Universidade de Brasília
Instituto de Ciências Exatas
Departamento de Matemática

DISSERTAÇÃO

Automorfismos coprimos de 2-grupos finitos

Aluna: Maria de Sousa Leite Filha

Orientador: Pavel Shumyatsky

Brasília - DF
setembro/2012

Sumário

Agradecimentos

A DEUS, pela minha vida, por todo o seu amor e auxílio em todos os momentos da minha existência. Aos amigos espirituais (Abelardo, João, André, etc) que têm continuamente iluminado meus passos e inspirado em dias tão decisivos.

Aos meus pais, por toda confiança que depositaram em mim, pelo amor e carinho, pelas lições de vida que jamais esquecerei. Por tudo que enfrentaram e superaram para dar a mim e a meus irmãos uma vida digna.

Aos meus irmãos, sobrinhos e familiares que sempre confiaram em mim.

Aos meus professores e colegas da Universidade Federal de Campina Grande, onde passei cincos importantes anos de minha vida, em especial aos professores Francisco A. M. de Souza (Chico) e Antônio Brandão. Às minhas amigas Raquel Aline, Débora, Aline, Ana Claúdia, Adrícia, Lívia Maria e amigas da Residência Universitária Feminina de Campina Grande, aos meus amigos e colegas da UFCG.

Agradeço de coração aos amigos que aqui conquistei e muito devo pela força em todos os momentos: Keidna, Ilana, Mônica, Kaliana, Thaynara, Renata, Luiz, Júnior (Zé), Otto, Eudes, Joaby, Linniker, Elon, Fábio, Lauro, Verena, Luciana, Rafael, Letícia, Arnoud, Dádico, André, Rafael Gauche, etc. Jamais esquecerei vocês.

Aos professores do Mat-UnB que sempre se dispuseram a me ajudar.

Aos funcionários do mat de um modo geral, em especial a Claúdia (portaria) e Marta (secretaria).

Em especial agradeço aos meus orientadores Pavel Shumyatsky e Cristina Acciarri, matemáticos inspiradores e talentosos, que pacientemente me apoiaram e auxiliaram nesta caminhada.

A pessoa que me fez redescobrir o quanto é gratificante e prazeroso estudar matemática: Cristina Acciarri. Obrigada por tudo minha querida.

Agradeço aos amigos do Grupo de estudo Espírita na UnB, meus queridos Ricardo, Landoaldo, Sérgio e Iris. Sem palavras para expressar minha imensa gratidão ao Grupo Espírita Casa do Caminho finalizo esta página de coração leve e confiante no futuro, na caridade e amor ao próximo. O que no GECAM

comecei a aprender é para toda vida, para todas as vidas. Meus irmão obrigada. Que DEUS continue a iluminar a todos.

Dedicatória

À minha família, amigos, vô Sebastião e à Cristina.

Pensamentos

"Embora nínguem possa voltar no tempo e fazer um novo começo, qualquer um pode começar agora e fazer um novo final."

Chico Xavier

Resumo

A presente dissertação tem por base os trabalhos de M. Isaacs e G. Navarro [**5**] e de Z. Marciniak [**7**]. Suponhamos que um p'-grupo finito K age por autormorfismos sobre um p-grupo finito P e vamos discutir sobre hipóteses que garantem que K age trivialmente sobre P. Em [**4**] é apresentado um resultado que assegura que, se P é abeliano e K fixa todos os elementos de ordem p em P, então K age trivialmente sobre P e que, se, além disso, o primo p é diferente de 2, então a hipótese de P ser abeliano não é necessária. Mas se $p = 2$ e temos apenas que K fixa todos os elementos de ordem 2 em P, não podemos concluir que a ação de K sobre P é trivial.

No caso de $p = 2$, por [**2**], é conhecido que se K fixa todos os elementos de ordem 2 e todos os elementos de ordem 4 em P, então K age trivialmente sobre P e por [**8**], sabemos que se K fixa todos os elementos racionais de P, então a ação de K sobre P é trivial. Em 2010, M. Isaacs e G. Navarro, demonstram que se K fixa, além de todos os elementos de ordem 2, todos os elementos reais de ordem 4 em P, então K age trivialmente sobre P. A demonstração por eles apresentada usa recursos de teoria de caracteres e, além disso, os autores ressaltam que até aquele momento não viam como mostrar a veracidade do resultado sem utilizar caracteres. No entanto, Marciniak, em [**7**], consegue demonstrar este resultado sem recorrer a caracteres.

Abstract

This dissertation is based on the works of M. Isaacs and G. Navarro [**5**] and Z. Marciniak [**7**]. Suppose that a finite p'-group K acts by automorphisms on a finite p-group P and go to debate above hypothesis that guaranteeb that K acts trivially on P. In [**4**] is presented a result that affirm that if P is an abelian group and K fixes all elements of order p in P, then K acts trivially on P e that, if, moreover, the prime p is other than 2, then it is not necessary to assume that P is abelian. However if $p = 2$ and we only suppose that K fixes all elements of order 2 in P, then we cannot conclude that the action of K on P is trivial.

In the case when $p = 2$, by [**2**], it is known that if K fixes all elements of order 2 and all elements of order 4 in P, then K acts trivially on P and by [**8**], known that K fixes all rational elements in P, then the action of K on P is trivial. In 2010, M. Isaacs and G. Navarro showed that if K fixes all elements of order 2 and all real elements of order 4 in P, then K acts trivially on P. They proved the result using arguments from character theory. Moreover they observed that until that moment they did not see how to show the correctness of the result without using characters. However, later Marciniak, in [**7**], gave an alternative proof without using characters.

Introdução

Consideremos uma ação por automorfismos de um p'-grupo finito K sobre um p-grupo finito P e vamos discorrer sobre condições que assegurem que K age trivialmente sobre P.

Em [**4**] Isaacs apresenta o seguinte resultado devido a Fitting: Se um grupo K age por automorfismos sobre um grupo abeliano P, onde K e P são finitos e têm ordens relativamente primas, então $P = C_P(K) \times [P, K]$. Como consequência deste resultado temos que se um p'-grupo finito K age por automorfismos sobre um p-grupo finito abeliano P e K fixa todos os elementos de ordem p em P, então K age trivialmente sobre P. Isto, naturalmente, nos incita o interesse de saber o que ocorre no caso em que P não é abeliano. Surpreendentemente, se supormos que o primo p é diferente de 2, então a hipótese de ser P abeliano não é necessária. O resultado para o caso $p > 2$ também é apresentado em [**4**].

Entretanto, se $p = 2$ não podemos conlcuir que K age trivialmente sobre P, se considerarmos apenas que K fixa todos os elementos de ordem 2 em P. Para ver isto vamos considerar o grupo dos quatérnios $Q_8 = \langle i, j, k \mid i^2 = j^2 = k^2 = ijk; i^4 = j^4 = k^4 = 1 \rangle$ e definir uma ação por automorfismos de um grupo $K = \langle a \rangle$ cíclico de ordem 3 sobre Q_8 pondo: $i^a = j$, $j^a = k$ e $k^a = i$. Assim, podemos observar que K fixa todos os elementos de ordem 2 em Q_8, à saber ijk, mas K não age trivialmente sobre Q_8.

Agora, nosso interesse é saber o que acontece quando p é igual a 2. O primeiro resultado neste sentido é uma consequência do seguinte resultado de [**2**]: Sejam P um p-grupo finito e α um automorfismo de P cuja ordem é coprima com p. Se $p = 2$ suponha que α fixa todos os elementos de ordem 2 e 4 em P, então $\alpha = 1$. Ou seja, como consequência disso obtemos que se um grupo de ordem ímpar K age por automorfismos sobre um 2-grupo finito P e fixa todos os elementos de ordem 2 e 4 em P, então a ação de K sobre P é trivial. Um outro resultado neste sentido foi apresentado por G. Navarro e L. Sanus em [**8**] e assevera o seguinte: Se um $2'$-grupo finito K age por automorfismos sobre um 2-grupo finito P e fixa todos os elementos

racionais em P, então K age trivialmente sobre P. (Um elemento $x \in P$ é dito racional se sempre que $\langle x \rangle = \langle x^r \rangle$, então x e x^r são conjugados em P.)

Sabendo que todo elemento de ordem 2 é racional e um elemento de ordem 4 é racional se, e somente se, é real, em 2010, M. Isaacs e G. Navarro observaram uma interessante relação entre as hipóteses dos resultado anteriores e demonstraram que se um grupo de ordem ímpar K age por automorfismos sobre um 2-grupo finito P e fixa todos os elementos de ordem 2 e todos os elementos reais de ordem 4 em P, então K age trivialmente sobre P. (Um elemento $x \in P$ é dito real se é conjugado com seu inverso, ou seja, se existe $g \in P$ tal que $x^g = x^{-1}$.) Na demonstração do resultado os autores utilizam recursos de teoria de caracteres e além disso, os autores comentam que até aquele momento não viam como demonstrar o resultado sem o auxílio de caracteres. Porém, Marciniak, em [**7**], consegue apresentar uma demonstração deste fato sem teoria de caracteres. Neste trabalho optamos por expor a demonstração dada por Marciniak.

A organização deste trabalho visa fornecer ao leitor, uma sequência lógica de informações, conceitos e resultados, que serão importantes na apresentação da demonstração do principal teorema desta dissertação, que é exatamente o resultado provado por M. Isaacs e G. Navarro e Marciniak. Assim, dedicamos o Capítulo 1 ao tratamento de conceitos básicos da teoria de grupos, deste modo, os resultados desta seção são amplamente conhecidos e, portanto optamos por omitir a demonstração de alguns deles.

No Capítulo 2 nos atemos ao estudo de ações por automorfismos, destacando, em especial, o caso em que estas ações são coprimas. Além disso, apresentamos propriedades e resultados acerca de elementos fixos e subgrupos invariantes por automorfismos.

É no Capítulo 3, que apresentamos o principal resultado tratado neste trabalho, ou seja, que se um grupo de ordem ímpar K age por automorfismos sobre um 2-grupo P, e K fixa todos os elementos de ordem 2 e todos os elementos reais de ordem 4 em P, então K age trivialmente sobre P.

No Capítulo 4 apresentamos alguns critérios clássicos de p-nilpotência, como por exemplo, os critérios de Burnside e de Frobenius. Além disso, vemos como, aplicando os resultados do terceiro capítulo, é possível deduzir o seguinte critério de 2-nilpotência: se P é um 2-subgrupo de Sylow de um grupo finito G e todos os elementos de ordem 2 em P são centrais em G e todos os elementos de ordem 4 em P são centrais em P, então G é 2-nilpotente. Outra consequência dos resultados do Capítulo 3 é o critério de

2-nilpotência à seguir: se P é um 2-subgrupo de Sylow de um grupo finito G e $x^G \cap P = x^P$, para qualquer $x \in P$ de ordem ≤ 4, então G possui um 2-complemento normal.

CAPíTULO 1

Conceitos Preliminares

Este capítulo tem o obejetivo de apresentar os conceitos da teoria de grupos envolvidos na elaboração deste trabalho. Primeiramente tratamos as noções básicas e em seguida abordamos conceitos e resultados relacionados a comutadores. Finalmente, definimos o conceito ação de grupos e apresentamos alguns exemplos.

1.1. Fatos Básicos de Teoria de Grupos

Relembremos que um grupo G é dito cíclico quando pode ser gerado por um único elemento, ou seja, quando existe $g \in G$ tal que $G = \langle g \rangle$; e que G é dito um grupo abeliano quando $gh = hg$, para quaisquer $g, h \in G$. Claro que, se G é cíclico, então G é abeliano. Seja G um grupo, então para cada $g \in G$, podemos considerar o seguinte subconjunto de G,

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

constituído de todos os elementos de G que comutam com g. Este conjunto é chamado o *centralizador* de g em G.

LEMA 1.1.1. *Seja $g \in G$, então $C_G(g)$ é um subgrupo de G.*

De modo similar à definição de centralizador de um elemento $g \in G$, podemos definir o centralizador de um subconjunto arbitrário X de G.

DEFINIÇÃO 1.1.2. Seja $X \subseteq G$ um subconjunto qualquer de G. Definimos o *centralizador* de X em G, como sendo o conjunto

$$C_G(X) = \{y \in G \mid xy = yx, \text{ para todo } x \in X\}.$$

Observe que, $C_G(X) = \bigcap_{x \in X} C_G(x)$. De fato, se $y \in C_G(X)$, então, por definição, $yx = xy$ para todo $x \in X$, logo, $y \in C_G(x)$, para qualquer $x \in X$. Assim, $y \in \bigcap_{x \in X} C_G(x)$. Reciprocamente, se $y \in \bigcap_{x \in X} C_G(x)$, então $y \in C_G(x)$, para todo $x \in X$, logo, $yx = xy$, para qualquer $x \in X$ e então $y \in C_G(X)$.

Como a interseção de subgrupos é ainda um subgrupo, segue que $C_G(X)$ é um subgrupo de G. Em particular, quando $X = G$, o centralizador de G

em G, será um subgrupo de G. Este subgrupo será denotado por $Z(G)$ e chamado de *centro* de G. Assim,

$$Z(G) = C_G(G) = \{y \in G \mid yx = xy, \text{ para todo } x \in G\}.$$

Claro que o centro $Z(G)$ de G é um grupo abeliano e G é abeliano se, e somente se, $Z(G) = G$. Pode ocorrer, ainda, que o centro de um grupo seja trivial. Por exemplo, considere o grupo diedral D_{2n}. Temos:

$$|Z(D_{2n})| = \begin{cases} 1, \text{ se } n \text{ é ímpar} \\ 2, \text{ se } n \text{ é par.} \end{cases}$$

O lema a seguir mostra como podemos aplicar o fato de o centralizador de um subconjunto X de G ser um subgrupo de G e não apenas um subconjunto.

LEMA 1.1.3. **[3]** *Seja X um subconjunto de G tal que $xy = yx$, para quaisquer $x, y \in X$. Então, $\langle X \rangle$ é abeliano.*

OBSERVAÇÃO 1.1.4. Se $\theta : G_1 \to G_2$ é um isomorfismo do grupo G_1 no grupo G_2, observe que $\theta(Z(G_1)) = Z(G_2)$. Efetivamente, queremos verificar que $\theta(Z(G_1)) \subseteq Z(G_2)$ e que $Z(G_2) \subseteq \theta(Z(G_1))$. Primeiramente vejamos que, se $z \in \theta(Z(G_1))$, então $z \in Z(G_2)$, isto é, $zs = sz$, para qualquer $s \in G_2$. Seja então $z \in \theta(Z(G_1))$ e $s \in G_2$ arbitrários. Assim, existem $a \in Z(G_1)$ e $b \in G_1$ tais que $z = \theta(a)$ e $s = \theta(b)$. Logo,

$$zs = \theta(a)\theta(b) = \theta(ab) = \theta(ba) = \theta(b)\theta(a) = sz.$$

Onde a segunda e a quarta igualdades seguem do fato de θ ser isomorfismo e a terceira igualdade segue do fato de $a \in Z(G_1)$. Portanto, $z \in Z(G_2)$. Verifiquemos agora que, $Z(G_2) \subseteq \theta(Z(G_1))$. Seja, $z \in Z(G_2)$. Como θ é um isomorfismo, temos que $\theta(G_1) = G_2$, e assim, existe $a \in G_1$ tal que $z = \theta(a)$. Queremos provar que $z \in \theta(Z(G_1))$, ou seja, que, como $z = \theta(a)$, então $a \in Z(G_1)$. Sabemos que, dado arbitrariamente $s \in G_2$, extiste $b \in G_1$ tal que $s = \theta(b)$ e como $z \in Z(G_2)$, segue que $zs = sz$. Logo, por um lado, $\theta(a)\theta(b) = \theta(ab)$ e, por outro lado, $\theta(b)\theta(a) = \theta(ba)$ e como θ é injetiva, temos $ab = ba$. Pela arbitrariedade de $s \in G_2$, concluímos que $ab = ba$ para todo $b \in G_1$. Logo, $a \in Z(G_1)$ e, consequentemente, $z \in \theta(Z(G_1))$, como queríamos provar.

DEFINIÇÃO 1.1.5. Um automorfismo é um isomorfismo $\theta : G \to G$ de um grupo G nele mesmo.

Um exemplo elementar de automorfismo de um grupo G é a aplicação *identidade*. Disto segue que o conjunto dos automorfismos de um grupo G, $\mathrm{Aut}(G)$ é sempre não-vazio. Além disso, munido da composição de aplicações, o conjunto $\mathrm{Aut}(G)$ é um grupo, chamado grupo dos automorfismos de G. Pela Observação 1.1.4, temos que, para qualquer automorfismo de um grupo G, o centro $Z(G)$ de G é levado nele mesmo, ou seja, o centro de G é invariante em relação a qualquer automorfismo de G. Além do centro, um grupo pode possuir outros objetos que permanecem invariantes por qualquer de seus automorfismos. Esta propriedade é definida formalmente na próxima definição.

Definição 1.1.6. Um subgrupo $H \leq G$ é chamado subgrupo *característico* de G quando $\theta(H) = H$, para qualquer automorfismo θ de G. Neste caso, escrevemos: H char G.

Dados um grupo G e x um elemento arbitrário de G, se $g \in G$, o elemento $x^g = g^{-1}xg$ é chamado o elemento conjugado de x por g. O conjunto $C_x = \{x^g \mid g \in G\}$ é chamado *classe de conjugação* de x em G. Ou seja, se $x, y \in G$ e existe $g \in G$ tal que $y = x^g$, então o elemento y é conjugado do elemento x. É possível observar que esta relação é uma relação de equivalência. Assim, cada elemento de G pertence a uma única classe de conjugação, e duas classes de conjugação C_x e C_y coincidem se, e somente se, x e y são conjugados. De outra forma, são disjuntas.

Se G é um grupo finito e existem n classes de conjugação (em G) com representantes $x_1, x_2, \ldots, x_n$, então

$$G = C_{x_1} \cup C_{x_2} \cup \cdots \cup C_{x_n},$$

onde esta união é disjunta. Obtemos assim, a equação

$$|G| = |C_{x_1}| + \cdots + |C_{x_n}|. \tag{1.1.1}$$

A identidade (1.1.1) é chamada *Equação de Classe*. Observe que $x \in Z(G)$ se, e somente se, $C_x = \{x\}$. E então a equação de classe torna-se:

$$|G| = |Z(G)| + \sum_{x_i \notin Z(G)} |C_{x_i}|. \tag{1.1.2}$$

Vamos agora usar o conceito de elemento conjugado para apresentar importantes exemplos de automorfismos de um grupo G, eles são os chamados *automorfismos internos*. Para cada $g \in G$, definimos: $\theta_g : G \to G$, pondo

$$\theta_g(x) = g^{-1}xg.$$

Observe que, quando x e g comutam, então $x^g = x$. Assim, em um grupo abeliano, automorfismos internos são triviais. Denotamos por $\mathrm{Inn}(G)$ o conjunto dos automorfismos internos de G. Claro que $\mathrm{Inn}(G)$ é um subgrupo de $\mathrm{Aut}(G)$.

Notemos que dado um isomorfismo $\theta : G_1 \to G_2$, então $\theta(H)$ é um subgrupo de G_2, para todo $H \leq G_1$. Em particular, automorfismos de um grupo G levam subgrupo em subgrupo.

Definição 1.1.7. Seja H um subgrupo de G. O subgrupo

$$H^g = \{h^g \mid h \in H\}$$

de G é chamado *subgrupo conjugado* de H. Claramente, H^g é a imagem de H pelo automorfismo interno θ_g.

Como subgrupos característicos são invariantes por automorfismos, em particular, são invariantes por automorfismos internos. Assim, se C char G, então $C^g = C$, para todo $g \in G$. Note que, em geral, a equação $C^g = C$ não implica que $x^g = x$, para qualquer $x \in C$. A observação precedente é o ponto de partida para a definição a seguir.

Definição 1.1.8. Seja $N \leq G$ um subgrupo de G. Ele é dito um subgrupo *normal* de G quando $N^g = N$, para todo $g \in G$. Neste caso, usamos a notação $N \lhd G$.

Em outras palavras, os subgrupos normais de um grupo são exatamente aqueles que são invariantes por todos os automorfismos internos. Em particular, os subgrupos característicos são normais. Além disso, todos os subgrupos de um grupo abeliano são normais e os subgrupos 1 e G são sempre normais, para qualquer grupo G.

Lema 1.1.9. *Seja $H \leq G$ um subgrupo de G. Se $H^g \leq H$, para todo $g \in G$, então H é um subgrupo normal de G.*

Demonstração. Como $H^g \leq H$, para todo $g \in G$, obtemos:

$$H = (H^g)^{g^{-1}} \leq H^{g^{-1}}.$$

Como este resultado é válido para qualquer $g \in G$, colocando g^{-1} ao invés de g, obtemos:

$$H \leq H^{(g^{-1})^{-1}} = H^g.$$

Portanto, $H = H^g$. □

É importante observar que o Lema 1.1.9 não afirma que $H^g = H$, quando $H^g \leq H$, para algum $g \in G$. Como o automorfismo interno induzido pelo elemento g é uma bijeção, segue que $|H^g| = |H|$. Se, além disso, H é finito, então, juntamente com a hipótese de $H^g \leq H$, podemos concluír que $H^g = H$. Para grupos infinitos, no entanto, a implicação, geralmente, não é verdadeira. Vamos ver um exemplo disto.

EXEMPLO 1.1.10. Seja G o grupo das funções afins da reta. Ou seja, todo elemento $g \in G$ é uma aplicação $g : \mathbb{R} \to \mathbb{R}$, definida por: $g(x) = ax + b$, onde $a, b \in \mathbb{R}$ e $a \neq 0$. Afirmamos que o subgrupo H de G, formado pelas aplicações tais que $a = 1$ e $b \in \mathbb{Z}$, é tal que H^g está contido propriamente em H, para algum $g \in G$. Efetivamente, tome $g \in G$ como a aplicação que associa cada $x \in \mathbb{R}$ ao elemento $g(x) = \frac{1}{2}x$. Agora, seja $k \in H^g$. Assim, para todo $x \in \mathbb{R}$, temos $k(x) = (g^{-1}hg)(x)$, para algum $h \in H$. Daí, $k(x) = g^{-1}h(\frac{x}{2}) = g^{-1}(\frac{x}{2} + b) = x + 2b$, com $b \in \mathbb{Z}$. Logo, $k \in H$. Finalmente observe que $H^g < H$ está contido propriamente em H, uma vez que, por exemplo, a aplicação que leva $x \in \mathbb{R}$ em $x + 3$ pertence a H, mas não a H^g.

LEMA 1.1.11. **[3]** *Seja N um subgrupo normal de G e suponha que C* char *N. Então C é normal em G.*

Em contraste com o Lema 1.1.11, se temos apenas que C é normal em N e N é normal em G, não podemos concluir que C é normal em G ou ainda que se C é normal em N e N é característico em G, também não podemos afirmar que C é normal em G,

não segue que C é normal em G se tudo o que sabemos é que C é normal em N e N é normal em G ou N característico em G.

Sejam $X \subseteq G$ e $Y \subseteq G$ subconjuntos de G. Definimos:

$$XY = \{xy \mid x \in X,\ y \in Y\}.$$

Note que o fato X e Y serem subgrupos de G, não garante que XY seja subgrupo de G. Porém, com uma hipótese a mais sobre estes subgrupos, obtemos que o produto XY é um subgrupo de G.

LEMA 1.1.12. **[3]** *Sejam $H, K \leq G$ subgrupos de G. Então HK é subgrupo de G se, e somente se, $HK = KH$.*

Do Lema 1.1.12, obtemos o resultado a seguir.

PROPOSIÇÃO 1.1.13. *Sejam H e K subgrupos de G. Se pelo menos um deles é normal em G, então $HK = KH$ e, portanto, temos que HK é subgrupo de G. Além disso, se ambos H e K são normais em G, então HK é normal em G.*

DEMONSTRAÇÃO. Sem perda de generalidade suponha H normal em G. Vamos mostrar que $HK = KH$. Seja $x \in HK$, daí, $x = hk = kk^{-1}hkk = kh^k$, para algum $h \in H$ e algum $k \in K$. Como H é normal em G, temos que $h^k \in H$. Daí, $x \in KH$. Donde $HK \leq KH$. Agora seja $y = kh \in KH$, onde $k \in K$ e $h \in H$. Temos $y = khk^{-1}k = h^{k^{-1}}k$ e novamente como H é normal em G, temos que $h^{k^{-1}} \in H$, logo, $y \in HK$ e daí segue que $KH \leq HK$. Desta dupla inclusão concluímos que $HK = KH$. Suponhamos agora que H e K são normais em G. Pelo Lema 1.1.9, para provar que HK é subgrupo normal de G, basta verificar que $(HK)^g \leq HK$, para todo $g \in G$. Sejam $g \in G$ um elemento qualquer e $x \in (HK)^g$, daí $x = (hk)^g$, onde $h \in H$ e $k \in K$. Temos que $x = (hk)^g = h^g k^g$. Como H e K são normais em G, então $h^g \in H$ e $k^g \in K$ e segue que $x \in HK$. □

DEFINIÇÃO 1.1.14. Seja $H \leq G$ um subgrupo de G. Para cada $g \in G$, os conjuntos definidos por:

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

são chamados, respectivamente, a *classe lateral* à *direita* e a *classe lateral* à *esquerda* de H, determinadas por g.

Observe que, se $H \leq G$, então duas classes laterais à direita (e à esquerda) de H são iguais ou disjuntas. De fato, sejam $x, y \in G$, e suponha que $Hx \cap Hy \neq \emptyset$. Vejamos, primeiramente que, $Hh = H$ para todo $h \in H$, assim, $H(hx) = (Hh)x = Hx$. Logo, se $z \in Hx \cap Hy$, temos $Hz = Hx$ e $Hz = Hy$. Portanto, $Hx = Hy$. Um resultado análogo vale para as classes laterais à esquerda. Note também que se $g \in G$, então $g \in Hg$ e $g \in gH$. Segue portanto que, se H é um subgrupo de G, então G pode ser decomposto na união disjunta das distintas classes laterias à direita (ou à esquerda) de H.

LEMA 1.1.15. **[3]** *Seja $H \leq G$ um subgrupo de G. Então, para qualquer $g \in G$, temos*

$$|Hg| = |H| = |gH|.$$

Se H é um subgrupo de G, o *índice* de H em G, denotado por $|G : H|$, é definido como o número de classes laterais distintas à direita (ou à esquerda) de H em G.

O teorema seguinte é devido a Lagrange e estabelece uma relação entre a ordem de um grupo G e a ordem de um subgrupo H de G.

TEOREMA 1.1.16 (Lagrange). *Seja H um subgrupo de G. Então $|G| = |H||G : H|$. Em particular, se G é finito, então $|H|$ divide $|G|$ e $|G|/|H| = |G : H|$.*

DEMONSTRAÇÃO. Basta relembrar que G pode ser decomposto na união disjunta das distintas classes laterias à direita (ou à esquerda) de H e que estas classes têm a mesma ordem, à saber $|H|$. □

Um elemento $g \in G$ de um grupo G é dito ter *ordem* finita n se o subgrupo cíclico $\langle g \rangle$ gerado por g tem ordem n. Vamos denotar a ordem de g por $o(g)$. Uma consequência imediata do Teorema 1.1.16 é que, se G é um grupo finito e $g \in G$, então a ordem de g divide $|G|$.

O lema a seguir trata de propriedades de números inteiros positivos e é conhecido como Lema de Euclides.

LEMA 1.1.17. **[9]** *Seja c um número inteiro positivo que divide o produto ab de dois números inteiros positivos, a e b. Se c é relativamente primo com um destes dois números (por exemplo c é coprimo com a), então c é divisor do outro (por exemplo, c divide b).*

Vamos denotar o máximo divisor comum entre dois números inteiros n e m por (n, m).

LEMA 1.1.18. *Sejam G um grupo e g um elemento arbitrário de G. Então valem as seguintes afirmações.*

(i) *O elemento g tem ordem infinita se, e somente se, todas as potências de g são distintas.*
(ii) *Se g tem ordem finita n, então $g^m = 1$ se, e somente se, n divide m. Além disso, $\langle g \rangle$ consiste dos elementos distintos $1, g, g^2, \ldots, g^{n-1}$.*
(iii) *Se g tem ordem finita n, então a ordem de g^k é igual a $n/(n, k)$.*

DEMONSTRAÇÃO. Se todas as potências de g são distintas, temos que $\langle g \rangle$ é infinito. Reciprocamente, suponhamos que duas potências de g são iguais, digamos $g^l = g^m$, com $l < m$. Logo, $g^{m-l} = 1$. Então podemos escolher o menor inteiro positivo n tal que $g^n = 1$. Pelo algorítmo da divisão, podemos

escrever um inteiro arbitrário m na forma, $m = nq + r$, com q, r inteiros e $0 \leq r < n$. Segue daí que, $g^m = (g^n)^q g^r = g^r$. Logo, $\langle g \rangle = \{1, g, \ldots, g^{n-1}\}$. Portanto g tem ordem finita. Além disso, $g^m = 1$ se, e somente se, $r = 0$, e neste caso, pela minimalidade de n, segue que n divide m. Agora suponha que $g^j = g^i$, para alguns $0 \leq i \leq j < n$. Então, $g^{j-i} = 1$, e assim, n divide $j - i$. Mas isto ocorre somente quando $j = i$. Portanto, os elementos $1, g, \ldots, g^{n-1}$ são distintos e $o(g) = n$. Logo, (i) e (ii) valem. Finalmente, para provar (iii) observe que $(g^k)^{n/(n,k)} = (g^n)^{k/(n,k)} = 1$. Logo, se $o(g^k) = m$, então m divide $n/(n,k)$. Além disso, como $(g^k)^m = 1$ e $o(g) = n$, então por (ii), n divide km e então $n/(n,k)$ divide $(k/(n,k))m$. Assim, pelo Lema 1.1.17, $n/(n,k)$ divide m. Portanto, $m = n/(n,k)$. □

O próximo resultado apresenta uma relação entre a normalidade de um subgrupo e propriedades de suas classes laterais.

TEOREMA 1.1.19. *Seja $N \leq G$ um subgrupo de G. Então são equivalentes:*

(i) *N é um subgrupo normal de G.*
(ii) *$Ng = gN$ para todo $g \in G$.*
(iii) *Toda classe lateral à esquerda de N em G é uma classe lateral à direita.*
(iv) *O conjunto das classes laterais à direita de H em G é fechado com relação à multiplicação.*

DEMONSTRAÇÃO. Se (i) vale, então temos que $N^g = N$, para todo $g \in G$, ou seja, $g^{-1}Ng = N$, para todo $g \in G$. Donde, multiplicando à esquerda por g, obtemos, $Ng = gN$, para todo $g \in G$ e (ii) está provado.

A implicação de (ii) em (iii) é imediata. Vejamos agora que (iii) implica (iv). Queremos provar que dados $x, y \in G$, então $NxNy$ é uma classe lateral à direita. Por (iii), obtemos que $xN = Ng$ para algum $g \in G$. Daí, $NxNy = N(Ng)y = Ngy$, que é uma classe lateral à direita de N em G, como afirmamos. Por fim, suponhamos (iv) e vamos obter a afirmação de (i). Para todo $g \in G$, segue de (iv), que $Ng^{-1}Ng$ é uma classe lateral à direita de N em G, que contém $g^{-1}g = 1$. Assim, $g^{-1}Ng \leq Ng^{-1}Ng = N1 = N$. Portanto, do Lema 1.1.9, concluímos que N é subgrupo normal de G. □

COROLÁRIO 1.1.20. *Seja N um subgrupo de G. Então, são equivalentes:*

(i) *N é subgrupo normal de G.*
(ii) *Toda classe lateral à direita de N em G é uma classe lateral à esquerda de N em G.*

(iii) *O conjunto das classes laterais à esquerda de N em G é fechado em relação à multiplicação.*

Agora considere N um subgrupo normal de G. Denotamos por G/N o conjunto $\{Ng \mid g \in G\}$. Pelo Teorema 1.1.19, sabemos que G/N é fechado em relação à multiplicação.

TEOREMA 1.1.21. **[3]** *Sejam G um grupo e N um subgrupo normal de G. Então G/N é um grupo. O elemento identidade de G/N é a classe lateral N e o elemento inverso de cada classe Nx em G/N é Nx^{-1}. Além disso,*

$$(Nx)(Ny) = N(xy),$$

para quaisquer $x, y \in G$.

O grupo G/N é chamado *grupo quociente* de G por N. Observe que se G é um grupo finito e N é um subgrupo normal de G, então pelo Teorema 1.1.16, temos que $|G/N| = |G : N| = |G|/|N|$.

Agora vamos apresentar uma proposição que estabelece uma relação entre a classe de conjugação C_x de um elemento $x \in G$ e o centralizador $C_G(x)$ deste elemento.

PROPOSIÇÃO 1.1.22. *Sejam G um grupo finito e $x \in G$. Então o índice $|G : C_G(x)|$ é igual a ordem da classe de conjugação C_x de x. Em particular, $|C_x|$ é um divisor de $|G|$, para todo $x \in G$.*

Quando um subgrupo H de G não é normal em G, é interessante obter algum subgrupo K de G tal que H é normal em K. Partindo desta ideia, vamos definir o normalizador de um subconjunto de um dado grupo.

DEFINIÇÃO 1.1.23. Seja X um subconjunto do grupo G. Definimos o *normalizador* de X em G como sendo o conjunto

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

LEMA 1.1.24. *Seja X um subconjunto de um grupo G. Então $N_G(X)$ é subgrupo de G. Se X é um subgrupo de G, então X é subgrupo de $N_G(X)$.*

DEMONSTRAÇÃO. Observemos primeiramente que $N_G(X)$ é não-vazio, pois $X^1 = X$ e assim $1 \in N_G(X)$. Agora sejam $g, h \in N_G(X)$, assim, $X^g = X$ e $X^h = X$. Queremos provar que $gh \in N_G(X)$. Com efeito, $X^{gh} = (X^g)^h = X^h = X$. Agora, suponhamos que $g \in N_G(X)$ e vamos provar que $g^{-1} \in N_G(X)$. De fato, $X^{g^{-1}} = (X^g)^{g^{-1}} = X^{gg^{-1}} = X$.

Se X é um subgrupo de G, então a conjugação por qualquer elemento $x \in X$ define um automorfismo de X e, em particular a conjugação é sobrejetiva. Logo, $X^x = X$, e segue que, $X \leq N_G(X)$. □

Corolário 1.1.25. *Seja $H \leq G$ um subgrupo qualquer de G e escreva $N = N_G(H)$. Então H é subgrupo normal de N e se $K \leq G$ tal que $H \leq K$, então H é subgrupo normal de K se, e somente se, $K \leq N$.*

Sabemos da Proposição 1.1.13 que se N é normal em G, então $NH = HN$ e assim NH é subgrupo de G. Uma generalização deste fato é o corolário a seguir.

Corolário 1.1.26. *Sejam H, K subgrupos de G. Se $K \leq N_G(H)$, então $HK = KH$ e HK é subgrupo de G.*

1.2. Comutadores

Definição 1.2.1. Sejam G um grupo e $g, h \in G$ dois elementos arbitrários de G. Definimos o *comutador* de g e h como o elemento de G

$$[g, h] = g^{-1}h^{-1}gh.$$

O lema a seguir, apresenta identidades satisfeitas pelos comutadores de elementos em G.

Lema 1.2.2. *Sejam G um grupo e $x, y, z \in G$ elementos arbitrários de G. Então valem:*

(i) $[y, x] = [x, y]^{-1}$.
(ii) $[xy, z] = [x, z]^y[y, z]$.
(iii) $[x, yz] = [x, z][x, y]^z$.

Demonstração. Vejamos que a afirmação (i) é válida. Para isto basta verificar que $[y, x][x, y] = 1$. Temos $[y, x][x, y] = y^{-1}x^{-1}yxx^{-1}y^{-1}xy = 1$, como queríamos provar.

Agora vamos verificar a validade da afirmação (ii). Observe que, por um lado:

$$[xy, z] = (xy)^{-1}z^{-1}xyz = y^{-1}x^{-1}z^{-1}xyz. \tag{1.2.1}$$

Por outro lado,

$$[x, z]^y[y, z] = y^{-1}[x, z]y[y, z] = y^{-1}x^{-1}z^{-1}xyz. \tag{1.2.2}$$

Assim, por (1.2.1) e (1.2.2), obtemos a igualdade em (ii).

Finalmente vamos provar (iii). Com efeito, pelo item (i), temos que, $[x, yz] = [yz, x]^{-1}$. Assim, por (ii) temos:

$$[x, yz] = ([y, x]^z[z, x])^{-1} = (z^{-1}y^{-1}x^{-1}yzx)^{-1} = x^{-1}z^{-1}y^{-1}xyz. \tag{1.2.3}$$

Mas, temos também:

$$[x, z][x, y]^z = x^{-1}z^{-1}xzz^{-1}x^{-1}y^{-1}xyz = x^{-1}z^{-1}y^{-1}xyz. \tag{1.2.4}$$

Assim, por (1.2.3) e (1.2.4), obtemos a igualdade em (iii). □

Se o grupo G é abeliano, então $xy = yx$, para todo $x, y \in G$. Assim, $[x, y] = x^{-1}y^{-1}xy = xy^{-1}yx = 1$. Reciprocamente, se $[x, y] = 1$, para quaisquer $x, y \in G$, então x e y comutam, donde G é abeliano.

Na definição do comutador de x por y, podemos escrever: $[x, y] = x^{-1}x^y$, ou de modo similar, podemos escrever $[x, y] = (y^{-1})^x y$.

Partindo da definição de comutadores entre dois elementos de um grupo G, vamos definir o comutador de dois subgrupos de G.

Definição 1.2.3. Sejam H, K subgrupos de G, escrevemos $[H, K]$ para denotar o subgrupo de G gerado pelo conjunto $\{[h, k] \mid h \in H, k \in K\}$ de todos os comutadores de elementos de H com elementos de K. O subgrupo $[H, K]$ é chamado o *comutador* de H e K.

Em geral $[H, K]$ não é igual ao conjunto dos comutadores dos elementos de H com elementos de K, mas ele é o subgrupo gerado por este conjunto, ou equivalentemente, $[H, K]$ é o menor subgrupo de G que contém todos esses comutadores.

Proposição 1.2.4. *Sejam H, K subgrupos de G. O subgrupo comutador $[H, K]$ de H e K é trivial se, e somente, se $H \leq C_G(K)$ e $K \leq C_G(H)$,ou seja quando H e K centralizam um ao outro.*

Demonstração. Se $H \leq C_G(K)$ e $K \leq C_G(H)$, então $[h, k] = 1$ para quaisquer $h \in H$ e $k \in K$. Logo, o subgrupo gerado por estes comutadores é trivial, ou seja $[H, K] = 1$. A recíproca é imediata, pois se $[H, K] = 1$, logo $[h, k] = 1$ para todo $h \in H$ e todo $k \in K$ e assim, $H \leq C_G(K)$ e $K \leq C_G(H)$. □

A proposição seguinte é útil em diversas situações onde os conceitos relacionados a comutadores são usados.

Proposição 1.2.5. *Sejam H, K subgrupos de um grupo G. Então $[H, K] = [K, H]$.*

DEMONSTRAÇÃO. Sabemos que $[H,K] = \langle S_1 \rangle$, onde $S_1 = \{[h,k] \mid h \in H, k \in K\}$ e $[K,H] = \langle S_2 \rangle$, onde $S_2 = \{[k,h] \;\; k \in K, h \in H\}$. Mas, pelo Lema 1.2.2(i), temos que $[h,k] = [k,h]^{-1}$. Então os comutadores geradores de $[H,K]$ são exatamente os inversos dos comutadores geradores de $[K,H]$. Assim, $[H,K] = [K,H]$. □

Um caso particular da Definição 1.2.3 é quando tomamos H e K ambos iguais a G. O subgrupo gerado por todos os comutadores em G é chamado o subgrupo *derivado* ou subgrupo *comutador* de G e é denotado por G'. Assim, $G' = [G,G] = \langle S \rangle$, onde $S = \{[g,h] \mid g,h \in G\}$. Note que o grupo $[G,G]$ é gerado por todos os comutadores em G, mas não consiste, necessariamente, apenas de comutadores. Além disso, segue da Proposição 1.2.4, que $[G,G]$ é trivial se, e somente se, $G \leq C_G(G)$, ou seja, se, e somente se, G é abeliano.

LEMA 1.2.6. *Sejam G um grupo e G' o subgrupo derivado de G. Então as afirmações a seguir são verdadeiras:*

(i) *O subgrupo derivado G' é característico em G. Em particular, este subgrupo é normal em G.*
(ii) *O grupo quociente G/G' é abeliano.*
(iii) *Se N é um subgrupo normal de G e o grupo quociente G/N é abeliano, então G' é subgrupo de N. Ou seja, G' é o menor subgrupo normal de G tal que o grupo quociente é abeliano.*

LEMA 1.2.7. *Sejam H e K subgrupos de um grupo G. Então H e K normalizam $[H,K]$, ou equivalentemente, $[H,K]$ é subgrupo normal de $\langle H,K \rangle$, o subgrupo gerado por H e K.*

DEMONSTRAÇÃO. Como, pela Proposição 1.2.5, $[H,K] = [K,H]$, por simetria, é suficiente verificar que $H \leq N_G([H,K])$, ou seja, que para todo $x \in H$, temos $[H,K]^x = [H,K]$. Sejam $h, x \in H$ e $k \in K$ tomados arbitrariamente. Então, pelo Lema 1.2.2(ii), temos que, $[hx,k] = [h,k]^x[x,k]$, donde obtemos, $[h,k]^x = [hx,k][x,k]^{-1}$. Como $[hx,k] \in [H,K]$ e $[x,k]^{-1} \in [H,K]$, segue que, $[h,k]^x \in [H,K]$. Em outras palavras, conjugação por $x \in H$ leva cada gerador $[h,k]$ de $[H,K]$ em $[H,K]$ e, então, $[H,K]^x \subseteq [H,K]$. Como $[h,k]^x \in [H,K]$, para qualquer $x \in H$, em particular $[H,K]^{x^{-1}} \leq [H,K]$, daí segue que $[H,K] = ([H,K]^{x^{-1}})^x \leq [H,K]^x$. Portanto, $[H,K]^x = [H,K]$. □

Pela Proposição 1.2.4, sabemos que K centraliza H se, e somente se, $[H,K] = 1$. Este resultado pode ser "generalizado" como é apresentado no lema seguinte.

LEMA 1.2.8. *Sejam N um subgrupo normal de um grupo G e H, K subgrupos arbitrários de G. Escreva $\overline{G} = G/N$. Denotamos por $\overline{M}$ a imagem de um subgrupo qualquer M de G em G/N. Então, $\overline{[H,K]} = [\overline{H}, \overline{K}]$. E, em particular, $\overline{H}$ e $\overline{K}$ centralizam um ao outro em $\overline{G}$ se, e somente se, $[H,K] \leq N$.*

A relação "K normaliza H" também pode ser expressa em linguagem de comutadores.

LEMA 1.2.9. *Sejam H e K subgrupos de um grupo G. Então, $K \leq N_G(H)$ se, e somente se, $[H,K] \leq H$. Em particular, H é normal em G se, e somente se, $[H,G] \leq H$.*

DEMONSTRAÇÃO. Sejam $h \in H$ e $k \in K$ elementos arbitrários. Como $[h,k] = h^{-1}h^k$, segue daí que $h^k = h[h,k]$. Assim, $h^k \in H$ se, e somente se, $[h,k] \in H$. O resultado agora é imediato. □

Observe que, se H e K normalizam um ao outro, então, pelo Lema 1.2.9, $[H,K] \leq H \cap K$. Se, além disso, $H \cap K = 1$, então $[H,K] = 1$ e assim, H e K centralizam um ao outro.

Podemos generalizar a definição de comutador de dois elementos e de comutador de dois subgrupos do seguinte modo.

DEFINIÇÃO 1.2.10. Definimos o comutador de três elementos arbitrários x, y, z de G, pondo:

$$[x,y,z] = [[x,y],z].$$

Similarmente, definimos o comutador de três subgrupos arbitrários X, Y, Z de G, pondo:

$$[X,Y,Z] = [[X,Y],Z].$$

Mais geralmente, para $n > 2$, definimos o comutador de n elementos $x_j \in G$ de G, pondo:

$$[x_1, x_2, \cdots, x_n] = [[x_1, x_2, \cdots, x_{n-1}], x_n],$$

e o comutador de n subgrupos $X_j \leq G$ de G, pondo:

$$[X_1, X_2, \cdots, X_n] = [[X_1, X_2, \cdots, X_{n-1}], X_n].$$

Vamos apresentar agora a igualdade conhecida como identidade de *Hall-Witt*. A mesma afirma que, dados x, y e $z \in G$, onde G é um grupo qualquer, temos que:

$$[x, y^{-1}, z]^y [y, z^{-1}, x]^z [z, x^{-1}, y]^x = 1. \tag{1.2.5}$$

A verificação deste resultado consiste em expandir os comutadores e cancelar os termos obtidos. Esta igualdade é usada para provar o próximo lema, que é conhecido como *Lema dos Três Subgrupos*.

LEMA 1.2.11 (Lema dos Três Subgrupos). *Sejam X, Y e Z subgrupos arbitrários de um grupo G e suponha que $[X, Y, Z] = 1$ e $[Y, Z, X] = 1$. Então, $[Z, X, Y] = 1$.*

DEMONSTRAÇÃO. Queremos provar que $[Z, X, Y] = [[Z, X], Y] = 1$, ou seja que todo elemento do subgrupo $[Z, X]$ comuta com todo elemento do subgrupo Y. Para isto, é suficiente verificar que, para $y \in Y$, o centralizador de y em G, $C_G(y)$, contém todos os comutadores $[z, x]$, para qualquer $z \in Z$ e $x \in X$. Pois, sendo $C_G(y)$ subgrupo de G, se ele contém todos estes comutadores, contém também o subgrupo $[Z, X]$ gerado por estes comutadores. Portanto, é suficiente provar que $[[z, x], y] = 1$, para todo $z \in Z, x \in X, y \in Y$, ou equivalentemente, que $[z, x^{-1}, y] = 1$, para quaisquer $z \in Z, x \in X, y \in Y$.

Como $[x, y^{-1}] \in [X, Y]$, temos que, $[x, y^{-1}, z] \in [X, Y, Z]$. Mas sabemos, por hipótese, que $[X, Y, Z] = 1$, portanto, $[x, y^{-1}, z] = 1$. Analogamente, de $[Y, Z, X] = 1$, segue que $[y, z^{-1}, x] = 1$. Assim obtemos, $[x, y^{-1}, z]^y = 1$ e $[y, z^{-1}, x]^z = 1$. Daí, pela identidade (1.2.5), segue que $[z, x^{-1}, y]^x = 1$. Donde, $[z, x^{-1}, y] = 1$, como desejado. □

Combinando o Lema 1.2.8 com o Lema 1.2.11, temos o seguinte resultado.

COROLÁRIO 1.2.12. *Seja N um subgrupo normal de um grupo G e sejam X, Y, Z subgrupos arbitrários de G. Se $[X, Y, Z] \leq N$ e $[Y, Z, X] \leq N$, então $[Z, X, Y] \leq N$.*

1.3. Grupos Solúveis e Grupos Nilpotentes

Os grupos finitos simples são como "blocos", a partir dos quais, em certo sentido, todos os grupos finitos são construídos. Estes grupos simples são essencialmente de duas variedades: os grupos cíclicos de ordem prima e os grupos simples finitos não-abelianos. Nesta seção vamos tratar dos grupos cujos "blocos" simples são todos abelianos, e, portanto, de ordem prima. Estes grupos são os grupos finitos "solúveis".

A palavra "solúvel" associada a grupos é devida a *Evariste Galois* no início do século XIX. Galois mostrou que dado algum polinômio com coeficientes racionais, é possível associar um grupo a este polinômio, que hoje é chamado o "grupo de Galois" do polinômio. Ele ainda estabeleceu precisamente o que significa um polinômio ser "solúvel" por radicais. Não é grande

surpresa que o critério de solubilidade polinomial seja precisamente que o grupo de Galois do polinômio seja solúvel. Não vamos nos deter em solubilidade de polinômios, mas vale a pena destacar o seguinte exemplo: um polinômio de grau 5, geralmente, não é solúvel e isto é devido ao fato de o grupo simétrico S_5 não ser solúvel, pois A_5 é simples. A seguir daremos uma definição de grupo solúvel.

DEFINIÇÃO 1.3.1. Um grupo G é dito *solúvel* quando existe uma coleção finita de subgrupos normais $G_0, G_1, \dots\ G_n$ de G, tais que

$$1 = G_0 \leq\ G_1 \leq\ \cdots\ \leq\ G_n = G$$

e G_{i+1}/G_i é abeliano, para $0 \leq i < n$.

Observe que se G é abeliano, então os subgrupos 1 e G cumprem as condições da Definição 1.3.1, logo G é solúvel.

Relembremos que dado um conjunto não-vazio Ω, o conjunto, denotado por $Sym(\Omega)$, das aplicações bijetivas de Ω em Ω, munido da composição usual de funções, é um grupo, chamado *grupo de permutações* de Ω. Quando o conjunto Ω é finito e $|\Omega| = n$, comumente denotamos $Sym(\Omega)$ por S_n. O primeiro exemplo de grupo não abeliano solúvel é o grupo S_3.

Uma caracterização equivalente de solubilidade de um grupo, porém mais simples de ser aplicada, é dada em termos da *série derivada*. Sabemos que o subgrupo derivado G' de G é o subgrupo gerado por todos os comutadores $[x, y]$, para $x, y \in G$ e pelo Lema 1.2.6(iii), que G' é o menor subgrupo normal de G tal que o grupo quociente G/G' é abeliano.

Seja G um grupo e G' seu subgrupo derivado. O subgrupo derivado de G' é o subgrupo $(G')' = G'' = [G', G']$. O subgrupo derivado de G'' é o subgrupo $(G'')' = G''' = [G'', G'']$ e assim sucessivamente. Para estes subgrupos derivados, usaremos a notação:

$$G^{(0)} = G, G^{(1)} = G', G^{(2)} = G'', \dots,\ G^{(n)} = (G^{(n-1)})',$$

para $n > 0$. Assim, temos

$$G = G^{(0)} \geq\ G^{(1)} \geq \cdots \geq G^{(i)} \geq\ \cdots, \tag{1.3.1}$$

e esta série é chamada a *série derivada* de G.

LEMA 1.3.2. *Seja $\varphi : G_1 \to G_2$ um homomorfismo sobrejetivo entre os grupos G_1 e G_2. Então $\varphi(G_1^{(n)}) = G_2^{(n)}$, para todo $n \geq 0$. Além disso, $G_1^{(n)}$ é característico em G_1, para todo $n \geq 0$.*

DEMONSTRAÇÃO. Dados $x, y \in G_1$ arbitrários, temos que $\varphi([x,y]) = [\varphi(x), \varphi(y)]$, e como φ é sobrejetiva, temos que $\varphi(G_1) = G_2$. Assim, φ leva o conjunto dos comutadores de G_1 no conjunto dos comutadores de G_2. Segue daí que, $\varphi(G_1') = G_2'$. Repetindo este argumento, concluímos que $\varphi(G_1^{(n)}) = G_2^{(n)}$, para $n \geq 0$.

A afirmação de que $G_1^{(n)}$ é característico em G_1, para todo $n \geq 0$, segue da parte já provada do lema, no caso particular que $G_1 = G_2$ e $\varphi \in Aut(G_1)$. □

Agora podemos substituir a série normal não especificada da Definição 1.3.1, por uma série particular canônica.

TEOREMA 1.3.3. *Um grupo G é solúvel se, e somente se, $G^{(n)} = 1$ para algum inteiro n. Além disso, subgrupos e quocientes de grupos solúveis são solúveis.*

DEMONSTRAÇÃO. Suponha G um grupo solúvel, então por definição existe uma coleção finita de subgrupos normais $G_i \lhd G$ com

$$1 = G_0 \leq G_1 \leq \cdots \leq G_n = G,$$

e tais que G_{i+1}/G_i é abeliano, para todo $0 \leq i < n$. Assim, pelo Lema 1.2.6(iii), segue que $(G_{i+1})' \leq G_i$, para todo $0 \leq i < n$. Em particular, como $G_n/G_{n-1} = G/G_{n-1}$ é abeliano, então $G' \leq G_{n-1}$. Daí, $G'' = (G')' \leq (G_{n-1})' \leq G_{n-2}$, e continuando com este argumento, obtemos $G^{(k)} \leq G_{n-k}$, para $0 \leq k \leq n$. Assim, concluímos que $G^{(n)} \leq G_0 = 1$, como queríamos demonstrar. Reciprocamente, se $G^{(n)} = 1$, então a série

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

satisfaz as condições da Definição 1.3.1, uma vez que $G^{(k)}$ é subgrupo normal de G, para todo k.

Agora, considere $H \leq G$ um subgrupo arbitrário de G. Daí, $H' \leq G'$ e mais geralmente, temos que $H^{(k)} \leq G^{(k)}$. Assim, se G é solúvel, pela parte já demonstrada do teorema, sabemos que existe algum n tal que $G^{(n)} = 1$, e como $H^{(n)} \leq G^{(n)} = 1$, concluímos que $H^{(n)} = 1$, donde H é solúvel. Além disso, se N é um subgrupo normal de G, então, aplicando o Lema 1.3.2 ao homomorfismo canônico $\varphi : G \to G/N$, obtemos que $\varphi(G^{(k)}) = (G/N)^{(k)}$, assim, se $G^{(n)} = 1$, então $(G/N)^{(n)} = 1$, isto é, G/N é solúvel. □

Se um grupo G é solúvel, o *comprimento derivado* $dl(G)$ de G é definido como o menor inteiro não-negativo n tal que $G^{(n)} = 1$. Observe que os grupos com comprimento derivado 1, são exatamente os grupos abelianos

não triviais. Geralmente, grupos obtidos a partir de grupos solúveis são também solúveis, como nos afirma o lema a seguir.

LEMA 1.3.4. *Seja N um subgrupo normal do grupo G. Se N e G/N são, ambos, solúveis, então G é solúvel e, além disso,*

$$dl(G) \leq dl(N) + dl(G/N).$$

DEMONSTRAÇÃO. Sejam $dl(N) = n$ e $dl(G/N) = m$. Como o homomorfismo canônico $\varphi : G \to G/N$ leva $G^{(m)}$ em $(G/N)^{(m)} = 1$, obtemos que $G^{(m)} \leq N$. Assim, $G^{(m+n)} = (G^{(m)})^{(n)} \leq N^{(n)} = 1$. Donde seguem as afirmações. □

TEOREMA 1.3.5. *Seja G um grupo e sejam N e M subgrupos solúveis normais de G. Então o produto MN é solúvel.*

DEMONSTRAÇÃO. Como N é subgrupo normal de G, então segue da Proposição 1.1.13 que, MN é subgrupo de G. Agora, pelo Segundo Teorema de Isomorfismo, temos que $MN/N \cong M/M \cap N$. Como M é solúvel, pelo Teorema 1.3.3, temos que $M/M \cap N$ é solúvel. Logo, MN/N é solúvel. E como N é solúvel, pelo Lema 1.3.4, concluímos que MN é solúvel. □

Relembremos, sem demonstrar, alguns resultados que fornecem exemplos de grupos solúveis.

TEOREMA 1.3.6. **[3]** *Todo p-grupo finito, é solúvel.*

TEOREMA 1.3.7 (Burnside). *Todo grupo de ordem $p^a q^b$, onde p e q são primos distintos e a e b são inteiros não negativos é solúvel.*

TEOREMA 1.3.8 (Feit-Thompson). *Todo grupo finito de ordem ímpar é solúvel.*

Finalizando esta seção vamos abordar os grupos nilpotentes, que são uma subclasse da classe dos grupos solúveis.

DEFINIÇÃO 1.3.9. Um grupo G é dito *nilpotente* se existe uma coleção finita de subgrupos normais $G_0, G_1, \ldots, G_n$ com

$$1 = G_0 \leq G_1 \leq \ldots \leq G_n = G$$

e tais que $G_{i+1}/G_i \leq Z(G/G_i)$, para $0 \leq i < n$.

Pela Definição 1.3.1, segue que se G é nilpotente, então G é solúvel.

LEMA 1.3.10. *Seja G um grupo finito e assuma que $Z(G/N) > 1$ para todo subgrupo normal próprio N de G. Então G é nilpotente.*

DEMONSTRAÇÃO. Defina os subgrupos Z_i, para $i \geq 0$ como segue. Ponha $Z_0 = 1$ e $Z_1 = Z(G)$. O subgrupo Z_2 é definido como o subgrupo de G tal que $Z_2/Z_1 = Z(G/Z_1)$. Segue do Teorema da Correspondência, encontrado em **[3]**, que tal subgrupo existe e é único. Observe Z_2 é normal em G. Continuando com este processo, definimos Z_i como o único subgrupo de G tal que $Z_i/Z_{i-1} = Z(G/Z_{i-1})$, para $i > 0$. Por hipótese, se $Z_i < G$ é um subgrupo próprio de G, então $Z_i \leq Z_{i+1}$ e como G é finito, então $Z_n = G$, para algum n. Logo, G é nilpotente. □

COROLÁRIO 1.3.11. *Todo p-grupo finito é nilpotente.*

DEMONSTRAÇÃO. Observe que se P é um p-grupo não trivial, então P tem centro não trivial. Efetivamente, se $|P| = p^m$, então pela equação de classe (1.1.1), temos que $p^m = n_1 + n_2 + \cdots + n_k$, onde cada $n_i = |C_{x_i}|$, para todo $i = 1, 2, \cdots, k$. Pela Proposição 1.1.22, temos que cada n_i divide p^m e, então é uma potência de p. Se o centro $Z(P)$ fosse trivial, apenas um n_i seria igual a 1 e assim, $p^m \equiv 1 \bmod p$, o que é impossível, pois $p^m > 1$. Portanto, $Z(P) \neq 1$. Agora o resultado segue imediatamente do Lema 1.3.10. □

Um conjunto de subgrupos normais N_i em G tais que

$$N_0 \leq N_1 \leq \cdots \leq N_n$$

é chamada uma *série central* em G se $N_{i+1}/N_i \leq Z(G/N_i)$, para $0 \leq i < n$. Portanto, um grupo G é nilpotente se, e somente se, tem uma série central finita contendo 1 e G. Usando a ideia da demonstração do Lema 1.3.10, podemos construir uma série central em qualquer grupo. Para isto, defina $Z_0(G) = 1$ e indutivamente, defina $Z_i(G)$ pela equação

$$Z_i(G)/Z_{i-1}(G) = Z(G/Z_{i-1}(G)),$$

para $i > 0$. A coleção $\{Z_i(G) \mid i \geq 0\}$ é chamada *série central superior ou ascendente* de G. Claro que se $Z_n(G) = G$, para algum inteiro n, então G é nilpotente e já vimos também que a recíproca deste fato é verdadeira.

Outra série central relevante é a *série central inferior*. Seja G um grupo. Escrevemos $\gamma_1(G) = G, \gamma_2(G) = [\gamma_1(G), G] = [G, G] = G'$. Indutivamente, se temos $\gamma_{i-1}(G)$ definimos $\gamma_i(G)$ pondo $\gamma_i(G) = [\gamma_{i-1}(G), G]$, para todo $i > 0$.

Se $H \leq K \leq G$, então $[H,G] \leq [K,G]$. Assim, como $\gamma_2(G) \leq \gamma_1(G)$, obtemos $\gamma_3(G) \leq \gamma_2(G)$ e, mais geralmente, temos:

$$G = \gamma_1(G) \geq \gamma_2(G) \geq \gamma_3(G) \cdots . \tag{1.3.2}$$

A série central inferior de G é a coleção dos subgrupos $\gamma_i(G)$. Para verificar que $\{\gamma_i(G)\}$ é realmente um série central, precisamos mostrar que cada $\gamma_i(G)$ é normal em G e que $\gamma_{i-1}(G)/\gamma_i(G) \leq Z(G/\gamma_i(G))$, para todo $i \geq 2$. Como os subgrupos $\gamma_i(G)$ são característicos em G, logo são normais em G.

LEMA 1.3.12. *Sejam H e N subgrupos de G e suponha que N é normal em G. Então $[H,G] \leq N$ se, e somente se, $HN/N \leq Z(G/N)$.*

DEMONSTRAÇÃO. Seja $\varphi : G \to G/N$ o homomorfismo canônico. Temos que $\varphi(H)$ é central em $\varphi(G)$ se, e somente se, $1 = [\varphi(H), \varphi(G)] = \varphi([H,G])$ e isto ocorre se, e somente se, $[H,G] \leq \mathrm{Ker}(\varphi) = N$. Como $\varphi(G) = G/N$ e $\varphi(H) = HN/N$, então segue o resultado. □

COROLÁRIO 1.3.13. *A série central inferior de G é uma série central para G.*

TEOREMA 1.3.14. *Sejam G um grupo qualquer e $n \geq 1$ um inteiro. Então as afirmações são equivalentes:*

(i) $\gamma_{n+1}(G) = 1$.
(ii) $Z_n(G) = G$.

Além disso, G é nilpotente se, e somente se, (i) e (ii) valem para algum inteiro n.

DEMONSTRAÇÃO. Se (i) ou (ii) vale, então G é nilpotente. Podemos então supor que G é nilpotente e provar que (i) e (ii) valem para o mesmo inteiro n. Agora seja $1 = N_0 \leq N_1 \leq \cdots \leq N_k = G$ uma série central para G. Como $N_{i+1}/N_i \leq Z(G/N_i)$, segue do Lema 1.3.12 que $[N_{i+1}, G] \leq N_i$. Temos $\gamma_1(G) = N_k$ e $\gamma_2(G) = [G,G] \leq [N_k, G] \leq N_{k-1}$ e, similarmente, temos $\gamma_3(G) = N_{k-2}$. Mais geralmente, temos $\gamma_i(G) \leq N_{k-i+1}$ e, então $\gamma_{k+1}(G) = 1$ e (i) vale para algum inteiro n. Agora vejamos que (ii) implica (i). De fato, se $Z_n(G) = G$, para algum inteiro n, podemos fazer $N_i = Z_i(G)$ e $k = n$ e concluímos que $\gamma_{n+1}(G) = 1$.

Agora escreva $Z_i = Z_i(G)$ e vamos mostrar que $N_i \leq Z_i$, para todo i. Claro, que para $i = 0$, $N_0 \leq Z_0$. Trabalhando por indução, assumimos que

$i > 0$ e $N_{i-1} \leq Z_{i-1}$. Agora, $[N_i, G] \leq N_{i-1} \leq Z_{i-1}$ e então pelo Lema 1.3.12, temos

$$N_i Z_{i-1}/Z_{i-1} \leq Z(G/Z_{i-1}) = Z_i/Z_{i-1},$$

e temos $N_i \leq Z_i$, como queríamos. Segue daí que $Z_k(G) = G$ e (ii) vale para algum inteiro k. Agora finalmente vejamos que (i) implica (ii). Com efeito, se $\gamma_{n+1}(G) = 1$, fazendo $N_i = \gamma_{n-i}(G)$ e $k = n$, concluímos que $Z_n = G$. □

Definição 1.3.15. O menor inteiro n tal que $Z_n(G) = G$ é chamado a *classe de nilpotência* de G.

Assim, pelo Teorema 1.3.14, a classe de nilpotência de G pode ser definida, de modo equivalente, como o menor inteiro n tal que $\gamma_{n+1}(G) = 1$. Os grupos abelianos têm classe de nilpotência 1 e os grupos não abelianos tais que $G' \leq Z(G)$ são exatamente os grupos com classe de nilpotência 2.

Corolário 1.3.16. *Subgrupos e grupos quocientes de grupos nilpotentes são também nilpotentes.*

Demonstração. Seja H subgrupo arbitrário de G, daí $\gamma_n(H) \leq \gamma_n(G)$, logo, se $\gamma_n(G) = 1$, então $\gamma_n(H) = 1$ e H é nilpotente. Considere agora N um subgrupo normal de G. Note que se $\varphi : G \to G/N$ é o homomorfismo canônico, então $\varphi(\gamma_n(G)) = \gamma_n(G/N)$. Assim, se $\gamma_n(G) = 1$, temos $\gamma_n(G/N) = 1$ e G/N é nilpotente. □

Lema 1.3.17. **[3]** *Se $G_1, \ldots, G_n$ são grupos nilpotentes,então $G_1 \times \cdots \times G_n$ é nilpotente.*

Lema 1.3.18 (Argumento de Frattini). *Sejam G um grupo e N um subgrupo finito normal de G. Seja P um p-subgrupo de Sylow de N. Então $G = N_G(P)N$.*

Demonstração. Seja $g \in G$ e note que $P^g \leq N^g = N$. Como $|P^g| = |P|$, concluímos que P^g também é um p-subgrupo de Sylow de N, logo $P^{gn} = P$, para algum $n \in N$. Assim, $gn \in N_G(P)$ e então $g \in N_G(P)n^{-1} \leq N_G(P)N$. Como g foi tomado arbitrariamente em G, segue o resultado. □

Para grupos finitos certas condições são equivalentes à nilpotência como é enunciado no seguinte teorema.

Teorema 1.3.19. *Seja G um grupo finito. As afirmações a seguir são equivalentes:*

(i) *G é nilpotente.*

(ii) *Quando $H < G$, então $H \leq N_G(H)$.*

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

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

(v) *G é o produto direto de seus p-subgrupos de Sylow, com p primo.*

DEMONSTRAÇÃO. Assuma (i) e seja $1 = N_0 \leq N_1 \leq \cdots \leq N_n = G$ uma série central para G. Dado H um subgrupo próprio qualquer de G, seja k o maior inteiro tal que $N_k \leq H$ e note que $k < n$. Vamos justificar (ii), mostrando que $N_{k+1} \leq N_G(H)$. Pelo Lema 1.2.9, é suficiente demonstar que $[H, N_{k+1}] \leq H$. Como $\{N_i\}$ é uma série central, e então, pelo Lema 1.3.12, temos $[H, N_{k+1}] \leq N_k$. Assim, vale (ii), já que $N_k \leq H$.

Agora se $M < G$ é subgrupo maximal de G, então, por (ii) $N_G(M) > M$. Como M é maximal, temos $N_G(M) = G$ e assim, M é normal em G. E, portanto, (ii) implica (iii).

Assuma (iii) verdadeiro e seja $P \in Syl_p(G)$ um p-subgrupo de Sylow de G, para algum p primo. Se $N_G(P) < G$, escolha M um subgrupo maximal de G tal que $N_G(P) \leq M$. Como por (iii) M é normal em G, podemos aplicar o Lema 1.3.18 para concluir que $G = N_G(P)M$. Como, $N_G(P) \leq M < G$, chegamos a uma contradição. Então, devemos ter $N_G(P) = G$, isto é, P normal em G e (iv) está demonstrado.

Agora considere a hipótese de (iv). Pela normalidade de cada subgrupo de Sylow de G, então existe exatamente um p-subgrupo de Sylow de G para cada p primo. O produto de todos os subgrupos de Sylow é, claramente, direto e, tem que ser igual a G. Finalmente, observe que para verificar que (v) implica (i) é suficiente demonstrar que o produto direto de grupos nilpotentes é nilpotente. Assim, esta implicação é imediata do Lema 1.3.17. □

O resultado a seguir é devido a Fitting.

TEOREMA 1.3.20 (Teorema de Fitting). *Sejam M e N subrupos normais nilpotentes de um grupo G. Se c e d são a classe de nilpotência de M e N, respectivamente, então $L = MN$ é nilpotente de classe no máximo $c + d$.*

DEMONSTRAÇÃO. Vamos calcular os termos da série central inferior de L mostrando, por indução sobre i, que $\gamma_i(L)$ é o produto de todos os comutadores $[X_1, \cdots, X_i]$, onde $X_j = M$ ou $X_j = N$. Claramente, se $i = 1$, temos que $\gamma_1(L) = L = MN$ e o resultado é válido.

Observemos que, se U, V e W são subgrupos normais de G, então segue dos itens (ii) e (iii) do Lema 1.2.2, que $[UV, W] = [U, W][V, W]$ e $[U, VW] =$

$[U,V][U,W]$. Segue disto que

$$\gamma_{i+1}(L) = [\gamma_i(L), L] = [\gamma_i(L), M][\gamma_i(L), N]$$

e então, usando a hipótese intutiva, concluimos que $\gamma_{i+1}(L)$ é o produto de todos $[X_1, \cdots, X_i, X_{i+1}]$, com $X_j = M$ ou $X_j = N$.

Para completar a demonstração consideremos $i = c + d + 1$. Então no comutador $[X_1, \cdots, X_i]$ ou M ocorre no mínimo $c + 1$ vezes ou N ocorre no mínimo $d + 1$ vezes. Além disso, sabemos pelo Lema 1.2.9, que se A é subgrupo normal de G, então $[A, G]$ é subgrupo de A. Portanto, $[X_1, \cdots, X_i]$ está contido ou em $\gamma_{c+1}(M)$ ou em $\gamma_{d+1}(N)$, onde ambas as quais são iguais a 1. Consequentemente, $[X_1, \cdots, X_i] = 1$ e $\gamma_i(L) = 1$. Logo, L é nilpotente de classe de nilpotência no máximo $i - 1 = c + d$. □

Observemos que, pelo Teorema 1.3.20, todo grupo finito G possui um único maior subgrupo normal nilpotente que é conhecido como *subgrupo de Fitting* de G e denotado por $\mathrm{F}(G)$.

1.4. O Conceito de Ação de Grupos

Embora existam vantagens em trabalhar com a moderna definição axiomática de grupos ao invés da definição antiga de grupo, como grupo de permutações, existe também desvantagens neste tipo de abordagem. Com um grupo de permutação, temos um conjunto sendo permutado e isto proporciona ferramentas para o estudo do grupo. Por exemplo, se o conjunto possui exatamente n elementos, então pelo Teorema 1.1.16 a ordem do grupo de permutações divide $|S_n| = n!$. A ideia por trás da teoria de ações de grupos é ganhar novamente as vantagens de trabalhar com permutações de grupos enquanto lida com grupos abstratos.

Definição 1.4.1. Sejam G um grupo e Ω um conjunto não-vazio. Assuma que para cada $g \in G$ e cada $\alpha \in \Omega$, está definido um único elemento em Ω, denotado por $\alpha \cdot g$. Suponha que as seguintes condições são satisfeitas:

(i) $\alpha \cdot 1 = \alpha$, para todo $\alpha \in \Omega$ e

(ii) $(\alpha \cdot g) \cdot h = \alpha \cdot (gh)$, para quaisquer $g, h \in G$ e todo $\alpha \in \Omega$.

Então dizemos que G age sobre Ω, ou que "$\cdot$" é uma ação de G sobre Ω, ou ainda que Ω é um G-conjunto.

Exemplo 1.4.2. Os exemplos mais comuns de ação de grupo são os grupos de permutação. Seja $\Omega \neq \emptyset$ um conjunto não-vazio e considere $G \leq S_\Omega$ um subgrupo do grupo de permutações de Ω. Assim, para $\alpha \in \Omega$ e $g \in G$

defina $\alpha \cdot g$ pondo $\alpha \cdot g = g(\alpha)$. Na Definição 1.4.1, a condição (i) segue da definição do elemento identidade de S_Ω e a condição (ii) segue da definição de multiplicação em S_Ω. Portanto, todo subgrupo de S_Ω age sobre Ω.

Definição 1.4.3. Se G é um grupo e Ω um conjunto não-vazio, dizemos que uma ação de G sobre Ω é:

(a) *trivial* se $\alpha \cdot g = \alpha$ para todo $g \in G$ e todo $\alpha \in \Omega$.
(b) *fiel* quando $\alpha \cdot g = \alpha$, para todo $\alpha \in \Omega$, apenas quando g é o elemento identidade de G. Em outras palavras, uma ação é fiel se a identidade de G é o único elemento que fixa todos os pontos de Ω.

Assim, ação trivial é o exemplo mais elementar de ação que não é fiel.

Definição 1.4.4.

(i) Sejam G um grupo e $\Omega \neq \emptyset$. Dizemos que um elemento $g \in G$ *fixa* um elemento $\alpha \in \Omega$ quando, $\alpha \cdot g = \alpha$. Um elemento $\alpha \in \Omega$ é dito G-invariante, se todo $g \in G$ fixa α, ou seja, se $\alpha \cdot g = \alpha$, para todo $g \in G$. Mais geralmente, se G age sobre um subconjunto X de Ω, este é dito G-invariante, se $x \cdot g = x$, para todo $x \in X$ e $g \in G$.
(ii) Um elemento $\alpha \in \Omega$ é dito ser um *ponto fixo* de Ω, quando $\alpha \cdot g = \alpha$ para todo $g \in G$.
(iii) O *núcleo* de uma ação de um grupo G sobre um conjunto não vazio Ω é o conjunto $B = \{g \in G \mid \alpha \cdot g = \alpha, \text{ para todo } \alpha \in \Omega\}$ dos elementos $g \in G$ que agem como a identidade e fixam todos os elementos $\alpha \in \Omega$.

Se o grupo G age sobre o conjunto Ω e B é o núcleo desta ação, temos que B é um subgrupo normal de G e como os elementos de B agem trivialmente sobre Ω, temos que, dado $a \in G$ arbitrário, então todos os elementos da classe lateral Ba de B em G induzem a mesma ação sobre Ω. De fato, dados b_1a e b_2a elementos arbitrários em Ba, temos que $\alpha \cdot b_1a = \alpha \cdot a$ e $\alpha \cdot b_2a = \alpha \cdot a$, para todo $\alpha \in \Omega$. Portanto, resulta bem definida uma ação de $\overline{G} = G/B$ sobre Ω, dada por $\alpha \cdot \overline{a} = \alpha \cdot a$ e claramente, esta ação é fiel.

Vejamos agora alguns exemplo de ação de um grupo G sobre um conjunto não vazio, no caso em que este conjunto é o próprio G. Vejamos dois modos nos quais um grupo G pode agir sobre si mesmo (em outras palavras, estamos tomando $\Omega = G$). Primeiro, para $x, g \in G$ defina $x \cdot g = xg$. Observe que as condições (i) e (ii) da Definição 1.4.1 são satisfeitas. Sendo que a segunda condição segue diretamente da associatividade do grupo G. Neste caso, a

ação de G sobre si memso é chamada *ação regular*. É fácil observar que a ação regular é uma ação fiel. Agora, para $x, g \in G$ defina $x \cdot g = x^g = g^{-1}xg$. Afirmamos que esta aplicação é uma ação. De fato, $x \cdot 1 = x^1 = x$, para todo $x \in G$, logo a condição (i) da Definição 1.4.1 é satisfeita. Além disso,

$$\begin{aligned}(x \cdot g) \cdot h &= (x^g) \cdot h = (x^g)^h = (g^{-1}xg)^h \\ &= (gh)^{-1}xgh = x \cdot (gh),\end{aligned}$$

para todo x, g e $h \in G$. Logo a condição (ii) da Definição 1.4.1 também é satisfeita. Neste caso, a ação de G sobre si memso, é chamada *ação por conjugação* e o centro $Z(G)$ de G é o núcleo desta ação.

Se $X \subseteq G$ é um subconjunto qualquer de G e $g \in G$, então definimos o produto $Xg = \{xg \mid x \in X\}$. Este produto pode ser usado para definir uma ação de G sobre o conjunto Ω de todos os subconjuntos de G. De fato, se $X \in \Omega$ e $g \in G$, definimos $X \cdot g = Xg$. Esta também é uma ação. Com efeito, se $X \in \Omega$, então $X \cdot 1 = X1 = X$ e, além disso, para $g, h \in G$, arbitrários, temos, $(X \cdot g) \cdot h = Xg \cdot h = (Xg)h = X(gh) = X \cdot (gh)$.

Agora se X é ainda um subconjunto de G, então definimos o conjunto $X^g = \{x^g = g^{-1}xg \mid g \in G\}$. Continuemos considerando Ω o conjunto dos subconjuntos de G e estabeleça a seguinte relação $X \cdot g = X^g$, para $X \in \Omega$ e $g \in G$. Observe que aqui temos também uma ação por conjugação. Efetivamente, temos que $X^1 = X$, para todo $X \in \Omega$ e a condição (i) da Definição 1.4.1 é satisfeita. Além disso, $(X \cdot g) \cdot h = X^g \cdot h = (X^g)^h = X^{(gh)} = X \cdot (gh)$ e, então também vale a condição (ii) da Definição 1.4.1. Agora, seja G um grupo e H um subgrupo de G. Vamos definir uma relação entre um elemento de G e um elemento do conjunto $\Omega = \{Hx \mid x \in G\}$ das classes laterais à direita de H em G. Para cada $Hx \in \Omega$ e $g \in G$, defina $Hx \cdot g = H(xg)$. Vejamos que esta relação define uma ação de G sobre Ω.

Se G é um grupo que age sobre algum conjunto Ω e $\alpha \in \Omega$ é um elemento arbitrário de Ω, escrevemos $G_\alpha = \{g \in G \mid \alpha \cdot g = \alpha\}$. Observe que, para cada $\alpha \in \Omega$, G_α é um subgrupo de G. O subgrupo G_α é chamado o *estabilizador* do elemento α em G. Na ação regular de G sobre si mesmo, por exemplo, o estabilizador G_x de um ponto $x \in G$ é o subgrupo trivial. Na ação por conjugação de G, o estabilizador de $x \in G$ é o centralizador $C_G(x)$ e na ação por conjugação de G sobre todos os seus subconjuntos, o estabilizador de um subconjunto X é o normalizador $N_G(X)$.

Agora considere a ação de G sobre o conjunto das classes laterias à direita de H em G, quando H é um subgrupo de G. O estabilizador de uma classe

lateral Hx é o conjunto de todos os elementos $g \in G$ tal que $Hxg = Hx$, logo, g pertence ao estabilizador de Hx se, e somente se, $xg \in Hx$. Segue daí que, g estabiliza Hx se, e somente se, $g \in x^{-1}Hx = H^x$. Portanto, o estabilizador de Hx é exatamente o subgrupo H^x. Assim, o núcleo da ação de G sobre o conjunto das classes laterais à direita de H em G, é exatamente $\bigcap_{x\in G} H^x$.

Observemos que, quando se tem uma ação de um grupo G sobre um conjunto não vazio Ω, se $\alpha \cdot g = \beta$, então os estabilizadores G_α e G_β são conjugados em G e vale $(G_\alpha)^g = G_\beta$.

Para finalizar esta seção sobre conceitos básicos de ação de grupos vamos abordar a noção de *órbita* de uma ação e o conceito de ação *transitiva*.

Suponha que um grupo G age sobre um conjunto não vazio Ω. Se $\alpha \in \Omega$ é um elemento arbitrário de Ω, definimos o conjunto $O_\alpha = \{\alpha \cdot g |\ g \in G\}$ como a órbita de α em relação a ação dada. É fácil verificar que se $\beta \in O_\alpha$, então $O_\beta = O_\alpha$, donde segue que órbitas distintas são disjuntas. Além disso, como todo ponto de Ω está em apenas uma órbita, temos que órbitas de uma ação de G sobre Ω formam uma partição de Ω. Em particular, se Ω é finito, obtemos que $|\Omega| = \sum |O|$, onde nesta soma O percorre o conjunto de todas as órbitas em Ω.

Por exemplo, se H é um subgrupo de G, temos que H age em G por multiplicação à direita. Observe também que as órbitas desta ação são as classes laterais á esquerda de H em G.

Definição 1.4.5. Seja G um grupo que age sobre um conjunto não vazio Ω. Dizemos que G age *transitivamente* sobre Ω, se para quaisquer $\alpha, \beta \in \Omega$, existe $g \in G$ tal que $\alpha \cdot g = \beta$. Em outras palavras, quando em Ω existe apenas uma órbita.

Por exemplo a ação regular de G e a ação usual de G sobre o conjunto das classes laterais à direita de um subgrupo são ações transitivas. Em geral, a ação conjugação de G sobre si mesmo não é transitiva, pois se $x, y \in G$ são elementos de ordens difirentes, então pode não existir um elemento $g \in G$ tal que $x^g = y$. De fato, a conjugação por $g \in G$ define um automorfismo e então preserva as ordens dos elementos.

CAPíTULO 2

Ações de Grupos

Neste capítulo continuamos falando de ações de grupos, só que de modo mais profundo, nos concentramos no conceito de *ação por automorfismos*. Trataremos primeiramente os conceitos de *produto semi-direto* e *complemento* de um subgrupo normal N de um grupo G dado. Em seguida abordamos as noções de *ação coprima* e *pontos fixos* e apresentamos resultados que serão úteis na demonstração dos resultados do Capítulo 3.

Todos os resultados apresentados neste capítulo podem ser encontrados, pelo leitor, em [**4**].

2.1. Complemento e Ação Por Automorfismos

Suponha que um grupo G pode ser escrito como um produto $G = NH$ de um subgrupo normal N e um subgrupo H, onde a interseção $H \cap N = 1$. Então G é chamado o *Produto Semi-direto* de N e H. Neste caso, usamos a notação $G = N \rtimes H$. Por exemplo, o grupo diedral D_{2n} é um produto semi-direto de um grupo cíclico de ordem n e um grupo de ordem 2.

Se G é o produto semi-direto de N e H, então todo elemento $g \in G$ pode ser escrito de modo único na forma $g = nh$, com $n \in N$ e $h \in H$. De fato, suponha que possamos escrever $g = n_1h_1$ e também $g = n_2h_2$, com $n_1, n_2 \in N$ e $h_1, h_2 \in H$. Assim, $n_2^{-1}n_1 = h_2h_1^{-1}$. Como $n_2^{-1}n_1 \in N$ e $h_2h_1^{-1} \in H$, pela igualdade verificada, concluímos que $n_2^{-1}n_1 \in H \cap N$, mas $H \cap N = 1$, portanto, $n_1 = n_2$ e, analogamente, $h_1 = h_2$.

Definição 2.1.1. Dados G um grupo e N um subgrupo normal de G, dizemos que um subgrupo H de G é um *complemento* para N em G quando, $NH = G$ e $N \cap H = 1$.

Neste caso, observe que G é um produto semi-direto de N e H. Assim, se H complementa N em G, então cada elemento $g \in G$ é da forma $g = nh$, com $n \in N$ e $h \in H$ e esta forma de escrever cada elemento $g \in G$ é única. Observe que também podemos escrever cada $g \in G$ de modo único, na forma $g = hn$, com $h \in H$ e $n \in N$. Com efeito, seja $g = nh$, com $n \in N$ e $h \in H$ e suponhamos que podemos escrever $g = \widetilde{h}\widetilde{n}$, com $\widetilde{n} \in N$ e $\widetilde{h} \in H$. Como N

é normal em G, temos $g \in Nh = hN$, donde teria que ser $h = \widetilde{h}$. Agora da equação $h\widetilde{n} = nh$, obtemos $\widetilde{n} = n^h$.

Observe que se H complementa N em G, então $H \cong H/N \cap H$, uma vez que $N \cap H = 1$ e, além disso, $NH/N = G/N$. Daí, pelo Segundo Teorema de Isomorfismo, $H/H \cap N \cong NH/N$ e, portanto temos que $H \cong G/N$. Assim, todos os complementos de N em G são isomorfos a G/N e, então, são isomorfos entre si. O que pode acontecer, no entanto, é que um subgrupo normal de um grupo não possua complemento neste grupo.

Exemplo 2.1.2. Considere o grupo cíclico C_4 de ordem 4 e N o único subgrupo de ordem 2 de C_4. Se N tivesse um complemento em C_4, digamos um subgrupo H, então H seria isomorfo a C_4/N, que tem ordem 2. Pela unicidade de N deveríamos ter $N = H$, mas um subgrupo normal não pode ser seu próprio complemento.

Se H complementa N em G, então, todo subgrupo conjugado de H em G também complementa N. Em geral, no entanto, um subgrupo normal N de G pode ter complementos não-conjugados, embora, como já vimos, todos os complementos sejam isomorfos. O próximo exemplo ilustra este caso.

Exemplo 2.1.3. Considere o grupo de Klein $G = C_2 \times C_2$. Se N é um dos três subgrupos de G de ordem 2, então os outros dois subgrupos de ordem 2 são, ambos, complementos de N em G, mas estes subgrupos não são conjugados em G, já que G é abeliano.

No estudo de complemento de um subgrupo normal de um dado grupo, o principal objetivo é construir, a menos de isomorfismo, todos os grupos G, a partir de dois grupos N e H dados, que possui um subgrupo normal N_0 complementado por um subgrupo H_0, onde $N \cong N_0$ e $H \cong H_0$. Neste caso, o grupo G é chamado uma extensão *split* de N por H. Em outras palavras, se G é uma extensão *split* de N por H, então G é o produto direto de N e H.

O conceito de extensão é mais amplo que o de extensão split. Dados dois grupos arbitrários N e H. Um grupo G é dito uma *extensão* de N por H se existe um subgrupo N_0 normal de G tal que $N_0 \cong N$ e $G/N_0 \cong H$. Quando G é um extensão de N por H, então o subgrupo normal N_0 de G tal que $N_0 \cong N$ e $G/N_0 \cong H$ não é unicamente determinado. Pode ocorrer, por exemplo, que com uma dada escolha de N_0 a extensão é split, mas com uma outra escolha, tal extensão não o seja. Assim, sabendo que um grupo G é uma extensão de N por H, é natural perguntar se esta extensão é split ou

não. Por exemplo, o grupo $G = \{1, a, b, ab\}$ de Klein é uma extensão split de $N = \langle a \rangle$ por $H = \langle b \rangle$, mas o grupo $C_4 = \langle a \rangle = \{1, a, a^2, a^3\}$ cíclico de ordem 4 possui apenas um subgrupo de ordem 2, logo não é extensão split desse subgrupo.

Suponha que G é uma extensão split de um subgrupo normal N e que H é um complemento de N em G. Como N é normal, temos que H age por conjugação sobre N e de fato, a conjugação por $h \in H$ induz um automorfismo de N. Se H também é normal em G, como $H \cap N = 1$, vemos que H centraliza N e então, a ação por conjugação de H sobre N é trivial. Assim, para construir extensões split, que não são simplesmente produtos diretos, é necessário considerar ações por conjugação de H sobre N não-triviais. É importante notar que os subgrupos N e H e a ação por conjugação de H sobre N determinam completamente G (a menos de isomorfismo). Antes de apresentar esse resultado de unicidade, vamos introduzir uma notação. Considere N e N_0 grupos isomorfos, onde algum isomorfismo é dado. Para $n \in N$, escreveremos $n_0 \in N_0$ para denotar a imagem de n pelo isomorfismo dado de N em N_0. Portanto, podemos denotar com $()_0$ o isomorfismo entre N e N_0. A notação, $()_0$, será usada também para denotar um dado isomorfismo entre H e H_0.

LEMA 2.1.4. [**4**] *Sejam G e G_0 grupos e suponha que N é um subgrupo normal de G, que é complementado por H e que N_0 é um subgrupo normal de G_0, que é complementado por H_0. Assuma que $N \cong N_0$ e $H \cong H_0$, onde cada um desses isomorfismos é denotado por $()_0$ e suponha que*

$$(n^h)_0 = (n_0)^{h_0},$$

para quaisquer $n \in N$ e $h \in H$. Então, existe um único isomorfismo de G em G_0 que estende os isomorfismos dados $N \to N_0$ e $H \to H_0$.

Relembremos que se um grupo H age sobre um conjunto Ω, então cada $h \in H$ induz uma aplicação $\pi_h : \Omega \to \Omega$ definida por $\alpha \mapsto \alpha \cdot h$, que é uma permutação de Ω. Além disso a aplicação dada por $h \mapsto \pi_h$, é um homomorfismo de H em $Sym(\Omega)$. Assim, uma ação de H sobre Ω é completamente determinada por este homomorfismo de H em $Sym(\Omega)$.

Suponha agora que H age sobre o conjunto K, onde K é também um grupo. Pelas observações do parágrafo anterior $\pi_h : K \to K$ é uma permutação. Sendo K um grupo, é natural requerer que π_h também seja um automorfismo de K. Para isto, como π_h é uma bijeção, é suficiente verificar que é um homomorfismo, ou equivalentemente, que $(xy) \cdot h = (x \cdot h)(y \cdot h)$,

para todos $x, y \in K$. É, portanto, natural intoduzir um novo tipo de ação de grupos.

DEFINIÇÃO 2.1.5. Dados os grupos H e K, dizemos que H age por *automorfismos* sobre K, se H age sobre K, como um conjunto, e, além disso, $(xy) \cdot h = (x \cdot h)(y \cdot h)$, para quaisquer $x, y \in K$ e $h \in H$. Em outras palavras, quando, para cada $h \in H$, a aplicação $\pi_h : K \to K$, dada por $x \mapsto \pi_h(x) = x \cdot h$ é um automorfismo. Note que uma ação por automorfismos de H sobre K determina e é determinado por um homomorfismo $H \to Aut(K)$.

Os exemplos mais naturais de ação por automorfismos são dados quando H é um subgrupo de $\mathrm{Aut}(K)$ e $k \cdot h$ é simplesmente o automorfismos h aplicado ao elemento k, $h(k)$. Outros exemplos de ação por automorfismos ocorrem quando H e K são ambos subgrupos de algum grupo G com $H \leq N_G(K)$ e a ação é dada por conjugação em G. Em particular, a ação por conjugação de um grupo arbitrário G sobre si mesmo é uma ação por automorfismos. Note que é comum usar a notação exponencial para ação por automorfismos, ou seja, ao invês de usar $k \cdot h$ usar k^h, para $k \in K$ e $h \in H$. Esta notação, claro, é natural quando a ação é por conjugação, mas não quando se trata de uma ação por automorfismos, que não for definida por conjugação em um dado grupo. O resultado a seguir afirma que toda ação por automorfismos é essencialmente uma ação por conjugação em um grupo adequado e, portanto, isto justifica a notação exponencial para ação por automorfismos.

TEOREMA 2.1.6. [**4**] *Sejam H e N grupos e suponha que H age por automorfismos sobre N. Então existe um grupo G contendo um subgrupo normal $N_0 \cong N$ que é complementado por um subgrupo $H_0 \cong H$, e tal que, para quaisquer $n \in N$ e $h \in H$, tem-se:*

$$(n^h)_0 = (n_0)^{h_0}.$$

Aqui, $n^h \in N$ é o resultado da ação de h sobre n e $(n_0)^{h_0}$ é o resultado da conjugação de n_0 por h_0 em G.

Observe que do Lema 2.1.4, segue que o grupo G do Teorema 2.1.6 é unicamente determinado por N e H e pela ação por automorfismos de H sobre N. O grupo G é o *produto semi-direto* de N e H com respeito à ação dada. Além disso, ainda pelo Lema 2.1.4, todo grupo G com um subgrupo normal N, que é complementado por um subgrupo H, é isomorfo ao produto

semi-direto de N por H. Assim, sendo válido o Teorema 2.1.6, podemos dizer que todAs (a menos de isomorfismo) as possíveis extensões split foram construídas.

2.2. Ações Coprimas e Pontos Invariantes

Seja A um grupo que age por automorfismos sobre algum grupo G. Por definição A permuta os elementos de G, mas por se tratar de uma ação por automorfismos, A pode permutar outros "objetos teóricos" associados com o grupo G. Por exemplo, A age sobre o conjunto de todas as classes de conjugação de G. É interessante descrever, ou, pelo menos, mostrar a existência de objetos A-invariantes em G. Pois uma vez encontrado um objeto A-invariante, outras ações podem ser estudadas. Por exemplo, se H é um subgrupo A-invariante de G, então A age sobre o conjunto das classes laterais à direita de H em G e sobre o conjunto das classes de conjugação de H.

Claramente, o tipo mais elementar de objeto A-invariante em G é um elemento A-invariante. Estes pontos de G invariantes por todos os elementos de A, formam um subgrupo, denotado por $C_G(A)$. Para ver que esta notação é realmente natural, olhamos A e G em seu produto semi-direto $\Gamma = G \rtimes A$. Sabemos que a ação original de A sobre G é realizada por conjugação em Γ, e então $g^a = g$ se, e somente se, g e a comutam em Γ. Portanto o subgrupo de G dos pontos invariantes por A é exatamente o centralizador de A em G. Isto justifica a notação $C_G(A)$ que é usada para denotar o subgrupo dos pontos fixos, mesmo quando o produto semi-direto não é mencionado. De forma similar, trabalhando no produto semi-direto Γ, vemos que $C_A(G)$ é o conjunto dos elementos de A que agem trivialmente sobre G, ou, em outras palavras, ele é o núcleo da ação de A sobre G.

Definição 2.2.1. Sejam A e G grupos finitos e suponha que A age sobre G. Dizemos que a ação de A sobre G é *coprima* quando as ordens de A e G são relativamente primas, ou seja, se $(|A|, |G|) = 1$.

Note que é mais simples encontrar objetos A-invariantes em G, quando a ação de A sobre G é coprima, como mostra o resultado a seguir.

Lema 2.2.2 (Glauberman). *Seja A um grupo que age por automorfismos sobre um grupo G, onde A e G são grupos finitos e suponha que $(|A|, |G|) = 1$. Assuma também que pelo menos um desses grupos, ou A ou G, é solúvel. Suponha ainda que A e G agem sobre um conjunto não vazio Ω e que a*

ação de G sobre Ω é transitiva. Finalmente assuma a seguinte condição de compatibilidade:

$$(\alpha \cdot g) \cdot a = (\alpha \cdot a) \cdot g^a, \tag{2.2.1}$$

para todo $\alpha \in \Omega$, todo $a \in A$ e todo $g \in G$. Então valem:

(a) *Existe um elemento A-invariante $\alpha \in \Omega$.*
(b) *Se $\alpha, \beta \in \Omega$ são A-invariantes, então existe $c \in C_G(A)$ tal que $\alpha \cdot c = \beta$.*

A solubilidade assumida no Lema 2.2.2 e em outros resultados sobre ação coprima desta seção, não é realmente necessária. De fato, pelo menos um dos dois grupos, ou A ou G tem ordem ímpar, e, portanto, aplicando o Teorema 1.3.8 (Feit-Thompson), temos que ou A ou G é solúvel.

Vamos agora considerar classes de conjugação. Note que, em geral, se K é uma classe de conjugação de G e H é um subgrupo de G, então $K \cap H$ pode ser vazio e se for diferente de vazio, a única coisa que podemos dizer sobre $K \cap H$ é que é a união de classes de H. De fato, se $x \in K \cap H$ e y pertence a uma classe de conjugação de H que contém x, então $y \in K \cap H$. Geralmente, $K \cap H$ não é uma única classe de H. A situação torna-se mais simples quando o subgrupo em questão é o conjunto dos pontos fixos de uma ação coprima.

TEOREMA 2.2.3. *Seja A um grupo que age por automorfismos sobre um grupo G, onde A e G são grupos finitos e escreva $C = C_G(A)$. Suponha que $(|A|, |G|) = 1$ e que pelo menos um deles, ou A ou G é solúvel. Então a aplicação $K \mapsto K \cap C$ define uma bijeção entre o conjunto das classes de conjugação A-invariantes de G e o conjunto de todas as classes de conjugação de C.*

DEMONSTRAÇÃO. Seja K uma classe A-invariante de G. Então A age sobre K e G age transitivamente sobre K por conjugação. Neste caso, a condição de compatibilidade do Lema 2.2.2 é que $(x^g)^a = (x^a)^{g^a}$, para quaisquer $x \in K$, $a \in A$ e $g \in G$ e ela é trivialmente verdadeira. Pelo Lema 2.2.2(a), K possui um elemento A-invariante, e então $K \cap C$ é não vazio. Agora, a afirmação (b) do mesmo lema, assegura que, todos os elementos de $K \cap C$ são conjugados em C e assim, $K \cap C$ é uma classe de conjugação de C.

Portanto a aplicação $K \mapsto K \cap C$ do conjunto das classes de conjugação A-invariantes de G no conjunto de todas as classes de conjugação de C.

Vamos mostrar agora que esta aplicação é uma bijeção. Se K e L são duas classes A-invariantes de G, com $K \cap C = L \cap C$, então como $K \cap C$ é não vazio e está contido em K e em L, segue daí que $K \cap L$ é não vazio e, portanto $K = L$. Assim, vemos que a aplicação é injetiva. Para a sobrejetividade é suficiente mostrar que todo elemento de C pertence a $K \cap C$ para alguma classe A-invariante K de G. Temos que cada elemento $c \in C$ está em uma única classe K de G, e então basta demonstrar que K é A-invariante. Se $a \in A$, então K^a é uma classe de G, e como $c^a = c$, temos que $c \in K \cap K^a$. Logo, as classes K e K^a não são disjuntas e assim, concluímos que $K = K^a$. Isto é, que K é A-invariante, como queríamos. □

Agora consideremos classes laterais. Se A age sobre G e H é um subgrupo A-invariante de G, então A permuta as classes laterias à direita de H em G e também as classes laterais à esquerda de H em G. No caso de uma ação coprima, podemos determinar quais classes laterias à direita e quais classes laterais à esquerda de H em G são A-invariantes.

TEOREMA 2.2.4. *Seja A um grupo que age por automorfismos sobre G, onde A e G são grupos finitos e escreva $C = C_G(A)$. Seja H um subgrupo A-invariante de G e suponha que $(|A|, |H|) = 1$ e que pelo menos um deles, ou A ou H, é solúvel. Então as classes laterais à esquerda e as classes laterais à direita A-invariantes de H em G, são exatamente as classes laterais de H que contem elementos de C.*

DEMONSTRAÇÃO. Se $a \in A$ e $c \in C$, então $(Hc)^a = H^a c^a = Hc$ e, analogamente, $(cH)^a = c^a H^a = cH$. Logo, as classes laterias de H que contém elementos de C são A-invariantes. Suponha agora que X é uma classe lateral à esquerda A-invariante de H em G. Então H age transitivamente por multiplicação à direita sobre X e, claro, A age sobre X e A age por automorfismos sobre H. A condição de compatibilidade do Lema 2.2.2 neste caso é $(xh)^a = x^a h^a$, para quaisquer $x \in X$, $h \in H$ e $a \in A$. Note que isto vale porque a ação de A sobre G é uma ação por automorfismos. Portanto, pelo item (a) do Lema 2.2.2, concluímos que X contém um elemento de C, como queríamos mostrar.

Para mostrar o resultado no caso das classes laterais à direita, é sufuciente observar o seguinte. Toda classe lateral à direita de H em G tem a forma $X^{-1} = \{x^{-1} \mid x \in X\}$ para alguma classe lateral à esquerda X de H em G. Como X é A-invariante se, e somente se, X^{-1} o é, o resultado para classes

laterais à direita é uma consequência do resultado para as classes laterais à esquerda. □

Ações sobre classes laterais são especialmente interessantes para subgrupos normais. Seja A um grupo que age por automorfismos sobre G e suponha que N é um subgrupo normal A-invariante de G . Como as classes laterais de N em G são os elementos do grupo quociente G/N e como estes elementos são permutados por A, vemos que A age sobre G/N e, além disso, esta ação é por automorfismos. De fato, temos que

$$(NxNy)^a = (Nxy)^a = Nx^a y^a = Nx^a Ny^a = (Nx)^a (Ny)^a.$$

As classes laterias A-invariantes de N em G, são, protanto, os elementos do subgrupo dos pontos fixos $C_{G/N}(A)$. Vamos usar a notação $\overline{G} = G/N$ no grupo quociente e reformulamos o Teorema 2.2.4 neste caso particular.

Corolário 2.2.5. *Seja A um grupo que age por automorfismos sobre um grupo G, onde A e G são grupos finitos. Seja N um subgrupo normal A-invariante de G. Assuma, que $(|A|, |N|) = 1$ e que pelo menos um deles, ou A ou N é solúvel. Escrevendo $\overline{G} = G/N$, temos que*

$$C_{\overline{G}}(A) = \overline{C_G(A)}.$$

Demonstração. Os elementos de $\overline{G}$ invariantes por A são exatamente as classes laterais A-invariantes de N. Pelo Teorema 2.2.4, essas classes são justamente as classes laterais de N que contêm elementos de $C_G(A)$. Por outro lado, as classes laterais de N que possuem elementos de $C_G(A)$ formam a imagem de $C_G(A)$ em $\overline{G}$, isto é, $\overline{C_G(A)}$. □

Notemos que o resultado do corolário anterior pode ser resumido dizendo que, em ações coprimas "pontos fixos provêm de pontos fixos". O exemplo seguinte mostra a importância de ser a ação coprima, ou seja, podemos mostrar que se a ação não é coprima, pontos fixos em $\overline{G}$ podem não ser provenientes de pontos fixos de G.

Exemplo 2.2.6 (Example 2.10 **[6]**). Consideremos o grupo dos quatérnios $Q_8 = \langle u, v \mid u^4 = v^4 = 1; u^2 = v^2; u^v = u^3 \rangle$ e a aplicação φ definida levando $u \mapsto v$ e $v \mapsto u$. Claro que esta aplicação se estende a um automorfismo de Q_8. Observemos que o subgrupo de Q_8 gerado por u^2, $\langle u^2 \rangle$, é um subgrupo φ-invariante normal de Q_8. Usando a notação referida acima para grupo quociente, temos que $\overline{Q_8} = Q_8/\langle u^2 \rangle$ é o produto direto $\langle \overline{u} \rangle \times \langle \overline{v} \rangle$ de dois grupos cíclicos de ordem 2. Notemos que, o automorfismo induzido por φ,

ou seja, o automorfismo $\overline{\varphi}$ definido por $\overline{u} \mapsto \overline{v}$ e $\overline{v} \mapsto \overline{u}$, fixa o elemento $\overline{u}\,\overline{v}$, mas este ponto não é a imagem de nenhum ponto fixo de φ, uma vez que $C_{Q_8}(\varphi) = \langle u^2 \rangle$. E, claro, neste caso não temos uma ação coprima, uma vez que Q_8 tem ordem 8 e φ tem ordem potência de 2.

Se um grupo A age por automorfismos sobre um grupo G, então A e G podem ser vistos como subgrupos do produto semi-direto $\Gamma = G \rtimes A$ e assim podemos calcular o comutador $[G, A]$ como subgrupo de Γ. Mas G é um subgrupo normal de Γ, e, então $[G, A]$ é um subgrupo de G. Portanto, é possível, e ás vezes conveniente, pensar $[G, A]$ como sendo calculado inteiramente dentro de G e por isso conhecer o produto semi-direto Γ é irrelevante. Observemos que, dados $g \in G$ e $a \in A$, então $[g, a] = g^{-1}a^{-1}ga = g^{-1}g^a$. Assim, podemos ver g^a como o resultado da conjugação de g por a em Γ ou ainda como o resultado que obtemos aplicando a ao elemento g na ação original de A sobre G. Portanto, o comutador $[G, A]$ é o subgrupo $\langle g^{-1}g^a \mid g \in G, a \in A \rangle$ e podemos cálcula-lo sem necessariamente conhecer o produto semi-direto Γ.

Observação 2.2.7. Geralmente, se H é um subgrupo arbitrário A-invariante de G, temos uma ação natural de A sobre H. Neste caso, dizemos que H admite ação de A. Observe também que $[G, A]$ é um subgrupo A-invariante de G. De fato, seja $y \in [G, A]$. Assim, y é da forma:

$$y = [g_1, a_1]^{\alpha_1}[g_2, a_2]^{\alpha_2} \dots [g_n, a_n]^{\alpha_n},$$

onde $\alpha_i \in \mathbb{Z}, \forall\ 1 \leq i \leq n$ e $g_i \in G, a_i \in A, \forall\ 1 \leq i \leq n$. Daí, dado $a \in A$, obtemos

$$\begin{aligned} y^a &= ([g_1, a_1]^{\alpha_1}[g_2, a_2]^{\alpha_2} \cdots [g_n, a_n]^{\alpha_n})^a \\ &= [g_1^a, a_1^a]^{\alpha_1}[g_2^a, a_2^a]^{\alpha_2} \cdots [g_n^a, a_n^a]^{\alpha_n} \\ &= [\widetilde{g_1}, \widetilde{a_1}]^{\alpha_1}[\widetilde{g_2}, \widetilde{a_2}]^{\alpha_2} \cdots [\widetilde{g_n}, \widetilde{a_n}]^{\alpha_n}, \end{aligned}$$

para alguns $\widetilde{g_i}$ em G, para todo $i = 1, \dots, n$ e $\widetilde{a_i}$ em A, para todo $i = 1, \dots, n$. Segue daí que, $y^a \in [G, A]$. Como $y \in [G, A]$ e $a \in A$ foram tomados arbitrariamente, concluímos que $[G, A]$ é A-invariante.

Assim, pela observação anterior, temos que $[G, A]$ admite ação de A, e daí podemos calcular $[G, A, A]$. Note que $[G, A, A]$ é subgrupo normal de $[G, A]$, mas não necessariamente de G. Com ideia similiar, vemos que $[G, A, A]$ também admite ação de A, e assim, podemos calcular $[G, A, A, A]$, e podemos continuar com este processo.

Relembremos que se A age por automorfismos sobre G e H é um subgrupo A-invariante de G, então A permuta o conjunto das classes laterais à esquerda (e à direita) de H em G. Em particular, se H é subgrupo normal de G, então A age por automorfismos sobre o grupo quociente G/H. Esta ação é chamada *ação induzida* de A sobre G/H.

LEMA 2.2.8. *Suponha que A age por automorfismos sobre G, onde A e G são grupos finitos. Seja N um subgrupo A-invariante normal de G. Se $g \in G$ e $a \in A$ são elementos arbitrários, então $\overline{[G,A]} = [\overline{G}, A]$.*

DEMONSTRAÇÃO. Dados $g \in G$ e $a \in A$, temos $(gN)^a = g^a N$. Se escrevemos $\overline{G} = G/N$, então temos que $(\overline{g})^a = \overline{g^a}$. Daí,

$$\overline{[g,a]} = \overline{g^{-1}g^a} = (\overline{g^{-1}})\overline{g^a} = (\overline{g})^{-1}(\overline{g})^a = [\overline{g}, a].$$

Portanto, $\overline{[G,A]} = [\overline{G}, A]$, como queríamos demonstrar. □

O próximo resultado é uma caracterização do grupo $[G, A]$.

LEMA 2.2.9. *Suponha que A age por automorfismos sobre G, onde A e G são grupos finitos. Então $[G, A]$ é o único menor subgrupo normal A-invariante de G tal que a ação induzida de A sobre o grupo quociente é trivial.*

DEMONSTRAÇÃO. Suponha que N é um subgrupo A-invariante normal de G e escreva $\overline{G} = G/N$. Então, A age trivialmente sobre G/N se, e somente se, $[\overline{G}, A] = 1$. Logo, pelo Lema 2.2.8, isto é equivalente a $\overline{[G,A]} = 1$, ou em outras palavras que $[G, A] \leqslant N$. O resultado segue. □

COROLÁRIO 2.2.10. *Suponha que A age por automorfismos sobre G, onde A e G são grupos finitos. Considere $H \leqslant G$ um subgrupo arbitrário de G. São equivalentes:*

(i) *Toda classe lateral à direita de H em G é um conjunto A-invariante.*
(ii) *Toda classe lateral à esquerda de H em G é um conjunto A-invariante.*
(iii) *O comutador $[G, A]$ é subgrupo de H.*

Em particular, $[G, A]$ é o único menor subgrupo de G tal que todas as suas classes laterais à direita (e à esquerda) são A-invariantes.

DEMONSTRAÇÃO. Primeiramente observe que se X é um subconjunto de G e escrevemos $X^{-1} = \{x^{-1} \mid x \in X\}$, então a aplicação $X \to X^{-1}$ leva as classes laterais à direita de H em G nas classes laterais à esquerda de H em G e vice versa. Segue daí que um automorfismo de G fixa todas as

classes laterais à direita de H em G se, e somente se, ele fixa todas as classes laterais à esquerda de H em G. Portanto (i) e (ii) são equivalentes.

Agora suponha (ii), assim, toda classe lateral à esquerda de H em G é A-invariante. Então para cada $g \in G$ e todo $a \in A$, temos que $g^a \in (gH)^a = gH$. Portanto, $[g, a] = g^{-1}g^a \in H$ e (iii) é verdadeiro.

Finalmente, assuma (iii) e então $[G, A]$ é um subgrupo de H. Cada classe lateral à direita de H em G é a união das classes laterais à direita de $[G, A]$ em G. Mas todas as classes de $[G, A]$ em G são A-invariantes, pelo Lema 2.2.9 e, então a união dessas classes é também A-invariante e assim (i) é verdadeiro. □

Suponha que um grupo A age por automorfismos sobre um grupo G e relembremos que o núcleo desta ação é o subgrupo normal de A, $B = \{a \in A \mid g^a = g, \text{para todo} \, g \in G\}$. Este é o maior subgrupo de A tal que $[G, B] = 1$. Além disso, como B é normal em A, vemos que a ação natural de $\overline{A} = A/B$ sobre G é dada por $g^{\overline{a}} = g^a$, para qualquer $g \in G$ e todo $a \in A$. Disto segue que se H é um subgrupo de G, então H é A-invariante se, e somente se, é $\overline{A}$-invariante. Portanto, em outras palavras, podemos dizer que H admite ação de A se, e somente se, admite ação de $\overline{A}$. Além disso, temos que $[g, \overline{a}] = g^{-1}(\overline{a})^{-1}g\overline{a} = g^{-1}g^{\overline{a}} = g^{-1}g^a = [g, a]$, para quaisquer $g \in G$ e $a \in A$. Assim se H admite ação de A e de $\overline{A}$, segue que $[H, A] = [H, \overline{A}]$.

Continuamos nosso estudo de comutadores que surgem quando A age por automorfismos sobre G, porém agora vamos considerar especificamente ações coprimas, ou seja, quando $(|A|, |G|) = 1$.

O resutado seguinte depende fundamentalmente do Lema 2.2.2 e, por isso em seu enunciado tem a hipótese de solubilidade. Na verdade essa hipótese não é realmente necessária se aplicarmos o Teorema 1.3.8 (Feit-Thompson).

LEMA 2.2.11. *Seja A um grupo que age por automorfismos sobre um grupo G, onde A e G são grupos finitos e $(|A|, |G|) = 1$. Assuma que pelo menos um destes grupos, ou A ou G, é solúvel. Então $G = C_G(A)[G, A]$.*

DEMONSTRAÇÃO. Escreva $\overline{G} = G/[G, A]$. Pelo Corolário 2.2.5 temos que $C_{\overline{G}}(A) = \overline{C_G(A)}$. Como A age trivialmente sobre $G/[G, A]$, então o lado esquerdo desta equação é todo o grupo $\overline{G}$. Assim,

$$\overline{C_G(A)[G, A]} = \overline{C_G(A)} = \overline{G}.$$

Pelo teorema da correspondência ([**3**]), segue que $[G, A]C_G(A) = G$. □

Observamos que cada classe de $[G, A]$ em G é A-invariante e, então pelo Lema 2.2.2, temos que cada classe lateral contém um elemento invariante por A. O resultado a seguir será bastante usado.

LEMA 2.2.12. *Seja A um grupo que age por automorfismos sobre um grupo G, onde A e G são grupos finitos e assuma que $(|A|, |G|) = 1$. Então $[G, A, A] = [G, A]$.*

DEMONSTRAÇÃO. Claro que $[G, A, A] \leq [G, A]$, logo, é suficiente demonstrar a inclusão contrária. Para isto vamos mostrar que $[g, a] \in [G, A, A]$ para todo $g \in G$ e todo $a \in A$. Assim, como $[G, A]$ é gerado por comutadores deste tipo, então concluímos que $[G, A] \leq [G, A, A]$.
Suponha primeiramente que A é solúvel. Pelo lema 2.2.11 obtemos que $G = C_G(A)[G, A]$ e, então se $g \in G$, podemos escrever $g = cx$, onde $c \in C_G(A)$ e $x \in [G, A]$. Agora seja $a \in A$ um elemento arbitrário e observemos que $[c, a] = 1$. De fato, $[c, a] = c^{-1}c^a = c^{-1}c = 1$. Daí, segue que

$$[g, a] = [cx, a] = [c, a]^x[x, a] = [x, a] \in [G, A, A].$$

Logo, $[g, a] \in [G, A, A]$, como queríamos demonstrar. Isto mostra que o resultado é verdadeiro quando A é solúvel. Consideremos agora o caso geral. Sejam $g \in G$ e $a \in A$ elementos arbitrários. Temos

$$[g, a] \in [G, \langle a \rangle] = [G, \langle a \rangle, \langle a \rangle] \leq [G, A, A],$$

pois o grupo cíclico $\langle a \rangle$ é solúvel. E isto completa a demonstração do teorema. □

Retornemos à situação considerada no Lema 2.2.11 onde A age por automorfismos sobre G e a ordem de A e G são coprimas, então sabemos que $G = C_G(A)[G, A]$. No caso de ser G um grupo abeliano, temos ainda as informações à seguir.

TEOREMA 2.2.13. *Seja A um grupo que age por automorfismos sobre um grupo abeliano G, assuma que A e G são finitos e que $(|A|, |G|) = 1$. Então $G = C_G(A) \times [G, A]$.*

DEMONSTRAÇÃO. Como G é abeliano, temos que todos os seus subgrupos são normais. Em particular, $C_G(A)$ e $[G, A]$ são normais e assim, para demonstrar que G é o produto direto de $C_G(A)$ e $[G, A]$ é suficiente demonstrar que $G = C_G(A)[G, A]$ e $C_G(A) \cap [G, A] = 1$. Sendo G abeliano, então G é solúvel, assim, podemos aplicar o Lema 2.2.11 para concluir que

$G = C_G(A)[G, A]$. Agora, resta-nos mostrar a segunda afirmação. Considere a aplicação $\theta : G \to G$ definida por

$$\theta(g) = \prod_{b \in A} g^b.$$

Note que, como G é abeliano, a ordem dos fatores neste produto é irrelevante e, então θ está bem definida. Além disso, se $x, y \in G$, então $(xy)^b = x^b y^b$, para todo $b \in A$. Assim, usando, novamente, o fato de ser G um grupo abeliano, é fácil ver que $\theta(xy) = \theta(x)\theta(y)$, logo, θ é um homomorfismo.

Agora se $g \in C_G(A)$, então $g^b = g$, para todo $b \in A$ e daí $\theta(g) = \prod_{b \in A} g^b = g^{|A|}$. Além disso, como $|A|$ e $|G|$ são coprimas, temos que se $g \neq 1$, então $g^{|A|} \neq 1$, e assim, $C_G(A) \cap \mathrm{Ker}(\theta) = 1$. Portanto, é suficiente mostrar que $[G, A] \leq \mathrm{Ker}(\theta)$. Como $[G, A]$ é gerado pelos comutadores da forma $[g, a]$, onde $g \in G$ e $a \in A$, para demonstrar que $[G, A] \leq \mathrm{Ker}(\theta)$, é suficiente demonstrar que cada um destes comutadores pertence a $\mathrm{Ker}(\theta)$. Sejam $g \in G$ e $a \in A$, elementos tomados arbitrariamente, então temos que

$$\theta(g^a) = \prod_{b \in A} (g^a)^b = \prod_{b \in A} g^{ab} = \theta(g),$$

onde a terceira igualdade segue porque ab percorre A quando b percorre A. Segue daí que

$$\theta([g, a]) = \theta(g^{-1}g^a) = \theta(g^{-1})\theta(g^a) = \theta(g)^{-1}\theta(g) = 1.$$

Logo, $[g, a] \in \mathrm{Ker}(\theta)$ e isto conclui a demonstração. □

O conceito de p-grupo é amplamente utilizado neste trabalho, relembremos agora um outro conceito, também relacionado a um primo p dado.

Definição 2.2.14. Sejam p um primo e G um grupo finito. Dizemos que um elemento $x \in G$ é um p'-elemento quando p não divide a ordem de x e dizemos que G é um p'-grupo quando p não divide a ordem de G.

Observemos que se G é um p'-grupo, então, pelo Teorema 1.1.16, todo elemento x em G é um p'-elemento.

Como aplicação do Teorema 2.2.13 obtemos o corolário a seguir.

Corolário 2.2.15. *Seja K um grupo que age por automorfismos sobre um p-grupo abeliano P e assuma que K é um p'-grupo. Se K fixa todos os elementos de ordem p em P, então K age trivialmente sobre P.*

Demonstração. Pelo Teorema 2.2.13, temos que $P = C_P(K) \times [P, K]$. Temos também, por hipótese, que K fixa todos os elemenots de ordem p

em P, o que é equivalente a dizer que $C_P(K)$ contém todos os elementos de ordem p em P. Como $C_P(K) \cap [P, K] = 1$, segue que $[P, K]$ não contém elementos de ordem p em P. Mas, pelo Teorema 1.1.16, $[P, K]$ é um p-grupo e como todo p-grupo não trivial contém elementos de ordem p, concluimos que $[P, K] = 1$. Portanto, K age trivialmente sobre P. □

CAPíTULO 3

p'-automorfismos em p-grupos

No final do Capítulo 2 mostramos que se um p'-grupo finito K age por automorfismos sobre um p-grupo abeliano P e fixa todos os elementos de ordem p em P, então K age trivialmente sobre P. Surpreendentemente, se supormos que o primo p é maior que 2, veremos que a hipótese de que P é abeliano não é necessária. Se $p = 2$ não podemos concLuir, nestas condições, que a ação é trivial, como veremos no Exemplo 3.1.3, porém se adicionalmente supormos outras condições, como K fixando todos os elementos de ordem 4 ou mesmo, fixando apenas todos os elementos reais de ordem 4, podemos afirmar que a ação de K sobre P é trivial.

3.1. Caso $p > 2$

No primeiro resultado deste capítulo vemos como a hipótese de ser P um grupo abeliano do Corolário 2.2.15 pode ser suspensa caso consideremos o primo p maior que 2.

Teorema 3.1.1. [**4**] *Seja K um grupo que age por automorfismos sobre um p-grupo finito P, com $p > 2$, e K é um p'-grupo finito. Se K fixa todos os elementos de ordem p em P, então K age trivialmente sobre P.*

Note que a ideia da demonstração do Teorema 3.1.1 é bastante simples. Vamos mostrar que se P é um grupo de ordem minimal para o qual o teorema não vale, então podemos encontrar um grupo abeliano de mesma ordem para o qual o teorema também não vale, e isto contradiz o Corolário 2.2.15. É possível demonstrar que um contra-exemplo minimal teria classe de nilpotência no máximo 2 (e isto não exige que $p > 2$), mas passar de um contra-exemplo de classe de nilpotência no máximo 2 a um abeliano exige uma nova ideia. Esta ideia é conhecida como *"truco de Baer"*, e é descrito no lema a seguir.

Lema 3.1.2 (Truco de Baer). *Seja G um grupo finito nilpotente de ordem ímpar e classe de nilpotência no máximo 2. Então existe uma operação adição $x + y$ definida para elementos $x, y \in G$ tal que $(G, +)$ é um grupo abeliano com respeito a esta operação. Além disso, valem as seguintes afirmações.*

(i) *Se $xy = yx$, para quaisquer $x, y \in G$, então $x + y = xy$.*

(ii) *Para cada $x \in G$, sua ordem aditiva é igual à sua ordem multiplicativa.*

(iii) *Todo automorfismo de G é também um automorfismo do grupo aditivo $(G, +)$.*

Antes de apresentarmos a demonstração do Lema 3.1.2, precisamos introduzir algumas notações. Se m é um inteiro e G é um grupo de ordem relativamente prima com m, então a aplicação $x \mapsto x^m$, tem uma inversa, à saber, a aplicação $x \mapsto x^n$, onde n é escolhido de modo que $mn \equiv 1 \bmod |G|$. Assim, dado $x \in G$, existe um único elemento $y \in G$ tal que $y^m = x$ e, de fato, y é uma potência de x.

No caso em que $|G|$ é ímpar e $m = 2$, escrevemos $y = \sqrt{x}$ para denotar o único elemento $y \in G$, tal que $y^2 = x$. Obeserve que se H é um subgrupo de G, então dado $h \in H$ existe um único $y \in G$ tal que $y^2 = h$, ou seja, $y = \sqrt{h}$. Agora como y é uma potência de h, em particular $\sqrt{h} \in H$, para todo $h \in H$. Além disso, observemos também que $\sqrt{x^{-1}} = (\sqrt{x})^{-1}$, para qualquer $x \in G$. Agora se x e y comutam, segue também que $\sqrt{xy} = \sqrt{x}\sqrt{y}$.

Demosntração do Lema 3.1.2. Dados quaisquer $x, y \in G$, defina $+ : G \times G \to G$, pondo

$$x + y = xy\sqrt{[y, x]}.$$

Observemos, primeiramente, que a operação "+" é comutativa. Para isto, precisamos verificar que $x + y = y + x$, para quaisquer $x, y \in G$, ou equivalentemente que,

$$yx\sqrt{[x, y]} = xy\sqrt{[y, x]}.$$

Mas, isto é equivalente a:

$$y^{-1}x^{-1}yx = \sqrt{[y, x]}\big(\sqrt{[x, y]}\big)^{-1}.$$

Como sabemos que $\big(\sqrt{[x, y]}\big)^{-1} = \sqrt{[x, y]^{-1}} = \sqrt{[y, x]}$, então temos que mostrar que,

$$[y, x] = (\sqrt{[y, x]})^2.$$

Agora a última identidade é trivial e, portanto, a comutatividade de "+" está verificada. Note que, se x e y comutam, então, $[y, x] = 1$ e como $\sqrt{1} = 1$, vê-se facilmente que $x + y = xy\sqrt{[y, x]} = xy$. E isto mostra (i). Em particular, como 1 e x comutam, segue que $1 + x = 1x = x$ para todo $x \in G$. Portanto 1 é o elemento neutro da adição. Por outro lado, dado $x \in G$, sabemos que x e x^{-1} comutam, e assim $x + x^{-1} = xx^{-1} = 1$, ou seja, x^{-1} é o inverso

aditivo de x em G. Vamos demonstrar agora que a adição é associativa. Dados $x, y, z \in G$, arbitrários, temos

$$x + (y + z) = x + yz\sqrt{[z, y]} = xyz\sqrt{[z, y]}\sqrt{[yz\sqrt{[z, y]}, x]}. \tag{3.1.1}$$

Por hipótese sabemos que G tem classe de nilpotência no máximo 2 e, portanto $G' \leq Z(G)$, ou seja, todos os comutadores em G são centrais. Disto segue que a aplicação $[\cdot, x]$ é um homomorfismo. De fato, dados $a, b, x \in G$, temos $[ab, x] = [a, x]^b[b, x] = [a, x][b, x]$, pois $G' \leq Z(G)$. Assim, obtemos:

$$[yz\sqrt{[z, y]}, x] = [y, x][z, x][\sqrt{[z, y]}, x],$$

mas como $[z, y] \in Z(G)$, temos também que $\sqrt{[z, y]} \in Z(G)$, logo o fator $[\sqrt{[z, y]}, x]$ é trivial. Daí, a equação (3.1.1) fica:

$$x + (y + z) = xyz\sqrt{[z, y]}\sqrt{[y, x][z, x]} = xyz\sqrt{[z, y][y, x][z, x]}, \tag{3.1.2}$$

onde a segunda igualdade segue do fato de $[z, y]$ comutar com $[y, x][z, x]$.

Por outro lado,

$$(x + y) + z = xy\sqrt{[y, x]} + z = xy\sqrt{[y, x]}z\sqrt{[z, xy\sqrt{[y, x]}]}. \tag{3.1.3}$$

Assim como vimos que $[\cdot, x]$ é um homomorfismo e de modo análogo, é possível ver que $[z, \cdot]$ é um homomorfismo. Assim a expressão em (3.1.3), torna-se

$$(x + y) + z = xyz\sqrt{[y, x][z, x][z, y]}. \tag{3.1.4}$$

Como os comutadores comutam, de (3.1.2) e (3.1.4), segue que

$$x + (y + z) = (x + y) + z.$$

Portanto, $(G, +)$, é um grupo abeliano.

Agora, para o grupo abeliano $(G, +)$ escrevemos nx para denotar a soma de n cópias de x, quando n é um inteiro positivo e $x \in G$. Vamos demonstrar, por indução sobre n, que $nx = x^n$. Óbvio que, para $n = 1$, o resultado é válido. Para $n > 1$, temos

$$nx = x + (n - 1)x = x + x^{n-1} = xx^{n-1} = x^n,$$

onde a segunda igualdade segue da hipótese de indução e a terceira, do item (i), já que x e x^{n-1} comutam em G. Segue portanto que $nx = 1$ se, e somente se, $x^n = 1$. Mas, já vimos que 1 é o elemento neutro aditivo (além de ser o elemento identidade da multiplicação), portanto, para cada $x \in G$ sua ordem aditiva é igual à sua ordem multiplicativa. E isto demonstra (ii).

Finalmente, a adição em G é unicamente determinada pela multiplicação, e então qualquer permutação de elementos de G que preserva multiplicação também irá preservar adição. Assim temos que (iii) vale e isto completa a demosntração. □

Agora podemos demonstrar o Teorema 3.1.1, ou seja, mostrar que se um p'-grupo finito K age por automorfismos sobre um p-grupo finito P e se K fixa todos os elementos de ordem p em P, então K age trivialmente sobre P.

Demosntração do Teorema 3.1.1. Suponha P não trivial, uma vez que neste caso não há nada a fazer. Vamos demonstrar o resultado por contradição. Tome P como o grupo de menor ordem possível dentre os quais o teorema não é válido. Assim, se H é um subgrupo próprio de P que admite ação de K, como os elementos de ordem p em H são invariantes por K, segue da minimalidade de P, que K age trivialmente sobre H, isto é, $[H, K] = 1$, isto é, $C_H(K) = H$.

Em particular, notamos que se $[P, K] < P$, como pela Observação 2.2.7, o subgrupo $[P, K]$ é K-invariante, então $[P, K]$ admite ação de K. Logo, $[[P, K], K] = 1$. Além disso do Lema 2.2.12, segue que $[P, K, K] = [P, K]$, donde $[P, K] = 1$, o que contradiz a hipótese de que $C_P(K) \neq P$, logo temos que $[P, K] = P$.

Consideremos agora o subgrupo derivado P' de P. Sabemos que $P' = [P, P]$, logo ele é K-invariante, pois P o é. Assim, P' admite ação de K. Além disso, P é um p-grupo finito, logo, por 1.3.6, temos que P é solúvel não abeliano, daí, P' é subgrupo próprio de P, logo segue que $[P', K] = 1$, donde obtemos $[P', K, P] = 1$. Por outro lado, como P' é normal em P, então pelo Lema 1.2.9, obtemos que $[P, P'] \leq P'$, logo, $[P, P', K] \leq [P', K] = 1$. E, portanto, $[P, P', K] = 1$. Assim, pelo Lema 1.2.11, segue que $[K, P, P'] = 1$. Pela Proposição 1.2.5 sabemos que $[K, P] = [P, K]$, logo $[K, P] = P$. Daí, $[P, P'] = 1$ e P' é central em P, logo, a classe de nilpotência de P é no máximo 2. Portanto podemos aplicar o Lema 3.1.2 para construir o grupo aditivo abeliano $(P, +)$.

Tome agora, $a \in K$ arbitrariamente. Como K age por automorfismos sobre P, vimos no Capítulo 2 que K pode ser visto como um subgrupo de $\mathrm{Aut}(P)$. Assim, a induz um automorfismo de P. Logo, pelo Lema 3.1.2(iii), obtemos que a também é um automorfismo do grupo aditivo abeliano $(P, +)$. Segue então que K age por automorfismos sobre $(P, +)$. Ainda Pelo Lema 3.1.2(ii), sabemos que os elementos de ordem p em $(P, +)$ são exatamente os elementos de ordem p em P, e, por hipótese, estes são invariantes por K.

Portanto, pelo Corolário 2.2.15, segue que K age trivialmente sobre $(P, +)$, logo, a ação de K sobre P também é trivial. Chegamos a uma contradição e isto completa a demonstração. □

O exemplo a seguir mostra que se $p = 2$, a conclusão do Teorema 3.1.1 pode não ser verdadeira.

Exemplo 3.1.3. Consideremos o grupo dos quatérnios

$$Q_8 = \langle i, j, k \mid i^2 = j^2 = k^2 = ijk; i^4 = j^4 = k^4 = 1 \rangle.$$

Lembramos algumas regras de multiplicação úteis que valem neste grupo:

$$ij = k, ji = -k,\ jk = i,\ kj = -i,\ ki = j \text{ e } ik = -j.$$

O único elemento de ordem 2 em Q_8 é ijk. Agora, consideremos o grupo cíclico $K = \langle a \mid a^3 = 1 \rangle$ gerado por a e vamos estabelecer uma ação por automorfismos de K sobre Q_8 do seguinte modo:

$$i^a = j,\ j^a = k,\ k^a = i.$$

Observemos que K fixa todos os elementos de ordem 2 em Q_8. De fato, temos que $(ijk)^a = i^a j^a k^a = jki = j^2 = ijk$, por outro lado, $(ijk)^{a^2} = i^{a^2} j^{a^2} k^{a^2} = kij = k^2 = ijk$ e claramente, $(ijk)^1 = ijk$. Mas, como é fácil de verificar esta ação não é trivial, já que, por exemplo, $i^a = j$.

Assim, temos um grupo de ordem ímpar agindo por automorfismos sobre um 2-grupo finito não abeliano e fixando todos os elementos de ordem 2 neste grupo, mas a ação não é trivial.

3.2. Caso $p = 2$

Agora a questão gira em torno de saber o que ocorre quando o primo p é igual a 2. O primeiro resultado neste sentido nos diz que se K fixa todos os elementos de ordem 2 e todos os elementos de ordem 4 em um 2-grupo P e K é um grupo de ordem ímpar que age por automorfismos sobre P, então K age trivialmente sobre P. Este resultado é consequência do lema a seguir.

Lema 3.2.1 (Satz IV.5.12 [**2**]). *Sejam P um p-grupo e α um automorfismo de P cuja ordem é coprima com p. Se $p = 2$ e α fixa todos os elementos de ordem 2 e 4 em P, então $\alpha = 1$.*

Neste ponto precisamos estabelecer dois conceitos que serão necessários nas próximas considerações.

DEFINIÇÃO 3.2.2. Sejam G um grupo e x um elemento de G. Dizemos que:

(a) O elemento x é real se existe um elemento $g \in G$ tal que $x^g = x^{-1}$.
(b) O elemento x é racional se sempre que $\langle x \rangle = \langle x^r \rangle$, então x e x^r são conjugados em G.

Em 2010, M. Isaacs e G. Navarro mostraram em [**5**], que não é necessário assumir que todos os elementos de ordem 4 em P sejam invariantes por K, basta apenas que os elementos reais de ordem 4 o sejam. Neste artigo os autores demonstram o resultado usando recursos da teoria de caracteres. Porém no ano seguinte, Z. Marciniak em [**7**], apresenta uma demonstração do mesmo resultado sem utilizar caracteres. Optamos por apresentar aqui a demonstração devida a Marciniak.

TEOREMA 3.2.3. *Seja K um grupo de ordem ímpar que age por automorfismos sobre um 2-grupo finito P. Suponha ainda que K fixa todos os elementos de ordem 2 em P e todos os elementos reais de ordem 4 em P. Então K age trivialmente sobre P.*

O Teorema 3.2.3 é também uma generalização do seguinte resultado.

TEOREMA 3.2.4 (Theorem 2.1 [**8**]). *Suponha que um grupo de ordem ímpar K age por automorfismos sobre um 2-grupo P. Se K fixa todos os elementos racionais de P, então K age trivialmente sobre P.*

Notemos que um elemento de ordem 2 é automaticamente racional e um elemento de ordem 4 é racional se, e somente se, ele é um elemento real. De fato, se $x \in G$ tem ordem 2, logo $\langle x \rangle = \{1, x\}$. Assim temos somente que $\langle x \rangle = \langle x^{-1} \rangle$ e portanto, x é racional, já que $x = x^{-1}$. Agora seja $o(x) = 4$. Se x é real, então existe $g \in G$ tal que $x^g = x^{-1}$. Como x possui ordem 4, segue que $\langle x \rangle = \langle x^3 = \langle x^{-1} \rangle$ e notamos que $x^3 = x^{-1}$. Disto e do fato de x ser real obtemos que x e x^3 são conjugados em G. Concluímos, portanto, que x é racional. Finalmente, se x é racional, temos que se $\langle x \rangle = \langle x^s \rangle$, então x e x^s são conjugados em G, ou seja, existe $g \in G$ tal que $x^g = x^s$. Como $o(x) = 4$, então $s = 3$ ou $s = -1$. Sendo $x^3 = x^{-1}$, em particular temos que x é conjugado com seu inverso e portanto, x é real.

Observemos que a hipótese no Teorema 3.2.3 de que K fixa todos os elementos de ordem 2 e todos os elementos reais de ordem 4 pode então ser vista como a "interseção" de duas condições suficientes já vistas para que a ação de K sobre P seja trivial: a primeira destas condições é aquela

apresentada no Lema 3.2.1, ou seja, que K fixa todos os elementos de ordem no máximo 4 em P; a segunda condição é justamente aquela do Teorema 3.2.4.

Demosntração do Teorema 3.2.3. Queremos demonstrar que K age trivialmente sobre P, ou equivalentemente que $[P, K] = 1$.

Como $|K|$ é finita, podemos decompor a ordem de K em:

$$m = q_1^{\alpha_1} q_2^{\alpha_2} \dots q_r^{\alpha_r},$$

onde q_i são primos distintos, para $i = 1, \dots, r$ e α_i são inteiros. Além disso, como $|K|$ é ímpar, todos os primos q_i são primos ímpares. Sabemos que dado um primo q_i que divide $|K|$, existe $k \in K$ tal que $o(k) = q_i$. Observamos que podemos supor que a ação de K sobre P é fiel, e então, sem perda de generalidade, podemos reduzir nosso problema a um caso mais simples, assumindo que o grupo K é cíclio de ordem prima. Seja, portanto, $|K| = q$, onde q é um primo ímpar e considere $K = \langle x \rangle$.

A demonstração será feita por contradição. Suponha, por absurdo, que K não age trivialmente sobre P e tome, então, P como o grupo de ordem minimal dentre os grupos para os quais o teorema não é válido, ou seja, temos que $[P, K] > 1$.

Se Q é um subgrupo próprio de P, então observamos que o conjunto dos elementos de ordem 2 e dos elementos reais de ordem 4 de Q está contido no conjunto dos elementos de ordem 2 e dos elementos reais de ordem 4 de P. Se, além disso, Q é K-invariante, então pela minimalidade de P segue que $[Q, K] = 1$.

Vamos, primeiramente, considerar o subgrupo $Q = [P, K]$ de P. Já vimos na Observação 2.2.7 que $[P, K]$ é K-invariante. Agora, se $[P, K]$, é subgrupo próprio de P, então pela minimalidade de P, segue que $[[P, K], K] = 1$. Por outro lado, K age por automorfismos sobre P, os grupos K e P são finitos e tais que $(|K|, |P|) = 1$, então, pelo Lema 2.2.12, temos que $[P, K, K] = [P, K]$. Donde segue que, $[P, K] = 1$, o que é uma contradição. Logo, devemos ter $[P, K] = P$.

Apliquemos, agora, nossa primeira observação no caso em que $Q = P'$. Sabemos que, $P' = [P, P] < P$ e que P' é K-invariante, pois P o é. Assim, também, pela minimalidade de P, temos que $[P', K] = 1$. Além disso, sendo P' subgrupo normal de P, então, pelo Lema 1.2.9, $[P', P] < P'$ e assim, $[P', P, K] < [P', K] = 1$. Por outro lado, $[K, P', P] = [[P', K], P]$. Como já vimos que, $[P', K] = 1$, segue daí $[K, P', P] = 1$. Assim, pelo Lema 1.2.11,

temos que $[P, K, P'] = 1$. Agora como $[P, K] = P$, segue que $[P, P'] = 1$. Portanto P' é central em P. Sabemos que a série central inferior de P á dada por :

$$\gamma_1(P) = P \geq \gamma_2(P) = [P, P] \geq \gamma_3(P) = [P', P] = 1.$$

Segue daí que a classe de nilpotência de P é no máximo 2.

Agora note que, como P' é subgrupo normal de P e P' é K-invariante, vimos no Capítulo 2, que K age por automorfismos sobre P/P'. Então pelo Lema 2.2.8, segue que $[P/P', K] = [P, K]P'/P'$, mas como $[P, K] = P$, obtemos que $[P/P', K] = P/P'$. Por outro lado, P/P' é abeliano e é um 2-grupo finito, e assim, $(|K|, |P/P'|) = 1$. Então pelo Teorema 2.2.13, temos que

$$P/P' = C_{P/P'}(K) \times [P/P', K].$$

E como $[P/P', K] = P/P'$, obtemos $C_{P/P'}(K) = 1$. Segue de $C_{P/P'}(K) = 1$ e da minimalidade de P, que P/P' não possui subgrupo próprio K-invariante. De fato, suponha que P/P' possui um subgrupo próprio K-invariante, digamos $\overline{H} = H/P'$. Note que também H seria um subgrupo próprio K-invariante de P e, então pela minimalidade de P, teríamos que $[H, K] = 1$. Assim, dados $h \in H$ e $k \in K$, teríamos que, $h^k = h$. Assim segueria que H/P' está contido em $C_{P/P'}(K)$, o que é uma contradição, pois $C_{P/P'}(K) = 1$. Portanto, P/P' não possui subgrupo próprio K-invariante e disto segue que P/P' é abeliano elementar. Efetivamente, suponha, por absurdo, que P/P' não é abeliano elementar, assim, existe $\overline{g} \in P/P'$ tal que $\overline{g}^2 \neq \overline{1}$. Portanto, o subgrupo $\overline{H} = \langle \overline{g}^2 \mid \overline{g} \in P/P' \rangle$ é não trivial. Como P/P' é K-invariante, segue que, $(\overline{g}^2)^k = (\overline{g}^k)^2 = \overline{g_1}^2$ para todo $k \in K$, donde, $\overline{H}^K \leq \overline{H}$. E assim, P/P' possuiria um subgrupo próprio K-invariante, o que é um absurdo. E, portanto, P/P' deve ser abeliano elementar.

Observe agora que, P não é abeliano, ou seja, que existem $a, b \in P$ tais que $[a, b] \neq 1$. Com efeito, se $P' = 1$, teríamos $P \cong P/P'$. Como P/P' é abeliano elementar, segueria que P também é abeliano elementar. Sendo P um 2-grupo, então todo elemento de P teria ordem 2. Mas, por hipótese, K fixa todos os elementos de ordem 2 de P, e portanto teríamos que $[P, K] = 1$, o que é um absurdo. Portanto, P não pode ser abeliano.

Mas, por outro lado, dados $a, b \in P$, temos que $[a, b^2] = [a, b]^2 = 1$. Efetivamente, sabemos pelo Lema 1.2.2(iii) que $[a, b^2] = [a, b][a, b]^b$, mas como P' é central em P, obtemos, $[a, b^2] = [a, b]^2$. Além disso, como P/P' é abeliano elementar, temos $\overline{b^2} = \overline{b}^2 = \overline{1}$, daí, $b^2 \in P'$, para todo $b \in P$.

Portanto, realmente vale $[a, b^2] = [a, b]^2 = 1$, para quaisquer $a, b \in P$, pois $b^2 \in P'$ e $P' \leq Z(P)$. Segue daí, que todo gerador de P' tem ordem 2 e como P' é abeliano, logo, todo elemento de P' tem ordem 2, ou seja, P' é abeliano elementar. Portanto P tem expoente no máximo 4.

Os argumentos apresentados até o presente momento são devidos a Isaacs e Navarro [**5**]. A partir deste ponto da demonstração seguimos as considerações de Marciniak, feitas em [**7**]. Tome $a \in P$ arbitrariamente e relembremos que $K = \langle x \rangle$. Defina $a_i = a^{x^i}$, para $0 \leq i < q$. A partir de a_i, defina $b_i = a_i a_{i+1}^{-1}$. Observe que, a priori, b_i está definido para todo i, mas como seu valor depende de a_i e este está definido apenas para $0 \leq i < q$, então na definição de b_i, tomamos os índices sendo congruentes módulo q.

Um primeiro fato que pode ser observado com relação a b_i é o seguinte:

$$b_{i+1}^2 = (b_i^2)^x = b_i^2. \tag{3.2.1}$$

Com efeito, desenvolvendo a expressão de b_{i+1}^2, obtemos

$$b_{i+1}^2 = a_{i+1}a_{i+2}^{-1}a_{i+1}a_{i+2}^{-1} = a^{x^{i+1}}(a^{x^{i+2}})^{-1}a^{x^{i+1}}(a^{x^{i+2}})^{-1}. \tag{3.2.2}$$

Por outro lado, desenvolvendo a expressão de $(b_i^2)^x$, temos que

$$(b_i^2)^x = (a_i a_{i+1}^{-1} a_i a_{i+1}^{-1})^x = a^{x^{i+1}}(a^{x^{i+2}})^{-1}a^{x^{i+1}}(a^{x^{i+2}})^{-1}. \tag{3.2.3}$$

Mas como visto anteriormente, $b_i^2 \in P'$ e $[P', K] = 1$, portanto segue disto que $(b_i^2)^x = b_i^2$ e das igualdades (3.2.2) e (3.2.3) que, $b_{i+1}^2 = b_i^2$, como havíamos afirmado.

Observemos agora o seguinte:

$$b_0 b_1 \cdots b_{q-1} = a_0 a_1^{-1} a_1 a_2^{-1} \cdots a_{q-1} a_0^{-1} = 1. \tag{3.2.4}$$

Chame $c = b_0 b_1 \cdots b_{q-3}$. Temos

$$c^{b_{q-2}} = b_{q-2}^{-1} c b_{q-2} = b_{q-2}^{-1}(b_0 b_1 \cdots b_{q-3} b_{q-2} b_{q-1}) b_{q-1}^{-1}. \tag{3.2.5}$$

Segue de (3.2.4) que $c^{b_{q-2}} = b_{q-2}^{-1} b_{q-1}^{-1}$. Além disso, segue de (3.2.1) que, em particular,

$$b_{q-1}^2 = b_{q-2}^2. \tag{3.2.6}$$

Como P' é um 2-grupo elementar abeliano, então todo elemento de P' é igual a seu inverso, e já sabemos que $b_{q-2}^2 \in P'$, logo

$$b_{q-2}^2 = b_{q-2}^{-2}. \tag{3.2.7}$$

De (3.2.6) e (3.2.7), obtemos que $b_{q-2}^{-2} = b_{q-1}^2$. Agora, multiplicando ambos os membros desta igualdade, à esquerda por b_{q-2} e à direita por b_{q-1}^{-1}, concluímos que

$$b_{q-2}^{-1}b_{q-1}^{-1} = b_{q-2}b_{q-1}. \tag{3.2.8}$$

Portanto, como $c^{b_{q-2}} = b_{q-2}^{-1}b_{q-1}^{-1}$ e vale (3.2.8), temos que

$$c^{b_{q-2}} = b_{q-2}b_{q-1}. \tag{3.2.9}$$

Observemos ainda que, como $c = b_0b_1\cdots b_{q-3}$, então usando a identidade (3.2.4), obtemos $cb_{q-2}b_{q-1} = 1$, logo

$$c^{-1} = b_{q-2}b_{q-1}. \tag{3.2.10}$$

Assim de (3.2.9) e (3.2.10) temos que

$$c^{-1} = c^{b_{q-2}}. \tag{3.2.11}$$

Portanto, temos duas possibilidades: ou $b_{q-2} = 1$ ou $b_{q-2} \neq 1$. No primeiro caso, temos que $c = c^{-1}$ e isto implica $c^2 = 1$. No caso em que $b_{q-2} \neq 1$, então c é conjugado com seu inverso c^{-1}, logo c é um elemento real de ordem 4.

Por hipótese K fixa todos os elementos de ordem 2 e todos os elementos reais de ordem 4 em P, assim, em ambos os casos acima, temos

$$a_0a_{q-2}^{-1} = b_0b_1\cdots b_{q-3} = c \in C_P(K). \tag{3.2.12}$$

Finalmente, temos que

$$[x^{q-2}, a^{-1}] = (x^{q-2})^{-1}ax^{q-2}a^{-1} = a^{x^{q-2}}a^{-1} = a_{q-2}a_0^{-1}. \tag{3.2.13}$$

Assim, por, (3.2.12) e (3.2.13), concluímos que

$$[x^{q-2}, a^{-1}] = c^{-1} \in C_P(K). \tag{3.2.14}$$

Como $K = \langle x\rangle$ e a ordem de x é um primo ímpar q, pelo Lema 1.1.18, segue que todo elemento não trivial de K gera K. Em particular, x^{q-2} gera K. Além disso, $a \in P$ foi tomado de modo inteiramente arbitrário e então por (3.2.14), obtemos que $[K, P] \leq C_P(K)$. Concluímos que $[K, P] = [P, K] = [P, K, K] = 1$, mas isto é uma contradição. E isto conclui a demonstração.

□

CAPíTULO 4

Critérios de p-nilpotência

Neste capítulo vamos apresentar alguns critérios clássicos de p-nilpotência de um dado grupo finito G. Vamos também expor dois novos critérios de p-nilpotência que são consequências dos Teoremas 3.1.1 e 3.2.3.

4.1. Critérios Clássicos de p-nilpotência

Primeiramente vamos estabelecer o conceito de p-nilpotência. Seja N um subgrupo normal de G e p um número primo. Dizemos que H é um *p-complemento* de N em G se o índice de H em G, $|G : H|$, é uma potência de p e a ordem de H, $|H|$, não é divisível por p. Em outras palavras, H é um subgrupo cujo índice é a ordem de um p-subgrupo de Sylow de G.
Se na definição de p-complemento, o grupo H é normal em G, diremos que H é um p-complemento normal.

Definição 4.1.1. Um grupo finito G é dito *p-nilpotente*, para algum primo p, se G possui um p-complemento normal.

Nesta seção temos unicamente o objetivos de apresentar critérios de p-nilpotência geralmente encontrados na literatura.

Definição 4.1.2. Sejam G um grupo e H um subgrupo de G. O *subgrupo focal* de H em G é definido como o subgrupo

$$Foc_G(H) = \langle x^{-1}y \mid x, y \in H \text{ e } x, y \text{ sejam conjugados em } G \rangle.$$

Note que se $x, h \in H$, então x e x^h são certamente elementos de H conjugados em G, uma vez que eles são conjugados em H. Segue daí que $[x, h] = x^{-1}x^h \in Foc_G(H)$. Portanto, vemos que o subgrupo derivado de H, H', é um subgrupo de $Foc_G(H)$. Sejam agora x, y elementos de H que são conjugados em G, ou seja, existe $g \in G$ tal que $x^g = y$, mas não são conjugados em H. Neste caso, temos que $x^{-1}y = [x, g] \in G'$ e, portanto segue que $Foc_G(H) \leq G'$. Como já vimos no Capítulo 2, se X é uma classe de conjugação de G e H é um subgrupo de G, então $X \cap H$ pode ser ou não vazia. No segundo caso, tudo o que podemos afirmar é que $X \cap H$ é uma união de classes de conjugação de H.

Dizemos que as classes Y_1 e Y_2 de H estão *fundidas* em G se Y_1 e Y_2 estão contidas na mesma classe de conjugação de G.

Se $H \leq K \leq G$, dizemos que K controla G-fusão em H se quaisquer duas classes de conjugação de H que estão fundidas em G também estão fundidas em K. Ou equivalentemente, K controla G-fusão em H se, e somente se, todo par de elementos de H que são conjugados em G, são também conjugados em K. Disto segue, em particular, que $Foc_K(H)$ e $Foc_G(H)$ possuem os mesmos geradores e, portanto, $Foc_K(H) = Foc_G(H)$. Assim, G sempre controla G-fusão em H e H controla G-fusão em si mesmo precisamente quando não existem duas classes distintas de H que estão fundidas em G.

LEMA 4.1.3 (Lemma 5.12 [**4**]). *Seja P um p-subgrupo de Sylow de um grupo finito G. Então $N_G(P)$ controla G-fusão em $C_G(P)$.*

O Lema 4.1.3 é utilizado para demonstrar o critério de p-nilpotência devido a Burnside, que apresentamos no teorema à seguir. Os leitores interessados podem ver a demonstração dos resultados desta seção em [**4**].

TEOREMA 4.1.4 (Theorem 5.13 [**4**]). *Seja P um p-subgrupo de Sylow de um grupo finito G e suponha que $P \leq Z(N_G(P))$. Então G possui um p-complemento normal.*

O Teorema 4.1.4 garante a existência de p-complemento normal se $P \leq Z(N_G(P))$, quando P é um p-subgrupo de Sylow de G. Note que a hipótese deste teorema vale somente quando P é abeliano. Portanto, o critério de Burnside não nos diz nada quando o subgrupo P não é abeliano. A seguir apresentamos o bem conhecido Teorema do Subgrupo Focal.

TEOREMA 4.1.5 (Theorem 5.21 [**4**]). *Suponha que P é um p-subgrupo de Sylow de um grupo finito G. Então*

$$Foc_G(P) = P \cap G'.$$

O teorema do Subgrupo Focal pode ser usado para demonstrar uma condição necessária e suficiente para que um grupo finito G possua um p-complemento normal sem a hipótese de que o subgrupo de Sylow seja abeliano. Este critério é apresentado no teorema a seguir.

TEOREMA 4.1.6 (Theorem 5.25 [**4**]). *Um grupo finito G possui um p-complemento normal se, e somente se, existe um p-subgrupo de Sylow de G que controla G-fusão em si mesmo.*

Embora o Teorema 4.1.6, apresente uma condição necessária e suficiente para determinar se um dado grupo finito é ou não p-nilpotente, ele apresenta desvantagens no sentido que sua aplicabilidade é limitada, já que em geral é difícil determinar se um p-subgrupo de Sylow de G controla ou não sua própria G-fusão. Um critério mais profundo e muito mais util para ver se um grupo G possui um p-complemento normal é um resultado devido a Frobenius, mostra que a existência de um p-complemento normal em G é determinada pelos p-subgrupos locais de G.

Relembremos que um subgrupo N de G é dito p-local em G se $N = N_G(X)$, onde X é algum p-subgrupo de G não trivial.

TEOREMA 4.1.7 (Theorem 5.26 [**4**]). *Sejam G um grupo finito e p um primo. Então as seguintes sentenças são equivalentes:*

(i) *O grupo G possui um p-complemento normal.*

(ii) *O subgrupo $N_G(X)$ possui um p-complemento normal para todo p-subgrupo não trivial X de G.*

(iii) *O quociente $N_G(X)/C_G(X)$ é um p-grupo para todo p-subgrupo X de G.*

Observe que se na afirmação (ii) o conjunto X não precisa ser necessariamente não trivial, para que o Teorema 4.1.7 continue valendo, mas isto não é tão interessante. De fato, se $X = 1$, então $N_G(X) = G$ e a implicação (ii) em (i) seria trivial. Além disso, a afirmação (iii) é automaticamente verdadeira quando $X = 1$ e, portanto é irrelevante se restringirmos ou não em (iii) X a um subgrupo não trivial. Vale destacar ainda que, em geral, não é verdade que se X é um p-subgrupo de G e $N_G(X)/C_G(X)$ é um p-grupo, então $N_G(X)$ possui um p-complemento normal. O Teorema 4.1.7 diz-nos que se para todo p-subgrupo X de G é verdade que $N_G(X)/C_G(X)$ é um p-grupo, então é também verdade que $N_G(X)$ possui um p-complemento normal para todo p-subgrupo X de G.

4.2. Outros Critérios de p-nilpotência

Resultados como os Teoremas 3.1.1 e 3.2.3 nos fornecem outros recursos quando precisamos decidir se um dado grupo finito é ou não p-nilpotente. Vejamos o primeiro critério de p-nilpotência que pode ser deduzido destes teoremas

TEOREMA 4.2.1. *Sejam P um p-subgrupo de Sylow de um dado grupo G e suponha que todos os elementos de ordem p em P são centrais em G. Se*

$p = 2$ suponha ainda que todos os elementos de ordem 4 em P são centrais em P. Então G possui um p-complemento normal.

DEMONSTRAÇÃO. Primeiramente observemos que se $p = 2$, então G não possui elemento real de ordem 4. De fato, suponha por absurdo, que existe $x \in G$ um elemento real de ordem 4. Segue daí que existe $y \in G$ tal que $x^y = x^{-1}$. Como x e x^y têm mesma ordem, ou seja, têm ordem 4, temos que y é um 2-elemento de G. Logo, o subgrupo $\langle x, y\rangle$ é um 2-subgrupo de G. Note que $\langle x, y\rangle$ está contido em algum p-subgrupo de Sylow de G e, portanto segue que $\langle x, y\rangle^g$ está contido em P, para algum $g \in G$. Agora observemos que x^g tem ordem 4, pois é conjugado com x, e, além disso, x^g não central em P. Efetivamente, suponha que x^g é central em P, daí, em particular x^g comuta com y^g, ou seja, $g^{-1}xyg = g^{-1}yxg$, donde segue que $xy = yx$, em outras palavras, que x e y comutam, mas isto é uma contradição, uma vez que $x^y = x^{-1}$. Além disso, como todos os elementos de ordem p em P são centrais em G, segue que todos os elementos de ordem p em G são centrais em G.

Sabemos pelo Teorema 4.1.7 que uma condição necessária e suficiente para que um grupo finito G seja p-nilpotente é que o grupo quociente $N_G(U)/C_G(U)$ é um p-grupo para todo p-subgrupo U de G. Vejamos agora que se para todo p-subgrupo U de G e todo K p'-subgrupo de $N_G(U)$ tem-se $[U, K] = 1$, então $N_G(U)/C_G(U)$ é um p-grupo. De fato, chamemos $N_G(U) = N$ e $C_G(U) = C$ e suponhamos, por absurdo, que N/C não é um p-grupo. Segue daí que N/C possui um p'-subgrupo T/C. Assim, T não é um p-grupo e então podemos escolher em T um p'-elemento não trivial t. Como $t \in N$, por hipótese, segue que $[U, t] = 1$, ou seja, $t \in C$, então a imagem, pelo homomorfismo canônico, de t em T/C é trivial. Logo, T/C não é um p'-subgrupo, o que é uma contradição. Portanto N/C é um p-grupo e G é p-nilpotente, como queríamos demonstrar.

Agora para ver que G possui um p-complemento normal aplicamos o Teorema 4.1.7 e, pelo argumento anterior, basta mostrar que para todo p-subgrupo U de G e todo p'-subgrupo K de $N_G(U)$, temos $[U, K] = 1$. Sabemos que K fixa todos os elementos de ordem p em U e U não possui elementos reais de ordem 4, então pelos Teorema 3.1.1 e 3.2.3 concluímos que K age trivialmente sobre U ou seja, $[U, K] = 1$. Isto concluí a demonstração. □

Vamos apresentar agora um outro critério de p-nilpotência, um pouco mais sutil, que também segue dos Teoremas 3.1.1 e 3.2.3. Já vimos no Teorema 4.1.6, que se P é um p-subgrupo de Sylow de G e P controla sua

própria G-fusão, então G possui um p-complemento normal. Dizer que P controla sua própria G-fusão significa, em outras palavras, que para cada elemento $x \in P$, temos que $x^G \cap P = x^P$, onde escrevemos x^G e x^P para denotar, respectivamente, as classes de conjugação de x em G e em P.

De fato, não é necessário assumir que $x^G \cap P = x^P$ para todo $x \in P$. Um resultado de J. González-Sánchez [Main Theorem **[1]**] mostra que se $x^G \cap P = x^P$ para todos os elementos $x \in P$ de ordem p ou 4, então G é p-nilpotente. Usando o Teorema 3.2.3 esse resultado pode ser ligeiramente melhorado, como mostra o teorema a seguir.

TEOREMA 4.2.2. *Seja P um p-subgrupo de Sylow de um grupo G e suponha que $x^G \cap P = x^P$ para todos os elementos $x \in P$ de ordem p e, se $p = 2$, assuma ainda que isto é válido para todo $x \in P$ de ordem 4. Então G é p-nilpotente.*

DEMONSTRAÇÃO. Como já vimos no Teorema 4.2.1, para garantir que G possui um p-complemento normal é suficiente mostrar que $[U, K] = 1$, para quaisquer p-subgrupo U de P e todo p'-subgrupo K de $N_G(U)$. Vamos demonstrar este resultado por indução sobre $|U|$. Podemos assumir $U > 1$. Se $[U, K]$ é subgrupo próprio de U, por hipótese de indução, temos que $[U, K, K] = 1$. Logo, pelo Lema 2.2.12 temos $[U, K] = [U, K, K]$, logo, $[U, K] = 1$, como desejamos mostrar.

Podemos assumir $[U, K] = U$ e trabalhamos para obter uma contradição. Seja S o subconjunto de U formado por todos os elementos de U que ou têm ordem p ou são reais e têm ordem 4. Claro que não existirão elementos do segundo tipo a menos que seja $p = 2$. Agora, seja $V = \langle S \rangle$. Pela forma como é definido o conjunto S, segue que V é característico em U e, então V admite ação de K. Se V é subgrupo próprio de U, então, por hipótese de indução, temos que $[V, K] = 1$ e dos Teoremas 3.1.1 e 3.2.3, segue que $[U, K] = 1$, como queríamos. Então podemos assumir $V = U$, assim U é gerado por S e podemos escrever todo elemento $u \in U$ da forma $u = s_1 s_2 \cdots s_r$, onde $s_i \in S$ e $r \geq 0$.

Vamos mostrar agora que $[U, K] \leq [U, P]$. Para isto, vamos demonstrar que $[u, k] \in [U, P]$, para quaisquer $u \in U$ e $k \in K$. Vamos proceder por indução sobre r, onde $u = s_1 s_2 \cdots s_r$, com $s_i \in S$. Se $r = 0$, então $u = 1$, e portanto $[u, k] = 1 \in [U, P]$. Podemos então assumir $r \geq 1$ e escrever $u = vs$, onde v é um produto de um número menor que r de termos de S e $s \in S$. Então, pelo Lema 1.2.2(ii), $[u, k] = [vs, k] = [v, k]^s [s, k]$. Assim é suficiente verificar que ambos os fatores, $[v, k]^s$ e $[s, k]$ pertencem a $[U, P]$.

Por hipótese de indução, sabemos que $[v,k] \in [U,P]$ e como $s \in S$, temos que $[v,k]^s \in [U,P]^s = [U,P]$. Para demonstrar que o fator $[s,k] \in [U,P]$, observemos que como $s \in S$, temos que $s^G \cap P = s^P$ e, portanto $s^k = s^t$, para algum $t \in P$. Logo, $[s,k] = s^{-1}s^k = s^{-1}s^t = [s,t] \in [U,P]$.

Agora temos que $U = [U,K] \leq [U,P]$, assim, aplicando um número arbitrário de vezes esta propriedade, concluímos que $U \leq [U,P,\cdots,P]$ para um número arbitrário de comutações por P. Mas $U \leq P$ e P é nilpotente, logo pelo Teorema 1.3.14 existe m inteiro tal que $\gamma_{m+1}(P) = [P,\cdots,P] = 1$, e, então $U = 1$, o que é uma contradição. □

Referências Bibliográficas

[1] J. GONZÁLEZ-SÁNCHEZ, A p-nilpotency criterion, *Arch. Math.* **94** (2010), 201-205.

[2] B. HUPPERT, *Endliche Gruppen I*, Springer-Verlag, Berlin, 1967.

[3] I. M. ISAACS, *Algebra. A Graduate Course*. Amer. Math. Soc., Graduate Studies in Mathematics. Volume 100. 2005.

[4] I. M. ISAACS, *Finite Group Theory*, Amer. Math. Soc., Providence (2008).

[5] I. M. ISAACS, G. NAVARRO, Normal p-complements and fixed elements. *Arch. Math.* **95** (2010), 208-211.

[6] E. I. KHUKHRO, *p-Automorphisms of Finite p-Groups*, London Mathematical Society Lecture Note Series, vol. 246, Cambridge University Press, Crambridge, 1998.

[7] Z. MARCINIAK, Fixed elements in 2-groups reviseted. *Arch. Math.* **97** (2011), 207-208.

[8] G. NAVARRO, L. SANUS, Rational and normal p-complement. *J. Algebra*, **320** (2008), 2451-2454.

[9] D. S. ROBINSON, *A Course in the Theory of Groups*. 2nd Edition, Graduate Texts in Mathematics, Springer, 1995.