UNIVERSIDADE FEDERAL DE MINAS GERAIS
INSTITUTO DE CIÊNCIAS EXATAS
DEPARTAMENTO DE MATEMÁTICA

Dissertação de Mestrado

Sobre uma classe especial de grupos nilpotentes

Claudiano Henrique da Cunha Melo

Belo Horizonte
2015

UNIVERSIDADE FEDERAL DE MINAS GERAIS
INSTITUTO DE CIÊNCIAS EXATAS
DEPARTAMENTO DE MATEMÁTICA

Claudiano Henrique da Cunha Melo

Sobre uma classe especial de grupos nilpotentes

Dissertação apresentada ao corpo docente de Pós-Graduação em Matemática do Instituto de Ciências Exatas da Universidade Federal de Minas Gerais, para a obtenção de Título de Mestre em Matemática, na Área de Álgebra.

Orientadora: Ana Cristina Vieira

Belo Horizonte
2015

Melo, Claudiano Henrique da Cunha

Sobre uma classe especial de grupos nilpotentes

50 páginas

Dissertação (Mestrado) - Instituto de Ciências Exatas da Universidade Federal de Minas Gerais. Departamento de Matemática.

1. álgebra
2. p-grupos
3. classificação

I. Universidade Federal de Minas Gerais. Instituto de Ciências Exatas. Departamento de Matemática.

Comissão Julgadora:

Prof. Dr.
Nome

Prof. Dr.
Nome

Prof. Dr.
Ana Cristina Vieira

Dedicatória

À toda minha família.

Agradecimentos

Agradeço à minha orientadora Ana Cristina Vieira, pela paciência e pelo incentivo; aos demais professores do Departamento de Matemática, que colaboraram para minha formação; à CAPES, pelo auxílio financeiro; aos meus amigos e à minha família pelo apoio constante.

Resumo

Os p-grupos finitos formam uma classe especial de grupos nilpotentes e são objetos de grande importância na teoria dos grupos. Neste trabalho, apresentamos resultados clássicos da teoria de p-grupos finitos e alguns resultados de classificação, como por exemplo uma classificação simples para os grupos de ordem p^4 usando o conceito de extensões tipo.

Palavras-chave: álgebra, p-grupos, classificação

Abstract

Finite p-groups form a particular class of nilpotent groups and are very important objects in group theory. In this work, we present classical results from the finite p-groups theory and some results of classification such as a simple classification of the groups of order p^4 using the concept of extension types.

Keywords: algebra, p-groups, classification

Introdução

Neste trabalho abordamos resultados clássicos a respeito de uma classe particular de grupos nilpotentes: os p-grupos finitos. Entendendo a estrutura dos p-grupos obtemos informações que nos ajudam a compreender a estrutura dos grupos nilpotentes finitos, já que estes podem ser decompostos como produto direto de seus p-subgrupos de Sylow que, por sua vez, são p-grupos.

No primeiro capítulo desta dissertação, apresentamos resultados básicos [4, 11] sobre a teoria de p-grupos finitos.

No segundo capítulo, usando resultados sobre automorfismos de p-grupos, damos uma classificação de alguns tipos especiais de p-grupos, a saber: [11] os p-grupos que contém um subgrupo maximal cíclico e os p-grupos que contém um único subgrupo cíclico de ordem p.

Já no terceiro capítulo, seguindo os passos de [1] Adler, apresentamos ainda uma classificação dos grupos de ordem p^4 usando o conceito de extensões tipo. Essa classificação é interessante pois usa apenas resultados elementares, e é, portanto, mais simples que as classificações apresentadas em 1893 independentemente por Otto Ludwig Hölder (1859-1937) e Jacob William Albert Young (1865-1948) e que a apresentada no livro texto Endliche Gruppen I [5], de 1967, cujo autor é Bertram Huppert.

Terminamos o trabalho fazendo algumas considerações sobre os grupos de ordem p^5, p^6 e p^7. Ao longo deste trabalho, p denotará um primo e G será um grupo finito, a menos que algo seja dito em contrário.

Sumário

Capítulo 1

Resultados Preliminares

Neste capítulo apresentamos resultados clássicos sobre a teoria de p-grupos e de grupos nilpotentes, suas estruturas e seus automorfismos.

1.1 p-Grupos finitos

Dado um primo p, um grupo G é dito um p-grupo se todo elemento de G tem ordem potência de p. Quando G é um p-grupo finito, o teorema de Cauchy garante que $|G| = p^n$, para algum $n \in \mathbb{N}$.

Os p-grupos têm natural importância na teoria de grupos finitos devido ao clássico Teorema de Sylow.

Teorema 1.1. (Teorema de Sylow) Seja G um grupo de ordem $p^n m$, com $n \geq 1$ e $(p, m) = 1$. Então G contém um subgrupo de ordem p^i para cada $1 \leq i \leq n$.

Temos ainda que todo subgrupo de G de ordem p^i $(i < n)$ é normal em algum subgrupo de ordem p^{i+1}. Um subgrupo de G com ordem p^n é dito um p-subgrupo de Sylow de G.

Dado um grupo G, o conjunto dos elementos que comutam com todos os outros elementos de G é chamado de centro de G e é denotado por $Z(G)$.

Teorema 1.2. Se G é um p-grupo, então G tem centro não trivial.

Demonstração. Sejam $|G| = p^n$ e $\{x_1, x_2, ..., x_t\}$ um conjunto completo de representantes das classes de conjugação de G. Assim, $G = \mathcal{C}(x_1) \dot{\cup} \mathcal{C}(x_2) \dot{\cup} ... \dot{\cup} \mathcal{C}(x_t)$. Portanto, $|G| = n_1 + n_2 + ... + n_t$, onde $n_i = |\mathcal{C}(x_i)|$.

Suponha, por contradição, que o centro de G é trivial. Então existe apenas uma classe de conjugação de G que contém um único elemento que é a classe do elemento neutro de G, digamos $n_1 = 1$ e $n_i > 1$ para todo $i > 1$. Sabemos que cada $n_i | p^n$, então juntando essa informação ao fato de que $n_i > 1$ para todo $i > 1$, concluímos que todo n_i, com $i > 1$, é potência de p.

Logo $p^n = |G| = 1 + \sum_{i=2}^{t} n_i = 1 + kp$, para algum inteiro k, um absurdo. □

Queremos obter informações sobre a estrutura de p-grupos finitos exclusivamente a partir de sua ordem. Obviamente, quando $|G| = p$ então G é um grupo cíclico e, neste caso, escreveremos $G \simeq C_p$. Vamos ver o que podemos dizer sobre p-grupos com ordem pequena.

A próxima observação será útil no nosso trabalho.

Observação 1.3. Se $G/Z(G)$ é cíclico, então G é abeliano.

De fato, seja $yZ(G)$ um elemento de $G/Z(G)$ que o gera. Então todo elemento de G é da forma $y^i z$ para algum $z \in Z(G)$. Sejam $g_1, g_2 \in G$, temos que $g_1 = y^{i_1} z_1$ e $g_2 = y^{i_2} z_2$, para algum $z_1, z_2 \in Z(G)$. Então

$$g_1 g_2 = y^{i_1} z_1 y^{i_2} z_2 = y^{i_1} y^{i_2} z_1 z_2 = y^{i_2} y^{i_1} z_2 z_1 = y^{i_2} z_2 y^{i_1} z_1 = g_2 g_1.$$

Com isso, o centro de um grupo nunca é de índice primo. Consequentemente, é claro que se $|G| = p^n$, então $|Z(G)| \neq p^{n-1}$.

Teorema 1.4. Todo grupo G de ordem p^2 é abeliano.

Demonstração. Como G é um p-grupo, tem centro não trivial e além disso, $|Z(G)| \neq p$ pela observação anterior. Apenas nos resta $|Z(G)| = p^2$. □

Dado um grupo G e um elemento $x \in G$, definimos o centralizador do elemento x em G como $C_G(x) := \{g \in G \mid gx = xg\}$. Podemos estender essa definição para um subconjunto $X \subseteq G$ não vazio e definir o centralizador de X em G como $C_G(X) := \{g \in G \mid gx = xg \text{ para todo } x \in X\}$.

Dado um subconjunto $X \subseteq G$ não vazio e um elemento $g \in G$, definimos o conjugado de X por g como $X^g := gXg^{-1} = \{gxg^{-1} \mid x \in X\}$ e o normalizador de X em G como $N_G(X) := \{g \in G \mid X^g = X\}$. Se H é um subgrupo de G então $N_G(H)$ é o maior subgrupo de G no qual H é normal.

Teorema 1.5. Sejam G um grupo e p o menor primo que divide $|G|$. Se G possui um subgrupo H tal que $[G : H] = p$, então $H \lhd G$. Em particular um subgrupo de índice 2 é sempre normal.

Demonstração. Defina $S := \{gH;\ g \in G\}$ e considere a ação de multiplicação à esquerda φ de G em $Sym(S)$, que tem ordem $p!$ já que H tem p classes laterais a esquerda. Para cada $g_0 \in G$ temos

$$\begin{aligned} \varphi(g_0) : S &\longrightarrow S \\ gH &\longmapsto g_0.gH. \end{aligned}$$

Defina $K := ker(\varphi)$, então claramente K é subgrupo de H. Digamos que $[H : K] = k$, então $[G : K] = [G : H].[H : K] = pk$. Defina também $L := Im(\varphi)$ subgrupo de $Sym(S)$. Então $|L|$ divide $p!$.

Pelo Primeiro Teorema do Isomorfismo, $G/K \simeq L$, com isso concluímos que $pk = [G : K]$ divide $p!$. Ou seja, k divide $p!/p = (p-1)!$. Como p foi tomado como o menor primo que divide $|G|$, todo número primo divisor de k é maior ou igual a p.

Por outro lado, todo número primo que divide $(p-1)!$ é menor que p. Então, devemos ter $k = 1$ e com isso $H = K$. Como toda ação é um homomorfismo, devemos ter $K \lhd G$ e, portanto, $H \lhd G$. □

1.2 Grupos solúveis e nilpotentes

Os p-grupos finitos fazem parte de classes maiores de grupos, como definidas abaixo.

Definição 1.6. Dizemos que um grupo G é solúvel se ele possui uma série abeliana que começa em $\{1\}$ e termina em G, ou seja, se ele possui subgrupos G_i tais que $\{1\} = G_0 \lhd G_1 \lhd ... \lhd G_n = G$ e cada quociente G_{i+1}/G_i é abeliano.

Então se G é um p-grupo finito, de ordem p^n, o Teorema de Sylow garante que ele possui um subgrupo G_{n-1} de ordem p^{n-1}. Como o índice $[G : G_{n-1}] = p$ temos que $G_{n-1} \lhd G$ e que o quociente $G/G_{n-1} \simeq C_p$, que é cíclico, logo abeliano. Repetindo o raciocínio para o grupo G_{n-1} obteremos uma série abeliana que estabiliza em $\{1\}$, donde concluímos que todo p-grupo finito é solúvel.

Dado um grupo G, definimos o subgrupo $G' = [G, G] \leq G$ como o subgrupo gerado por todos os comutadores de G, ou seja, $G' = [G, G] = \langle [g, h] = ghg^{-1}h^{-1} \mid g, h \in G \rangle$. Esse subgrupo é normal e o quociente G/G' é abeliano.

Uma propriedade importante que temos aqui é que o quociente G/G' é o maior grupo quociente de G que é abeliano, ou seja, se existe um subgrupo normal $H \lhd G$ tal que G/H é abeliano, então $G' \leq H$.

Formando subgrupos derivados repetidas vezes, obtemos uma sequência decrescente de subgrupos:

$$G = G^{(0)} \geq G^{(1)} \geq G^{(2)} \geq ...$$

onde $G^{(n+1)} = (G^{(n)})'$. Esta é chamada de série derivada de G. Como os quocientes $G^{(n)}/G^{(n+1)} = G^{(n)}/(G^{(n)})'$ são abelianos, esta é uma série abeliana. Note que ela não alcança necessariamente o subgrupo identidade, mas isto sempre ocorre quando G é solúvel.

Teorema 1.7. Se $\{1\} = G_0 \lhd G_1 \lhd ... \lhd G_n = G$ é uma série abeliana de um grupo solúvel G então $G^{(i)} \leq G_{n-i}$. Em particular $G^{(n)} = 1$.

Demonstração. O caso em que $i = 0$ é óbvio. Usaremos indução em i. Suponha que $G^{(j)} \leq G_{n-j}$ para todo $j < i$.

Se $i > 0$, temos que $G^{(i)} = (G^{(i-1)})' \leq (G_{n-(i-1)})'$ pela hipótese de indução. Também $(G_{n-(i-1)})' \leq G_{n-i}$, já que o quociente G_{n-i+1}/G_{n-i} é abeliano. Logo, $G^{(i)} \leq G_{n-i}$ para todo i. Em particular $G^{(n)} \leq G_0 = \{1\}$. □

Dizemos que uma série de subgrupos $G_0 \leq G_1 \leq ... \leq G_i \leq G_{i+1} \leq ...$ é normal se cada subgrupo G_i for normal em G. Uma série normal tal que G_{i+1}/G_i está contido no centro de G/G_i para todo i é dita uma série central de G.

Uma outra série definida a partir do subgrupo derivado de um grupo G é a série central inferior:

$$G = \gamma_1(G) \geq \gamma_2(G) \geq ... \geq \gamma_i(G) \geq \gamma_{i+1}(G) \geq ...$$

onde $\gamma_{i+1}(G) = [\gamma_i(G), G]$.

Note que o quociente $\gamma_n(G)/\gamma_{n+1}(G)$ está contido no centro de $G/\gamma_{n+1}(G)$, portanto esta é uma série central. Assim como a série derivada, a série central inferior não alcança necessariamente o subgrupo identidade.

Podemos também definir uma sequência ascendente de subgrupos a partir do centro de um grupo G. A chamada série central superior:

$$\{1\} = Z_0(G) \leq Z_1(G) \leq ...$$

onde cada quociente $Z_{i+1}(G)/Z_i(G) = Z(G/Z_i(G))$. Claramente, $Z_1(G) = Z(G)$.

Definição 1.8. Dizemos que um grupo G é nilpotente se ele possui uma série central que começa em $\{1\}$ e termina em G. O tamanho da menor série central de G é chamado de classe de nilpotência de G.

O seguinte teorema traz alguns resultados importantes sobre grupos nilpotentes.

Teorema 1.9. Seja $\{1\} = G_0 \leq G_1 \leq \ ... \ \leq G_n = G$ uma série central de um grupo nilpotente G. Então

(i) $\gamma_i(G) \leq G_{n-i+1}$, logo $\gamma_{n+1}(G) = \{1\}$;

(ii) $G_i \leq Z_i(G)$, logo $Z_n(G) = G$;

(iii) a classe de nilpotência de G é igual ao tamanho das séries centrais superior e inferior.

Demonstração. (i) O caso em que $i = 1$ é óbvio. Usaremos indução em i. Suponha que $\gamma_j(G) \leq G_{n-j+1}$ para todo $j < i$.

Para $i > 1$, sabemos pela definição de série central que o quociente G_{n-i+1}/G_{n-i} está contido no centro de G/G_{n-i}. Isso quer dizer que $[G_{n-i+1}, G] \leq G_{n-i}$. Usando a hipótese de indução, temos que $\gamma_i(G) = [\gamma_{i-1}(G), G] \leq [G_{n-i+2}, G] \leq G_{n-i+1}$.

(ii) O caso em que $i = 0$ é trivial. Novamente usaremos indução em i. Suponha que $G_j \leq Z_j(G)$ para todo $j < i$.

Dado $i > 0$, usando a hipótese de indução, temos que $G_{i-1} \leq Z_{i-1}(G)$. Como a série é central vale $G_i/G_{i-1} \leq Z(G/G_{i-1})$ donde $[G_i, G] \leq G_{i-1} \leq Z_{i-1}(G)$. Isto quer dizer que $G_i/Z_{i-1} \leq Z(G/Z_{i-1}(G))$ e portanto $G_i \leq Z_i$.

(iii) Segue de (i) e (ii) que estas são as menores séries centrais de G. □

Um fato importante sobre os grupos nilpotentes finitos é que eles são caracterizados como o produto direto de seus subgrupos de Sylow, que são p-grupos.

Outra característica dos grupos nilpotentes finitos é que eles têm sempre centro não trivial. Mais do que isso, dado qualquer subgrupo normal não trivial de um grupo nilpotente G, ele intercepta o centro de G não trivialmente como vemos no próximo resultado.

Teorema 1.10. Se G é um grupo nilpotente finito e $\{1\} \neq N \lhd G$, então $N \cap Z(G) \neq \{1\}$.

Demonstração. Como G é nilpotente, $G = Z_c(G)$ para algum c. Assim, existe um menor inteiro positivo i tal que $N \cap Z_i(G) \neq \{1\}$. Vale que $[N \cap Z_i(G), G] \leq [N, G] \subset N$ e $[N \cap Z_i(G), G] \leq [Z_i(G), G] \subset Z_{i-1}(G)$. Portanto, $[N \cap Z_i(G), G] \subset N \cap Z_{i-1}(G) = \{1\}$. Isso quer dizer que $\{1\} \neq N \cap Z_i(G) \subset N \cap Z(G)$. □

Teorema 1.11. Um p-grupo finito é nilpotente.

Demonstração. Seja G um grupo de ordem p^n. Usaremos o fato de que um p-grupo tem centro não trivial para construir a série central superior. Temos então $\{1\} < Z(G) = Z_1(G)$.

Agora, o quociente $G/Z(G)$ é também um p-grupo. Por isso $Z(G/Z(G)) > \{1\}$ e então existe $Z_2(G)$ subgrupo de G tal que $Z(G/Z(G)) = Z_2(G)/Z_1(G)$. Então $\{1\} < Z_1(G) < Z_2(G)$. Como cada inclusão é estrita e n é fixo, esta série alcançará G após no máximo n passos. Logo G é nilpotente. □

Não é difícil mostrar que subgrupos e imagens homomórficas de grupos nilpotentes são ainda nilpotentes. Usaremos este fato no próximo resultado.

Teorema 1.12. Se A é um subgrupo normal abeliano maximal do grupo nilpotente G, então $A = C_G(A)$.

Demonstração. Como A é abeliano, vale a inclusão $A \leq C := C_G(A)$. Além disso $C \lhd G$, uma vez que $gxg^{-1} \in C$ para quaisquer $g \in G$ e $x \in C$. Para mostrar que vale a igualdade, suponha por contradição que $A \neq C$. Então C/A é um subgrupo normal não trivial de G/A, e pelo Teorema 1.10 existe um elemento $xA \in (C/A) \cap Z(G/A)$ com $x \notin A$. Agora $\langle x, A\rangle$ é abeliano e é normal em G pois $\langle x, A\rangle/A \leq Z(G/A)$. Daí, $x \in A$ pela maximalidade de A. Este absurdo garante que $A = C$. □

1.3 Automorfismos de p-grupos

Começamos com um resultado básico sobre automorfismos de modo geral.

Teorema 1.13. Seja H um subgrupo de um grupo G. Então $C_G(H) \lhd N_G(H)$ e o quociente $N_G(H)/C_G(H)$ é isomorfo a um subgrupo de $Aut(H)$.

Demonstração. Dados um grupo G e um subgrupo $H \leq G$, para qualquer elemento $h \in N_G(H)$ temos o seguinte autormorfismo de H:

$$\begin{aligned} Int_h : H &\longrightarrow H \\ x &\longmapsto Int_h(x) = hxh^{-1}. \end{aligned}$$

Então considere a aplicação $\Phi : N_G(H) \to Aut(H)$ que leva cada $h \in N_G(H)$ em $Int_h \in Aut(H)$. Esta aplicação é um homomorfismo cujo núcleo é o centralizador $C_G(H)$.

Logo, $N_G(H)/C_G(H) = N_G(H)/ker(\Phi) \simeq Im(\Phi)$ que é um subgrupo de $Aut(H)$. □

Teorema 1.14. Seja G um grupo cíclico de ordem n, então $Aut(G)$ consiste de todos automorfismos $\alpha_k : g \mapsto g^k$, onde $1 \leq k < n$ e $(k, n) = 1$.

Demonstração. Sejam $G = \langle g \rangle$ e $\alpha \in Aut(G)$. Como $\alpha(g^n) = (\alpha(g))^n$, o automorfismo α é totalmente determinado por $\alpha(g)$. Note que $\alpha(g)$ precisa gerar G, logo $|\alpha(g)| = n$.

Então $\alpha(g) = x^k$ para algum $k \in \mathbb{N}$ tal que $1 \leq k < n$ e $(k, n) = 1$.

Analogamente, se k é tal que $1 \leq k < n$ e $(k, n) = 1$, a aplicação $g \mapsto g^k$ é um automorfismo. □

Com isso, a aplicação $k + n\mathbb{Z} \mapsto \alpha_k$ é um isomorfismo entre $U(\mathbb{Z}_n)$, o grupo das unidades de $\mathbb{Z}_n$, e $Aut(G)$. Em particular $Aut(G)$ é abeliano e tem ordem $\phi(n)$, onde ϕ é a função de Euler.

Vamos agora analisar os automorfismos não triviais de ordem p de $C_{p^2} \times C_p$. Para isso tomemos um gerador x de C_{p^2} e um gerador y de C_p. Então os automorfismos de $C_{p^2} \times C_p$ são da forma

$$\begin{cases} x \longmapsto x^a y^b \\ y \longmapsto x^c y^d \end{cases}$$

para a e c inteiros módulo p^2, e b e d inteiros módulo p. Como um automorfismo preserva a ordem dos elementos, devemos ter $(x^a y^b)^p \neq 1$ donde podemos ver que p não divide a e também $(x^c y^d)^p = 1$ donde concluímos que p divide c. Podemos representar este automorfismo pela matriz $\begin{pmatrix} a & c \\ b & d \end{pmatrix}$. Nesta representação, veremos que a composição de automorfismos é compatível com o produto de matrizes.

De fato, se tomarmos dois automorfismos

$$\tau : \begin{cases} x \longmapsto x^a y^b \\ y \longmapsto x^c y^d \end{cases} \quad \text{e} \quad \phi : \begin{cases} x \longmapsto x^e y^f \\ y \longmapsto x^g y^h \end{cases}$$

Então

$$\phi \circ \tau : \begin{cases} x \longmapsto \phi(x^a y^b) = (\phi(x))^a (\phi(y))^b = (x^e y^f)^a (x^g y^h)^b = x^{ea+gb} y^{fa+hb} \\ y \longmapsto \phi(x^c y^d) = (\phi(x))^c (\phi(y))^d = (x^e y^f)^c (x^g y^h)^d = x^{ec+gd} y^{fc+hd} \end{cases}$$

e a representação deste automorfismo coincide com o produto de matrizes

$$\begin{pmatrix} e & g \\ f & h \end{pmatrix} \begin{pmatrix} a & c \\ b & d \end{pmatrix} = \begin{pmatrix} ea+gb & ec+gd \\ fa+hb & fc+hd \end{pmatrix}.$$

Aqui usamos um abuso de notação, uma vez que a multiplicação de matrizes com entradas em anéis distintos não é bem definida. Considere o seguinte homomorfismo de anéis

$$\begin{array}{ccc} \pi : \mathbb{Z}_{p^2} & \to & \mathbb{Z}_p \\ \bar{a} \pmod{p^2} & \longmapsto & \bar{a} \pmod{p} \end{array}$$

e então os elementos denotados por "$ea+gb$", "$fa+hb$", "$ec+gd$"e "$fc+hd$"são na verdade os elementos "$ea+g.\pi^{-1}(b)$", "$f.\pi(a)+hb$", "$ec+g.\pi^{-1}(d)$"e "$f\pi(c)+hd$", respectivamente, com todos os elementos no mesmo anel.

Agora, considerando o homomorfismo

$$\begin{array}{rcl} \varphi : Aut(C_{p^2} \times C_p) & \to & GL(2;\mathbb{F}_p) \\ \begin{pmatrix} a & c \\ b & d \end{pmatrix} & \longmapsto & \begin{pmatrix} \pi(a) & \pi(c) \\ b & d \end{pmatrix} \end{array}$$

temos que a imagem por φ de um automorfismo de $C_{p^2} \times C_p$ é um elemento de $GL(2;\mathbb{F}_p)$, onde $\mathbb{F}_p$ é o corpo com p elementos. Este homomorfismo está bem definido, uma vez que π também está.

Agora, precisamos usar o seguinte teorema de Álgebra Linear.

Teorema 1.15. (Forma Canônica de Jordan para Matrizes) Seja A uma matriz $n \times n$ sobre um corpo F e assuma que F contém os autovalores de A. Então:

1. A matriz A é semelhante a uma matriz na forma canônica de Jordan, isto é, existe uma matriz sobre F, $n \times n$ e invertível, P tal que PAP^{-1} é uma matriz diagonal em blocos cujos blocos diagonais são os blocos de Jordan.

2. A forma canônica de Jordan é única a menos de uma permutação dos blocos de Jordan ao longo da diagonal. Os blocos de Jordan são submatrizes (a_{ij}), $1 \leq i, j \leq m$ e $m \leq n$ com elementos a_{ii} iguais a um determinado autovalor de A, elementos a_{kl} iguais a 1 se $l = k-1$, $2 \leq l \leq m$, e os demais elementos iguais a 0.

Como estamos considerando os automorfismos de ordem p sobre o corpo $\mathbb{F}_p$, a imagem deles por φ é raiz do polinômio $X^p - 1 = (X-1)^p$, ou seja, todos os autovalores são iguais a 1. Com isso, ela é conjugada a $\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ ou a $\begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}$.

Portanto, se A é a imagem do automorfismo τ - de ordem p de $C_{p^2} \times C_p$ - por φ em $GL(2;\mathbb{F}_p)$, existe uma matriz P tal que PAP^{-1} tem a forma acima. Assim, tomando qualquer automorfismo $\sigma \in \varphi^{-1}(P)$, a composição $\sigma \circ \tau \circ \sigma^{-1}$ tem a forma

$$\begin{pmatrix} 1+ps & pr \\ 0 & 1 \end{pmatrix} \text{ ou } \begin{pmatrix} 1+ps & pr \\ 1 & 1 \end{pmatrix},$$

onde $r, s \in \{0, 1, ..., p-1\}$, que são exatamente as pré imagens dos possíveis valores de $PAP^{-1} = \varphi(\sigma \circ \tau \circ \sigma^{-1})$. Como estamos tomando apenas automorfismos de ordem p, este automorfismo não é o automorfismo identidade, logo r e s não são simultaneamente nulos no primeiro caso.

Analogamente ao que foi feito com $C_{p^2} \times C_p$, vamos analisar os automorfismos não triviais de ordem p de $C_p \times C_p \times C_p$. Neste caso teremos $Aut(C_p \times C_p \times C_p) \simeq GL(3; \mathbb{F}_p)$.

Novamente, usando o Teorema 1.15 e o fato de que estamos considerando os automorfismos de ordem p, temos que os autovalores da matrizes associadas são iguais a 1. Com isso, elas são conjugadas a

$$\begin{pmatrix} 1 & 0 & 0 \\ 1 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \text{ ou } \begin{pmatrix} 1 & 0 & 0 \\ 1 & 1 & 0 \\ 0 & 1 & 1 \end{pmatrix}.$$

Outro resultado que será útil neste trabalho diz respeito à ordem do grupo de automorfismos de $C_p \times C_p = \langle x, y \rangle$. Para obtermos informações sobre um automorfismo, basta saber como ele age em cada gerador do grupo. Dado $\tau \in Aut(C_p \times C_p)$, sabemos que $\tau(x) = x^a y^b$ e $\tau(y) = x^c y^d$ para naturais $0 \leq a, b, c, d \leq p-1$.

Primeiramente, temos $p^2 - 1$ opções de escolhas para a e b, já que eles podem assumir quaisquer valores exceto ambos simultaneamente nulos. Para a imagem de y temos $p^2 - p$ opções de escolhas para c e d, já que eles não podem assumir os valores dos elementos gerados pela imagem de x.

Logo, $|Aut(C_p \times C_p)| = (p^2 - 1)(p^2 - p) = p(p-1)^2(p+1)$.

1.4 Classificações iniciais

Recordemos que, pelo teorema de classificação dos grupos abelianos finitos, um grupo finito G é abeliano se e somente se é produto direto de grupos cíclicos com ordem potência de primos.

Desta forma, usando o Teorema 1.4, podemos concluir que se um grupo tem ordem p^2 então ele é isomorfo a

$$C_{p^2} \quad \text{ou} \quad C_p \times C_p.$$

Agora apresentaremos uma classificação para os grupos de ordem p^3.

Se G tem ordem p^3 e é abeliano, a classificação dos grupos abelianos finitos nos diz que:

$$G \simeq C_{p^3} \qquad \text{ou} \qquad G \simeq C_{p^2} \times C_p \qquad \text{ou} \qquad G \simeq C_p \times C_p \times C_p.$$

Para G não abeliano de ordem p^3, analisamos separadamente os casos em que $p = 2$ e $p \neq 2$.

Teorema 1.16. Seja G um grupo não abeliano de ordem 8. Então $G \simeq D_8$ ou $G \simeq Q_8$, onde:

$D_8 = \langle a, b \mid a^4 = b^2 = 1,\ a^b = a^{-1} \rangle$ (grupo diedral de ordem 8)

$Q_8 = \langle a, b \mid a^4 = 1,\ b^2 = a^2,\ a^b = a^{-1} \rangle$ (grupo dos quatérnios).

Demonstração. Como G é não abeliano, não temos nenhum elemento de ordem 8 em G e pelo menos um elemento de ordem 4, já que se todo elemento não trivial de G tem ordem 2 então G é abeliano.

Seja a um elemento de ordem 4 e defina $A := \langle a \rangle \lhd G$. Então para qualquer $b \in G \backslash A$ temos $G = \langle a, b \rangle$.

Como $[G : A] = 2$, temos que $b^2 \in A$. Mas se $b^2 = a$ ou $b^2 = a^3$, então a ordem de b seria 8, o que não pode acontecer. Logo, $b^2 = 1$ ou $b^2 = a^2$.

Como $A \lhd G$, temos que $a^b \in A$. Mas $a^b \neq 1$ pois $a \neq 1$, $a^b \neq a$ pois G é não abeliano e $a^b \neq a^2$ pois se $a^b = a^2$ teríamos $a = a^{(b^2)} = b^2ab^{-2} = (a^b)^b = (a^2)^b$, mas $(a^2)^b = (a^b)^2 = a^4 = 1$, uma contradição. Logo, nos resta que $a^b = a^3 = a^{-1}$.

Com isso, concluímos que que se $b^2 = 1$ então $G \simeq D_8$ e se $b^2 = a^2$ então $G \simeq Q_8$. $\square$

Teorema 1.17. Seja G um grupo não abeliano de ordem p^3, onde $p \neq 2$. Então $G \simeq G_1$ ou $G \simeq G_2$, onde:

$G_1 = \langle a, b \mid a^{p^2} = b^p = 1,\ bab^{-1} = a^{1+p} \rangle \simeq C_{p^2} \rtimes C_p$

$G_2 = \langle a, b, c \mid a^p = b^p = c^p = 1,\ ab = cba,\ ca = ac,\ cb = bc \rangle \simeq (C_p \times C_p) \rtimes C_p.$

Demonstração. Como G é um grupo não abeliano, não temos nenhum elemento de ordem p^3 em G. Então vamos analisar dois casos, se G possui elemento de ordem p^2 ou se todo elemento não trivial de G tem ordem p.

Se G possui um elemento a de ordem p^2, definimos $A := \langle a \rangle$, que é normal em G pois tem índice p. Então tomando qualquer $b_1 \in G \backslash A$, temos $G = \langle a, b_1 \rangle$. Como $[G : A] = p$, temos $b_1^p \in A$ e $b_1 a b_1^{-1} = a^r$ para algum $1 < r < p^2$; portanto, $b_1^j a b_1^{-j} = a^{r^j}$ para todo j. Em particular, como $b_1^p \in A$ e A é abeliano, temos $a = b_1^p a b_1^{-p} = a^{r^p}$. Além disso, a ordem de a é p^2 logo devemos ter $r^p \equiv 1 \pmod{p^2}$.

Pelo Teorema de Fermat $r^p \equiv r \pmod{p}$, e com essas duas equivalências concluímos que $r \equiv 1 \pmod{p}$. Então podemos escrever $r = 1 + sp$, com $s \in \mathbb{N}$.

Como $1 < r < p^2$ segue que s e p são coprimos; logo podemos escolher $k \in \mathbb{N}$ de modo que $ks \equiv 1 \pmod{p}$.

Usando novamente que a ordem de a é p^2, temos: $b_1^k a b_1^{-k} = a^{(1+sp)^k} = a^{1+ksp} = a^{1+p}$. Como k e p são coprimos, temos $b_1^k \notin A$ e podemos trocar b_1 por $b_2 := b_1^k$ e temos $G = \langle a, b_2 \rangle$, onde $b_2 a b_2^{-1} = b_1^k a b_1^{-k} = a^{1+p}$. Segue daí que $b_2 a^i b_2^{-1} = (b_2 a b_2^{-1})^i = (a^{1+p})^i = a^{i(1+p)}$. Como $b_2^p = b_1^{kp} \in A$ e a ordem de b_2 é diferente de p^3 temos que $b_2^p = a^t$, onde t é múltiplo de p.

Nestas condições escrevemos $b_2^p = a^{up}$ e encontramos:

$$(b_2^{-1}a^u)^p = b_2^{-p} a^{u[1+(p+1)+(p+1)^2+\ldots+(p+1)^{p-1}]} = b_2^{-p} a^{up+up[1+2+\ldots+(p-1)]} = b_2^{-p} a^{up} = 1,$$

pois $\sum_{i=1}^{p-1} i = p(p-1)/2$, p é ímpar e $|a| = p^2$. Portanto, com $b := b_2^{-1} a^u$, temos que $bab^{-1} = b_2^{-1} a^u a a^{-u} b_2 = b_2 a b_2^{-1} = a^{1+p}$, e então $G \simeq G_1$.

Se G não possui elemento de ordem p^2, todo elemento não trivial tem ordem p. Tome $a \in G$ e $b \in G \backslash \langle a \rangle$, então $a^p = b^p = 1$. Agora, como $|G| = p^3$, sabemos que $|Z(G)|$ só pode assumir os valores p ou p^3. Mas G é não abeliano, logo $|Z(G)| = p$.

Notamos agora que, como o grupo $G/Z(G)$ tem ordem p^2, ele é abeliano; com isso, $G' \leq Z(G)$. Considere $c = aba^{-1}b^{-1} \in G' \leq Z(G)$, então $\langle c \rangle \leq Z(G)$. Se $c = 1$, temos que a e b comutam, donde $G = \langle a, b, Z(G) \rangle$ é abeliano. Um absurdo! Então $c \neq 1$, donde $\langle c \rangle = Z(G)$, pois $c^p = 1$. Com isso, temos $G \simeq G_2$. □

Capítulo 2

Alguns tipos especiais de p-grupos

Seria muito interessante se pudéssemos classificar todos os p-grupos finitos, mas mesmo com os grandes avanços na teoria de grupos essa tarefa se mostrou demasiadamente complexa. Então podemos tentar classificar p-grupos finitos com alguma propriedade adicional. Começamos com a classificação de p-grupos finitos que contém um subgrupo maximal cíclico. Usamos [4] e [11] como principais referências para as demonstrações neste capítulo.

2.1 p-Grupos finitos contendo um subgrupo maximal cíclico

No caso abeliano, p pode ser um primo qualquer.

Teorema 2.1. G é um grupo abeliano de ordem p^n contendo um subgrupo cíclico de ordem p^{n-1} se, e somente se, G é de um dos seguintes tipos:

1. $G \simeq C_{p^n}$
2. $G \simeq C_{p^{n-1}} \times C_p$.

Demonstração. Claramente, os dois tipos de grupos apresentados possuem um subgrupo cíclico de ordem p^{n-1}.

Agora, suponha que G satisfaz as hipóteses do teorema e considere N um subgrupo cíclico de ordem p^{n-1} de G, digamos $N = \langle a \rangle$. Como $[G : N] = p$, temos que $N \lhd G$. Além disso, $G/N \simeq \mathbb{C}_p$ e então para qualquer $x \in G \backslash N$ temos que $G/N = \langle xN \rangle$. Então $G = \langle a, x \rangle$, onde $|a| = p^{n-1}$ e $x^p \in N$, ou seja, $x^p = a^i$ para algum $i \in \{1, 2, ..., p^{n-1}\}$.

Se p não divide i, então a^i também gera N. Então $N = \langle a \rangle = \langle a^i \rangle = \langle x^p \rangle$ e, com isso, podemos escrever a como uma potência de x. Portanto $G = \langle a, x \rangle = \langle x \rangle$, com $|x| = p^n$, pois $|x^p| = p^{n-1}$. Então G é do tipo **1**.

Se p divide i, então $x^p = a^i = a^{cp}$ para algum $c \in \mathbb{N}$. Tome $b = xa^{-c}$. Então $b^p = (xa^{-c})^p = x^p a^{-cp} = 1$, pois G é abeliano. Como $x \in G \backslash N$, então $b \in G \backslash N$ e $G = \langle a \rangle \times \langle b \rangle$. Então G é do tipo **2**. □

Agora, vamos tratar o caso não abeliano em que p é um primo ímpar.

Teorema 2.2. *G é um grupo não abeliano de ordem p^n, com p ímpar, contendo um subgrupo cíclico de ordem p^{n-1} se, e somente se,*

3 $G \simeq M_{p^n} = \left\langle a, b \mid a^{p^{n-1}} = b^p = 1,\ a^b = a^{p^{n-2}+1} \right\rangle$.

Demonstração. Claramente, M_{p^n} possui um subgrupo cíclico de ordem p^{n-1}.

Agora, suponha que G satisfaz as hipóteses do teorema e considere N um subgrupo cíclico de ordem p^{n-1} de G, digamos $N = \langle a \rangle$. Como $[G : N] = p$, temos que $N \lhd G$. Além disso, $G/N \simeq \mathbb{C}_p$ e então para qualquer $x \in G \backslash N$ temos que $G/N = \langle xN \rangle$. Então $G = \langle a, x \rangle$, onde $|a| = p^{n-1}$ e $x^p \in N$, ou seja, $x^p = a^i$ para algum $i \in \{1, 2, ..., p^{n-1}\}$. Como G é não abeliano, temos $n \geq 3$ e $[G : Z(G)] > p$, pela Observação 1.3.

O elemento x induz um automorfismo $\tau_x : N \to N$ por conjugação $\tau_x(a) = a^x$. Como um automorfismo deve levar gerador em gerador, temos $\tau_x(a) = a^x = a^m$, para algum $m \in \mathbb{N}$ tal que $(m, p) = 1$ e $1 < m < p^{n-1}$.

Este automorfismo tem ordem p, pois $\tau_x^p(a) = a^{m^p} = a^{x^p} = a^{a^i} = a$, então $m^p \equiv 1 \pmod{p^{n-1}}$. Pelo Pequeno Teorema de Fermat $m^{p-1} \equiv 1 \pmod{p}$, então segue que $m \equiv 1 \pmod{p}$ e podemos escrever $m = 1 + kp^i$, onde $(k,p) = 1$ e $0 < i < n-1$.

Agora, $m^p = (1+kp^i)^p = 1 + \binom{p}{1}kp^i + \binom{p}{2}k^2p^{2i} + ... + \binom{p}{p}k^pp^{pi}$, e como p^{i+2} divide $\binom{p}{2}k^2p^{2i} + ... + \binom{p}{p}k^pp^{pi}$ temos $m^p \equiv 1 + kp^{i+1} \pmod{p^{i+2}}$, donde $m^p - 1 = kp^{i+1} + lp^{i+2}$. Mas $m^p \equiv 1 \pmod{p^{n-1}}$, então $m^p - 1 = l'p^{n-1}$. Portanto, $kp^{i+1} + lp^{i+2} = l'p^{n-1}$. Se $i+1 < n-1$, dividimos tudo por p^{i+1} e teremos $k \equiv 0 \pmod{p}$. ABSURDO, pois $(k,p) = 1$. Então $i+1 = n-1$ e temos $m = 1 + kp^{n-2}$.

Como $(k,p) = 1$, existe k' tal que $kk' \equiv 1 \pmod{p}$, ou seja, $kk' = 1 + dp$, para algum $d \in \mathbb{N}$. Assim, $a^{x^{k'}} = a^{m^{k'}} = a^{(1+kp^{n-2})^{k'}} = a^{1+\binom{k'}{1}kp^{n-2}+...+\binom{k'}{k'}k^{k'}p^{k'(n-2)}}$. Como p^{n-1} divide $\binom{k'}{2}k^2p^{2(n-2)} + ... + \binom{k'}{k'}k^{k'}p^{k'(n-2)}$ e $|a| = p^{n-1}$, temos $a^{x^{k'}} = a^{1+k'kp^{n-2}} = a^{1+(1+dp)p^{n-2}} = a^{1+p^{n-2}+dp^{n-1}} = a^{1+p^{n-2}}$. Então podemos trocar x por $x^{k'}$ e assumir $m = 1 + p^{n-2}$.

Agora, a^p centraliza a e x, pois $(a^p)^a = a^p$ e $(a^p)^x = (a^x)^p = (a^{1+p^{n-2}})^p = a^{p+p^{n-1}} = a^p$. Então $a^p \in Z(G)$, donde $\langle a^p \rangle \leq Z(G) \leq G$. Além disso $[G : \langle a^p \rangle] = p^2$ e $[G : Z(G)] > p$, logo devemos ter $Z(G) = \langle a^p \rangle$. Portanto, G é nilpotente de classe 2.

Agora, $x^p \in N$, mas não o gera, já que se gerasse, G seria cíclico. Então $x^p \in \langle a^p \rangle$, donde $x^p = a^{jp}$ para algum j. Tome $b = xa^{-j}$. Temos que $[a^j, x] = a^j(a^{-j})^x = a^j(a^x)^{-j} = a^j(a^{1+p^{n-2}})^{-j} = a^{-jp^{n-2}}$. Então $[a^j, x] \in \langle a^p \rangle = Z(G)$. Então $b^p = x^pa^{-jp}[a^j, x]^{1+2+...+p-1} = x^pa^{-jp}[a^j, x]^{\binom{p}{2}} = 1(a^{-jp^{n-2}})^{\binom{p}{2}} = 1$, pois $[a^j, x] \in Z(G)$ e, como p é ímpar, p divide $\binom{p}{2}$. Além disso, $a^b = bab^{-1} = xa^{-j}aa^jx^{-1} = xax^{-1} = a^x = a^{1+p^{n-2}}$.

Então $G \simeq M_{p^n}$. □

Por fim, temos o caso em que G é não abeliano de ordem 2^n.

Teorema 2.3. *G é um grupo não abeliano de ordem 2^n contendo um subgrupo cíclico de ordem 2^{n-1} se, e somente se, G é de um dos seguintes tipos:*

4. $G \simeq D_{2^n} = \left\langle a, b \mid a^{2^{n-1}} = b^2 = 1,\ a^b = a^{-1} \right\rangle,\ n \geq 3$

5. $G \simeq Q_{2^n} = \left\langle a, b \mid a^{2^{n-1}} = 1,\ b^2 = a^{2^{n-2}},\ a^b = a^{-1} \right\rangle,\ n \geq 3$

6. $G \simeq M_{2^n} = \left\langle a, b \mid a^{2^{n-1}} = b^2 = 1,\ a^b = a^{2^{n-2}+1} \right\rangle,\ n > 3$

7. $G \simeq SD_{2^n} = \left\langle a, b \mid a^{2^{n-1}} = b^2 = 1,\ a^b = a^{2^{n-2}-1} \right\rangle,\ n > 3.$

Demonstração. Claramente, os quatro tipos de grupos apresentados possuem um subgrupo cíclico de ordem 2^{n-1}.

Agora, suponha que G satisfaz as hipóteses do teorema e considere N um subgrupo cíclico de ordem 2^{n-1} de G, digamos $N = \langle a \rangle$. Como $[G : N] = 2$, temos que $N \lhd G$. Além disso, $G/N \simeq C_2$ e então para qualquer $x \in G \backslash N$ temos $x^2 \in N$, ou seja, $x^2 = a^i$ para algum $i \in \{1, 2, ..., 2^{n-1}\}$ e $G = \langle a, x \rangle$, onde $|a| = 2^{n-1}$. Novamente, como G é não abeliano, temos $n \geq 3$.

Se $n = 3$, temos $|a| = 4$ e então N possui um único automorfismo não trivial: para qualquer $b \notin N$ temos $G = \langle a, b \rangle$ e $\tau_b : N \to N$ satisfaz $\tau_b(a) = a^b = a^{-1}$. Novamente $b^2 \in N$, mas não o gera pois já que se gerasse, G seria cíclico. Então $b^2 \in \langle a^2 \rangle$, donde $b^2 = 1$ ou $b^2 = a^2$.

Se $b^2 = 1$, G é do tipo **4**, com $n = 3$.

Se $b^2 = a^2$, G é do tipo **5**, com $n = 3$.

Se $n > 3$ temos que $\tau_x : N \to N$ satisfaz $\tau_x(a) = a^x = a^m$, onde m é ímpar, digamos $m = 2k+1$. De $m^2 \equiv 1 \pmod{2^{n-1}}$ segue que 2^{n-1} divide $m^2 - 1 = 4k(k+1)$ e então 2^{n-3} divide $k(k+1)$. Donde $k \equiv 0 \pmod{2^{n-3}}$ ou $k \equiv 0 \pmod{2^{n-3}}$. Como $1 < m < 2^{n-1}$, temos $k < 2^{n-2}$.

Se $k \equiv 0 \pmod{2^{n-3}}$, temos $k = l2^{n-2}$. Se l é par, contradiz a condição $k < 2^{n-2}$. Então l é ímpar, e $m = 2k + 1 = l2^{n-2} + 1$.

Se $k \equiv -1 \pmod{2^{n-3}}$, temos $k = l2^{n-3}-1$, donde $m = 2k+1 = 2(l2^{n-3}-1)+1 = l2^{n-2}-2+1 = l2^{n-2}-1$.

No primeiro caso, trocando novamente x por uma potência apropriada (como fizemos no caso em que p é ímpar), podemos assumir que $m = 2^{n-2}+1$. Enquanto no segundo caso, ou l é ímpar e podemos assumir $m = 2^{n-2}-1$, ou l é par e podemos assumir $m = 2^{n-1}-1$.

Existem, portanto, três casos a examinar.

Se $m = 2^{n-1}-1$, então $a^x = a^m = a^{-1}$, pois $|a| = 2^{n-1}$. Além disso, $x^2 \in N$ mas não o gera, portanto, $a^{2i} = x^2 = (x^2)^x = (a^{2i})^x = (a^x)^{2i} = a^{-2i}$, donde $a^{4i} = a^0 = a^{2^{n-1}}$, com isso $i = 0$ ou $i = 2^{n-3}$.

Se $i = 0$, temos $x^2 = 1$. Então G é do tipo **4**, com $n > 3$.

Se $i = 2^{n-3}$, temos $x^2 = a^{2^{n-2}}$. Então G é do tipo **5**, com $n > 3$.

Se $m = 2^{n-2}+1$, então $a^x = a^m = a^{2^{n-2}+1}$. Além disso, $x^2 \in N$ mas não o gera, portanto, $x^2 = a^{2i}$. Tome $y = a^{i(2^{n-3}-1)} \neq 1$, pois $n > 3$ e $b = yx$. Então

$$\begin{aligned}
b^2 &= (yx)^2 = y^2x^2[x,y] = a^{2i(2^{n-3}-1)}a^{2i}y^xy^{-1} = \\
&= a^{2i(2^{n-3}-1)+2i}(a^{i(2^{n-3}-1)})^x a^{-i(2^{n-3}-1)} = \\
&= a^{2i(2^{n-3}-1)+2i-i(2^{n-3}-1)}(a^x)^{i(2^{n-3}-1)} = \\
&= a^{i(2^{n-3}-1)+2i}(a^{2^{n-2}+1})^{i(2^{n-3}-1)} = \\
&= a^{i(2^{n-3}-1)+2i}a^{(2^{n-2}+1)i(2^{n-3}-1)} = \\
&= a^{i(2^{n-3}-1)(1+2^{n-2}+1)+2i} = \\
&= a^{i(2^{n-3}-1)(2^{n-2}+2)+2i} = \\
&= a^{i(2^{2n-5}+2^{n-2}-2^{n-2}-2+2)}
\end{aligned}$$

Então $b^2 = a^{i.2^{2n-5}} = a^{i.2^{n-4+n-1}} = (a^{2^{n-1}})^{r.2^{n-4}} = 1$ e G é do tipo **6**.

Se $m = 2^{n-2} - 1$, então $a^x = a^m = a^{2^{n-2}-1}$. Além disso, $x^2 \in N$ mas não o gera, portanto,

$$a^{2i} = x^2 = (x^2)^x = (a^{2i})^x = (a^x)^{2i} = (a^{2^{n-2}-1})^{2i} = a^{2i(2^{n-2}-1)} = a^{i2^{n-1}-2i},$$

donde $a^{4i} = a^0 = a^{2^{n-1}}$ e então $i = 0$ ou $i = 2^{n-3}$.

Se $i = 0$ então $x^2 = 1$ e G é do tipo **7**.

Se $i = 2^{n-3}$ então $x^2 = a^{2^{n-2}}$. Neste caso, trocamos x por $y = ax$ e então

$$\begin{aligned} y^2 &= (ax)^2 = axax = axax^{-1}xx = a.a^x.x^2 = a.a^{2^{n-2}-1}.a^{2^{n-2}} \\ &= a^{2^{n-2}+2^{n-2}} = a^{2^{n-1}} = 1. \end{aligned}$$

Temos também $a^y = a^{ax} = (ax)a(ax)^{-1} = axax^{-1}a^{-1} = a.a^x.a^{-1} = a^{1+2^{n-2}-1-1} = a^{2^{n-2}-1}$. Então, novamente, G é do tipo **7**.

Os grupos apresentados são não isomorfos. Para verificar isso observe que Q_{2^n} possui um único elemento de ordem 2, M_{2^n} possui 3 elementos de ordem 2, são eles: b, $a^{2^{n-2}}$ e $ba^{2^{n-2}}$. Em D_{2^n}, além de b e $a^{2^{n-2}}$ todo elemento da forma ba^i tem ordem 2. Já em SD_{2^n}, além de b e $a^{2^{n-2}}$ todo elemento da forma ba^{2j} tem ordem 2.

□

Podemos, então, reunir todas estas classificações no seguinte resultado.

Teorema 2.4. *G é um grupo de ordem p^n contendo um subgrupo cíclico de ordem p^{n-1} se, e somente se, G é de um dos seguintes tipos:*

1. $G \simeq C_{p^n}$
2. $G \simeq C_{p^{n-1}} \times C_p$
3. $G \simeq M_{p^n} = \left\langle a, b \mid a^{p^{n-1}} = b^p = 1,\ a^b = a^{p^{n-2}+1} \right\rangle,\ n \geq 3,\ p \neq 2$
4. $G \simeq D_{2^n} = \left\langle a, b \mid a^{2^{n-1}} = b^2 = 1,\ a^b = a^{-1} \right\rangle,\ n \geq 3$

5. $G \simeq Q_{2^n} = \left\langle a, b \mid a^{2^{n-1}} = 1,\ b^2 = a^{2^{n-2}},\ a^b = a^{-1} \right\rangle,\ n \geq 3$

6. $G \simeq M_{2^n} = \left\langle a, b \mid a^{2^{n-1}} = b^2 = 1,\ a^b = a^{2^{n-2}+1} \right\rangle,\ n > 3$

7. $G \simeq SD_{2^n} \simeq \left\langle a, b \mid a^{2^{n-1}} = b^2 = 1,\ a^b = a^{2^{n-2}-1} \right\rangle,\ n > 3.$

2.2 p-Grupos finitos que contém um único subgrupo cíclico de ordem p

Agora vamos fazer a classificação de p-grupos finitos que contém um único subgrupo cíclico de ordem p.

Teorema 2.5. Um grupo G de ordem p^n tem exatamente um subgrupo cíclico de ordem p se, e somente se, $G \simeq C_{p^n}$ ou $G \simeq Q_{2^n}$.

Demonstração. Primeiramente, C_{p^n} e Q_{2^n} têm exatamente um subgrupo cíclico de ordem p, logo a recíproca é imediata.

Seja agora um grupo G de ordem p^n que tem exatamente um subgrupo cíclico de ordem p.

Se G é abeliano, o teorema de classificação dos grupos abelianos finitos nos diz que G tem que ser cíclico, caso contrário teria mais de um subgrupo cíclico de ordem p.

Suponha que G é não abeliano, com isso devemos ter $n \geq 3$, já que grupos de ordem p e p^2 são abelianos.

Se $n = 3$, a classificação dos grupos não abelianos de ordem p^3 nos diz que G deve ser isomorfo a um dos seguintes grupos: D_8 ou Q_8 (se $p = 2$), $(C_p \times C_p) \rtimes C_p$ ou $C_{p^2} \rtimes C_p$ (se $p \neq 2$). Então temos que $G \simeq Q_8$, já que todas as outras opções têm mais de um grupo cíclico de ordem p.

Para terminar a demonstração usaremos indução sobre a ordem de G. Suponha p ímpar e seja H um subgrupo maximal de G. O teorema é válido para G não abeliano com $n = 3$. Nossa hipótese de indução é que ele seja válido para todo grupo com ordem

menor que p^n. Logo, o teorema vale para H, e como estamos supondo p ímpar então $H \not\simeq Q_{2^m}$, logo H é cíclico. Então G atende às hipóteses do Teorema 2.2 e concluímos que $G \simeq M_{p^n}$. Mas M_{p^n} tem mais de um subgrupo cíclico de ordem p. Com isso, p não pode ser ímpar no caso G não abeliano. Portanto, $p = 2$.

Assim, G é um grupo de ordem 2^n com exatamente um subgrupo cíclico de ordem 2. Este subgrupo é normal e abeliano, portanto G tem um subgrupo normal abeliano maximal não trivial. Seja A um subgrupo normal abeliano maximal de G de ordem 2^m. Usando a hipótese de indução A é cíclico, pois é abeliano. Digamos que A seja gerado por a. Pelo Teorema 1.12, $A = C_G(A)$. Seja xA um elemento de G/A com ordem 2. Então $\langle x, A\rangle$ é não abeliano e tem um subgrupo maximal cíclico. Então, pelo Teorema 2.3, $\langle x, A\rangle \simeq Q_{2^{m+1}}$ é um quatérnio generalizado, já que todas as outras opções ($D_{2^{m+1}}$, $M_{2^{m+1}}$ e $SD_{2^{m+1}}$) têm mais de um subgrupo de ordem 2. Daí, $a^x = a^{-1}$, o que implica que G/A tem apenas um elemento de ordem 2. De fato, se G/A tivesse outro elemento yA de ordem 2, por argumento análogo teríamos $a^y = a^{-1}$ e assim

$$a^x = a^y \Rightarrow a^{xy^{-1}} = a \Rightarrow xy^{-1} \in C_G(A) = A \Rightarrow xA = yA.$$

Agora, pelo Teorema 1.13, $N_G(A)/C_G(A) = G/A$ é isomorfo a um subgrupo de $Aut(A)$ e, pelo Teorema 1.14, $Aut(A) \simeq U(\mathbb{Z}_{2^m})$. Daí, G/A é abeliano e $|G/A|$ divide $|Aut(A)| = |U(\mathbb{Z}_{2^m})| = 2^{m-1}$ e portanto $m > 1$. Como $|G/A| < |G|$, e G/A é abeliano, pela hipótese de indução, temos que G/A é cíclico. Pelos isomorfismos citados acima temos $xA \leftrightarrow Int_x \leftrightarrow -1$. Como -1 não é um quadrado módulo 2^m, pois $m > 1$, concluímos que G/A tem ordem 2. Portanto, $G = \langle x, a\rangle \simeq Q_{2^n}$. □

Capítulo 3

Classificação de grupos de ordem p^4

Otto Ludwig Hölder (1859-1937) e Jacob William Albert Young (1865-1948) classificaram, independentemente, em 1893 os grupos de ordem p^4. Em 2005, Marcel Wild classificou de maneira simples os 14 grupos de ordem 16 usando o conceito de extensões tipo e o Teorema da Extensão Cíclica para o qual ainda não havia uma demonstração simples.

Em maio de 2006, Michael Garlow, seguindo os passos de Wild, apresentou em sua tese de mestrado uma demonstração elementar para tal teorema e uma classificação, também simples, dos grupos de ordem 81. Pouco tempo depois, em julho de 2006, Michael Garlow juntamente com seu orientador Jeffrey D Adler e Ethel R Wheland apresentaram um preprint classificando os grupos de ordem p^4 para $p \neq 2$ também usando extensões tipo.

3.1 Extensões cíclicas

Definição 3.1. Se um grupo finito G possui um subgrupo normal $N \lhd G$, tal que o quociente G/N é isomorfo ao grupo cíclico de ordem n, dizemos que G é uma extensão cíclica de N.

Exemplo 3.2. O grupo de simetrias do hexágono $G = D_6 = \langle x, y | x^6 = y^2 = (xy)^2 = 1 \rangle$ possui um subgrupo normal $N = \langle x^2, y \rangle$ isomorfo ao grupo de permutações de três elementos S_3. Como o quociente G/N tem ordem 2, temos G/N cíclico. Logo, G é uma extensão cíclica de N.

Se tomarmos qualquer $a \in G \backslash N$ tal que a classe aN gere G/N, temos que $v := a^n \in N$. Além disso, podemos definir o automorfismo $\tau \in Aut(N)$, que age via conjugação por a. Então $\tau(v) = ava^{-1} = aa^n a^{-1} = a^n$. Em outras palavras, τ fixa v. Também, para $x \in N$, vale $\tau^n(x) = a^n x a^{-n} = vxv^{-1}$. Isto é, $\tau^n = Int_v$. Em particular, se N é um grupo abeliano, então τ^n é o automorfismo identidade.

Cabe então a pergunta: Será que o grupo G fica totalmente determinado por um subgrupo normal N, um número natural n, um automorfismo $\tau \in Aut(N)$ e um elemento $v \in N$? Isto nos motiva a seguinte definição:

Definição 3.3. Uma extensão tipo para um grupo N é uma quádrupla (N, n, τ, v), onde $n \in \mathbb{N}$, $v \in N$, e $\tau \in Aut(N)$ são tais que $\tau(v) = v$ e $\tau^n = Int_v$.

Exemplo 3.4. $(S_3, 2k, \tau, 1)$, $(S_3, 2k+1, \tau, \alpha)$, onde α é um elemento de ordem 2 de S_3, τ é o automorfismo que age via conjugação por α, e $k \in \mathbb{N}$.

Exemplo 3.5. $(S_3, 3k, \tau, 1)$, $(S_3, 3k+1, \tau, \beta)$, $(S_3, 3k+2, \tau, \beta^2)$, onde β é um elemento de ordem 3 de S_3, τ é o automorfismo que age via conjugação por β, e $k \in \mathbb{N}$.

Note que se tivermos um grupo G que é extensão cíclica de N, podemos tomar um elemento $a \in G \backslash N$ tal que aN gere G/N e obteremos uma extensão tipo (N, n, τ, v) como acima.

Definição 3.6. Dizemos que uma extensão tipo (N, n, τ, v) determina o grupo G quando G for extensão cíclica de ordem n de um grupo M, existir um isomorfismo $\phi : M \to N$ e um elemento $a \in G \backslash M$ tal que aM gere G/M, $\phi(a^n) = v$ e $\phi^{-1} \circ \tau \circ \phi = Int_a|_M$.

Segue desta definição que se existe um isomorfismo $\varphi : N_1 \to N_2$ e (N_1, n, τ, v) determina o grupo G, então $(N_2, n, \varphi \circ \tau \circ \varphi^{-1}, \varphi(v))$ também determina G.

Teorema 3.7. (Teorema da Extensão Cíclica): Cada extensão tipo (N, n, τ, v) determina um grupo.

Demonstração. Seja C o grupo cíclico infinito gerado pelo elemento w e tome $G = C \ltimes_\tau N/\langle w^n v^{-1} \rangle$. Como $w^n v^{-1}$ é central, o subgrupo $\langle w^n v^{-1} \rangle$ é normal em $C \ltimes_\tau N$ e a extensão tipo (N, n, τ, v) determina G. □

Este teorema nos garante que uma extensão tipo determina pelo menos um grupo. Mas, mais que isso, a extensão tipo determina G a menos de isomorfismo. Uma vez que se G_2 é um outro grupo determinado por (N, n, τ, v), ele possuirá um subgrupo M isomorfo a N e um elemento $a \in G_2 \backslash M$ tal que aM gera G_2/M. Se φ é o isomorfismo entre M e N, definimos $\psi : G_2 \longrightarrow G$ como $\psi(a^i v^j) = w^i \varphi(v)^j$ que é também um isomorfismo.

3.2 Equivalências de extensões tipo

A partir de agora, vamos considerar p um primo ímpar, a menos que seja dito algo contrário. Lembre-se que pelo Teorema de Sylow cada grupo G de ordem p^4 possui um subgrupo de ordem p^3, e este é normal pelo Teorema 1.5. Assim, para que possamos construir todos os grupos de ordem p^4, seria suficiente construir todas as extensões tipo (N, p, τ, v), onde N é um grupo de ordem p^3.

Contudo, o número de tais extensões tipo é grande e muitas vezes elas determinam grupos isomorfos. Apresentamos então algumas técnicas para identificar quando isso acontece e limitar nossa coleção de extensões tipo.

Definição 3.8. Dizemos que duas extensões tipo (N, n, τ, v) e (M, m, σ, w) são equivalentes se elas determinam o mesmo grupo (a menos de isomorfismo).

Exemplo 3.9. $(S_3, 2, \tau, x^2)$, onde $S_3 \simeq \langle x, y \mid x^3 = y^2 = xyxy = 1\rangle$ e $\tau = Int_b$, determina D_6, pois em $C \ltimes_\tau S_3/\langle w^2x^{-2}\rangle$ temos $w^2 = x^2$, donde $w^6 = x^6 = 1$; $y^2 = 1$; e também $(yw)^2 = y\tau(y)x^2 = yInt_x(y)x^2 = yxyx^{-1}x^2 = 1$. Portanto, $C \ltimes_\tau S_3/\langle w^2x^{-2}\rangle \simeq D_6 = \langle a, b \mid a^6 = b^2 = (ab)^2 = 1\rangle$

Além disso $(C_6, 2, \sigma, 1)$, onde $\sigma : d \mapsto d^5$, d um gerador de C_6, também determina D_6, pois em $C \ltimes_\sigma C_6/\langle w^2\rangle$ temos $d^6 = 1$; $w^2 = 1$; e $(dw)^2 = d\sigma(d)1 = dd^5 = 1$. Assim, $C \ltimes_\sigma C_6/\langle w^2\rangle \simeq D_6$.

Lema 3.10. Seja N um grupo abeliano finito, seja $n \in \mathbb{N}$, e $i \in \mathbb{Z}$ relativamente primo com $|N|$. Então as extensões tipo (N, n, τ, v) e (N, n, τ, v^i) são equivalentes.

Demonstração. Por hipótese, a aplicação $\varphi : N \to N$ definida por $\varphi(x) = x^i$ tem núcleo trivial, e então é um automorfismo. Para todo $x \in N$, $\varphi(\tau(x)) = (\tau(x))^i = \tau(x^i) = \tau(\varphi(x))$, ou seja, $\varphi\tau = \tau\varphi$.

Seja G o grupo determinado por (N, n, τ, v), então G é extensão cíclica de um grupo M, existe um isomorfismo a $\phi : M \to N$ e um elemento $a \in G\backslash M$ tal que $\phi(a^n) = v$ e $\phi^{-1} \circ \tau \circ \phi = Int_a|_M$.

Então $\varphi \circ \phi : M \to N$ é também um isomorfismo e o elemento $a \in G\backslash M$ satisfaz $\varphi \circ \phi(a^n) = v^i$ e $\phi^{-1} \circ \varphi^{-1} \circ \tau \circ \varphi \circ \phi = \phi^{-1} \circ \tau \circ \phi = Int_a|_M$. Logo (N, n, τ, v^i) também determina G. □

Considere N um grupo. Dado $\tau \in Aut(N)$ e $n \in \mathbb{N}$, definimos a função

$$\begin{aligned} \mathcal{N}_{\tau,n} : \quad & N \longrightarrow N \\ & x \longmapsto \mathcal{N}_{\tau,n}(x) = x\tau(x)\tau^2(x)...\tau^{n-1}(x). \end{aligned}$$

Lema 3.11. Sejam G um grupo, $a \in G$, $N \lhd G$ e $\tau = Int_a|_N$. Então $(xa)^n = \mathcal{N}_{\tau,n}(x)a^n$ para todo $x \in N$.

Demonstração. Temos que

$$\begin{aligned}(xa)^n &= (xa)(xa^{-1}a^2)(xa^{-2}a^3)...(xa^{-(n-1)}a^n) = \\ &= x(axa^{-1})(a^2xa^{-2})...(a^{n-1}xa^{-(n-1)})a^n = \mathcal{N}_{\tau,n}(x)a^n\end{aligned}.$$

□

Dada uma extensão tipo (N_1, n, τ, v) construímos um grupo G como na prova do Teorema 3.7. Escolhendo um subgrupo normal N_2 de índice n em G (frequentemente, mas nem sempre, igual a N_1), e um elemento $a_2 \in G\backslash N_2$ tal que a_2N_2 gere G/N_2, definimos $\sigma = Int_{a_2}|_{N_2}$, e $w = (a_2)^n$. Então obtemos uma extensão tipo (N_2, n, σ, w). Como esta extensão tipo determina G, ela é equivalente a (N_1, n, τ, v).

Lema 3.12. Para $x \in N$, as extensões tipo (N, n, τ, v) e $(N, n, Int_x \circ \tau, \mathcal{N}_{\tau,n}(x)v)$ são equivalentes.

Demonstração. Seja G o grupo determinado por (N, n, τ, v), $G = N \ltimes C/\langle a^n v^{-1}\rangle$, onde a é o gerador de C. Mostraremos que G também é determinado por $(N, n, Int_x \circ \tau, \mathcal{N}_{\tau,n}(x)v)$. Considere $a_2 = xa$ e $\sigma = Int_{a_2}|_N \in Aut(N)$. Para $y \in N$, temos $\sigma(y) = a_2y(a_2)^{-1} = (xa)y(a^{-1}x^{-1}) = x(aya^{-1})x^{-1} = x\tau(y)x^{-1} = Int_x \circ \tau(y)$, então $\sigma = Int_x \circ \tau$. Do lema anterior, $(a_2)^n = \mathcal{N}_{\tau,n}(x)v$. □

Corolário 3.13. Se N é abeliano e $x \in N$ então (N, n, τ, v) e $(N, n, \tau, \mathcal{N}_{\tau,n}(x)v)$ são equivalentes.

Lema 3.14. Se $i \in \mathbb{Z}$ é relativamente primo com n, então as extensões tipo (N, n, τ, v) e (N, n, τ^i, v^i) são equivalentes.

Demonstração. Seja G o grupo determinado por (N, n, τ, v). Esta extensão tipo é dada por escolhas de N e $a \in G\backslash N$. Poderíamos escolher $a^i \in G\backslash N$ e a extensão tipo resultante seria (N, n, τ^i, v^i). □

3.3 A escolha do subgrupo N

Sendo p um primo ímpar, e N um grupo de ordem p^3, a classificação dos grupos de tal ordem nos informa que N deve ser isomorfo a $G \simeq C_{p^3}$ ou $G \simeq C_{p^2} \times C_p$ ou $G \simeq C_p \times C_p \times C_p$, caso seja abeliano e isomorfo a $(C_p \times C_p) \rtimes C_p$ ou $C_{p^2} \rtimes C_p$, caso seja não abeliano. Temos a princípio 5 possibilidades para a escolha de N e nesta seção reduziremos este número.

Teorema 3.15. Todo grupo G de ordem p^4 possui um subgrupo abeliano de ordem p^3.

Demonstração. Se G é abeliano, pelo Teorema de Sylow ele tem um subgrupo de ordem p^3 que é abeliano pois herda essa propriedade de G.

Agora, se G é não abeliano temos $|Z(G)| \neq p^4$. Sabemos que, como $Z(G)$ é um subgrupo de G, $|Z(G)|$ divide p^4. Usando também os resultados do Teorema 1.2 e da Observação 1.3, temos que $|Z(G)|$ somente pode assumir os valores p ou p^2.

Afirmação: G possui um subgrupo normal M de ordem p^2.

Se $|Z(G)| = p^2$, tomemos $M = Z(G)$.

Se $|Z(G)| = p$, então pelo Teorema 1.2, basta procurarmos um subgrupo normal de $\bar{G} = G/Z(G)$ de ordem p. Como $\bar{G}$ é um p-grupo, seu centro possui ordem no mínimo p, logo $Z(\bar{G})$ possui um subgrupo $\bar{M}$ de ordem p. Além disso, $\bar{M} \lhd \bar{G}$. Pelo Teorema 2, $\bar{M}$ é da forma $M/Z(G)$ para algum subgrupo normal M de G. Como $|M/Z(G)| = p$ e $|Z(G)| = p$, concluímos que M tem ordem p^2.

Seja $\Phi : G \longrightarrow Aut(M)$ a ação de G sobre M por conjugação: $\Phi(g) = Int_g : M \longrightarrow M$, onde $Int_g(x) = gxg^{-1}$ para todo elemento $x \in N$.

Afirmação: $M \subset ker(\Phi)$.

Como M tem ordem p^2, M é abeliano. Então consideremos y um elemento qualquer

de M, assim $\Phi(y) = Int_y$ e $Int_y(x) = yxy^{-1} = xyy^{-1} = x$, ou seja, $\Phi(y) = Id$. Portanto, $y \in ker(\Phi)$.

Agora vamos mostrar que $M \neq ker(\Phi)$, e para isso suponha que $M = ker(\Phi)$; logo $|G/ker(\Phi)| = p^2$, pois $|G| = p^4$ e $|M| = p^2$. Sabemos que $G/ker(\Phi) \simeq Im(\Phi)$, que é um subgrupo de $Aut(M)$, então devemos ter que p^2 divide $|Aut(M)|$. Pela classificação dos grupos abelianos finitos, temos $M \simeq C_{p^2}$ ou $M \simeq C_p \times C_p$. Se $M \simeq C_{p^2}$, temos $|Aut(M)| = \phi(p^2) = p^2 - p$ e, se $M \simeq C_p \times C_p$, temos $|Aut(M)| = p(p-1)^2(p+1)$; mas p^2 não divide $|Aut(M)|$ em nenhum destes casos. Logo $M \neq ker(\Phi)$.

Para finalizar, seja $g \in ker(\Phi)\backslash M$. Então $N := \langle g, M\rangle$ é abeliano e tem ordem $\geq p^3$ pois contém M estritamente. Por outro lado, se N tivesse ordem p^4 teríamos $N = G$, mas estamos tratando o caso em que G é não abeliano. Logo, N é o subgrupo abeliano de ordem p^3 de G que queríamos encontrar. □

Este resultado é particularmente importante pois além de limitar o número de escolhas para N, ele também limita nossas escolhas para o automorfismo τ, já que devemos ter $\tau^p = Int_v$ para um elemento $v \in N$, e N ser abeliano implica $Int_v = Id$, o automorfismo identidade.

O número de possibilidades para a escolha de N é apenas 3, uma quantidade razoável. Mas ainda podemos diminuir mais.

Teorema 3.16. Se um grupo não abeliano G de ordem p^4, $p \neq 2$, contém um subgrupo isomorfo a C_{p^3}, então G também contém um subgrupo isomorfo a $C_{p^2} \times C_p$.

Demonstração. Se G é não abeliano de ordem p^4, onde p é ímpar, e que contém um subgrupo isomorfo a C_{p^3} então usando o resultado do Teorema 2.2 temos que $G \simeq \left\langle a, b \mid a^{p^3} = b^p = 1,\ a^b = a^{p^2+1} \right\rangle$.

Então tomando $c = a^p$ temos $c^{p^2} = (a^p)^{p^2} = a^{p^3} = 1$, e também $[b, c] = bcb^{-1}c^{-1} = ba^pb^{-1}a^{-p} = (ba^pb^{-1})a^{-p} = (bab^{-1})^pa^{-p} = (a^{p^2+1})^pa^{-p} = a^{p^3}a^pa^{-p} = 1$.

Logo, $\left\langle c, b \mid c^{p^2} = b^p = [b, c] = 1 \right\rangle \simeq C_{p^2} \times C_p$. □

A partir destes resultados concluímos que precisamos tomar apenas as extensões tipo $(C_{p^2} \times C_p, p, \tau, v)$ e $(C_p \times C_p \times C_p, p, \tau, v)$.

3.4 A escolha do automorfismo τ

Assim como fizemos com a coleção de subgrupos de ordem p^3, precisamos limitar nossa coleção de automorfismos. Para isso usaremos o seguinte resultado.

Lema 3.17. Se $N = C_{p^2} \times C_p$ precisamos apenas considerar os automorfismos de N representados pelas seguintes matrizes:

$$\begin{pmatrix} 1 & p \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1+p & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}, \begin{pmatrix} 1 & p \\ 1 & 1 \end{pmatrix}, \begin{pmatrix} 1 & p\varepsilon \\ 1 & 1 \end{pmatrix}$$

onde ε é um não quadrado módulo p.

Demonstração. Usando as observações feitas na Seção 1.3, precisamos apenas considerar os automorfismos representados pelas matrizes

$$\begin{pmatrix} 1+ps & pr \\ 0 & 1 \end{pmatrix} \text{ ou } \begin{pmatrix} 1+ps & pr \\ 1 & 1 \end{pmatrix},$$

onde $r, s \in \{0, 1, ..., p-1\}$. Lembramos que os elementos da primeira linha de nossas matrizes são dados módulo p^2 e os da segunda linha módulo p.

Primeiramente, analisaremos as matrizes $\begin{pmatrix} 1+ps & pr \\ 0 & 1 \end{pmatrix}$, onde $r, s \in \{0, 1, ..., p-1\}$.

Se $r \neq 0$, podemos tomar $0 < t < p$ tal que $rt \equiv 1 \pmod{p}$. Sabemos que $\begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix} \begin{pmatrix} \alpha & \beta \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}^{-1} = \begin{pmatrix} \alpha-\beta & \beta \\ 0 & 1 \end{pmatrix}$, e aplicando esta conjugação t vezes na matriz $\begin{pmatrix} 1+ps & pr \\ 0 & 1 \end{pmatrix}$ vemos que ela é conjugada a $\begin{pmatrix} 1 & pr \\ 0 & 1 \end{pmatrix}$, que é igual a $\begin{pmatrix} 1 & p \\ 0 & 1 \end{pmatrix}^r$.

Pelo Lema 3.14, nossa matriz $\begin{pmatrix} 1+ps & pr \\ 0 & 1 \end{pmatrix}$, com $r \neq 0$, pode ser substituída pela matriz $\begin{pmatrix} 1 & p \\ 0 & 1 \end{pmatrix}$.

Se $r = 0$, então $s \neq 0$. Sabemos que $\begin{pmatrix} 1+p & 0 \\ 0 & 1 \end{pmatrix}^s = \begin{pmatrix} 1+ps & 0 \\ 0 & 1 \end{pmatrix}$. Então pelo Lema 3.14, $\begin{pmatrix} 1+ps & 0 \\ 0 & 1 \end{pmatrix}$ pode ser substituída por $\begin{pmatrix} 1+p & 0 \\ 0 & 1 \end{pmatrix}$.

Agora, passamos a analisar as matrizes $\begin{pmatrix} 1+ps & pr \\ 1 & 1 \end{pmatrix}$, onde $r, s \in \{0, 1, ..., p-1\}$.

Sabemos que $\begin{pmatrix} 1 & -p \\ 0 & 1 \end{pmatrix} \begin{pmatrix} \alpha & \beta \\ 1 & 1 \end{pmatrix} \begin{pmatrix} 1 & -p \\ 0 & 1 \end{pmatrix}^{-1} = \begin{pmatrix} \alpha - p & \beta \\ 1 & 1 \end{pmatrix}$. Aplicando esta conjugação s vezes na matriz $\begin{pmatrix} 1+ps & pr \\ 1 & 1 \end{pmatrix}$, vemos que ela é conjugada a $\begin{pmatrix} 1 & pr \\ 1 & 1 \end{pmatrix}$. Se $r = 0$ ou $r = 1$, acabou.

Sabemos também que $\begin{pmatrix} 1 & pr \\ 1 & 1 \end{pmatrix}^q = \begin{pmatrix} 1+p\binom{q}{2}r & pqr \\ q & 1 \end{pmatrix}$ para qualquer $0 < q < p$.

Novamente conjugando $\binom{q}{2}r$ vezes esta última matriz por $\begin{pmatrix} 1 & -p \\ 0 & 1 \end{pmatrix}$, concluímos que $\begin{pmatrix} 1+p\binom{q}{2}r & pqr \\ q & 1 \end{pmatrix}$ é conjugada a $\begin{pmatrix} 1 & pqr \\ q & 1 \end{pmatrix}$.

Note agora que $\begin{pmatrix} q & 0 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & pqr \\ q & 1 \end{pmatrix} \begin{pmatrix} q & 0 \\ 0 & 1 \end{pmatrix}^{-1} = \begin{pmatrix} 1 & pq^2r \\ 1 & 1 \end{pmatrix}$, e novamente pelo Lema 3.14, nossa matriz $\begin{pmatrix} 1+ps & pr \\ 1 & 1 \end{pmatrix}$ pode ser substituída pela matriz $\begin{pmatrix} 1 & pr' \\ 1 & 1 \end{pmatrix}$.

Observe que se r' é um quadrado módulo p, podemos considerar $r = 1$ e esta matriz

poderá ser substituída por $\begin{pmatrix} 1 & p \\ 1 & 1 \end{pmatrix}$.

Então no caso geral, basta considerarmos as matrizes $\begin{pmatrix} 1 & pr' \\ 1 & 1 \end{pmatrix}$, onde r' pode ser $0, 1$ ou ε. □

Lema 3.18. Se $N = C_p \times C_p \times C_p$, precisamos considerar apenas os automorfismos representados pelas matrizes

$$\begin{pmatrix} 1 & 0 & 0 \\ 1 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \text{ ou } \begin{pmatrix} 1 & 0 & 0 \\ 1 & 1 & 0 \\ 0 & 1 & 1 \end{pmatrix}.$$

Demonstração. Segue das observações feitas na Seção 1.3. □

3.5 A escolha do elemento v

Para terminar precisamos analisar a escolha do elemento $v \in N$. Para cada um dos sete automorfismos da seção anterior encontraremos um conjunto de elementos v de forma que nossas extensões tipo sejam suficientes para construir todos os grupos não abelianos de ordem p^4.

Vimos que devemos ter $\tau(v) = v$. Então começaremos calculando os pontos fixos de cada automorfismo da seção anterior.

Os pontos fixos de $\begin{pmatrix} 1 & p \\ 0 & 1 \end{pmatrix}$ são da forma $\begin{pmatrix} x^i \\ 0 \end{pmatrix}$, onde $0 \leq i \leq p^2 - 1$.

Os pontos fixos de $\begin{pmatrix} 1+p & 0 \\ 0 & 1 \end{pmatrix}$ são da forma $\begin{pmatrix} x^{pi} \\ y^j \end{pmatrix}$, onde $0 \leq i, j \leq p - 1$.

Os pontos fixos de $\begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}$, também são da forma $\begin{pmatrix} x^{pi} \\ y^j \end{pmatrix}$, onde $0 \leq i, j \leq p - 1$.

Os pontos fixos de $\begin{pmatrix} 1 & p \\ 1 & 1 \end{pmatrix}$, são da forma $\begin{pmatrix} x^{pi} \\ 0 \end{pmatrix}$, onde $0 \leq i \leq p-1$.

Os pontos fixos de $\begin{pmatrix} 1 & p\varepsilon \\ 1 & 1 \end{pmatrix}$, são da forma $\begin{pmatrix} x^{pi} \\ 0 \end{pmatrix}$, onde $0 \leq i \leq p-1$.

Os pontos fixos de $\begin{pmatrix} 1 & 0 & 0 \\ 1 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$, são da forma $\begin{pmatrix} x^i \\ 0 \\ z^k \end{pmatrix}$, onde $0 \leq i, k \leq p-1$.

Os pontos fixos de $\begin{pmatrix} 1 & 0 & 0 \\ 1 & 1 & 0 \\ 0 & 1 & 1 \end{pmatrix}$, são da forma $\begin{pmatrix} x^i \\ 0 \\ 0 \end{pmatrix}$, onde $0 \leq i \leq p-1$.

Do Corolário 3.13 temos que se duas escolhas de pontos fixos v de τ diferem por um elemento na imagem de $\mathcal{N}_{\tau,p}$, temos extensões equivalentes. Uma vez que N é abeliano, N^τ - o conjunto dos elementos de N fixos por τ - e $Im(\mathcal{N}_{\tau,p})$ são grupos, estamos interessados então em encontrar um conjunto de representantes em $N^\tau/Im(\mathcal{N}_{\tau,p})$. Então computaremos a imagem de $\mathcal{N}_{\tau,p}$ para restringir nossas escolhas para v. Observe que $\mathcal{N}_{\tau,p}$ tem representação matricial igual a $Id + \tau + \tau^2 + ... + \tau^{p-1}$.

Se $\tau = \begin{pmatrix} 1 & p \\ 0 & 1 \end{pmatrix}$ então $\mathcal{N}_{\tau,p} = \begin{pmatrix} p & 0 \\ 0 & 0 \end{pmatrix}$.

Se $\tau = \begin{pmatrix} 1+p & 0 \\ 0 & 1 \end{pmatrix}$ então $\mathcal{N}_{\tau,p} = \begin{pmatrix} p & 0 \\ 0 & 0 \end{pmatrix}$.

Se $\tau = \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}$ então $\mathcal{N}_{\tau,p} = \begin{pmatrix} p & 0 \\ 0 & 0 \end{pmatrix}$.

Se $\tau = \begin{pmatrix} 1 & p \\ 1 & 1 \end{pmatrix}$ então $\mathcal{N}_{\tau,p} = \begin{pmatrix} z & 0 \\ 0 & 0 \end{pmatrix}$, onde $z = p$ ou $z = 2p$.

Se $\tau = \begin{pmatrix} 1 & p\varepsilon \\ 1 & 1 \end{pmatrix}$ então $\mathcal{N}_{\tau,p} = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$, se $p = 3$; e $\mathcal{N}_{\tau,p} = \begin{pmatrix} p & 0 \\ 0 & 0 \end{pmatrix}$, se $p > 3$.

Se $\tau = \begin{pmatrix} 1 & 0 & 0 \\ 1 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$ então $\mathcal{N}_{\tau,p} = \begin{pmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix}$.

Se $\tau = \begin{pmatrix} 1 & 0 & 0 \\ 1 & 1 & 0 \\ 0 & 1 & 1 \end{pmatrix}$ então $\mathcal{N}_{\tau,p} = \begin{pmatrix} 0 & 0 & 1 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix}$, se $p = 3$; e $\mathcal{N}_{\tau,p} = \begin{pmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix}$, se $p > 3$.

Do Lema 3.10 temos que dois representantes v e v^i nos dão extensões tipo equivalentes se i for relativamente primo com p, ou seja, se eles geram o mesmo subgrupo de N^τ. Essa informação já é suficiente para limitarmos nossa escolha de v para uma ou duas opções, exceto no caso em que

$$N = C_p \times C_p \times C_p \text{ e } \tau = \begin{pmatrix} 1 & 0 & 0 \\ 1 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}.$$

Mas neste caso, se $v \neq 1$, mostraremos que o grupo G determinado por (N, p, τ, v) deve possuir um subgrupo isomorfo a $C_{p^2} \times C_p$ e portanto, já terá sido construído.

Note que podemos ver N como um $\mathbb{F}_p$-espaço vetorial de dimensão 3. Tome um elemento $a \in G \backslash N$ tal que $\tau = Int_a|_N$. Como v tem ordem p, a tem ordem p^2. O conjunto de pontos fixos de τ pode ser visto como um $\mathbb{F}_p$-subespaço vetorial de N de dimensão 2. Por outro lado, $\langle v \rangle$ é um $\mathbb{F}_p$-subespaço vetorial de N de dimensão 1, portanto $N^\tau \setminus \langle v \rangle$ é não vazio. Logo, se tomarmos $x = a$ e $y \in N^\tau \setminus \langle v \rangle$ teremos $xyx^{-1}y^{-1} = \tau(y)y^{-1} = 1$ e, assim, $\langle x \rangle \times \langle y \rangle \simeq C_{p^2} \times C_p$.

Assim, precisamos apenas considerar v sendo trivial e podemos reunir estas informações na seguinte tabela:

τ	N^τ	$\mathcal{N}_{\tau,p}$	$Im(\mathcal{N}_{\tau,p})$	escolhas para v	
$\begin{pmatrix}1 & p\\ 0 & 1\end{pmatrix}$	$\left\langle \begin{pmatrix}1\\0\end{pmatrix} \right\rangle$	$\begin{pmatrix}p & 0\\ 0 & 0\end{pmatrix}$	$\left\langle \begin{pmatrix}p\\0\end{pmatrix} \right\rangle$	$\begin{pmatrix}0\\0\end{pmatrix}, \begin{pmatrix}1\\0\end{pmatrix}$	
$\begin{pmatrix}1+p & 0\\ 0 & 1\end{pmatrix}$	$\left\langle \begin{pmatrix}p\\0\end{pmatrix}, \begin{pmatrix}0\\1\end{pmatrix} \right\rangle$	$\begin{pmatrix}p & 0\\ 0 & 0\end{pmatrix}$	$\left\langle \begin{pmatrix}p\\0\end{pmatrix} \right\rangle$	$\begin{pmatrix}0\\0\end{pmatrix}, \begin{pmatrix}0\\1\end{pmatrix}$	
$\begin{pmatrix}1 & 0\\ 1 & 1\end{pmatrix}$	$\left\langle \begin{pmatrix}p\\0\end{pmatrix}, \begin{pmatrix}0\\1\end{pmatrix} \right\rangle$	$\begin{pmatrix}p & 0\\ 0 & 0\end{pmatrix}$	$\left\langle \begin{pmatrix}p\\0\end{pmatrix} \right\rangle$	$\begin{pmatrix}0\\0\end{pmatrix}, \begin{pmatrix}0\\1\end{pmatrix}$	
$\begin{pmatrix}1 & p\\ 1 & 1\end{pmatrix}$	$\left\langle \begin{pmatrix}p\\0\end{pmatrix} \right\rangle$	$\begin{pmatrix}z & 0\\ 0 & 0\end{pmatrix}$	$\left\langle \begin{pmatrix}p\\0\end{pmatrix} \right\rangle$	$\begin{pmatrix}0\\0\end{pmatrix}$	$z = p$ ou $z = 2p$
$\begin{pmatrix}1 & p\varepsilon\\ 1 & 1\end{pmatrix}$	$\left\langle \begin{pmatrix}p\\0\end{pmatrix} \right\rangle$	$\begin{pmatrix}0 & 0\\ 0 & 0\end{pmatrix}$	$\left\langle \begin{pmatrix}0\\0\end{pmatrix} \right\rangle$	$\begin{pmatrix}0\\0\end{pmatrix}, \begin{pmatrix}p\\0\end{pmatrix}$	$p = 3$
		$\begin{pmatrix}p & 0\\ 0 & 0\end{pmatrix}$	$\left\langle \begin{pmatrix}p\\0\end{pmatrix} \right\rangle$	$\begin{pmatrix}0\\0\end{pmatrix}$	$p > 3$
$\begin{pmatrix}1 & 0 & 0\\ 1 & 1 & 0\\ 0 & 0 & 1\end{pmatrix}$	$\left\langle \begin{pmatrix}0\\1\\0\end{pmatrix}, \begin{pmatrix}0\\0\\1\end{pmatrix} \right\rangle$	$\begin{pmatrix}0 & 0 & 0\\ 0 & 0 & 0\\ 0 & 0 & 0\end{pmatrix}$	$\left\langle \begin{pmatrix}0\\0\\0\end{pmatrix} \right\rangle$	$\begin{pmatrix}0\\0\\0\end{pmatrix}$	$(*)$
$\begin{pmatrix}1 & 0 & 0\\ 1 & 1 & 0\\ 0 & 1 & 1\end{pmatrix}$	$\left\langle \begin{pmatrix}0\\1\\0\end{pmatrix} \right\rangle$	$\begin{pmatrix}0 & 0 & 0\\ 0 & 0 & 0\\ 1 & 0 & 0\end{pmatrix}$	$\left\langle \begin{pmatrix}0\\0\\1\end{pmatrix} \right\rangle$	$\begin{pmatrix}0\\0\\0\end{pmatrix}$	$p = 3$
		$\begin{pmatrix}0 & 0 & 0\\ 0 & 0 & 0\\ 0 & 0 & 0\end{pmatrix}$	$\left\langle \begin{pmatrix}0\\0\\0\end{pmatrix} \right\rangle$	$\begin{pmatrix}0\\0\\0\end{pmatrix}, \begin{pmatrix}0\\1\\0\end{pmatrix}$	$p > 3$

Tabela 3.1: Escolhas para v

3.6 Classificação

Temos agora todas as ferramentas para classificar os grupos de ordem p^4.

Teorema 3.19. As extensões tipo apresentadas na seguinte tabela determinam todos os 10 grupos não abelianos de ordem p^4

Demonstração. Analisando as escolhas que temos para v na Tabela 3.1, temos 11 extensões tipo a considerar e estas são suficientes para determinar todos os grupos não abelianos de ordem p^4. Todas estas opções aparecem na Tabela 3.2 com exceção de $\left(C_{p^2} \times C_p, p, \begin{pmatrix}1 & 0\\ 1 & 1\end{pmatrix}, \begin{pmatrix}0\\1\end{pmatrix}\right)$. Mas veremos no próximo lema que esta é equivalente

	τ	v	Centro	número de elementos de ordem p	
				$p=3$	$p>3$
	$\begin{pmatrix}1 & p\\ 0 & 1\end{pmatrix}$	$\begin{pmatrix}0\\0\end{pmatrix}$	C_{p^2}	p^3-1	
	$\begin{pmatrix}1 & p\\ 0 & 1\end{pmatrix}$	$\begin{pmatrix}1\\0\end{pmatrix}$	C_{p^2}	p^2-1	
$(*)$	$\begin{pmatrix}1+p & 0\\ 0 & 1\end{pmatrix}$	$\begin{pmatrix}0\\0\end{pmatrix}$	$C_p\times C_p$	p^3-1	
	$\begin{pmatrix}1+p & 0\\ 0 & 1\end{pmatrix}$	$\begin{pmatrix}0\\1\end{pmatrix}$	$C_p\times C_p$	p^2-1	
$(*)$	$\begin{pmatrix}1 & 0\\ 1 & 1\end{pmatrix}$	$\begin{pmatrix}0\\0\end{pmatrix}$	$C_p\times C_p$	p^3-1	
$(**)$	$\begin{pmatrix}1 & p\\ 1 & 1\end{pmatrix}$	$\begin{pmatrix}0\\0\end{pmatrix}$	C_p	p^3-1	
$(**)$	$\begin{pmatrix}1 & p\varepsilon\\ 1 & 1\end{pmatrix}$	$\begin{pmatrix}0\\0\end{pmatrix}$	C_p	$p^4-p^3+p^2-1$	p^3-1
	$\begin{pmatrix}1 & p\varepsilon\\ 1 & 1\end{pmatrix}$	$\begin{pmatrix}p\\0\end{pmatrix}$	C_p	p^2-1	Desconsiderado Ver tabela 3.1
	$\begin{pmatrix}1 & 0 & 0\\ 1 & 1 & 0\\ 0 & 0 & 1\end{pmatrix}$	$\begin{pmatrix}0\\0\\0\end{pmatrix}$	$C_p\times C_p$	p^4-1	
	$\begin{pmatrix}1 & 0 & 0\\ 1 & 1 & 0\\ 0 & 1 & 1\end{pmatrix}$	$\begin{pmatrix}0\\0\\0\end{pmatrix}$	C_p	$2p^3-p^2-1$	p^4-1
$(**)$	$\begin{pmatrix}1 & 0 & 0\\ 1 & 1 & 0\\ 0 & 1 & 1\end{pmatrix}$	$\begin{pmatrix}0\\1\\0\end{pmatrix}$	C_p	Desconsiderado Ver tabela 3.1	p^3-1

Tabela 3.2: Extensões tipo que determinam todos os grupos não abelianos de ordem p^4

a $\left(C_{p^2}\times C_p, p, \begin{pmatrix}1+p & 0\\ 0 & 1\end{pmatrix}, \begin{pmatrix}0\\1\end{pmatrix}\right)$.

Portanto, falta apenas mostrar que os grupos determinados pelas extensões tipo apresentadas acima são todos não isomorfos. Para isto analisaremos o centro e a quantidade de elementos de ordem p de cada grupo determinado pelas extensões tipo, isto já garantirá que a maioria destes grupos são não isomorfos.

Se (N, p, τ, v) determina o grupo G então o centro de G é precisamente o grupo N^τ, e a partir da Tabela 3.1 podemos comparar os centros de cada grupo.

Para contar os elementos de G de ordem p primeiro notamos que

$$G = N \dot{\cup} Na \dot{\cup} ... \dot{\cup} Na^{p-1}.$$

É fácil encontrar o número de elementos de ordem p em N. Se $N = C_{p^2} \times C_p$, existem $p^2 - 1$ tais elementos. E se $N = C_p \times C_p \times C_p$, existem $p^3 - 1$.

Agora, para $0 < i < p$, a aplicação $za \mapsto (za)^i$ é uma bijeção entre os conjuntos Na e Na^i que, em particular, é uma bijeção entre os elementos de ordem p. Portanto, basta contar os elementos de ordem p em Na.

Pelo Lema 3.11, sabemos que para qualquer $x \in N$ temos $(xa)^p = \mathcal{N}_{\tau,p}(x)v$. Então se $v \notin Im(\mathcal{N}_{\tau,p})$, então $(xa)^p \neq 1$, e portanto, Na não possui elementos de ordem $\leq p$. Se $v \in Im(\mathcal{N}_{\tau,p})$, então os elementos de ordem $\leq p$ em Na estão em bijeção com os elementos de $ker(\mathcal{N}_{\tau,p})$. Sabemos que $|ker(\mathcal{N}_{\tau,p})| = p^3/|Im(\mathcal{N}_{\tau,p})|$ e $Im(\mathcal{N}_{\tau,p})$ é dada na Tabela 3.1. Podemos então contar os elementos de G de ordem p. Os resultados aparecem na Tabela 3.2.

Após esta análise, concluímos que apenas podem ser isomorfos os grupos determinados pelas extensões tipo das duas linhas marcadas com $(*)$; e se $p > 3$ os grupos determinados pelas extensões tipo das três linhas marcadas com $(**)$.

No Lema 3.21 veremos que não existe um isomorfismo entre os grupos determinados pelas extensões tipo das linhas marcadas com $(*)$.

Para as três linhas marcadas com $(**)$, cada uma determina um grupo que possui exatamente $p^3 - 1$ elementos de ordem p. No terceiro caso, todos estes devem ser elementos de N, de forma que todos eles comutam entre si. Já nos dois primeiros casos, encontramos exemplos de elementos de ordem p que não comutam. Portanto, o terceiro grupo não pode ser isomorfo a nenhum dos dois primeiros. No Lema 3.22 veremos que os dois primeiros grupos também são não isomorfos.

Assim, uma vez provados os Lemas 3.20, 3.21 e 3.22 o teorema está provado. □

Vamos agora à demonstração dos lemas mencionados durante a prova do teorema. A partir de agora $N = C_{p^2} \times C_p$.

Lema 3.20. As extensões tipo $\left(N, p, \begin{pmatrix} 1+p & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 0 \\ 1 \end{pmatrix}\right)$ e $\left(N, p, \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}, \begin{pmatrix} 0 \\ 1 \end{pmatrix}\right)$ são equivalentes.

Demonstração. Suponha que $\left(N, p, \begin{pmatrix} 1+p & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 0 \\ 1 \end{pmatrix}\right)$ determina G, o grupo construído como na demonstração do Teorema 3.7.

Sejam x e y os geradores de C_{p^2} e C_p, respectivamente, em N. Defina então $x' = a^{p-1}$, $y' = x^p$, $a' = x$, $v' = (a')^p = x^p = y'$; $N' = \langle x', y' \rangle$ e $\tau' = Int_{a'}|_{N'}$. Então

$$\begin{aligned} \tau'(x') &= a'x'(a')^{-1} = xa^{p-1}x^{-1} = x\tau^{p-1}(x^{-1})a^{p-1} = x(x^{-1})^{(1+p)^{(p-1)}}a^{p-1} = \\ &= x(x^{-1})^{1+(p-1)p}a^{p-1} = xxp - 1a^{p-1} = x^pa^{p-1} = y'x' = x'y', \\ \tau'(y') &= a'y'(a')^{-1} = xx^px^{-1} = x^p = y'. \end{aligned}$$

Com respeito aos geradores x' e y', τ' e v' têm representações $\begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}$ e $\begin{pmatrix} 0 \\ 1 \end{pmatrix}$ respectivamente.

Portanto, $\left(N', p, \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}, \begin{pmatrix} 0 \\ 1 \end{pmatrix}\right)$ também determina G. □

Lema 3.21. As extensões tipo $\left(N, p, \begin{pmatrix} 1+p & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 0 \\ 0 \end{pmatrix}\right)$ e $\left(N, p, \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}, \begin{pmatrix} 0 \\ 0 \end{pmatrix}\right)$ não são equivalentes.

Demonstração. Sejam G_1 e G_2 os grupos respectivamente determinados pelas extensões tipo dadas. Defina $H_1 := \{g^p \mid g \in G_1\}$ e $H_2 := \{g^p \mid g \in G_2\}$. Usando o Lema 3.11 podemos ver facilmente que $H_1 = H_2 = \left\langle \begin{pmatrix} p \\ 0 \end{pmatrix} \right\rangle$.

Segue então que cada $H_1 \leq Z(G_1)$ e $H_2 \leq Z(G_2)$, logo $H_1 \lhd G_1$ e $H_2 \lhd G_2$. Então para mostrar que G_1 e G_2 não são isomorfos é suficiente mostrar que G_1/H_1 e G_2/H_2 não o são. Veremos que de fato não o são uma vez que G_1/H_1 é abeliano e G_2/H_2 não.

Agora, considerando o homomorfismo $\varphi : Aut(N) \to Aut(N/H_i) \simeq Aut(C_p \times C_p) = GL_2(\mathbb{F}_p)$ que age reduzindo módulo p a primeira linha das matrizes que representam cada automorfismo, temos que a imagem de $\tau_1 = \begin{pmatrix} 1+p & 0 \\ 0 & 1 \end{pmatrix}$ em $GL_2(\mathbb{F}_p)$ é a identidade e a imagem de $\tau_2 = \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}$ é diferente da identidade.

Assim, τ_1 age trivialmente em N/H_1, portanto G_1/H_1 é abeliano. Por outro lado τ_2 não age trivialmente em N/H_2, portanto G_2/H_2 não é abeliano. □

Observe que se $p = 3$ não precisamos considerar avaliar as linhas marcadas com $(**)$, já que elas possuem quantidades diferentes de elementos com ordem $\leq p$. Já se $p > 3$ precisamos do seguinte resultado.

Lema 3.22. As extensões tipo $\left(N, p, \begin{pmatrix} 1 & p \\ 1 & 1 \end{pmatrix}, \begin{pmatrix} 0 \\ 0 \end{pmatrix}\right)$ e $\left(N, p, \begin{pmatrix} 1 & p\varepsilon \\ 1 & 1 \end{pmatrix}, \begin{pmatrix} 0 \\ 0 \end{pmatrix}\right)$ não são equivalentes.

Demonstração. Seja G um grupo determinado por $\left(N, p, \begin{pmatrix} 1 & p \\ 1 & 1 \end{pmatrix}, \begin{pmatrix} 0 \\ 0 \end{pmatrix}\right)$. Então G tem geradores x, y e a, onde x e y geram N. Para que a segunda extensão tipo determine também G, precisamos encontrar x', y' e a' que satisfaçam as mesmas relações que x, y e a com exceção da conjugação por a' (o automorfismo τ') em $N' := \langle x', y' \rangle$, que passaria a ser representado por $\begin{pmatrix} 1 & p\varepsilon \\ 1 & 1 \end{pmatrix}$.

Por contradição, suponha que existam tais x', y' e a'.

Sejam $Z := Z(G)$ e $H := G' = [G, G]$. É fácil ver que $Z = \langle x^p \rangle$ e $H = \langle x^p, y \rangle$. Como y é um elemento de ordem p que pertence a $H \backslash Z$, o mesmo deve acontecer com

y'.

Como x comuta com y, o mesmo deve acontecer com x' e y'. Para $z \in N$ e $k \not\equiv 0 \pmod{p}$, temos $(za^k)y'(za^k)^{-1} \neq y'$ para $y' \in H \backslash Z$. Portanto, para x' comutar com y' devemos ter $x' \in N$, logo $N' = N$.

Para qualquer $z \in N$, za' e a' induzem a mesma ação via conjugação em N. Portanto, podemos assumir que $a' = a^k$ para algum $0 < k < p$.

Para um homomorfismo qualquer $\varphi : N \to N$, considere o homomorfismo $\varphi - I$ que leva um elemento z em $\varphi(z)z^{-1}$. Para obter a representação matricial de $\varphi - I$ basta tomar a matriz que representa φ e subtrair a matriz identidade. Com respeito aos geradores x e y a representação de $(\tau^k - I)$ é dada por $\begin{pmatrix} \binom{k}{2}k & kp \\ k & 0 \end{pmatrix}$. Portanto a composição $(\tau^k - I)^2$ é representada por $\begin{pmatrix} k^2p & 0 \\ 0 & 0 \end{pmatrix}$. Com respeito aos geradores x' e y', $(\tau' - I)$ é representada por $\begin{pmatrix} p\varepsilon & 0 \\ 0 & 0 \end{pmatrix}$.

Como x' tem ordem p^2, devemos ter $x' = x^c y^d$ para c e d com $c \not\equiv 0 \pmod{p}$. Note que $(x')^p = (x^p)^c$.

Para um elemento qualquer $z \in N$, temos $[a, z] = aza^{-1}z^{-1} = \tau(z)z^{-1} = (\tau - I)(z)$.

Calculamos agora $[a', [a', x']]$ de duas maneiras distintas. Primeiro,

$$[a', [a', x']] = (\tau - I)^2(x') = x'^{p\varepsilon} = x^{cp\varepsilon}.$$

Segundo,

$$[a', [a', x']] = [a^k, [a^k, x']] = (\tau^k - I)^2(x^c y^d) = x^{k^2 cp}.$$

Mas os resultados destes dois cálculos não podem ser iguais pois $k^2 \not\equiv \varepsilon \pmod{p}$, uma vez que ε é um não quadrado módulo p. □

Com todos estes resultados em mãos podemos organizar uma nova tabela com os resultados obtidos e a classificação final.

	N	τ	v
G_1	$C_{p^2} \times C_p$	$x \mapsto x,\ y \mapsto x^p y$	1
G_2	$C_{p^2} \times C_p$	$x \mapsto x,\ y \mapsto x^p y$	x
G_3	$C_{p^2} \times C_p$	$x \mapsto x^{1+p},\ y \mapsto y$	1
G_4	$C_{p^2} \times C_p$	$x \mapsto x^{1+p},\ y \mapsto y$	y
G_5	$C_{p^2} \times C_p$	$x \mapsto xy,\ y \mapsto y$	1
G_6	$C_{p^2} \times C_p$	$x \mapsto xy,\ y \mapsto x^p y$	1
G_7	$C_{p^2} \times C_p$	$x \mapsto xy,\ y \mapsto x^{p\varepsilon} y$	1
G_8	$C_p \times C_p \times C_p$	$x \mapsto xy,\ y \mapsto y,\ z \mapsto z$	1
G_9	$C_p \times C_p \times C_p$	$x \mapsto xy,\ y \mapsto yz,\ z \mapsto z$	1
G_{10} $(p = 3)$	$C_{p^2} \times C_p$	$x \mapsto xy,\ y \mapsto x^{p\varepsilon} y$	x^p
$\bar{G}_{10}$ $(p > 3)$	$C_p \times C_p \times C_p$	$x \mapsto xy,\ y \mapsto yz,\ z \mapsto z$	y

Tabela 3.3: Extensões tipo e grupos determinados por elas

Nesta tabela temos

$G_1 \simeq \langle x, y, a \mid x^{p^2} = y^p = a^p = [x, y] = [x, a] = 1, [y, a] = x^p \rangle$;

$G_2 \simeq \langle a, y \mid a^{p^3} = y^p = 1, a^y = a^{p^2-1} \rangle$;

$G_3 \simeq \langle x, y, a \mid x^{p^2} = y^p = a^p = [x, y] = [y, a] = 1, x^a = x^{1+p} \rangle$;

$G_4 \simeq \langle x, a \mid x^{p^2} = a^{p^2} = 1, x^a = x^{1+p} \rangle$;

$G_5 \simeq \langle x, y, a \mid x^{p^2} = y^p = a^p = [x, y] = [y, a] = 1, [a, x] = y \rangle$;

$G_6 \simeq \langle x, y, a \mid x^{p^2} = y^p = a^p = [x, y] = 1, [a, x] = y, [a, y] = x^p \rangle$;

$G_7 \simeq \langle x, y, a \mid x^{p^2} = y^p = a^p = [x, y] = 1, [a, x] = y, [a, y] = x^{p\varepsilon} \rangle$;

$G_8 \simeq \langle x, y, z, a \mid x^p = y^p = z^p = a^p = [x, y] = [x, z] = [y, z] = [y, a] = [z, a] = 1, [a, x] = y \rangle$;

$G_9 \simeq \langle x, y, z, a \mid x^p = y^p = z^p = a^p = [x, y] = [x, z] = [y, z] = [z, a] = 1, [a, x] = y, [a, y] = z \rangle$;

$G_{10} \simeq \langle x, y, a \mid x^9 = y^3 = [x, y] = 1, a^3 = x^3, [a, x] = y, [a, y] = x^{3\varepsilon} \rangle,\ p = 3$;

$\bar{G}_{10} \simeq \langle x, z, a \mid x^p = z^p = a^{p^2} = [x, z] = [z, a] = 1, [a, x] = a^p \rangle,\ p > 3$.

Considerações finais

Bertram Huppert, no seu clássico livro Endlich Gruppen I (1967) apresenta também uma classificação dos grupos de ordem p^4, $p > 3$. Para os casos em que G é abeliano é usado o teorema da classificação dos grupos abelianos finitos e para os casos em que G é não abeliano a demonstração é dividida em 3 casos. No primeiro caso todo subgrupo normal abeliano de G tem no máximo 2 geradores e para esta classificação são usados resultados de Blackburn (1961). No segundo caso G possui um subgrupo normal abeliano U do tipo (p, p, p), ou seja $U \simeq C_p \times C_p \times C_p$, e $exp(G) = p$, ou seja p é o menor inteiro tal que $g^p = 1$ para todo $g \in G$, e para esta classificação são usados resultados sobre os automorfismos em U. No terceiro caso G possui um subgrupo normal abeliano U do tipo (p, p, p) e $exp(G) = p^2$ e para esta classificação são usados resultados sobre a decomponibilidade de U em G-módulos irredutíveis e resultados sobre os automorfismos de U.

Apesar de considerarmos a classificação feita por Huppert mais simples que as classificações apresentadas em 1893, consideramos a classificação por extensões tipo ainda mais simples.

Em 1896, G. A. Miller apresentou uma lista de 51 grupos de ordem 32. Essa lista foi modificada em 1936, onde foram retirados 4 grupos que estavam supostamente duplicados. Em 1940, Philip Hall desenvolveu um método para classificação de grupos finitos (especialmente para p-grupos, onde p é primo) e, usando o método de P. Hall, James K. Senior preparou uma lista com (novamente) 51 grupos de ordem 32, determinando

a lista final de grupos de ordem 32, e confirmando que a lista de Miller estava correta. Mais que isso, Marshall Hall e J. K. Senior, em 1964, produziram uma lista completa de todos os grupos de ordem 2^n para $n \leq 6$.

Já em 2007, Wan-Ju Lin classificou estes 51 grupos usando extensões cíclicas e produto semidireto. Lin analisa em cada caso o expoente do grupo.

Nos casos em que $exp(G) = 2$ e $exp(G) = 32$, devemos ter $G \simeq C_2 \times C_2 \times C_2 \times C_2 \times C_2$ e $G \simeq C_{32}$, respectimente. Resta analisar os casos em que $exp(G) \in \{4, 8, 16\}$.

Se $exp(G) = 16$, tomamos um subgrupo cíclico H gerado por um elemento de ordem 16. Tomando $x \in G \backslash H$, temos quatro opções de automorfismos de H. Além disso, devemos também olhar para a ordem dos elementos de $G \backslash H$.

Primeiro, se existe $x \in G \backslash H$ de ordem 2. Segundo, se a ordem de todo elemento $g \in G \backslash H$ é ≥ 4 e existe um $x \in G \backslash H$ de ordem 4. Terceiro, se a ordem de todo elemento $g \in G \backslash H$ é ≥ 8 e existe um $x \in G \backslash H$ de ordem 8, neste caso chegamos apenas a contradições. Por último, se a ordem de todo elemento $x \in G \backslash H$ é 8, este caso também só nos leva a contradições.

Se $exp(G) = 8$, chamamos de H_i o subgrupo gerado pelo i-ésimo elemento de ordem 8. Temos então três opções. Primeiro, existe $n \in \mathbb{N}$ tal que $H_n \lhd G$ e $G/H_n \simeq C_4$. Segundo, $G/H_n \simeq C_2 \times C_2$ para todo $n \in \mathbb{N}$. Terceiro, nenhum H_n é normal em G.

Se $exp(G) = 4$, chamamos de H_i o subgrupo gerado pelo i-ésimo elemento de ordem 4. Novamente temos três casos a analisar. Primeiro, existe $n \in \mathbb{N}$ tal que $H_n \lhd G$ e $G/H_n \simeq C_4 \times C_2$, ou D_8 ou Q_8. Segundo, $G/H_n \simeq C_2 \times C_2 \times C_2$ para todo $n \in \mathbb{N}$. Terceiro, nenhum H_n é normal em G.

Para os grupos de ordem p^n para $n \geq 6$ e de ordem p^5 para $p \neq 2$ não encontramos uma referência de uma classificação que faça uso de extensões tipo, mas analisamos alguns trabalhos que fazem algumas destas classificações. No trabalho de H. A. Bender, 1927, é feita uma classificação dos grupos de ordem p^5 para $p \neq 2$ separando-os em três casos. No caso abeliano, temos sete grupos não isomorfos. No caso não abeliano, são

analisados separadamente os grupos que possuem um subgrupo abeliano de ordem p^4, neste caso existem $p+39$ grupos, se $p-1 \neq 3k$, e $p+41$ grupos, se $p-1=3k$. Já no caso dos grupos de ordem p^5 não abelianos e que não possuem subgrupo abeliano de ordem p^4 existem $p+19$ grupos, se $p=12k-1$; $p+21$ grupos, se $p=12k\pm 5$; $p+23$ grupos, se $p=12k+1$ e finalmente 17 grupos, se $p=3$

Para os grupos de ordem p^6, com $p \neq 2$, analisamos o trabalho de Rodney James, 1980. Nele, novamente é usado o método de P. Hall e são classificados os 491 grupos não abelianos de ordem 3^6 e os grupos não abelianos de ordem p^6, para $p>3$, que são

$$\frac{1}{4}[13p^2+145p+1338+80(p-1,3)+45(p-1,4)+8(p-1,5)+8(p-1,6)],$$

onde $(p-1,n)$ denota o maior divisor comum entre $p-1$ e n.

Em 1990 Rodney James, M. F. Newman e E. A. O'Brien classificaram os 2328 grupos de ordem 2^7.

Para os grupos de ordem p^7, com $p \neq 2$, analisamos o trabalho de E. A. O'Brien e M. R. Vaughan-Lee, 2005. Nele são classificados os 9310 grupos de ordem 3^7, os 34297 grupos de ordem 5^7, e os grupos de ordem p^7 para $p>5$, cuja quantidade é

$$3p^5+12p^4+55p^3+170p^2+707p+2455+[4p^2+44p+291](p-1,3)+[p^2+19p+135](p-1,4)+[3p+31](p-1,5)+4(p-1,7)+5(p-1,8)+(p-1,9).$$

Além disso, E. O'Brien também classificou os grupos de ordem 2^8 em [9].

Não existe esperança de se encontrar um conjunto finito de invariantes que irão definir todos os p-grupos finitos, de uma maneira útil, a menos de isomorfismo então é necessário encontrar um caminho de contornar esta dificuldade. O que alguns autores têm feito é oferecer uma classificação mais fraca do que "a menos de isomorfismo". Um invariante considerado tem sido a *coclasse* de um p-grupo que é definida como $n-c$ onde a ordem do grupo é p^n e c é a sua classe de nilpotência.

Um dos grandes centros de computação de p-grupos tem sido a Australian National University em Canberra, onde Mike Newman foi responsável pelo desenvolvimento e

implementação de poderosos algoritmos para computação de p-grupos finitos. Foi lá onde foram computados os grupos de ordem 2^7 e 2^8 por O'Brien que era um então estudante de Newman. Eles fizeram muitas conjecturas após a classificação dos 2-grupos de coclasse pequena.

Particularmente, Newman e O'Brien conjecturam que o número de 2-grupos de ordem 2^n é de coclasse r, para n suficientemente grande, depende somente do valor de n módulo 2^{r-1}. Para primos ímpares, é conhecido que a situação é bastante pior do que isto e ainda há muito o que se fazer.

Referências Bibliográficas

[1] Adler, Jeffrey D. ; Garlow, Michael and Wheland, Ethel R. *Groups of order p^4 made less difficult*, 2006, (`http://www.math.uakron.edu/~adler/papers/`).

[2] Bender, H. A. *A determination of the groups of order p^5*; Annals of Mathematics, vol. 29 (1927), pp. 61-72.

[3] Dummit, David S. and Foote, Richard M. *Abstract Algebra*, 3rd edition, John Wiley & Sons, Inc., 2004.

[4] Gorenstein, Daniel. *Finite Groups*, 2nd edition, Chelsea Publishing Company, 1980.

[5] Huppert, Bertram. *Endlich Gruppen I*, Springer-Verlag Berlim Heidelberg, 1967.

[6] James, Rodney. *The Groups of Order p^6 (p an Odd Prime)*, Mathematics of computation, vol. 34 (1980), number 150, pp. 613-637.

[7] James, Rodney; Newman, M.F. and O'Brien, E.A. *The Groups of order 128*, Journal of Algebra 129 (1990), pp. 136-158.

[8] Lin, Wan-Ju. *Groups of order thirty-two*, A Thesis of Master Science: 2007, (`http://etds.lib.ncku.edu.tw/etdservice/view_metadata?etdun=U0026-0812200914325503`).

[9] O'Brien, E. A. *The groups of order 256*, Journal of Algebra, 143 (1991) pp 219 - 235.

[10] O'Brien, E. A. and Vaughan-Lee, M. R. *The groups of order p^7 for odd prime p*, Journal of Algebra 292 (2005), pp. 243-258.

[11] Robinson, Derek J. S. *A Course in the Theory of Groups*, 1st edition, Springer-Verlag New York Inc., 1982.

[12] Sophie, M. *A note on the groups of order thirty-two*; Illinois J. Math. (1962), pp. 630-633.

[13] Wild, Marcel. *The Groups of Order Sixteen Made Easy*, The American Mathematical Monthly, Vol 112 (2005), Number 1, pp. 20-31.