UNIVERSIDADE FEDERAL DO CEARÁ
CENTRO DE CIÊNCIAS
DEPARTAMENTO DE MATEMÁTICA
PROGRAMA DE PÓS-GRADUAÇÃO EM MATEMÁTICA

NEFRAN SOUSA CARDOSO

ANÉIS DE GRUPOS INTEIROS DE GRUPOS DE FROBENIUS

FORTALEZA
2002

NEFRAN SOUSA CARDOSO

ANÉIS DE GRUPOS INTEIROS DE GRUPOS DE FROBENIUS

Dissertação submetida à Coordenação do Curso de Pós-Graduação em Matemática da Universidade Federal do Ceará, como requisito parcial para a obtenção do Grau de Mestre em Matemática.

Área de Concentração: Álgebra

Orientador: Prof. Dr. José Robério Rogério

FORTALEZA

2002

Dados Internacionais de Catalogação na Publicação
Universidade Federal do Ceará
Biblioteca do Curso de Matemática

Cardoso, Nefran Sousa
N265a Anéis de grupos inteiros de grupos de Frobenius / Nefran Sousa Cardoso. - 2002.
37 f.; 31cm

Dissertação(mestrado) - Universidade Federal do Ceará, Centro de Ciências , Departamento de Matemática, Programa de Pós-Graduação em Matemática, Fortaleza, 2002.
Área de Concentração: Álgebra
Orientação: Prof. Dr. José Robério Rogério
1. Anéis (álgebra). 2. Grupos finitos. 1. Título.

CDD 512.2

Aos meus pais Francisco das Chagas Cardoso
e Maria Necy Sousa.

Agradecimentos

A todos aqueles que contribuíram de forma direta ou indiretamente na conquista desse trabalho. Em especial a Arnaldo Silva Brito, Gildo Jesus Sousa, Márcia Cristina Silva Brito, Maria Gisélia Vasconcelos e Isaías Pereira de Jesus.

À Andrea pela prestatividade, competência e agilidade.

Ao CNPq pelo apoio financeiro.

Não deixaria de agradecer à banca examinadora na pessoa do meu orientador professor José Robério Rogério.

O temor do Senhor é o princípio do conhecimento; mas os insensatos desprezam a sabedoria e a instrução.
(Prov.1:7).

Resumo

Esta dissertação está dividida em dois capítulos.
O primeiro capítulo apresenta os Anéis de Grupos, os Grupos de Frobenius e suas respectivas propriedades.
No início do segundo capítulo são apresentadas as Conjecturas de Zassenhaus. A versão mais fraca dessas conjecturas é demonstrada para Grupos de Amitsur. No final do segundo capítulo, a validade dessa mesma versão é provada para Grupos de Frobenius. Tais Grupos de Frobenius são aqueles cujo complemento verifica-se a validade dessa conjectura. Na parte final são apresentados os subgrupos de Hall e o Teorema de Schur-Zassenhaus.

Palavras-chave: Anéis de Grupos, Conjecturas de Zassenhaus, Grupos de Amitsur, Grupos de Frobenius.

Abstract

This dissertation is divided into two chapters.
The first chapter introduces the Group Rings, the Frobenius Groups and their properties.
In the beginning of the second chapter are presented Conjectures of Zassenhaus . The weaker version of these conjectures is demonstrated for Amitsur Groups. At the end of the second chapter, the validity of that version is proven to Frobenius Groups. Such Frobenius Groups are those whose complement, checks the validity of this conjecture. In the final part we present the Hall subgroups and Schur-Zassenhaus Theorem.

Keywords: Group Rings, Conjectures of Zassenhaus , Amitsur Groups, Frobenius Groups.

Sumário

Introdução

H. J. Zassenhaus formulou uma conjectura que neste trabalho denotaremos por (ZC1) como em [7]. Sendo $\mathbb{Z}G$ o anel de grupo inteiro de um grupo G temos:

(ZC1) *Se* $u \in \mathcal{U}_1(\mathbb{Z}G) = \{$*unidades de* $\mathbb{Z}G$ *de aumento* $1\}$, *então existe* $\beta \in \mathcal{U}(\mathbb{Q}G) = \{$*unidades de* $\mathbb{Q}G\}$ *tal que* $\beta^{-1}u\beta \in G$.

Uma versão fraca dessa conjectura que em [7] é chamada de Problema (de investigação) 8, e que denotaremos por (P8) é a seguinte:

(P8) *Se* $u \in \mathcal{U}_1(\mathbb{Z}G)$ *tem ordem finita* $\circ(u)$, *então existe* $g \in G$ *de ordem* $\circ(g)$ *tal que* $\circ(g) = \circ(u)$

O principal objetivo deste trabalho é mostrar que (P8) vale para grupos de Frobenius cujo complemento pode ser imerso em um anel de divisão e para grupos de Frobenius de ordem ímpar. O trabalho é dividido em dois capítulos. No primeiro estudamos os anéis de grupos e as propriedades de grupos de Frobenius. No segundo capítulo obtemos o principal teorema deste trabalho.

Teorema: *Se* $u \in \mathcal{U}_1(\mathbb{Z}G)$, *então* $\circ(u)$ *divide* $|X|$ *ou* $\circ(u)$ *divide* $|N|$, *onde* $G = N \rtimes X$ *é um grupo de Frobenius finito com núcleo de Frobenius* N *e complemento de Frobenius* X.

Posteriormente usando esse teorema obteremos:

Teorema: *Se* G *é um grupo de Frobenius finito com complemento* X. *Se (P8) vale para* $\mathbb{Z}X$, *então vale para* $\mathbb{Z}G$.

Desse último resultado obteremos a validade de (P8) para os casos desejados.

Capítulo 1

Preliminares

Neste capítulo apresentaremos algumas definições e resultados básicos que serão importantes no capítulo posterior. Se G for um grupo denotaremos sua ordem por $|G|$ e para $g \in G$, sua ordem é denotada por $\circ(g)$. Se $G = N \rtimes X$ (produto semi direto de N por X), quer dizer que $G = NX,\ N \cap X = 1$ e que $N \trianglelefteq G$. Indicaremos (m, n) o máximo divisor comum entre inteiros m e n. Se $(m, n) = 1$, diremos que m e n são coprimos.

1.1 Anéis de Grupos

O anel de grupo de um grupo G sobre o anel K, com identidade, é o anel KG de todas as somas formais

$$\lambda \ = \ \sum_{g \in G} \lambda(g) g, \qquad \lambda(g) \in K$$

tal que

$$supp(\lambda) \ = \ \{g \in G : \lambda(g) \neq 0\},$$

o suporte de λ, é finito; com as seguintes propriedades operacionais

$$\sum_{g \in G} \lambda(g) g = \sum_{g \in G} \mu(g) g \ \Leftrightarrow \ \lambda(g) = \mu(g) \qquad \forall g \in G, \tag{1.1}$$

$$\sum_{g \in G} \lambda(g) g + \sum_{g \in G} \mu(g) g \ = \ \sum_{g \in G} \Big(\lambda(g) + \mu(g)\Big) g, \tag{1.2}$$

$$\Big(\sum_{g \in G} \lambda(g) g\Big)\Big(\sum_{g \in G} \mu(g) g\Big) \ = \ \sum_{g \in G} \nu(g) g, \tag{1.3}$$

onde

$$\nu(g) \ = \ \sum_{h \in G} \lambda(h) \mu(h^{-1} g) = \sum_{xy = g} \lambda(x) \mu(y)$$

Sendo 1_G o elemento identidade de G, a aplicação de K em KG definida por $k \to k \cdot 1_G$ é um homomorfismo injetor. Portanto podemos assumir que K está contido em KG. O elemento $1 \cdot 1_G$ será a identidade do anel KG e o denotaremos por 1. A aplicação de KG em K denotada por ε e definida por

$$\lambda = \sum_{g \in G} \lambda(g) g \quad \stackrel{\varepsilon}{\to} \sum_{g \in G} \lambda(g)$$

é um homomorfismo chamado função de aumento de KG. O núcleo deste homomorfismo,

$$\Delta_K(G) \;=\; \Big\{ \lambda = \sum_{g \in G} \lambda(g) g \in KG : \sum_{g \in G} \lambda(g) = 0 \Big\}$$

é chamado ideal de aumento de KG. Para um subgrupo normal N de G temos o homomorfismo natural ψ de KG em $K(G/N)$ definido por

$$\lambda = \sum_{g \in G} \lambda(g) g \quad \stackrel{\psi}{\to} \sum_{g \in G} \lambda(g) gN$$

O núcleo desse homomorfismo denotado por $\Delta_K(G, N)$, é o ideal gerado por todos $x - 1,\ x \in N$. A prova desse resultado é dada a seguir.

Teorema 1.1 *O ideal $\langle x - 1 : x \in N \rangle$ de KG, é o núcleo do homomorfismo ψ definido acima.*

Prova: Seja $T = \{x_i\}_{i \in I}$ um conjunto de representantes de classes de G determinadas por N, i.e., $G = \bigcup_{i \in I} \bar{x}_i$, onde $\bar{x}_i = x_i N$. Para cada $g \in G$, existe $i \in I$e $n_g \in N$ tal que $g = x_i n_g$. Portanto se $\lambda = \sum_{g \in G} \lambda(g) g$, então $\psi(\lambda) = \sum_{i \in I} \sum_{g \in \bar{x}_i} \lambda(x_i n_g) \bar{x}_i$. Se $\lambda \in \Delta_K(G, N)$, teremos $\sum_{g \in \bar{x}_i} \lambda(x_i n_g) = 0,\ \forall\ i \in I$. Assim,

$$\begin{aligned}
\lambda \;&=\; \sum_{g \in G} \lambda(g) g = \sum_{i \in I} \sum_{g \in \bar{x}_i} \lambda(x_i n_g) x_i n_g \\
&=\; \sum_{i,g} \lambda(x_i n_g) x_i n_g - \sum_{i \in I} \sum_{g \in \bar{x}_i} \lambda(x_i n_g) x_i \\
&=\; \sum_{i,g} \lambda(x_i n_g) x_i (n_g - 1) \;\in \langle x - 1 : x \in N \rangle
\end{aligned}$$

Assim, $\Delta_K(G, N) \subset \langle x - 1 : x \in N \rangle$. A outra inclusão segue trivialmente.

■

Definição 1.1 *Um elemento r de um anel R é chamados de unidade se ele possuir um inverso s, i.e., $rs = 1 = sr$. O conjunto de todas as unidades de R forma um grupo $\mathcal{U}(R)$, chamado grupo das unidades de R.*

A seguir, daremos alguns exemplos de unidades em $\mathbb{Z}G$:

1. Os elementos $\pm g$, $g \in G$ são obviamente unidades com inversos $\pm g^{-1}$.

   Esses elementos são chamados de **unidades triviais**.

2. Para $\lambda \in \mathbb{Z}G$, denotaremos sua ordem por $\circ(\lambda)$. Seja $g \in G$ com ordem finita. Escrevamos g como sendo

$$\hat{g} = \sum_{i=1}^{\circ(g)} g^i$$

   Então $(1-g)\hat{g} = 0$ e para qualquer $h \in G$, $\Big((1-g)h\hat{g}\Big)^2 = 0$. Portanto $u_{g,h} = 1 + (1-g)h\hat{g}$ têm inverso $1-(1-g)h\hat{g}$. As unidades $u_{g,h}, h, g \in G$ são chamadas **unidades bicíclicas** de $\mathbb{Z}G$.

Observação 1.1 *Se $u \in \mathcal{U}(\mathbb{Z}G)$, então existe $v \in \mathbb{Z}G$ tal que $uv = 1$. Logo $\varepsilon(u)\varepsilon(v) = \varepsilon(1) = 1$. Assim $\varepsilon(u) = \pm 1$, e portanto temos $\mathcal{U}(\mathbb{Z}G) = \pm\mathcal{U}_1(\mathbb{Z}G)$ onde $\mathcal{U}_1(\mathbb{Z}G)$ são todas unidades de aumento 1.*

Definição 1.2 *Seja H um subgrupo de $\mathcal{U}_1(\mathbb{Z}G)$. Se existir um $\alpha \in \mathcal{U}(\mathbb{Q}G)$ tal que $H^\alpha = \alpha^{-1}H\alpha \subset G$, diremos que H é racionalmente conjugado a um subgrupo de G. Se $H = \langle\alpha\rangle$ for racionalmente conjugado a um subgrupo de G, diremos que u é racionalmente conjugado a um elemento de G.*

O próximo resultado é essencial no estudo de unidades.

Teorema 1.2 (Berman-Higman) *Seja G um grupo finito. Suponha que $\gamma = \sum \gamma(g)g \in \mathbb{Z}G$ seja uma unidade de torção, a saber $\gamma^n = 1$ para algum n e $\gamma(1) \neq 0$. Então $\gamma = \pm 1$.*

Prova: Para cada $x \in \mathbb{Q}G$ vamos considerar a representação regular de $\mathbb{Q}G$ dada po

$$\begin{aligned} L_x : \mathbb{Q}G &\to \mathbb{Q}G \\ y &\mapsto xy \end{aligned}$$

Represente L_x por uma matriz em relação à base $\{g_1, g_2, \ldots, g_m\}$ de $\mathbb{Q}G$ formada por elementos de G, onde $m = |G|$. Para $g \in G$, $L_g(g_i) = g_i$ se, e somente se, $g = 1$. Portanto para $g \in G$ o traço de L_g, trL_g é dado por

$$trL_g = \begin{cases} 0, & \text{se} \quad g \neq 1 \\ |G|, & \text{se} \quad g = 1 \end{cases} \tag{1.4}$$

Como $\gamma^n = 1$, então $(L_\gamma)^n = I_m$, onde I_m representa a matriz identidade de ordem m. Podemos então diagonalizar L_γ. Seus autovalores são raízes n-ésimas da unidade ζ_i, $i \leq i \leq m$. Portanto, temos

$$\sum_{i=1}^{m} \zeta_i = trL_g \quad = \quad \sum_g \gamma(g) trL_g = \gamma(1)|G| \tag{1.5}$$

Como $\gamma(1) \neq 0$ e é inteiro, temos que $|\gamma(1)| \geq 1$. Além disso, $|\zeta_i| = 1$. Assim obtemos

$$|\sum_i \zeta_i| \quad \leq \quad \sum_i |\zeta_i| = m = |G| \tag{1.6}$$

e

$$|\gamma(1)|G|| \quad \geq \quad |G| \tag{1.7}$$

Por (1.5), (1.6) e (1.7), temos que $|\sum_1^m \zeta_i| = \sum_1^m |\zeta_i| = |G|$.

Portanto $\zeta_i = \zeta$ para todo i. Segue-se que $L_\gamma = \zeta I_m$, e assim $\gamma = \zeta \cdot 1$. Como $\gamma \in \mathbb{Z}G$ temos que $\zeta = \pm 1$.

■

Equivalentemente, temos o seguinte corolário:

Corolário 1.1 *Seja $\gamma \in \mathbb{Z}G$ uma unidade de ordem finita n tal que $\gamma \neq \pm 1$. Então $\gamma(1) = 0$.*

Corolário 1.2 *Seja A um grupo abeliano finito. Então todas as unidades de torção de $\mathbb{Z}A$ são triviais.*

Prova: Seja $\gamma = \sum \gamma(g)g \in \mathbb{Z}A$ de ordem finita n. Como $\gamma \neq 0$, existe $g_0 \in A$ tal que $\gamma(g_0) \neq 0$ e $\circ(g_0) = k < \infty$. Usando a comutatividade de A, temos

$$(\gamma g_0^{-1})^{nk} \quad = \quad \gamma^{nk}(g_0^{-1})^{nk} = 1$$

Além disso, $(\gamma g_0^{-1})(1) = \gamma(g_0) \neq 0$. Pelo Corolário (1.1), segue-se que $\gamma g_0^{-1} = \pm 1$, portanto $\gamma = \pm g_0$.

■

Teorema 1.3 *Sejam K um corpo de característica 0 e G um grupo finito. Seja $e = \sum_g e(g)g \neq 0, 1$ um idempotente não trivial de KG. Então $e(1) \in \mathbb{Q}$, $|G|e(1) \in \mathbb{Z}$, e $0 < e(1) < 1$.*

Prova: Para cada $x \in KG$, considere a representação regular $L_x \in KG$ definida por $L_x(y) = xy$ como no Teorema (1.2). Os $|G|$ autovalores de L_e são 0 e 1. Sendo m o número de autovalores de L_e iguais a 1, temos que $0 < m < |G|$, pois $e \neq 0, 1$. Além disso

$$m = trL_e \quad = \quad \sum_g e(g) trL_g = e(1)|G|$$

Assim, $0 < e(1) < 1$ e $|G|e(1) \in \mathbb{Z}$.

■

Teorema 1.4 *Seja $\mathbb{Z}G$ o anel de grupo dos inteiros de um grupo finito G. Suponha que $\gamma \in \mathbb{Z}G$ tenha ordem multiplicativa n. Se $\varepsilon(\gamma) = 1$, então n é um divisor da ordem do grupo G.*

Prova: Considere $e = (1 + \gamma + \ldots + \gamma^{n-1})/n$.

$$e\gamma = \{(1 + \gamma + \ldots + \gamma^{n-1})/n\}\gamma = (\gamma + \gamma^2 + \ldots + \gamma^n)/n = e$$

Então $e^2 = e$, pois

$$e^2 = e(1 + \gamma + \ldots + \gamma^{n-1})/n = (e + e\gamma + \ldots + e\gamma^{n-1})/n = \frac{ne}{n} = e$$

Como $\circ(\gamma) = n$, temos que $\gamma^i \neq \pm 1$ para $1 \leq i \leq n-1$. Pelo Corolário (1.1), $\gamma^i(1) = 0$. Segue então que

$$e(1) = \frac{1}{n}\sum_{i=0}^{n-1} \gamma^i(1) = \frac{1}{n}$$

Pelo Teorema (1.3) existe $k \in \mathbb{Z}$ tal que $e(1) = \frac{k}{|G|}$. Portanto $kn = |G|$.

■

Definição 1.3 *Para um anel R, definimos $[R, R]$ como o grupo aditivo gerado por todos produtos de Lie $[x, y] = xy - yx$ para $x, y \in R$.*

Teorema 1.5 *Seja R um anel de característica prima p, com unidade. Então para $x, y \in R$ e números naturais n temos*

$$(x + y)^{p^n} \equiv x^{p^n} + y^{p^n} \qquad mod\ [R, R]$$

Prova: Vamos provar por indução sobre n. Para o caso $n = 1$.

$$(x + y)^p = x^p + y^p + \sum_{z_i \in \{x,y\}} z_1 z_2 \ldots z_p$$

Para cada termo $z_1 z_2 \ldots z_p$ associe-o com suas permutações cíclicas

$$z_1 z_2 \ldots z_p,\ z_2 z_3 \ldots z_p z_1,\ \ldots,\ z_p z_1 z_2 \ldots z_{p-1}$$

Note que,

$$\begin{aligned} z_1 z_2 \ldots z_p - [z_1, z_2 z_3 \ldots z_p] &= z_2 z_3 \ldots z_p z_1 \\ z_1 z_2 \ldots z_p - [z_1 z_2, z_3 \ldots z_p] &= z_3 z_4 \ldots z_p z_1 z_2 \\ \vdots &= \vdots \\ z_1 z_2 \ldots z_p - [z_1 z_2 \ldots z_{p-1}, z_p] &= z_p z_1 z_2 \ldots z_{p-1} \end{aligned}$$

Segue-se então que a soma dessas permutações cíclicas é $pz_1z_2\ldots z_p$ módulo $[R,R]$ e portanto pertence a $[R,R]$, pois R tem característica p. Observe que

$$\begin{aligned}(xy-yx)^p &\equiv (xy)^p-(yx)^p \qquad mod\ [R,R]\\ &\equiv [x,(yx)^{p-1}y] \qquad mod\ [R,R]\end{aligned}$$

Portanto,

$$\gamma\in[R,R] \;\Rightarrow\; \gamma\in[R,R]$$

Suponha o resultado válido para n. Então existe $\alpha\in[R,R]$, tal que,

$$(x+y)^{p^n} = x^{p^n}+y^{p^n}+\alpha$$

Pelo caso $n=1$ existem $\alpha_0,\alpha_1\in[R,R]$ tais que

$$\begin{aligned}(x^{p^n}+y^{p^n}+\alpha)^p &= (x^{p^n}+y^{p^n})^p+\alpha^p+\alpha_0\\ &= x^{p^{n+1}}+y^{p^{n+1}}+\alpha_1+\alpha^p+\alpha_0\end{aligned}$$

Segue-se então que $(x+y)^{p^{n+1}}\equiv x^{p^{n+1}}+y^{p^{n+1}} \qquad mod[R,R]$ ■

Definição 1.4 *Denotando por $\sim$ a relação de conjugação no grupo G, definimos para um elemento $\alpha=\sum_g \alpha(g)g$ do anel de grupo RG,*

$$\tilde{\alpha}(g) = \sum_{h\sim g}\alpha(h)$$

Teorema 1.6 *Se $\alpha\in[RG,RG]$, então $\tilde{\alpha}(x)=0$ para todo $x\in G$.*

Prova:

$$\begin{aligned}\alpha &= \Big[\sum_g \beta(g)g,\sum_h\gamma(h)h\Big]\\ &= \sum_{g,h}\beta(g)\gamma(h)[g,h]\\ &= \sum_{g,h}\beta(g)\gamma(h)(gh-hg)\end{aligned}$$

Como gh e $hg(=g^{-1}ghg)$ são conjugados, podemos concluir que $\tilde{\alpha}(x)=0$ para todo $x\in G$.

■

Teorema 1.7 (Zassenhaus) *Se $u \in \mathcal{U}(\mathbb{Z}G)$ com $\circ(u) = p^n, p$ um primo e $|G| < \infty$. Então existe um elemento $g \in supp(u)$ tal que $\circ(g) = p^n$ e $\tilde{u}(g) \neq 0$.*

Prova: Sendo $u = \sum u(g)g$, pelo Teorema (1.5), para $R = \mathbb{Z}G/p\mathbb{Z}G$ obtemos:

$$1 = u^{p^n} \equiv \sum u(g)^{p^n} + \beta \mod p\mathbb{Z}G$$

para algum $\beta \in [\mathbb{Z}G, \mathbb{Z}G]$. Do Teorema (1.6), $\beta(1) = 0$ e portanto,

$$\begin{aligned} 1 &\equiv \sum_{g^{p^n}=1} u(g)^{p^n} \mod p \\ &\equiv \sum_{\circ(g)=p^n} u(g)^{p^n} + \sum_{g^{p^{n-1}}=1} u(g)^{p^n} \mod p \\ &\equiv \sum_{\circ(g)=p^n} u(g)^{p^n} + \Big(\sum_{g^{p^{n-1}}=1} u(g)^{p^{n-1}} \Big)^p \mod p \end{aligned}$$

Como $\circ(u) = p^n$, pelo Corolário (1.1) temos

$$u^{p^{n-1}}(1) \equiv \sum_{g^{p^{n-1}}=1} u(g)^{p^{n-1}} \equiv 0 \mod p$$

Assim, concluímos que

$$\sum_{\circ(g)=p^n} u(g)^{p^n} \not\equiv 0 \mod p$$

Segue-se então que existe $g_0 \in G$ de ordem p^n com $u(g_0) \neq 0$ e $\tilde{u}(g_0) \neq 0$.

■

Os três Teoremas seguintes são mostrados em [7].

Teorema 1.8 *Se $G = N \rtimes X$, onde N é nilpotente. Então qualquer subgrupo finito H de $\mathcal{U}_1(\mathbb{Z}G)$ com $(|H|, |N|) = 1$ é conjugado a um subgrupo de $\mathcal{U}_1(\mathbb{Z}G)$, i.e, $H^\alpha \subset \mathcal{U}_1(\mathbb{Z}G)$ para algum $\alpha \in \mathcal{U}(\mathbb{Q}G)$.*

Teorema 1.9 *Seja $G = \langle a \rangle \rtimes \langle x \rangle$ tal que $(\circ(a), \circ(x)) = 1$. Então qualquer subgrupo finito de $\mathcal{U}_1(\mathbb{Z}G)$ é racionalmente conjugado a um subgrupo de G.*

Teorema 1.10 *Se $G = P \rtimes X$, onde P é im p-grupo que não divide $|X|$. Seja H um subgrupo finito de $\mathcal{U}(1 + \Delta(G, P))$. Então existe um $\alpha \in \mathcal{U}(\mathbb{Q}G)$ tal que $H^\alpha \subset G$.*

Sendo N um subgrupo normal de um grupo finito G e ψ a aplicação natural de $\mathbb{Z}G$ em $\mathbb{Z}(G/N)$, temos o seguinte teorema cuja demonstração pode ser encontrada em [2].

Teorema 1.11 *Seja H um subgrupo finito de $\mathcal{U}_1(\mathbb{Z}G)$ tal que $(|H|, |N|) = 1$ e G_0 um subgrupo de G com $(|G_0|, |N|) = 1$. Então H é racionalmente conjugado a G_0 se, e somente se $\psi(H)$ for conjugado de $\psi(G_0)$ em $\mathbb{Q}(G/N)$. Neste caso se H for um subgrupo próprio de $\mathcal{U}_1(\mathbb{Z}G)$, então ψ é injetora sobre H.*

1.2 Grupos de Frobenius

Definição 1.5 *Um grupo G é de Frobenius se existe um subgrupo H próprio não trivial tal que $H \cap H^x = 1$, para todo $x \in G \setminus H$.*

No caso em que G for um grupo finito, o seguinte teorema garante que $N = G \setminus \bigcup_{x \in G} (H^x - 1)$ é um subgrupo normal de G.

Teorema 1.12 (Wielandt) *Suponha que G seja um grupo finito com subgrupos H e K tais que $K \trianglelefteq H$ e $H \cap H^x \leq K$ para todo $x \in G \setminus H$. Seja N o conjunto de todos elementos de G que não pertencem a nenhum conjugado de $H \setminus K$. Então N é subgrupo normal de G tal que $G = HN$ e $H \cap N = K$.*

A demonstração desse teorema pode ser encontrada na referência [6].

Sendo G um grupo finito, H é chamado de um *complemento de Frobenius* e N o *núcleo de Frobenius*. Além disso G pode ser representado por

$$G = N \rtimes H$$

Teorema 1.13 (Propriedades) *Seja um grupo de Frobenius finito com complemento H e núcleo $N = G \setminus \bigcup_{x \in G} (H^x - 1)$. Então temos as seguintes propriedades:*

(i) *Se $g \in G$, então $\circ(g)$ divide $|H|$ ou $|N|$;*

(ii) *Se $1 \neq x \in N$, então $C_G(x) \subset N$;*

(iii) *Se $1 \neq x \in H$, então $C_G(x) \subset H$;*

(iv) *$|H|$ e $|N|$ são coprimos;*

(v) *N é nilpotente*

(vi) *Os p-subgrupos de Sylow são cíclicos se $p > 2$, e se $p = 2$ os 2-subgrupos de Sylow são cíclicos ou quatérnios*

(vii) *Se $2 \mid |G|$, então G possui um único elemento de ordem 2 e que deve pertencer ao centro de G.*

Prova: Seja $g \in G$. Se $\circ(g)$ divide $|N|$, então $g \neq N$. Logo $g = h^x$ para algum $h \in H$ e para algum $x \in G$. Então $\circ(x) = \circ(h) \mid |H|$.

Seja agora $1 \neq x \in N$. Se $y \in C_G(x)$ e $y \notin N$, então $y = h^g$ para algum $h \in H$ e para algum $g \in G$. Como $y^x = y$, então $h^{gx} = h^g$ e portanto $h^{gxg^{-1}} = h$. Note que $gxg^{-1} \in H$, pois caso contrário $h = 1$ e assim $y = 1 \in N$. Logo $x \in H^g$, implicando que $x^{g^{-1}} \in H \cap N = 1$ e assim $x = 1$. Absurdo.

Mostremos agora que $C_G(x) \subset H$, para $1 \neq x \in H$. Se $y \in C_G(x)$, então $1 \neq x = x^y \in H^y \cap H$. Logo $y \in H$.

Suponha que $(|N|, |X|) \neq 1$. Então existe um primo p que divide $|H|$ e $|N|$. Seja P um p-subgrupos de Sylow de H e Q um p-subgrupos de Sylow de G tal que $P \subset Q$, com $P \neq Q$. Assim P é um subgrupo próprio do normalizador $N_Q(P)$ de P em Q. Seja $x \in N_Q(P)$ tal que x não pertença a P. Como $P = P^x \subset H^x \cap H$ e G é de Frobenius, x deverá pertencer a H. Logo $P \neq P\langle x \rangle$ é um p-grupo de H diferente de P, o que é um absurdo. Logo $(|N|, |X|) = 1$.

Para $(v), (vi)$ e (vii) veja referência [5].

■

Teorema 1.14 *Seja G um grupo finito. As seguintes condições são equivalentes.*

(i) *G é um grupo de Frobenius com complemento H de ordem m.*

(ii) *G tem um subgrupo próprio não trivial de ordem n se $|G| = mn$.*

(iii) *$|G| = mn$, com $(m.n) = 1$. Se $g \in G$ então $g^m = 1$ ou $g^n = 1$.*

Além disso se $N = \{g \mid g^n = 1\}$ então N é um subgrupo normal próprio não trivial de G.

Prova: Veja [5].

Capítulo 2

Conjecturas de Zassenhaus

Pelo Corolário (1.2), temos que as unidades de torção de $u \in \mathcal{U}_1(\mathbb{Z}G)$ são triviais, i.e., pertencem a G, se G for abeliano. Uma conjectura de Zassenhaus, extende esse resultado, sem que G não seja necessariamente comutativo. Denotaremos essa conjectura por (ZC1) como em [7]. Essa conjectura diz que se $u \in \mathcal{U}_1(\mathbb{Z}G)$ é de ordem finita, então existe $\alpha \in \mathcal{U}(\mathbb{Q}G)$ tal que $\alpha^{-1}u\alpha \in G$. Uma versão mais forte dessa conjectura, que denotaremos por (ZC3) como em [7], afirma que se H é um subgrupo finito de $\mathcal{U}_1(\mathbb{Z}G)$ então H é racionalmente conjugado a um subgrupo de G. Uma versão mais fraca de (ZC1) é chamada de Problema (de investigação) 8 em [7] e que denotaremos por (P8).

(P8) *Sejam G um grupo e $u \in \mathcal{U}_1(\mathbb{Z}G)$ de ordem finita. Então existe um elemento $g \in G$ tal que $\circ(u) = \circ(g)$*

Temos então:

$$(ZC3) \Longrightarrow \ (ZC1) \ \Longrightarrow (P8)$$

Se $G = \langle a \rangle \rtimes \langle x \rangle$ tal que $(\circ(a), \circ(x)) = 1$, então pelo Teorema (1.9), podemos dizer que (ZC1) vale para $\mathbb{Z}G$ e portanto (P8) se verifica para $\mathbb{Z}G$. Também temos que essas três conjecturas valem para grupos nilpotentes, pois já foi provado por A. Weiss que se G for nilpotente então (ZC3) vale para $\mathbb{Z}G$.

Seja G um grupo de Frobenius finito com núcleo de Frobenius N e complemento de Frobenius X. Pelo Teorema (1.14) a ordem de qualquer elemento de G divide $|X|$ ou divide $|N|$. Mostremos algo similar para unidades no anel $\mathbb{Z}G$, i.e., se G forum grupo de Frobenius com núcleo de Frobenius N e complemento de Frobenius X, então para toda unidade de torção $\mathcal{U}_1(\mathbb{Z}G)$, a ordem de u divide $|N|$ ou divide $|X|$. Esse será nosso principal resultado que será utilizado para verificar a validade de (P8) para grupo de Frobenius em que seu complemento possa ser imerso em um anel de divisão e para grupo de Frobenius de ordem ímpar.

2.1 Resultado Principal

Teorema 2.1 (Teorema Principal) *Seja G um grupo de Frobenius com núcleo de Frobenius N e complemento de Frobenius X. Se $u \in \mathcal{U}_1(\mathbb{Z}G)$, é uma unidade de ordem finita, então $\circ(u)$ divide $|N|$ ou $\circ(u)$ divide $|X|$.*

Prova: Sejam $n = |N|$ e $m = |X|$. Suponha que exista uma unidade de torção $u \in \mathcal{U}_1(\mathbb{Z}G)$ tal que $\circ(u)$ não divida n e $\circ(u)$ não divida m. Portanto, $(n, \circ(u)) \neq 1$ e $(m, \circ(u)) \neq 1$. De fato, se $(n, \circ(u)) = 1$ existiriam $a, b \in \mathbb{Z}$, tais que,

$$1 \;=\; \circ(u)a + nb$$

Como $|G| = mn$, pelo Teorema (1.4) existe $d \in \mathbb{Z}$, tal que, $mn = |G| = \circ(u)d$. Logo

$$m = \circ(u)am + \circ(u)bd \;\Rightarrow\; \circ(u) \mid m$$

Absurdo, pois estamos supondo que $\circ(u)$ não divida m. Assim existem primos p, q tais que $p \mid \circ(u)$, $p \mid n$, $q \mid \circ(u)$ e $q \mid m$. Como G é de Frobenius, $(n, m) = 1$ e portanto $p \neq q$. Sejam $v, w \in \langle u \rangle$ com $\circ(v) = p$ e $\circ(w) = q$. Pondo $u' = vw$ e como v e w comutam, temos

$$(vw)^{pq} \;=\; v^{pq}w^{pq} = 1$$

Se $\circ(u') = 1$, $v = w^{-1}$. Assim $v \in \langle w \rangle$ e portanto p dividiria q. Supondo que $\circ(u') = p$, teremos $w^p = 1$ e assim q dividiria p. Analogamente p dividiria q se suposéssemos que $\circ(u') = q$. Segue-se então que $\circ(u') = pq$. Como u' é potência de u, $\varepsilon(u') = 1$. Além disso, $\circ(u')$ não divide n e $\circ(u')$ não divide m. Caso $\circ(u') \mid n$, existirá $k \in \mathbb{Z}$, tal que, $n = pqk$, e assim q dividiria n. Analogamente, obteríamos que p dividiria m se suposéssemos que $\circ(u') \mid m$. Então podemos supor desde o ínicio que $u = vw$, com $\circ(v) = p$ e $\circ(w) = q$.

Seja $\psi : \mathbb{Z}G \to \mathbb{Z}X$ o homomorfismo induzido pelo homomorfismo natural $G \to X \simeq G/N$. Se $\psi(v) \neq 1$, então $\circ(\psi(v)) = p$. Como $\varepsilon(\psi(v)) = 1$, pelo Teorema (1.4) teremos que $p \mid m$ contradizendo nossa hipótese. Assim devemos ter que $\psi(v) = 1$. Pelo Teorema (1.8) existe $\gamma \in \mathcal{U}_1(\mathbb{Q}G)$ tal que $w^\gamma = \gamma^{-1}w\gamma \in \mathcal{U}_1(\mathbb{Z}G)$. Então $w^\gamma = \psi(w^\gamma) = \psi(w)^{\psi(\gamma)}$. Se $\psi(w) = 1$, então $w^\gamma = 1$, e portanto $w = 1$. Absurdo, pois $\circ(w) = q$. Logo $\psi(w) \neq 1$, e portanto $\psi(u) \neq 1$. Além disso $\psi(u) \neq -1$, pois $\varepsilon(u) = 1$. Pelo Corolário (1.1)

$$\sum_{g \in N} u(g) \;=\; 0 \tag{2.1}$$

Como p e q são primos distintos $q \not\equiv 0 \; mod \; p$. Portanto existe um inteiro positivo t tal que,

$$q^t \equiv 1 \; mod \; p$$

Logo $\exists\, r \in \mathbb{Z}$; $q^t = 1 + pr$. Como v e w comutam,

$$u^{q^t} = (vw)^{q^t} = v^{q^t} w^{q^t} = v^{q^t} = v^{pr+1} = v$$

Sendo $R = \mathbb{Z}G/q\mathbb{Z}G$ um anel de característica prima q e $I = q\mathbb{Z}G$, tem-se pelo Teorema (1.5)

$$(u+I)^{q^t} \equiv \sum (u(g)g + I)^{q^t} \qquad mod\; [R,R]$$

Como podem existir $h, g \in G$ com $g^{q^t} = h^{q^t}$, teremos

$$u^{q^t} + I \equiv \sum \dot{u}(g) g^{q^t} + I \qquad mod\; [R,R]$$

onde a soma é sobre elementos distintos de G e $\dot{u}(g) = \sum_{h^{q^t} = g^{q^t}} u(h)$. Sendo $[R,R] \simeq ([\mathbb{Z}, G\mathbb{Z}G] + I)/I$, existem $\alpha \in [\mathbb{Z}G, \mathbb{Z}G]$ e $\beta \in \mathbb{Z}G$, tais que,

$$u^{q^t} = \sum \dot{u}(g) g^{q^t} + \alpha + q\beta$$

Como $u^{q^t} = v$, então $u^{q^t} \neq \pm 1$ e assim pelo Corolário (1.1) temos $u^{q^t}(1) = 0$. Segue-se que

$$u^{q^t} = \sum_{1 \neq g \in N} \Big(\dot{u}(g) g^{q^t} + \alpha(g) g + q\beta(g) g \Big) + \sum_{g \notin N} \Big(\dot{u}(g) g^{q^t} + \alpha(g) g + q\beta(g) g \Big)$$

Mostremos agora que,

$$1 \neq g^{q^t} \in N \;\Leftrightarrow\; 1 \neq g \in N$$

Seja $1 \neq g^{q^t} \in N$. Então $1 \neq \circ(g^{q^t})$ é um divisor de $|N|$. Como $\circ(g^{q^t}) \mid \circ(g)$, temos que $(|N|, \circ(g)) \neq 1$. Como G é de Frobenius $\circ(g) \mid |N|$ ou $\circ(g) \mid |X|$. Se $\circ(g)$ dividisse $|X|$ teríamos $(|N|, |X|) \neq 1$ já que $\circ(g) \neq 1$. Absurdo. Logo $\circ(g) \mid |N|$. Se $g \notin N$, então $g = h^x$; $h \in X$ e $x \in G$ e novamente teríamos que $\circ(g) \mid |X|$. Portanto $1 \neq g \in N$. Suponha agora que $1 \neq g \in N$. Então $g^{q^t} \in N$ e $g^{q^t} \neq 1$, pois se $g^{q^t} = 1$, $\circ(g)$ seria uma potência de q e como $\circ(g)$ divide $n = |N|$ implicaria que $q \mid n$, o que é uma contradição. Pelo Teorema (1.6), $\tilde{\alpha}(g) = 0,\ \forall\ g \in G$. Então,

$$1 = \psi(v) = \psi(u^{q^t}) = \sum_{1 \neq g \in N} \Big(\dot{u}(g) + q\beta(g) \Big) \tag{2.2}$$

Mas $0 = (u^{q^t})(1) = \dot{u}(1) + q\beta(1)$, pois $\alpha(1) = 0$. Logo (2.2) pode ser substituído por

$$1 \;=\; \sum_{g\in N} \Big(\dot{u}(g) + q\beta(g)\Big)$$

Cada $\dot{u}(g)$ é uma soma de q^t-ésimas potências de coeficientes de u e como para todo inteiro a, temos $a^{q^t} \equiv a \; mod \; q$, obtemos

$$1 \;\equiv\; \sum_{g\in N} u(g) \quad mod\; q \tag{2.3}$$

Assim (2.3) contradiz (2.1), terminando portanto nossa demonstração.

■

Corolário 2.1 *Seja G um grupo de Frobenius de ordem p^nq^m, onde p, q são primos. Então (ZC1) vale para G, i.e., para todo $u \in \mathcal{U}_1(\mathbb{Z}G)$ de ordem finita, existe $\alpha \in \mathcal{U}(\mathbb{Q}G)$ tal que $\alpha^{-1}u\alpha = g \in G$.*

Prova: Seja N o núcleo de Frobenius de G e X um complemento de Frobenius de G. Como $(|N|, |X|) = 1$, podemos supor que $|N| = p^n$ e $|X| = q^m$. Seja $u \in \mathcal{U}_1(\mathbb{Z}G)$ de ordem finita. Pelo Teorema (2.1) $\circ(u) \mid |N|$ ou $\circ(u) \mid |X|$.

Suponha inicialmente que $\circ(u)$ divida $|N| = p^n$. Seja $\psi : \mathbb{Z}G \to \mathbb{Z}(G/N)$ o homomorfismo canônico. Como $\varepsilon(u) = 1$ então $\varepsilon(\psi(u)) = 1$ e uma vez que $\circ(\psi(u)) \mid \circ(u)$, então $\circ(\psi(u)) < \infty$. Pelo Teorema (1.4) $\circ(\psi(u)) \mid |G/N| = |X| = q^m$. Além disso $\circ(\psi(u)) \mid |N|$. Logo $\circ(\psi(u)) = 1$ o que implica $u - 1 \in \Delta(G, N)$. Pelo Teorema (1.10) existe $\alpha \in \mathcal{U}(\mathbb{Q}G)$ tal que $\langle u\rangle^\alpha \subset G$, e assim $u^\alpha \in G$.

Agora se $\circ(u) \mid |X|$, considere $\psi : \mathbb{Z}G \to \mathbb{Z}(G/N) \simeq \mathbb{Z}X$ a aplicação induzida pelo homomorfismo natural. Neste caso, $(\circ(u), |N|) = 1$ e como $|X|$ é potência de um primo, X é nilpotente. Pelo Teorema (1.8) (ZC3) é válido para X. Logo $\exists\ \beta \in \mathcal{U}(\mathbb{Q}X)$ tal que $\psi(u)^\alpha = x \in X \simeq G/N$. Sendo $\psi(x) = x$, pelo Teorema (1.11), u é racionalmente conjugado a x, concluindo assim nossa demonstração.

■

Lema 2.1 *Seja G um grupo de Frobenius com núcleo de Frobenius N e complemento de Frobenius X. Seja $u \in \mathcal{U}_1(\mathbb{Z}G)$, uma unidade de torção de ordem prima p. Então u é racionalmente conjugado a um elemento em G.*

Prova: Se $\circ(u) = 2$ e não existir $F \trianglelefteq G$ tal que $G/F \simeq S_5$ ou $\circ(u) = p > 2$ o resultado já foi mostrado em [3]. Portanto precisamos considerar somente o caso quando $p = 2$ e quando existir $F \trianglelefteq G$ tal que $G/F \simeq S_5$. Neste caso G não é solúvel, pois caso contrário G/F seria solúvel e portanto S_5 seria solúvel, o que é um absurdo, pois S_5 não é solúvel. X também não é solúvel, já que $X \simeq G/N$ e N é solúvel.

Como todo grupo de ordem ímpar é solúvel, temos que 2 divide $|X|$ e 2 não divide $|N|$ pois $(|N|, |X|) = 1$. Assim $(\circ(u), |N|) = 1$ e pelo Teorema (1.8) existe $u \in \mathcal{U}(\mathbb{Q}G)$, tal que, $u^\alpha = u_1 \in \mathbb{Z}X$. Pelo Teorema (1.13) existe um único elemento de ordem 2 em X e portanto pertence ao centro de X. Pelo Teorema (1.7) existe $g \in \sup(u_1)$ tal que $\circ(g) = \circ(u_1) = 2$. Logo g é o único elemento de ordem 2 de X e que pertence ao

centro de X. Sendo $v = u_1 g$, então $v(1) = u_1(g) \neq 0$. Pelo Teorema (1.2), $v = \pm 1$. Se $v = -1$, então

$$-1 \;\; = \;\; \varepsilon(v) = \varepsilon(u_1)\varepsilon(g) = 1$$

Absurdo. Logo $v = 1$ e portanto

$$u^{\alpha} \;\; = \;\; u_1 = g^{-1} = g \;\; \in X \leq G$$

■

Teorema 2.2 *Seja G um grupo de Frobenius finito e seja H uma base de grupo normalizada de $\mathbb{Z}G$, i.e., $H \leq \mathcal{U}_1(\mathbb{Z}G)$, tal que $|H| = |G|$. Então H é um grupo de Frobenius.*

Prova: Seja G um grupo de Frobenius com núcleo de Frobenius N e complemento de Frobenius X. Seja H uma base de grupo normalizada. Defina $H_0 = H \cap (1 + \Delta(G, N))$. Queremos mostrar que todo primo p que divide $|H_0|$, p deverá dividir $|N|$. Com efeito, se $p \mid |H_0|$, existe $h \in H_0$ de ordem p. Seja $h = 1 + \tau$; $\tau \in \Delta(G, N)$. Pelo Lema (2.1), existe $\alpha \in \mathbb{Q}G$ e $g \in G$, tal que $g = \alpha^{-1} h \alpha$, e portanto $g = 1 + \alpha^{-1}\tau\alpha$, onde $\alpha^{-1}\tau\alpha \in \Delta_{\mathbb{Q}}(G, N) \cap \mathbb{Z}G \subset \Delta(G, N)$. Portanto $g = \alpha^{-1} h \alpha \in (1 + \Delta(G, N)) \cap G = N$. Logo pelo Teorema de Lagrange $p = \circ(g) = \circ(h) \mid |N|$. Seja $\psi : \mathbb{Z}G \to \mathbb{Z}(G/N)$ a aplicação natural $\varphi : H \to \mathcal{U}_1(\mathbb{Z}(G/N))$ definida por $\varphi(\lambda) = \psi(\lambda)$.
Observe que φ é um homomorfismo de grupos. Além disso,

$$Ker\varphi = \{\lambda \in H; \varphi(\lambda) = 1\} \;\; = \;\; H \cap (1 + \Delta(G, N)) = H_0$$

Assim $H_0 = Ker\varphi \trianglelefteq H$. Pelo Teorema de Isomorfismo de Grupos,

$$H/H_0 = H/Ker\varphi \simeq Im\varphi \;\; \simeq \;\; \mathcal{U}_1(\mathbb{Z}(G/N)) \simeq \mathcal{U}_1(\mathbb{Z}X)$$

Deste modo $(H : H_0) \mid |X|$. Como $|H_0|$ divide $|G| = |N||X|$ e $(|N|, |X|) = 1$, então $|H_0| \mid |N|$. Portanto $(|H_0|, (H : H_0)) = 1$. Pelo Teorema de Schur-Zassenhauses [6]; 9.1.2 $H = H_0 X_0$, como $|X_0| = (H : H_0)$ e como $H_0 \trianglelefteq H$, podemos escrever $H = H_0 \rtimes X_0$. Sendo $|H| = |G|$, então

$$|N||X| = |H_0||X_0| \;\; \Rightarrow \;\; \frac{|X_0|}{|X|} = \frac{|N|}{|H_0|} \in \mathbb{Z}$$

Mas $|X_0| \mid |X|$, e então $|X| = |X_0|$ e $|N| = |H_0|$. Daí se $k \in H$, pelo Teorema (2.1) $\circ(k) \mid |X_0|$. Pelo Teorema (1.14) H é de Frobenius.

■

2.2 Problema 8

Lema 2.2 *Seja H um subgrupo de um grupo G. Se (ZC1) vale para $\mathbb{Z}G$, então (P8) é válido para $\mathbb{Z}H$.*

Prova: Seja $\alpha \in \mathcal{U}_1(\mathbb{Z}H)$ uma unidade de torção. Como (ZC1) vale em $\mathbb{Z}G$, existe $\beta \in \mathbb{Q}G$ tal que $\beta^{-1}\alpha\beta = g \in G$. Sendo $\beta^{-1} = \gamma,\ \beta = \sum_{x\in G}\beta(x)x,\ \gamma = \sum_{y\in G}\gamma(y)y$, então

$$\begin{aligned}\alpha &= \Big(\sum_{x\in G}\beta(x)x\Big)g\Big(\sum_{y\in G}\gamma(y)y\Big)\\ &= \sum_{y\in G}\beta(y^{-1})\gamma(y)y^{-1}gy + \sum_{y\in G}\Big(\sum_{x\neq y^{-1}}\beta(x)\gamma(y)xgy\Big)\end{aligned}$$

Logo $\tilde{\alpha}(g) = \sum_{y\in G}\beta(y^{-1})\gamma(y) = 1$.
Como $\alpha = \sum_{t\in H}\alpha(t)t$, existe $h \in supp(\alpha) \subset H$ que é conjugado a g em G. Assim, $\circ(h) = \circ(g) = \circ(\alpha)$. Portanto (P8) vale para $\mathbb{Z}H$.

■

Lema 2.3 *Seja $G = G_1 \times G_2$ um produto direto de dois grupos G_1 e G_2 com $(|G_1|, |G_2|) = 1$. Se (P8) vale para $\mathbb{Z}G_1$ e para $\mathbb{Z}G_2$, então (P8) é válido para $\mathbb{Z}G$.*

Prova: Seja $\alpha \in \mathcal{U}_1(\mathbb{Z}G)$. Sejam $|G_1| = p_1^{n_1}\cdot\ldots\cdot p_r^{n_r}$ e $|G_2| = q_1^{m_1}\cdot\ldots\cdot q_s^{m_s}$ as decomposições em fatores primos. Como $|G_1|$ e $|G_2|$ são coprimos,

$$G_1 \cap G_2 = 1$$

Também temos que $|G| = |G_1||G_2|$. Pelo Teorema (1.14) $\circ(\alpha) = p_1^{n_1'}\cdot\ldots\cdot p_r^{n_r'}\cdot q_1^{m_1'}\cdot\ldots\cdot q_s^{m_s'}$. Sendo P_i o p_i-subgrupo de Sylow de $\langle\alpha\rangle$ para $i = 1,\ldots,r$ e Q_i o q_i-subgrupo de Sylow de $\langle\alpha\rangle$ para $j = 1,\ldots,s$

$$\begin{aligned}\alpha &= \alpha_1\alpha_2;\\ \alpha_1 &\in P_1\times\ldots P_r,\\ \alpha_2 &\in Q_1\times\ldots Q_s.\end{aligned}$$

Neste caso α_1 e α_2 são potências de α, portanto α_1 e α_2 comutam e uma vez que $(\circ(\alpha_1), \circ(\alpha_2)) = 1$ temos que, $\circ(\alpha) = \circ(\alpha_1)\cdot\circ(\alpha_2)$.
Seja $\psi_1 : \mathbb{Z}G \to \mathbb{Z}(G/G_1) \simeq \mathbb{Z}G_2$ o homomorfismo natural. Como (P8) vale para $\mathbb{Z}G_2$, existe $g_2 \in G_2$ tal que $\circ(g_2) = \circ(\psi_1(\alpha_2))$.
Mostremos agora que $\circ(\alpha_2) = \circ(\psi_1(\alpha_2))$. De fato,

$$(\psi_1(\alpha_2))^{\circ(\alpha_2)} = \psi_1({\alpha_2}^{\circ(\alpha_2)}) = 1$$

portanto, $\circ(\psi_1(\alpha_2)) \mid \circ(\alpha_2)$. Como podemos ver G_1 como subgrupo normal de G, $\langle\alpha_2\rangle$ como subgrupo de $\mathcal{U}_1(\mathbb{Z}G)$ e G_2 como subgrupo de G, pelo Teorema (1.11) ψ_1 é injetivo sobre $\langle\alpha_2\rangle$ e sendo $(\psi_1(\alpha_2))^{\circ(\psi_1(\alpha_2))} = \psi_1({\alpha_2}^{\circ(\psi_1(\alpha_2))}) = 1$, teremos ${\alpha_2}^{\circ(\psi_1(\alpha_2))} = 1$ e assim $\circ(\alpha_2) \mid \circ(\psi_1(\alpha_2))$. Segue-se então que $\circ(g_2) = \circ(\psi_1(\alpha_2)) = \circ(\alpha_2)$.
Definindo agora $\psi_2 : \mathbb{Z}G \to \mathbb{Z}(G/G_2) \simeq \mathbb{Z}G_1$ de forma natural e vendo $\langle\alpha_1\rangle$ como subgrupo de $\mathcal{U}_1(\mathbb{Z}G)$, G_2 como subgrupo normal de G e G_1 como subgrupo de G obteremos de maneira análoga um elemento $g_1 \in G_1$ tal que $\circ(g_1) = \circ(\alpha_1)$. Sendo $G_1 \trianglelefteq G$ e $G_2 \trianglelefteq G$ teremos que

$$g_1g_2(g_2g_1)^{-1} \;=\; g_1g_2g_1^{-1}g_2^{-1} \;\in G_1 \cap G_2 = 1,$$

e então $g_1g_2 = g_2g_1$.
Segue-se que para $g = g_1g_2 \in G$,

$$\circ(g) \;=\; \circ(g_1) \circ (g_2) = \circ(\alpha_1) \circ (\alpha_2) = \circ(\alpha)$$

■

Teorema 2.3 *Seja G um grupo com todos subgrupos de Sylow cíclicos. Então (ZC3) é verdade para $\mathbb{Z}G$.*

Prova: Por um Teorema de Hölder, Burnside e Zassenhaus de [[6], 10.1.10] G é da forma

$$G \;=\; \langle a,\ b \mid a^m = b^m = 1,\ b^{-1}ab = a^r\rangle,$$

onde $r^n \equiv 1\ mod\ m$, m é ímpar, $0 \leq r < m$ e $(m, n(r-1)) = 1$.
Sendo m e $n(r-1)$ são coprimos teremos que $(m, n) = 1$. Logo $\langle a\rangle \cap \langle b\rangle = 1$.
Além disso,

$$\langle a\rangle \;\trianglelefteq\; G,$$

pois $b^{-1}ab = a^r$.
Assim $G = \langle a\rangle \rtimes \langle b\rangle$, e pelo Teorema (1.9), (ZC3) vale para $\mathbb{Z}G$. Segue-se então que (P8) também é válido para $\mathbb{Z}G$.

■

Nosso objetivo agora é estudar (P8) para $\mathbb{Z}D'$, onde D' é um subgrupo do grupo multiplicativo de um anel de divisão D. Se D tiver característica prima p, I. N. Herstein mostrou que qualquer subgrupo D' finito de D é um p'-grupo cíclico e portanto pelo Teorema (1.7), (P8) vale para $\mathbb{Z}D'$. Quando $carD = 0$, S. Amitsur classificou os subgrupos D, que neste caso chamaremo-os de *grupos de Amitsur*. O Teorema de classificação é dado a seguir e omitiremos sua demonstração que pode ser encontrada [1].

Teorema 2.4 (Grupos deAmitsur) *Seja G um grupo finito. Então G é subgrupo de um anel de divisão de característica zero se e somente se G for isomorfo a um dos seguintes grupos:*

(i) Um subgrupo de um anel de divisão cujo os subgrupos de Sylow são cíclicos;

(ii) O grupo octaedral binário de ordem 48;

(iii) Um grupo da forma $C_m \rtimes \mathcal{Q}_{2^n}$, onde C_m é um grupo cíclico de ordem ímpa m, $\mathcal{Q}_{2^n} = \langle a,\ b \mid a^{2^{n-2}} = b^2,\ b^4 = 1,\ a^b = a^{-1}\rangle$ é um grupo quartérnio de ordem 2^n, e onde a centraliza C_m e b inverte os elementos de C_m;

(iv) Um grupo da forma $\mathcal{Q} \times M$, onde $\mathcal{Q}$ é o grupo dos quartérnio de ordem 8, M é um grupo de ordem ímpar cujos todos subgrupos de Sylow são cíclicos e 2 tem ordem multiplicativa módulo $|M|$;

(v) Um grupo da forma $SL(2,3) \times M$, onde M é um grupo cujos todos subgrupos de Sylow são cíclicos, $(|M|, 6) = 1$ e 2 tem ordem multiplicativa módulo $|M|$;

(vi) O grupo binário icosaedral $SL(2,5)$.

Agora já podemos mostrar que (P8) é válido para grupos de Amitsur.

Teorema 2.5 *Seja G um grupo de Amitsur. Se $\alpha \in \mathcal{U}_1(\mathbb{Z}G)$ tem ordem finita, então existe um elemento $g \in G$ tal que $\circ(\alpha) = \circ(g)$.*

Prova:

Estudarmos os casos possíveis de G de acordo com o Teorema (2.4). Para o caso (i), todos os subgrupos de Sylow de G são cíclicos. Portanto pelo Teorema (2.3) teremos que (ZC3) vale para $\mathbb{Z}G$ e assim (P8) também.

Por [2], (ZC3) vale para um grupo binário octaedral. Segue-se então (P8) para $\mathbb{Z}G$, onde G é o grupo do caso (ii).

No caso (iii), podemos supor que $G = C_m \rtimes \mathcal{Q}_{2^n}$, onde C_m é um grupo cíclico de ordem ímpa m, $\mathcal{Q}_{2^n} = \langle a,\ b \mid a^b = a^{-1},\ a^{2^{n-2}} = b^2\rangle$, $a \in C_G(C_m)$ e $b^{-1}cb = b^{-1}$, $\forall\ c \in C_m$. Então para $\alpha \in \mathcal{U}_1(\mathbb{Z}G)$, $\circ(\alpha) < \infty$, podemos escrever $\alpha = \alpha_1\alpha_2$ tal que $\circ(\alpha_1)$ seja ímpar e $\circ(\alpha_2) = 2^t$. Como a ordem de α_2 é potência de um primo, pelo Teorema (1.7) existe $g_0 \in G$ tal que $\circ(\alpha_2) = \circ(g_0) = 2^t$. Assim, $g_0 \in \mathcal{Q}_{2^n}^h$ para algum $h \in G$ e portanto existe $g_0' \in \mathcal{Q}_{2^n}$ tal que $\circ(g_0') = 2^t$. Uma vez que $mmc\mathcal{Q}_{2^n} = mmc\{\circ(g) \mid g \in \mathcal{Q}_{2^n}\} = 2^{n-1} = \circ(a)$, temos que $\circ(g_0') \mid \circ(a)$. Sendo $\langle a\rangle$ cíclico podemos obter $g_2 \in \langle a\rangle$ de modo que $\circ(g_2) = \circ(\alpha_2)$. Como $\varepsilon(\alpha_1) = 1$, pelo Teorema (1.4) $\circ(\alpha_1)$ divide $|G| = 2^n m$, i.e., existe $r \in \mathbb{Z}$ tal que $2^n m = \circ(\alpha_1)r$ e sendo $(\circ(\alpha_1), 2^n) = 1$, existem $x, y \in \mathbb{Z}$, tais que

$$1 = \circ(\alpha_1)x + 2^n y \quad \Rightarrow \quad m = \circ(\alpha_1)xm + \circ(\alpha_1)ry \Rightarrow \circ(\alpha_1) \mid m$$

Como C_m é cíclico, existe $g_1 \in C_m$ tal que $\circ(g_1) = \circ(\alpha_1)$. Então $(\circ(g_1), \circ(g_2)) = 1$ e como a centraliza C_m, $g_1g_2 = g_2g_1$. Tome $g = g_1g_2$, e então $\circ(g) = \circ(g_1) \circ (g_2) = \circ(\alpha_1) \circ (\alpha_2) = \circ(\alpha)$.

Se G for como em (iv), i.e., $G \simeq \mathcal{Q} \times M$, onde $\mathcal{Q}$ é o grupo dos quartérnio de ordem 8, M é um grupo de ordem ímpar, cujos todos subgrupos de Sylow são cíclicos e 2 não divide $|M|$. Como $|\mathcal{Q}| = 2^3$, pelo Teorema (1.7), (P8) vale para $\mathcal{Q}$, pelo Teorema (2.3), também vale para M. O resultado segue-se novamente do Lema (2.3).

Como $SL(2,3)$ é um subgrupo do grupo octaedral binário, pelo Lema (2.2) (P8) vale para $\mathbb{Z}SL(2,3)$, e como vimos anteriormente também vale para M e como $(|M|, 6) = 1$, então para o caso (v), o resultado segue-se novamente do Lema (2.3).

Por [3], (ZC3) vale para $SL(2,5)$, portanto (P8) vale no caso (vi).

■

Teorema 2.6 *Seja G um grupo de Frobenius com núcleo N e complemento X. Se (P8) vale para $\mathbb{Z}X$, então também é válido para $\mathbb{Z}G$.*

Prova: Seja $\alpha \in \mathcal{U}_1(\mathbb{Z}G)$ de ordem finita n. Pelo Teorema (2.1) teremos que n divide $|N|$ ou $|X|$. Suponha inicialmente que n seja um divisor de $|N|$. Então

$$\alpha \;=\; \alpha_1\alpha_2 \cdot \ldots \cdot \alpha_t$$

onde a ordem de cada α_i é uma potência de um primo p_i que é divisor de $|N|$, $1 \leq i \leq t$. Seja P_i o p_i-subgrupo de Sylow de N, $1 \leq i \leq t$. Mostremos que $P_i \trianglelefteq G$. Como $N \trianglelefteq G$, basta verificar que P_i é subgrupo característico de N. Para todo $\sigma \in AutN$, o conjunto

$$\sigma(P_i) \;=\; \{\sigma(h);\ h \in P_i\}$$

é um subgrupo de N de ordem $|P_i|$, i.e., $\sigma(P_i)$ é p_i-subgrupo de Sylow de N. Como N é nilpotente, $\sigma(P_i) = P_i$, $\forall\ \sigma \in AutN$.
Além disso, cada P_i é p_i-subgrupo de Sylow de G. Caso contrário, P_i seria subgrupo próprio de um p_i-subgrupo de Sylow de G, P_i'. Então p_i dividiria $(G : P_i')(P_i' : P) = (G : P_i)$. Mas p_i não divide $(G : N)$ e nem $(N : P_i)$. Logo p_i não divide $(G : N)(N : P_i) = (G : P_i)$. Absurdo.

Pelo Teorema (1.7), para cada i existe $g_i \in G$ tal que $\circ(g_i) = \circ(\alpha_i)$. Sendo $P_i \trianglelefteq G$, então $g_i \in P_i$. Assim para $1 \leq i, j \leq t,\ i \neq j$, temos $g_ig_j = g_jg_i$.
De fato,

$$\begin{aligned} P_i \trianglelefteq G \;&\Rightarrow\; g_jg_i^{-1}g_j^{-1} \in P_i \Rightarrow g_ig_jg_i^{-1}g_j^{-1} \in P_i, \\ P_j \trianglelefteq G \;&\Rightarrow\; g_ig_j^{-1}g_i^{-1} \in P_j \Rightarrow g_ig_jg_i^{-1}g_j^{-1} \in P_j. \end{aligned}$$

Como $P_i \cap P_j = 1$, segue-se que $g_ig_j = g_jg_i$. Sendo $g = \prod_{i=1}^{t} g_i \in G$, temos que,

$$\circ(g_i) \;=\; \prod_{i=1}^{t} \circ(g_i) = \prod_{i=1}^{t} \circ(\alpha_i) = \circ(\alpha)$$

Agora se $n \mid |X|$, pelo Teorema (1.8) α é racionalmente conjugado a um elemento $u \in \mathcal{U}_1(\mathbb{Z}X)$. Como (P8), existe $x \in X \leq G$ tal que $\circ(x) = \circ(u) = \circ(\alpha)$ e segue o resultado.

■

Corolário 2.2 *Seja G um grupo de Frobenius com complemento X. Se X for de Amitsur então (P8) vale para $\mathbb{Z}G$.*

Prova: Pelo Teorema (2.5) (P8) vale para $\mathbb{Z}X$ e o resultado segue-se então do Teorema (2.6).

■

Corolário 2.3 *Seja G um grupo de Frobenius de ordem ímpar com complemento X. Então (P8) vale para $\mathbb{Z}G$.*

Prova: Pelo Teorema (1.13) todo subgrupo de Sylow de X são cíclicos. Assim pelo Teorema (2.5), (P8) é válido para $\mathbb{Z}X$ e o resultado segue-se novamente do Teorema (2.6).

■

Apêndice A

O Teorema de Schur-Zassenhaus

A.1 Subgrupos de Hall

Considere G um grupo finito e π um conjunto não-vazio de primos.

Definição A.1 *Um subgrupo H de G é dito ser um subgrupo de Halll se $(|H|, |G : H|) = 1$. Dizemos ainda que H é um π-subgrupo de Hall de G se $|H|$ é um π-número e $|G : H|$ é um π'-número, onde π' é o conjugado dos primos que não estão em π.*

Observação A.1 *Segue-se da definição acima que se H é um π-subgrupo de Hall, então $(|H|, |G : H|) = 1$ e portanto, H é um subgrupo de Hall. Além disso, $|H|$ deve ser o maior π-número que divide a ordem de G. Por um Teorema de P. Hall, se G for solúvel, sempre existe um π-subgrupo de Hall de G para qualquer conjunto de primos π e quaisquer dois desse subgrupos são conjugados. Veja ainda que se $\pi = \{p\}$, então um π-subgrupo de Hall de G é um p-subgrupo de Sylow de G. Finalmente, observe que, para um dado conjunto de primos π, nem sempre existe um π-subgrupo de Hall para um grupo finito G qualquer. De fato, considere $G = A_5$ e $\pi = \{2, 5\}$. Se A_5 tem um π-subgrupo de Hall H, então $|H| = 20$. Tomando a ação $\varphi : G \to S_X$, onde $X = \{xH;\ x \in A_5\}$, dada por*

$$\begin{array}{rcl} \varphi : G & \to & S_X \\ g & \mapsto & \varphi_g : xH \mapsto gxH \end{array}$$

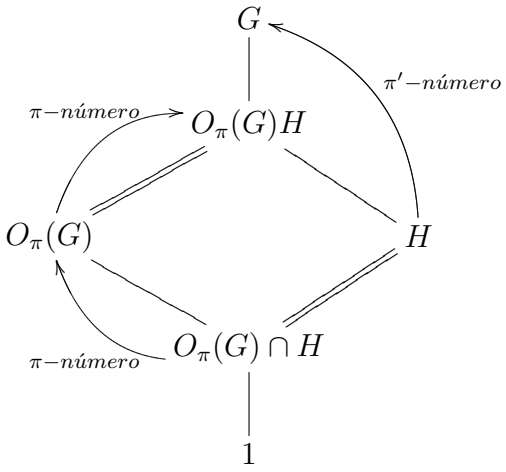
obteríamos, $A_5 \simeq Im\varphi \leq S_X \simeq S_3$, o que é absurdo.

Considere novamente π um conjunto não-vazio de primos. Denotaremos por $O_\pi(G)$ o subgrupo gerado por todos os π-subgrupos normais de G. Em particular, $O_\pi(G)$ é o maior π-subgrupo normal em G.

O lema a seguir será útil na demonstração do Teorema de Schur-Zassenhaus.

Lema A.1 *Seja G um grupo e π um conjugado de primos. Então, $O_\pi(G) \leq H$, $\forall H$, π-subgrupo de Hall de G.*

Prova: Considere H um π-subgrupo de Hall de G. Então,



como $|O_\pi(G)H : O_\pi(G)|$ e $|O_\pi(G) : O_\pi(G) \cap H|$ são π-número segue que $|O_\pi(G)H : H|$ é π-número pois:

$$|O_\pi(G)H : O_\pi(G)||O_\pi(G) : O_\pi(G) \cap H| \;=\; |O_\pi(G)H : H||H : O_\pi(G) \cap H|$$

Mas, por outro lado, $|O_\pi(G)H : H|$ é um π'-número, visto que $|G : H|$ é um π'-número e $|G : H| = |G : O_\pi(G)H||O_\pi(G)H : H|$. Portanto, $|O_\pi(G)H : H|$ é um π-número e π'-número. Logo $|O_\pi(G)H : H| = 1$, ou seja, $O_\pi(G)H = H$. Portanto, $O_\pi(G) \leq H$.

■

A.2 O Teorema de Schur-Zassenhaus

Teorema A.1 (Schur-Zassenhaus) *Se G é um grupo finito e $N \trianglelefteq G$ com $(|G : N|, |N|) = 1$, então existe $H \leqslant G$ tal que $|H| = |G : N|$ e dois quaisquer subgrupos de ordem $|G : N|$ são conjugados.*

Observe que se $H \leqslant G$ com $|H| = |G : N|$, então $G = NH$ e $H \cap N = 1$.
Com efeito, note que $|H \cap N| \mid |H|$ e $|H \cap N| \mid |N|$, portanto $|H \cap N| \mid (|H|, |N|) = 1$. Logo, $H \cap N = 1$. Do Teorema do ìndice segue-se que:

$$|HN| = \frac{|H||N|}{|H \cap N|} \;=\; |G : N||N| = |G|$$

Logo, $G = HN$ e $\frac{G}{N} = \frac{HN}{N} \simeq \frac{H}{H \cap N} = H$.

Prova do Teorema:

1^0 Caso: (Schur) N é abeliano.

EXISTÊNCIA

Seja $Q = \frac{G}{N}$. Note então que Q age sobre N. Basta considerarmos a aplicação

$$\begin{array}{rcll} \psi : Q & \to & AutN & \\ x & \mapsto & n^x, & x = gN \end{array}$$

onde, $n^x = \psi_x : N \to N$ dada por $\psi_x(n) = n^g,\ \forall n \in N$.
Observe então que ψ está bem definida pois se

$$\begin{aligned} x = g_1N = g_2N \Rightarrow g_1N = Ng_2 \Rightarrow g_1 = mg_2,\ m \in N \\ \Rightarrow n^{g_1} = n^{mg_2} = (n^m)^{g_2} = n^{g_2},\ \forall n \in N \end{aligned}$$

Denotemos $n^g = \psi_x(n) := n^x$. Neste caso, para $x \in N$ temos $n^x = n^{1N} = n$. Além disso, segue-se que dados $x, y \in Q$, vale $n^{xy} = (n^x)^y$. De fato, $x = g_1N$ e $y = g_2N$, logo $xy = g_1Ng_2N = g_1g_2N$, donde $n^{xy} = n^{g_1g_2}$ e, por outro lado, $(n^x)^y = (n^{g_1})^y = (n^{g_1})^{g_2} = n^{g_1g_2}$. Portanto, $n^{xy} = (n^x)^y$, ou seja $\psi(xy) = \psi(x)\psi(y)$, donde ψ é um homomorfismo.
Considere agora $T = \{t_x; x \in Q\}$ um transversal de N em G. Note que

$$t_xt_y \in t_xt_yN = t_{xy}N \Rightarrow t_xt_y = t_xt_yc_{(x,y)}, \quad \text{onde } c_{(x,y)} \in N$$

De $(t_xt_y)t_z = t_x(t_yt_z)$ e sendo $z = t_zN$ obtemos que:

$$(t_xt_y)t_z = (t_{xy}c_{(x,y)})t_z = t_{xy}t_zt_z^{-1}c_{(x,y)}t_z = t_{xy}t_z{c_{(x,y)}}^{t_z} = (t_{(xy)z}c_{(xy,z)}){c_{(x,y)}}^z$$

Por outro lado,

$$t_x(t_yt_z) = t_x(t_{yz}c_{(y,z)}) = (t_xt_{yz})c_{(y,z)} = (t_{x(yz)}c_{(x,yz)})c_{(y,z)}$$

Logo,

$$c_{(xy,z)}{c_{(x,y)}}^z = c_{(x,yz)}c_{(y,z)} \tag{A.1}$$

Definamos agora para cada $y \in Q$, $d(y) = \prod_{x \in Q} c_{(x,y)}$. Então valem:

- (i) Como N é abeliano, para um $y \in Q$ fixado temos $d(y) = \prod_{x \in Q} c_{(x,z)} = \prod_{x \in Q} c_{(xy,z)}$.

- (ii) $d(y)^z = \Big(\prod_{x\in Q} c_{(x,z)}\Big)^z = \prod_{x\in Q} {c_{(xy,z)}}^z$
- (iii) $d(yz) = \prod_{x\in Q} c_{(x,yz)}$

Assim,

$$\begin{aligned}
d(z)d(y)^z &\overset{(i)}{=} \Big(\prod_{x\in Q} c_{(xy,z)}\Big)\Big(\prod_{x\in Q} c_{(x,y)}\Big)^z \\
&\overset{(ii)}{=} \Big(\prod_{x\in Q} c_{(xy,z)}\Big)\Big(\prod_{x\in Q} {c_{(x,y)}}^z\Big) \\
&= \prod_{x\in Q} c_{(x,yz)}{c_{(x,y)}}^z \\
&\overset{(A.1)}{=} \prod_{x\in Q} c_{(x,yz)}c_{(y,z)} \\
&= \Big(\prod_{x\in Q} c_{(x,yz)}\Big)\Big(c_{(y,z)}\Big)^m \qquad c_{(y,z)} \text{ não depende de } x \\
&\overset{(iii)}{=} d(yz){c_{(y,z)}}^m
\end{aligned}$$

onde, $m = |Q|$.
Logo obtemos,

$$d(yz) = d(z)d(y)^z {c_{(y,z)}}^{-m} = d(y)^z d(z){c_{(y,z)}}^{-m} \tag{A.2}$$

Como $(m, n_0) = 1$, onde $n_0 = |N|$, e $d(y) \in N$, existe $e_y \in N$ tal que $d(y)^{-1} = {e_y}^m$. Para ver isto basta notar que existem $r, s \in \mathbb{Z}$ tais que $rm+sn_0 = 1$ e tomar $e_y = d(y)^{-r}$. Assim, $d(y) = {e_y}^{-m}$. Portanto,

$${e_{yz}}^{-m} = d(yz) = d(y)^z d(z){c_{(y,z)}}^{-m} = ({e_y}^{-m})^z {e_z}^{-m}{c_{(y,z)}}^{-m} = ({e_y}^z e_z c_{(y,z)})^{-m}$$

E como $(m, n_0) = 1$ segue que $e_{yz} = {e_y}^z e_z c_{(y,z)}$
Defina $s_x = t_x e_x,\ x \in Q$. Então temos que:

$$\begin{aligned}
s_y s_z &= (t_y e_y)(t_z e_z) = (t_y t_z {t_z}^{-1} e_y)(t_z e_z) \\
&= (t_y t_z){e_y}^{t_z} e_z = (t_{yz} c_{(y,z)}){e_y}^z e_z \\
&= t_{yz}({e_y}^z e_z c_{(y,z)}) = t_{yz} e_{yz} \\
&= s_{yz}
\end{aligned}$$

Segue então que a aplicação

$$\begin{aligned}
\theta : Q &\to G \\
x &\mapsto s_x
\end{aligned}$$

é um homomorfismo. Mais ainda, $s_x = 1$ implica que $t_x e_x = 1$, donde, $t_x \in N$. Assim, $x = N$ e, portanto, $x = 1_Q$. Logo, $Ker\theta = 1$ e portanto, θ é injetiva.
Tome $H = \theta(Q) \leq G$. Certamente $|H| = |Q| = m = |G : N|$. Isto prova a existência de H em G.

CONJUGAÇÃO

Considere H e H^* subgrupos de G com $|H| = |H^*| = |G : N| = m$. Então, $G = HN = H^*N$, com $H \cap N = H^* \cap N = 1$. Definamos então a seguinte aplicação:

$$\begin{aligned} \Psi : Q &\to H \\ x &\mapsto u_x \end{aligned}$$

onde $x = u_x N$. Veja que $x \in Q = \frac{HN}{N}$, então $x = u_x n_x N = u_x N$, onde $u_x \in H$ e $n_x \in N$. Observe que se $x = h_1 N = h_2 N$, então $h_2^{-1} h_1 N = N$, donde, $h_2^{-1} h_1 \in HN = 1$ e, neste caso, $h_1 = h_2$. Isto garante que u_x é o único elemento de H tal que $x = u_x N$. Daí Ψ é uma bijeção.
Observe agora que: $u_{xy} N = xy = (u_x N)(u_y N) = u_x u_y N$. Portanto, $u_{xy} = u_x u_y$, visto que o representante é único.
Da mesma forma,

$$\begin{aligned} \Psi : Q &\to H^* \\ x &\mapsto {u_x}^* \end{aligned}$$

é um isomorfismo, tal que ${u_{xy}}^* = {u_x}^* {u_y}^*$.
Ora, $x = u_x N = {u_x}^* N$ e, daí, ${u_x}^* = u_x a_x,\ a_x \in N$. Assim,

$${u_{xy}}^* = {u_x}^* {u_y}^* = u_x a_x u_y a_y = u_x u_y {u_y}^{-1} a_x u_y a_y = u_{xy} {a_x}^{u_y} a_y = u_{xy} {a_x}^y a_y$$

Por outro lado,

$${u_{xy}}^* = u_{xy} a_{xy}$$

Logo,

$$a_{xy} = {a_x}^y a_y \tag{A.3}$$

Defina $b = \prod_{x \in Q} a_x$. Para algum $y \in Q$ fixo temos:

$$b = \prod_{x \in Q} a_x = \prod_{x \in Q} a_{xy} \overset{(A.3)}{=} \prod_{x \in Q} {a_x}^y a_y = \Big(\prod_{x \in Q} a_x \Big)^y {a_y}^m = b^y {a_y}^m$$

Novamente pelo fato de termos $(m, n_0) = 1$, segue a exiatência de $c \in N$ tal que $b = c^m$. Logo,

$$\begin{aligned} c^m &= (c^m)^y {a_y}^m = (c^y a_y)^m \Rightarrow [\underbrace{c^{-1}(c^y a_y)}_{\in N}]^m = 1 \Rightarrow c^{-1}(c^y a_y) = 1 \\ &\Rightarrow a_y = c^{-y}c \end{aligned} \tag{A.4}$$

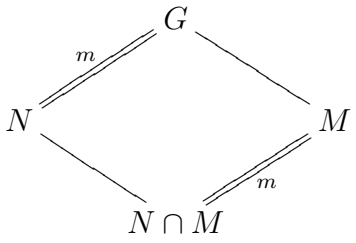
Portanto, ${u_y}^* = u_y a_y \overset{(A.4)}{=} u_y c^{-y} c = u_y (c^{-1})^{u_y} c = c^{-1} u_y c$.
Sendo Ψ e Ψ^* sobrejetoras segue-se que

$$H^* = \{{u_y}^*;\ y \in Q\} = c^{-1}\{u_y;\ y \in Q\}c = c^{-1}Hc = H^c$$

2^0 Caso: Caso Geral

EXISTÊNCIA

Seja p um divisor primo de $|N|$ e seja $P \in SylpN$. Considere $L = N_G(P)$, $C = Z(P) \neq 1$ e faça $M = N_G(C)$. Temos $C \overset{\lhd}{car} P \trianglelefteq L$, donde, $C \trianglelefteq L$. Logo $L \leq M$.
Pelo Argumento de Fratini, $G = LN = MN$. Assim:



Fazendo $N_1 = N \cap M$, segue do 2^0 Teorema dos Isomorfismos que
$|M : N_1| = |G : N| = m$. Então, $\left|\frac{M}{C}\right| < |G|$ e $\frac{N_1}{C} \trianglelefteq \frac{M}{C}$ com: $\left(\left|\frac{M}{C} : \frac{N_1}{C}\right|, \left|\frac{N_1}{C}\right|\right) = 1$, visto que $\left|\frac{M}{C} : \frac{N_1}{C}\right| = |M : N_1| = m$ e $\left|\frac{N_1}{C}\right| \mid |N|$.
Por indução, existe $\frac{K}{C} \leq \frac{M}{C}$, com $\left|\frac{K}{C}\right| = m = |G : N|$. Assim, $\frac{M}{C} = \frac{K}{C}\frac{N_1}{C}$ e $\frac{N}{C} \cap \frac{N_1}{C} = \bar{1}$ e portanto $M = KN_1$ e $K \cap N_1 = C$.
Observe agora que $|C|$ é um divisor de $|N|$ e daí, como $|K : C| = m = |G : N|$, conclui-se que $(|C|, |K : C|) = 1$ e pelo fato de C ser abeliano segue do 1^0 Caso a existência de $H \leq K$ com $|H| = |K : C| = |G : N|$. Como $H \leq G$ fica provada a existência no 2^0 Caso.

CONJUGAÇÃO

1^0 Subcaso: $\frac{G}{N}$ é solúvel

Seja π o conjunto de primos que dividem $m = |G : N|$ e considere $R = O_\pi(G)$. Tomemos então H e K subgrupos de G tais que $|H| = |K| = m$. Ora, $|H| = |G : N|$

implica que $|N| = |G : H|$ e do mesmo modo $|N| = |G : K|$. Portanto, $(|H|, |G : H|) = (|N|, |G : K|) = 1$.
Isto garante que H e K são ambos π-subgrupo de Hall de G. Logo pelo Lema (A.1), $R \leq H$ e $R \leq K$, ou seja, $R \leq H \cap K$.
Como $|G : NR| \mid |G : N|$, $|N|$ é π'-número. Pelo 2^0 Teorema dos Isomorfismos vale:

$$\bar{N} = \frac{NR}{R} \simeq \frac{N}{R \cap N} \simeq N$$

Temos ainda que:

$$\Big(\Big|\frac{G}{R} : \frac{NR}{R}\Big|, \Big|\frac{NR}{R}\Big|\Big) = (|G : NR|, |N|) = 1$$

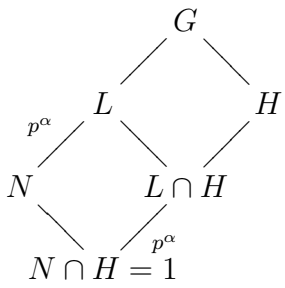
Ainda,

$$\Big|\frac{H}{R}\Big| = \frac{|G : N|}{|R|} = \frac{|G|}{|N||R|} = \frac{|G|}{|NR|} = \frac{|G|}{|R|}\frac{|R|}{|NR|} = \Big|\frac{G}{R} : \frac{NR}{R}\Big|$$

e do mesmo modo, $\left|\frac{K}{R}\right| = \left|\frac{G}{R} : \frac{NR}{R}\right|$.
Assim, se $R \neq 1$, $\left|\frac{G}{R}\right| < |G|$ e por indução, $\frac{H}{R} = \frac{K^{\bar{g}}}{R}$, onde $\bar{g} = gR$, para algum $g \in G$.
Portanto,

$$\frac{H}{R} = \frac{g^{-1}RKgR}{R} = \frac{g^{-1}RKg}{R} = \frac{g^{-1}Kg}{R} \Rightarrow H = K^g$$

Logo podemos supor que $R = 1$ e além disso assumir que $m > 1$ e, portanto, $N \neq G$.
Seja $\frac{L}{N} \trianglelefteq \frac{G}{N}$. Sendo $\frac{G}{N}$ solúvel, segue que $\frac{L}{N}$ é p-abeliano elementar para algum primo em π.
Por Dedekind temos $N(L \cap H) = (NH) \cap L = G \cap L = L$ (*).



Assim, $L \cap H \in SylpL$, visto que temos:

$$H \cap L \simeq \frac{H \cap L}{N \cap (L \cap H)} \simeq \frac{N(L \cap H)}{N} = \frac{L}{N}$$

e ainda,

$$|L : L \cap H| \;=\; |HL : H| = |G : H| = |N| = n_0 \quad \text{e} \quad p \nmid n_0$$

Do mesmo modo $L \cap K \in SylpL$.
Pelo 2^0 Teorema de Sylow, existe $g \in L$ tal que $L \cap H = (L \cap K)^g$.
Mas, $(L \cap K)^g = L^g \cap K^g = L \cap K^g$. Fazendo $S = L \cap H$ segue que $S \trianglelefteq \langle H, K^g \rangle = J$, pois $S \trianglelefteq H$ e $S \trianglelefteq K^g$. Se $J = G$, então $S \trianglelefteq G$ e como S é um π-subgrupo teríamos $S \leq O_\pi(G) = R = 1$. Daí, $L \cap H = 1$ e por $(^*)$ $L = N$. Isto é um absurdo, pois $\frac{L}{N} = \bar{1}$ e $\frac{L}{N} \trianglelefteq \frac{G}{N}$.
Assim, $J \neq G$ e, portanto, $N_0 = N \cap J \trianglelefteq J$ e $(|H|, |N_0|) = (|K^g|, |N_0|) = 1$. Por indução, $H = (K^g)^j = K^{gj}$ para algum $j \in J$, provando que H e K são conjugados em G.

2^0 Subcaso: N é solúvel

Sejam H e K subgrupos de G tais que $|H| = |K| = m$. Podemos supor $N' \neq 1$, pois do contrário N é abeliano e o resultado segue pelo 1^0 Caso.
Ora, como $N' \leq N$ temos $N' \cap H = 1$ e ainda $N' \overset{\triangleleft}{car}\, N \trianglelefteq G$, donde, $N' \trianglelefteq G$. Temos também que $\frac{HN'}{N'} \simeq \frac{H}{N' \cap H} \simeq H$ e, do mesmo modo, $\frac{HN'}{N'} \simeq K$. Além disso, $\frac{N}{N'}$ é abeliano e, portanto, $\frac{N}{N'} \trianglelefteq \frac{G}{N'}$. Pelo 1^0 Caso, $\frac{HN'}{N'}$ e $\frac{KN'}{N'}$ são conjugados em $\frac{G}{N'}$. Logo, $\left(\frac{HN'}{N'}\right)^{\bar{g}} = \frac{KN'}{N'}$ para algum $\bar{g} = gN' \in \frac{G}{N'}$. Assim,

$$\frac{KN'}{N'} \;=\; \left(\frac{HN'}{N'}\right)^{\bar{g}} = \frac{g^{-1}N'HN'gN'}{N'} = \frac{g^{-1}HN'gN'}{N'} = \frac{g^{-1}HgN'}{N'} = \frac{H^gN'}{N'} \;\Rightarrow H^g \leq KN'$$

Agora, $|HN'| = |K||N'| < |K||N| = |G|$, visto que N é solúvel. Novamente por indução. $H^{gx} = K$, $\exists\, x \in KN'$.

3^0 Subcaso: Geral

Sendo $(|N|, |G : N|) = 1$, segue-se que $|G : N|$ ou $|N|$ é ímpar. Então pelo Teorema de Feit-Thompson $\frac{G}{N}$ ou N é solúvel. Pelo subcasos anteriores o resultado segue. ■

Observação A.2 *Vale ressaltar que a condição $N \trianglelefteq G$ é essencial para a demonstração do Teorema de Schur-Zassenhaus. Com efeito, se considerarmos o grupo A_5 e N um 2-subgrupo de Sylow de A_5 temos $(|N|, |A_5 : N|) = 1$ porém, não existe um subgrupo de ordem $|A_5 : N| = 15$ em A_5.*

Observação A.3 *Vale ainda observar que a existência de um complemento N no caso provado por Schur no Teorema A.1 é, na realidade, uma consequência imediata de um teorema mais geral que diz que:*

Teorema A.2 *Se G é um grupo finito, N um subgrupo abeliano normal em G e existe $H \leqslant G$ tal que $N \leqslant H$, $(|G : H|, |N|) = 1$ e N tem complemento em H, então N tem complemento em G.*

Uma prova deste resultado pode ser encontrada em [[8], Teorema 9.3.5].

De posse desse resultado, a existência de um complemento para N, abeliano, segue ao fazermos $H = N$.

Referências Bibliográficas

[1] AMITSUR, S. A. Finite subgroups of division rings. *Trans. Amer. Math. Soc.,* v. 80, p. 361-386, 1955.

[2] DODUCHAEV, M. A.; JURIAANS. S. O. Finite subgroups in integral groups rings. *Canadian Journal of Math.,* v. 48, p. 1170-1179, 1996.

[3] DODUCHAEV, M. A.; JURIAANS. S. O.; POLCINO MILIES, C. Integral group rings of Frobenius groups and the conjectures of H. J. Zassenhaus. *Commum in Algebra,* v. 25, p. 3211-3225, 1997.

[4] JURIAANS. S. O.; POLCINO MILIES, C. Units of integral group rings of Frobenius groups. *J. Group Theory,* v. 3, p. 277-284, 2000.

[5] PASSMAN, D. S. Permutations groups. *New York: W. A. Benjamin,* 1968.

[6] ROBINSON, D. J. S. A course in the theory of groups. *New York: Springer-Verlag,* 1980.

[7] SEHGAL, S. K. Units of integral groups rings. *New York: Longman,* 1993.

[8] SCOTT, W. R. Group Theory. *Englewood Cliffs, NJ.: Prentice-Hall,* 1964.