Universidade Federal de Campina Grande
Centro de Ciências e Tecnologia
Unidade Acadêmica de Matemática
Curso de Graduação em Matemática

Nilpotência e p-Nilpotência de Grupos Finitos

por

Thiago Felipe da Silva

sob orientação do

Prof. Dr. Antônio Pereira Brandão Júnior

Campina Grande - PB
Abril, 2015

Universidade Federal de Campina Grande
Centro de Ciências e Tecnologia
Unidade Acadêmica de Matemática
Curso de Graduação em Matemática

Thiago Felipe da Silva

Nilpotência e p-Nilpotência de Grupos Finitos

Trabalho apresentado ao Curso de Graduação em Matemática da Universidade Federal de Campina Grande como requisito para a obtenção do título de Bacharel em matemática.

Orientador: Prof. Dr. Antônio Pereira Brandão Júnior

Campina Grande - PB, Abril de 2015
Curso de Matemática, modalidade Bacharelado

Nilpotência e p-Nilpotência de Grupos Finitos

Thiago Felipe da Silva

Trabalho de conclusão de curso defendido em 13 de abril de 2015, pela Comissão Examinadora constituída pelos professores:

Prof. Dr. Antônio Pereira Brandão júnior
Orientador

Profª. Ma. Miriam Costa
Examinadora

com nota igual a:

Dedicatória

In memoriam a meu pai Emanuel Joaquim da Silva.

Agradecimentos

A Deus, sou grato por definição, uma vez que ele é o responsável não só por essa conquista em minha vida e sim pela existência dela, por esse motivo omitirei seu nome em minha lista de agradecimento.

Existem pessoas na vida que é sempre um motivo de orgulho e de prestígio poder dizer que somos seus amigos, a felicidade de citar os nomes de algumas delas ameniza o sentimento de injustiça das que agora esqueço.

De coração extasiado de felicidade agradeço;

Aos meus pais que me ensinaram, não com palavras e sim com gestos, a enfrentar a vida com equidade e honradez, fazendo da justiça o meu forte brasão.

Aos meus digníssimos irmãos, e em especial à minha amorável irmã Fabiana da Silva.

Ao Meu fiel e cortês amigo Carlos André e família, em especial ao seu nobre irmão Edivan Silva e à vossa equânime mãe Maria José, que fora minha professora no primário.

Ao meu respeitável e inesquecível professor Josenildo da Cunha Lima.

Aos meus autênticos, íntegros e engraçados amigos Ivan Sérgio e Adriano Dantas, muitos foram os bons momentos que vivemos juntos.

A todos os integrantes do grupo Pet-matemática, simplesmente essas pessoas mudaram a minha vida.

Ao meu Afável, íntegro, meigo,..., todos os adjetivos acima + todos do Aurélio, Professor, tutor e amigo Daniel Cordeiro de Morais Filho. Nunca esquecerei de seus ensinamentos.

Ao meu professor e orientador, do presente trabalho, Antônio Pereira Brandão Júnior, esse antecede sua fama e seu título de doutorado, se não fosse questão de estética o prefixo Dr. viria após o seu nome.

O brado latente sem sentido
O rugido fugaz sem esperança
Traduz a vida sem lembrança
Se nesta não se apinha amigo
(Thiago Felipe)

Obrigado!

Resumo

Nosso trabalho é dedicado ao estudo de nilpotência e p-nilpotência de grupos finitos. Inicialmente, apresentaremos a definição e propriedades básicas de grupos nilpotentes, bem como a caracterização dos grupos nilpotentes finitos. No estudo de p-nilpotência, veremos a sua relação com o conceito de nilpotência e usaremos o *Homomorfismo Transfer* com o intuito de obter o importante *Critério de Burnside*, o qual apresenta uma condição suficiente para que um grupo finito seja p-nilpotente, onde p é um divisor primo de sua ordem. Por fim, apresentaremos algumas aplicações do Critério de Burnside.

Abstract

Our work is dedicated to the study of nilpotency and p-nilpotency of finite groups. Initialy, we will present the definition and basic properties of nilpotent groups, as well as characterization of finite nilpotent groups. In the study of p-nilpotency, we will see its relation with the concept of nilpotency and use the *Transfer Homomorphism* with the goal of obtaining the important *Burnside's Criterion*, which presents a suficient condition for a finite group to be p-nilpotent, where p is a prime divisor of its order. At last, we will show some applications of the Burnside's Criterion.

Sumário

Introdução

Sejam G um grupo finito e p um divisor primo de $|G|$. Um subgrupo de G cuja ordem é a maior potência de p que divide $|G|$ é dito um *p-subgrupo de Sylow de G* (a existência de um tal subgrupo é garantida pelo Primeiro Teorema de Sylow). Dizemos que G é *p-nilpotente* se existe algum subgrupo normal K de G tal que $KP = G$ e $K \cap P = \{e\}$, onde P é um p-subgrupo de Sylow de G. Um subgrupo K nestas condições é dito um *p-complemento normal em G* e satisfaz $|K| = |G : P| = |G|/|P|$.

Dizemos que um grupo G é *nilpotente* se possui uma série central de subgrupos, ou seja, uma série

$$\{e\} = N_0 \leq N_1 \leq N_2 \leq ... \leq N_{n-1} \leq N_n = G$$

onde cada N_i é um subgrupo normal de G e $N_{i+1}/N_i \subseteq Z(G/N_i)$ (o centro de G/N_i) para todo $i = 0, 1, ..., n-1$. Os conceitos de nilpotência e p-nilpotência estão bastante relacionados, uma vez que um grupo finito é nilpotente se, e somente se, é p-nilpotente para todo divisor primo p de sua ordem.

Motivado pela importância dos conceitos de nilpotência e p-nilpotência de grupos finitos, o presente trabalho tem como objetivo fazer um estudo introdutório desses conceitos, além de apresentar o *homomorfismo transfer* como ferramenta no estudo da p-nilpotência.

O homomorfismo transfer foi introduzido em [1] por W. Burnside, que logo depois desenvolveu a ideia e a usou para provar o que hoje chamamos de *Teorema do Transfer de Burnside*, o qual pode ser encontrado em [2] e segue enunciado a seguir:

Teorema do Transfer de Burnside. *Seja G um grupo finito. Se para algum primo p divisor de $|G|$ um p-subgrupo de Sylow P de G é tal que $C_G(P) = N_G(P)$, então G é p-nilpotente.*

Quando a questão é extrair informações acerca da estrutura dos grupos finitos, o homomorfismo transfer é uma ferramenta muito poderosa, sendo a beleza e a elegância das técnicas inerentes a ela bastante cativantes. Por este motivo e por sua relação com o tema, o estudo do homomorfismo transfer é muito oportuno neste trabalho.

O desenvolvimento do presente trabalho, especialmente baseado no capítulo 10 de [6], onde é estudado o *homomorfismo transfer* e suas aplicações, é feito em três capítulos. No primeiro são abordados, embora sem demonstrações, alguns requisitos básicos, tais como resultados básicos da teoria de grupos, comutadores de conjuntos e elementos, subgrupos normais e gru-

pos quocientes, classes laterais e o Teorema de Lagrange, homomorfismo de grupos e os teoremas de Sylow.

No segundo capítulo, estudaremos os grupos nilpotentes e apresentaremos um teorema que caracteriza a estrutura dos grupos nilpotentes finitos. Além disso, faremos uma breve introdução sobre p-nilpotência de grupos, finalizando com a demonstração do seguinte resultado comentado anteriormente: *um grupo finito é nilpotente se, e somente se, é p-nilpotente para todo p divisor primo da ordem do grupo em questão.*

Finalmente, no terceiro capítulo, introduziremos o homomorfismo transfer e suas propriedades básicas, e faremos uso dele na demonstração do Teorema do Transfer de Burnside (enunciado acima), também conhecido com Critério de p-nilpotência de Burnside. Para concluir, mostraremos algumas consequências deste resultado.

Capítulo 1

Definições e Resultados Preliminares

No desenvolvimento desse trabalho assumiremos que o leitor tenha familiaridade com conceitos e resultados básicos da teoria de grupos. Destarte, nesse capítulo apresentaremos alguns resultados preliminares que serão usados frequentemente no decorrer do texto e, por serem resultados básicos, omitiremos suas demonstrações, as quais podem ser encontradas nas referências [3], [4], [6] e [7].

1.1 Grupos e Subgrupos

Nessa seção apresentaremos alguns resultados conhecidos acerca da teoria de grupos, aproveitaremos o ensejo para numerá-los e posteriormente apenas mencioná-los sempre que necessário.

Definição 1. *Sejam G um conjunto não vazio e $* : G \times G \longrightarrow G$ uma operação binária em G. Dizemos que o par $(G, *)$ é um* grupo *se as seguintes condições são satisfeitas:*

i) A operação " $*$ " é associativa, ou seja, $(a * b) * c = a * (b * c)$ para quaisquer $a, b, c \in G$.

ii) Existe $e \in G$ tal que $a * e = e * a = a$, para todo $a \in G$.

iii) Para cada $a \in G$ existe $a^{-1} \in G$ tal que $a * a^{-1} = a^{-1} * a = e$.

Por simplicidade denotemos $(G, *)$ simplesmente por G, ficando então a operação subtendida. Na definição acima nos referimos a e como sendo o elemento neutro do grupo G e a a^{-1} como sendo o inverso de $a \in G$. É fato

conhecido que o elemento neutro e o inverso de cada elemento são únicos em um grupo.

Observação 1. *As propriedades básicas que seguem de forma direta das definições acima, serão deixadas a cargo do leitor, como acordado no início do texto. Adotaremos ao longo desse trabalho a notação* multiplicativa*, salvo quando dissermos o contrário. Dessa forma escrevemos $a * b$ simplesmente por ab, para quaisquer a e b pertencentes ao grupo em questão.*

Definição 2. *Seja G um grupo. Dizemos que G é* abeliano *ou* comutativo *se $ab = ba$, para quaisquer $a, b \in G$.*

Definição 3. *Definimos a* ordem *do grupo G, denotado por $|G|$, como sendo o número de elementos de G.*

Definição 4. *Sejam G um grupo, $a, b \in G$ e $n \in \mathbb{N}$. Definimos*

i) O conjugado de a por b, denotado por a^b, como sendo o elemento $a^b = b^{-1}ab$ de G.

ii) A n-ésima potência do elemento $a \in G$, denotado por a^n, como sendo o elemento de G

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

Definição 5. *Seja G um grupo e $a \in G$. Dizemos que*

i) O elemento a tem ordem infinita, e denotamos por $\circ(a) = \infty$, se não existe $n \in \mathbb{N}$ tal que $a^n = e$.

ii) O elemento a tem ordem finita se existe $n \in \mathbb{N}$ tal que $a^n = e$. Neste caso, definiremos a ordem de a, denotada por $\circ(a)$, como sendo $\circ(a) = min\{n \in \mathbb{N} \mid a^n = e\}$.

Exemplo 1. *O grupo de* Klein *é um grupo abeliano de ordem 4, onde todos os elementos não neutros têm ordem 2, enquanto que o grupo aditivo $\mathbb{R}$ dos números reais é um grupo abeliano onde todos os elementos não neutros tem ordem infinita.*

Exemplo 2. *Sejam $G_1, ..., G_n$ grupos. Considere o produto cartesiano $G = G_1 \times .... \times G_n$. Definimos em G a operação*

$$(a_1, ..., a_n).(b_1, ..., b_n) = (a_1b_1, ..., a_nb_n)$$

para $(a_1, ..., a_n), (b_1, ..., b_n) \in G$, onde a operação da i-ésima coordenada é a operação do i-ésimo grupo. Munido dessa operação $G = G_1 \times .... \times G_n$ é um grupo chamado de produto direto de $G_1, ..., G_n$. *Ademais, o produto direto é abeliano se, e somente se cada fator é abeliano.*

Exemplo 3. *Seja X um conjunto não vazio. Chama-se permutação de um conjunto X a uma função bijetiva α que leva X em X. Consideremos o conjunto de todas as permutações de X denotando-o por S_X. Não é difícil ver que S_X munido da operação composição é um grupo, o qual nos referimos como* grupo simétrico sobre X. *Mais comumente, se $X = \{1, ..., n\}$ denotemos S_X simplesmente por S_n.*

Definição 6. *Seja G um grupo. Diremos que G* é um grupo de torção *se todo elemento de G tem ordem finita. Se todo elemento de G diferente do elemento neutro tiver ordem infinita diremos que G é livre de torção.*

Observe o exemplo acima e note que o grupo de *Klein* é de torção enquanto que o grupo aditivo $\mathbb{R}$ dos números reais é livre de torção.

Definição 7. *Sejam G um grupo e H um subconjunto não vazio de G. Dizemos que H é um subgrupo de G e denotamos por $H \leq G$ se:*

i) Para quaisquer $x, y \in H$ tem-se que $xy \in H$.

ii) Para quaisquer $x \in H$ tem-se que $x^{-1} \in H$.

Observe que H é um subgrupo de G se H por si é um grupo com a mesma operação de G a ele restrita. Dessa forma é fácil ver que se G é abeliano, então H também o será.

Exemplo 4. *Sendo G um grupo é fácil ver que $\{e\}$ e G são subgrupos de G, chamados de subgrupos* triviais.

Exemplo 5. *Sejam G um grupo e H subgrupo de G. Fixemos um elemento $g \in G$, então o conjunto $H^g = \{h^g \mid h \in H\}$ é um subgrupo de G chamado de* subgrupo conjugado de H por g .

Definição 8. *Sejam G um grupo e H um subgrupo de G. Definimos o* normalizador de H em G, *denotado por $N_G(H)$, como sendo*

$$N_G(H) = \{g \in G \mid H^g = H\}$$

.

Não é difícil ver que $N_G(H)$ é um subgrupo de G que contém H.

Exemplo 6. *Sejam G um grupo e X um subconjunto não vazio de G. Então o conjunto $C_G(X) = \{g \in G \mid gx = xg, \forall x \in X\}$ é um subgrupo de G, referido como* o centralizador de X em G. *Nos casos particulares em que $X = \{a\}$ ou $X = G$, chamaremos de* centralizador de a em G, *denotando por $C_G(a)$, ou* centralizador de G em G, *denotando por $Z(G)$ e referido como o* centro de G, *respectivamente.*

Definição 9. *Sejam G um grupo e H e N subgrupos de G. Definimos o produto de H por N, denotado por HN, como sendo o conjunto $HN = \{hn \mid h \in H, n \in N\}$.*

Observação 2. *observe que $H \subseteq HN$ e $N \subseteq HN$, além disso não é difícil provar que se H e N são subgrupos finitos de um grupo G, então HN é finito e*

$$|HN| = \frac{|H||N|}{|H \cap N|}$$

Perceba que na equação ligeiramente acima não nos preocupamos com o fato de HN ser ou não um subgrupo de G. O fato é que existem condições necessárias e suficientes e outras apenas suficientes para que o produto de subgrupos ainda seja um subgrupo. Como por exemplo, $HN = NH$ é uma condição necessária e suficiente para que HN seja subgrupo de G.

Lema 1. *Sejam G um grupo e H e N subgrupos não triviais de G. Se $H \subseteq N_G(N)$ ou $N \subseteq N_G(H)$, então o produto HN é um subgrupo de G.*

Definição 10. *Seja G um grupo e S um subconjunto de G. Definimos o* subgrupo de G gerado por S, *denotado por $\langle S \rangle$, como sendo a interseção de todos os subgrupos de G que contem S.*

Definição 11. *Seja G um grupo. Diremos que G é finitamente gerado se G possui um subconjunto gerador finito, isto é, G é finitamente gerado se existe $S \subseteq G$ finito tal que $\langle S \rangle = G$.*

Observação 3. *Sejam G um grupo, H subgrupo e S um subconjunto de G. Convencionaremos que $\langle \emptyset \rangle = \{e\}$. No mais, segue de forma direta da definição acima que:*

i) $S \subseteq \langle S \rangle$.

ii) Se $H \leq G$ *e* $S \subseteq H$, *então* $\langle S \rangle \subseteq H$.

iii) Se $H \leq G$, *então* $\langle H \rangle \leq H$.

Teorema 1. *Sejam G um grupo e S um subconjunto de G. Então*

$$\langle S\rangle = \{x_1x_2...x_n \mid n \in \mathbb{N}, x_i \in S \cup S^{-1}\}$$

onde $S^{-1} = \{s^{-1} \mid s \in S\}$.

Corolário 1. *Sendo G um grupo e g um elemento de G, temos que conjunto $\langle g\rangle = \{g^n \mid n \in \mathbb{Z}\}$ é um subgrupo de G chamado de* subgrupo gerado por g. *Além disso, $|\langle g\rangle| = \circ(g)$ e quando $\circ(g)$ é finita, $\langle g\rangle = \{e, g, ..., g^{\circ(g)-1}\}$.*

Observação 4. *Sendo G um grupo e g um elemento de G, se por ventura tivermos que $\langle g\rangle = G$ dizemos que G é* cíclico. *Não é difícil ver que todo grupo cíclico é abeliano, mas nem todo grupo abeliano é cíclico, a saber o grupo de* Klein. *Também, é fácil ver que se G é um grupo cíclico, então $\circ(g) = |G|$, onde g é um gerador de G.*

O teorema abaixo fornece um resultado muito forte, acerca de grupos abelianos, que será utilizado no terceiro capítulo desse trabalho.

Teorema 2. *Seja G é um grupo abeliano de torção e finitamente gerado, então G é finito.*

1.2 Classes Laterais e o Teorema de Lagrange

O Teorema de *Lagrange* é um dos mais famosos e importantes da teoria de grupos, e a demonstração desse teorema é extremamente fácil quando se faz uso das *classes laterais* que são como definidas a seguir.

Definição 12. *Sejam G um grupo, H um subgrupo e g um elemento de G. Definimos as classes laterais à direita e à esquerda de H contendo g, denotadas por Hg e gH, respectivamente, como sendo*

$$Hg = \{hg \mid h \in H\} \qquad e \qquad gH = \{gh \mid h \in H\}$$

.

É fato conhecido que distintas classes laterais à esquerda (ou à direita) são disjuntas e que $xH = yH$ se, e somente, $x^{-1}y \in H$. Ao definirmos a bijeção $h \longmapsto xh$ de H em xH, fica fácil ver que H e xH tem a mesma cardinalidade, seja qual for $x \in G$. Também destacamos aqui, o fato de que a união de todas as classes laterais à esquerda(respectivamente, à direita) de H em G resulta em G.

Pelo axioma da escolha sempre podemos escolher um subconjunto não vazio T de G tal que $\bigcup_{t\in T} tH = G$ e $t_1H \neq t_2H$, sempre que t_1 e t_2 forem

elementos distintos em T. Neste caso, dizemos que T é um *transversal à esquerda* para H em G. Analogamente, dizemos que T é um *transversal à direita* para H em G se $\bigcup_{t\in T} Ht = G$ e $Ht_1 \neq Ht_2$ sempre que t_1 e t_2 forem elemento distintos em T.

Sendo T um transversal à esquerda(respectivamente, à direita) para H em G, como mencionado acima, podemos escrever G como união disjunta de classes laterais da forma tH(respectivamente, Ht) com $t \in T$. A cardinalidade de T(seja T transversal à direita ou à esquerda) é chamado de índice de H em G e é denotado por $|G : H|$.

Teorema 3. ***(Lagrange)*** *Sejam G um grupo finito e H um subgrupo de G. Então $|G| = |G : H||H|$ e consequentemente $|H|$ divide $|G|$.*

Observação 5. *É fato conhecido que, em geral, a recíproca do Teorema de Lagrange é falsa. No entanto, se o grupo em questão for abeliano, a recíproca torna-se verdadeira.*

Corolário 2. *Todo grupo finito de ordem prima possui apenas os subgrupos triviais e consequentemente é cíclico(em particular, abeliano).*

Corolário 3. *Se G é um grupo finito e g é um elemento de G, então $\circ(g)$ divide $|G|$.*

Corolário 4. *Sejam G um grupo e H e K subgrupos de G, com H finito. Então $|H \cap K|$ divide $|H|$. Ademais, se K também é finito, então $|H \cap K|$ divide $mdc(|H|, |K|)$.*

Usando o teorema de Lagrange e o conceito de transversal podemos demonstrar o

Teorema 4. *Sejam G um grupo e H e N subgrupos de G, com $N \subseteq H$, então $|G : N| = |G : H||H : N|$.*

1.3 Subgrupos Normais e Grupos Quociente

O conceito de *subgrupo normal* exerce um papel importante na teoria dos grupos, pois baseados nele podemos definir os grupos quocientes que por sua vez, abrem uma nova vertente de estudos, sobre os quais podemos exibir resultados maravilhosos acerca das estruturas dos grupos.

Definição 13. *Sejam G um grupo e H um subgrupo de G. Dizemos que H um subgrupo normal de G(ou que o subgrupo H é normal em G), e denotamos por $H \trianglelefteq G$, se $gH = Hg$ para todo $g \in G$.*

Observação 6. *Observamos primeiramente que seja qual for o grupo G em questão, sempre temos que $\{e\}$ são G normais em G. Quando $\{e\}$ e G forem os únicos subgrupos normais de G, dizemos que G é um* grupo simples.

Na caracterização de subgrupos normais temos a

Proposição 1. *Sejam G um grupo e H um subgrupo de G. Então, são equivalentes:*

i) H é um subgrupo normal em G.

ii) $H^g = H$ para todo $g \in G$, isto é, $N_G(H) = G$.

iii) $H^g \subseteq H$ para todo $g \in G$, isto é $g^{-1}hg \in H$, para quaisquer $g \in G$ e $h \in H$.

Exemplo 7. *Seja G um grupo abeliano. Então, se H é um subgrupo de G devemos ter, em verdade, que H é subgrupo normal em G.*

Exemplo 8. *Se G é um grupo e H é um subgrupo de G tal que $|G : H| = 2$, então H é normal em G.*

Observação 7. *Recordemos agora que se G é um grupo, então valem:*

i) Se $H \subseteq Z(G)$, então devemos ter $H \trianglelefteq G$.

ii) Sendo G um grupo e $H, N \leqslant G$ com $N \subseteq H$, temos que $N \trianglelefteq H$ se, e somente se, $H \subseteq N_G(N)$.

iii) Se $H, N \trianglelefteq G$, então $HN \trianglelefteq G$ e $H \cap N \trianglelefteq G$.

Lema 2. *Sejam G um grupo finito e H e N subgrupos de G, com $mdc(|G|, |G : N|) = 1$. Então valem:*

i) Se HN é subgrupo de G, então $|H \cap N| = mdc(|H|, |N|)$.

ii) Se N é normal em G e $|H|$ divide $|N|$, então $H \subseteq N$.

Lema 3. *Sejam G um grupo e $H_1, H_2, ..., H_n$ subgrupos normais em G, com $mdc(|H_i|, |H_j|) = 1$, para $i \neq j$. Então, $|H_1H_2...H_n| = |H_1||H_2|...|H_n|$.*

Observação 8. *Sejam G um grupo e N um subgrupo normal em G. Neste caso, para $g \in G$ adotamos a notação $\overline{g}$ para significar a classe lateral gN contendo g em G, isto é $\overline{g} = gN$ para qualquer $g \in G$.*

Sejam G um grupo e N um subgrupo normal em G. Consideremos o conjunto $G/N = \{gN \mid \in G\} = \{\overline{g} \mid g \in G\}$. Definamos em G/N a seguinte operação

$$\begin{array}{rccl} \cdot : G/N & \times & G/N & \longrightarrow & G/N \\ & & (aN, bN) & \longmapsto & (aN).(bN) = (ab)N = \overline{ab} \end{array}$$

Observação 9. *Observemos que se (aN, bN), $(a_1N, b_1N) \in G/N \times G/N$ são tais que $(aN, bN) = (a_1N, b_1N)$, então $aN = a_1N$ e $bN = b_1N$, dai $aNbN = a_1Nb_1N$ e pelo fato de N ser normal em G temos $abN = a_1b_1N$, e portanto a operação acima está bem definida. Ademais, G/N munido da operação " $\cdot$ " é um grupo. Neste caso nos referimos a G/N como sendo* o grupo quociente *de G por N.*

Observação 10. *Dados G um grupo e N um subgrupo normal em G. Considerando o grupo quociente G/N, não é difícil ver que:*

i) $eN = N$ é o elemento neutro de G/N, denotado também por $\overline{e}$.

ii) Se $g \in G$, então $(gN)^{-1} = g^{-1}N$ em G/N, isto é, $\overline{g}^{-1} = \overline{g^{-1}}$, para todo $g \in G$.

iii) Sendo G um grupo e $N \trianglelefteq G$, então $N = G$ se, e somente se, $G/N = \{eN\} = \{\overline{e}\}$.

iv) Se $g \in G$ e $n \in \mathbb{Z}$, $(gN)^n = g^nN$, ou seja, $\overline{g}^n = \overline{g^n}$, para quaisquer $g \in G$ e $n \in \mathbb{N}$.

v) Se G é abeliano, então G/N é abeliano.

vi) Se G é finito, então $|G/N| = |G : N| = |G|/|N|$.

vii) Sejam G um grupo cíclico, $g \in G$ um gerador de G, isto é $G = \langle g \rangle$, e $N \trianglelefteq G$. Segue diretamente do item (iv) que G/N é cíclico e $gN = \overline{g}$ é um gerador.

Como todo grupo, G/N também tem seus subgrupos. O fato é que se H é um subgrupo de G que contém N, então $H/N = \{hN \mid h \in H\}$ é um subgrupo de G/N. Ademais, temos uma caracterização dos subgrupos de G/N com o seguinte teorema.

Teorema 5. *(Teorema da Correspondência) Sejam G um grupo e N um subgrupo normal em G . Então valem:*

i) Todo subgrupo de G/N é da forma H/N, onde H é um subgrupo de G contendo N.

ii) Sejam H_1 e H_2 são subgrupos de G, ambos contendo N, então $H_1/N = H_2/N$ se, e somente se, $H_1 = H_2$.

iii) Se H é um subgrupo de G contendo N, então $H/N \trianglelefteq G/N$ se, e somente se, $H \trianglelefteq G$.

Exemplo 9. *Considere o grupo aditivo $\mathbb{Z}$ dos números inteiros e o subgrupo $n\mathbb{Z}$, com n um inteiro não negativo. Temos*

$$\mathbb{Z}/n\mathbb{Z} = \{\overline{0}, \overline{1}, ..., \overline{n-1}\}$$

onde $\overline{a} = a + n\mathbb{Z} = \{a + x \mid x \in n\mathbb{Z}\}$ e a operação definida por $\overline{x} + \overline{y} = \overline{x+y}$.

1.4 Homomorfismos de Grupos

Nas diversas áreas da matemática, quando estamos trabalhando com conjuntos ou estruturas é sempre vantajoso poder definir certas aplicações. Na álgebra geralmente trabalhamos com os homomorfismos.

Definição 14. *Uma aplicação φ de um grupo G em um grupo G_1 chama-se um homomorfismo quando $\varphi(xy) = \varphi(x)\varphi(y)$, para quaisquer $x, y \in G$.*

Definição 15. *Sendo $\varphi : G \longrightarrow G_1$ um homomorfismo de grupos, definimos:*

i) O núcleo de φ, denotado por $Ker\varphi$, como sendo $Ker\varphi = \{x \in G \mid \varphi(x) = e_1\}$, onde e_1 é o elemento neutro de G_1.

ii) A imagem de φ, denotada por $Im\varphi$, como sendo $Im\varphi = \{\varphi(x) \mid x \in G\}$

Observação 11. *Considere $\varphi : G \longrightarrow G_1$ um homomorfismo de grupos. Agora, passaremos a listar algumas propriedades de homomorfismo de grupos, embora sem demonstrações, que julgamos ser necessárias no desenvolvimento desse trabalho.*

i) $Ker\varphi$ é subgrupo de G e $Im\varphi$ é subgrupo de G_1.

ii) $\varphi(e) = e_1$, $\varphi(x^{-1}) = \varphi(x)^{-1}$ e $\varphi(x^n) = \varphi(x)^n$, para quaisquer $x, y \in G$ e $n \in \mathbb{Z}$.

iii) Se H é subgrupo de G, então $\varphi(H) = \{\varphi(h) \mid h \in H\}$ é um subgrupo de G_1. Particularmente, $Im\varphi$ é subgrupo de G_1.

iv) Se K é um subgrupo de G_1, então $\varphi^{-1}(K) = \{x \in G \mid \varphi(x) \in K\}$ é um subgrupo de G. Particularmente, $Ker\varphi = \varphi^{-1}(\{e_1\})$ é um subgrupo de G.

v) φ *é injetiva se, e somente se,* $Ker\varphi = \{e\}$.

vi) Se φ *é sobrejetivo e* K *é subgrupo de* G_1*, então* $\varphi(\varphi^{-1}(K)) = K$.

vii) Se H *é um subgrupo normal em* G*, então* $\varphi(H)$ *é um subgrupo normal em* $Im\varphi$.

Exemplo 10. *A aplicação* $\varphi : G \longrightarrow G_1$*, definida por* $\varphi(x) = e_1$ *para todo* $x \in G$*, é um homomorfismo de grupos, o qual é referido como sendo o* homomorfismo trivial.

Exemplo 11. *Sejam* G *um grupo e* N *um subgrupo normal de* G*, então a aplicação*

$$\begin{array}{rcl} \pi : G & \longrightarrow & G/N \\ g & \longmapsto & \pi(g) = gN \end{array}$$

é um homomorfismo sobrejetivo, chamado de projeção canônica.

Definição 16. *Dados* G *e* G_1 *grupos e* $\varphi : G \longrightarrow G_1$ *uma aplicação. Diremos que* φ *é um isomorfismo de grupos se* φ *é um homomorfismo bijetivo.*

Quando G e G_1 são grupos e existe um isomorfismo $\varphi : G \longrightarrow G_1$, diremos que G e G_1 são isomorfos e denotaremos por $G \simeq G_1$. Ademais, se $\varphi : G \longrightarrow G$ é um isomorfismo então, φ será referido como um automorfismo do grupo G.

Observação 12. *Seja* G *um grupo. É fato conhecido que o conjunto de todos os automorfismos do grupo* G*, munido da operação* composição*, é um grupo chamado de* grupo dos automorfismos de G *e denotado por* $AutG$*, cujo elemento neutro é o automorfismo identidade que é denotado por* Id_G.

Proposição 2. *Sejam* G *um grupo e* H *um subgrupo de* G*. Então, valem:*

i) $C_G(H) \trianglelefteq N_G(H)$ *e o quociente* $N_G(H)/C_G(H)$ *é isomorfo a um subgrupo de* $AutH$*. Consequentemente, pelo Teorema de Lagrange,* $|N_G(H)/C_G(H)|$ *divide* $|AutH|$.

ii) Se G *é cíclico finito, então* $|AutG| = \phi(|G|)$*, onde* ϕ *é a função de Euler.*

iii) Se $G \simeq \mathbb{Z}_p \times \mathbb{Z}_p$*, onde* p *é um primo, então* $|AutG| = (p^2 - 1)(p^2 - p)$

Observação 13. *A demonstração da proposição acima pode ser encontrada em [6].*

Exemplo 12. *Sejam G um grupo e H e N subgrupos de G tais que $N, H \trianglelefteq G$, $HN = G$ e $H \cap N = \{e\}$. Neste caso diremos que G é o produto direto interno de H e N. Consideremos o produto direto $H \times N$ e a aplicação*

$$\begin{array}{rcl} \varphi : H \times N & \longrightarrow & G \\ (h, n) & \longmapsto & \varphi(h, n) = hn \end{array}$$

Com alguns cálculos elementares, não é difícil ver que φ é um isomorfismo de grupos. Logo $G \simeq H \times N$.

Exemplo 13. *Seja G um grupo cíclico, então:*

i) Se G é infinito, devemos ter $G \simeq \mathbb{Z}$.

ii) Se G é finito de ordem k, devemos ter $G \simeq \mathbb{Z}_k$.

Agora, passaremos a apresentar alguns teoremas de destaque envolvendo homomorfismo de grupos, que serão usados constantemente no desenvolvimento do presente trabalho.

Teorema 6. *(1º Teorema de isomorfismo). Sejam G e G_1 grupos, $\varphi : G \longrightarrow G_1$ um homomorfismo e $N = ker\varphi$. Então, a aplicação*

$$\begin{array}{rcl} \overline{\varphi} : \dfrac{G}{N} & \longrightarrow & Im\varphi \\ overline{g} & \longmapsto & \overline{\varphi}(\overline{g}) = \varphi(g) \end{array}$$

é bem definida e é um isomorfismo. Portanto, $\dfrac{G}{N} \simeq Im\varphi$.

Teorema 7. *(2º Teorema de isomorfismo). Sejam G um grupo e H e N subgrupos de G, com $N \trianglelefteq G$. Então, $H \cap N \trianglelefteq H$ e $\dfrac{H}{H \cap N} \simeq \dfrac{HN}{N}$.*

Teorema 8. *(3º Teorema de isomorfismo). Se G é um grupo e $H, N \trianglelefteq G$, com $N \subseteq H$, então $\dfrac{H}{N} \trianglelefteq \dfrac{G}{N}$ e $\dfrac{G/N}{H/N} \simeq \dfrac{G}{H}$.*

.

Teorema 9. *(Teorema da Representação) Sejam G um grupo e H um subgrupo de G com $|G : H| = n$. Então, existe $N \trianglelefteq G$, com $N \subseteq H$, tal que G/N é isomorfo a um subgrupo de S_n. Particularmente, $|G/N|$ divide $n!$.*

Agora apresentaremos uma aplicação que será muito importante para o desenvolvimento desse trabalho.

Exemplo 14. *Sejam G um grupo finito e n um inteiro não nulo tal que $mdc(|G|, n) = 1$. Então a aplicação*

$$\begin{array}{rcl} \varphi : G & \longrightarrow & G \\ g & \longmapsto & \varphi(g) = g^n \end{array}$$

é uma bijeção. De fato, pela identidade de Bezout *existem $p, q \in \mathbb{Z}$ tais que $nq + |G|p = 1$. Daí, se $x \in G$, então $(x^q)^n = x^{qn} = x^{qn}e = x^{qn}x^{|G|p} = x^{qn+|G|p} = x^1 = x$. Logo, $x = (x^n)^q = (x^q)^n = \varphi(x^q)$. Isso mostra que se $x \in G$, então $x \in \langle x^n \rangle$ além disso, obtermos que φ é sobrejetiva. Como G é finito temos que φ é injetiva, consequentemente bijetiva.*

Sendo G um grupo, considerando a aplicação acima obtemos que se H é um subgrupo de G, então $\varphi(H) = H$. Daí, se $x \in G$ é tal que $x^n \in H$ devemos ter na verdade que $x \in H$. Ademais, se G é abeliano é fácil ver que A aplicação φ é um homomorfismo, e portanto automorfismo de grupos.

1.5 Comutadores e Grupos solúveis

Nessa seção definiremos o que vêm a ser comutadores de subconjuntos não vazios e de elementos de um grupo qualquer, bem como definiremos também grupos solúveis. Apresentaremos alguns resultados importantes acerca desses tópicos e finalizaremos com resultados que mostram a estreita relação entre esses dois conceitos.

Definição 17. *Sejam X e Y subconjuntos não vazios de um grupo G, definimos o subgrupo comutador de X por Y, denotado por $[X, Y]$, como sendo o subgrupo de G gerado pelo conjunto $\{[x, y] | x \in X, y \in Y\}$, ou seja,*

$$[X, Y] = \langle [x, y] \mid x \in X, y \in Y \rangle$$

onde $[x, y]$ é definido como sendo o comutador de x por y, que é o elemento $x^{-1}y^{-1}xy$ de G. No caso especial em que $X = Y = G$, o subgrupo comutador $[X, Y] = [G, G]$, será denotado por G', e neste caso nos referimos a $[G, G] = G'$ como sendo o subgrupo derivado *de G.*

Vejamos algumas propriedades básicas de comutadores de elementos e subgrupos, as quais podem ser facilmente demonstradas. Por formalidade apresentaremos tais propriedades como

Lema 4. ***(propriedades básicas)*** *Se G é um grupo e $x, y, z \in G$, então valem:*

i) $xy = yx \iff [x, y] = e$.

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

iii) $[xy,z] = [x,z]^y[y,z]$ *e* $[x,yz] = [x,z][x,y]^z$

iv) Se $N \trianglelefteq G$ *e* $x \in N$, *então* $[x,y] \in N$.

Observação 14. *Das propriedades acima podemos obter facilmente que* $G' = \{e\}$ *se, e somente se,* G *é um grupo abeliano.*

Observação 15. *Não é difícil ver que comutadores de subconjuntos(não vazios) preservam inclusão, isto é, sendo* G *um grupo e* X, Y, X_1, Y_1 *subconjuntos não vazios de* G *tais que* $X \subseteq X_1$ *e* $Y \subseteq Y_1$, *devemos ter* $[X,Y] \subseteq [X_1,Y_1]$. *Ademais, segue que se* H *é um subgrupo de* G, *então* $H' = [H,H] \subseteq [G,G] \subseteq G'$.

Lema 5. *Consideremos* G *um grupo e* H *e* N *subgrupos de* G. *Observemos que é suficiente que* N *esteja contido no centro de* G *para que tenhamos* $[HN,K] = [H,K]$. *Ademais, não é difícil ver que se* $N \trianglelefteq G$, *então* $\left[\dfrac{HN}{N}, \dfrac{KN}{N}\right] = \dfrac{[H,K]N}{N}$.

Uma das propriedades de comutadores de subconjuntos mais recorridas em nosso trabalho será apresentada no seguinte lema.

Lema 6. *Sejam* G *um grupo e* H *e* N *subgrupos de* G, *então* $[H,N] \subseteq N$ *se, e somente se,* $H \subseteq N_G(N)$. *Particularmente, se* N *é normal em* G, *então* $[H,N] \subseteq N$.

Observação 16. *Recorde que, se* G *é um grupo e* N *é um subgrupo normal em* G, *então* $Z(G/N) = K/N$ *onde*

$$K = \{x \in G \mid [x,G] \in N, \forall g \in G\} = \{x \in G \mid [x,G] \subseteq N\}$$

Logo, $Z_{k+1}(G) = \{x \in G \mid [x,G] \subseteq Z_k(G)$.

Como consequência da observação acima temos o lema.

Lema 7. *Sejam* G *um grupo e* H *e* N *subgrupo de* G, *com* N *normal em* G *e* $N \subseteq H$. *Então,* $H/N \subseteq Z(G/N)$ *se, e somente se,* $[H,G] \subseteq N$.

Teorema 10. *Sejam* G *um grupo e* H *e* N *subgrupos normais em* G, *então* $[H,N] \trianglelefteq G$.

Definição 18. *Sendo* G *um grupo e* H *um subgrupo de* G, *dizemos que* H *é um* subgrupo característico *de* G *se* $\varphi(H) \subseteq H$ *para todo* $\varphi \in AutG$, *ou seja,* H *é invariante por todos os automorfismos de* G.

Observação 17. *Sejam G um grupo e H um subgrupo de G. Tomemos $g \in G$ e consideremos a aplicação*

$$\begin{array}{rccc} \varphi_g : G & \longrightarrow & G \\ x & \longmapsto & \varphi_g(x) = x^g \end{array}$$

É fácil observar que $\varphi_g \in AutG$, para todo $g \in G$. Logo, se H é um subgrupo característico de G, devemos ter $H^g = \varphi_g(H) \subseteq H$ para todo $g \in G$. Sendo assim, obtemos que todo subgrupo característico é normal. Observemos também que se $\varphi \in Aut(G)$ e $x, y \in G$, então $\varphi([x, y]) = [\varphi(x), \varphi(y)] \in G$. Dessa forma, G' é um subgrupo característico de G e consequentemente tem-se que $G' \trianglelefteq G$.

Agora passaremos a apresentar, embora sem demonstrações, alguns resultados envolvendo grupos solúveis que serão referenciados ao longo deste trabalho. Primeiro vamos à definição.

Definição 19. *Seja G um grupo. Dizemos que G é um grupo solúvel se existe uma série de subgrupos*

$$G = H_0 \trianglerighteq H_1 \trianglerighteq H_2 \trianglerighteq ... \trianglerighteq H_{n-1} \trianglerighteq H_n = \{e\}$$

com H_i/H_{i+1} abeliano para todo $i = 0, 1, ..., n-1$.

Uma série de subgrupos de G como na definição acima é chamada de *série abeliana*.

Exemplo 15. *Todo grupo abeliano é solúvel.*

Definição 20. *Sejam G um grupo e H e K dois subconjuntos de G, denotaremos por $[H, K]$ o subgrupo de G gerado pelo conjunto $\{[h, k] \mid h \in H, k \in K\}$. No caso particular em que $H = K = G$, temos o grupo $G' = [G, G]$ o qual é referido como* subgrupo comutador *ou* subgrupo derivado de G.

Agora definimos uma a seguinte sequência de subgrupos de G:

$$\begin{array}{rcl} G^{(0)} & = & G \\ G^{(1)} & = & G' \\ G^{(2)} & = & (G^{(1)})' = G'' \\ & \vdots & \\ G^{(n)} & = & (G^{(n-1)})' \end{array}$$

O subgrupo $G^{(n)}$ é chamado de *o n-ésimo grupo derivado de G* e a sequência

$$G = G^{(0)} \supseteq G^{(1)} \supseteq \ldots \supseteq G^{(n)} \supseteq \ldots$$

chama-se a *sequência derivada de G*.

A proposição seguinte exibe um resultado muito interessante envolvendo subgrupo derivado que será bastante recorrida no escorrer do texto.

Proposição 3. *Sejam G um grupo e N um subgrupo de G. Então, são equivalentes:*

i) $G' \subseteq N$.

ii) $N \trianglelefteq G$ *e* G/N *é abeliano.*

Proposição 4. *Sejam G um grupo e H e N subgrupos de G, com N normal em G. Então vale:*

i) Se G é solúvel, então H e G/N *são solúveis.*

ii) G é solúvel se, e somente se, N e G/N *são solúveis.*

O próximo resultado relaciona a ideia de comutador com solubilidade

Teorema 11. *Um grupo G é solúvel se, e somente se, existe* $n \in \mathbb{N}$ *tal que* $G^{(n)} = \{e\}$.

Definição 21. *Seja G um grupo solúvel. Consideremos sua sequência derivada*

$$G = G^{(0)} \supseteq G^{(1)} \supseteq \ldots \supseteq G^{(n)} \supseteq \ldots$$

Definimos o comprimento derivado de G, denotado por $d(G)$*, como sendo*

$$d(G) = min\{n \in \mathbb{N} \mid G^{(n)} = \{e\}\}.$$

O teorema seguinte apresenta um resultado muito forte acerca de grupos solúveis.

Teorema 12. *Sejam p,q e r números primos, então todos os grupos de ordens* $p^m, p^m q, p^2 q^2$ *ou pqr são solúveis.*

Por último temos o Teorema de Burnside

Teorema 13. *(Burnside) Sejam p e q primos. Então um grupo que tenha ordem* $p^m q^n$ *é solúvel.*

1.6 Teoremas de Sylow

Os famosos Teoremas de Sylow ocupam lugar de destaque em nosso trabalho, uma vez que serão acionados constantemente nos próximos capítulos.

Teorema 14. *(Teorema de Cauchy) Seja G um grupo finito. Se p é um divisor primo de $|G|$, então G possui algum elemento de ordem p.*

Teorema 15. *(1^o Teorema de Sylow) Sejam G um grupo finito, p um divisor primo de $|G|$ e p^n a maior potência de p que divide $|G|$. Se $k \in \{1, ..., n\}$, então G possui pelo menos um subgrupo de ordem p^k. Ademais se $1 \leq k < n$ e H é um subgrupo de G de ordem p^k, então existe K subgrupo de G tal que $|K| = p^k$ e $H \trianglelefteq K$.*

Sendo G um grupo finito e p^k uma potência de um primo p divisor de $|G|$, o teorema acima garante que existe subgrupo de G de ordem p^k. Se p^n é a maior potência do primo p que divide $|G|$, então os subgrupos de G de ordem p^n são chamados de *p-subgrupos de Sylow* ou *S_p-subgrupo*de G.

Teorema 16. *(2^o Teorema de Sylow) Seja G um grupo finito e p um divisor primo de $|G|$. Se P_1 e P_2 são p-subgrupos de Sylow de G, então P_1 e P_2 são conjugados.*

Corolário 5. *Segue de forma imediata do teorema acima que se um p-subgrupo de Sylow P de G é normal, então P é o único p-subgrupo de Sylow de G. De fato, supondo P_1 e P_2 p-subgrupo de Sylow de G, existe $x \in G$ tal que $P_1 = P_2^x = P_2$.*

Teorema 17. *(3^o Teorema de Sylow) Sejam G um grupo finito, p um divisor primo de $|G|$ e n_p o número de p-subgrupos de Sylow de G. Então, $n_p \equiv 1 \pmod{p}$ e n_p divide $|G : P|$, onde P é um p-subgrupo de Sylow de G.*

Dizemos que um grupo G é um p-grupo finito se $|G| = p^n$, onde $p \in \mathbb{N}$ é primo e n é um inteiro não nulo. Além dos teoremas de Sylow, o próximo teorema também será útil no desenvolvimento desse trabalho.

Teorema 18. *Se G é um p-grupo finito não trivial, então $Z(G)$ tem ordem divisível por p.*

Capítulo 2

Grupos Nilpotentes

A classe dos grupos nilpotentes finitos é de grande interesse no presente trabalho, visto que essa teoria nos permite exibir resultados fascinantes acerca da estrutura dos grupos finitos.

2.1 Séries Centrais e Grupos Nilpotentes

Nessa seção definiremos o que vêm a ser grupos nilpotentes e introduziremos as series centrais, que serão definidas a seguir.

Definição 22. *Seja G um grupo. Dizemos que G é um grupo* nilpotente *se existe uma série de subgrupos*

$$\{e\} = N_0 \leq N_1 \leq N_2 \leq ... \leq N_{n-1} \leq N_n = G$$

com $N_i \trianglelefteq G$ e $N_{i+1}/N_i \subseteq Z(G/N_i)$ para todo $i = 0, 1, ..., n-1$.

Uma série de subgrupos de G como na definição acima é chamada de série *central (ascendente)*. Observemos que pelo Lema 7 $N_{i+1}/N_i \subseteq Z(G/N_i)$ se, e somente se, $[N_{i+1}, G] \subseteq N_i$.

Observemos primeiramente que as condições exigidas na definição de nilpotência são claramente mais exigentes do que aquelas que aparecem na definição de grupo solúvel. Assim sendo, naturalmente podemos imaginar que todo grupo nilpotente é solúvel. Veremos adiante que isso de fato é verdadeiro, sendo a recíproca, no entanto, falsa.

Exemplo 16. *Todo grupo abeliano é nilpotente. De fato, supondo G um grupo abeliano, então facilmente podemos observar que a série $\{e\} = N_0 \leq N_1 = G$ é uma série central de subgrupos de G.*

Exemplo 17. *Se G é um p-grupo finito, então G é nilpotente.* Em primeiro lugar, observemos que se N é um subgrupo normal próprio de G, então G/N é um p-grupo (não trivial). Por G/N ser um p-grupo (não trivial), lembremos que $Z(G/N)$ deve ter ordem divisível por p e dessa forma, existe H subgrupo de G, com $N \subseteq H$, de maneira que H/N seja um subgrupo de $Z(G/N)$ de ordem p. Estando $H/N \subseteq Z(G/N)$, devemos ter que $H/N \trianglelefteq G/N$ e portanto temos que $H \trianglelefteq G$. Ademais, note que $|H| = p|N|$.

Agora vamos de fato ao exemplo. Se $|G| = p$, nada a fazer. Suponha $|G| = p^n$, com $n > 1$. Por $Z(G)$ ter ordem divisível por p, já que G é um p-grupo finito, temos que existe N_1 subgrupo de G, tal que $N_1 \subseteq Z(G)$ e $|N_1| = p$. Por $N_1 \subseteq Z(G)$ segue que $N_1 \trianglelefteq G$. Assim, pelo o que foi observado acima, temos que existe $N_2 \trianglelefteq G$, com $N_1 \subseteq N_2$ tal que $N_2/N_1 \subseteq Z(G/N_1)$ e $|N_2| = p|N_1|$. Se $N_2 = G$, então a série

$$\{e\} = N_0 \leq N_1 \leq N_2 = G$$

é claramente uma série central de subgrupos de G, e portanto G é nilpotente. Se por acaso $N_2 \lneq G$, podemos raciocinar de mesma forma para encontrar um subgrupo $N_3 \trianglelefteq G$, tal que $N_2 \subseteq N_3$, $N_3/N_2 \subseteq Z(G/N_2)$ e $|N_3| = p|N_2|$, seguindo com esse raciocínio indutivamente concluímos que existe um série central de subgrupos de G do tipo

$$\{e\} = N_0 \leq N_1 \leq N_2 \leq N_3 \leq \ldots \leq N_k \leq N_{k+1} \leq \ldots$$

de maneira que $|N_{k+1}| = p|N_k|$. Como $|G| = p^n$ e $|N_0| = 1$, temos que $N_n = G$, donde segue que G é nilpotente.

Exemplo 18. *Se G é um grupo não trivial, tal que $Z(G) = \{e\}$, então G não pode ser nilpotente.* De fato, Suponha por contradição a existência de uma série central

$$\{e\} = N_0 \leq N_1 \leq N_2 \leq N_3 \ \leq ... \leq N_n = G$$

de subgrupos de G. Como $N_1 \subseteq Z(G) = \{e\}$, devemos ter $N_1 = \{e\}$. Dessa maneira, G/N_1 é isomorfo a G e portanto seu centro também deve ser trivial. Note agora que $N_2/N_1 \subseteq Z(G/N_1) = \{\overline{e}\}$, donde temos que $N_2/N_1 = \{\overline{e}\}$, ou seja $N_2 = N_1 = \{e\}$. Usando esse mesmo argumento indutivamente obtemos que $N_k = \{e\}$, para todo $k = 1, ..., n$, e daí $\{e\} = N_n = G$, uma contradição. Portanto G não pode ser nilpotente.

2.2 Classe de Nilpotência

A teoria das séries centrais possibilita duas caracterizações alternativas e muito úteis de nilpotência. Nessa seção, veremos surgir a relação entre nil-

potência e comutadores, tal como em *solubilidade*. Comecemos por definir a primeira das séries, a qual é chamada de *série central inferior*.

Seja G um grupo. Definimos $\gamma_1(G) = G, \gamma_2(G) = [\gamma_1(G), G] = [G, G]$, $\gamma_3(G) = [\gamma_2(G), G]$ e, seguindo indutivamente, definimos $\gamma_{n+1}(G) = [\gamma_n(G), G]$, para $n \in \mathbb{N}$.

Obviamente temos que $\gamma_1(G) = G \trianglelefteq G$ e que $\gamma_2(G) = [\gamma_1(G), G] = [G, G] = G' \trianglelefteq G$. Seguindo por indução e usando o Teorema 10 é fácil ver $\gamma_n(G) \trianglelefteq G$ para todo $n \in \mathbb{N}$. Pelo fato de $\gamma_n(G) \trianglelefteq G$ podemos usar o Lema 6 para justificar que $\gamma_{n+1}(G) \subseteq \gamma_n(G)$ para todo $n \in \mathbb{N}$. Observemos que, usando o Lema 7, podemos ver que essa série de subgrupos de G é central (descendente), da forma

$$G = \gamma_1(G) \geq \gamma_2(G) \geq \cdots \geq \gamma_n(G) \geq \gamma_{n+1}(G) \geq \cdots$$

O motivo do nome da série acima fica claro com o próximo resultado.

Lema 8. *Seja G um grupo. Considere que a série de subgrupos normais de G*

$$G = N_1 \geq N_2 \geq \cdots \geq N_k \geq N_{k+1} \geq \cdots$$

seja uma série central. Então $\gamma_n(G) \subseteq N_n$ para todo $n \in \mathbb{N}$.

Demonstração. Como a série é central, temos que $[N_k, G] \subseteq N_{k+1}$ para todo $k \in \mathbb{N}$. Logo, o resultado é óbvio para $n = 1$. Suponha, por indução, que $\gamma_k(G) \subseteq N_k$ para algum $k \in \mathbb{N}$. Recorde que $[\gamma_k(G), G] \subseteq [N_k, G]$, e daí $\gamma_{k+1}(G) \subseteq N_{k+1}$. Portanto o resultado é válido para todo $n \in \mathbb{N}$. □

Nos apoiemos agora no conceito de centro de um grupo para definirmos uma outra série importante de subgrupos, a qual é chamada de *série central superior*.

Seja G um grupo. Definimos $Z_0(G) = \{e\}$ e $Z_1(G) = Z(G)$. Considerando o grupo quociente $G/Z_1(G)$, é possível mostrar, usando o Teorema da Correspondência, que existe um subgrupo $Z_2(G)$ de G tal que $Z(G/Z_1(G)) = Z_2(G)/Z_1(G)$. Como $Z_2(G)/Z_1(G) = Z(G/Z_1(G)) \trianglelefteq G/Z_1(G)$ segue do teorema da correspondência que $Z_2(G) \trianglelefteq G$. Nos referimos a $Z_2(G)$ como sendo o 2^o *centro de* G . Ao considerarmos o grupo quociente $G/Z_2(G)$, pelos mesmos argumentos acima, temos que existe $Z_3(G)$ subgrupo normal em G tal que $Z(G/Z_2(G)) = Z_3(G)/Z_2(G)$. $Z_3(G)$ é referido como sendo o 3^o *centro de* G. Seguindo indutivamente e usando o teorema da correspondência em cada passo de indução, uma vez já definido o subgrupo $Z_n(G)$, que é normal em G, definimos $Z_{n+1}(G)$ como sendo o subgrupo de normal de G, tal que $Z(G/Z_n(G)) = Z_{n+1}(G)/Z_n(G)$. O subgrupo $Z_n(G)$ é chamado de *n-ésimo centro de G*.

Segue imediatamente da construção que a série ascendente de subgrupos normais de G

$$\{e\} = Z_0(G) \leq Z_1(G) \leq Z_2(G) \leq \cdots \leq Z_n(G) \leq Z_{n+1}(G) \leq \cdots$$

é uma série central de subgrupos de G.

Assim como na primeira série, a justificativa para o nome da série acima é legitimada pelo próximo resultado.

Lema 9. *Sejam G um grupo e*

$$\{e\} = H_0 \leq H_1 \leq H_2 \leq \cdots \leq H_k \leq H_{k+1} \cdots$$

uma série central de subgrupos de G. Então, $H_n \subseteq Z_n(G)$ para todo $n \in \mathbb{N}$.

Demonstração. De fato, claramente temos que $H_0 = Z_0(G)$ e $H_1 \subseteq Z_1(G)$. Agora, suponhamos por indução a inclusão $H_k \subseteq Z_k(G)$ para algum $k \in \mathbb{N}$. Como a série acima é central temos que $[H_{k+1}, G] \subseteq H_k \subseteq Z_k(G)$ (vide Lema 7). Logo, pela Observação 16, segue que $H_{k+1} \subseteq Z_{k+1}(G)$. Portanto, por indução, $H_n \subseteq Z_n(G)$ para todo $n \in \mathbb{N}$. □

Veremos relevantes resultados a seguir que destacam a importância dessas duas séries centrais na caracterização de nilpotência de um grupo. Mas antes disso, precisamos do seguinte lema.

Lema 10. *Seja G um grupo. Então, são equivalentes:*

i) G é nilpotente.

ii) Existe $n \in \mathbb{N}$ tal que $Z_n(G) = G$.

iii) Existe $m \in \mathbb{N}$ tal que $\gamma_m(G) = \{e\}$.

iv) Existem $n_1, n_2 \in \mathbb{N}$ tais que $\gamma_{n_1}(G) \subseteq Z_{n_2}(G)$.

Demonstração. Em primeiro lugar mostremos

$$\gamma_{n-k+1}(G) \subseteq N_k \subseteq Z_k(G) \tag{2.1}$$

para todo $k = 0, 1, ..., n$, onde $\{e\} = N_0 \leq N_1 \leq N_2 \leq \cdots \leq N_n = G$ é uma série central qualquer de G. Basta-nos mostrar que $\gamma_{n-k+1}(G) \subseteq N_k$ para cada $k \in \mathbb{N}$, já que a segunda inclusão está feita acima. Usaremos indução em k. Observemos que a inclusão é claramente verdadeira para $k = 0$. Suponhamos, por indução que $\gamma_{n-k+1}(G) \subseteq N_k$ para algum $k = 1, ..., n$. Notemos que

$$\gamma_{n-(k-1)+1}(G) = \gamma_{n-k+2}(G) = [\gamma_{n-k+1}(G), G] \subseteq [N_k, G] \subseteq N_{k-1}$$

uma vez que a série acima é central. Portanto o resultado segue para todo $k = 0, 1, ..., n$.

Segue de forma imediata por (2.1) que i)⇒ ii). Para provar ii)⇒ iii) basta tomar $N_k = Z_k(G)$ para termos que

$$\{e\} = N_0 \leq N_1 \leq N_2 \leq \cdots \leq N_n = G$$

é uma série central de G. Portanto, segue também de (2.1) que existe $m \in \mathbb{N}$ tal que $\gamma_m(G) = \{e\}$, bastando tomar $m = n + 1$.

iii)⇒ iv) Nada a fazer. Finalmente provemos iv)⇒ i) usando indução em n_1. Claramente, se $n_1 = 1$ então $Z_{n_2}(G) = G$. Sendo $n_1 > 1$, observemos que $[\gamma_{n_1-1}(G), G] = \gamma_{n_1}(G) \subseteq Z_{n_2}(G)$. Como $Z_{n_2+1}(G) = \{g \in G \mid [g, G] \subseteq Z_{n_2}(G)\}$, temos que $\gamma_{n_1-1}(G) \subseteq Z_{n_2+1}(G)$. Por indução, podemos concluir que $G = \gamma_1(G) \subseteq Z_{n_1+n_2-1}(G)$, donde segue que existe $n \in \mathbb{N}$ tal que $Z_n(G) = G$. Como

$$\{e\} = Z_0(G) \leq Z_1(G) \leq Z_2(G) \leq \cdots \leq Z_{n-1}(G) \leq Z_n(G) = G$$

é uma série central de G, obtemos que G é nilpotente. □

Observação 18. *Sendo G um grupo nilpotente. De acordo com o lema acima podemos obter*

$$n_0 = min\{n \in \mathbb{N} \mid Z_n(G) = G\}$$

e

$$m_0 = min\{m \in \mathbb{N} \mid \gamma_{m+1}(G) = \{e\}\}.$$

Mostremos agora que $n_0 = m_0$. Com efeito, segue de (2.1) que $\gamma_{n_0-k+1}(G) \subseteq Z_k(G)$ para todo $k = 0, 1, ..., n_0$. Concluímos daí que $\gamma_{n_0+1}(G) = \{e\}$, e portanto $m_0 \leq n_0$.

Por outro lado, tomando $N_k = \gamma_{m_0-k+1}(G)$ para todo $k = 0, 1, ..., m_0$, temos que os $N_{i's}$ formam uma série central de G da forma

$$\{e\} = N_0 \leq N_1 \leq ... \leq N_{m_0-1} \leq N_{m_0} = G$$

Portanto, segue de (2.1) que $\gamma_{m_0-k+1}(G) = N_k \subseteq Z_k(G)$ para todo $k = 0, 1, ..., m_0$. Assim temos, $Z_{m_0}(G) = G$, donde segue que $n_0 \leq m_0$. Concluímos que $n_0 = m_0$.

Definição 23. *Seja G um grupo nilpotente. Definimos a* classe de nilpotência de G, *denotada por $cl(G)$, como sendo*

$$cl(G) = n_0 = min\{n \in \mathbb{N} \mid Z_n(G) = G\} = min\{m \in \mathbb{N} \mid \gamma_{m+1}(G) = \{e\}\}.$$

Exemplo 19. *Observe que os grupos de classe de nilpotência igual a 1 são justamente os grupos abelianos. De fato, sendo G um grupo, é fato que G é abeliano se, e somente se, $\{e\} = G' = \gamma_2(G)$. Daí, $cl(G) = 1$.*

Como primeiro resultado das definições acima temos a seguinte proposição.

Proposição 5. *Seja G um grupo nilpotente. Então valem:*

i) Todo subgrupo de G é nilpotente e tem classe de nilpotência menor ou igual a $cl(G)$.

ii) Todo grupo quociente de G é nilpotente e tem classe de nilpotência menor ou igual a $cl(G)$.

Demonstração. Para demonstrar (i) consideremos H um subgrupo de G. É fato que $\gamma_1(H) = H \subseteq G = \gamma_1(G)$. Suponhamos, por indução, a veracidade da inclusão $\gamma_k(H) \subseteq \gamma_k(G)$ para algum $k \in \mathbb{N}$. Observe que

$$\gamma_{k+1}(H) = [\gamma_k(H), H] \subseteq [\gamma_k(G), G] = \gamma_{k+1}(G)$$

Por indução obtemos $\gamma_n(H) \subseteq \gamma_n(G)$ para todo $n \in \mathbb{N}$. Agora, por G ser um grupo nilpotente deve existir $n_0 \in \mathbb{N}$ tal que $n_0 = cl(G)$, isto é, $\gamma_{n_0+1}(G) = \{e\}$. Pelo obtido acima temos $\gamma_{n_0+1}(H) \subseteq \gamma_{n_0+1}(G) = \{e\}$ e portanto H é nilpotente com $cl(H) \leq n_0 = cl(G)$.

Mostremos agora (ii). Suponhamos N um subgrupo normal de G. Com razão escrevemos $GN = G$, e dessa forma temos a seguinte igualdade

$$\gamma_1(G/N) = G/N = GN/N = \gamma_1(G)N/N$$

Suponhamos, por indução, que exista $k \in \mathbb{N}$ tal que $\gamma_k(G/N) = = \gamma_k(G)N/N$. Constatemos que

$$\gamma_{k+1}(G/N) = [\gamma_k(G/N), G/N] = [\gamma_k(G)N/N, G/N] =$$

$$= [\gamma_k(G)N/N, GN/N] = [\gamma_k(G), G]N/N = \gamma_{k+1}(G)N/N$$

. A penúltima igualdade está afiançada pelo Lema (5). Dessa maneira, obtemos que $\gamma_n(G/N) = \gamma_n(G)N/N$ para todo $n \in \mathbb{N}$. Por G ser nilpotente, $cl(G) = n_0$ para algum $n_0 \in \mathbb{N}$, dessa maneira perceba que $\gamma_{n_0+1}(G)N/N = \{e\}N/N = \{\overline{e}\}$. Sendo assim, $\gamma_{n_0+1}(G/N) = \{\overline{e}\}$, donde segue que G/N é nilpotente. Ademais, $cl(G/N) \leq n_0 = cl(G)$.

□

Já estamos em condições de demonstrar o que comentamos no início da seção, que é o fato de todo grupo nilpotente ser solúvel.

Teorema 19. *Seja G um grupo nilpotente, então G é solúvel. Além disso, $d(G) \leq cl(G)$.*

Demonstração. Observemos que $G^{(1)} = [G, G] = \gamma_2(G)$. Suponhamos, por indução, que $G^{(k)} \subseteq \gamma_{k+1}(G)$ para algum $k \in \mathbb{N}$. Como

$$G^{(k+1)} = [G^{(k)}, G^{(k)}] \subseteq [G^{(k)}, G]\gamma_{k+1}(G)$$

temos que $G^{(n)} \subseteq \gamma_{n+1}(G)$ para todo $n \in \mathbb{N}$. Daí, fica extremamente fácil ver que se G é nilpotente, então G é solúvel e $d(G) \leq cl(G)$. □

Observação 19. *Ao analisarmos o grupo S_3 não é difícil observar que $Z(S_3) = \{Id\}$. Logo, pelo Exemplo 18 temos que S_3 não pode ser nilpotente. Por outro lado, $|S_3| = 6 = 2.3$ e portanto S_3 é um grupo solúvel, ficando assim provado que a recíproca do teorema acima não é verdadeira.*

Nem todo resultado que vale para grupos nilpotentes vale para grupos solúveis. Lembre-se que se G um grupo e N é um subgrupo normal em G, então G é solúvel se, e somente se, N e G/N são solúveis. Veremos a seguir que a recíproca desse resultado deixa de ser verdadeira se a propriedade em questão for nilpotência ao invés de solubilidade.

De fato, olhemos para o grupo S_3. Observe que A_3 e S_3/A_3 são nilpotentes pois, $|A_3| = 3$ e $|S_3/A_3| = 2$, e no entanto já vimos S_3 não é nilpotente.

Depois do exposto acima, nos permitimos indagar sobre quais são as propriedades de grupos solúveis que ainda continuam válidas para grupos nilpotentes. É fato que o produto cartesiano finito de grupos solúveis é solúvel. Essa propriedade continua sendo válida para grupos nilpotentes, bastando mostrá-la para dois grupos. Então, vamos ao resultado

Teorema 20. *Se G_1 e G_2 são grupos nilpotentes, então $G_1 \times G_2$ é nilpotente. Mais geralmente, o produto cartesiano de uma família finita de grupos nilpotentes é nilpotente.*

Demonstração. Em primeiro lugar, afirmamos que $\gamma_n(G_1 \times G_2) \subseteq$ $\subseteq \gamma_n(G_1) \times \gamma_n(G_2)$ para todo $n \in \mathbb{N}$. Claramente, a inclusão é válida para $n = 1$. Suponha, por indução, que $\gamma_k(G_1 \times G_2) \subseteq \gamma_k(G_1) \times \gamma_k(G_2)$ para algum $k \in \mathbb{N}$. Tomemos $x \in \gamma_k(G_1 \times G_2)$ e $y \in G_1 \times G_2$. Logo, $x \in \gamma_k(G_1) \times \gamma_k(G_2)$ e assim $x = (x_1, x_2)$ e $y = (g_1, g_2)$, com $x_1 \in \gamma_k(G_1)$, $x_2 \in \gamma_k(G_2)$, $g_1 \in G_1$ e $g_2 \in G_2$, donde

$$[x, y] = [(x_1, x_2), (g_1, g_2)] = (x_1^{-1}, x_2^{-1})(g_1^{-1}, g_2^{-1})(x_1, x_2)(g_1, g_2) = (x_1^{-1}g_1^{-1}x_1g_1, x_2^{-1}g_2^{-1}x_2g_2) =$$

$$= ([x_1, g_1], [x_2, g_2]) \in \gamma_{k+1}(G_1) \times \gamma_{k+1}(G_2)$$

Nessas condições, temos

$$\gamma_{k+1}(G_1 \times G_2) = [\gamma_k(G_1 \times G_2), G_1 \times G_2] \subseteq \gamma_{k+1}(G_1) \times \gamma_{k+1}(G_2)$$

, e portanto $\gamma_n(G_1 \times G_2) \subseteq \gamma_n(G_1) \times \gamma_n(G_2)$ para todo $n \in \mathbb{N}$. Observemos que $\gamma_{k+1}(G_2) \times \gamma_{k+1}(G_2)$ é um subgrupo de $G_1 \times G_2$, uma vez que produto cartesiano de subgrupos é subgrupo. Observemos também que $\gamma_{k+1}(G_1 \times G_2)$ é o subgrupo de $G_1 \times G_2$ gerado pelo conjunto $\{[x, y] \mid x \in \gamma_k(G_1 \times G_2), y \in G_1 \times G_2\}$.

Agora, sendo G_1 e G_2 nilpotentes temos que existem $n_1, n_2 \in \mathbb{N}$ tais que $cl(G_1) = n_1$ e $cl(G_2) = n_2$, ou seja, $\gamma_{n_1+1}(G_1) = \{e_1\}$ e $\gamma_{n_2+1}(G_2) = \{e_2\}$, e portanto, tomando $n_0 = max\{n_1, n_2\}$, temos $\gamma_{n_0+1}(G_1 \times G_2) \subseteq \gamma_{n_0+1}(G_1) \times \gamma_{n_0+1}(G_2) = \{e_1\} \times \{e_2\}$, donde $G_1 \times G_2$ é nilpotente. □

O próximo teorema apresenta uma condição suficiente para garantir a nilpotência de um grupo.

Teorema 21. *Seja G um grupo. Se $G/Z(G)$ é nilpotente, então G também o é. Ademais, $cl(G) = cl(G/Z(G)) + 1$.*

Demonstração. De fato, seja $n_0 = cl(G/Z(G))$. Então $\gamma_{n_0+1}(G/Z(G)) = \{\overline{e}\}$, donde $\gamma_{n_0+1}(G)Z(G)/Z(G) = \{\overline{e}\}$(vide demonstração da Proposição 5, ou seja, $\gamma_{n_0+1}(G)Z(G) = Z(G)$. Daí, $\gamma_{n_0+1}(G) \subseteq Z(G)$ e consequentemente $\gamma_{n_0+2}(G) = \{e\}$. Logo G é nilpotente. Agora, por $n_0 = cl(G/Z(G))$ segue que $\gamma_{n_0}(G/Z(G)) \neq \{\overline{e}\}$, e daí temos $\gamma_{n_0}(G) \nsubseteq Z(G)$. Assim $\gamma_{n_0+1}(G) \neq \{e\}$, donde $cl(G) = n_0 + 1$. □

Agora apresentaremos uma condição necessária e suficiente para garantir a nilpotência de um grupo.

Proposição 6. *Um grupo G é nilpotente de classe menor ou igual a n se, e somente se, a igualdade $[x_1, x_2, ..., x_n, x_{n+1}] = e$ é válida sejam quais forem $x_1, x_2, ..., x_n, x_{n+1} \in G$.*

Demonstração. Mostremos por indução que $[x_1, ..., x_n] \in \gamma_n(G)$ para todo $n \in \mathbb{N}$. De fato, claramente esse fato é verdadeiro para $n = 1$ e $n = 2$. Agora suponha, por indução, $[x_1, ..., x_k] \in \gamma_k(G)$ para algum $k \in \mathbb{N}$. Observe que $[[x_1, ..., x_k], x_{k+1}] = [x_1, ..., x_k, x_{k+1}]$, e como $[[x_1, ..., x_k] \in \gamma_k(G)$ e $x_{k+1} \in G$ temos que $[x_1, ..., x_k, x_{k+1}] = [[x_1, ..., x_k], x_{k+1}] \in [\gamma_k(G), G] = \gamma_{k+1}(G)$. Logo, $[x_1, ..., x_n] \in \gamma_n(G)$ para todo $n \in \mathbb{N}$. Notemos agora que se G tem classe de nilpotência menor ou igual a n, então $\gamma_{n+1}(G) = \{e\}$. Pelo que foi feito acima

temos $[x_1, ..., x_n, x_{n+1}] = e$ para quaisquer $x_1, ..., x_n, x_{n+1} \in G$, e portanto a condição é necessária.

Reciprocamente, se $n = 1$, isto é, $[x_1, x_2] = e$, para quaisquer $x_1, x_2 \in G$, temos que G é abeliano, e portanto $cl(G) = 1$. Agora suponhamos o resultado válido para algum $k \in \mathbb{N}$, e suponhamos também que $[x_1, ..., x_k, x_{k+1}, x_{k+2}] = e$ para quaisquer $x_1, ..., x_k, x_{k+1}, x_{k+2} \in G$, ou seja, $[[x_1, ..., x_k, x_{k+1}], x_{k+2}] = e$ quaisquer que sejam $x_1, ..., x_k, x_{k+1}, x_{k+2} \in G$. Daí, $[x_1, ..., x_k, x_{k+1}]$ para quaisquer $x_1, ..., x_k, x_{k+1} \in G$. Logo, $\overline{e} = \overline{[x_1, ..., x_n, x_{n+1}]} = [\overline{x_1}, ..., \overline{x_n}, \overline{x_{n+1}}]$ no grupo quociente $G/Z(G)$, e temos por hipótese de indução que $G/Z(G)$ é nilpotente tal que $cl(G/Z(G)) \leqslant n$. Segue do teorema anterior que G é nilpotente e $cl(G)$ é menor ou igual a $n + 1$. Dessa forma segue por indução que o resultado é válido para todo $n \in \mathbb{N}$. □

Teorema 22. *Sejam G um grupo nilpotente e H um subgrupo normal de G, tal que $H \neq \{e\}$. Então, $H \cap Z(G) \neq \{e\}$.*

Demonstração. Sendo G nilpotente, existe $n \in \mathbb{N}$ tal que $Z_n(G) = G$. Considere $n_0 = min\{n \in \mathbb{N} \mid H \cap Z_n(G) \neq \{e\}\}$. Por H ser normal em G, $H \cap Z_{n_0}(G) \subseteq H$ e $H \cap Z_{n_0}(G) \subseteq Z_{n_0}(G)$ temos que $[H \cap Z_{n_0}(G), G] \subseteq H$ e $[H \cap Z_{n_0}(G), G] \subseteq Z_{n_0-1}(G)$. Logo,

$$[H \cap Z_{n_0}(G), G] \subseteq H \cap Z_{n_0-1}(G) = \{e\}$$

e portanto $\{e\} \neq H \cap Z_{n_0}(G) \subseteq H \cap Z(G)$. □

Observação 20. *Sejam G um grupo e N e M subgrupos de G. Então,*

i) Dizemos que M é um subgrupo maxial *de G se $M \neq G$ e não existe M_1 subgrupo de G tal que $M \subsetneq M_1 \subsetneq G$.*

ii) Dizemos que N é um subgrupo minimal *de G se $\{e\} \neq N$ e não existe subgrupo N_1 de G tal que $\{e\} \subsetneq N_1 \subsetneq N$.*

Corolário 6. *Um subgrupo normal minimal de um grupo nilpotente está contido no seu centro.*

Outro importante resultado é apresentado a seguir.

Teorema 23. *Seja G um grupo nilpotente. Se H é um subgrupo próprio de G, então $N_G(H) \neq H$.*

Demonstração. Sabemos que existe um menor $n \in \mathbb{N}$ tal que $\gamma_n(G) = \{e\}$ e $\gamma_1(G) = G$. Então podemos tomar $n_0 = min\{n \in \mathbb{N} \mid \gamma_{n+1}(G) \subseteq H\}$.

Observe que $\gamma_{n_0} \nsubseteq H$. Afirmamos que $\gamma_{n_0}(H) \subseteq N_G(H)$. De fato, perceba que

$$[\gamma_{n_0}(G), H] \subseteq [\gamma_{n_0}(G), G] = \gamma_{n_0+1}(G) \subseteq H$$

Nessas condições, recorde que devemos ter $\gamma_{n_0}(H) \subseteq N_G(H)$(vide Lema 6). Dessa forma, devemos ter $H \subsetneq N_G(H)$, e portanto segue o teorema. □

Corolário 7. *Sejam G um grupo nilpotente e M um subgrupo maximal de G. Então, M normal é em G.*

Demonstração. Por M ser um subgrupo maximal é fato que M é um subgrupo próprio de G, e assim segue do teorema anterior que $N_G(M) \neq M$. Logo, $M \subsetneq N_G(M)$ e segue da maximalidade de M que $N_G(M) = G$. Donde, $M \trianglelefteq G$. □

2.3 Grupos Nilpotentes Finitos

Nossa intenção nessa seção é mostrar uma importante caracterização dos grupos nilpotentes finitos. A seguir apresentaremos 7 condições que equivalem à nilpotência, no caso de grupo finito.

Eis o resultado.

Teorema 24. *Sejam G um grupo finito. Então são equivalentes:*

i) G é nilpotente.

ii) Se H é um subgrupo próprio de G, então $N_G(H) \neq H$.

iii) Todo subgrupo maximal de G é normal em G.

iv) Todo subgrupo de Sylow de G é normal em G.

v) $G \simeq G_1 \times G_2 \times ... \times G_m$, onde G_i é potência de primo.

vi) Dado n um divisor de $|G|$, existe algum $H \trianglelefteq G$ com $|H| = n$.

vii) Dados $a, b \in G$, com $mdc(o(a), o(b)) = 1$, tem-se $ab = ba$.

viii) Para todo N subgrupo normal próprio de G tem-se $Z(G/N)$ não trivial.

Demonstração. Pelo Teorema 23 e o Corolário 7 já temos i)⇒ ii) e ii) ⇒ iii). Agora, suponha que iii) seja verdadeira e iv) seja falsa. Então deve existir p divisor primo de $|G|$ tal que algum S_p-subgrupo P de G não seja normal, ou seja, $N_G(P) \neq G$. Tomemos agora M subgrupo maximal de G que contenha

$N_G(P)$. Sendo $g \in G$, um elemento arbitrário, temos $P^g \subseteq M^g \subseteq M$, já que M é normal. Temos que P e P^g são S_p-subgrupos de G contidos em M e então, por maior razão, P e P^g são S_p-subgrupos de M. Logo, pelo Segundo Teorema de Sylow, deve existir $x \in M$ tal que $P^g = P^x$, donde $gx^{-1} \in N_G(P) \subseteq M$. Daí, é fácil ver que $g \in N_G(P)$. Como g foi tomado arbitrário, segue que $N_G(P) = G$, mas isso é um absurdo, já que M é maximal. Recorde que essa contradição foi gerada ao supor que nem todo subgrupo de Sylow é normal em G. Portanto, iv) não pode ser falsa.

iv)$\Rightarrow$ v) Sejam $p_1, ..., p_m$ todos os divisores primos de $|G|$. Considere P_i um $S_{p_i} - subgrupo$ de G para cada $i = 1, ..., m$. Recorde que iv) garante a normalidade de cada P_i em G. Ademais, é fácil ver que $P_j \cap (P_1...P_{j-1}P_{j+1}...P_m) = \{e\}$ (vide Corolário 1 e o Teorema 3), com $j = 1, ..., m$ e $P_1...P_m = G$. Dessa maneira temos que G é o produto direto interno de $P_1, ..., P_m$ e portanto, $G \simeq P_1 \times ... \times P_m$. Agora, basta tomar $G_i = P_i$, com $i = 1, ..., m$ para ter o resultado.

v) $\Rightarrow$ *vi)* Sendo $G \simeq G_1 \times ... \times G_m$, consideremos $|G_i| = p_i^{k_i}$, para cada $i = 1, ..., m$. Não é difícil ver que $|G| = |G_1|...|G_m| = p_1^{k_1}...p_m^{k_m}$. Logo, se n é um divisor de $|G|$ temos que $n = p_1^{l_1}...p_m^{l_m}$, com $0 \leq l_i \leq k_i$ e $i = 1, ..., m$. O Exemplo 24 assegura a existência de subgrupos normais N_i de G_i tais que $|N_i| = p_i^{l_i}$ para cada $i = 1, ..., m$. Agora, consideremos $\varphi : G_1 \times ... \times G_m \longrightarrow G$ um isomorfismo e tomemos $H = \varphi(N_1 \times .... \times N_m)$. Temos claramente que H é um subgrupo normal de G de ordem $|H| = |\varphi(N_1 \times .... \times N_m)| = |N_1 \times .... \times N_m| = |N_1|....|N_m| = p_1^{l_1}...p_m^{l_m} = n$, donde segue o resultado.

vi) $\Rightarrow$ *vii)* Tomemos $a, b \in G$ tais que $\circ(a)$ e $\circ(b)$ sejam relativamente primas. Como $\circ(a)$ e $\circ(b)$ dividem $|G|$ é fácil ver que podemos escrever $|G| = mn$, com m e n relativamente primos e tais que $\circ(a)$ divide m e $\circ(b)$ divida n. Desde que *vi)* garante a existência de subgrupos N e H normais em G de ordens m e n, respectivamente, observemos que $|\langle a \rangle|$ divide $|N| = n$ e $|\langle b \rangle|$ divide $|H| = m$. Como estamos nas hipóteses do Lema 2, podemos garantir que $< a > \subseteq N$ e $< b > \subseteq H$, donde $a \in N$ e $b \in H$. Por outro lado, $[N, H] \subseteq N \cap H = \{e\}$ e portanto $[a, b] = e$. Logo, $ab = ba$.

vii) $\Rightarrow$ *viii)* Seja N um subgrupo normal próprio de G. Temos que, existe p primo divisor de $|G : N|$. Logo, sendo P um S_p-subgrupo de G, ao escrevermos $N_1 = P \cap N \trianglelefteq P$, devemos ter $N_1 \neq P$, pois p divide $|G : N|$ e assim $P \nsubseteq N$. Note que P/N_1 é um p-grupo não trivial, donde $Z(P/N_1)$ tem ordem divisível por p, portanto é não trivial. Então existe $\overline{a} \in Z(P/N_1)$, com $a \in P - N_1$, e assim $[a, x] \in N_1$ para todo $x \in P$. Consideremos, o subconjunto K_a de G, dado por

$$K_a = \{x \in G \mid [a, x] \in N\}$$

e observemos que:

i) $e = [a, e]$. Logo, $e \in K_a$.

ii) Se $x, y \in K_a$, então $[a, x], [a, y] \in N$, donde $[a, xy] = [a, y][a, x]^y \in N$, já que N é normal.

iii) Se $x \in K_a$, temos $[a, x] \in N$, logo$e[a, xx^{-1}] = [a, x^{-1}][a, x]^{-1} \in N$ e assim $[a, x^{-1}] \in N$. Portanto $x^{-1} \in K_a$.

Dessa forma temos que K_a é um subgrupo. Agora, afirmamos que em verdade temos $K = G$. Claramente $P \subseteq K_a$. Agora, tomemos q divisor primo de $|G|$, com $p \neq q$, e consideremos Q um $S_q - subgrupo$ de G. Com efeito, $\circ(a)$ é relativamente prima com a ordem de qualquer elemento de Q e então, por hipótese temos $ag = ga$ para todo $g \in Q$, ou seja, $[a, g] = e \in N$ para todo $g \in Q$. Logo $Q \subseteq K_a$. Sendo assim, temos que $|P|$ e $|Q|$ dividem $|K_a|$, o que nos dá $|K_a| = |G|$ e consequentemente temos a afirmação. Dessa forma, $[a, x] \in N$ para todo $x \in G$, e daí $\overline{a} = aN \in Z(G/N)$. Isso conclui a demonstração, pois $\overline{a} \neq \overline{e}$, já que $a \notin N$.

viii) $\Rightarrow$ *i)* Claramente $Z_0(G) \subsetneq Z_1(G)$. Se $Z_1(G) = G$, a demonstração acaba aqui, pois já teríamos G nilpotente. Do contrário, por $Z_1(G) \trianglelefteq G$, temos por hipótese, que $Z(G/Z_1(G)) = Z_2(G)/Z_1(G)$ é não trivial, donde $Z_1(G) \subsetneq Z_2(G)$. Seguindo o raciocínio indutivamente, temos que se para um certo $k \in \mathbb{N}$ for verdade que $Z_k(G) = G$, já teremos o resultado desejado; caso contrário, como $Z_K(G) \trianglelefteq G$ por hipótese segue que $Z(G/Z_k(G)) = Z_{k+1}(G)/Z_k(G)$ é não trivial, e portanto $Z_k(G) \subsetneq Z_{k+1}(G)$. Dessa forma temos a série central ascendente

$$Z_0(G) \subsetneq Z_1(G) \subsetneq ... \subsetneq Z_k(G) \subsetneq Z_{k+1}(G) \subsetneq ...$$

de subgrupos de G. Sendo G finito, deve existir $n \in \mathbb{N}$ tal que $Z_n(G) = G$ e o resultado segue.

□

2.4 p-Nilpotência de Grupos

Nesta seção daremos uma breve introdução do que vem a ser p-nilpotência de grupos e retornaremos a este assunto no próximo capítulo, após o estudo do homomorfismo transfer. Este, por sua vez, servirá de ferramenta para mostrarmos uma condição suficiente para que um grupo finito seja p-nilpotente para algum p primo divisor da ordem do grupo em questão. Antes disso, precisaremos de algumas definições e resultados , os quais passamos a tratar logo a seguir.

Definição 24. *Sejam G um grupo e H e K subgrupos de G. Dizemos que K é um complemento para H em G se $G = HK$ e $K \cap H = \{e\}$.*

Da definição acima é fácil ver que K também é complemento para qualquer conjugado de H.

Observação 21. *Sendo K um complemento para H em G, observemos que $|G| = |KH| = |K||H|/|K \cap H| = |K||H|$, donde $|K| = |G|/|H| = |G : H|$.*

Definição 25. *Sejam G um grupo finito e H um subgrupo de G. Dizemos que H é um um subgrupo de* Hall *de G se $mdc(|H|, |G : H|) = 1$.*

Observação 22. *Não é difícil ver que se G é um grupo finito e H e K são subgrupos de G, com H subgrupo de Hall,então K é um complemento para H em G se, e somente se, $|K| = |G : H|$.*

Definição 26. *Sejam G um grupo finito e p um divisor primo de $|G|$. Dizemos que um subgrupo N de G é um p-complemento em G se N é um complemento para algum p-subgrupo de Sylow de G.*

Observação 23. *Observemos que um p-complemento é um subgrupo de ordem $|G : P|$, onde P é um p-subgrupo de Sylow de G.*

Definição 27. *Sejam G um grupo finito e p um divisor primo de $|G|$. Consideremos P um p-subgrupo de Sylow de G. Diremos que G é p-nilpotente se existe N subgrupo normal em G tal que $G = PN$ e $P \cap N = \{e\}$, neste caso, N é referido como sendo um p-complemento normal em G.*

Para fixar as ideias vamos a alguns exemplos.

Exemplo 20. *Seja G um grupo de ordem 22, então G é 2-nilpotente.* De fato, segue dos Teoremas de Sylow que existem subgrupos H e N de G de ordens 2 e 11 , respectivamente. Ademais, N é o único subgrupo de ordem 11 e dessa forma N é normal em G. Por outro lado, $N \cap H = \{e\}$ e $G = HN$. Logo, N é 2-complemento normal para H em G, e portanto o resultado segue.

Exemplo 21. *Sendo G um grupo abeliano finito, então G é p-nilpotente para todo p primo divisor da ordem de $|G|$.* De fato, consideremos p um primo divisor de $|G|$ e P um p-subgrupo de Sylow de G. Tomemos $n = |G : P|$. Como $n = |G : P|$ divide $|G|$ temos pela Observação 5 que exite N subgrupo de G de ordem n. Desde que G seja abeliano temos que N é normal em G e consequentemente PN é um subgrupo de G tal que $mdc(|N|, |P|) = madc(|G : P|, |P|) = 1$. Logo, $P \cap N = \{1\}$ e dai $|G| = |G : P||P| = |N||P|/|P \cap N| = |PN|$ e assim $G = PN$, logo N é um p-complemento normal em G. Donde segue que G é p-nilpotente.

Teorema 25. *Um grupo finito G é nilpotente se, e somente se, é p-nilpotente para todo p primo divisor de $|G|$.*

Demonstração. Sejam $p_1, ..., p_m$ todos os divisores primos de $|G|$. Pelo item (iv) do Teorema 24 temos que $P_i \trianglelefteq G$ para todo $i = 1, ..., m$. Logo $P_1...P_m$ é um subgrupo de G e, pelo Lema 3, temos que $|G| = |P_1|...|P_m| = |P_1...P_m|$, e portanto temos $G = P_1...P_m$. Basta notar agora que $P_i \cap (P_1...P_{i-1}P_{i+1}...P_m) = \{1\}$, pois $mdc(|P_i|, |P_1...P_{i-1}P_{i+1}...P_n|) = 1$ para todo $i = 1, ..., m$, para concluir que $(P_1...P_{i-1}P_{i+1}...P_m)$ é um p_i-complemento normal, para cada $i = 1, ..., m$, e portanto G é p_i-nilpotente para todo p_i.

Reciprocamente, consideremos $p_1, ..., p_m$ todos os divisores primos de $|G|$, P_i um p_i-subgrupo de Sylow de G e N_i um p_i-complemento normal em G, para cada $i = 1, ..., m$. Temos que $|G| = |P_i||N_i|$ para cada $i = 1, ..., m$.

Afirmamos que $P_i = N_1 \cap \cdots \cap N_{i-1} \cap N_{i+1} \cap \cdots \cap N_n$. No intuito de simplificar as notações, mostremos que $P_1 = N_2 \cap \cdots \cap N_n$ (o caso geral segue de forma análoga). De fato, não é difícil ver que $|P_1|$ divide $|N_i|$, para cada $i = 2, ..., m$ (basta notar que $|P_1||N_1| = |G| = |P_i||N_i|$ e que $mdc(|P_1|, |P_i|) = 1$. Como N_i é normal em G e $mdc(|N_i|, |G : N_i|) = 1$, temos pelo Lema 2 que $P_1 \subseteq N_i$ para cada $i = 2, ..., m$. Logo $P_1 \subseteq N_2 \cap \cdots \cap N_n$.

Por outro lado, observa-se que $|P_1| = mdc(|N_2|, ..., |N_n|)$, pois p_i não divide $|N_i|$, para cada $i = 2, ..., m$, donde p_i não divide $mdc(|N_2|, ..., |N_n|)$, para cada $i = 2, ..., m$, e assim $mdc(|N_2|, ..., |N_n|)$ deve ser potência de p_1. Como $|N_2 \cap \cdots \cap N_n|$ divide $|N_i|$,para cada $i = 2, ..., m$, sendo $|N_2 \cap \cdots \cap N_n|$ potência de p_1 e divisor de $|G|$, deve divide $|P_1|$, donde segue a afirmação. Como a interseção de subgrupos normais é normal, temos que P_1 é normal. Repetindo o mesmo argumento podemos concluir que $P_i \trianglelefteq G$, e daí P_i é o único p_i-subgrupo de Sylow de G (vide o Corolário 5 do Segundo Teorema de Sylow), para todo $i = 1, ..., n$. Segue do Teorema 24 que G é nilpotente, o que encerra a demonstração.

□

Capítulo 3

O Homomorfismo Transfer

Neste capítulo estudaremos o homomorfismo transfer com o intuito de obter resultados sobre um importante critério de p-nilpotência de grupos, o de Burnside.

Considere G um grupo e H um subgrupo de índice n em G. Agora, escolhamos um transversal à direita $\{t_1, ..., t_n\}$ para H em G. Observemos, em primeiro lugar, que se multiplicarmos um elemento $g \in G$ à direita por uma classe lateral à direita Ht_i, teremos ainda uma classe lateral à direita, a saber Ht_ig, e esta será uma das classes Ht_j, para algum $j \in \{1, 2, \ldots, n\}$, já que $G = \bigcup_{i=1}^{n} Ht_i$, ou seja, $Ht_ig = Ht_{(i)g}$, com $(i)g \in \{1, 2, \ldots, n\}$. Mostremos que a aplicação $i \longmapsto (i)g$ é uma permutação do conjunto $\{1, 2, \ldots, n\}$. Vejamos a injetividade; sejam $i, j \in \{1, 2, \ldots, n\}$ tais que $(i)g = (j)g$. Daí,

$$Ht_{(i)g} = Ht_{(j)g}.$$

Portanto, $Ht_ig = Ht_jg$, donde, $Ht_i = Ht_j$. Logo, $i = j$. Recorde que toda aplicação injetiva de um conjunto finito em si próprio é sobrejetora. Dessa forma temos que a aplicação $i \mapsto (i)g$ é uma bijeção e portanto uma permutação do conjunto $\{1, 2, \ldots, n\}$. Ademais, observe que $t_igt_{(i)g}^{-1} \in H$, para todo $i \in \{1, 2, \ldots, n\}$.

Agora, considere A um grupo abeliano qualquer e $\theta : H \longrightarrow A$ um homomorfismo de grupos. Definimos o *transfer de* θ como sendo a aplicação $\theta^* : G \longmapsto A$ tal que

$$\theta^*(x) = \prod_{n=1}^{n} \theta(t_ixt_{(i)x}^{-1}),$$

para todo $x \in G$. Observe que $t_ixt_{(i)x}^{-1} \in H$ e $\theta(t_ixt_{(i)x}^{-1}) \in A$, para quaisquer $i \in \{1, \ldots, n\}$ e $x \in G$.

Um fato vantajoso da aplicação $\theta^* : G \longrightarrow A$, que nos permite obter vários resultados interessantes da teoria de grupos, é que esta aplicação é um homomorfismo que independe da escolha do transversal (sendo assim bem definido). Por formalidade iremos enunciar esse resultado como

Lema 11. *A aplicação $\theta^* : G \longrightarrow A$ é um homomorfismo o qual independe da escolha do transversal.*

Demonstração. i) Primeiro mostraremos a independência do transversal. Seja $\{t_1^{'}, \ldots, t_n^{'}\}$ um outro transversal à direita para H em G. Perceba que podemos supor $Ht_i = Ht_i^{'}$ para cada $i = 1, ..., n$ (caso não seja, reorganize os t_i's). Dessa forma teremos $t_i^{'}t_i^{-1} \in H$, isto é, $t_i^{'} = h_i t_i$, para todo $i = 1, ..., n$.

Tomemos $x \in G$ e observemos que

$$t_i^{'} x t_{(i)x}^{'-1} = h_i t_i x t_{(i)x}^{-1} h_{(i)x}^{-1}.$$

Como A é abeliano e θ é um homomorfismo temos que

$$\begin{aligned}
\prod_{i=1}^{n} \theta(t_i^{'} x t_{(i)x}^{'-1}) &= \prod_{i=1}^{n} \theta(h_i t_i x t_{(i)x}^{-1} h_{(i)x}^{-1}) \\
&= \prod_{i=1}^{n} \theta(h_i)\theta(t_i x t_{(i)x}^{-1})\theta(h_{(i)x}^{-1}) \\
&= \prod_{i=1}^{n} \theta(t_i x t_{(i)x}^{-1})\theta(h_i)\theta(h_{(i)x}^{-1}) \\
&= \prod_{i=1}^{n} \theta(t_i x t_{(i)x}^{-1}) \prod_{i=1}^{n} \theta(h_i)\theta(h_{(i)x}^{-1}) = \prod_{i=1}^{n} \theta(t_i x t_{(i)x}^{-1}).
\end{aligned}$$

Observe que na última igualdade usamos o fato de $i \mapsto (i)x$ ser uma permutação do conjunto $\{1, \ldots, n\}$.

ii) Mostremos agora que θ^* é um homomorfismo. Primeiro note que se $x, y \in G$, então

$$Ht_{(i)xy} = Ht_i xy = H(t_i x)y = Ht_{((i)x)y}.$$

Portanto, $t_{(i)xy} = t_{((i)x)y}$. Daí,

$$\begin{aligned}
\theta^*(xy) &= \prod \theta(t_i x y t_{(i)xy}^{-1}) = \prod \theta(t_i x y t_{((i)x)y}^{-1}) \\
&= \prod \theta(t_i x t_{(i)x}^{-1} t_{(i)x} y t_{((i)x)y}^{-1}) \\
&= \prod \theta(t_i x t_{(i)x}) \theta(t_{(i)x} y t_{((i)x)y}) \\
&= \prod \theta(t_i x t_{(i)x}) \prod \theta(t_{(i)x} y t_{((i)x)y}^{-1}) \\
&= \theta^*(x)\theta^*(y).
\end{aligned}$$

Observe que na penúltima igualdade usamos o fato de A ser abeliano e na última o fato de $i \mapsto (i)x$ ser permutação.

□

Como θ^* independe da escolha do transversal à direita, é natural nos perguntarmos se existe uma melhor escolha do transversal de tal forma que o cálculo do valor de $\theta^*(x)$ se torne mais simples, para um dado $x \in G$. A resposta a essa pergunta é positiva e passaremos agora a mostrar como isso pode ser feito. Para não fugirmos do rigor matemático, vamos ao

Lema 12 (Cálculo de θ^*)**.** *Sejam H um subgrupo de G de índice n e $\theta : H \to A$ um homomorfismo, onde A é um grupo abeliano. Então, para cada $x \in G$, existem $k, l_1, \ldots, l_k \in \mathbb{N}$ e $s_1, ..., s_k \in G$ tais que*

$$\theta^*(x) = \prod_{i=1}^{k} \theta(s_i x^{l_i} s_i^{-1}),$$

onde $\sum_{i=1}^{k} l_i = n$.

Demonstração. Tomemos $s_1 \in G$, fixo, e consideremos as classes laterais à direita de H e G

$$Hs_1, Hs_1x, Hs_1x^2, \ldots$$

Observe que existe um número finito de classes laterais, pois $|G : H| = n$. Portanto, podemos tomar $l_1 = \min\{n \in \mathbb{N} \mid Hs_1x^n = Hs_1\}$. Temos as classes

$$Hs_1, \ldots, Hs_1x^{l_1-1}. \tag{3.1}$$

Se estas não forem todas as classes laterais à direita de H em G, escolha $s_2 \in G$ tal que $Hs_2 \neq Hs_1x^i$, para todo $i = 0, \ldots, l_1 - 1$. Procedendo de maneira análoga, tomemos $l_2 \in \mathbb{N}$ o menor natural tal que $Hs_2 = Hs_2x^{l_2}$. Portanto, temos as classes

$$Hs_2, Hs_2x, \ldots, Hs_2x^{l_2-1}. \tag{3.2}$$

Se as classes laterais obtidas em (3.1) juntamente com as classes obtidas em (3.2) ainda não formam todas as classes laterais à direita para H em G, repita o processo até que esse fato ocorra (isso é possível pois $|G : H| = n$). Dessa forma, encontramos $k \in \mathbb{N}$ e $l_1, \ldots, l_k \in \mathbb{N}$ tais que

$$Hs_1, \ldots, Hs_1x^{l_1-1}, Hs_2, \ldots, Hs_2x^{l_2-1}, \ldots, Hs_kx^{l_k-1} \tag{3.3}$$

são todas as classes laterais à direita de H em G.

Observe que da construção obtemos $\sum_{i=1}^{k} l_i = n$ e

$$T = \{s_1, s_1x, \ldots, s_1x^{l_1-1}, s_2, s_2x, \ldots, s_2x^{l_2-1}, \ldots, s_k, \ldots, s_kx^{l_k-1}\}$$

é um transversal à direita para H em G.

Afiançado pelo lema anterior, trabalhemos com o transversal T. Escrevamos:

$$\begin{array}{rclcrclcrcl}
t_1 & = & s_1, & & t_2 & = & s_1x, & \ldots, & t_{l_1} & = & s_1x^{l_1-1}, \\
t_{l_1+1} & = & s_2, & & t_{l_1+2} & = & s_2x, & \ldots, & t_{l_1+l_2} & = & s_2x^{l_2-1}, \\
 & & & & & & & \vdots & & & \\
t_{(\sum_{i=1}^{k-1} l_i+1)} & = & s_k, & t_{(\sum_{i=1}^{k-1} l_i+2)} & = & s_kx, & \ldots, & & t_{(\sum_{i=1}^{k} l_i)} & = & s_kx^{l_k-1}.
\end{array}$$

Observe que

$$\begin{array}{rclcrcl}
Ht_{(1)x} & = & Ht_1x & = & Hs_1x & = & Ht_2, \\
Ht_{(2)x} & = & Ht_2x & = & Hs_2x & = & Ht_3, \\
 & & & \vdots & & & \\
Ht_{(l_1)x} & = & Ht_{l_1}x & = & Hs_1x^{l_1-1}x & = & Hs_1 = Ht_1.
\end{array}$$

Da mesma forma

$$\begin{array}{rcl}
Ht_{(l_1+1)x} = Ht_{(l_1+1)}x & = & Hs_2x = Ht_{(l_1+2)}, \\
Ht_{(l_1+2)x} = Ht_{(l_1+2)}x & = & H(s_2)x \cdot x = Hs_2x^2 = Ht_{(l_1+3)}, \\
 & \vdots & \\
Ht_{(l_1+l_2)x} = Ht_{(l_1+l_2)}x = H(s_2x^{l_2-1})x & = & Hs_2x^{l_2} = Hs_2 = Ht_{(l_1+1)}, \\
 & \vdots & \\
Ht_{(l_1+\cdots+l_{k-1}+1)x} = Ht_{(l_1+\cdots+l_{k-1}+1)}x & = & Hs_kx = Ht_{(l_1+\cdots+l_{k-1}+2)}, \\
Ht_{(l_1+\cdots+l_{k-1}+2)x} = Ht_{(l_1+\cdots+l_{k-1}+2)}x & = & Hs_kx^2 = Ht_{(l_1+\cdots+l_{k-1}+3)}, \\
 & \vdots & \\
Ht_{(\sum_{i=1}^{k} l_i)x} = Ht_{(\sum_{i=1}^{k} l_i)}x = Ht_nx & = & Hs_kx^k = Hs_k = Ht_{(l_1\cdots+l_{k-1}+1)},
\end{array}$$

e portanto $(i)x = i + 1$, $(l_1)x = 1$ e $(l_1 + \cdots + l_j)x = l_1 + \cdots + l_{j-1} + 1$, para todo $j = 2, \ldots, k$, donde

$$
\begin{aligned}
\theta^*(x) &= \prod_{i=1}^{n} \theta(t_1 x t_{(i)x}^{-1}) \\
&= \theta(t_1 x t_2^{-1})\theta(t_2 x t_3^{-1}) \cdot \ldots \cdot \theta(t_{l_1-1} x t_{l_1}^{-1})\theta(t_{l_1} x t_1^{-1}) \cdot \\
&\cdot \quad \theta(t_{l_1+1} x t_{l_1+2}^{-1})\theta(t_{l_1+2} x t_{l_1+3}^{-1}) \cdot \ldots \cdot \theta(t_{(l_1+l_2-1)} x t_{(l_1+l_2)}^{-1})\theta(t_{(l_1+l_2)} x t_{l_1+1}^{-1}) \\
&\vdots \\
&\cdot \quad \theta(t_{(l_1+\cdots+l_{k-1}+1)} x t_{(l_1+\cdots+l_{k-1}+2)}^{-1}) \cdot \ldots \cdot \theta(t_{(l_1+\cdots+l_k)} x t_{(l_1+\cdots+l_{k-1}+1)}) \\
&= \theta(t_1 x^{l_1} t_1^{-1})\theta(t_{(l_1+1)} x^{l_2} t_{(l_1+1)}^{-1}) \cdot \ldots \cdot \theta(t_{(l_1+\cdots+l_{k-1})} x^{l_k} t_{(l_1+\cdots+l_{k-1}+1)}^{-1}) \\
&= \theta(s_1 x^{l_1} s_1^{-1})\theta(s_2 x^{l_2} s_2^{-1}) \cdot \ldots \cdot \theta(s_k x^{l_k} s_k^{-1}) \\
&= \prod_{i=1}^{k} \theta(s_i x^{l_i} s_i^{-1}).
\end{aligned}
$$

□

3.1 O Homomorfismo Transfer sobre Subgrupos

Sendo G um grupo e H um subgrupo de G, observe que sempre podemos exibir um homomorfismo $\theta : H \to A$, onde A é um grupo abeliano. Basta tomar $A = H/H'$ e θ a projeção canônica, isto é,

$$
\begin{aligned}
\theta : H &\longrightarrow H/H' \\
h &\longmapsto \theta(h) = H'h
\end{aligned}
$$

Por estética matemática, denotemos $H/H' = H_{ab}$. Dessa forma o transfer $\theta* : G \longrightarrow H_{ab}$ é referido como sendo o transfer de G sobre H_{ab}. Se H for abeliano, então $H/H^{'}$ é isomorfo a H e θ pode ser vista como a aplicação identidade de H.

Veremos a seguir que o homomorfismo transfer, quando definido sobre subgrupos, se torna uma ferramenta muito poderosa para se obter resultados interessantíssimos e de maneira elegante, cujas demonstrações seriam tarefas muito difíceis sem o seu uso.

Teorema 26 (Schur)**.** *Sejam G um grupo e H um subgrupo de G tais que $H \subseteq Z(G)$ e $|G : H| = n$. Considere o homomorfismo $\theta : H \to H$, dado por $\theta(h) = h$, para todo $h \in H$. Então, o transfer de G em H é exatamente a aplicação $\theta^* : G \to H$, definida por $\theta^*(x) = x^n$, para todo $x \in G$.*

Demonstração. Usando o lema anterior temos que

$$\theta^*(x) = \prod_{i=1}^{k} \theta(s_i x^{l_i} s_i^{-1}).$$

Perceba que $s_i x^{l_i} s_i^{-1} = z_i \in H \subseteq Z(G)$, para todo $i = 1, \ldots, k$. Logo, $x^{l_i} = z_i \in Z(G)$, para todo $i = 1, \ldots, n$, uma vez que $x^{l_i} = s_i^{-1} z_i s_i = s_i^{-1} s_i z_i = z_i$. Portanto,

$$\begin{aligned} \theta^*(x) &= \prod_{i=1}^{k} \theta(s_i x^{l_i} s_i^{-1}) = \prod_{i=1}^{k} (s_i x^{l_i} s_i^{-1}) \\ &= \prod_{i=1}^{k} x^{l_i} = x^{l_1} \cdot \ldots \cdot x^{l_k} = x^{l_1 + \cdots + l_k} \\ &= x^n, \end{aligned}$$

já que $\sum_{i=1}^{n} l_i = n$. □

Outro resultado que ilustra a importância do homomorfismo transfer é o seguinte.

Teorema 27 (Schur)**.** *Seja G um grupo tal que $G/Z(G)$ é finito. Então G' é finito. Ademais, se $|G : Z(G)| = n$, então $x^n = 1$, para todo $x \in G'$.*

Demonstração. Sabemos, pelo lema anterior, que a aplicação $\theta^* : G \to Z(G)$ definida por $\theta^*(x) = x^n$, para todo $x \in G$, é o transfer de

$\theta : Z(G) \to Z(G)$, onde θ é dada por $\theta(z) = z$, para todo $z \in Z(G)$. Segue do 1° Teorema de Isomorfismo que

$$\frac{G}{\ker \theta^*} \simeq \operatorname{Im} \theta^* \leq Z(G).$$

Portanto, $G/\ker \theta^*$ é abeliano, donde segue que $G' \subseteq \ker \theta^*$. Logo, $x^n = 1$ para todo $x \in G'$. Desde que $G/Z(G)$ é finito devem existir $g_1, \ldots, g_n \in G$ tais que

$$\frac{G}{Z(G)} = \{Z(G)g_1, \ldots, Z(G)g_n\}.$$

Agora tomemos $x, y \in G$, arbitrários. Temos que $Z(G)x, Z(G)y \in G/Z(G)$ e logo existem $i, j \in \{1, \ldots, n\}$ tais que $Z(G)x = Z(G)g_i$ e $Z(G)y = Z(G)g_j$. Daí, $x = c_i g_i$ e $y = c_j g_j$, com $c_i, c_j \in Z(G)$. Observe que

$$\begin{aligned} [x, y] &= [c_i g_i, c_j g_j] = (c_i g_i)^{-1} (c_j g_j)^{-1} (c_i g_i)(c_j g_j) \\ &= g_i^{-1} c_i^{-1} g_j^{-1} c_j^{-1} c_i g_i c_j g_j = g_i^{-1} g_j^{-1} g_i g_j \\ &= [g_i, g_j]. \end{aligned}$$

Daí, $G' = \langle [x,y] \mid x,y \in G \rangle = \langle [g_i, g_j] | i,j \in \{1,\ldots,n\} \rangle$. Logo, G' é finitamente gerado. Pelo 2° teorema do isomorfismo temos

$$\frac{G'}{G' \cap Z(G)} \simeq \frac{G'Z(G)}{Z(G)}.$$

Observe que $G'Z(G)/Z(G)$ é finito, já que é subgrupo de $G/Z(G)$. Assim, $G'/G' \cap Z(G)$ é finito. Segue de (1.6.11) de [6] que $G' \cap Z(G)$ é finitamente gerado. Recorde que $G' \cap Z(G) \subset Z(G)$, $G' \cap Z(G)$ é finitamente gerado e $G' \cap Z(G)$ é de torção ($x^n = 1$ para todo $x \in G' \cap Z(G)$). Portanto, segue do Teorema 2 que $G' \cap Z(G)$ é finito, o que conclui a demonstração. □

3.2 Transfer sobre p-subgrupos de Sylow

Vimos anteriormente resultados belíssimos acerca da teoria de grupos, que surgem da definição do homomorfismo transfer sobre subgrupos. Veremos adiante que a beleza e importância dos resultados só aumentam se os subgrupos em questão forem p-subgrupos de Sylow do grupo abordado.

Continuemos com a mesma notação. Dado um grupo finito G e p um divisor primo de $|G|$, denotemos por $G'(p)$ a interseção de todos os subgrupos normais N de G tais que G/N seja um p-grupo abeliano.

Sejam $N_1, \ldots, N_m$ todos os subgrupos normais de G tais que G/N_i é p-grupo abeliano, isto é, $G'(p) = N_1 \cap \ldots \cap N_m$. Definamos a aplicação

$$\begin{array}{rcl} \varphi : G & \longrightarrow & G/N_1 \times \cdots \times G/N_m \\ g & \longmapsto & \varphi(g) = (N_1 g, \ldots, N_m g) \end{array}.$$

É fácil ver que φ é um homomorfismo tal que $\ker \varphi = G'(p)$. Daí,

$$\frac{G}{G'(p)} \simeq \operatorname{Im} \varphi \leq \frac{G}{N_1} \times \cdots \times \frac{G}{N_m}.$$

donde temos que $G/G'(p)$ é um p-grupo abeliano. Além disso, segue da construção que $G/G'(p)$ é o maior p-quociente abeliano de G. Ademais, $G' \subseteq G'(p)$, já que $G/G'(p)$ é, em particular, abeliano.

Proposição 7. *Seja $\tau : G \to P_{ab}$ o transfer de um grupo finito G sobre um p-subgrupo de Sylow P. Então, $G'(p)$ é o núcleo de τ e $P \cap G'$ é o núcleo de τ restrito a P.*

Demonstração. Escrevamos $K = \ker \tau$. Em primeiro lugar observemos que $G'(p) \subseteq K$, já que G/K é um p-grupo abeliano. Agora, fixado $x \in G$

arbitrário, escrevamos G como união das classes laterais à direita de P, como em (3.3), para obtermos

$$\tau(x) = P' \prod_{i=1}^{k} s_i x^{l_i} s_i^{-1},$$

com $\sum_{i=1}^{n} l_i = n$. Afirmamos que $G = PG'(p)$. De fato, $PG'(P) \subseteq G$. Por outro lado temos, $|G| = p^k \cdot n$, com $mdc(n, p) = 1$. Além disso,

$$n = |G : P| = |G : PG'(p)||PG'(p) : P| \text{ e}$$

$$p^{k_1} = |G : G'(p)| = |G : PG'(p)||PG'(p) : G'(p)|,$$

com $k_1 \leq k$. Daí, $|G : PG'(p)|$ divide n e p^{k_1}. Portanto, $|G : PG'(p)| = 1$, donde $G = PG'(p)$. Dessa forma podemos escolher os s_i's em $G'(p)$, e desse modo podemos escrever $\tau(x) = P'x^n c$, onde $c \in G'(p)$. De fato, passando a 'barra' com respeito ao grupo quociente $G/G'(p)$ (que é abeliano) obtemos,

$$\begin{aligned}
\overline{\prod_{i=1}^{k} s_i x^{l_i} s_i^{-1}} &= \prod_{i=1}^{k} \overline{s_i x^{l_i} s_i^{-1}} = \prod_{i=1}^{k} \overline{s_i} \cdot \overline{x^{l_i}} \cdot \overline{s_i^{-1}} \\
&= \prod_{i=1}^{k} \overline{x^{l_i}} = \overline{x^{l_i}} \cdot \ldots \cdot \overline{x^{l_k}} \\
&= \overline{x^{l_1} \cdot \ldots \cdot x^{l_k}} = \overline{x^n},
\end{aligned}$$

onde $n = |G : P|$. Portanto, se $x \in K$, então $P'x^n c = \tau(x) = \{\overline{e}\}$ em P_{ab}, donde, $x^n c \in P' \subset P'G'(p)$.

Observe agora que

$$\frac{G}{G'(p)} = \frac{PG'(p)}{G'(p)} \simeq \frac{P}{P \cap G'(p)},$$

pelo 2° Teorema de Isomorfismo, donde obtemos que $P/P \cap G'(p)$ é abeliano. Consequentemente, $P' \subset P \cap G'(p)$ e assim $P' \subset G'(p)$. Logo, $P'G'(p) = G'(p)$. Como $x^n c \in P'G'(p) = G'(p)$ e $c \in G'(p)$, temos que $x^n \in G'(p)$.

Em resumo, temos $x^n \in G'(p)$, para todo $x \in K$. Passando a 'barra' com respeito ao grupo quociente $G/G'(p)$, temos $\overline{x}^n = \overline{x^n} = \overline{e}$. Esse fato nos permite concluir que $o(\overline{x})$ divide n, para todo $\overline{x} \in K/G'(p)$. Portanto, pelo Teorema de Cauchy, $K/G'(p)$ é um grupo de ordem não divisível por p. Como $|K/G'(p)|$ deve dividir $|G/G'(p)|$, que é um p-grupo, devemos ter $|K/G'(p)| = 1$, ou seja, $K = G'(p)$, e isso completa a primeira parte da demonstração.

Agora, observemos que $\ker\tau|_P = P \cap \ker\tau = G'(p) \cap P \supseteq P \cap G'$. Segue imediato da Observação 2 que $k_1 = |PG'|/|P| = |G'|/|P \cap G'|$ e que $k_2 = |PG'(p)|/|P| = |G'(p)|/|P \cap G'(p)|$, e daí k_1 e k_2 não são divisíveis por p. Por outro lado, segue da definição de $G'(p)$, que $k = |G'(p)|/|G'|$ não é divisível por p. Temos que $|G'| = k_1|P \cap G'|$ e $|G'(p)| = k_2|P \cap G'(p)|$, e daí $kk_1|P \cap G'| = k_2|P \cap G'(p)|$, donde

$$kk_1 = k_2\frac{|P \cap G'(p)|}{|P \cap G'|}$$

e assim $|P\cap G'(p)|/|P\cap G'|$ não é divisível por p. Mas, $P\cap G'(p)$ e $P\cap G'$ são subgrupos de P, com $P\cap G' \subseteq P\cap G'(p)$, logo devemos ter $P\cap G' = P\cap G'(p)$. □

Se exigirmos que um p-subgrupo de Sylow P de um grupo finito G seja abeliano, os resultados obtidos com o auxílio do transfer são ainda mais interessantes, como veremos com o próximo teorema.

Observação 24. *Sejam G um grupo e H um subgrupo de G tal que $|G : H| = n$. Então, se $y \in N_G(H)$ e $\{t_1, ..., t_n\}$ é um transversal à direita para H em G, devemos ter que:*

i) Se $Ht_i^y = Ht_j^y$, então $t_i^y(t_i^y)^{-1} \in H$. Mas, $(t_it_j^{-1})^y = t_i^y(t_i^y)^{-1} \in H$, e daí $t_it_j^{-1} \in H$. Logo $i = j$, donde segue que $\{t_1^y, ..., t_n^y\}$ também é um transversal à direita para H em G.

ii) Se $x \in G$, então $Ht_ix = Ht_{(i)x}$. Logo $Ht_i^yx^y = Ht_{(i)x}^y$.

Teorema 28. *Seja G um grupo finito que possui um p-subgrupo de Sylow P abeliano. Denotando $N_G(P)$ por N, devemos ter que $P = C_P(N) \times [P, N]$. Além disso, se $\tau : G \to P$ é o transfer da identidade $\theta : P \to P$, então $\operatorname{Im}\tau = C_P(N)$ e $P \cap \ker\tau = [P, N]$.*

Demonstração. Como anteriormente, fixado $x \in G$ (arbitrário) podemos escrever $\tau(x) = \prod_{i=1}^k s_ix^{l_i}s_i^{-1}$, com $s_i \in G$ e $l_1 + ... + l_n = n = |G : P|$. Sendo $x \in P$, escrevamos $y_i = x^{l_i}$. Claramente $y_i \in P$, e $y_i^{s_i^{-1}} = s_iy_is_i^{-1} \in P$, pela forma como os $s_i's$ são tomados. Como P é abeliano, não é difícil ver que $P, P^{s_i^{-1}} \subseteq C_G(y_i^{s_i^{-1}})$. Denotemos $C_G(y_i^{s_i^{-1}})$ por C. Sendo $P, P^{s_i^{-1}} \subseteq C$, com $P, P^{s_i^{-1}}$ S_p-subgrupos de G, em particular de C, temos pelo 2° Teorema de Sylow que P e $P^{s_i^{-1}}$ são conjugados em C, isto é, existe $c_i \in C$ tal

que $(P^{s_i^{-1}})^{c_i} = P$. Daí, $r_i = s_i^{-1}c_i \in N_G(P) = N$. Agora, observemos que $y_i^{r_i} = y_i^{s_i^{-1}c_i} = c_i^{-1}s_iy_is_i^{-1}c_i = c_i^{-1}y_i^{s_i^{-1}}c_i = y_i^{s_i^{-1}}$, pois $c_i \in C = C_G(y_i^{s_i^{-1}})$. Logo,

$$\tau(x) = \prod_{i=1}^{n} s_i x^{l_i} s_i^{-1} = \prod_{i=1}^{n} y_i^{s_i^{-1}} = \prod_{i=1}^{n} y_i^{r_i} = \prod_{i=1}^{n} (x^{l_i})^{r_i}.$$

Recorde que $r_i \in N$, e portanto $(x_i^{l_i})^{r_i} \in P$, já que $x^{l_i} \in P$. Por P ser abeliano temos

$$\begin{aligned}
\tau(x) &= \prod_{i=1}^{n} (x^{l_i})^{r_i} = \prod_{i=1}^{n} x^{l_i}[(x^{l_i})^{-1}(x^{l_i})^{r_i}] \\
&= \prod_{i=1}^{n} x^{l_i} \prod_{i=1}^{n} [(x^{l_i})^{-1}(x_{l_i})^{r_i}] \\
&= \prod_{i=1}^{n} x^{l_i} \prod_{i=1}^{n} (x^{l_i})^{-1} r_i^{-1} x^{l_i} r_i \\
&= \prod_{i=1}^{n} x^{l_i} \prod_{i=1}^{n} [x^{l_i}, r_i] = x^n d, \qquad (3.4)
\end{aligned}$$

onde $d = \prod_{i=1}^{n} [x^{l_i}, r_i] \in [P, N]$ e $[G : P] = n$. Da última equação tiramos que $x^n = \tau(x)d^{-1}$, ou seja, $x^n \in \tau(P)[P, N]$, para todo $x \in P$ (vide Exemplo 14). Claramente temos, $\tau(P), [P, N] \subseteq P$ e, como P é abeliano, $\tau(P)[P, N]$ é subgrupo de P. Como $mdc(n, p) = 1$, temos que $x \in \tau(P)[P, N]$ para todo $x \in P$. Portanto

$$P = \tau(P)[P, N]. \qquad (3.5)$$

Afirmamos que

$$\tau(P) \cap \ker \tau = \{1\} \qquad (1 = e_G). \qquad (3.6)$$

De fato, seja $x \in P$ tal que $\tau(x) \in \tau(P) \cap \ker \tau$. Então

$$1 = \tau(\tau(x)) = \tau(x^n d) = \tau(x^n)\tau(d) = \tau(x)^n \tau(d)$$

tendo sido utilizada (3.4) na segunda igualdade da equação anterior. Pelo 2° Teorema de Isomorfismo temos que

$$\frac{G}{\ker \tau} \simeq \operatorname{Im} \tau \leq P.$$

Logo, $G/\ker \tau$ é abeliano, donde $G' \subseteq \ker \tau$. Assim, $\tau(d) = 1$, pois $d \in [P, N] \subseteq G'$, e dessa forma $\tau(x)^n = 1$. Como $mdc(|P|, n) = 1$, segue do

Exemplo 14 que $\tau(x) = 1$, e portanto a afirmação segue. Recorde que $G = PG'(P)$ e $G'(P) = \ker\tau$ (vide Proposição 7). Daí,

$$\operatorname{Im}\tau = \tau(G) = \tau(PG'(P)) = \tau(P)\tau(G'(P)) = \tau(P)\tau(\ker\tau) = \tau(P). \quad (3.7)$$

Juntando esse fato com (3.5) temos $P = (\operatorname{Im}\tau)[P, N]$.

Mostremos agora que $\operatorname{Im}\tau \trianglelefteq N$. Como $\operatorname{Im}\tau = \tau(P)$, basta mostrarmos que $\tau(x)^y \in \operatorname{Im}\tau$, para todo $x \in P$ e $y \in N$. Assim,

$$(\tau(x))^y = \prod_{i=1}^{n}(t_i x t_{i(x)}^{-1})^y = \prod_{i=1}^{n} t_i^y x^y (t_{(i)x}^{-1})^y = \prod_{i=1}^{n} t_i^x x^y (t_{(i)x}^y)^{-1},$$

onde $\{t_1, \ldots, t_n\}$ é um transversal à direita para P em G. Como τ independe da escolha do transversal, segue da observação acima que $\tau(x)^y = \tau(x^y) \in \operatorname{Im}\tau$. Logo, $\operatorname{Im}\tau \trianglelefteq N$, ou ainda, $N \subseteq N_G(\operatorname{Im}\tau)$. Nessas condições, devemos ter $[\operatorname{Im}\tau, N] \subseteq \operatorname{Im}\tau$. Por outro lado, $[\operatorname{Im}\tau, N] \subseteq [P, N]$. Logo,

$$[\operatorname{Im}\tau, N] \subseteq \operatorname{Im}\tau \cap [P, N] = \tau(P) \cap [P, N] \subseteq \tau(P) \cap G' \subseteq \tau(P) \cap \ker\tau = \{1\},$$

tendo sido utilizada a equação (3.6). Portanto, $\operatorname{Im}\tau \subseteq C_P(N)$. Seja $x \in C_P(N) \subseteq P$. Segue por (3.4) que $\tau(x) = x^n d$, com $d = \prod_{i=1}^{n}[x^{l_i}, r_i]$, onde $x^{l_i} \in P$ e $r_i \in N$. Mas, se $x \in C_P(N)$ temos que $x^{l_i} \in C_P(N)$ e daí $d = 1$. Portanto, $x^n = \tau(x) \in \operatorname{Im}\tau$, e segue do Exemplo 14 que $x \in \operatorname{Im}\tau$. Logo,

$$\operatorname{Im}\tau = C_P(N). \quad (3.8)$$

Segue de (3.5), (3.6), (3.7) e (3.8) que $P = C_P(N) \times [P, N]$.

Agora, seja $x \in P \cap \ker\tau$. Então $x \in P$ e $x \in \ker\tau$, e assim $1 = \tau(x) = x^{nd}$. Daí $x^n = d^{-1} \in [P, N]$, donde, pelo Exemplo 14, temos que $x \in [P, N]$. Portanto $P \cap \ker\tau \subseteq [P, N]$. Por outro lado, observemos que $[P, N] \subseteq P$ e $[P, N] \subseteq [G, G] = G' \subseteq \ker\tau$. Logo $[P, N] \subseteq P \cap \ker\tau$, donde segue que $P \cap \ker\tau = [P, N]$. □

Como prometido no capítulo 2, mostraremos agora, com o auxílio do homomorfismo transfer, uma condição suficiente para que o grupo finito G seja p-nilpotente para algum p divisor de $|G|$.

Teorema 29 (Burnside)**.** *Seja G um grupo finito. Se para algum primo p divisor de $|G|$ um p-subgrupo de Sylow P de G for tal que $C_G(P) = N_G(P)$, então G é p-nilpotente.*

Demonstração. Observe que, por hipótese, P é abeliano. Segue do teorema anterior que se $\tau : G \to P$ é o transfer de $\theta : P \to P$, onde $\theta = Id_P$,

então $P \cap \ker \tau = [P, N]$, com $N = N_G(P)$. Como $N = C_G(P)$, temos que $P \subseteq C_G(N)$. Logo, $P \cap \ker \tau = 1$ e $\operatorname{Im} \tau = C_P(N) = P$. Observe que $P \ker \tau$ é um subgrupo de G de ordem $|P||\ker \tau|$. Daí, p não pode dividir a ordem de $|\ker \tau|$.

Por outro lado, segue do 1º Teorema de isomorfismo que $G/\ker \tau \simeq \operatorname{Im} \tau = P$, isto é, $|G/\ker \tau| = |G : \ker \tau| = |P|$. Portanto $\ker \tau$ é um p-complemento normal em G e assim G é p-nilpotente. □

O conceito de p-nilpotência nos permite extrair resultados fascinantes acerca das estruturas dos grupos finitos, como veremos no próximo resultado

Teorema 30. *Sejam G um grupo finito e p o menor primo divisor de $|G|$. Assuma que G não seja p-nilpotente. Então, os p-subgrupos de Sylow de G não são cíclicos. Ademais, $|G|$ é divisível por p^3 ou por 12.*

Demonstração. Seja P um p-subgrupo de Sylow de G. Denotemos por N e C o normalizador e centralizador de P em G respectivamente. Por G não ser p-nilpotente, segue que do teorema anterior que $C \subsetneq N$. Portanto, podemos garantir, assegurado Pela Proposição 2, que N/C é isomorfo a um subgrupo não trivial de $\operatorname{Aut} P$, donde, $|N/C|$ divide $|\operatorname{Aut} P|$.

Agora, suponha, por contradição, que P seja cíclico. Então pela Proposição 2 temos que $|\operatorname{Aut} P| = \Phi(|P|)$. Desde que $|P| = p^k$, tem-se que $|\operatorname{Aut} P| = \Phi(|P|) = (p-1)p^{k-1}$. Assim, $|N/C|$ divide $(p-1)$, já que $P \subset C$ e daí p não pode dividir $|N/C|$. Por outro lado, existe q primo divisor de $|N/C|$. Por transitividade, q deve dividir $p-1$ donde $q \leq p-1$ e daí $q < p$. Basta observar agora que, sendo q divisor de $|N/C|$,tem-se que q divide $|N|$, donde q divide $|G|$, o que é um absurdo. Portanto, P não é cíclico.

Por último, suponha que p^3 não divide $|G|$. Então $|P| = p$ ou $|P| = p^2$. Da primeira parte da demonstração tem-se que $|P| \neq p$, haja visto que P não é cíclico. Assim, $|P| = p^2$, com P não cíclico. Portanto, $P \simeq \mathbb{Z}_p \times \mathbb{Z}_p$, donde temos P abeliano e $|\operatorname{Aut} P| = p(p+1)(p-1)^2$. Tomemos q primo divisor de $|N/C|$. Então q divide $|G|$ e $|\operatorname{Aut} P|$. Sendo P abeliano, $P \subseteq C$ e assim p não divide $|N/C|$. Portanto p é diferente de q, logo $p < q$. Daí, $p+1 \leq q$. Recorde que q divide $p(p+1)(p-1)^2$ e que $p < q$. Logo q deve dividir $p+1$ e assim $q \leq p+1$. Dessa forma temos $q = p+1$ e assim, como q é primo, devemos ter $p = 2$ e $q = 3$. Por último, observe que $p^2q = 12$ divide $|G|$. □

Observação 25. *Segue de forma direta do teorema anterior que se G é um grupo simples finito, cuja ordem é composta, então $|G|$ é divisível por 12 ou pelo cubo do menor primo divisor de $|G|$.*

3.3 Aplicações

Nessa seção, voltaremos nossa atenção para algumas aplicações, dentre as quais destacamos os Teoremas 33 e 29, que estão entre os mais interessantes e motivadores do presente trabalho.

Teorema 31. *Se todos os subgrupos de Sylow de um grupo finito G são cíclicos, então G é solúvel.*

Demonstração. Mostraremos esse fato usando indução sobre $|G|$. Se $|G| = 2$ é óbvio que o teorema é verdadeiro. Suponha, por indução, que o resultado seja válido para todos os grupos que satisfazem as hipóteses do teorema e cuja ordem seja menor do que a ordem de $|G|$. Mostremos que o resultado também é válido para G.

Se $|G|$ possui um único divisor primo então G é um p-grupo finito e o resultado segue (vide os Teoremas 17 e 19). Se, porém, $|G|$ possuir mais de um divisor primo, seja p o menor deles. Agora, considere P um p-subgrupo de Sylow de G. Segue do Teorema 30 que G é p-nilpotente, ou seja, P possui algum complemento normal N em G. Logo, $G/N \simeq P$, donde, G/N é cíclico, e portanto solúvel. Por outro lado, $mdc(|N|, |G : N|) = 1$, logo os subgrupos de Sylow de N são subgrupos de Sylow de G. Como $|N| < |G|$, segue da hipótese de indução que N é solúvel. Assim G/N e N são solúveis, donde G é solúvel e o resultado segue. □

Como resultado direto do teorema acima temos que todo grupo finito de ordem livre de quadrado é solúvel, bastando observar que, neste caso, todos os subgrupos de Sylow do grupo em questão têm ordem prima, logo são cíclicos. Portanto, recaímos nas hipóteses do teorema e segue o resultado.

Teorema 32. *Sejam n e m números naturais maiores do que 1. Se existe algum grupo G de ordem n tal que* $\operatorname{Aut} G$ *possui algum subgrupo de ordem m, então existe grupo não abeliano de ordem mn.*

Demonstração. Consideremos K um subgrupo de $\operatorname{Aut} G$ de ordem m e sobre o produto cartesiano $G \times K$ a seguinte operação

$$(x, \varphi) * (y, \psi) = (x\varphi(y), \varphi \circ \psi),$$

com $x, y \in G$ e $\varphi, \psi \in K$.

Mostremos que $G \times K$, que passaremos a denotar por $G \rtimes K$, munido da operação " $*$ ", é um grupo.

i) Sejam $(x,\varphi),(y,\psi),(z,\eta) \in G \rtimes K$, então

$$\begin{aligned}\big((x,\varphi)*(y,\psi)\big)*(z,\eta) &= (x\varphi(y),\varphi\circ\psi)*(z,\eta)\\ &= (x\varphi(y)(\varphi\circ\psi)(z),\varphi\circ\psi\circ\eta)\\ &= (x\varphi(y)\varphi(\psi(z)),\varphi\circ\psi\circ\eta)\\ &= (x\varphi(y\psi(z)),\varphi\circ(\psi\circ\eta))\\ &= (x,\varphi)*(y\psi(z),\psi\circ\eta)\\ &= (x,\varphi)*\big((y,\psi)*(z,\eta)\big).\end{aligned}$$

Logo, $*$ é associativa.

ii) Verificaremos se existe $(y,\psi) \in G \rtimes K$ fixo tal que $(y,\psi)*(x,\varphi) = (x,\varphi)*(y,\psi) = (x,\varphi)$, para todo $(x,\varphi) \in G \rtimes K$, ou seja,

$$\begin{aligned}(y,\psi)*(x,\varphi) &= (y\psi(x),\psi\circ\varphi) = (x,\varphi),\\ (x,\varphi)*(y,\psi) &= (x\varphi(y),\varphi\circ\psi) = (x,\varphi).\end{aligned}$$

Portanto, $(y,\psi)*(x,\varphi) = (x,\varphi)*(y,\psi) = (x,\varphi)$ ocorre se, e somente se, $\psi\circ\varphi = \varphi\circ\psi = \varphi$ e $y\psi(x) = x\varphi(y) = x$, para todo $(x,\varphi) \in G \rtimes K$, particularmente para $\varphi = \mathrm{Id}_G$. Dessas últimas igualdades tiramos que $\psi = \mathrm{Id}_G$ e $y = e$. Portanto, $G \rtimes K$ possui elemento neutro que é (e, Id_G).

iii) Dado $(x,\varphi) \in G \rtimes K$ verifiquemos se existe $(z,\eta) \in G \rtimes K$ tal que $(x,\varphi)(z,\eta) = (e,\mathrm{Id}_G) = (z,\eta)(x,\varphi)$, ou seja, $x\varphi(z) = e = z\eta(x)$ e $\varphi\circ\eta = \eta\circ\varphi = \mathrm{Id}_G$. Basta tomar $\eta = \varphi^{-1}$ e $z = \varphi^{-1}(x^{-1})$. Logo, o inverso de (x,φ) é $(\varphi^{-1}(x^{-1}),\varphi^{-1})$.

Portanto, $G \rtimes K$ é um grupo. Observe agora que $G \rtimes K$ não é abeliano. De fato, tomemos $\varphi \in K$ tal que $\varphi(g) \neq g$ para algum $g \in G$ ($\varphi \neq \mathrm{Id}_G$). Assim,

$$\begin{aligned}(g,\varphi)*(g,\mathrm{Id}_G) &= (g\varphi(g),\varphi) \text{ e}\\ (g,\mathrm{Id}_G)*(g,\varphi) &= (g^2,\varphi).\end{aligned}$$

Como $\varphi(g) \neq g$, temos que (g,φ) e (g,Id_G) não comutam. □

Observação 26. *Denotando por Φ a função de Euler, é um fato conhecido que se m e n são números naturais tais que m divide n, então $\Phi(m)$ divide $\Phi(n)$. Para um estudo detalhado da função de Euler indicamos as referências [5] e [8].*

Teorema 33. *Seja $n \in \mathbb{N}$, com $n > 1$. Então são equivalentes:*

i) $\mathrm{mdc}(n, \Phi(n)) = 1$

ii) todo grupo de ordem n é cíclico.

Demonstração. Mostremos que (i) $\Rightarrow$ (ii). Suponha que (i) seja verdadeira e (ii) falha. Tomemos um grupo G como contra-exemplo de ordem mínima. Consideremos p o menor divisor primo de $|G|$ e P um p-subgrupo de Sylow de G. Observemos, em primeiro lugar, que $|G| \neq p$, já que G não é cíclico. Em segundo lugar, a ordem de G não pode ser potência de primo, pois, caso fosse, teríamos $|G| = p^k$, com $k \geq 2$, donde

$$\Phi(n) = \Phi(|G|) = \Phi(p^k) = (p-1)p^{k-1} = p^k - p^{k-1} = p(p^{k-1} - p^{k-2}).$$

Logo, p dividiria $\Phi(n)$, contrariando (i). Dessa forma, $|G|$ não pode ser potência de p e então podemos escrever $n = |P|n_1$, com $\mathrm{mdc}(p, n_1)$ e $n_1 > 1$. Como $|P|$ divide n, temos que $\Phi(|P|)$ divide $\Phi(n)$. Recordando que $|P|$ divide n, podemos concluir que $\mathrm{mdc}(|P|, \Phi(|P|)) = 1$, haja vista que $\mathrm{mdc}(n, \Phi(n)) = 1$. Como $|P| < |G|$ e $\mathrm{mdc}(|P|, \Phi(|P|)) = 1$, segue da hipótese de indução que P é cíclico. Nessas condições, o Teorema 30 garante que P possui um complemento normal N em G, isto é, $G = PN$ e $P \cap N = 1$. Daí, $\mathrm{mdc}(|P|, |N|) = 1$ e $n = |G| = |P||N|$. Logo, $\Phi(|N|)$ divide $\Phi(n)$. Como $|N|$ divide n e $\mathrm{mdc}(n, \Phi(n)) = 1$, devemos ter $\mathrm{mdc}(|N|, \Phi(|N|)) = 1$. Ao recordarmos que $|N| < |G|$, temos, por hipótese de indução que N também é cíclico. Nesta ocasião, consideremos $x \in P$ tal que $P =< x >$ e a aplicação

$$\begin{aligned} \varphi : N &\to N \\ g &\mapsto \varphi(g) = xgx^{-1}. \end{aligned}$$

Não é difícil ver que $\varphi \in \mathrm{Aut}\, N$. Daí, $o(\varphi)$ divide $|\mathrm{Aut}\, N| = \Phi(|N|)$ (veja Proposição 2). Por outro lado, também é fácil observar que $\varphi^m(g) = x^m g(x^{-1})^m$, para quaisquer $g \in N$ e $m \in \mathbb{N}$. Logo, $\varphi^{|P|} = \mathrm{Id}_N$ e portanto $o(\varphi)$ também divide $|P|$. Dessa forma podemos concluir que $o(\varphi) = 1$, à vista que $|P|$ divide n e $\Phi(|N|)$ divide $\Phi(n)$. Daí concluímos que $x \in C_G(N)$, e consequentemente $P \subseteq C_G(N)$. Sendo P cíclico, com maior razão abeliano, temos $P \subseteq C_G(P)$.

Recordemos que $G = PN$. Logo, $P \subseteq Z(G)$ e, por conseguinte, $P \trianglelefteq G$. Juntando os fatos obtidos temos que $G = PN$, $P \cap N = 1$ e $P, N \trianglelefteq G$. Daí, pelo Exemplo 12 $G \simeq P \times N$, donde segue que G é cíclico, em vista que $\mathrm{mdc}(|P|, |N|) = 1$. Mas, isso é um absurdo, pois G não é cíclico. Portanto, (ii) é verdadeira.

Reciprocamente, suponha (ii) e não (i), isto é, $\mathrm{mdc}(n, \Phi(n)) > 1$. Consideremos p primo divisor comum de n e $\Phi(n)$. Afirmamos que p^2 não divide n,

caso contrário, teríamos o grupo $\mathbb{Z}_p \times \mathbb{Z}_p \times \mathbb{Z}_{n/p^2}$ não cíclico de ordem n. Dessa maneira, $n = pm$, com $\text{mdc}(p, m) = 1$. Daí, $\Phi(n) = \Phi(p)\Phi(m) = (p-1)\Phi(m)$ e, como p divide $\Phi(n)$, por hipótese, segue que p divide $\Phi(m)$. Considerando G_1 um grupo cíclico de ordem m, temos pela Proposição 2 que $|\operatorname{Aut} G_1| = \Phi(G_1) = \Phi(m)$. Desde que p divide $|\operatorname{Aut} G_1|$, deve existir H subgrupo de $\operatorname{Aut} G_1$ de ordem p. Logo, pelo Teorema 32, existe grupo não abeliano de ordem $pm = n$, o que é uma contradição. Logo, (i) é verdadeira. □

Como último resultado do texto temos o

Teorema 34. *Sejam $n = p_1^{k_1} \cdot \ldots \cdot p_m^{k_m}$, onde $p_1, \ldots, p_m$ são primos dois a dois distintos e $k_1, \ldots, k_m \in \mathbb{N}$. Então, são equivalentes:*

i) todo grupo de ordem n é abeliano.

ii) $k_i \leq 2$ e $\text{mdc}(n, p_i^{k_i} - 1) = 1$, para todo $i = 1, \ldots, m$.

Demonstração. Suponhamos que (i) seja verdadeira. Tomemos um primo p divisor de $|G|$. Consideremos o grupo cíclico $\mathbb{Z}_{p^2}$ e observemos que $|\operatorname{Aut} \mathbb{Z}_{p^2}| = p(p-1)$ (vide Proposição 2). Daí, p divide $|\operatorname{Aut} \mathbb{Z}_{p^2}|$ e assim segue do Teorema 32 que existe grupo não abeliano de ordem p^3, e portanto podemos concluir que p^3 não divide n, pois, caso contrário, o tal grupo não abeliano seria um subgrupo de algum grupo de ordem n, que por hipótese é abeliano. Como p foi tomado arbitrário obtemos que $|k_i| \leq 2$, para todo $i = 1, \ldots, m$, o que completa a primeira parte da demonstração. Na segunda parte da demonstração, suponhamos, por absurdo, que $\text{mdc}(n, p_j^{k_j} - 1) > 1$, para algum $j \in \{1, \ldots, m\}$. Assim, deve existir $i \in \{1, \ldots, m\}$ tal que p_i é divisor comum de n e $p_j^{k_j} - 1$. Da primeira parte da demonstração temos que $k_j \leq 2$. Suponhamos que $k_j = 1$. Então, p_i divide $p_j - 1 = |\operatorname{Aut} \mathbb{Z}_{p_j}|$(vide Proposição 2), e daí, pelo Teorema 32, temos que existe grupo não abeliano de ordem $p_i p_j$, o que é um absurdo, pois $p_i p_j$ divide n. Supondo $k_j = 2$, então p_i deve dividir $p_j^2 - 1$. Consideremos o grupo abeliano $\mathbb{Z}_{p_j} \times \mathbb{Z}_{p_j}$ e notemos que $|\operatorname{Aut}(\mathbb{Z}_{p_j} \times \mathbb{Z}_{p_j})| = (p_j^2 - 1)(p_j^2 - p_j)$(vide Proposição 2), e assim p_i divide $|\operatorname{Aut}(\mathbb{Z}_{p_j} \times \mathbb{Z}_{p_j})|$. Logo, pelo Teorema 32, existe grupo não abeliano de ordem $p_i \cdot |\mathbb{Z}_{p_j} \times \mathbb{Z}_{p_j}| = p_i p_j^2$, o que também é um absurdo. Observe que essa série de absurdos foi gerado ao supormos que $\text{mdc}(n, p_y^{k_2} - 1) > 1$. Dessa forma devemos ter $\text{mdc}(n, p_j^{k^j} - 1) = 1$ para todo $j = 1, ..., m$, e isso completa a demonstração.

Reciprocamente, suponha (ii) verdadeira e consideremos G um grupo de ordem n. Observemos primeiramente que todos os subgrupos de Sylow de G são abelianos, uma vez que suas ordens são no máximo p_i^2. Afirmamos que

G é p_i-nilpotente para todo $i = 1, \ldots, m$. De fato, fixemos $i \in \{1, \ldots, m\}$, arbitrário, e consideremos P um p_i-subgrupo de Sylow de G. Assumindo que $N_G(P) = C_G(P)$, então pelo Teorema de Burnside temos que a afirmação é verdadeira. Suponha que $N_G(P) \neq C_G(P)$ e tomemos q primo divisor de $|N_G(P)/C_G(P)|$. Perceba que $|N_G(P)/C_G(P)|$ divide $|\operatorname{Aut} P|$ e assim q também divide $|\operatorname{Aut} P|$. Por outro lado, q divide n, já que $|N_G(P)/C_G(P)|$ divide $|G|$, e assim temos por (ii) que q não pode dividir $p_i^{k_i} - 1$. Observemos ainda que $p_i \neq q$, haja visto que P é abeliano e daí $P \subseteq C_G(P)$ (donde p_i não divide $|N_G(P)/C_G(P)|$). Temos as seguintes possibilidades para P:

i) $P \simeq \mathbb{Z}_{p_i}$

ii) $P \simeq \mathbb{Z}_{p_i^2}$

iii) $P \simeq \mathbb{Z}_{p_i} \times \mathbb{Z}_{p_i}$

De (i) temos que $|\operatorname{Aut} P| = p_i - 1$, o que é uma contradição, uma vez que $k_i = 1$ e q não divide $p_i - 1$. De (ii) obtemos $|\operatorname{Aut} P| = p_i(p_i - 1)$, outra contradição, pois $k_i = 2$, q não divide p_i e nem $p_i - 1$ (já que não divide $p_i^2 - 1 = (p_i - 1)(p_i + 1)$). De (iii) tiramos que $|\operatorname{Aut} P| = (p_i^2 - 1)(p_i^2 - p_i) = p_i(p_i^2 - 1)(p_i - 1)$, o que também é uma contradição, já que q não divide p_i, $p_i^2 - 1$ e $p_i - 1$. Dessa forma, temos $N_G(P) = C_G(P)$ e G p_i-nilpotente para todo $i = 1, \ldots, m$. Assim, pelo Teorema 25, G é nilpotente. Segue do Teorema 24 que $G \simeq P_1 \times \cdots \times P_m$, onde P_i é o p_i-subgrupo de Sylow de G. Portanto, G é abeliano, uma vez que cada P_i é abeliano. $\square$

Conclusão

Concluímos que o estudo do homomorfismo transfer é imprescindível quando se quer estudar mais afundo as estruturas dos grupos finitos, pois, como vimos no presente trabalho, com o auxílio do transfer é possível exibir belíssimos resultados com extrema elegância e classe, e sem perder o rigor matemático, que sem o seu suporte seria uma tarefa muito difícil.

Referências Bibliográficas

[1] W. Burnside, *On transitive groups of degree n and class n-1*, Proc. London Math. Soc. 32 (1900), 240-246.

[2] W. Burnside, *On some properties of groups of odd order*, Proc. London Math. Soc. 32 (1900), 162-185, 257-268.

[3] A. Garcia, Y. Lequain, *Elementos de Álgebra*, Rio de Janeiro, Brasil: Associação Instituto Nacional de Matemática Pura e Aplicada, 2003.

[4] A. Gonçalves, *Introdução à Álgebra*, Rio de Janeiro, Brasil: Projeto Euclides, Impar, 1979.

[5] A. Hefez, *Elementos de Aritmética*, Rio de Janeiro, Brasil: Sociedade Brasileira de Matemática, 2005.

[6] D. J. S. Robinson *A Course in the Theory of Groups*, New York, USA: Springer, 1995.

[7] J. J. Rotman *An Introduction to the Theory of Groups*, New York, Usa: Springer, 4th. 1995.

[8] J. P. O. Santos *Introdução à Teoria dos Números*, Coleção Matemática Universitária-IMPA, Rio de Janeiro, Brasil, 1998.