_{i+1}(G)/\zeta_i(G)$ é sem torção, como afirmamos. □

Corolário 5.11 *Se G é um grupo nilpotente sem torção então todos os fatores de sua série central superior também são livres de torção. Mais ainda, se G é finitamente gerado então G admite uma série central*

$$\{1\} = G_0 \subset G_1 \subset \cdots \subset G_n = G$$

tal que todos os seus fatores são grupos cíclicos infinitos.

Demonstração. A primeira parte da nossa afirmação segue imediatamente do lema acima. Agora, se G é finitamente gerado, então cada fator central $\zeta_i(G)/\zeta_{i-1}(G)$ é finitamente gerado e sem torção; logo, pode ser escrito como o produto direto de um número finito de grupos cíclicos infinitos. Segue então que a série central superior pode ser refinada a uma série cental ascendente onde cada fator é cíclico infinito. □

Definição 5.12 *Um grupo G diz-se* **ordenado** *se existe uma relação $\leq$ definida em G tal que:*

(i) $g \leq g$ para todo elemento $g \in G$.

(ii) *Se* $g \leq h$ *e* $h \leq g$ *então* $g = h$.

(iii) *Se* $g \leq h$ *e* $h \leq k$ *então* $g \leq k$.

(iv) *Dados* $g, h \in G$ *tem-se que* $g \leq h$ *ou* $h \leq g$.

(v) *Dados* $g, h \in G$ *tais que* $g \leq h$, *para todo* $a \in G$ *tem-se que* $ag \leq ah$ *e* $ga \leq ha$.

As condições (i) a (iii) da definição acima dizem que $\leq$ é uma relação de ordem, a condição (iv) diz que essa ordem é *total* e, finalmente, a condição (v) estabelece que a ordem é *compatível, à direita e à esquerda*, com a operação do grupo. Naturalmente, escreveremos $g < h$ para indicar que $g \leq h$ mas $g \neq h$.

Um exemplo simples de grupo ordenado é o grupo cíclico infinito. De fato, seja $G = \langle a \rangle$. Dados $x, y \in G$ podemos escrever univocamente $x = a^i$ e $y = a^j$, com i, j números inteiros. Dizemos então que $x \leq y$ se e somente se $i \leq j$.

Se G é um grupo abeliano livre e finitamente gerado então, de acordo com o Teorema 2.19, ele é da forma $G \simeq C \times \cdots \times C$, onde C denota um grupo cíclico infinito e o número de fatores diretos é igual ao posto de G. Se denotamos por $a_1, \ldots a_n$ os geradores destes grupos cíclicos, dados dois elementos $x, y \in G$ podemos escrever:

$$x = a_1^{t_1} \cdots a_n^{t_n} \quad \text{e} \quad y = a_1^{s_1} \cdots a_n^{s_n}.$$

Então, podemos ordenar G *lexicograficamente* da seguinte forma: dados $x \neq y$ em G, se i é o primeiro índice para o qual $t_i \neq s_i$, então diz-se que $x < y$ se $t_i < s_i$.

A próxima proposição exibe mais um exemplo de grupo ordenado.

Proposição 5.13 *Seja* G *um grupo nilpotente, finitamente gerado, sem torção. Então* G *pode ser ordenado.*

Demonstração. Sabemos, do Corolário 5.11 que G admite uma série central

$$\{1\} = G_0 \subset G_1 \subset \cdots \subset G_n = G$$

tal que todos os seus fatores são grupos cíclicos infinitos. Como observado acima, isto implica que cada um dos fatores G_i/G_{i-1} é ordenado.

Note que, dado um elemento arbitrário $g \in G$, como $G_0 = \{1\}$ e $G_n = G$, deve existir um índice i tal que $g \in G_i$ mas $g \notin G_{i-1}$. Podemos definir então uma ordem em G da seguinte forma: dados $x \neq y$ em G, determinamos primeiro índices i e j tais que

$$x \in G_i \setminus G_{i-1} \quad \text{e} \quad y \in G_j \setminus G_{j-i}.$$

Dizemos então que $x < y$ se $i < j$ ou, no caso em que $i = j$, se $\overline{x} < \overline{y}$ em G_i/G_{i-1}. É facil verificar diretamente que esta é uma ordem em G. □

Agora, o Corolário 5.9 e a Proposição 5.13 permitem obter imediatamente uma versão mais precisa do Teorema 5.8 sobre a estrutura de um grupo nilpotente G, no caso em que ele é finitamente gerado.

Teorema 5.14 *Seja G um grupo nilpotente finitamente gerado. Então $T(G)$ é um grupo finito e $G/T(G)$ é ordenado.*

Finalmente, vamos mostrar que vale um resultado que, de certa forma, é "dual" do anterior; se G é nilpotente, finitamente gerado, então ele contém um subgrupo característico, sem torção H, tal que o quociente G/H é finito (veja o Teorema 5.23). Para isso, mais uma vez precisaremos demonstrar antes vários lemas técnicos.

Começamos exibindo mais uma situação em que subgrupos de grupos finitamente gerados são finitamente gerados.

Proposição 5.15 *Um subgrupo H de índice finito de um grupo finitamente gerado G é finitamente gerado.*

Demonstração. Seja $G = \langle g_1, \ldots, g_n \rangle$, e seja $\{1 = h_1, h_2, \ldots, h_s\}$ um conjunto completo de representantes de classes laterais à esquerda de H em G. Para cada par de índices i, j, o conjunto $g_i h_j H$ é novamente uma classe lateral à esquerda de H em G, portanto existe um índice j'tal que $g_i h_j H = h_{j'} H$. Note que isto significa que a aplicação $j \mapsto j'$ é uma permutação do conjunto $\{1, \ldots, s\}$ e existe um elemento $h_{i,j} \in H$ tal que $g_i h_j = h_{j'} h_{i,j}$. Definimos

$$K = \langle h_{i,j} \mid 1 \leq i \leq n,\ 1 \leq j \leq s \rangle.$$

Claramente, K é um subgrupo de H. Seja $X = \cup_{j=1}^{s} h_j K$. Então, para cada índice i temos que

$$g_i X = \cup_{j=1}^{s} g_i h_j K = \cup_{j=1}^{s} h_{j'} h_{i,j} K = \cup_{j=1}^{s} h_{j'} K,$$

pois $h_{i,j} \in K$. Logo $X = g_i X$ para cada índice i, donde $X = GX = G$. Agora, $H \subset G = \cup_{j=1}^{s} h_j K$ e, como H é disjunto de $h_j H$ se $j \neq 1$, temos que $H \subset h_1 K$. Segue imediatamente que $H = K$, que é finitamente gerado. □

Lema 5.16 *Seja G um grupo finitamente gerado e seja $n \geq 1$ um inteiro fixo. Então G contém somente um número finito de subgrupos cujo índice é menor o igual a n.*

Demonstração. Seja H um subgrupo de G com $(G : H) \leq n$ e seja $\{H_1, \ldots, H_m\}$ o conjunto de classes laterais à direita de H em G. Dado um elemento $g \in H$, temos que $\{H_1 g, \ldots, H_m g\}$ é novamente o conjunto de classes laterais à direita de H em G. Denotamos então $H_i g = H_{\sigma_g(i)}$. A aplicação $g \to \sigma_g$ é um homomorfismo de grupos de G em S_m e claramente $Ker(\sigma) \subset H$. Então $H = \sigma^{-1}(W)$ para algum subgrupo W de S_m.

Como σ é determinado pelas imagens dos geradores de G, que são em número finito, vemos que existe apenas um número finito de aplicações $\sigma : G \to S_m$ e, como S_m contém apenas um número finito de subgrupos, segue o resultado. □

Definição 5.17 *Seja $\mathcal{X}$ uma classe de grupos. Um grupo G diz-se* **poli-$\mathcal{X}$** *se G contém uma série subnormal*

$$\{1\} = G_0 \triangleleft G_1 \triangleleft \cdots \triangleleft G_n = G$$

tal que cada fator G_i/G_{i-1}, $1 \leq i \leq n$, pertence à classe $\mathcal{X}$.

Mostramos na Proposição 3.13 que grupos solúveis finitos são policíclicos (donde isto também vale para grupos nilpotentes finitos). Também, o Teorema 5.8 mostra que se G é um grupo nilpotente finitamente gerado, então $G/T(G)$ é poli-(cíclico infinito). Segue então imediatamente que *um grupo nilpotente finitamente gerado é policíclico.*

Num dos artigos de uma série em que investigava grupos solúveis noetherianos (i.e., grupos solúveis nos quais toda família de subgrupos contém um maximal), K.A. Hirsch [11] provou que tais grupos possuem uma série subnormal em que todos os fatores são cíclicos, embora não lhes desse um nome particular. O termo *policíclico*, mais uma vez, é devido a P. Hall [9].

Lema 5.18 *Seja $\mathcal{X}$ uma classe de grupos. Se $\mathcal{X}$ é fechada para subgrupos (isto é, se $G \in \mathcal{X}$ implica que $H \in \mathcal{X}$ para todo subgrupo H de G), então a classe dos grupos poli-$\mathcal{X}$ também é fechada para subgrupos.*

Demonstração. Seja

$$\{1\} = G_0 \lhd G_1 \lhd \cdots \lhd G_n = G$$

uma série subnormal tal que $G_i/G_{i-1} \in \mathcal{X}$, $1 \leq i \leq n$, e seja H um subgrupo de G. Então

$$\{1\} = G_0 \cap H \lhd (G_1 \cap H) \lhd \cdots \lhd (G_n \cap H) = H$$

é uma série subnormal para H e

$$\frac{G_i \cap H}{G_{i-1} \cap H} \simeq \frac{G_{i-1}(H \cap G_i)}{G_{i-1}}$$

que é um subgrupo de G_i/G_{i-1}. Como $\mathcal{X}$ é fechada para subgrupos, temos que $(G_i \cap H)/(G_{i-1} \cap H) \in \mathcal{X}$, donde segue a tese. □

Vamos precisar do seguinte resultado elementar.

Lema 5.19 *Sejam H e K subgrupos de índice finito de um grupo G. Então:*

$$(G : H \cap K) \leq (G : H)(G : K).$$

Demonstração. Vamos denotar por L_H, L_K e L os conjuntos de classes laterais à esquerda de H, K e $H \cap K$ em G respectivamente.

Definimos uma aplicação $\phi : L \to L_H \times L_K$ por $x(H \cap K) \mapsto (xH, xK)$ e afirmamos que esta aplicação é injetora. De fato, se $(xH, xK) = (yH, yK)$ para algum $x, y \in G$, temos que $xH = yH$ e $xK = yK$ donde $y^{-1}x \in H \cap K$ e portanto $x(H \cap K) = y(H \cap K)$.

A injetividade de ϕ implica que $|L| \leq |L_H||L_K|$ logo $(G : H \cap K) \leq (G : H)(G : K)$, como afirmado. □

Usando indução segue imediatamente o seguinte resultado.

Lema 5.20 (Poincaré) *A interseção de um número finito de subgrupos de índice finito num grupo G é de índice finito em G.*

O seguinte resultado será necessário no decorrer da prova do nosso próximo teorema.

Lema 5.21 *Seja N um subgrupo normal de um grupo G tal que G/N é finito ou cíclico infinito. Se N contém um subgrupo característico H, de índice finito, tal que H é poli-(cíclico infinito), então G contém um subgrupo normal W que é, ele próprio, poli-(cíclico infinito).*

Demonstração. Como H *car* N e $N \triangleleft G$ temos que $H \triangleleft G$. Sejam $K_1 = G/H$ e $K_2 = N/H$. Se G/N é fnito, então o próprio H é um subgrupo nas condições do enunciado.

Se G/N é cíclico infinito, então

$$\frac{K_1}{K_2} \simeq \frac{G/H}{N/H} \simeq \frac{G}{N},$$

donde K_1/K_2 também é cíclico infinito.

Dado um elemento $x \in G$, denotaremos por x_0 sua classe em K_1 e por $\overline{x_0}$ a classe de x_0 em K_1/K_2. Como acabamos de provar que este último grupo é cíclico infinito, segue que existe $g \in G$ tal que $K_1/K_2 = \langle \overline{g_0} \rangle$ donde, em particular, temos que g é um elemento de G de ordem infinita e que $K_1 = \langle K_2, g_0 \rangle$.

Como H é de índice finita em N, temos que K_2 é finito. Ainda, como a conjugação por g_0 induz um automorfismo de K_2, que deve ser de ordem finita, segue que existe um inteiro positivo t tal que g_0^t centraliza K_2. Temos então que $\langle g_o^t \rangle$ é um subgrupo central de K_1.

Sejam então $W = \langle N, g^t \rangle$ e $\overline{W} = \langle K_2, g_0^t \rangle$. Como $K_2 \triangleleft K_1$ temos que $\overline{W} \triangleleft K_1$, donde $W \triangleleft G$.

Finalmente, note que $W/N \simeq \langle g^t \rangle$ é cíclico infinito e, como N é poli-(cíclico infinito) segue que W também o é. □

Teorema 5.22 *Seja G um grupo poli-(finito ou cíclico). Então, G contém um subgrupo característico H tal que $H = \{1\}$ ou é poli-(cíclico infinito) e tal que G/H é finito.*

Demonstração. Seja

$$\{1\} = G_0 \triangleleft G_1 \triangleleft \cdots \triangleleft G_n = G$$

uma série subnormal tal que cada fator G_i/G_{i-1} é finito ou cíclico. Vamos provar, por indução em i, que cada subgrupo G_i contém um subgrupo característico H_i, de índice finito, que é poli-(cíclico infinito), $1 \leq i \leq n$.

O resultado é verdadeiro se $i = 1$. De fato, temos que G_1 é finito ou cíclico infinito. No primeiro caso, tomamos $H = \{1\}$ e, no segundo, tomamos $H = G_1$.

Assim, vamos assumir, por indução, que um tal subgrupo H_i existe em G_i. Do lema anterior, sabemos que existe $W \triangleleft G_{i+1}$, de índice finito e tal que W é poli-(cíclico infinito). Por outro lado, como é claro que G_{i+1} é finitamente gerado, o Lema 5.16 nos diz que existe apenas um número finito de subgrupos de G_{i+1} cujo índice é igual a $(G_{i+1} : W)$.

Seja H_{i+1} a interseção de todos estes subgrupos. Então H_{i+1} é necessariamente característico e segue do Lema 5.20 (de Poincaré) que ele é de índice finito.

Da própria definição de H_{i+1} temos que $H_{i+1} \subset W$ de modo que o Lema 5.18 mostra que H_{i+1} é poli-(cíclico infinito), o que completa a demonstração. □

Como consequência imediata, temos o seguinte.

Teorema 5.23 *Um grupo nilpotente finitamente gerado G contém um subgrupo característico H que é sem torção (na verdade, é poli-(cíclico infinito)) e tal que G/H é finito.*

Exercícios

1. Seja G um grupo finito nilpotente de ordem n. Prove que, para cada divisor d de n, G contém um subgrupo de ordem d.

2. Seja H um subgrupo de um grupo finito nilpotente G. Definimos $N_1 = N_G(H)$ e, indutivamente, $N_i = N_G(N_{i-1})$. Prove que existe um inteiro positivo k tal que $N_k = G$.

3. Seja G um grupo nilpotente. Prove que todo subgrupo maximal próprio H de G é normal e que $(G : H)$ é um número primo.

4. Mostre que, se um grupo G é tal que $G/\mathcal{Z}(G)$ é nilpotente, então G é nilpotente.

5. Mostre que um grupo nilpotente finito tem uma série central cujos fatores são de ordem prima.

6. Seja K um corpo e $UT(n, K)$ o grupo linear unitriangular superior de grau $n > 1$ sobre K. Mostre que:

   (i) Se K é um corpo infinito, de característica prima p e t é um inteiro positivo tal que $p^t > n$, então $UT(n, K)$ é um grupo infinito, de torção e todos seus elementos tem ordem divisor de p^t.

   (ii) Se K é de característica 0, então $UT(2, K)$ é um grupo nilpotente, sem torção.

7. Seja G um grupo nilpotente infinito que é finitamente gerado. Prove que $\mathcal{Z}(G)$ contém em elemento de ordem infinita.

8. Seja
$$\{1\} = G_0 \subset G_1 \subset \cdots \subset G_n = G$$
uma série central de um grupo G tal que todos os seus fatores são grupos cíclicos infinitos e seja $u_i \in G$ um elemento tal que $G_i/G_{i-1} = \langle \overline{u_i} \rangle$, $1 \leq i \leq n$. Prove que todo elemento $g \in G$ pode-se escrever de modo único na forma
$$g = u_1^{a_1} \cdots u_n^{a_n},$$
onde $a_1, \ldots a_n$ são inteiros.

   Utilize esta representação para provar que um grupo nilpotente, finitamente gerado, sem torção, é ordenado.

9. Seja $G = \langle a, x \mid a^9 = 1,\ x^{-1}ax = a^7 \rangle$. Determine $\mathcal{Z}(G), G', T(G)$ e prove que G é nilpotente de classe 2. Mostre que não é possível escrever
$$G \simeq T(G) \times \frac{G}{T(G)}.$$

10. Prove que o conjunto de elementos de ordem finita do *grupo diedral infinito*
$$D_\infty = \langle x, y \mid y^2 = 1,\ x^y = x^{-1} \rangle$$
não é um subgrupo.

11. Seja F um grupo livre com dois geradores a e b. Prove que o conjunto de elementos $\{a, a^b, a^{b^2}, \ldots, a^{b^n}, \ldots\}$ gera um grupo livre.

12. Seja $\mathcal{X}$ uma classe de grupos que é fechada para imagens homomorfas. Prove que a classe dos grupos poli-$\mathcal{X}$ também é fechada para imagens homomorfas.

13. Seja $\pi = \{p_1, \ldots, p_n\}$ um conjunto finito de inteiros primos. Um grupo G diz-se *π-livre* se para todo elemento $g \in G$ e todo primo $p \in \pi$ temos que $g^p = 1$ implica $g = 1$. Prove que se o centro de um grupo é π-livre então os fatores da série central superior também são π-livres.

Referências

[1] Burnside, W., *The theory of groups of finite order*, 2nd ed., Cambridge Univ. Press, Cambridge, 1911.

[2] Cayley, A., On the theory of groups as depending on the symbolic equation $\theta^n = 1$, *Phil. Mag.*, **7** (1854), 40-47.

[3] Chandler, B. e Magnus, W., *The History of Combinatorial Group Theory: a case study in the History of Ideas*, Springer-Verlag, New York, 1982.

[4] Dedekind, R., Über Gruppen, deren sämtliche Teiler Normalteiler sind., *Math. Annalen*, **48** (1897), .

[5] Fite, W.B., Groups whose orders are powers of a prime, *Trans. Amer. Math. Soc.*, **7** (1906), 61-68.

[6] Frobenius, F.G., Über Endliche Gruppen, *Sitzungsberichte d. K. Press. Akad. d. Wissensch. Berlin*, (1895), 81-112.

[7] Hall, M. *The Theory of Groups*, MacMillan, New York, 1959.

[8] Hall, P., A contribution to the theory of groups of prime power order, *Proc. London Math. Soc.*. **36** (1933), 29-95.

[9] Hall, P., Finiteness conditions for soluble groups, *Proc. London Math. Soc.*, **4** (1954), 419-436.

[10] Hall, P., *The Edmonton notes on nilpotent groups*, Queen Mary College Mathematical Notes, 1969.

[11] Hirsch, K.A. On infinite soluble groups I, *Proc. London Math. Soc.*, **44** (1938), 53-60.

[12] Jordan, C., *Sur le nombre des valeurs des fonctions*, Tese, Paris, 1860.

[13] Jordan, C., *Traité des substitutions et des équations algébriques*, Paris, 1870.

[14] Miller, G.A., *Quarterly J. of Math.*, **28** (1896), .

[15] Miller, G.A., History of the theory of groups to 1900, *The Collected works of George Abraham Miller*, Vol. 1, No 62, Univ. of Illinois, Urbana, 1935, pp. 427-467.

[16] Polcino Milies, C. e Sehgal, S.K., *An Introduction to Group Rings*, Kluwer Acad. Publishers, Dordrecht, 2002.

[17] Levi, F., Über die Untergruppen der freien Gruppen, *Math. Z.*, **37** (1933), 90-97.

[18] Robinson, D.J.S., *A course in the Theory of Groups*, Springer-Verlag, New York, 1982.

[19] Rotman, J.J., *The Theory of Groups: an introduction*, 2nd ed., Allyn and Bacon, Boston, 1973.

[20] Scott, W.R., Group Theory, Prentice-Hall, Englewood Clffs, N.J., 1964.

[21] Sylow, L., Théorèmes sur les groupes des substitutions, *Math. Annalen*, **5** (1872), 584-594.

[22] Weber, H., *Lehrbuch der Algebra*, 2 vols., Vieweg & Sohn, Braunschweig II.14, 1894.

[23] Wielant, H., Zum Satz von Sylow. *Math. Z.*, **60** (1954), 407-408.

Instituto de Matemática e Estatística
USP Rua do Matão, 1010
CEP 05508-090
São Paulo Brasil
polcino@ime.usp.br