A NILPOTÊNCIA DO GRUPO DE UNIDADES DE UM ANEL DE GRUPO

Francisco César Polcino Milies

Tese apresentada ao Instituto de Matemática e Estatística da Universidade de São Paulo para a obtenção do título de DOUTOR EM MATEMÁTICA

Orientador: Prof. Dr. Alfredo R. Jones Rodriguez

Durante a elaboração deste trabalho, o autor recebeu apoio financeiro do B.N.D.E., contratos FUNTEC nº 100 e nº 154 e FINEP convênio 134/C.T.

São Paulo, dezembro de 1974

Aos meus pais

A memória do Prof.

Dr. CARLOS BENJAMIN DE LYRA

A G R A D E C I M E N T O S

Foram tantas as pessoas que colaboraram na nossa formação matemática, que agradecimentos detalhados se tornam impossíveis sem se cometer injustas omissões. Mesmo assim queremos / agradecer particularmente às seguintes pessoas:

Aos Professores Fernando Fortaleza e Jorge Lewowicz da Universidad de la República, cuja assistência e conselhos nos começos de nosso estudo foram bem além do que poderíamos merecer.

Ao Professor Waldyr Muniz Oliva, pela orientação e estímulo, durante os nossos estudos no I.M.E.- U.S.P.

Ao colega Luiz Gonzaga Xavier de Barros, pelas conversas úteis quando da realização dêste trabalho.

O Professor Alfredo R. Jones merece agradecimentos especiais. Não sòmente nos orientou na realização desta tese, como acompanhou inteiramente a nossa carreira. Sua influência foi decisiva na nossa escolha da matemática como profissão e da álgebra como área de especialização, tendo nos orientado desde os começos do nosso estudo, até o estágio que ora alcançamos.

Finalmente, agradecemos à Secretaria do Departamento de Matemática do I.M.E.- U.S.P., pelo trabalho de datilografia e ao Snr. Armando G. Segura pela impressão; ambas as tarefas / executadas com dedicação bem acima da estritamente profissional.

C.P.M.

PREFÁCIO

Para desenvolver a teoria dos grupos podem-se seguir / duas linhas de ação: ou atacar os problemas da forma direta, utilizando sua forma abstrata ou utilizar realizações concretas. Esta última linha é a seguida na teoria de representações de grupos finitos e o seu uso tem permitido obter resultados cuja demonstração por métodos diretos ainda não foi obtida ou é bem mais complicada.

A teoria de representações foi desenvolvida de forma / bastante completa e útil por G. Frobenius nas últimas duas décadas do século dezenove. O primeiro tratamento sistemático é devido a W. Burnside "The theory of Groups of Finite Order" publicado pela Cambridge University Press em 1911.

Segundo Curtis-Reiner |9|um segundo estágio de desenvolvimento da teoria de representações teve início em 1929 com os trabalhos de E. Noether quando a teoria foi absorvida no estudo / de módulos e álgebras. Tal coisa foi possível através da noção de álgebra de grupo, que é tão antiga quanto a própria noção de grupo, associando a cada representação de um grupo G sôbre um corpo/ K um módulo sôbre a álgebra KG.

Este fato talvez seja suficiente para dar uma idéia da importância dos anéis de grupo. Ainda, tais anéis são objetos algébricos interessantes em si mesmos e seu estudo é facilitado pelo fato de ter duas operações (soma e produto) além de estrutura de módulo sôbre o anel dos coeficientes. Provavelmente quando a

teoria estiver suficientemente desenvolvida poder-se-a obter novas informações sôbre a teoria dos grupos em geral.

Nos últimos anos tem-se estudado anéis de grupo não apenas com coeficientes num corpo mas considerando-se, em geral, coeficientes em anéis; particularmente no anel dos números inteiros. Neste contexto os anéis de grupo emcontram aplicação também em outras áreas tais como álgebra homológica, cohomologia de grupos e K-teoria.

Nos artigos recentes de P.I.Plotkin |19| e I.Reiner |23| o leitor encontrará uma resenha dos progressos nesta área assim como uma bibliografia abundante.

Nosso propósito neste trabalho é obter condições necessárias e sufucientes para que o grupo das unidades de .. certos/ anéis de grupo seja nilpotente. Nesta direção existem já algumas informações.

Em 1968 J.M.Bateman e D.B.Coleman |1| demonstraram o seguinte:

Teorema - Seja G um grupo finito e K um corpo. Então o grupo das unidades do anel de grupo KG é nilpotente se e sòmente se:

(i) car K = 0 e G é abeliano

(ii) car K = p ≠ 0 e G é o produto direto de um p-grupo e um grupo abeliano.

No ano seguinte K.Motose e H.Tominaga |16| corrigiram um pequeno êrro na demonstração do teorema acima e estenderam o

para o caso em que K é um anel artiniano semisimples(que deve / ser comutativo para que o grupo das unidades seja nilpotente)

No capítulo II estendemos de forma natural estes resultados para anéis comutativos de característica não nula. Para isso estudamos em primeiro lugar os anéis de grupo de p-grupos sobre anéis de inteiros módulo p^n e verificamos que vale um resultado análogo à parte (ii) do teorema de Bateman-Coleman. No caso geral provamos:

Teorema(II.2.3) - Seja R um anel comutativo, com unidade tal que car R = p^n onde p é um inteiro primo e seja G um grupo finito. Então U(RG) é nilpotente se e sòmente se G é o produto direto de um p-grupo e um grupo abeliano.

Teorema(II.2.5) -Seja R um anel comutativo, de característica / $m \neq 0$ tal que $m = p_1^{\alpha}1 \ldots p_t^{\alpha}t$ com $t \geq 2$ é a decomposição em fatores primos de m e seja G um grupo finito. Então U(RG) é nilpotente se e sòmente se G é abeliano.

O primeiro destes resultados foi publicado recentemente I.I.Khripta |15| mas nós o obtivemos independentemente e a nossa técnica é diferente daquela por êle empregada.

Quando se volta a atenção para os anéis de grupos sôbre anéis de característica 0 percebe-se que não será possível estender a condição (i) do teorema citado, já que existem anéis

de grupos não comutativos, sôbre os inteiros, que tem grupo de unidades nilpotente.

Assim, no capítulo III decidimos estudar o caso que a nosso ver é mais importante: os anéis de grupos com coeficientes inteiros. Os principais resultados deste capítulo são:

Teorema (III.1.6) Seja G um grupo finito. Então $U(\mathbb{Z}G)$ é nilpotente se e sòmente se G é comutativo ou um 2-grupo Hamiltoniano.

Teorema (III.1.9) - Seja G um grupo finito, não abeliano. Então, as seguintes afirmações são equivalentes.

(i) $U(\mathbb{Z}G)$ é nilpotente

(ii) $U(\mathbb{Z}G)$ é periódico

(iii) $U(\mathbb{Z}G) = \{\pm 1\} \times G$

(iv) G é um 2-grupo Hamiltoniano

No capítulo IV consideramos anéis de grupos com coeficientes num anel de inteiros p-ádicos. O resultado neste caso é o seguinte:

Teorema (IV.2.1) - Seja p um inteiro primo, $\mathbb{Z} = \lim_{\leftarrow} J_{p^n}$ o anel dos inteiros p-ádicos e G um grupo finito. Então $U(\mathbb{Z}G)$ é nilpotente se e sòmente se G é abeliano.

Quando começamos o estudo dos anéis de grupos sôbre os inteiros, os únicos exemplos por nós conhecidos eram os de Higman |12| e o grupo das unidades de $\mathbb{Z} S_3$ (onde S_3 indica o grupo das permutações de três elementos) que foi estudado por I. Hughes e K.R. Pearson |14|. Utilizando métodos similares decidimos estudar o grupo das unidades de $\mathbb{Z} D_4$, onde D_4 indica o grupo diedral de ordem 8. O resultado deste estudo é o conteúdo do capítulo I.

Os resultados aqui contidos foram anunciados em |21| exceto o teorema (III.1.6) que era então uma conjetura.

Í N D I C E

INDICE DE SÍMBOLOS

CAPÍTULO 0

CONCEITOS BÁSICOS

O propósito deste capítulo é introduzir certas noções e resultados que serão usados frequentemente no presente trabalho. Todos esses conceitos são bem conhecidos e se encontram, por exemplo, no texto clássico de C.W. Curtis e I. Reiner | 9 |, nos livros de D. S. Passman | 18 | e P. Ribemboim | 24 | ou em artigos tais como G. Higman | 12 | ou I. Hughes e K. R. Pearson | 14 |.

Estes fatos serão utilizados nos próximos capítulos sem nenhuma referência específica.

Começaremos construindo o anel de grupo de um grupo finito G (cujo elemento neutro notaremos por e) sobre um anel comutativo com unidade 1.

Indica-se por A^G o conjunto de todas as funções definidas em G com valores em A. Se $\alpha \in A^G$ é usual indicar α pela combinação linear formal $\alpha = \sum_{g \in G} \alpha(g)$. Ainda, indexando os elementos de

G e escrevendo $a_i = \alpha(g_i)$ é usual denotar $\alpha = \sum_{i=1}^{|G|} a_i\, g_i = \sum_i a_i\, g_i$

Definem-se operações em AG por:

$$\sum a_i\, g_i + \sum_i a'_i\, g_i = \sum_i (a_i + a'_i)\, g_i$$

$$\left(\sum_i a_i\, g_i\right)\left(\sum_i a'_i\, g_i\right) = \sum_{i,j} a_i\, a'_j\, g_i\, g_j = \sum_k c_k\, g_k$$

com $c_k = \sum_{(i,j)} a_i\, a'_j$ onde os pares de índices (i,j) são todos aqueles para os quais $g_i\, g_j = g_k$.

Em termos de funções, estamos definindo soma na forma usual:

$$(\alpha+\alpha')(g) = \alpha(g)+\alpha'(g)$$

e produto, pelo produto de convolução:

$$(\alpha\alpha')(g) = \sum_{h\in G} \alpha(h)\ \alpha'(h^{-1}.g)$$

Finalmente define-se o produto de um elemento $\alpha = \sum_i a_i\, g_i$ e AG por um elemento a e A por:

$$a\alpha = \sum_i (aa_i)\, g_i$$

É fácil verificar que, com as operações definidas, AG é uma álgebra com unidade sobre A, onde o elemento unidade é

$1 = \sum_{g\in G} \alpha(g)g$ com $\alpha(e) = 1$ e $\alpha(g) = 0$ se $g \neq e$. Daqui em diante indicaremos por 1 indistintamente a unidade de AG, a unidade de A e o elemento neutro de G.

Definição:- Seja G um grupo finito e A um anel comutativo com unidade. A álgebra construida acima chama-se álgebra de grupo ou anel de grupo de G sobre A e se indica por AG.

A função $i: A \to AG$ definida por $i(a) = a.1$, $\forall a \in A$, é um monomorfismo de anéis; portanto é usual identificar A com a sua imagem em AG.

Da mesma forma, a função $i: G \to AG$ que a cada elemento $g \in G$ associa o elemento $\sum_i a_i g_i$ com $a_i = 0$ se $g_i \neq g$ e $a_i = 1$ para $g_i = g$ é monomorfismo de grupos mutiplicativos e também identificaremos G com a sua imagem em AG.

Proposição:- Sejam A e A' anéis comutativos com unidade, G um grupo finito e $f: A \to A'$ um homomorfismo de anéis com unidade. Então, a função $\bar{f}: AG \to A'G$ definida por $\bar{f}\left(\sum_i a_i g_i\right) = \sum_i f(a_i) g_i$ é um homomorfismo de anéis com unidade.

Ainda, se f é respectivamente monomorfismo, epimorfismo ou isomorfismo, $\bar{f}$ também o é.

A demonstração é trivial.

De forma análoga, vale:

Proposição:- Sejam G e G' grupos finitos, A um anel comutativo com unidade e $f: G \to G'$ um homomorfismo de grupos. Então, a função $\bar{f}: AG \to AG'$ definida por $\bar{f}\left(\sum_i a_i g_i\right) = \sum_i a_i f(g_i)$ é um homomorfismo de álgebras.

Ainda, se f é respectivamente monomorfismo, epimorfismo ou isomorfismo, $\bar{f}$ também o é.

Um caso particularmente interessante é o seguinte: o homomorfismo trivial $G \to \{1\}$ se estende a um epimorfismo de álgebras $\varepsilon: AG \to A$ tal que $\varepsilon(\sum_i a_i g_i) = \sum_i a_i$. Esta função que chamaremos <u>índice</u> (chamada <u>augmented function</u> na literatura em inglês) aparecerá com bastante frequência no nosso trabalho.

<u>Definição</u>:- Um elemento $\alpha \in AG$ diz-se uma <u>unidade</u> de AG se existe $\alpha^{-1} \in AG$ tal que $\alpha\alpha^{-1} = \alpha^{-1}\alpha = 1$. O conjunto de todas as unidades de AG é um grupo multiplicativo que notaremos por U(AG).

É fácil ver que se a é uma unidade de A todo elemento da forma ag é uma unidade de AG. Estas unidades são chamadas as <u>unidades triviais</u> de AG. Assim o grupo das unidades triviais de AG é $U(A) \times G$ onde U(A) indica o conjunto das unidades de A.

Define-se $V(AG) = \{\alpha \in U(AG) \mid \varepsilon(\alpha) = 1\}$. Um elemento $\alpha \in V(AG)$ diz-se uma <u>unidade normalizada</u> de AG. É fácil verificar que

$$U(AG) = U(A) \times V(AG).$$

Finalmente, um automorfismo $\phi: AG \to AG$ diz-se um <u>automorfismo normalizado</u> se leva os elementos de G em unidades normalizadas de AG i.e., se $\varepsilon \circ \phi(g) = 1$, $\forall g \in G$.

No caso particular em que K é um corpo de característica p e G um p-grupo tem-se que:

$$U(KG) = \{\alpha \in KG \mid \varepsilon(\alpha) \neq 0\}$$

Consequentemente:

$$V(KG) = \{\alpha \in KG \mid \varepsilon(\alpha) = 1\}.$$

Ver: D.B. Coleman | 7 |.

CAPÍTULO I

O GRUPO DAS UNIDADES DE $\mathbb{Z}D_4$

I.1.- INTRODUÇÃO.- Ao longo deste capítulo, indicaremos por D_4 o grupo dihedral de ordem 8, i.é., o grupo com dois geradores a e b, verificando as relações: $a^4 = b^2 = baba = 1$.

Explìcitamente podemos escrever:

$$D_4 = \{1, a, a^2, a^3, b, ab = ba^3, a^2b = ba^2, a^3b = ba\}$$

No que segue, caracterizaremos o grupo das unidades de $\mathbb{Z}D_4$ em forma muito similar à dada por Hughes e Pearson |14| para o anel de grupo $\mathbb{Z}S_3$, onde S_3 indica o grupo simétrico das permutações de três elementos.

No artigo mencionado os autores propõem várias questões, a saber:

(a) Toda unidade de ordem finita de $\mathbb{Z}G$ é conjugada de uma unidade trivial?

(b) Quais são os subgrupos finitos maximais de $U(\mathbb{Z}G)$?

(c) Todo automorfismo normalizado de $\mathbb{Z}G$ é o produto de um automorfismo interior por um automorfismo de G ?

Utilizaremos a nossa caracterização para responder estas perguntas no caso particular em que $G = D_4$.

I.2. - CARACTERIZAÇÃO DE $U(\mathbb{Z}D_4)$

Consideremos inicialmente a álgebra de grupo $\mathbb{Q}D_4$. Existem cinco representações irredutíveis, não equivalentes de D_4 sôbre $\mathbb{Q}$, definidas nos geradores de D_4 por:

$$T_1(a) = 1,\ T_1(b) = 1;\quad T_2(a) = 1,\ T_2(b) = -1\ ;$$

$$T_3(a) = -1,\ T_3(b) = 1\ ;\ T_4(a) = -1,\ T_4(b) = -1\ ;$$

$$T_5(a) = \begin{bmatrix} -0 & -1 \\ 1 & 0 \end{bmatrix} \qquad T_5(b) = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$$

Consequentemente, existe um isomorfismo de $\mathbb{Q}$ - álgebras:

$$(1) \qquad \phi : \mathbb{Q}D_4 \to \mathbb{Q} \oplus \mathbb{Q} \oplus \mathbb{Q} \oplus \mathbb{Q} \oplus M_2(\mathbb{Q})$$

onde $M_2(\mathbb{Q})$ indica o anel de todas as matrizes de 2x2 com coeficientes em $\mathbb{Q}$. Este isomorfismo está determinado pelo seu valor sobre os geradores de D_4 :

$$(2) \qquad \begin{aligned} \phi\ (a) &= \left(1,\ 1,\ -1,\ -1,\ \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix}\right) \\ \phi\ (b) &= \left(1,\ -1,\ 1,\ -1,\ \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}\right) \end{aligned}$$

Em particular, ϕ é $\mathbb{Q}$-isomorfismo de espaços vetoriais. Em $\mathbb{Q}D_4$ podemos considerar a $\mathbb{Q}$ - base constituída pelos elementos de D_4. Identificando a soma direta de (1) com $\mathbb{Q}^8$ pelo isomorfismo:

$$(x_1, x_2, x_3, x_4, \begin{bmatrix} x_5 & x_6 \\ x_7 & x_8 \end{bmatrix}) \rightarrow (x_1, \ldots, x_8)$$

podemos considerar nela a base canônica de $\mathbb{Q}^8$. Para obter a matriz associada a ϕ nestas bases calculamos:

$$\phi(1) = (1, 1, 1, 1, \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix})$$

$$\phi(a) = (1, 1, -1, -1, \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix})$$

$$\phi(a^2) = (1, 1, 1, 1, \begin{bmatrix} -1 & 0 \\ 0 & -1 \end{bmatrix})$$

$$\phi(a^3) = (1, 1, -1, -1 \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix})$$

$$\phi(b) = (1, -1, 1, -1, \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix})$$

$$\phi(ab) = (1, -1, -1, 1, \begin{bmatrix} -1 & 0 \\ 0 & 1 \end{bmatrix})$$

$$\phi(a^2b) = (1, -1, 1, -1, \begin{bmatrix} 0 & -1 \\ -1 & 0 \end{bmatrix})$$

$$\phi(a^3b) = (1, -1, -1, 1, \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix})$$

Logo a matriz é:

$$A = \begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 & -1 & -1 & -1 & -1 \\ 1 & -1 & 1 & -1 & 1 & -1 & 1 & -1 \\ 1 & -1 & 1 & -1 & -1 & 1 & -1 & 1 \\ 1 & 0 & -1 & 0 & 0 & -1 & 0 & 1 \\ 0 & -1 & 0 & 1 & 1 & 0 & -1 & 0 \\ 0 & 1 & 0 & -1 & 1 & 0 & -1 & 0 \\ 1 & 0 & -1 & 0 & 0 & 1 & 0 & -1 \end{bmatrix}$$

cuja inversa é:

$$A^{-1} = \frac{1}{8} \begin{bmatrix} 1 & 1 & 1 & 1 & 2 & 0 & 0 & 2 \\ 1 & 1 & -1 & -1 & 0 & -2 & 2 & 0 \\ 1 & 1 & 1 & 1 & -2 & 0 & 0 & -2 \\ 1 & 1 & -1 & -1 & 0 & 2 & -2 & 0 \\ 1 & -1 & 1 & -1 & 0 & 2 & 2 & 0 \\ 1 & -1 & -1 & 1 & -2 & 0 & 0 & 2 \\ 1 & -1 & 1 & -1 & 0 & -2 & -2 & 0 \\ 1 & -1 & -1 & 1 & 2 & 0 & 0 & -2 \end{bmatrix}$$

Como A é uma matriz de coeficientes inteiros, é claro que $\phi(\mathbb{Z} D_4) \subset \mathbb{Z} \oplus \mathbb{Z} \oplus \mathbb{Z} \oplus \mathbb{Z} \oplus M_2(\mathbb{Z})$.

Recìprocamente, usando a expressão de A^{-1} segue que dado um elemento $X=(x_1, x_2, x_3, x_4, \begin{vmatrix} x_5 & x_6 \\ x_7 & x_8 \end{vmatrix}) \in \mathbb{Z} \oplus \mathbb{Z} \oplus \mathbb{Z} \oplus \mathbb{Z} \oplus M_2(\mathbb{Z})$ tem-se que $\phi(X) \in \mathbb{Z} D_4$ se e sòmente se as componentes de X verifi-

cam o seguinte sistema de congruências (obtido a partir das filas de A^{-1}) :

$$(A_1)\quad x_1 + x_2 + x_3 + x_4 + 2x_5 + 2x_8 \equiv 0 \pmod 8$$

$$(A_2)\quad x_1 + x_2 - x_3 - x_4 - 2x_6 + 2x_7 \equiv 0 \pmod 8$$

$$(A_3)\quad x_1 + x_2 + x_3 + x_4 - 2x_5 - 2x_8 \equiv 0 \pmod 8$$

$$(A_4)\quad x_1 + x_2 - x_3 - x_4 + 2x_6 - 2x_7 \equiv 0 \pmod 8$$

$$(A_5)\quad x_1 - x_2 + x_3 - x_4 + 2x_6 + 2x_7 \equiv 0 \pmod 8$$

$$(A_6)\quad x_1 - x_2 - x_3 + x_4 - 2x_5 + 2x_8 \equiv 0 \pmod 8$$

$$(A_7)\quad x_1 - x_2 + x_3 - x_4 - 2x_6 - 2x_7 \equiv 0 \pmod 8$$

$$(A_8)\quad x_1 - x_2 - x_3 + x_4 + 2x_5 - 2x_8 \equiv 0 \pmod 8$$

Operando com o sistema na forma usual podemos reduzi-lo a uma forma escalonada. Fazendo inicialmente :

$$(B_1) = (A_1) \text{ e } (B_i) = (A_1) - (A_i), i = 2,\ldots,8$$

temos:

$$(B_1)\quad x_1 + x_2 + x_3 + x_4 + 2x_5 + 2x_8 \equiv 0 \pmod 8$$

$$(B_2)\quad x_3 + x_4 + x_5 + x_6 - x_7 + x_8 \equiv 0 \pmod 4$$

$$(B_3)\quad x_5 + x_8 \equiv 0 \pmod 2$$

$$(B_4)\quad x_3 + x_4 + x_5 - x_6 + x_7 + x_8 \equiv 0 \pmod 4$$

$$(B_5)\quad x_2 + x_4 + x_5 - x_6 - x_7 + x_8 \equiv 0 \pmod 4$$

(B_6) $\quad x_2 + x_3 \quad +2x_5 \equiv 0 \pmod 4$

(B_7) $\quad x_2 \quad + x_4 + x_5 + x_6 + x_7 + x_8 \equiv 0 \pmod 4$

(B_8) $\quad x_2 + x_3 \quad + 2x_8 \equiv 0 \pmod 4$

Agora tomamos $(C_1) = (B_1)$; $(C_2) = (B_8)$; $(C_3) = (B_8) - (B_7)$; $(C_4) = (B_8) - (B_6)$; $(C_5) = (B_8) - (B_5)$; $(C_6) = (B_4)$; $(C_7) = (B_2)$ e $(C_8) = (B_3)$ e obtemos:

(C_1) $\quad x_1 + x_2 + x_3 + x_4 + 2x_5 \quad + 2x_8 \equiv 0 \pmod 8$

(C_2) $\quad x_2 + x_3 \quad + 2x_8 \equiv 0 \pmod 4$

(C_3) $\quad x_3 - x_4 - x_5 - x_6 - x_7 + x_8 \equiv 0 \pmod 4$

(C_4) $\quad x_5 \quad - x_8 \equiv 0 \pmod 2$

(C_5) $\quad x_3 - x_4 - x_5 + x_6 + x_7 + x_8 \equiv 0 \pmod 4$

(C_6) $\quad x_3 + x_4 + x_5 - x_6 + x_7 + x_8 \equiv 0 \pmod 4$

(C_7) $\quad x_3 + x_4 + x_5 + x_6 - x_7 + x_8 \equiv 0 \pmod 4$

(C_8) $\quad x_5 \quad + x_8 \equiv 0 \pmod 4$

Notamos que as equações de congruência (C_4) e (C_8) são equivalentes; podemos, portanto, suprimir uma delas. Tomamos agora: $(D_1) = (C_1)$; $(D_2) = (C_2)$; $(D_3) = (C_3)$; $(D_4) = (C_3) - (C_5)$; $(D_5) = (C_3) - (C_6)$; $(D_6) = (C_3) - (C_7)$ e $(D_7) = (C_8)$. Resulta:

$$
\begin{aligned}
&(D_1)\ x_1 + x_2 + x_3 + x_4 + 2x_5 + 2x_8 \equiv 0 \pmod 8\\
&(D_2)\ x_2 + x_3 + 2x_8 \equiv 0 \pmod 4\\
&(D_3)\ x_3 - x_4 - x_5 - x_6 - x_7 + x_8 \equiv 0 \pmod 4\\
&(D_4)\ - x_6 - x_7 \equiv 0 \pmod 2\\
&(D_5)\ - x_4 - x_5 - x_7 \equiv 0 \pmod 2\\
&(D_6)\ - x_4 - x_5 - x_6 \equiv 0 \pmod 2\\
&(D_7)\ x_5 + x_8 \equiv 0 \pmod 2
\end{aligned}
$$

Finalmente temos o sistema reduzido a uma forma escalonada tomando $(E_1) = (D_1)$; $(E_2) = (D_2)$; $(E_3) = (D_3)$; $(E_4) = -(D_5)$; $(E_5) = (D_7)$ e $(E_6) = -(D_4)$. Nòte-se que $(D_5) - (D_6)$ dá a equação $-x_6 + x_7 \equiv 0 \pmod 2$ que é equivalente a (D_4) e não é necessário inclui-la. Temos:

$$
(3)\quad \left[\begin{aligned}
&(E_1)\ x_1 + x_2 + x_3 + x_4 + 2x_5 + 2x_8 \equiv 0 \pmod 8\\
&(E_2)\ x_2 + x_3 + 2x_8 \equiv 0 \pmod 4\\
&(E_3)\ x_3 - x_4 - x_5 - x_6 - x_7 + x_8 \equiv 0 \pmod 4\\
&(E_4)\ x_4 + x_5 + x_7 \equiv 0 \pmod 2\\
&(E_5)\ x_5 + x_8 \equiv 0 \pmod 2\\
&(E_6)\ x_6 + x_7 \equiv 0 \pmod 2
\end{aligned}\right.
$$

Queremos, na verdade, conhecer os elementos $\chi \in \phi(U(\mathbb{Z}D_4))$. Como as imagens de unidades são unidades, as componentes de χ devem verificar, além das condições (3), as seguintes:

(4) $\quad x_i = \pm 1$, $i = 1, 2, 3, 4$ e $x_5x_8 - x_6x_7 = \pm 1$.

Vamos determinar as matrizes $X = \begin{bmatrix} x_5 & x_6 \\ x_7 & x_8 \end{bmatrix}$ $\in$ $GL(2, \mathbb{Z})$ tais que existem x_i, $i = 1, 2, 3, 4$ verificando as condições (3) e (4), i.é., tais que $\chi = (x_1, x_2, x_3, x_4, X) \in \phi(U(\mathbb{Z} D_4))$.

Notamos inicialmente que (4) junto com (E_5) e (E_6) implica que os elementos de X devem verificar:

(5) $\quad (x_5 + x_7)(x_6 + x_8) \equiv 1 \pmod 2$

Assim, qualquer que seja a escolha de $x_4 = \pm 1$ a equação (E_4) está sempre verificada.

Agora, de (E_6) podemos escrever $x_6 + x_7 = -2k$ e de (E_5) temos $x_8 = x_5 + 2h$. Substituindo em (E_3) temos:

$$x_3 - x_4 + 2(k + h) \equiv 0 \pmod 4$$

Então:

(a) Se $h + k \equiv 0 \pmod 2$ i.é. se $x_8 \equiv x_5 + x_6 + x_7 \pmod 4$ a única solução de (E_3) é $x_3 = x_4$

(b) Se $h + k \equiv 1 \pmod 2$ i.é. se $x_8 \equiv x_5 + x_6 + x_7 + 2 \pmod 4$ a única solução de (E_3) é $x_3 = -x_4$.

Em ambos os casos (E_3) determina o valor de x_3 em função de x_4 .

Para estudar (E_2) devemos considerar também duas possibilidades:

(a) Se $x_8 \equiv 0 \pmod 2$ então $x_2 = -x_3$

(b) Se $x_8 \equiv 1 \pmod 2$ então $x_2 = x_3$

Novamente, (E_2) determina o valor de x_2 .

Finalmente, para estudar (E_1) devemos considerar quatro casos que surgem da combinação das possibilidades acima.

1º Caso - $x_8 \equiv 1 \pmod 2$ e $x_8 \equiv x_5 + x_6 + x_7 \pmod 4$

Dos casos anteriores temos $x_2 = x_3 = x_4$ e substituindo em (E_1) resulta:

$$x_1 + 3x_4 + 2(x_5 + x_8) \equiv 0 \pmod 8 .$$

Temos novamente duas possibilidades:

(a) Se $x_5 + x_8 \equiv 0 \pmod 4$ temos $x_1 + 3x_4 \equiv 0 \pmod 8$ que é incompatível em presença das condições (4)

(b) Se $x_5 + x_8 \equiv 2 \pmod 4$ temos $x_1 + 3x_4 + 4 \equiv 0 \pmod 8$ é a única solução de (E_1) e $x_1 = x_4$.

2º Caso - $x_8 \equiv 1 \pmod 2$ e $x_8 \equiv x_5 + x_6 + x_7 + 2 \pmod 4$

Dos casos anteriores temos agora $x_2 = x_3 = -x_4$. Substituindo em (E_1) vem

$$x_1 - x_4 + 2(x_5 + x_8) \equiv 0 \pmod 8$$

Mais uma vez, devemos considerar dois casos:

(a) Se $x_5 + x_8 \equiv 0 \pmod 4$ temos $x_1 - x_4 \equiv 0 \pmod 8$ e a solução de (E_1) é $x_1 = x_4$

(b) Se $x_5 + x_8 \equiv 2 \pmod 4$ temos $x_1 - x_4 + 4 \equiv 0 \pmod 8$ que é incompatível (sempre em presença das condições (4)).

<u>3º Caso</u> - $x_8 \equiv 0 \pmod 2$; $x_8 \equiv x_5 + x_6 + x_7 \pmod 4$

Temos $x_2 = -x_3 = -x_4$. (E_1) fica então:

$$x_1 + x_4 + 2(x_5 + x_8) \equiv 0 \pmod 8$$

(a) $x_5 + x_8 \equiv 0 \pmod 4$ dá $x_1 + x_4 \equiv 0 \pmod 8$ i.é. $x_1 = -x_4$

(b) $x_5 + x_8 \equiv 2 \pmod 4$ dá $x_1 + x_4 + 4 \equiv 0 \pmod 8$ que é incompatível.

<u>4º Caso</u> - $x_8 \equiv 0 \pmod 2$; $x_8 \equiv x_5 + x_6 + x_7 + 2 \pmod 4$

Das condições anteriores vem $x_2 = -x_3 = x_4$. (E_1) fica:

$$x_1 + x_4 + 2(x_5 + x_8) \equiv 0 \pmod 8$$

e:

(a) $x_5 + x_8 \equiv 0 \pmod 4$ dá $x_1 + x_4 \equiv 0 \pmod 8$ i.é. $x_1 = -x_4$

(b) $x_5 + x_8 \equiv 2 \pmod 4$ dá $x_1 + x_4 + 4 \equiv 0 \pmod 8$ incompatível

Resumindo a informação acima temos que dada uma matriz:

$$X = \begin{bmatrix} x_5 & x_6 \\ x_7 & x_8 \end{bmatrix} \quad \in \quad GL(2, \mathbb{Z}) \text{ verificando as condi-}$$

ções (E_5) e (E_6) existem $x_i = \pm 1$, $i = 1, 2, 3, 4$ tais que:

$$\chi = (x_1, x_2, x_3, x_4, X) \in \phi(U(\mathbb{Z} D_4))$$

se e sòmente se está verificada uma das seguintes condições:

$$\text{(i)} \quad x_8 \equiv 1 \pmod 2 \; ; \; x_5 + x_6 + x_7 - x_8 \equiv 0 \pmod 4 \; ; \; x_5 + x_8 \equiv 2 \pmod 4$$

$$\text{(ii)} \quad x_8 \equiv 1 \pmod 2 \; ; \; x_5 + x_6 + x_7 - x_8 \equiv 2 \pmod 4 \; ; \; x_5 + x_8 \equiv 0 \pmod 4 \qquad (5)$$

$$\text{(iii)} \quad x_8 \equiv 0 \pmod 2 \; ; \; x_5 + x_8 \equiv 0 \pmod 4$$

Em cada um destes casos o nosso estudo mostra que existem exatamente dois elementos $X \in \phi(U(\mathbb{Z} D_4))$ cuja componente matricial é precisamente X, dependendo da escolha de x_4 (ou equivalentemente de x_1).

(I.2.1) Definição -

Chamaremos Ω ao subgrupo de $GL(2, \mathbb{Z})$ das matrizes que verificam (E_5), (E_6) e uma das condições em (5).

Note-se que, se $\pi : \mathbb{Z} \oplus \mathbb{Z} \oplus \mathbb{Z} \oplus \mathbb{Z} \oplus M_2(\mathbb{Z}) \to M_2(\mathbb{Z})$ é a projeção canônica, segue que $\pi \circ \phi\ (U(\mathbb{Z}\, D_4)) = \Omega$.

Agora mostraremos que dado $\chi \in \phi(U(\mathbb{Z}\, D_4))$ então $\varepsilon \circ \phi^{-1}\ (\chi = x_1$.

De fato: $\phi^{-1}(\chi) = A^{-1} \cdot (x_1, x_2, \ldots\ldots, x_8) =$

$$= \frac{1}{8}\ ((x_1+x_2+x_3+x_4+2x_5+2x_8)1+(x_1+x_2-x_3-x_4-2x_6+2x_7)a$$

$$+(x_1+x_2+x_3+x_4-2x_5-2x_8)a^2 + (x_1+x_2-x_3-x_4+2x_6-2x_7)\ a^3$$

$$+(x_1-x_2+x_3-x_4+2x_6+2x_7)\ b + (x_1-x_2-x_3+x_4-2x_5+2x_8)\ ab$$

$$+(x_1-x_2+x_3-x_4-2x_6-2x_7)a^2b + (x_1-x_2-x_3+x_4+2x_5-2x_8)\ a^3b)$$

Somando todos os coeficientes vem:

(6) $\qquad \varepsilon \circ \phi^{-1}\ (\chi) = x_1$

Assim, para cada $X \in \Omega$ existe um único elemento $\alpha \in V(\mathbb{Z}\, D_4)$ tal que: $\pi \circ \phi\ (\alpha) = X$ e resulta que $\pi \circ \phi \mid V(\mathbb{Z}\, D_4) : V(\mathbb{Z}\, D_4) \to \Omega$ é um isomorfismo. Temos então:

(7) $\qquad V(\mathbb{Z}\, D_4) \cong \Omega \quad ; \quad U(\mathbb{Z}\, D_4) \cong \{\pm 1\} \times \Omega$.

I-3. - ALGUMAS PROPRIEDADES DE Ω

Nesta seção vamos obter algumas informações sobre Ω : as ordens possíveis para elementos de ordem finita em Ω e o índice de Ω em $\mathbf{GL}(2, \mathbb{Z})$.

Para isso começamos estabelecendo nosso único resultado geral deste capítulo.

(I.3.1) Proposição - Seja G um p-grupo finito. Se α é uma unidade normalizada de ordem finita de $\mathbb{Z}G$ então a ordem de α é uma potência de p.

Demonstração

Seja $\alpha \in V(\mathbb{Z}G)$ e J_p o corpo com p-elementos.

O homomorfismo canônico $\psi : \mathbb{Z} \to J_p$ se estende na forma usual a um homomorfismo $\psi' : \mathbb{Z}G \to J_p G$ que dá, por restrição, $\psi^* : U(\mathbb{Z}G) \to U(J_p G)$. ψ^* leva o grupo gerado por α - que notaremos por (α) - sôbre um subgrupo de unidades de $J_p G$.

Agora, indiquemos por g_1 o elemento neutro de G. Dado $x = \sum_i x_i g_i \in U(\mathbb{Z}G)$, se $x \in \mathrm{Ker}(\psi^*)$ então $x_1 \equiv 1 \pmod{p}$; em particular $x_1 \neq 0$.

Segundo Berman (| 2 | , Lema 2) as únicas unidades de ordem finita da forma $x = \sum_i x_i g_i$ com $x_1 \neq 0$ são $x = \pm 1$.

Como todo elemento de (α) é uma unidade normalizada de ordem finita, segue da observação acima que (α) é isomorfo a sua imagem em $V(J_p\, G)$.

Finalmente, se G é um p-grupo, conforme foi dito no Capítulo 0, o grupo das unidades normalizadas é:

$$V(J_p\, G) = \{\, v \in J_p\, G \mid \varepsilon(v) = 1 \,\}$$

e um cálculo direto mostra que:

$$| V(J_p\, G) | = p^{|G|} - 1$$

logo todo elemento em $V(J_p\, G)$ tem ordem igual a uma potência de p. □

Agora voltamos nossa atenção para Ω.

Um cálculo simples mostra que os elementos de ordem finita de $GL(2,\mathbb{Z})$ só podem ter ordem igual a 2, 3, 4 ou 6 (ver por exemplo, Newman | 17 |, capítulo IX). Deste resultado e da proposição anterior segue:

(I.3.2) Corolário. - Os elementos de ordem finita de Ω só podem ter ordens iguais a 2 ou 4.

Os elementos $\begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$ e $\begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix}$ de Ω mostram que ambas as ordens possíveis se realizam.

Finalmente, calculamos o índice de Ω em $GL(2, \mathbb{Z})$.

(I.3.3) - Lema. -

$$| GL(2, \mathbb{Z}) : \Omega | = 6.$$ Mais ainda:

$$W_1 = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \quad ; \quad W_2 = \begin{bmatrix} 1 & 2 \\ 0 & 1 \end{bmatrix} \quad ; \quad W_3 = \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}$$

$$W_4 = \begin{bmatrix} 1 & 1 \\ 2 & 1 \end{bmatrix} \quad ; \quad W_5 = \begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix} \quad ; \quad W_6 = \begin{bmatrix} 1 & 2 \\ 1 & 1 \end{bmatrix}$$

é um conjunto completo de representantes das classes laterais à esquerda determinadas por Ω em $GL(2,\mathbb{Z})$.

Demonstração . - A prova deste resultado requer a análise de vários casos.

Observemos inicialmente que se $A = \begin{bmatrix} m & n \\ r & s \end{bmatrix} \in GL(2,\mathbb{Z})$ a condição $\det(A) = \pm 1$ implica que, numa mesma fila ou numa mesma coluna não podem ser ambos os elementos pares; também não podem ser todos os elementos ímpares. Temos, então, duas possibilidades:

(I) Os elementos de uma diagonal são pares e os outros dois ímpares.

(II) Três elementos são ímpares e um é par.

Analisaremos separadamente as possíveis situações.

1º Caso - Se A verifica a condição (I), A pertence a Ω ou à classe de W_2 .

1-(a) - Suponhamos m,s pares e n,r ímpares.

Como $W_2^{-1} = \begin{bmatrix} 1 & -2 \\ 0 & 1 \end{bmatrix}$ temos $W_2^{-1} A = \begin{bmatrix} m-2r & n-2s \\ r & s \end{bmatrix}$

Chamando $x_5 = m - 2r$; $x_6 = n - 2s$; $x_7 = r$ e $x_8 = s$ vem:

$$x_8 = s \equiv 1 \pmod 2$$

$$x_5 + x_8 = m + s - 2r \equiv m + s \pmod 4 \quad \text{pois } r \text{ é par}$$

$$x_5 + x_6 + x_7 = m - 2r + n - 2s + r \equiv m+n+r+2 \pmod 4 \text{ pois } s \text{ é ímpar .}$$

Mostraremos que se A não verifica (i) nem (ii) de (5) i.é., se $A \notin \Omega$, então, $W_2^{-1} A$ verifica uma destas condições e $W_2^{-1} A \in \Omega$.

De fato, se A não verifica (i) nem (ii), então, $m+s \equiv m+n+r \pmod 4$ logo $x_5 + x_8 \equiv x_5 + x_6 + x_7 - x_8 + 2 \pmod 4$ e (i) ou (ii) estará verificada para $W_2^{-1} A$.

Recìprocamente, é fácil ver que, se $W_2^{-1} A \notin \Omega$, então, $A \in \Omega$.

1-(b) - Sejam agora m,s pares e n,r ímpares.

Indicando x_i, i = 5, 6, 7, 8, como no caso anterior as fórmulas (8) dão agora:

$$(8') \qquad \begin{aligned} x_8 &= s \equiv 0 \pmod 2 \\ x_5 + x_8 &= m + s - 2r \equiv m + s + 2 \pmod 4 \end{aligned}$$ pois r é ímpar

e é fácil ver que A verifica (iii) de (5) se e sòmente se $W_2^{-1} A$ não a verifica e recìprocamente.

Para estudar matrizes verificando (II) discutiremos segundo a posição do elemento par.

2º Caso - A verifica (II) e um dos elementos da primeira linha é par. Neste caso mostraremos que $A \in W_5 \Omega$ ou $A \in W_6 \Omega$.

2-(a) - Sejam m par e n, r, s ímpares.

Notaremos:

$$\begin{bmatrix} x_5 & x_6 \\ x_7 & x_8 \end{bmatrix} = W_5^{-1} \cdot A = \begin{bmatrix} 1 & 0 \\ -1 & 1 \end{bmatrix} \begin{bmatrix} m & n \\ r & s \end{bmatrix} = \begin{bmatrix} m & n \\ -m+r & -n+s \end{bmatrix}$$

$$\begin{bmatrix} x'_5 & x'_6 \\ x'_7 & x'_8 \end{bmatrix} = W_6^{-1} \cdot A = \begin{bmatrix} -1 & 2 \\ 1 & -1 \end{bmatrix} \begin{bmatrix} m & n \\ r & s \end{bmatrix} = \begin{bmatrix} -m+2r & -n+2s \\ m-r & n-s \end{bmatrix}$$

Como m - n + s é par temos que $m - n + s \equiv -(m - n + s) \pmod 4$ e como r é ímpar $m - n + s \equiv -m + n - s + 2r + 2 \pmod 4$. Temos assim:

$$x_8 = n - s \equiv s - n = x_8' \pmod 2$$

(9)

$$x_5 + x_8 = m - n + s \equiv -m + n - s + 2r + 2 =$$

$$= x_5' + x_8' + 2 \pmod 4$$

De (9) segue trivialmente que se W_5^{-1} A não verifica (iii) de (5), então, W_6^{-1} A verifica esta condição e reciprocamente. Logo $A \in W_5\Omega$ ou $A \in W_6\Omega$.

2.(b) - Sejam n par e m, r, s ímpares.

Nestas condições m - n + s e r tem a mesma paridade que no caso anterior. Temos, então:

$$x_8 = - n + s \equiv n - s = x_8' \equiv 1 \pmod 2$$

(9')

$$x_5 + x_8 \equiv x_5' + x_8' + 2 \pmod 4$$

$$x_5 + x_6 + x_7 - x_8 = s - r \equiv r-s=x_5' + x_6' + x_7' - x_8' \pmod 4$$

pois r - s é par.

Novamente, de considerações semelhantes as do caso 1-(a) , segue que $A \in W_5\Omega$ ou $A \in W_6\Omega$.

3º Caso- Se A verifica (II) e um dos elementos da segunda linha é par mostraremos que $A \in W_3\Omega$ ou $A \in W_4\Omega$.

3-a. - Sejam r par, m, n, s ímpares.

Notaremos:

$$\begin{bmatrix} x_5 & x_6 \\ x_7 & x_8 \end{bmatrix} = W_3^{-1}A = \begin{bmatrix} 1 & -1 \\ 0 & 1 \end{bmatrix} \begin{bmatrix} m & n \\ r & s \end{bmatrix} = \begin{bmatrix} m-r & n- \\ r & s \end{bmatrix}$$

$$\begin{bmatrix} x_5' & x_6' \\ \mathbf{x_7'} & x_8' \end{bmatrix} = W_4^{-1}A = \begin{bmatrix} -1 & 1 \\ \mathbf{2} & -1 \end{bmatrix} \begin{bmatrix} m & n \\ r & \mathbf{s} \end{bmatrix} = \begin{bmatrix} -m+r & -n+s \\ 2m-r & 2n-s \end{bmatrix}$$

Resulta agora:

$x_8 = s \equiv 2n - s = x_8' \equiv 1 \pmod 2$

(10) $x_5 + x_8 = m - r + s \equiv -(m-r+s) + 2n + 2 \equiv x_5' + x_8' + 2 \pmod 4$ pois $m - r + s$ é par e n ímpar.

$x_5 + x_6 + x_7 - x_8 = m + n - 2s \equiv m - n + 2s = x_5' + x_6' + x_7' - x_8' \pmod 4$

Assim, novamente uma análise semelhante à do caso 1-(a) mostra que $A \in W_3\Omega$ ou $A \in W_4\Omega$.

3-(b) . - Sejam s par e m, n, r ímpares.

Com a mesma rotação do caso anterior temos:

$x_8 = s \equiv 2n - s = x_8' \equiv 0 \pmod 2$

(10') $x_5 + x_8 = m - r + s \equiv -(m - r + s) + 2n + 2 = x_5' + x_8' + 2 \pmod 4$

E segue novamente que $A \in W_3\ \Omega$ ou $A \in W_4\ \Omega$ como nos casos anteriores.

I-4. A QUESTÃO DA CONJUGAÇÃO

Nesta seção daremos uma resposta negativa à pergunta (a) da introdução. Para isso vamos determinar as classes de conjugação de elementos de ordem 2 em $U(\mathbb{Z} D_4)$.

Em $GL(2, \mathbb{Z})$ existem três classes de conjugação de elementos de ordem 2, a saber:

$$C_0 = \{-I\}$$

$$C_1 = \{X = \begin{bmatrix} a & b \\ c & -a \end{bmatrix} \mid a^2 + bc = 1;\ a \text{ impar};\ b,c \text{ pares}\}$$

$$C_2 = \{X = \begin{bmatrix} a & b \\ c & -a \end{bmatrix} \mid a^2 + bc = 1,\ X \notin C_1\}$$

(Ver Hughes e Pearson | 14 |).

(I.4.1) - Proposição - Existem cinco classes de conjugação de elementos de ordem 2 em Ω .

Demonstração -

Mostraremos inicialmente que um elemento $Y \in C_1 \cap \Omega$ é conjugado a $X_1 = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$ ou a $Y_1 = \begin{bmatrix} 1 & 4 \\ 0 & -1 \end{bmatrix}$ em Ω

De fato, como $X_1 \in C_1$, Y e X_1 são conjugados em $GL(2,\mathbb{Z})$ e existe U inversível tal que $UYU^{-1} = X_1$. Como $U = W_i A$ para algum $A \in \Omega$ e algum i, $1 \leq i \leq 6$, temos:

(11) $$A Y A^{-1} = W_i^{-1} X_1 W_i$$

Se $i = 1$, então $U \in \Omega$ e Y é conjugado de X_1 em Ω.

Para $i = 3,\ldots,6$ temos:

$$\begin{bmatrix} 1 & -1 \\ 0 & 1 \end{bmatrix} \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix} \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} 1 & 2 \\ 0 & -1 \end{bmatrix}$$

$$\begin{bmatrix} -1 & 1 \\ 2 & -1 \end{bmatrix} \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix} \begin{bmatrix} 1 & 1 \\ 2 & 1 \end{bmatrix} = \begin{bmatrix} -3 & -2 \\ 4 & 3 \end{bmatrix}$$

$$\begin{bmatrix} 1 & 0 \\ -1 & 1 \end{bmatrix} \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix} \begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ -2 & -1 \end{bmatrix}$$

$$\begin{bmatrix} -1 & 2 \\ 1 & -1 \end{bmatrix} \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix} \begin{bmatrix} 1 & 2 \\ 1 & 1 \end{bmatrix} = \begin{bmatrix} -3 & -4 \\ 2 & 3 \end{bmatrix}$$

Estas matrizes não pertencem a Ω pois não verificam nenhuma das condições de (5). Como $A Y A^{-1} \in \Omega$ a equação (9) nestes casos é impossível.

Finalmente:

$$\begin{bmatrix} 1 & -2 \\ 0 & 1 \end{bmatrix} \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix} \begin{bmatrix} 1 & 2 \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} 1 & 4 \\ 0 & -1 \end{bmatrix} = Y_1 \in \Omega .$$

Para demonstrar que C_1 dá origem a duas classes em Ω deveremos demonstrar ainda que X_1 e Y_1 não são conjugados (em Ω).

Seja então $U = \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in G\,L(2,\mathbb{Z})$ tal que $UX_1 = Y_1U$.

Como $UX_1 = \begin{bmatrix} a & -b \\ c & -d \end{bmatrix}$ e $Y_1U = \begin{bmatrix} a + 4c & b + 4d \\ -c & -d \end{bmatrix}$

temos que $c = 0$ e $b = -2d$. As únicas matrizes de $G\,L(2,\mathbb{Z})$ desta forma são:

$$\begin{bmatrix} 1 & -2 \\ 0 & 1 \end{bmatrix}, \begin{bmatrix} 1 & 2 \\ 0 & -1 \end{bmatrix}, \begin{bmatrix} -1 & -2 \\ 0 & 1 \end{bmatrix}, \begin{bmatrix} -1 & 2 \\ 0 & -1 \end{bmatrix}$$

e é fácil ver que nenhuma delas pertence a Ω .

Da mesma forma, se $Y \in C_2 \cap \Omega$ mostraremos que é conjugado a

$$X_2 = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \text{ ou a } Y_2 = \begin{bmatrix} -2 & -3 \\ 1 & 2 \end{bmatrix}$$

Tal como no caso anterior, existem $A \in \Omega$ e i, $1 \leq i \leq 6$

tais que:

(12) $\quad A\ Y\ A^{-1} = W_i^{-1}\ X_2\ W_i$

Novamente, para i = 3,...,6 temos:

$$\begin{bmatrix} 1 & -1 \\ 0 & 1 \end{bmatrix} \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} -1 & 0 \\ 1 & 1 \end{bmatrix}$$

$$\begin{bmatrix} -1 & 1 \\ 2 & -1 \end{bmatrix} \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \begin{bmatrix} 1 & 1 \\ 2 & 1 \end{bmatrix} = \begin{bmatrix} -1 & 0 \\ 3 & 1 \end{bmatrix}$$

$$\begin{bmatrix} 1 & 0 \\ -1 & 1 \end{bmatrix} \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix} = \begin{bmatrix} 1 & 1 \\ 0 & -1 \end{bmatrix}$$

$$\begin{bmatrix} -1 & 2 \\ 1 & -1 \end{bmatrix} \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \begin{bmatrix} 1 & 2 \\ 1 & 1 \end{bmatrix} = \begin{bmatrix} 1 & 3 \\ 0 & -1 \end{bmatrix}$$

E mais uma vez é fácil ver que estas matrizes não pertencem a Ω .

Finalmente, para i = 2 temos:

$$\begin{bmatrix} 1 & -2 \\ 0 & 1 \end{bmatrix} \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \begin{bmatrix} 1 & 2 \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} -2 & -3 \\ 1 & 2 \end{bmatrix} = Y_2 \in \Omega$$

E deveremos mostrar que X_2 e Y_2 não são conjugados em Ω.

Seja novamente $U = \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in GL(2,\mathbb{Z})$ tal que $U\ X_2 = Y_2\ U$.

Como $U X_2 = \begin{bmatrix} b & a \\ d & c \end{bmatrix}$ e $Y_2 U = \begin{bmatrix} -2a - 3c & -2b - 3d \\ a + 2c & b + 2d \end{bmatrix}$

U deve ser da forma $U = \begin{bmatrix} a & -(2a + 3c) \\ c & a + 2c \end{bmatrix}$

Como $\det(U) = \pm 1$ segue que:

$a^2 + 4ac + 3c^2 = (a+3c)(a+c) = \pm 1$ e $a = \pm 1, c = 0$ ou $a = \pm 2, c = \mp 1$

e as únicas matrizes possíveis são:

$$\begin{bmatrix} 1 & -2 \\ 0 & 1 \end{bmatrix}; \begin{bmatrix} -1 & 2 \\ 0 & -1 \end{bmatrix}; \begin{bmatrix} 2 & -1 \\ -1 & 0 \end{bmatrix}; \begin{bmatrix} -2 & 1 \\ 1 & 0 \end{bmatrix}$$

É fácil ver que nenhuma destas matrizes pertence a Ω .

Novamente C_2 dá origem a duas classes de conjugação correspondentes a X_2 e Y_2 em Ω

(I.4.2) Corolário - Nem toda unidade normalizada de ordem finita é conjugada a um elemento de D_4 .

Demonstração -

Seja π a projeção canônica definida na observação que segue à definição (I.2.1).

Os elementos de ordem 2 em D_4 são: a^2, b, ab, a^2b e a^3b

Calculando, temos:

$$\pi \circ \phi\ (a^2) = \begin{bmatrix} -1 & 0 \\ 0 & -1 \end{bmatrix} = -I$$

$$\pi \circ \phi\ (b) = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \in X_2\Omega$$

$$\pi \circ \phi\ (ab) = \begin{bmatrix} -1 & 0 \\ 0 & 1 \end{bmatrix} \in X_1\Omega \qquad (\text{tomar } U = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix})$$

$$\pi \circ \phi\ (a^2b) = \begin{bmatrix} 0 & -1 \\ -1 & 0 \end{bmatrix} \in X_2\Omega \qquad (\text{tomar } U = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix})$$

$$\pi \circ \phi\ (a^3b) = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix} \in X_1\Omega$$

Logo, os elementos $\alpha \in V(\mathbb{Z}\, D_4)$ tais que $\pi \circ \phi\ (\alpha)$ pertence a $Y_1\ \Omega$ ou $Y_2\ \Omega$ são unidades normalizadas de $\mathbb{Z}\, D_4$, de ordem finita e não conjugadas a elementos de D_4

I-5 OS SUBGRUPOS MAXIMAIS

Levando em consideração os resultados da seção I.2, para responder à pergunta (b) da introdução será suficiente determinar os subgrupos maximais de Ω.

Os subgrupos finitos de $GL(2,\mathbb{Z})$ são bem conhecidos. Êles são isomorfos aos grupos diedrais D_1, D_2, D_3, D_4 ou D_6. (ver por exemplo M.Newman| 17 |, capítulo IX, § 14). Como G não contém elementos de ordem 3 os subgrupos finitos maximais de Ω devem ser isomorfos a D_4 e conforme |17| êles são conjugados, em $GL(2,\mathbb{Z})$, ao grupo gerado por:

$$A = \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix} \qquad e \qquad B = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$$

Seja Γ um tal subgrupo e $V \in GL(2,\mathbb{Z})$ uma matriz tal que:

$$\Gamma^V = V \Gamma V^{-1} = D_4^* \tag{13}$$

Podemos então escolher geradores X e Y de Γ tais que:

$$X^V = A \text{ e } Y^V = B \tag{14}$$

Como $Y \in C_2$, Y é conjugado em Ω de $X_2 = B$ ou de Y_2.

Suponhamos inicialmente que existe U em Ω tal que:

$$Y^U = B \tag{15}$$

De (14) e (15) segue fàcilmente que VU^{-1} deve pertencer ao centralizante de B em $GL(2,\mathbb{Z})$ que indicaremos por Z(B). Agora, é fácil, ver que uma matriz $A \in GL(2,\mathbb{Z})$ comuta com B se e sòmente se é da

forma $A = \begin{bmatrix} a & b \\ b & a \end{bmatrix}$. A condição $\det(A) = \pm 1$ mostra que os

únicos casos possíveis são $a = \pm 1$, $b = 0$ ou $a = 0$, $b = \pm 1$. Logo

$$Z(B) = \{\pm I, \pm B\}$$

e $V = \pm U$ ou $V = \pm B\,U$

Em ambos os casos $V \in \Omega$ e Γ e D_4^* são conjugados em Ω

Suponhamos agora que existe $U \in \Omega$ tal que:

(16) $$Y^U = Y_2$$

Tomando $W = \begin{vmatrix} 1 & 2 \\ 0 & 1 \end{vmatrix} \in GL(2,\mathbb{Z})$ é fácil verificar que $Y_2^W = B$, lo-

go

(17) $$Y^{WU} = B$$

De (14) e (17) segue de forma análoga que:

$$V\,U^{-1}\,W^{-1} \in Z(B)$$

logo:

(18) $$V = \pm W\,U \quad \text{ou} \quad V = \pm B\,W\,U$$

No primeiro caso temos:

$$X^U = X^{W^{-1}V} = W^{-1}\,X^V\,W = W^{-1}\,A\,W = \begin{vmatrix} -2 & -5 \\ 1 & 2 \end{vmatrix} = A'$$

e no segundo caso:

$$X^U = X^{(B\,W)^{-1}V} = (B\,W)^{-1}\,X^V\,B\,W = (BW)^{-1}A\,BW = \begin{bmatrix} 2 & 5 \\ -1 & -2 \end{bmatrix} = A'^3$$

Obviamente $(A', Y_2) = (A'^3, Y_2)$.

Reunindo as informações acima podemos enunciar:

(I.5.1) Proposição - Um subgrupo finito maximal Γ de Ω é conjugado a $D_4^* = (A,B)$ ou $D_4' = (A', Y_2)$ em Ω . Estes subgrupos não são conjugados entre si.

Demonstração - Só falta observar que D_4^* não é conjugado de D_4' e, de fato, da demonstração do Corolário(I.2.4) resulta que nenhum elemento de D_4^* é conjugado de Y_2 .

I.6. - OS AUTOMORFISMOS NORMALIZADOS

Se Θ é um automorfismo normalizado de $\mathbb{Z}\,D_4$ então a restrição $\bar{\Theta}$ de Θ a $V(\mathbb{Z}\,D_4)$ é um automorfismo de $V(\mathbb{Z}\,D_4)$.

Então, $\Theta^* = (\pi\circ\phi)\circ\bar{\Theta}\circ(\pi\circ\phi)^{-1}$ é um automorfismo de Ω.

Vamos definir um morfismo $\psi : \mathbb{Z}\,D_4 \to \mathbb{Z}\,D_4$ da seguinte forma.

Sobre os geradores de D_4 definimos:

$$\psi(a) = 2a - a^3 - b + ab + a^2b - a^3b$$

$$\psi(b) = a - a^3 + ab + a^2b - a^3b$$

Como $\psi(a)^4 = \psi(b)^2 = \psi(b)\ \psi(a)\ \psi(b)\ \psi(a) = 1$ podemos estender ψ a um homomorfismo de D_4 definindo:

$$\psi(1) = 1,$$
$$\psi(a^2) = \psi(a)^2 = a^2$$
$$\psi(a^3) = \psi(a)^3 = -a + 2a^3 + b - ab - a^2b + a^3b\ ,$$
$$\psi(ab) = \psi(a)\ \psi(b) = a - a^3 - b + ab + a^2b,$$
$$\psi(a^2b) = \psi(a)^2\ \psi(b) = -a + a^3 + b - ab + a^3b,$$
$$\psi(a^3b) = \psi(a)^3\ \psi(b) = -a + a^3 + b - a^2b + a^3b,$$

então ψ se estende naturalmente a um morfismo de $\mathbb{Z}\, D_4$ em $\mathbb{Z}\, D_4$.

Em relação à base de $\mathbb{Z}\, D_4$ formada pelos elementos de D_4, a matriz associada a ψ é:

$$M = \begin{vmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 2 & 0 & -1 & 1 & 1 & -1 & -1 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & -1 & 0 & 2 & -1 & -1 & 1 & 1 \\ 0 & -1 & 0 & 1 & 0 & -1 & 1 & 1 \\ 0 & 1 & 0 & -1 & 1 & 1 & -1 & 0 \\ 0 & 1 & 0 & -1 & 1 & 1 & 0 & -1 \\ 0 & -1 & 0 & 1 & -1 & 0 & 1 & 1 \end{vmatrix}$$

Como $\det(M) = 1$, $M \in G\,L(2, \mathbb{Z})$ e ψ é um automorfismo de $\mathbb{Z}\, D_4$.

Suponhamos agora que ψ seja o produto de um automorfismo de D_4 e de um automorfismo interior γ_u definido por $\gamma_u(x) = u\,x\,u^{-1}$, $\forall x \in \mathbb{Z}\,D_4$, com $u \in V(\mathbb{Z}\,D_4)$.

Seja $U = \pi \circ \phi\,(u) \in \Omega$ e $\gamma_U : \Omega \to \Omega$ o automorfismo interior correspondente. Então, o seguinte diagrama é comutativo:

$$\begin{array}{ccc} V(\mathbb{Z}\,D_4) & \xrightarrow{\gamma_u} & V(\mathbb{Z}\,D_4) \\ {\scriptstyle \pi\circ\phi}\downarrow & & \downarrow{\scriptstyle \pi\circ\phi} \\ \Omega & \xrightarrow{\gamma_U} & \Omega \end{array}$$

pois $\pi\circ\phi\circ\gamma_u\,(x) = \pi\circ\phi(u\,x\,u^{-1}) = U\,(\pi\circ\phi(x))\,U^{-1} = \gamma_U \circ \pi\circ\phi$.

Logo: $\gamma_U \circ \pi\circ\phi\,(D_4) = \pi\circ\phi\circ\gamma_U(D_4)$

Como $\pi\circ\phi\,(D_4) = D_4^*$ e $\gamma_u(D_4) = \psi\,(D_4)$ temos:

(19) $\gamma_U\,(D_4^*) = \pi\circ\phi\circ\psi\,(D_4)$

Finalmente:

$$\pi\circ\phi\circ\psi(a) = \pi\circ\phi(2a-a^3-b+ab+a^2b-a^3b) = \pi\left(1,1,-1,-1,\begin{bmatrix}-2 & -5\\ 1 & 2\end{bmatrix}\right) = A'$$

$$\pi\circ\phi\circ\psi(b) = \pi\circ\phi(a-a^3+ab+a^2b-a^3b) = \pi\left(1,-1,1,-1,\begin{bmatrix}-2 & -3\\ 1 & 2\end{bmatrix}\right) = Y_2$$

Logo $\pi \circ \phi \circ \psi (D_4) = D_4'$ e na fórmula (19) resulta:

(20) $\qquad \gamma_U (D_4^*) = D_4'$

o que contradiz a proposição (I.5.1)

Assim, $\psi : \mathbb{Z} D_4 \to \mathbb{Z} D_4$ é um automorfismo normalizado que não é produto de um automorfismo interior por um automorfismo de G.

S.K.Sehgal | 26 | demonstrou que todo automorfismo normalizado do anel de grupo sôbre os inteiros de um grupo nilpotente G de classe 2 é o produto de um automorfismo de G por um automorfismo interior γ_u onde $u \in U(\mathbb{Q} G)$.

O resultado desta seção mostra que nem sempre é possível escolher u em $U(\mathbb{Z} G)$.

I.7. - $U(\mathbb{Z} D_4)$ NÃO É NILPOTENTE

Do teorema (III.2.5) segue, em particular, que $U(\mathbb{Z} D_4)$ não é nilpotente. Antes de concluir o capítulo vamos dar aqui uma demonstração direta deste fato.

Seja $\alpha = -a+a^3+b-a^2b+a^3b=\psi(a^3b)$. Então $\alpha^2 = \psi((a^3b)^2) = 1$.

Para cada inteiro n definimos $\beta(n) = 1-na+na^3+nb-na^2b$.

Pode-se verificar diretamente que $\beta(n)^{-1} = 1+na-na^3-nb+na^2b$.

Calculando, vem:

$$(\beta(n), \alpha) = \beta(n)\ \alpha\ \beta(n)^{-1}\ \alpha = \beta(2n)$$

Assim, para todo inteiro $k > 0$ é possível definir comutadores de classe k, diferentes de 1. Portanto, $U(\mathbb{Z} D_4)$ não é nilpotente. ⌋

CAPÍTULO II

ANÉIS DE GRUPO COM COEFICIENTES NUM ANEL COMUTATIVO, DE CARACTERÍSTICA DIFERENTE DE ZERO.

II.1. - ANÉIS DE GRUPO SÔBRE INTEIROS MÓDULO p^n

Seja p um inteiro primo e n > 0 um inteiro. Notaremos por $J_p n$ o anel dos inteiros módulo p^n.

Demonstraremos inicialmente um lema que relaciona os grupos de unidades de $J_p n\ G$ e $J_p m\ G$ — onde G é um grupo finito.

Aplicando esse resultado no caso em que G é um p-grupo daremos uma caracterização de $U(J_p n\ G)$ e mostraremos em particular, que é nilpotente. Desta forma teremos exibido uma família de exemplos que verificam as hipóteses do teorema (II.2.3).

Para todo inteiro n > m consideramos o epimorfismo canônico $J_p n \to J_p m$ e seja $\Phi_{mn} : J_p n\ G \to J_p m\ G$ o epimorfismo induzido nos anéis de grupo.

(II.1.1) - Lema - Seja G um grupo finito e $\Phi_{mn}\ J_p n\ G \to J_p m\ G$ o epimorfismo acima. Então, $\Phi_{mn}\ (U(J_p n\ G)) = U(J_p m\ G)$.

Demonstração - É claro que a imagem de uma unidade de $J_p n\ G$ é uma unidade em $J_p m\ G$. O único ponto interessante é mostrar que

$$\Phi_{mn}(U(J_p n\ G)) \supset U(J_p m\ G).$$

Seja, então, $\alpha \in U(J_p m\ G)$ com inverso α^{-1}, e seja $\alpha^* \in J_p n\ G$ uma pré imagem qualquer de α. Mostraremos que :

$$\alpha^* \in U(J_p n\ G)$$

De fato, se α' é uma pré imagem qualquer de α^{-1} temos que:

(1) $\qquad \alpha^* \alpha' = 1 + u \quad , \quad \alpha' \alpha^* = 1 + v,$

onde $u, v \in \ker(\Phi_{mn}) = p^m \cdot J_p n\ G$.

Óbviamente u e v são elementos nilpotentes (pois certamente $u^n = v^n = 0$). Chamando n_1 e n_2 aos respectivos índices de nilpotência temos que $1 + u$ e $1 + v$ são unidades com inversos:

$$\beta = (1 + u)^{-1} = 1 - u + u^2 - \ldots\ldots + (-1)^{n_1} u^{n_1}$$

$$\gamma = (1 + v)^{-1} = 1 - v + v^2 + \ldots\ldots + (-1)^{n_2} v^{n_2}$$

Em (1) vem:

(2) $\qquad (\gamma\alpha')\ \alpha^* = \alpha^*(\alpha'\beta) = 1$

Logo $\gamma\alpha' = \alpha'\beta = (\alpha^*)^{-1}$ e $\alpha^* \in U(J_p n\ G)$ □

Note-se que, da demonstração, segue um pouco mais: provamos que

$$U(J_p n\ G) = \Phi_{mn}^{-1}\ (U(J_p m\ G))$$

No restante desta seção G será sempre um p-grupo finito.

Precisaremos agora a notação que vamos utilizar na próxima proposição. Se $\alpha \in J_p n\ G$, então, α se escreve na forma:

$$\alpha = \sum_i (\lambda_i + (p^n))g_i \quad \text{onde}$$

$\lambda_i \in \mathbb{Z}$, $1 \leq i \leq |G|$; logo $\varepsilon(\alpha) = (\sum_i \lambda_i) + (p^n) \in J_p n$.

Para facilitar a notação escreveremos apenas $p|\varepsilon(\alpha)$ quando $p|\sum_i \lambda_i$.

(II.1.2) Proposição - Seja G um p-grupo finito. Então:

(i) O grupo das unidades de $J_p n\ G$ é:

$$U(J_p n\ G) = \{\ \alpha \in J_p n\ G |\ p \nmid \varepsilon(\alpha)\}$$

(ii) O único ideal maximal de $J_p n\ G$ é:

$$J(J_p n\ G) = \{\alpha \in J_p n\ G \mid p \mid \varepsilon(\alpha)\}.$$

Demonstração -

Consideremos inicialmente o anel $J_p G$ (onde J_p é um corpo). Como dizemos no Capítulo 0, tem-se que:

$$U(J_pG) = \{\alpha \in J_pG \mid p \dagger \varepsilon(\alpha)\}$$

Do lema anterior, temos que $U(J_pnG) = \Phi_{1n}^{-1}(U(J_pG))$

Seja, então, $\alpha = \sum_i (\lambda_i + (p^n))g_i \in J_pn\,G$ e $\lambda_i = pq_i + r_i$ com $0 \leq r_i < p$, $i = 1,\ldots,|G|$. Logo:

$$\Phi_{1n}(\alpha) = \sum_i r_i\, g_i$$

e claramente $p \dagger (\sum_i r_i)$ se e sòmente se $p \dagger (\sum_i \lambda_i)$. Segue / imediatamente (i).

Para obter (ii) basta observar que $J(J_pnG)$ é de fato um ideal e que todo elemento que não pertence a êle é uma unidade. □

(II.1.3) Corolário - Se G é um p-grupo finito o ideal fundamental $I = \mathrm{Ker}\,(\varepsilon)$ de $J_pn\,G$ é um ideal nilpotente.

Demonstração-

Como $J_pn\,G$ é finito então é um anel com C.C.D; logo o radical $J(J_pn\,G)$ é um ideal nilpotente.

Ainda, $\mathrm{Ker}\,(\varepsilon) = \{ \sum_i (\lambda_i + (p^n))g_i \mid p^n \mid (\sum_i \lambda_i) \}$ está contido em $J(J_pn\,G)$ logo é, êle próprio, um ideal nilpotente. □

O corolário acima é um caso particular do Teorema 9 de Connell | 8 | .

(II.1.4) Proposição - Seja G um p-grupo finito. Então $U(J_p n\ G)$ é um grupo nilpotente.

Demonstração -

Temos que $U(J_p n\ G) = U(J_p n) \times V(J_p n\ G)$ onde:

$$V(J_p n\ G) = \{\alpha \in J_p n\ G \mid \varepsilon(\alpha) = 1\}$$

e $U(J_p n)$ é comutativo.

Agora um simples cálculo combinatório mostra que:

$$| V(J_p n\ G) | = p^{n|G|} / p^n = p^{n(|G|-1)}$$

Assim, $V(J_p n\ G)$ é um p-grupo. $U(J_p n\ G)$ é, então, nilpotente. □

Para concluir esta seção daremos uma caracterização do centro de $U(J_p n\ G)$. Este resultado, porém, não será usado no que segue.

Seja $C = \{g_1, g_2, \ldots, g_s\}$ o centro do grupo G e $W = U(J_p n\ C)$. Indicaremos por $C_1, \ldots, C_t$ as classes de conjugação não unitárias de G; consideraremos os elementos:

$$\gamma_j = \sum_{g \in C_i} g \qquad 1 \leq j \leq t\ ,$$

e seja Γ o conjunto:

$$\Gamma = \{ \sum_{j=1}^{t} y_j \gamma_j \mid y_j \in J_p n\ ,\ 1 \leq j \leq t \}$$

(II.1.5) Proposição - Seja Z o centro de $U(J_p n\ G)$. Com as notações acima temos:

$$Z = V \cdot (1 + \Gamma) = \{ \alpha \cdot \beta \mid \alpha \in V,\ \beta \in 1 + \Gamma \}.$$

Demonstração -

O conjunto $\{g_1, \ldots, g_s, \gamma_1, \ldots, \gamma_t\}$ é uma base do centro do anel $J_p n\ G$.

(Ver Curtis-Reiner | 9 |, teorema (27.24), cuja demonstração pode adaptar-se a este caso.
Claramente $V \subset Z$ e também $1 + \Gamma \subset Z$ (note-se que, para cada i, $i \leq i \leq t$, $|C_i|$ é uma potência de p, logo se $\alpha \in 1 + \Gamma$, $\varepsilon(\alpha) \equiv 1 \pmod p$ e, da preposição (II.1.2) $\alpha \in U(J_p n\ G)$). Logo:

(3) $\qquad V(1 + \Gamma) \subset Z$

Seja então $\alpha \in Z$. Como α comuta em particular com todo elemento de G, α pertence ao centro do anel $J_p n$ G e pode-se escrever α na forma:

$$\alpha = \sum_{i=1}^{s} x_i g_i + \sum_{j=1}^{t} y_j \gamma_j \qquad x_i, y_j \in J_p n \ ,$$

Então, $\varepsilon(\alpha) = \sum_{i=1}^{s} x_i + \sum_{j=1}^{t} y_j\ \varepsilon(\gamma_j)$. Como $p \mid \varepsilon(\gamma_j)$, $1 \leq j \leq t$ e $p \nmid \varepsilon(\alpha)$ vem imediatamente que $p \nmid \sum_{i=1}^{s} x_i$; portanto, o elemento $\alpha_1 = \sum_{i=1}^{s} x_i\ g_i$ é inversível i.é., $\alpha_1 \in V$.

Finalmente, temos que $\alpha = \alpha_1(1 + \alpha_1^{-1} \cdot \sum_{j=1}^{t} y_j \gamma_j)$. Como produto por elementos centrais leva elementos conjugados em elementos conjugados segue que $\alpha_1^{-1} \cdot \sum_{j=1}^{t} y_j \gamma_j \in \Gamma$ e $\alpha \in V(1 + \Gamma)$, logo

(4) $\qquad Z \subset V(1 + \Gamma)$.

De (3) e (4) segue a igualdade □

Observações

1. - O resultado acima permite dar outra demonstração da proposição (II.1.4). De fato, segue fàcilmente que

$$\left| \frac{U(J_p^n G)}{Z} \right| = \frac{|U(J_p^n G)|}{|Z|} = p^{n(|G| - (s+t))}.$$

Agora, se o quociente de um grupo por seu centro é nilpotente, então, o grupo é nilpotente.

2. - A formulação da proposição (II.1.5) poderia levar a pensar / que $1 + \Gamma$ é um subgrupo de Z. Isto não é, em geral, verdadeiro.

Pode-se dar um contra exemplo considerando o grupo quatérnio de ordem 8, i.é., o grupo Q com dois geradores a e b verificando as relações:

$$a^4 = 1;\ a^2 = b^2\ ;\ b^{-1}ab = a^{-1}$$

Explícitamente:

$$Q = \{1, a, a^2 = b^2, a^3 = b^2a, b, ab = ba^3, a^2b = b^3, a^3b = ba\}$$

As classes de conjugação não triviais de Q são:

$$C_1 = \{a, a^3\} \quad ; \quad C_2 = \{b, b^3\} \quad ; \quad C_3 = \{ab, a^3b\}$$

e o centro é:

$$C = \{1, a^2\}$$

Assim, $\gamma_1 = a + a^3$, $\gamma_2 = b + b^3$, $\gamma_3 = ab + a^3b$.

Calculando em $J_2\, Q$ temos:

$$(1 + \gamma_3)^2 = 1 + 2\gamma_3 + 2(1 + a^2) \notin 1 + \Gamma \ .$$

II.2. - COEFICIENTES NUM ANEL COMUTATIVO DE CARACTERISTICA DIFERENTE DE ZERO.

Nesta seção R indicará sempre um anel comutativo de característica diferente de zero. Começaremos estudanto o caso em que $R = p^n$ onde p indica um inteiro primo.

No decorrer da demonstração do próximo teorema precisaremos dos seguintes lemas:

(II.2.1) Lema - (Motose e Tominaga, |16|) - Seja S um anel com elemento unidade e N um ideal bilateral nilpotente de S. Se S/N é comutativo e $|N, S| = \{ xy - yx \mid x \in N, y \in S \}$ esta contido em N^2, então, o grupo das unidades de S é nilpotente.

(II.2.2) Lema - (Herstein e Small|11|). - Seja A uma álgebra sobre um anel comutativo R, finitamente gerada como R-módulo. Se A tem um conjunto finito de geradores cada um dos quais é um elemento nilpotente, então, A é nilpotente.

Agora estamos em condições de demonstrar:

(II.2.3.) Teorema - Seja R um anel comutativo com unidade tal que car $R = p^n$ onde p é um inteiro primo e seja G um grupo finito. Então, $U(RG)$ é nilpotente se e sòmente se G é o produto direto de um p-grupo e um grupo abeliano.

Demonstração -

Suponhamos que G seja da forma $P \times A$ onde P é um p-grupo e A um grupo abeliano. Escrevemos:

$$P = \{h_1, \ldots, h_s\} \quad , \quad A = \{a_1, \ldots, a_t\}$$

onde $h_1 = a_1 = 1$ (o elemento neutro de G). Então, todo elemento $x \in RG$ pode-se escrever na forma:

$$(5) \qquad x = \sum_{ij} k_{ij}\, a_i\, h_j \quad \text{com } k_{ij} \in R \quad 1 \leq i \leq t,\ 1 \leq j \leq s.$$

O epimorfismo natural $\Phi : G \to A$ se estende na forma usual a um epimorfismo $\Phi^* : RG \to RA$ definido por:

$$(6) \qquad x = \sum_{ij} k_{ij} a_i\, h_j \xmapsto{\Phi^*} \sum_{ij} \Phi(a_i h_j) = \sum_{i=1}^{t} \Big(\sum_{j=1}^{s} k_{ij} \Big)\, a_i$$

Do teorema do homomorfismo para anéis temos que $RG/\ker(\Phi^*) \cong RA$,

onde:

$$(7) \qquad \mathrm{Ker}(\Phi^*) = \{ \textstyle\sum_{ij} k_{ij} a_i \in RG \mid \sum_{j=1}^{s} k_{ij} = 0,\ 1 \leq i \leq t \} .$$

Mostraremos agora que tomando S = RG e N = $\mathrm{Ker}(\Phi^*)$ estamos nas condições do lema(II.2.1) e que mostrará que U(RG) é nilpotente.

De fato, do isomorfismo acima segue que RG/$\mathrm{Ker}(\Phi^*)$ é comutativo e N = $\mathrm{Ker}(\Phi^*)$ é claramente um ideal bilateral de RG.Mostraremos primeiro que é nilpotente.

De (7) segue que, se $x \in \mathrm{Ker}(\Phi^*)$ podemos escrever:

$$x = \textstyle\sum_{ij} k_{ij}\, a_i\, h_j = \sum_{ij} k_{ij}\, a_i\, h_j - \sum_{i=1}^{t} (\sum_{j=1}^{s} k_{ij}) a_i = \sum_{ij} k_{ij} a_i (h_j - 1)$$

logo o conjunto $\{a_i(h_j - 1) \mid 1 \leq i \leq t,\ 2 \leq j \leq s\}$ é um conjunto de geradores de $\mathrm{Ker}(\Phi^*)$ sôbre R.

Em presença do lema (II.2.2) será suficiente demonstrar / que todo elemento da forma a(h-1) com $a \in A$ e $h \in P$ é nilpotente. Como $(a(h-1))^k = a^k (h-1)^k$ mostraremos que, para cada $h \in P$, existe um inteiro positivo k tal que $(h-1)^k = 0$.

De fato:

$$(8) \qquad (1-h)^k = 1 - \binom{k}{1} h + \binom{k}{2} h^2 - \ldots\ldots + (-1)^k h^k$$

Se $o(h) = p^r$ a fórmula (8) pode escrever na forma:

$$(9) \qquad (1-h)^k = x_o + x_1 h + \ldots + x_{p^r-1} \cdot h^{p^r-1}$$

com $x_j = \sum_i (-1)^{j+ip^r} \binom{k}{j + ip^r}$ onde a soma se estende sôbre todos os inteiros $i \geq 0$ tais que $j + ip^r \leq k$.

Agora, da Proposição 13 de Connell |8| existe um inteiro u tal que p^u divide x_j, $0 \leq j \leq p^r - 1$, e $u \to \infty$ quando $k \to \infty$. Tomando k suficientemente grande para que $u > n$ temos que $(1-h)^k = 0$.

Finalmente, deveremos provar que $|Ker(\phi^*), RG| \subset Ker(\phi^*)^2$. Para isso será suficiente mostrar que, para todo $g \in G$ e todos / $a \in A$, $h \in P$ tem-se que:

$a(h-1)g - g\,a(h-1) \in Ker(\phi^*)^2$.

Agora, dado $g \in G$ existem $a' \in A$ e $h' \in P$ tais que /

$g = a'h' = a'(h' - 1) + a'$ (onde a' é um elemento central). Logo:

$a(h-1)g - ga(h-1) = a(h-1)\,a'(h'-1) - a'(h'-1)a\,(h-1) \in N^2$.

Recìprocamente, suponhamos que $U(J_p n\ G)$ seja nilpotente. Como G é um subgrupo de $U(J_p n\ G)$, G é nilpotente. Portanto para obter a tese bastará demonstrar que para todo primo $q \neq p$ o q-subgrupo de Sylow de G é comutativo.

Seja, então, $q \neq p$ primo e Q o q-subgrupo de Sylow de G. Como R é comutativo, de característica p^n, R contém um subanel / $\overline{R} \cong J_p n$. Então, $U(\overline{R}\ Q)$ é um subgrupo de U(RG) e, portanto, é nilpotente.

Como $U(J_p n\ Q) \cong U(\overline{R}\ Q)$ é nilpotente e do lema (II.1.1) existe um epimorfismo $\Phi_{ln} : U(J_p n\ Q) \longrightarrow U(J_p\ Q)$ este último grupo também é nilpotente.

Agora car $J_p = p$ não divide $|Q|$ portanto J_pQ é semisimples e, pelo teorema de Wedderburn, deve ser da forma:

$$J_pQ \cong M_{n_1}(D_1) \oplus \ldots \oplus M_{n_t}(D_t)$$

onde $M_{n_i}(D_i)$ indica o anel das matrizes de $n_i \times n_i$ com coeficientes no anel com divisão D_i (que contém J_p no seu centro). É bem sabido que o grupo das unidades de um anel de matrizes $M_{n_i}(D_i)$ não é nilpotente se $n_i \neq 1$; logo $J_p\ Q = D_1 \oplus \ldots \oplus D_t$. Ainda, segue de resultados de L.K.Hua |13| ou W.R.Scott |25| que o grupo das unidades de um anel com divisão não é nem solúvel quando o anel não é comutativo; portanto, $J_p\ Q$ deve ser soma direta de corpos e, consequentemente, Q é abeliano. □

Observamos que o teorema acima generaliza o resultado de Bateman - Coleman |1| .

O argumento do último parágrafo é relativamente "standard" e já foi usado por exemplo, por Motose e Tominaga |16| e Bhattacharya e Jain |3|.

(II.2.4) Lema - Seja G um grupo finito e $m > 0$ um inteiro. Se $m = p_1^{\alpha_1} \ldots p_t^{\alpha_t}$ é a decomposição em fatores primos de m, então:

(i) $J_m\, G \cong J_{p_1^{\alpha_1}} G \oplus \ldots \oplus J_{p_t^{\alpha_t}} G$,

(ii) $J_p\alpha\, G$ é indecomponível se e sòmente se G é um p-grupo.

Demonstração-

Pelo teorema do Resto Chinês, existe um isomorfismo:

$$\Phi : J_m \longrightarrow J_{p_1^{\alpha_1}} \oplus \ldots \oplus J_{p_t^{\alpha_t}}$$

que se estende na forma usual a um isomorfismo:

$$\Phi : J_m G \longrightarrow (J_{p_1^{\alpha_1}} \oplus \ldots \oplus J_{p_t^{\alpha_t}})G \cong J_{p_1^{\alpha_1}} G \oplus \ldots \oplus J_{p_t^{\alpha_t}} G.$$

Isto demonstra a parte (i) do enunciado.

Para demonstrar (ii) suponhamos inicialmente que G não é um p-grupo. Então, para algum primo $q \neq p$, G contém um subgrupo Q de ordem q.

Seja $e = \frac{1}{q} \sum_{x \in H} x$. É fácil verificar que $e \neq 0,1$ é um / idempotente em $J_p\alpha\, G$ (pois q é inversível em $J_p\alpha$); logo o anel de grupo é decomponível.

Recìprocamente, se $J_p\alpha\, G$ é indecomponível existe um idempotente $e \in J_p\alpha\, G$, $e \neq 0,1$. Como $e^2 = e$ temos que $e(e-1) = 0$ e segue que e é um divisor de 0. Da proposição (II.1.2) e $\in J(J_p\alpha\, G)$ e é, portanto, nilpotente. Isto é uma contradição, já que para todo $n > 0$ inteiro tem-se que $e^n = e$. □

Observamos que a parte (ii) do enunciado acima é análoga a um resultado de D.B.Coleman |6| para anéis de grupo RG onde G é finito e R um domínio de integridade.

(II.2.5) Teorema - Seja R um anel comutativo de característica / $m \neq 0$ tal que $m = p_1^{\alpha_1}.....p_t^{\alpha_t}$ com $t \geq 2$ é a decomposição em fatores primos de m e seja G um grupo finito. Então U(RG) é nilpotente se e sòmente se G é abeliano.

Demonstração -

De novo, se car R = m, R contém um anel $\bar{R} \cong J_m$ e $U(\bar{R}G)$ sendo um subgrupo de U(RG) é nilpotente.

Usando o lema anterior segue que $U(J_{p_1^{\alpha_1}}G \oplus ... \oplus J_{p_t^{\alpha_t}}G)$ é nilpotente e, portanto, cada subgrupo $U(J_{p_i^{\alpha_i}}G)$ também o é.

Seja agora P_i um p_i subgrupo de Sylow de G. Como $t \geq 2$ existe j com $p_i \neq p_j$. Consideramos, então, o grupo $U(J_{p_j^{\alpha_j}}P_i)$ que é nilpotente. Do teorema (II.2.3) segue que P_i é abeliano.

Assim, todo subgrupo de Sylow de G é abeliano e como o próprio G é nilpotente é abeliano. ⌋

CAPÍTULO III

AS UNIDADES DE $\mathbb{Z}$ G.

G.D.Higman caracterizou completamente, em |12|, os grupos finitos G tais que as únicas unidades de $\mathbb{Z}$ G são as triviais. Esta caracterização é dada pelo seguinte.

(III.1.1) Teorema (|12|, teorema 11) - $U(\mathbb{Z} G) = \{\pm 1\} \times G$ se e sòmente se alguma das seguintes condições está verificada.

(i) G é abeliano e todo elemento diferente da unidade / tem ordem 2,3,4 ou 6.

(ii) G é um 2-grupo Hamiltoniano.

Conforme o teorema de Bateman e Coleman|1|, se K é um corpo de característica 0 e G um grupo finito, então U(K G) é nilpotente se e sòmente se G é abeliano.

Podemos observar agora que este resultado não pode ser

generalizado para anéis de grupos sôbre os inteiros. De fato, se G é um 2-grupo Hamiltoniano, $U(\mathbb{Z}\,G) = \{\pm 1\} \times G$ é um 2-grupo, logo nilpotente e G não é abeliano.

Mostraremos aqui que os 2-grupos Hamiltonianos são os únicos grupos não comutativos G tais que $U(\mathbb{Z}\,G)$ é nilpotente. Apresentaremos a demonstração deste fato decomposta em vários passos sucessivos.

(III.1.2) Proposição - Seja G um grupo finito, não abeliano. Se $U(\mathbb{Z}\,G)$ é nilpotente, então G é um grupo Hamiltoniano (i.é. um grupo tal que todo subgrupo é normal).

Demonstração - Suponhamos que G não é Hamiltoniano. Então existem elementos $a,b \in G$ tais que $a^{-1}ba$ não pertence ao grupo cíclico gerado por b.

Sejam: $O(b) = n$ e $u = (1-b)a(1+b+\ldots+b^{n-1})$

Obviamente $u \neq 0$ e $u^2 = 0$. Assim $\alpha_0 = 1 + u$ é uma unidade de $\mathbb{Z}\,G$ cujo inverso é $\alpha^{-1} = 1 - u$.

Definimos por recorrência:

(8) $\alpha_1 = |\alpha_0, b| = \alpha_0 b\, \alpha_0^{-1}\, b^{-1}$ e $\alpha_k = |\alpha_{k-1}, b|$.

Mostraremos usando indução que:

(9) $\alpha_k = 1 + (1 - b)^k\, u.$

De fato, para $k = 1$ temos:

$$\alpha_1 = |\alpha_0, b| = (1 + u)\, b(1 - u)\, b^{-1}$$

Da própria definição de u segue que $ub^{-1} = u$, logo:

$$\alpha_1 = (b + u)(b^{-1} - u) = 1 - bu + u = 1 + (1 - b)u.$$

Suponhamos agora que $\alpha_{k-1} = 1 + (1 - b)^{k-1} u$. Então:

$\alpha_{k-1}^{-1} = 1 - (1 - b)^{k-1} u$ pois:

$$u(1-b)^{k-1} = u(1 - \binom{k-1}{1} b + \ldots + (-1)^{k-1} b^{k-1}) = (1 - \binom{k-1}{1} + \ldots + (-1)^{k-1})\, u = 0$$

Logo:

$$(1 + (1-b)^{k-1} u)(1 - (1-b)^{k-1} u) =$$

$$= 1 + (1-b)^{k-1} u - (1-b)^{k-1} u + (1-b)^{k-1} u - (1-b)^{k-1} u (1-b)^{k-1} u = 1$$

Calculando agora temos:

$$\alpha_k = (1 + (1-b)^{k-1} u)\, b (1 - (1-b)^{k-1} u)\, b^{-1}$$

$$= (b + (1-b)^{k-1} u)\, (b - (1-b)^{k-1} u)$$

$$= 1 - b(1-b)^{k-1} u + (1-b)^{k-1} u = 1 + (1-b)^k u.$$

Indiquemos $\Gamma = a(1 + b + \ldots + b^{n-1})$

Temos que:

(10)
$$(1-b)^{k-1} u = (1-b)^k a(1 + b + \ldots + b^{n-1}) =$$

$$= \Gamma - \binom{k}{1} b\Gamma + \ldots + (-1)^j \binom{k}{j} b^j \Gamma + \ldots + (-1)^k b^k \Gamma$$

Dado um elemento $\sum_i \alpha_i g_i \in \mathbb{Z} G$ chama-se <u>suporte</u> de x ao conjunto:

$$\mathrm{Sup}(\sum_i \alpha_i g_i) = \{g_i \in G \mid \alpha_i \neq 0\}$$

Notemos inicialmente que $\mathrm{Sup}(\Gamma) \cap \mathrm{Sup}(b^x \Gamma) = \phi$ se e so -

mente se $\Gamma = b^x \Gamma$. De fato, a suficiência é trivial e se $ab^i = b^x$ a b^j para algum par (i,j), então, a $b^{i+k} = b^x\ ab^{j+k}$. Quando ab^{i+k} percorre todos os elementos de $Sup(\Gamma)$, b^x a b^{j+k} percorre todos os elementos de $Sup(b^x\ \Gamma)$ e segue a igualdade.

Seja, então, $r = \min\{x > 0 \mid \Gamma = b^x\ \Gamma\}$

Agora é fácil ver que $Sup(b^h\Gamma) \cap Sup(b^t\Gamma) \neq \phi$ se e sòmente se $t \equiv h \pmod r$. De fato se b^h a $b^i = b^t\ ab^j$ para algum par (i,j), então, $ab^i = b^{t-h}\ ab^j$ e $\Gamma = b^{t-h}\ \Gamma$ de onde segue imediatamente que $t \equiv h \pmod r$. A recíproca é trivial.

Podemos agora escrever a fórmula (10) na forma:

$$(11) \qquad (1-b)^k\ u = x_o\ \Gamma + x_1\ b\ \Gamma + \ldots + x_{r-1}\ b^{r-1}\ \Gamma,$$

com $x_s = \sum_{i \geq 0} (-1)^{s+ir} \binom{k}{s+ir}$,

onde a soma se estende sôbre todos os valores de $i \geq 0$ tais que $s + ir \leq k$.

Como os somandos do segundo membro de (11) tem suporte disjunto segue que $(1-b)^k\ u = 0$ se e sòmente se $x_s = 0$ para todo s, $0 \leq s \leq r - 1$.

Finalmente, seja ξ uma raïz primitiva r-ésima da unidade. Então:

$$(1 - \xi)^k = x_o + x_1\ \xi + \ldots + x_{r-1}\xi^{r-1}$$

e se todo os coeficientes fossem 0 ter-se-ia $\xi = 1$ o que seria uma contradição.

Das considerações acima e da fórmula (9) segue que, para todo k, $\alpha_k \neq 1$, logo U(ℤ G) não é nilpotente. □

É um fato bem conhecido (M.Hall |10| teorema 12.5.4) que todo grupo Hamiltoniano G pode se escrever como um produto direto da forma $G = T_1 \times T_2 \times Q$ onde T_1 é um grupo abeliano tal que todo elemento tem ordem ímpar, T_2 é um grupo abeliano de expoente 2 e Q um grupo quatérnio de ordem 8.

Os próximos passos estarão destinados a provar que se G é um grupo Hamiltoniano tal que U(ℤ G) é nilpotente, então, quando decomposto na forma acima tem-se que $T_1 = \{1\}$. Para isso bastará / provar que para todo primo $p > 2$, T_1 não contém elementos de ordem p. Precisaremos discutir separadamente os casos $p = 3$ e $p > 3$.

(III.1.3) Lema - Seja $G = T \times Q$ o produto direto de um grupo abe - liano T por um grupo quatérnio de ordem 8. Se T contém algum elemento de ordem 3, então, U(ℤ G) não é nilpotente.

Demonstração

Adotamos novamente para os elementos de Q a notação da seção II.1.

Suponhamos que T contém um elemento g de ordem 3.

A.A.Bovdi exibiu em |4| a seguinte unidade de ℤ G:

$$u = 1 + (225(2 - g - g^2) + 390(bg^2 - bg))(1 - b^2)$$

cuja inversa é:

$$u^{-1} = 1 + (225(2 - g - g^2) - 390(bg^2 - bg))\ (1 - b^2)$$

Como g comuta com a e $aba^{-1} = b^3$, a b^2 $a^{-1} = b^2$ temos:

$$a\ u^{-1}\ a^{-1} = 1 + (225(2 - g - g^2) - 390(bg^2 - bg)\ b^2)(1 - b^2).$$

Ainda, como $b^2(1 - b^2) = -(1 - b^2)$ temos:

(12) $$a\ u^{-1}a^{-1} = 1 + (225(2-g-g^2) + 390(bg^2-bg))(1-b^2) = u.$$

Definimos por recorrência:

(13) $$\alpha_1 = |u, a| \qquad \text{e} \qquad \alpha_k = |\alpha_{k-1}, a|$$

Mostraremos, por indução, que $\alpha_k = u^{2^k}$. De fato, para $k = 1$ o resultado segue imediatamente de (12).

Suponhamos então que $\alpha_{k-1} = u^{2^{k-1}}$. Temos:

(14) $$\alpha_k = u^{2^{k-1}}\ a\ u^{-2^{k-1}}\ a^{-1} = u^{2^{k-1}}\ (a\ u^{-1}a^{-1})^{2^{k-1}} = u^{2^{k-1}}.u^{2^{k-1}} = u^{2^k}.$$

Agora mostraremos que u não é uma unidade de ordem finita. De fato, em caso contrário o coeficiente de 1 na expressão de u deveria ser 0 (ver Berman|2|, Takahashi|27|ou Cohn e Livingstone |5|) No caso, este coeficiente é $\lambda = 451$.

Segue da observação acima e da fórmula (14) que para todo k existem comutadores de ordem k, diferentes de 1; logo $U(\mathbb{Z}G)$ não é nilpotente. □

(III.1.4) Lema - Seja $G = T \times Q$ o produto direto de um grupo abeliano T por um grupo quatérnio de ordem 8. Se T contém um elemento de ordem prima $p > 3$ então $U(\mathbb{Z}G)$ não é nilpotente.

Demonstração

Suponhamos que T contém um elemento g de ordem prima / $p > 3$. Novamente com as notações do final da seção II.1 tomamos $a \in Q$ e consideramos $H = (g) \times (a)$ (onde (g) e (a) indicam os subgrupos cíclicos gerados por g e a respectivamente).

C.D.Berman demonstrou em |2|, lema 9, que a decomposição de $\mathbb{Q}H$ em soma direta de ideais bilaterais é:

$$\mathbb{Q}H = I_1 \oplus \ldots \oplus I_6 ,$$

onde os idempotentes e_i tais que $I_i = \mathbb{Q}He_i$ são:

$$e_1 = \frac{1}{4p}(1 + a + a^2 + a^3)(1 + g + \ldots + g^{p-1})$$

$$e_2 = \frac{1}{4p}(1 - a + a^2 - a^3)(1 + g + \ldots + g^{p-1})$$

$$e_3 = \frac{1}{2p}(1 - a^2)\ (1 + g + \ldots + g^{p-1}) \qquad (15)$$

$$e_4 = \frac{1}{4p}(1 + a + a^2 + a^3)(p - 1 - g - \ldots - g^{p-1})$$

$$e_5 = \frac{1}{4p}(1 - a + a^2 - a^3)(p - 1 - g - \ldots - g^{p-1})$$

$$e_6 = \frac{1}{2p}(1 - a^2)(p - 1 - g - \ldots - g^{p-1})$$

O elemento $\xi = ga\, e_6$ do corpo I_6 é uma raíz primitiva da unidade de grau 4p e $I_6 = \mathbb{Q}(\xi)$ (identificando $\mathbb{Q}$ com $\mathbb{Q}\, e_6 \subset I_6$)

Berman mostrou também que se s indica o número de classes residuais módulo 4p em $\mathbb{Q}(\xi)$ que são primas com 4p, então, a seguinte é uma unidade de $\mathbb{Z}H$ — e, portanto, de $\mathbb{Z}G$:

$$\alpha = e_1+\ldots+e_5+(1+ga+g^2a^2)^s\, e_6 = e_1+\ldots+e_5+(1+\xi+\xi^2)^s\, e_6 \,. \tag{16}$$

Na demonstração de que α é unidade intervém decisivamente o fato de que $p > 3$.

Note-se que, em geral, se $f \in \mathbb{Z}[X]$, como e_6 é idempotente, tem-se que $f(\xi) = f(\xi)e_6$ (onde $\mathbb{Z} \subset I_6$ está identificado com $\mathbb{Z}\, e_6$).

Ainda a dimensão de $\mathbb{Q}(\xi)$ sôbre $\mathbb{Q}$ é $\phi(\xi) = 2(p-1)$, logo todo elemento de $\mathbb{Z}(\xi)$, e em particular $(1+\xi+\xi^2)^s$, pode se escrever na forma $h(\xi)$ onde $h \in \mathbb{Z}[X]$ é um polinômio de grau menor ou igual a $2(p-1)-1$.

Na expressão reduzida de $(1+\xi+\xi^2)^s$ devem aparecer não nulos de grau par e de grau ímpar, como mostra o seguinte segmento (também devido a Berman):

Se só existissem termos de grau par ou só de grau ímpar ter-se-ia respectivamente:

$$(1+\xi+\xi^2)^s = \pm\,(1-\xi+\xi^2)^s,$$

e tomando módulos:

$$|1+\xi+\xi^2| = |1-\xi+\xi^2| \;;$$

esta última igualdade é impossível pois ξ e $1 + \xi^2$ pertencem à mesma reta do plano complexo.

Agora, mostraremos no próximo lema que se

$$u = e_1 + \ldots\ldots + e_5 + f(\xi)e_6 \in U(\mathbb{Z}\, G)$$

onde $f \in \mathbb{Z}[X]$ tem grau menor ou igual a $2(p-1) - 1$ e contém termos não nulos de ordem par e de ordem ímpar, então:

$$u^{-1}\, b^{-1}\, u\, b = e_1 + \ldots\ldots + e_5 + F(\xi)e_6 \neq 1 \quad ,$$

onde $F \in \mathbb{Z}[X]$ também é de grau menor ou igual a $2(p-1)-1$ e contém termos não nulos de ordem par e de ordem ímpar.

Da fórmula (16) segue que α é uma unidade nestas condições e um argumento de indução óbvio mostra que para todo inteiro $k > 0$ existem em $U(\mathbb{Z}\, G)$ comutadores de ordem k diferentes de 1; logo $U(\mathbb{Z}\, G)$ não é nilpotente. □

(III.1.5) Lema - Com as notações do lema anterior, seja

$$u = e_1 + \ldots\ldots + e_5 + f(\xi)$$

uma unidade de $\mathbb{Z}\, G$ onde $f \in \mathbb{Z}[X]$ é um polinômio de grau menor ou igual a $2(p-1) - 1$ que contém termos não nulos de grau par e de grau ímpar. Então $u^{-1}\, b^{-1}\, u\, b = e_1 + \ldots\ldots + e_5 + F(\xi)\, e_6$ onde / $F \in \mathbb{Z}[X]$ é um polinômio nas mesmas condições que f.

Demonstração

Notemos inicialmente que em Q temos:

$$b^{-1}\, a\, b = a^3,\ b^{-1}\, a^2\, b = a^2,\ b^{-1}\, a^3 b = a$$

logo, das expressões (15) segue que $b^{-1} e_i b = e_i$, $i = 1,\ldots,6$. Logo:

(17) $\quad b^{-1} u b = e_1 + \ldots + e_5 + b^{-1} f(\xi) b e_6$.

Seja então $f = \alpha_0 + \alpha_1 X + \ldots + \alpha_r X^r \in \mathbb{Z}|X|$ onde $r \leq 2(p-1) - 1$

Como $b^{-1} \alpha_i g^i a^i e_6^i b = \alpha_i g^i b^{-1} a^i b \, e_6$ e $b^{-1} a^i b = \begin{cases} a^i \text{ se } i \text{ é par} \\ a^{i+2} \text{ se } i \text{ é ímpar} \end{cases}$

temos:

(18) $b^{-1} f(\xi) b = \sum_{i \equiv 0 \,(\mathrm{mod}\ 2)} \alpha_i \xi^i + \sum_{i \equiv 1 \,(\mathrm{mod}\ 2)} \alpha_i g^i a^{i+2} e_6 =$

$$= \sum_{i \equiv 0 \,(\mathrm{mod}\ 2)} \alpha_i \xi^i + \sum_{i \equiv 1 \,(\mathrm{mod}\ 2)} (\alpha_i g^i a^i - \alpha_i g^i a^i (1-a^2)) e_6 =$$

$$= \sum_{i \equiv 0 \,(\mathrm{mod}\ 2)} \alpha_i \xi^i + \sum_{i \equiv 1 \,(\mathrm{mod}\ 2)} \alpha_i \xi^i - \Big(\sum_{i \equiv 1 \,(\mathrm{mod}\ 2)} \alpha_i g^i a^i \Big)(1-a^2) e_6$$

Chamando $h(X) = \sum_{i \equiv 1 \,(\mathrm{mod}\ 2)} \alpha_i X^i$, como $(1 - a^2) e_6 = 2e_6$ e

$g\ a\ e_6 = \xi$ temos:

$b^{-1} f(\xi) b = f(\xi) - 2h(\xi)$ e substituindo em (17) vem:

(19) $\quad b^{-1} u b = e_1 + \ldots + e_5 + (f(\xi) - 2h(\xi)) e_6$

Agora como u é uma unidade de $\mathbb{Z}$ H, u^{-1} também o é. Todo elemento de $\mathbb{Z}$ H é inteiro sôbre $\mathbb{Z}$, portanto quando decomposto em soma:

$$u^{-1} = u_1 + \ldots + u_5 + u_6,$$

cada u_i deve ser um inteiro algébrico do respectivo corpo I_i, / $i = 1, \ldots, 6$. Como o conjunto dos inteiros algébricos de I_6 é precisamente $\mathbb{Z}[\xi]$ segue que existe um polinômio $f^* \in \mathbb{Z}[X]$ com grau$(f^*)=2(p-1)-1$ tal que $f(\xi) \cdot f^*(\xi) = 1$ e

$$u^{-1} = e_1 + \ldots + e_5 + f^*(\xi)\, e_6$$

Podemos calcular:

$$u^{-1}\, b^{-1}\, u\, b = e_1 + \ldots + e_5 + f^*(\xi)(f(\xi) - 2h(\xi))\, e_6 . \tag{20}$$

Chamando $F(\xi) = 1 - 2 f^*(\xi)\, h(\xi)$ (uma vez reduzido a uma expressão de grau menor ou igual que $2(p-1)$) temos:

$$u^{-1}\, b^{-1}\, u\, b = e_1 + \ldots + e_5 + F(\xi)\, e_6 \tag{21}$$

Para concluir, mostraremos que $F(\xi)$ contém termos não / nulos de ordem ímpar e de ordem par.

Suponhamos inicialmente que $F(\xi)$ não contém termos de / grau ímpar. Ter-se-ia então $F(\xi) = F(-\xi)$ i.é.:

$$1 - 2 f^*(\xi)\, h(\xi) = 1 + 2 f^*(-\xi)\, h(\xi) . \tag{22}$$

(pois $h(\xi)$ só contém termos de ordem ímpar).

Como grau (h) $\leq$ grau (f) < 2(p - 1) = $\phi(4p)$ que é o grau do polinômio minimal de ξ sôbre $\mathbb{Q}$, $h(\xi) = 0$ se e sòmente se h é / o polinômio nulo e isto não acontece pois f contém termos não nu - los de grau ímpar. A fórmula (21) implica então:

(22) $\quad -f^*(\xi) = f^*(-\xi)$

Ainda como ξ é raiz primitiva da unidade de grau 4p, / $-\xi$ também o é, e existe um $\mathbb{Q}$ - automorfismo ϕ de $\mathbb{Q}(\xi)$ tal que $\phi(\xi) = -\xi$.

Como $f(\xi)\, f^*(-\xi) = 1$ aplicando ϕ segue que $f(-\xi)f^*(\xi)=1$ i.e. $f^*(\xi) = f(-\xi)^{-1}$ em I_6 .

Tomando inversos em (22) temos:

(23) $\quad -f(\xi) = f(-\xi)$

i.é. $\quad 2 \sum_{i \equiv 0 (\mathrm{mod}\ 2)} \alpha_i \xi^i = 0$

De novo, este é um polinômio não nulo, (pois f contém ter mos não nulos de grau par), de grau menor que $\phi(4p)$. Temos assim / uma contradição.

Finalmente, suponhamos que F não contém termos não nulos de grau par. Ter-se-ia $F(\xi) = -F(-\xi)$ i.é.

(24) $\quad 1 - 2 f^*(\xi) h(\xi) = -1 - 2 f^*(-\xi) h(\xi)$.

Logo

(25) $\quad 1 = (f^*(-\xi) - f^*(\xi))\, h(\xi)$.

Se $f^*(X) = \sum \beta_i X^i$ temos que $f^*(-\xi) - f^*(\xi) = -\sum_{i\equiv 1 (\mathrm{mod}\ 2)} 2\beta_i \xi^i$

Chamando $k(X) = -\sum_{i\equiv 1(\mathrm{mod}\ 2)} \beta_i X^i$ a fórmula (25) se expressa como:

$$2\, k(\xi).\, h(\xi) = 1$$

Assim, 1/2 seria um inteiro algébrico. □

Finalmente estamos em condições de enunciar o resultado principal deste Capítulo.

(III.1.6) Teorema - Seja G um grupo finito. Então U(ℤ G) é nilpotente se e sòmente se G é comutativo ou um 2-grupo Hamiltoniano.

Demonstração.

Suponhamos que U(ℤ G) é nilpotente. Se G não é abeliano segue da proposição (III.1.2) que G é um grupo Hamiltoniano; portanto, da forma $G = T_1 \times T_2 \times Q$ onde T_1 é abeliano tal que todo elemento é de ordem ímpar, T_2 é abeliano de expoente dois e Q o grupo quatérnio de ordem 8.

Então $U(\mathbb{Z}\, T_1 \times Q)$ também é nilpotente e segue dos lemas (III.1.3) e (III.1.4) que $T_1 = \{1\}$. Assim $G = T_2 \times Q$ é um 2-grupo.

Para a proposição recíproca observamos que se G é abeliano $U(\mathbb{Z}\, G)$ também é abeliano. Se G é um 2.grupo Hamiltoniano a tese resulta imediatamente da observação que segue ao Teorema (III.1.1).

(III.1.7) Corolário - Seja R um anel comutativo, de característica 0 que contém uma raíz primitiva n-ésima da unidade ξ, com $n \geq 2$. Então U(R G) é nilpotente se e sòmente se G é abeliano.

Demonstração

Seja $H = \{1, \xi, \ldots, \xi^{n-1}\}$

Indicando por f o polinômio minimal de ξ sôbre $\mathbb{Q}$ temos um isomorfismo de anéis:

$$\mathbb{Z}\, H \cong \frac{\mathbb{Z}\,[X]}{(f)} \cong \mathbb{Z}\,[\xi]$$

logo:

$$\mathbb{Z}\,(H \times G) = \mathbb{Z}H \underset{\mathbb{Z}}{\otimes} \mathbb{Z}\,G \cong \mathbb{Z}\,[\xi]\,G$$

Assim:

$$U(R\,G) \supset U(\mathbb{Z}\,[\xi]\,G) \cong U(\mathbb{Z}\,(H \times G))$$

Se G não é abeliano, como H é um 2-grupo segue do teorema (III.2.5) que $U(\mathbb{Z}\,(H \times G))$ não é nilpotente, logo U(R G) também não é nilpotente.

A recíproca é trivial. □

Em geral, se R é um anel de característica 0 e G um grupo, U(R G) nilpotente implica $U(\mathbb{Z}\,G)$ nilpotente e necessàriamente G é abeliano ou um 2-grupo Hamiltoniano.

Para complementar a informação dada pelo teorema (III.2.5) vamos demonstar ainda:

(III.1.8) Proposição - Seja R um domínio de integridade, de característica 0 e G um grupo finito. Se U(R G) é periódico, então G é um 2-grupo Hamiltoniano.

Demonstração

Mostraremos inicialmente que dados $\alpha,\beta \in R\,G$ se $\alpha\beta = 0$, então, $\beta\alpha = 0$. De fato, suponhamos que $\beta\alpha \neq 0$ e seja $u = 1 + \beta\alpha$. Como $(\beta\alpha)^2 = 0$, $u \in U(R\,G)$ e $u^{-1} = 1 - \beta\alpha$.

Ainda, é fácil ver que $(1 + \beta\alpha)^n = 1 + n\,\beta\alpha \neq 1$ para todo inteiro positivo n, o que é uma contradição pois estamos supondo que U(R G) é periódico . Logo $\beta\alpha = 0$.

Mostraremos agora que todo subgrupo cíclico de G deve ser normal o que provará que G é Hamiltoniano.

De fato, seja $a \in G$ de ordem n e $g \in G$ arbitrário. Definimos:

$\alpha = g(1 - a)$ $\qquad$ $\beta = 1 + a + \ldots + a^{n-1}$

então $\alpha\beta = 0$ e do lema anterior $\beta\alpha = 0$. Logo:

$g + ag + \ldots + a^{n-1}g = ga + aga + \ldots + a^{n-1}ga$.

Para algum r deve ser $ga = a^r g$, logo $gag^{-1} = a^r$.

Finalmente se G não for um 2-grupo, então G contem algum elemento de ordem prima $p > 2$ e, sendo G Hamiltoniano contém elementos de ordem 4 logo também contem elementos de ordem 4p.

É fácil demonstrar que se G é abeliano, finito, então

toda unidade de ordem finita de $\mathbb{Z}G$ é trivial (Higman|12|, teorema 3 ou Berman|2|, Corolário 2). Desta observação e do teorema (III.1.1) segue que se G é um grupo que contém algum elemento de ordem diferente de 2, 3, 4 ou 6, então $U(\mathbb{Z}G)$ contém elementos de ordem infinita.

Como $U(RG) \supset U(\mathbb{Z}G)$, se G contivesse algum elemento de ordem 4p, $U(RG)$ não seria periódico. □

Podemos enunciar finalmente:

(III.1,9) Teorema - Seja G um grupo finito não abeliano. Então, as seguintes afirmações são equivalentes:

(i) $U(\mathbb{Z}G)$ é nilpotente.

(ii) $U(\mathbb{Z}G)$ é periódico.

(iii) $U(\mathbb{Z}G) \simeq \{\pm 1\} \times G$

(iv) G é um 2-grupo Hamiltoniano.

Demonstração

Óbviamente (iv) $\Longleftrightarrow$ (iii), do teorema (III.1.1)

(iii) $\Longrightarrow$ (ii) trivialmente.

(iv) $\Longrightarrow$ (i) como já foi observado logo após o teorema (III.1.1).

Do teorema (III.1.6), (i) $\Longrightarrow$ (iv).

Finalmente, da proposição (III.1.8), (ii) $\Longrightarrow$ (iv). □

CAPÍTULO IV

ANÉIS DE GRUPO SÔBRE INTEIROS P-ÁDICOS

IV.1. A CLASSE DE NILPOTÊNCIA DE $U(J_p n\ G)$

Temos demonstrado no capítulo II que se G é um p-grupo finito, o grupo das unidades de $J_p n\ G$ é nilpotente. Para estudar unidades de anéis de grupos sôbre os inteiros p-ádicos precisaremos dar uma limitação inferior para a classe de nilpotência de $U(J_p n\ G)$. Tal é o objetivo desta seção.

(IV.1.1) Lema - Seja G um p-grupo finito, não abeliano e $n = 2m > 0$ um inteiro. Então a classe de nilpotência de $U(J_p n\ G)$ é maior que $m/2$.

Demonstração

Faremos a demonstração em vários passos.

1º Passo - Existem elementos $a, b \in G$ tais que $ab^p = b^p a$ e $ab^i \neq b^i a$ para todo inteiro i, $1 \leq i < p$.

Demonstração do 1º Passo - Como G não é abeliano, existem elementos $a, c \in G$ tais que $ac \neq ca$. O conjunto:

$$E = \{x \in \mathbb{Z} \mid ac^x = c^x a\}$$

é um subgrupo de $\mathbb{Z}$ e $E \neq (0)$ pois $o(c) \in E$. Como $o(c)$ é uma potência de p, o gerador positivo de E deve ser da forma p^r. Agora basta tornar $b = c^{p^{r-1}}$.

Daqui em diante, a e b indicarão sempre os elementos acima escolhidos.

2º Passo - Definimos

$$(a - b)^{(1)} = ab - ba$$
$$(a - b)^{(k)} = (a - b)^{(k-1)} b - b(a - b)^{(k-1)}$$

Então:

(i) $(a - b)^{(k)} = a\,b^k - \binom{k}{1} ba\,b^{k-1} + \binom{k}{2} b^2\,a\,b^{k-2} + \ldots + (-1)^k\,b^k a$

(ii) $(a - b)^{(k)}$ pode-se escrever na forma $(a - b)^{(k)} = p^e \delta$

onde $\delta \in J_p nG$ e $\delta \notin p.J_p nG$ e $e<k$.

Demonstração do 2º passo

(i) Resulta de um argumento de indução.

Se $k = 1$ temos $(a - b)^{(1)} = ab - ba$.

Suponhamos então que (i) vale para k e calculemos:

$$(a - b)^{k+1} = (a - b)^{(k)} b - b(a - b)^{(k)} =$$

$$= a\,b^{k+1} - (\binom{k}{1} + 1)\; bab^{k-1} + (\binom{k}{2} + \binom{k}{1}) b^2 ab^{k-2} + \ldots + (-1)^{k+1} b^{k+1} a =$$

$$= ab^{k+1} - \binom{k+1}{1}\; bab^{k-1} + \binom{k+1}{2} b^2 a\, b^{k-2} + \ldots + (-1)^{k+1} b^{k+1}\, a.$$

Para provar (ii) observamos inicialmente que :

$b^r\, a\, b^{k-r} = b^s\, a\, b^{k-s}$ se e sòmente se $r - s \equiv 0 \pmod p$.

Assim ter-se-á que:

(1) $$(a-b)^{(k)} = x_o ab^k + x_1 bab^{k-1} + x_2 b^2 ab^{k-2} + \ldots + x_{p-1} b^{p-1} ab^{k-p+1}$$

com $x_s = \sum_{i \geq 0} (-1)^{s+ip} \binom{k}{s+ip}$ onde a soma se estende sôbre todos os inteiros $i \geq 0$ tais que $s + ip \leq k$. Tal como na proposição (III.2.1) segue que não pode ser $x_s = 0$ para todo s, $0 \leq s \leq p - 1$.

Seja agora p^e a maior potência de p que divide todos os coeficientes x_s, $0 \leq s \leq p - 1$. Então:

(2) $$(a - b)^{(k)} = p^e \delta \quad \text{onde } \delta \notin p.J_p n\ G.$$

Ainda, como $|x_s| < \sum_{i=0}^{k} \binom{k}{i} = 2^k \leq p^k$

segue que $e < p$.

<u>3º Passo</u> - Seja $\alpha = 1 - p^m a$, $\beta = 1 - pb$. Definimos:

$$\alpha_1 = |\alpha^{-1}, \beta^{-1}| = \alpha^{-1}\, \beta^{-1} \alpha\beta \quad \text{e} \quad \alpha_k = |\alpha_{k-1}^{-1}, \beta^{-1}|$$

(tomamos comutadores de inversos de elementos apenas para facilitar os cálculos). Então:

(3) $$\alpha_k = 1 + (-1)^{k+1} p^{m+k} \left(1 + \sum_{h=1}^{2m-1} x_h\, p^h\, b^h\right)(a-b)^{(k)}$$

com $x_h \in J_{p^n}$, $1 \leq h \leq m - k - 1$.

Demonstração do 3º passo

Faremos indução em k. Se k = 1 temos:

$$\alpha_1 = 1 + \alpha^{-1}\, \beta^{-1}(\alpha\beta-\beta\alpha) = 1 + p^{m+1}\, \alpha^{-1}\, \beta^{-1}(ab - ba)$$

Claramente, $\alpha^{-1} = 1 + p^m a$ (pois $(1-p^m a)(1+p^m a) = 1$) e temos que $p^{m+1}\, \alpha^{-1} = p^{m+1}$ logo $\alpha_1 = 1 + p^{m+1}\, \beta^{-1}(a - b)^{(1)}$.

Ainda $\beta^{-1} = 1 + pb + p^2b^2 + \ldots + p^{2m-1}\, b^{2m-1}$ é da forma requerida.

Suponhamos agora o resultado válido para α_k. Vamos calcular α_{k+1} .

Notaremos : $$a_k = (-1)^{k+1} \left(1 + \sum_{h=1}^{2m-1} x_h\, p^h\, b^h\right)(a - b)^{(k)}$$

Assim $\alpha_k = 1 + p^{m+k}\, a_k$ e $\alpha_k^{-1} = 1 - p^{m+k}\, a_k$

Agora:

(4) $$\alpha_{k+1} = 1 + \alpha_k^{-1}\, \beta^{-1}(\alpha_k\beta - \beta\alpha_k) = 1 - p^{m+k+1}\, \alpha_k^{-1}\, \beta^{-1}(a_k\, b - b a_k)$$

onde:

$$a_k b - b a_k = (-1)^{k+1} \left(1 + \sum_{h=1}^{2m-1} x_h\, p^h\, b^h\right)(a - b)^{(k+1)}$$

e $p^{m+k+1}\,\alpha_k^{-1} = p^{m+k+1}$.

Substituindo em (4) vem:

$$(5)\quad \alpha_{k+1} = 1+(-1)^{k+2}\, p^{m+k+1}\, \beta^{-1}\Big(1 + \sum_{h=1}^{2m-1} x_h\, p^h\, b^h\Big)\, (a-b)^{(k+1)}$$

onde $\beta^{-1}\Big(1 + \sum_{h=1}^{2m-1} x_h\, p^h\, b^h\Big)$ também pode-se escrever na forma:

$$\Big(1 + \sum_{h=1}^{2m-1} y_h\, p^h\, b^h\Big)$$

com $y_h \in J_p n$, e fica assim demonstrado (3).

4º Passo - Se $k < m/2$ então $\alpha_k \neq 1$.

Demonstração do 4º Passo -

Da fórmula (3) segue que $\alpha_k = 1$ se e sòmente se:

$$p^{m+k}\Big(1 + \sum_{h=1}^{2m-1} x_h\, p^h\, b^h\Big)(a-b)^{(k)} = 0.$$

Ainda, da proposição (II.1.2): $1 + \sum_{h=1}^{2m-1} x_h p^h b^h \in U(J_p n\, G)$

logo $\alpha_k = 1$ se e só se $p^{m+k}(a-b)^{(k)} = 0$ e da parte (ii) do 2º passo temos que $p^{m+k}(a-b)^{(k)} = p^{m+k+e}\,\delta$ onde $\delta \notin p.J_p nG$.

Assim $p^{m+k+e}\,\delta = 0$ se e só se $m + k + e \geq 2m$. Ainda,

para $k < \frac{m}{2}$ temos $m + k + e < m + 2k \leq 2m$.

Temos exibido assim comutadores de ordem k diferentes de 1, quando $k < m/2$; logo, a classe de nilpotência de $U(J_p n\ G)$ é maior que $m/2$. □

IV.2. - AS UNIDADES DE $\mathbb{Z}_p\ G$

Para demonstrar o resultado principal desta seção usaremos a técnica dos limites inversos. Para isso consideraremos o anel dos inteiros p-ádicos definido por $\mathbb{Z}_p = \varprojlim J_p n$.

Em geral, se $\{A_\alpha\}$ é um sistema projetivo de anéis comutativos e $A = \varprojlim A_\alpha$ é o seu limite projetivo é muito fácil mostrar que, para todo grupo finito G tem-se que $AG = \varprojlim A_\alpha G$ e que $U(AG) = \varprojlim U(A_\alpha G)$ (a demonstração esta feita por exemplo no trabalho de Raggi Cárdenas|22|).

Ainda, os morfismos que tornam $\{A_\alpha G\}$ e $\{U_\alpha G\}$ sistemas projetivos são os induzidos em forma natural pelos morfismos do sistema A_α, como foi indicado na introdução e como foi feito no lema(II.1.1) para os morfismos $J_p n \to J_p m$.

(IV.2.1) Teorema - Seja p um inteiro primo, $\mathbb{Z}_p = \varprojlim J_p n$ o anel dos inteiros p-ádicos e G um grupo finito. Então $U(\mathbb{Z}_p\ G)$ é nilpotente se e sòmente se G é abeliano.

Demonstração -

Suponhamos que $U(\mathbb{Z}_p\ G)$ é nilpotente. Mostraremos que para todo primo q o q-subgrupo de Sylow de G é abeliano, de onde / sendo G nilpotente segue imediatamente a tese.

De fato, temos mostrado no lema (II.1.1) que os morfismos $\phi_{mn}: J_p n\ G \to J_p m\ G$ dão, por restrição, epimorfismos dos respectivos grupos de unidades, logo os morfismos

$$\phi_n : U(\mathbb{Z}_p\ G) \longrightarrow U(J_p n\ G)$$

também são epimorfismos.

Então a nilpotência de $U(\mathbb{Z}_p\ G)$ implica que todos os / grupos $U(J_p n\ G)$ são nilpotentes e do teorema(II.2.3) segue que / para todo primo $q \neq p$ o q-subgrupo de Sylow de G é abeliano.

Finalmente, a classe de nilpotência de cada grupo / $U(J_p n\ G)$ está limitada superiormente pela classe de nilpotência de $U(\mathbb{Z}_p\ G)$. Se o p-subgrupo de Sylow de G não fosse comutativo ter-se-ia uma contradição com o lema (IV.1.1). □

B I B L I O G R A F I A

1. Bateman, J.M. and Coleman, D.B. - Group Algebras with nilpotent Unit Groups. Proc. Amer. Math. Soc. 19, 2, (1968) 448-449.

2. Berman, S.D. - On the equation $X^m = 1$ in an integral group ring. Ukrain Mat Z 7, (1955) 253 - 261.

3. Battacharya, P.B and Jain, S.K. - A note on the Adjoint Group of a Ring. Archiv. der Math. 21 (1970) 366 - 368.

4. Bovdi, A.A. - The Periodic Normal Divisors of the multiplicative Group of a Group Ring II-Sibirsk. Mat. Z. 11, 3 (1970) 492- 511

5. Cohn, J.A. and Livingstone, D. - On the structure of Group Algebras I . Can. J. of Math. 17, 4 (1965) 583 - 593.

6. Coleman, D.B. - Idempotentes in Group Rings - Proc. Amer. Math. Soc. 17, 4, (1966) 962

7. Coleman, D.B. - On the modular group ring of a p-group - Proc. Amer. Math. Soc. 15, 4 (1964) 511-514.

8. Connell. I.G. - On the group ring - Can, J. of Math. 15 (1963) 650 - 685.

9. Curtis, C.and Reiner I.- Representation theory of finite Groups and Associative Algebras, Interscience, New York, 1962.

10. Hall, M. - The theory of Group - Macmillan, New York (1959)

11. Herstein, I. and Small, L. - Nil ring satisfying certain chain conditions: an addendum Can.J. of Math, 18(1966) 300 - 302.

12. Higman, G. - The units of Group Rings - Proc. London Math.Soc. 2,46,(1940) 231- 248.

13. Hua, L.K. - On the multiplicative group of a field. Acad.Sinica Science Rec. 3(1950) 1-6.

14. Hughes, I. and Pearson, K.R. - The group of units of the integral group ring $\mathbb{Z} S_3$. Can.Math. Bull. 15,4(1972) 529-534.

15. Khripta, I.I. - The nilpotence of the multiplicative group of a group ring Mat.Zametki 11(1972)191-200

16. Motose K and Tominaga M. Group rings with nilpotent unit groups Math. J. Okayama Univ.14(1969)43 - 46.

17. Newman, M. - Integral Matrices, Academic Press, New York,1972

18. Passman, D.S. - Infinite Group Rings Marcel Dekker, New York, 1972.

19. Plotkin, B.I. - General theory of Groups - J.of Soviet Math - 1, 5 (1973) 527 - 548.

20. Polcino Milies, C. - Sobre as unidades de Anéis de Grupos - Dissertação de Mestrado, IME-USP-1972

21. Polcino, Milies, C. - On the nilpotency of the group of units / of group rings - Anais Acad. Brasileira de Ciências . A aparecer.

22. Raggi, Cardenas, F.F. - Las unidades em anillos de grupos con coeficientes en $K_p n$, $\mathbb{Z}_p n$ y $\hat{\mathbb{Z}}_p$. An. Inst.Mat.Univ.Nac.Aut. Mexico 10(1970) 29 - 65.

23. Reiner, I. - A survey of integral representation theory - Bull. Amer.Math.Soc.76(1970) 159-227.

24. Ribemboim, P. - Rings and Modules - Interscience, New York, 1969

25. Scott, W.R. - On the multiplicative Group of a Divison Ring - Proc. Amer. Math.Soc.8(1957)303-305.

26. Sehgal, S.K. - On the isomorphism of integral Group Rings I. Can. J. Math. 21(1969)410-413.

27. Takahashi, S. - Some properties of the group ring over rational integers of a finite group. Notices Amer.Math.Soc.12(1965)463.

ABSTRACT

J.M.Bateman and D.B. Coleman |1| proved the following / result:

Theorem - Let G be a finite group and R a field. The group of / units of the group ring RG is nilpotent if and only if one of the following conditions holds:

(i) char R = 0 and G is abelian,

(ii) char R = p ≠ 0 and G is the direct product of a p-group and an abelian group.

In |16| K.Motose and H.Tominaga corrected a small gap in the proof of the theorem above and proved a similar result for / group rings RG where R is an artinian semisimple ring (which must be commutative for RG to be nilpotent).

The goal of this thesis is to study the nilpotency of the group of units of a group ring of a finite group G over an arbitrary commutative ring R.

We found that over rings of non-zero characteristic the theorem of Bateman and Coleman is generalized in a natural way. This is not the case over rings of 0 characteristic since there are group rings of non-commutative groups with nilpotent group / of units. We studied the case that we considered most interesting: the units of integral group rings.

Also in the final chapter we study the units of group

rings of finite groups over rings of p-adic integers.

Our main results are the following:

Theorem (II.2.3) - Let R be a commutative ring with unit element such that char R = p^n where p is a prime number and Let G be a finite group.

Then the group of units of the group ring RG is nilpotent if and only if G is the direct product of a p-group and an abelian group.

Theorem II.2.5. - Let R be a commutative ring with unit element such that char R = m $\neq$ 0 and let m de divisible by at least two different primes. Then U(R G) is nilpotent if and only if G is commutative.

Theorem III.1.6. - Let G be a finite group. Then U($\mathbb{Z}$ G) is nilpotent if and only if G is abelian or a Hamiltonian 2-group.

This result, together with proposition (III.2.7) and results of G.D. Higman |12| lead to the following.

Theorem III.1.9. - Let G be a non abelian finite group. Then the following statements are equivalent:

(i) U($\mathbb{Z}$ G) is nilpotent,

(ii) U($\mathbb{Z}$ G) is periodic,

(iii) U($\mathbb{Z}$ G) = {±1} x G (every unit in $\mathbb{Z}$ G is trivial),

(iv) G is a Hamiltonian 2-group.

Theorem (IV.2.1.) - Let p be a prime number and $\mathbb{Z}_p$ the ring of p-adic integers. Then $U(\mathbb{Z}_p G)$ is nilpotent if and only if G is commutative.

Finally, when we started our study of the units of integral group rings, the only example actually computed that we found was that of $U(\mathbb{Z} S_3)$ where S_3 stands for the symmetric group on three symbols; this is done in a paper due to I. Hughes and K.R. Pearson |14| . Thus we decided to study the units of the integral group ring of the dihedral group of eight elements. That is the content of chapter 1.