ANÉIS DE GRUPOS COM
GRUPOS DE UNIDADES SOLÚVEIS

Jairo Zacarias Gonçalves

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. Francisco Cesar Polcino Milies

Durante a elaboração deste trabalho, o autor recebeu
apoio financeiro do Conselho Nacional de Desenvolvimento
Científico e Tecnológico (CNPq).

São Paulo, julho de 1982

Ao

Ricardo

I N D I C E

INTRODUÇÃO	I
CAPÍTULO I - ANÉIS DE GRUPOS SOBRE OS INTEIROS p-ÁDICOS COM GRUPO DE UNIDADES SOLÚVEIS	1
I.1. - Anéis de grupos sobre os inteiros p-ádicos	1
CAPÍTULO II - ANÉIS DE GRUPOS SOBRE UM ANEL DE INTEIROS ALGÉBRICOS	14
II.1. - Anéis de grupo sobre os inteiros de um corpo de números algébricos totalmente real	14
II.2. - Anéis de grupo sobre os inteiros de um corpo de números algébricos que contém uma raiz complexa da unidade	25
CAPÍTULO III - SUBGRUPOS DE UNIDADES LIVRES EM ANÉIS DE GRUPOS	37
III.1. - O caso $p = 0$	37
III.2. - O caso $p > 0$	40
REFERÊNCIAS	47
ABSTRACT	51

INTRODUÇÃO

Seja RG o anel de grupo de um grupo G sobre um anel comutativo R , com unidade, e $U(RG)$ seu grupo de unidades.

Nos últimos anos várias propriedades algébricas do grupo das unidades $U(RG)$ foram estudadas no caso em que R é um corpo ou $\mathbb{Z}$, o anel dos inteiros, ou anéis contendo $\mathbb{Z}_{(p)}$, a localização de $\mathbb{Z}$ no ideal primo (p) .

Em (1), Bateman e Coleman caracterizam as álgebras de grupo KG , de um grupo finito G sobre um corpo K , cujo grupo de unidades é nilpotente. Este resultado foi estendido a grupos arbitrários por Khripta (6), (7) e Fisher, Parmenter e Sehgal (3).

A nilpotência de $U(\mathbb{Z}G)$ foi estudada por Polcino Milies em (10), por Parmenter e Polcino Milies em (9), por Sehgal e Zassenhaus em (21); a propriedade FC por Sehgal e Zassenhaus em (20) e por Merklen e Polcino Milies em (8).

No caso em que R é $\mathbb{Z}$, S.K. Sehgal provou o seguinte:

Teorema (19): Suponhamos que $U(\mathbb{Z}G)$ é solúvel. Então:

(*) O conjunto dos elementos de torção T , de G , forma um subgrupo abeliano ou 2-Hamiltoniano, tal que todo subgrupo é normal em G .

Reciprocamente, se G é um grupo solúvel satisfazendo (*) e G/T é nilpotente, então $U(\mathbb{Z}G)$ é solúvel.

Por sugestão do Prof. C. Polcino Milies, estudamos a extensão desses resultados a anéis locais de característica zero e anéis de inteiros algébricos.

Assim, no Capítulo I provamos o seguinte resultado:

Teorema I 1.5 : Seja $R = \mathbb{Z}_{(p)}$ ou $R = \mathbb{Z}_{\hat{p}}$, o anel dos inteiros p -ádicos e suponhamos que $U(RG)$ seja solúvel. Então:

(*) O conjunto dos elementos de torção T de G forma um subgrupo abeliano, tal que todo subgrupo de T é normal em G .

Reciprocamente, se G é um grupo satisfazendo (*), $\mathbb{Q}_{\hat{p}}$ representa o completamento p -ádico do corpo dos números racionais e

(i) T é um p -subgrupo abeliano

(ii) G/T é nilpotente

então $U(\mathbb{Q}_{\hat{p}}G)$ é solúvel.

No Capítulo II estudamos a solubilidade de $U(RG)$ quando R é o anel de inteiros de um corpo de números algébricos, obtendo:

Teorema II 1.6: Seja R o anel de inteiros de um corpo de números algébricos totalmente real e G um grupo finito. Então, as seguintes condições são equivalentes:

(i) $U(RG)$ é solúvel

(ii) $U(RG)$ é nilpotente

(iii) $U(RG)$ é FC

(iv) $T(U(RG)) = \pm G$

(v) $T(U(RG))$ é um subgrupo de $U(RG)$

(vi) G é um grupo abeliano ou 2-Hamiltoniano.

Infelizmente, quando K não é totalmente real, não conseguimos uma caracterização completa. Porém foi possível demonstrar o seguinte:

Teorema II 2.5: Seja G um grupo de torção e suponhamos que R contém uma raiz complexa da unidade. Então $U(RG)$ é solúvel se e só se G é abeliano.

Os exemplos (II 2.6) e (II 2.7) e o nosso estudo, sugerem fortemente que $U(RG)$ é solúvel se e só se G é abeliano ou, então, G é 2-Hamiltoniano e R é o anel de inteiros de um corpo de números algébricos totalmente real. Em caso contrário, $U(RG)$ contém um subgrupo livre de posto 2. Entretanto, ainda não fomos capazes de provar esta conjectura.

Para certas classes de grupos infinitos é possível estender o teorema II 1.6 . Isto foi feito no

Teorema II 1.9: Seja G uma extensão de um grupo de torção T , por um grupo nilpotente livre de torção G/T , e K um corpo de números algébricos totalmente real, satisfazendo a seguinte condição: para todo $g \in T$ de ordem prima p , p é inerte em K . Então, são equivalentes:

- (i) $U(RG)$ é solúvel
- (ii) T é abeliano ou 2-Hamiltoniano tal que todo subgrupo de T é normal em G
- (iii) $T(U(RG)) = \pm T$
- (iv) $T(U(RG))$ é um subgrupo de $U(RG)$

Finalmente, no Capítulo III, investigamos condições necessárias e suficientes para que $U(KG)$ não contenha um subgrupo livre de posto 2, quando K é um corpo e G é um grupo.

Em (4), Pickel e Hartley provaram:

Teorema : Seja G um grupo finito. Então ocorre exatamente uma das seguintes situações:

- (i) G é abeliano (e portanto $U(ZG)$)
- (ii) G é um grupo 2-Hamiltoniano e $U(ZG) = \pm G$
- (iii) $U(ZG)$ contém um subgrupo livre de posto 2.

Este resultado tem como consequência os teoremas de Polcino Milies (10) e Sehgal (19), sobre a nilpotência e a solubilidade de $U(ZG)$, respectivamente, e propõe naturalmente a seguinte questão: caracterizar os grupos G para os quais $U(KG)$ não contém um subgrupo livre de posto 2. Quando da sua primeira visita a São Paulo, o Prof. S.K. Sehgal nos sugeriu o estudo deste problema.

Nossos resultados são os seguintes:

Teorema III 1.4 : Seja G um grupo finito e K um corpo de característica zero. Então $U(KG)$ não contém um subgrupo livre de posto 2 e só se G é abeliano.

Teorema III 2.3 : Seja G um grupo finito e K um corpo de característica $p > 0$. Então $U(KG)$ não contém um subgrupo livre de posto 2 e só se vale uma das seguintes condições:

- (i) K é algébrico sobre $GF(p)$, o corpo primo de K
- (ii) $S_p(G)$, o p -subgrupo de Sylow de G é normal em G e $G/S_p(G)$ é abeliano.

Muitas pessoas colaboraram com o autor durante a execução deste trabalho e não seria possível mencionar todas. Porém, muito especialmente, gostaríamos de citar:

Os Professores Walter Ferrer, Sônia Coelho e Arnaldo Mandel, por terem ouvido, pacientemente, algumas de nossas exposições, nos ajudando com críticas e sugestões.

O Professor S.K. Sehgal, por nos ter sugerido o problema do Capítulo III, e por ter feito chegar às nossas mãos o "pré-print" de (4), que foi fundamental para o desenvolvimento deste trabalho.

O Professor Hector Merklen, pela sua constante boa vontade em esclarecer nossas dúvidas, e oferecer valiosas sugestões, colaborando decisivamente na nossa formação matemática.

O Professor Cesar Polcino, orientador e amigo, professor de matemática e artes marciais, nossa profunda gratidão. A ele devemos a escolha desta área de especialização e a confiança de poder chegar ao fim deste trabalho. Oss...

J. Z. G.

CAPÍTULO I

ANÉIS DE GRUPOS SOBRE OS INTEIROS p -ÁDICOS COM GRUPO DE UNIDADES SOLÚVEIS

(1) ANÉIS DE GRUPOS SOBRE OS INTEIROS p -ÁDICOS

Notaremos por $\mathbb{Z}_{(p)}$ a localização de $\mathbb{Z}$ no ideal primo (p) , por $\mathbb{Z}_{\hat{p}}$ o anel dos inteiros p -ádicos, por $\mathbb{Q}_{\hat{p}}$ o corpo de frações de $\mathbb{Z}_{\hat{p}}$ e por $\mathbb{H}_{(p)}$ o seguinte subanel do anel dos quatérnios racionais $\mathbb{H}$:

$$\mathbb{H}_{(p)} = \{x + yi + zj + wk \in \mathbb{H} / x, y, z, w \in \mathbb{Z}_{(p)}\}$$

Definimos também a função $N: \mathbb{H}_{(p)} \rightarrow \mathbb{Z}_{(p)}$, como a restrição da norma de $\mathbb{H}$, i.e.,

$$N(x + yi + zj + wk) = x^2 + y^2 + z^2 + w^2.$$

Proposição 1.1 $U(\mathbb{H}_{(p)})$ não é solúvel.

Demonstração: Faremos a demonstração analisando uma série de situações possíveis. Observemos inicialmente que o centro de $\mathbb{H}_{(p)}$, que denotaremos por $Z(\mathbb{H}_{(p)})$, é precisamente $\mathbb{Z}_{(p)}$ e que valem as seguintes igualdades:

$$i^{-1} = -i, \quad j^{-1} = -j, \quad k^{-1} = -k, \quad i^j = j^{-1}ij = -i, \quad i^k = -i, \quad j^i = -j, \\ \text{etc.}$$

Afirmamos que $L = U(\mathbb{H}_{(p)}) / U(\mathbb{Z}_{(p)})$ não possui subgrupos normais abelianos não triviais.

Com efeito, seja $N \triangleleft L$, abeliano, $\bar{\alpha} \in N$ e $\gamma \in U(\mathbb{H}_{(p)})$. Então $\bar{\alpha} \alpha^\gamma = \overline{\alpha^\gamma} \bar{\alpha}$, isto é, $\alpha \alpha^\gamma = \alpha^\gamma \alpha \delta$, onde $\delta \in U(\mathbb{Z}_{(p)})$. Tomando normas de ambos os lados concluímos que $N(\delta) = 1$. Mas $\delta \in U(\mathbb{Z}_{(p)})$ e portanto $\delta = \pm 1$.

Mostramos assim que se $\gamma \in U(\mathbb{H}_{(p)})$ então:

$$(a) \quad \alpha \alpha^\gamma = \alpha^\gamma \alpha \quad \text{ou} \quad (b) \quad \alpha \alpha^\gamma = -\alpha^\gamma \alpha.$$

Seja $\alpha = x + yi + zj + wk$, $\bar{\alpha} \neq \bar{1}$, $\gamma = i$ e suponhamos que vale (a). Então, de $\alpha \alpha^i = \alpha^i \alpha$ concluímos que:

$$[(x+yi) + (zj+wk)] [(x+yi) - (zj+wk)] = [(x+yi) - (zj+wk)] [(x+yi) + (zj+wk)]$$

ou, que $(x + yi)(zj + wk) = (zj + wk)(x + yi)$ ou equivalentemente que:

$$\begin{cases} yw = 0 \\ yz = 0 \end{cases}$$

Se $y \neq 0$ então temos que $w=z=0$ e α possui, no máximo, dois elementos não nulos em seu suporte. Vamos considerar este caso mais adiante,

Admitamos que $y = 0$ e $w \neq 0$

Conjugando α por j temos:

$$(a1) \quad \alpha \alpha^j = \alpha^j \alpha \quad \text{ou}$$

$$(b1) \quad \alpha \alpha^j = -\alpha^j \alpha$$

Admitamos (a1). Então $(x+zj)wk = wk(x+zj)$ ou $wz = 0$.

Logo $z = 0$.

Admitamos (b1). Então $(x+zj)^2 = (wk)^2$ ou equivalentemente temos

$$\begin{cases} zx = 0 \\ x^2 + w^2 = z^2 \end{cases}$$

Como $w \neq 0$, da última equação concluímos que $z \neq 0$. Logo $x = 0$.

Portanto temos que α é de uma das seguintes formas:

$$(A) \alpha = x + wk \quad \text{ou} \quad (B) \alpha = zj + wk$$

Admitamos (A) e seja $\gamma = 1 + pi$. Então $\gamma^{-1} = \frac{1-pi}{1+p^2} \in U(IH_p)$.
E temos:

$$(a2) \alpha \alpha^\gamma = \alpha^\gamma \alpha \quad \text{ou} \quad (b2) \alpha \alpha^\gamma = -\alpha^\gamma \alpha.$$

Admitamos (a2). Então:

$$\alpha \alpha^\gamma = \frac{1}{1+p^2} \left[x^2(1+p^2) - w^2(1-p^2) + 2pw^2i + 2pwxj + 2wxk \right]$$

$$\alpha \alpha^\gamma = \frac{1}{1+p^2} \left[x^2(1+p^2) - w^2(1-p^2) - 2pw^2i + 2pxwj + 2wxk \right]$$

e da igualdade dos coeficientes de i concluímos que $4pw^2 = 0$ ou $w = 0$, uma contradição.

Admitamos (b2). Então, da igualdade dos coeficientes de 1 e k , respectivamente, concluímos que:

$$\begin{cases} 4wx = 0 \\ 2x^2(1+p^2) = 2w^2(1-p^2) \end{cases}$$

donde $x = 0$ e $w = 0$, uma contradição.

Admitamos (B) e seja $\gamma = 1 + pi$. Então $\gamma^{-1} = \frac{1 - pi}{1 + p^2} \in U(\mathbb{H}_p)$ e temos

$$(a2) \quad \alpha \alpha^\gamma = \alpha^\gamma \alpha \quad \text{ou}$$

$$(b2) \quad \alpha \alpha^\gamma = -\alpha^\gamma \alpha$$

Admitamos (a2). Então

$$\alpha^\gamma \alpha = \frac{1}{1 + p^2} \left[- (1 - p^2) (w^2 + z^2) + 2p (z^2 + w^2) i \right]$$

$$\alpha \alpha^\gamma = \frac{1}{1 + p^2} \left[- (w^2 + z^2) (1 - p^2) - 2p (z^2 + w^2) i \right]$$

e da igualdade dos coeficientes de i concluímos que $z^2 + w^2 = 0$ e portanto $z = w = 0$, uma contradição.

Admitamos (b2). Então, da igualdade dos coeficientes de 1, concluímos que $(1 - p^2) (w^2 + z^2) = 0$ e portanto $z = w = 0$, novamente uma contradição.

Por outro lado, dado $\alpha = x + yi + zj + wk$ admitamos (b) e tomemos $\gamma = i$. Então, de $\alpha \alpha^i = -\alpha^i \alpha$ concluímos que $(x + yi)^2 = (zj + wk)^2$ ou, equivalentemente, que

$$\begin{cases} xy = 0 \\ x^2 + z^2 + w^2 = y^2 \end{cases}$$

Se $y = 0$ então $\alpha = 0$ e temos uma contradição. Logo $y \neq 0$ e $x = 0$. Portanto $\alpha = yi + zj + wk$ e $z^2 + w^2 = y^2$ (C).

Agora, novamente, temos duas possibilidades:

$$(a1) \quad \alpha \alpha^j = \alpha^j \alpha \quad \text{ou}$$

$$(b1) \quad \alpha \alpha^j = -\alpha^j \alpha$$

Admitamos (a1). Então, de $\alpha \alpha^j = \alpha^j \alpha$ concluímos que $(zj)(yi + wk) = (yi + wk)(zj)$ ou, equivalentemente

$$\begin{cases} yz = 0 \\ wz = 0 \end{cases}$$

Logo $z = 0$, $w = \frac{+}{-} y$ e $\alpha = yi + wk$

Admitamos (b1). Então, de $\alpha \alpha^j = -\alpha^j \alpha$ concluímos que $(zj)^2 = (yi + wk)^2$ ou, equivalentemente

$$z^2 = y^2 + w^2$$

Combinando esta equação com (C) concluímos que $y^2 = y^2 + 2w^2$ ou $w = 0$. Logo $\alpha = yi + zj$.

Em qualquer um dos casos, recaímos numa situação análoga a (B). Basta agora repetir o procedimento

Proposição 1.2 Seja $K_8 = \langle a, b / a^4 = 1, a^2 = b^2, bab^3 = a^3 \rangle$ o grupo quaternio de ordem 8. Então $U(\mathbb{Z}_{(p)} K_8)$ não é solúvel.

Demonstração: Seja $\zeta: \mathbb{Q} K_8 \longrightarrow \mathbb{Q} \oplus \mathbb{Q} \oplus \mathbb{Q} \oplus \mathbb{Q} \oplus \mathbb{H}$ o isomorfismo de $\mathbb{Q}$ -álgebras tal que

$$\zeta(a) = (1, 1, -1, -1, i)$$

$$\zeta(b) = (1, -1, 1, -1, j)$$

Notaremos por $\omega : \mathbb{Z}_{(p)} K_8 \longrightarrow (\bigoplus_{i=1}^4 \mathbb{Z}_{(p)}) \oplus \mathbb{H}_{(p)}$

a restrição de $\tilde{\omega}$ e consideraremos dois casos separadamente:

(i) $p \neq 2$ Seja $u = x_0 + x_1 a + x_2 a^2 + x_3 a^3 + y_0 b + y_1 ab + y_2 a^2 b + y_3 a^3 b$

um elemento de $\mathbb{Z}_{(p)} K_8$. Então $\omega(u) = (a, b, c, d, \alpha + \beta i + \gamma j + \delta k)$

onde

$$x_0 + x_2 + x_1 + x_3 + y_0 + y_2 + y_1 + y_3 = a$$

$$x_0 + x_2 + x_1 + x_3 - (y_0 + y_2) - (y_1 + y_3) = b$$

$$x_0 + x_2 - (x_1 + x_3) + (y_0 + y_2) - (y_1 + y_3) = c$$

$$x_0 + x_2 - (x_1 + x_3) - (y_0 + y_2) + (y_1 + y_3) = d$$

$$x_0 - x_2 + (x_1 - x_3)i + (y_0 - y_2)j + (y_1 - y_3)k = \alpha + \beta i + \gamma j + \delta k$$

Afirmamos que ω é um isomorfismo. Para isto basta provar que ω é sobrejetivo.

De fato, seja $(a, b, c, d, \alpha + \beta i + \gamma j + \delta k) \in (\bigoplus_{i=1}^4 \mathbb{Z}_{(p)}) \oplus \mathbb{H}_{(p)}$.

Então podemos resolver o sistema de equações acima em x_i e y_i , $0 \leq i \leq 3$, encontrando

$$x_0 = \frac{a + b + c + d + 4\alpha}{8} \quad x_2 = \frac{a + b + c + d - 4\alpha}{8} \quad x_1 = \frac{a + b - c - d + 4\beta}{8}$$

$$x_3 = \frac{a + b - c - d - 4\beta}{8} \quad y_0 = \frac{a - b + c - d + 4\gamma}{8} \quad y_2 = \frac{a - b + c - d - 4\gamma}{8}$$

$$y_1 = \frac{a - b - c + d + 4\delta}{8} \quad y_3 = \frac{a - b - c + d - 4\delta}{8}.$$

Como pela Proposição 1.1 $U(H_{(p)})$ não é solúvel, segue que $\omega(U(\mathbb{Z}_{(p)} K_8))$ não é solúvel, pois se $U(\mathbb{Z}_{(p)} K_8)$ fosse solúvel, também teríamos a solubilidade de $U(H_{(p)})$, uma contradição.

(ii) $p = 2$. Neste caso

$$\omega: \mathbb{Z}_{(2)} K_8 \longrightarrow \left(\bigoplus_{i=1}^4 \mathbb{Z}_{(2)} \right) \oplus H_{(2)}$$

é um monomorfismo.

Seja π a projeção da soma direta sobre o último componente e coloquemos $H_2 = \{x + yi + zj + wk / x, y, z, w \in GF(2)\}$, onde $GF(2)$ representa o corpo com dois elementos.

Ainda, $\emptyset: H_{(2)} \longrightarrow H_2$ representará o epimorfismo induzido pela projeção natural $\mathbb{Z}_{(2)} \longrightarrow GF(2)$.

Temos, então, o seguinte diagrama comutativo, onde a linha de baixo é uma sequência exata:

$$\begin{array}{ccccccc} 1 + 2\mathbb{Z}_{(2)} K_8 & \hookrightarrow & U(\mathbb{Z}_{(2)} K_8) & & & & \\ \downarrow \pi \circ \omega & & \downarrow \pi \circ \omega & & & & \\ 1 \longrightarrow 1 + 2H_{(2)} & \hookrightarrow & U(H_{(2)}) & \xrightarrow{\emptyset} & U(H_2) & \longrightarrow & 1 \end{array}$$

De fato, observemos de início que se R é um anel noetheriano, local e A é uma R -álgebra finitamente gerada, então $J(R)A \subseteq J(A)$, onde $J(R)$ e $J(A)$ indicam os radicais de Jacobson de R e A , respectivamente (veja Reiner, I., (12 a), pg. 25). Como $J(\mathbb{Z}_{(2)}) = 2\mathbb{Z}_{(2)}$, temos que $2\mathbb{Z}_{(2)}K_8 \subseteq J(\mathbb{Z}_{(2)}K_8)$. Agora, a projeção natural $\mathbb{Z}_{(2)} \longrightarrow GF(2)$ induz um epimorfismo $\tau: \mathbb{Z}_{(2)}K_8 \longrightarrow GF(2)K_8$, e $\alpha \in \mathbb{Z}_{(2)}K_8$ pertence ao Kernel de τ se e só se $\alpha \in 2\mathbb{Z}_{(2)}K_8 \subseteq J(\mathbb{Z}_{(2)}K_8)$. Logo τ induz um epimorfismo de grupo $\tau: U(\mathbb{Z}_{(2)}K_8) \longrightarrow U(GF(2)K_8)$ cujo Kernel é $1 + 2\mathbb{Z}_{(2)}K_8$. As verificações restantes são triviais.

Se assumirmos que $U(\mathbb{Z}_{(2)}K_8)$ é solúvel, segue que $1 + 2\mathbb{Z}_{(2)}K_8$ é solúvel e, portanto, $1 + 2\mathbb{H}_{(2)}$ é também solúvel. Por outro lado, como $|U(\mathbb{H}_2)| < 2^4$, sabemos que $U(\mathbb{H}_2)$ é solúvel. Finalmente, a exatidão da linha de baixo implica que $U(\mathbb{H}_{(2)})$ é solúvel, em contradição com a Proposição 1.1.

Proposição 1.3 Seja P um p -grupo abeliano finito. Para todo subgrupo H de P coloquemos $e_H = \frac{1}{|H|} \sum_{h \in H} h$. Então todo impodente de $\mathbb{Q}_{\hat{p}}^P$ é uma $\mathbb{Q}_{\hat{p}}$ -combinação linear dos idempotentes do conjunto $A = \{e_H / P/H \text{ é cíclico}\}$.

Demonstração: É suficiente provar que todo idempotente primitivo de $\mathbb{Q}_{\hat{p}}P$ é uma combinação linear dos elementos de A . Seja θ uma raiz primitiva p^a -ésima da unidade. Por (5), Exerc. 1, pg. 84, $[\mathbb{Q}_{\hat{p}}(\theta) : \mathbb{Q}_{\hat{p}}] = [\mathbb{Q}(\theta) : \mathbb{Q}]$ e por (19), Proposição II 2.6, o número de cópias de $\mathbb{Q}_{\hat{p}}(\theta)$ na decomposição de $\mathbb{Q}_{\hat{p}}P$ é igual ao número de fatores cíclicos de G de ordem p^a . Logo, o cardinal de A é igual ao número total de idempotentes primitivos de $\mathbb{Q}_{\hat{p}}P$; portanto, é suficiente mostrar que este conjunto é linearmente independente sobre $\mathbb{Q}_{\hat{p}}$. Mas (19), Proposição VI 1.6 mostra que A é linearmente independente sobre $\mathbb{Q}$. Como $\mathbb{Q}_{\hat{p}}P = \mathbb{Q}_{\hat{p}} \bigotimes_{\mathbb{Q}} \mathbb{Q}P$, segue que A também é linearmente independente sobre $\mathbb{Q}_{\hat{p}}$.

Lema 1.4 Seja G uma extensão de um grupo de torção T por um grupo nilpotente livre de torção. Se G é finitamente gerado, então T é finito.

Demonstração: Veja (19), Teorema VI 4.8.

Estamos em condições de provar o resultado principal deste capítulo.

Teorema 1.5 : Seja $R = \mathbb{Z}_{(p)}$ ou $\mathbb{Z}_{\hat{p}}$ e suponhamos que $U(RG)$ seja solúvel. Então vale a seguinte condição:

(*) O conjunto dos elementos de torção T de G forma um grupo abeliano, tal que todo subgrupo de T é normal em G .

Reciprocamente, se G é um grupo satisfazendo

(*) e

(i) T é um p -subgrupo abeliano

(ii) G/T é nilpotente

então $U(\mathbb{Q}_{\hat{p}}G)$ é solúvel.

Demonstração:

Necessidade: Como a solubilidade de $U(\mathbb{Z}_{(p)}G)$ implica a solubilidade de $U(\mathbb{Z}G)$ segue do resultado de Sehgal, (19), Teorema VI 4.8, que T é abeliano ou um 2-grupo Hamiltoniano. É bem conhecido que se T é não abeliano, então $T = \text{Ex}K_8$, o produto direto de um 2-grupo abeliano elementar pelo grupo quaternio de ordem 8. Portanto $U(\mathbb{Z}_{(p)}K_8)$ é solúvel, contrariando a Proposição 1.2

Suficiência: Seja $G \supset G^{(1)} \supset G^{(2)} \supset \dots \supset G^{(n-1)} \supset G^{(n)} = \{1\}$ a série dos comutadores de G . Afirmamos que $U(\mathbb{Q}_{\hat{p}}G)$ é solúvel com $U(\mathbb{Q}_{\hat{p}}G)^{(n+1)} = \{1\}$.

Podemos supor que G é finitamente gerado. Nestas circunstâncias, pelo Lema 1.4 T é finito. Logo

$$\mathbb{Q}_{\hat{p}}T = \bigoplus F_i$$

uma soma direta de corpos. A Proposição 1.3 juntamente com (19), Lema VI 3.22 implicam que todo $u \in U(\mathbb{Q}_{\hat{p}}G)$ pode ser escrito como

$$u = \sum f_i g_i$$

Novamente pela Proposição 1.3, os idempotentes de $\mathbb{Q}_{\hat{p}}T$ são centrais em $\mathbb{Q}_{\hat{p}}G$ e portanto, para todo $g \in G$ temos que

$$F_i^g \subseteq F_i$$

Logo

$$U(\mathbb{Q}_{\hat{p}}G)^{(1)} \subseteq \sum F_i G^{(1)}$$

Comutações repetidas implicam que

$$U(\mathbb{Q}_{\hat{p}}G)^{(n)} \subseteq \sum F_i, \quad U(\mathbb{Q}_{\hat{p}}G)^{(n+1)} = \{1\}.$$

Corolário 1.6: Seja G um grupo tal que T forma um subgrupo p -abeliano e G/T é nilpotente. Então $U(\mathbb{Z}_{\hat{p}}G)$ é solúvel se e só se $\mathbb{Z}_{\hat{p}}G$ não possui elementos nilpotentes não triviais.

Demonstração:

Necessidade: Sem perda de generalidade, podemos assumir que G é finitamente gerado e, como na prova de suficiência do Teorema 1.5 que P é finito.

Afirmamos que todo idempotente de $\mathbb{Q}_{\hat{p}}P$ é central em $\mathbb{Q}_{\hat{p}}G$. De fato, se existe algum idempotente de $\mathbb{Q}_{\hat{p}}P$ que não é central em $\mathbb{Q}_{\hat{p}}G$, então por (19), Lema VI 3.12, $U(\mathbb{Q}_{\hat{p}}G)$ contém uma cópia isomorfa de $GL(m, F)$, onde $m > 1$ e F é um corpo, que é uma extensão de $\mathbb{Q}_{\hat{p}}$. Mas pelo Teorema 1.5 $U(\mathbb{Q}_{\hat{p}}G)$ é solúvel, uma contradição pois $GL(m, F)$ não é solúvel, (15), Exercício 8.15.

Agora, podemos escrever $\mathbb{Q}_{\hat{p}}G$ na forma

$$\mathbb{Q}_{\hat{p}}G = (\mathbb{Q}_{\hat{p}}P) (G/P, \rho, \sigma), \text{ i.e.,}$$

como produto cruzado de G/P sobre $\mathbb{Q}_{\hat{p}}P$ com um sistema de fatores ρ e automorfismos σ .

Em (19), Prop. VI 1.8, temos uma condição suficiente para que o produto cruzado de um grupo ordenado sobre um anel não possua elementos nilpotentes não triviais. Portanto, basta mostrar que para todo $a \in \mathbb{Q}_{\hat{p}}P$ e $x = \bar{g} \in G/P$ tal que $a \cdot \sigma_x(a) = 0$, então $a = 0$.

Mas $\mathbb{Q}_{\hat{p}}^P = F_1 \oplus \dots \oplus F_k$, é uma soma direta de corpos, e como todo idempotente de $\mathbb{Q}_{\hat{p}}^P$ é central em $\mathbb{Q}_{\hat{p}}^G$, segue que $\sigma_x(F_i) \subseteq F_i$. Portanto $a \cdot \sigma_x(a) = 0$ implica $a = 0$, e $\mathbb{Q}_{\hat{p}}^G$ não tem elementos nilpotentes não triviais.

Suficiência: Se $\mathbb{Z}_{\hat{p}}^G$ não tem elementos nilpotentes não triviais, então o mesmo acontece com $\mathbb{Q}_{\hat{p}}^G$ e podemos imitar a prova da suficiência do Teorema 1.5.

C A P Í T U L O I I

ANÉIS DE GRUPOS SOBRE UM ANEL DE INTEIROS ALGÉBRICOS

1. Anéis de grupo sobre os inteiros de um corpo de números algébricos totalmente real

No que segue, R representará o anel de inteiros de um corpo de números algébricos K , totalmente real e $\mathbb{H}_R$ o seguinte subanel do anel dos quatêrnios reais $\mathbb{H}$,

$$\mathbb{H}_R = \{x_1 + x_2 i + x_3 j + x_4 k \mid x_1, x_2, x_3, x_4 \in R\}$$

Se $N(x_1 + x_2 i + x_3 j + x_4 k) = \sum_{m=1}^4 x_m^2$, podemos provar:

Proposição 1.1. O conjunto das unidades de torção de $U(\mathbb{H}_R)$ é $T(U(\mathbb{H}_R)) = \{\pm 1, \pm i, \pm j, \pm k\} = K_8$.

Demonstração: Seja $\alpha = x_1 + x_2 i + x_3 j + x_4 k \in T(U(\mathbb{H}_R))$ tal que $\alpha^n = 1$. Então $N(\alpha)^n = 1$ e portanto $N(\alpha) = x_1^2 + x_2^2 + x_3^2 + x_4^2 = 1$. Afirmamos que esta equação só tem soluções triviais.

De fato, suponhamos que x_1 , por exemplo, seja diferente de 0 e ± 1 . Então, por (12), Lema 10.10, algum conjugado de x_1 por um $\mathbb{Q}$ -monomorfismo σ , de K , tem valor absoluto

maior do que 1. Obviamente $\alpha_1 = (x_1) + \sigma(x_2)i + \sigma(x_3)j + \sigma(x_4)k$ é tal que $\alpha_1^n = 1$, logo $1 = \sigma(x_1)^2 + \sigma(x_2)^2 + \sigma(x_3)^2 + \sigma(x_4)^2 = |\sigma(x_1)|^2 + |\sigma(x_2)|^2 + |\sigma(x_3)|^2 + |\sigma(x_4)|^2 \gg \sigma(x_1)^2 > 1$, uma contradição.

Seja L um corpo de números algébricos, A uma L -álgebra central simples e seja P um primo de L . Notaremos por L_P o completamento P -ádico de L . Então $A_P = L_P \otimes_L A$ é o completamento P -ádico de A . Como A_P é uma L_P -álgebra central simples, ela é da forma $A_P \cong M_r(S)$, onde S é um anel com divisão de índice m_P sobre o centro L_P .

Definição: Dizemos que A se ramifica em P , ou que P é ramificado em A se $m_P > 1$.

Definição: Uma L -álgebra central simples A é chamada uma álgebra de quatérnios totalmente definida se todo primo infinito de L é ramificado em A e se, ademais, $A_P \cong \mathbb{H}$, a álgebra dos quatérnios reais.

Seja $\mathcal{O}$ uma ordem de uma álgebra de quatérnios A , totalmente definida, sobre um corpo de números algébricos K totalmente real, e seja $\mathcal{O}^*$ o grupo das unidades de $\mathcal{O}$. Seja ainda W o grupo das unidades de $\mathcal{O}$ de norma reduzida 1. Nestas condições temos:

Teorema 1.2 (a) $(\theta^* : W \times U(R)) = 4$, se W é cíclico, gerado por s_{2n} de ordem $2n$ e se existem duas unidades de θ , e_1, e_2 , cujas normas reduzidas não sejam quadrados e verificando:

$$(a1) \text{ se } n = 1, \quad e_1 e_2 = -e_2 e_1$$

$$(a2) \text{ se } n \neq 1, \quad e_1 \in K(S_{2n}), \quad e_2 \cdot S_{2n} = S_{2n}^{-1} \cdot e_2$$

(b) $(\theta^* : W \times U(R)) = 2$, se não for 4, e se existir uma unidade $e_1 \in \theta$, cuja norma reduzida não seja um quadrado e

$$(b1) \text{ se } W \text{ é cíclico, gerado por } S_{2n}, \quad e_1 \in K(S_{2n}) \text{ e } e_1 S_{2n} = S_{2n}^{-1} e_1$$

$$(b2) \text{ se } W \text{ é dicíclico, } W = \langle S_{2n}, j \rangle, \text{ de ordem } 4n \text{ e } e_1 \in (1 + S_{2n})K^*$$

$$(b3) \text{ se } W = E_{48}, \text{ o grupo binário octaedral e } e_1 \in (1 + i)K^*$$

$$(c) \quad (\theta^* : W \times U(R)) = 1 \text{ em caso contrário.}$$

Demonstração: Ver (23), Teorema 6.

Proposição 1.3 Com as mesmas notações do início do capítulo II, $U(IH_R) = U(R)K_\theta$.

Demonstração: Vamos mostrar que o índice de $U(R) \times K_\theta$ em $U(IH_R)$ é igual a 1.

Suponhamos inicialmente que $\sqrt{2} \in R$ e que $(U(IH_R) : U(R) \times K_8) \neq 1$. Então, do Teorema 1.2 e da Proposição 1.1 segue que existe uma unidade $\varepsilon \in (1+i)K^*$ e $N(\varepsilon) \notin K^{*2}$. Logo $\varepsilon = (1+i)\gamma$, $\gamma \in K^*$ e $N(\varepsilon) = 2\gamma^2 = (\sqrt{2}\gamma)^2 \in K^{*2}$, uma contradição.

Por outro lado, se $\sqrt{2} \notin R$, consideremos a extensão $K(\sqrt{2})$ e o fecho inteiro S de $K(\sqrt{2})$ em R . Então, pela primeira parte

$(U(IH_S) : T(U(IH_S)) \times U(S)) = 1$ e portanto $U(IH_S) = T(U(IH_S)) \times U(S)$. Logo $U(IH_R) = U(IH_S) \cap U(IH_R) = (T(U(IH_S)) \times U(S)) \cap U(IH_R) = (K_8 \times U(S)) \cap U(IH_R) = K_8 \times U(R)$.

A seguir, estenderemos um conhecido resultado de G. Higman, (19), Proposição II 2.1.

Proposição 1.4 Seja $\langle c \rangle$, $c^2 = 1$, o grupo cíclico de ordem dois e seja G um grupo finito tal que $T(U(RG)) = \pm G$. Então $T(U(R\langle c \rangle \times G)) = \pm \langle c \rangle \times G$.

Demonstração: Como a função $\psi : R\langle c \rangle \longrightarrow R \oplus R$ definida por $\psi(\alpha + \beta c) = (\alpha + \beta, \alpha - \beta)$ é um monomorfismo,

a aplicação $\psi : (R\langle c \rangle)G \longrightarrow RG \oplus RG$

tal que $\psi(\sum (\alpha_i + \beta_i c) g_i) = (\sum (\alpha_i + \beta_i) g_i, \sum (\alpha_i - \beta_i) g_i)$ é também um monomorfismo, e se $\sum (\alpha_i + \beta_i c) g_i$ é uma unidade de torção, segue que existem i' e j' tais que:

$$\begin{cases} \alpha_i + \beta_i = \pm 1 & \text{se } i = i' \\ \alpha_i + \beta_i = 0 & \text{se } i \neq i' \end{cases} \quad \begin{cases} \alpha_j - \beta_j = \pm 1 & \text{se } j = j' \\ \alpha_j - \beta_j = 0 & \text{se } j \neq j' \end{cases}$$

Como $2 \nmid U(R)$ segue das equações acima $i' = j'$.
Portanto ou $\alpha_{i'} = \pm 1, \beta_{i'} = 0, \alpha_i = \beta_i = 0$ se $i \neq i'$ ou
 $\alpha_{i'} = 0, \beta_{i'} = \pm 1, \alpha_i = \beta_i = 0$ se $i \neq i'$. A nossa conclusão segue.

Proposição 1.5 Se G é um 2-grupo Hamiltoniano então $T(U(RG)) = \pm G$.

Demonstração: É suficiente observar que a Proposição 1.1 permite estender a prova conhecida de (19), Proposição II 2.2, concluindo que $T(U(RK_8)) = \pm G$. A conclusão segue então da Proposição 1.4.

Teorema 1.6 Seja G um grupo finito. Então as seguintes condições são equivalentes:

- (i) $U(RG)$ é solúvel
- (ii) $U(RG)$ é nilpotente
- (iii) $U(RG)$ é FC
- (iv) $T(U(RG)) = \pm G$
- (v) $T(U(RG))$ é um subgrupo de $U(RG)$
- (vi) G é um grupo abeliano ou um 2-grupo Hamiltoniano.

Demonstração: Vamos mostrar que cada uma das proposições (i), (ii), (iii), (iv) e (v) é equivalente a (vi). Temos que (19), Teorema VI 4.8, (19), Teorema VI 3.23, (19), Teorema VI 5.3 e (11), respectivamente, implicam que (i) $\Rightarrow$ (vi), (ii) $\Rightarrow$ (vi), (iii) $\Rightarrow$ (vi) e (v) $\Rightarrow$ (vi). Para provar a recíproca, consideremos dois casos:

(1) G é abeliano : aqui (19), Corolário II 1.2, mostra que (vi) $\Rightarrow$ (iv), que é a única implicação não trivial.

(2) G é 2-Hamiltoniano : então G é da forma $G = \text{ExK}_8$, o produto direto de um 2-grupo abeliano elementar pelo grupo quaternio de ordem oito. Temos portanto um monomorfismo

$$\psi: R(\text{ExK}_8) \longrightarrow \bigoplus_{i=1}^{2^{|E|}} \left(\bigoplus_{j=1}^4 R \right) \oplus \mathbb{H}_R$$

e portanto um monomorfismo de grupos

$$\psi: U(R(\text{ExK}_8)) \longrightarrow \prod_{i=1}^{2^{|E|}} \left(\left(\prod_{j=1}^4 U(R) \right) \times U(\mathbb{H}_R) \right) = \prod_{i=1}^{2^{|E|}} \left(\prod_{j=1}^4 (U(R) \times K_8) \right)$$

pela Proposição 1.3. Portanto (vi) $\Rightarrow$ (i), (vi) $\Rightarrow$ (ii), (vi) $\Rightarrow$ (iii). Finalmente a Proposição 1.5 nos dá que (vi) $\Rightarrow$ (iv).

Precisamos agora, para a demonstração do próximo teorema, das seguintes proposições sobre números algébricos:

Proposição 1.7 Seja L um corpo de números algébricos, A o anel de inteiros de L , $p \in \mathbb{Z}$ um primo iner-
te em L e r um elemento de $\mathbb{N} - \{0\}$. Então $\phi_{p^r}(X)$, o poli-
nômio ciclotômico de índice p^r , é irredutível sobre L .

Demonstração: Sabemos que $\phi_{p^r}(X) = (X^{p^r} - 1) / (X^{p^{r-1}} - 1) =$
 $X^{p^{r-1}(p-1)} + X^{p^{r-1}(p-2)} + \dots + X^{p^{r-1}} + 1.$

Assim, se θ é uma raiz primitiva da unidade de ordem p^r , será
suficiente provar que $(L(\theta) : L) = p^{r-1}(p-1).$

Coloquemos $p^{r-1}(p-1) = e$ e $\theta_1, \dots, \theta_e$ as
raizes primitivas p^r -ésimas da unidade. Como o termo constan-
te de $\phi_{p^r}(X+1)$ é p , temos:

$$\prod_{j=1}^e (1 - \theta_j) = p$$

Seja B o anel de inteiros de $L(\theta)$. Temos
evidentemente que $\theta_j \in B$ e também que $1 - \theta_j$ pertence ao ideal
 $B(1 - \theta_k)$ para todo j e k , pois $\theta_j = \theta_k^q$ e $1 - \theta_k^q = (1 - \theta_k)(1 + \theta_k + \dots + \theta_k^{q-1})$.
Assim, todos os ideais da forma $B(1 - \theta_k)$ são iguais. Portanto
 $Bp = B(1 - \theta_1)^e.$

Escrevamos agora $Bp = \prod_{i=1}^q Q_i^{e_i}$, a decomposição
de Bp em ideais primos de B . Os expoentes e_i são, então, to-
dos múltiplos de e . Mas $e \gg (L(\theta) : L) = \sum_{i=1}^q e_i f_i$ onde

$f_i = (B/Q_i : A/Q_i \wedge A)$. Desta desigualdade concluímos que $q = 1$,
 $e = e_1$, $f_i = 1$ e $(L(\theta) : L) = e$.

Proposição 1.8 Seja $m \in \mathbb{N} - \{0\}$ e L um corpo de números
 algébricos tal que, para todo primo racional $p \mid m$, tem-se que p é inerte em L . Então $\phi_m(X)$ é irredutível sobre L .

Demonstração: Vamos usar indução sobre m . Já sabemos
 que a proposição é verdadeira quando m é potência de um primo.

Seja $m = p^a n$ com p primo, $p \nmid n$. Então, se θ_{p^a} e θ_n são raízes primitivas da unidade de ordens p^a e n , respectivamente, temos $L(\theta_m) = L(\theta_{p^a})L(\theta_n)$. Afirmamos também que $L(\theta_{p^a}) \cap L(\theta_n) = L$.

De fato, para qualquer subcorpo L' tal que $L \subseteq L' \subseteq L(\theta_{p^a})$ o índice de ramificação de p em L' é igual a $(L' : L)$. Agora, em qualquer subcorpo L'' com $L \subseteq L'' \subseteq L(\theta_n)$, o primo p tem índice de ramificação 1 pois não é ramificado em L e nem em $L(\theta_n)$, (13), Teorema 10.7.0. Assim, L é o único subcorpo comum a $L(\theta_{p^a})$ e $L(\theta_n)$.

Da teoria de Galois vem que:

$$\begin{aligned} \text{Gal}(L(\theta_m)/L) &= \text{Gal}(L(\theta_m)/L(\theta_n)) \times \text{Gal}(L(\theta_m)/L(\theta_{p^a})) \cong \\ &\text{Gal}(L(\theta_{p^a})/L) \times \text{Gal}(L(\theta_n)/L). \end{aligned}$$

Pela hipótese de indução $|Gal\ L(\theta_m)/L| = \phi(p^a)\phi(n) = \phi(m)$.

Teorema 1.9: Seja G uma extensão de um grupo de torção T por um grupo nilpotente livre de torção G/T e seja K um corpo que satisfaz a seguinte propriedade: para todo elemento $g \in T$ de ordem prima p , o inteiro p é inerte em K . Então, as seguintes condições são equivalentes:

- (i) $U(RG)$ é solúvel
- (ii) T é abeliano ou um 2-grupo Hamiltoniano tal que todo subgrupo de T é normal em G .
- (iii) $T(U(RG)) = \pm T$
- (iv) $T(U(RG))$ é um subgrupo de $U(RG)$

Demonstração: (i) $\Rightarrow$ (ii). Como $U(RG)$ é solúvel, $U(\mathbb{Z}G)$ também é solúvel e basta aplicar o resultado de Sehgal, (19), Teorema VI 4.8.

(ii) $\Rightarrow$ (iii). Vamos considerar dois casos:

- (1) T é abeliano. Sem perda de generalidade podemos assumir que G é finitamente gerado e T é finito. Portanto, pela Proposição 1.8 e argumentando como na Proposição I 1.3, todo idempotente de KT é central em KG por ser uma K -combinação linear dos idempotentes do conjunto $\{\varepsilon_H / H = \frac{1}{|H|} \sum_{h \in H} h, H \text{ subgrupo de } T\}$. Por (19), Lema VI 3.22

temos que $U(RG) = U(RT)G$. Portanto, de (19), Corolário II 1.2 temos que $T(U(RG)) = T(U(RT)) = T(U(R))T = \pm T$.

(2) T é um 2-grupo Hamiltoniano. Podemos assumir, como anteriormente, que G é finitamente gerado e T é finito. Portanto, $T = E \times K_8$, o produto direto de um 2-grupo abeliano elementar E pelo grupo quaternio de ordem 8.

$$\text{Agora } KE = \underbrace{K \oplus K + \dots \oplus K}_{|E| \text{ vezes}}$$

e todo idempotente de KE é central em KG. Afirmamos que todo idempotente de KK_8 também é central em KG.

Em primeiro lugar, observemos que em virtude de K ser um subcorpo do corpo dos números reais, $\mathbb{H}_K$ é um anel com divisão.

Seja $x \in G \setminus T$. A função

$$\Psi : KK_8 \longrightarrow K \oplus K \oplus K \oplus K \oplus \mathbb{H}_K \text{ definida por:}$$

$$\Psi(a) = (1, 1, -1, -1, i)$$

$$\Psi(b) = (1, -1, 1, -1, j)$$

define um isomorfismo de K-álgebra; portanto, os idempotentes centrais de KK_8 são:

$$\Psi^{-1}(1, 0, 0, 0, 0) = e_1 = \frac{1}{8} (1 + a + a^2 + a^3 + b + ab + a^2b + a^3b)$$

$$\Psi^{-1}(0, 1, 0, 0, 0) = e_2 = \frac{1}{8} (1 + a + a^2 + a^3 - b - ab - a^2b - a^3b)$$

$$\Psi^{-1}(0,0,1,0,0) = e_3 = \frac{1}{8} (1 - a + a^2 - a^3 + b - ab + a^2b - a^3b)$$

$$\Psi^{-1}(0,0,0,1,0) = e_4 = \frac{1}{8} (1 - a + a^2 - a^3 - b + ab - a^2b + a^3b)$$

$$\Psi^{-1}(0,0,0,0,1) = e_5 = \frac{1}{2} (1 - a^2)$$

Agora, consideremos

$\emptyset : KK_8 \longrightarrow KK_8$ definida por:

$\emptyset(\alpha) = \alpha^x$ para todo $\alpha \in KK_8$.

Como $\emptyset$ mantém invariantes todos os subgrupos de K_8 , considerando o reticulado dos subgrupos de K_8 , vemos que as únicas possibilidades para $\emptyset$ são as seguintes:

$$\begin{array}{llll} a \mapsto a & a \mapsto a & a \mapsto a^3 & a \mapsto a^3 \\ b \mapsto b & b \mapsto a^2b & b \mapsto b & b \mapsto a^2b \end{array}$$

Portanto $\emptyset(e_j) = e_j$, $1 \leq j \leq 5$ e nossa afirmação está provada.

Agora, $K(ExK_8) = (KE)K_8 = (K \oplus \dots \oplus K)K_8 =$
 $KK_8 \oplus \dots \oplus KK_8 = \left(\left(\bigoplus_{i=1}^4 K \right) \oplus IH_K \right) \oplus \dots \oplus \left(\left(\bigoplus_{i=1}^4 K \right) \oplus IH_K \right)$ é
 uma soma direta de anéis com divisão de característica zero tal que todo idempotente é central em KG . Portanto por
 (19), Lema VI 3.22 $U(RG) = U(RT)G$. Logo $T(U(RG)) = T(U(RT))$
 e pela Proposição 1.5 $T(U(RT)) = \pm T$.

(iii) $\implies$ (iv) Trivial

(iv) $\implies$ (i) Como $T(U(\mathbb{Z}G))$ é um subgrupo de $U(\mathbb{Z}G)$, por (11), T é um grupo abeliano ou 2-Hamiltoniano, tal que todo subgrupo de T é normal em G . Argumentando como anteriormente, concluímos que $U(RG) = U(RT)G$. Portanto $U(RG)$ é solúvel.

2. Anéis de grupo sobre os inteiros de um corpo de números algébricos que contém uma raiz complexa da unidade.

Como anteriormente, K representará um corpo de números algébricos e R seu anel de inteiros.

Proposição 2.1: Seja G um grupo finito e seja e um idempotente central em KG . Então, pela projeção natural, $U(RG)$ é levado sobre um subgrupo de índice finito de $U(RGe)$.

Demonstração: Consideremos a situação, ilustrada pelo diagrama abaixo:

$$\begin{array}{ccc} U(KG) & \xrightarrow{\pi} & U(KGe) \\ i \uparrow & & \uparrow i \\ U(RG) & \xrightarrow{\pi} & U(RGe) \end{array}$$

onde $(U(RG)) = U(RG)e \subseteq U(RGe)$

Como $K = R / (\mathbb{Z} - \{0\})$, podemos escolher um inteiro $m \in \mathbb{Z}$, $m > 1$, tal que $me \in RG$. O anel RG_e / mRG_e é finito, pois $RG_e / mRG_e \cong (R/mR)G_e$, G é finito e $|R/mR| = N(R)$, a norma do ideal mR . Agora, restringindo o epimorfismo canônico

$$RG_e \longrightarrow RG_e / mRG_e$$

ao grupo das unidades de RG_e , obtemos o epimorfismo multiplicativo

$$\omega : U(RG_e) \longrightarrow L$$

onde

$L = \omega(U(RG_e))$ é um subgrupo do grupo finito $U(RG_e / mRG_e)$. Desse modo

$H = \text{Ker } \omega = \{ \xi \in U(RG_e) / \xi \equiv e \pmod{mRG_e} \}$ é um subgrupo normal de índice finito de $U(RG_e)$.

Seja $\xi \in H$ e consideremos o elemento $\beta = 1 - e + e\xi \in KG$. Por definição $\xi = e + me\gamma$ para algum $\gamma \in RG$, donde $\beta = 1 + me\gamma \in RG$. Do mesmo modo, como $\beta^{-1} = (1-e) + e\xi^{-1}$, temos que $\beta^{-1} \in RG$ pelo mesmo motivo. Portanto, $\beta \in U(RG)$ e $\pi(U(RG)) \supseteq H$.

O lema abaixo, que será utilizado na demonstração do próximo teorema, é devido a Brenner, J.L., (2).

A prova apresentada a seguir, entretanto, é de nossa autoria.

Lema 2.2: O subgrupo de $SL(2, \mathbb{Z})$ gerado por $A = \begin{bmatrix} 1 & m \\ 0 & 1 \end{bmatrix}$ e $B = \begin{bmatrix} 1 & 0 \\ m & 1 \end{bmatrix}$, $m \geq 2$, é livre.

Demonstração: Seja $\psi: SL(2, \mathbb{Z}) \rightarrow PSL(2, \mathbb{Z})$ a função definida por:

$$\psi(X) = X(\pm I), \text{ onde } I = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}.$$

É bem conhecido que $PSL(2, \mathbb{Z}) = \langle x \rangle * \langle y \rangle$, o produto livre do grupo cíclico de ordem dois gerado por $x = \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix}$ pelo grupo cíclico de ordem 3 gerado por $y = \begin{bmatrix} 0 & 1 \\ -1 & -1 \end{bmatrix}$.

$$\text{Como } \psi\left(\begin{bmatrix} 1 & m \\ 0 & 1 \end{bmatrix}\right) = (xy)^m \text{ e } \psi\left(\begin{bmatrix} 1 & 0 \\ m & 1 \end{bmatrix}\right) = (xy^2)^m,$$

afirmamos que $(xy)^m$ e $(xy^2)^m$ geram livremente um grupo livre.

$$\text{Seja } W = (w_1, w_2), w_1 = \prod_{j=1}^m xy \text{ e } w_2 = \prod_{j=1}^m xy^2.$$

Consideremos o produto W-reduzido $v = w_1^{\epsilon_1} w_2^{\epsilon_2} \dots w_n^{\epsilon_n}$, $i' \in (1, 2)$, $\epsilon_i = \pm 1$, i.e., $i' = (i+1)'$ implica $\epsilon_i \neq -\epsilon_{i+1}$.

Vamos mostrar por indução em n que:

$$(1) \text{ Se } n' = 1 \begin{cases} \epsilon_n = 1 & v \text{ termina em } y \\ \epsilon_n = -1 & v \text{ termina em } y^2 x \end{cases}$$

$$(2) \text{ Se } n' = 2 \begin{cases} \varepsilon_n = 1 & v \text{ termina em } y^2 \\ \varepsilon_n = -1 & v \text{ termina em } yx \end{cases}$$

$$\text{Se } n=1 \text{ então } w_1 = \prod_{j=1}^m xy, \quad w_1^{-1} = \prod_{j=1}^m y^2x, \quad w_2 = \prod_{j=1}^m xy^2, \quad w_2^{-1} = \prod_{j=1}^m yx$$

e a indução começa. Vamos assumir, agora, a afirmação verdadeira para n e prová-la para $n + 1$.

$$(1) \quad \underline{n = 1}$$

(a) $\varepsilon_n = 1$. Então, pela hipótese de indução $w_1^{\varepsilon_1} \dots w_n^{\varepsilon_n}$ termina em y . Se $(n+1)' = 1$ então, como v é um produto reduzido devemos ter $\varepsilon_{n+1} = 1$ e v termina em $y \prod_{j=1}^m xy$. Assim v termina em y como o desejado.

Se $(n+1)' = 2$ e $\varepsilon_{n+1} = 1$ então v termina em $y \prod_{j=1}^m xy^2$ e portanto v termina em y^2 . Se $(n+1)' = 2$ e $\varepsilon_{n+1} = -1$ então v termina em $y \prod_{j=1}^m yx$ e portanto v termina em yx .

(b) $\varepsilon_n = -1$. Então, pela hipótese de indução $w_1^{\varepsilon_1} \dots w_n^{\varepsilon_n}$ termina em y^2x . Se $(n+1)' = 1$ então, v é um produto reduzido, devemos ter $\varepsilon_{n+1} = -1$. Portanto v termina em $y^2x \prod_{j=1}^m y^2x$ e portanto v termina em y^2x ,

Se $(n+1)' = 2$ e $\varepsilon_{n+1} = 1$ então v termina na em $y^2 \times \prod_{j=1}^m xy^2 = y \prod_{j=2}^m xy^2$, e portanto v termina em y^2 .
Se $(n+1)' = 2$ e $\varepsilon_{n+1} = -1$ então v termina em $y^2 \times \prod_{j=1}^m yx$ e v termina em yx .

(2) $n' = 2$

(a) $\varepsilon_n = 1$. Então, pela hipótese de indução $w_1^{\varepsilon_1} \dots w_n^{\varepsilon_n}$ termina em y^2 . Se $(n+1)' = 2$, como v é uma palavra reduzida, devemos ter $\varepsilon_{n+1} = 1$ e portanto v termina em $y^2 \prod_{j=1}^m xy^2$ e portanto v termina em y^2 .

Se $(n+1)' = 1$ e $\varepsilon_{n+1} = 1$ então v termina em $y^2 \prod_{j=1}^m xy$ e portanto v termina em y . Se $(n+1)' = 1$ e $\varepsilon_{n+1} = -1$ então v termina em $y^2 \prod_{j=1}^m y^2x = yx \prod_{j=2}^m y^2x$ e v termina em y^2x .

(b) $\varepsilon_n = -1$. Então, pela hipótese de indução $w_1^{\varepsilon_1} \dots w_n^{\varepsilon_n}$ termina em yx . Se $(n+1)' = 2$, como v é uma palavra reduzida, devemos ter $\varepsilon_{n+1} = -1$ e v termina em $yx \prod_{j=1}^m yx$ e v termina em yx .

Se $(n+1)' = 1$ e $\varepsilon_{n+1} = 1$ então v termina em $yx \prod_{j=1}^m xy = y^2 \prod_{j=2}^m xy$ e portanto v termina em y . Se $(n+1)' = 1$ e $\varepsilon_{n+1} = -1$ então v termina em $yx \prod_{j=1}^m y^2x$ e portanto v termina em y^2x . Isto completa o passo de indução.

Agora, pela propriedade universal dos grupos livres a função $(xy)^m \mapsto A$, $(xy^2)^m \mapsto B$ se estende a um único homomorfismo $\psi: \langle (xy)^m, (xy^2)^m \rangle \rightarrow SL(2, \mathbb{Z})$. Logo A e B geram livremente um grupo livre.

Lema 2.3: Sejam A_1 e A_2 duas matrizes diagonalizáveis de $GL(2, \mathbb{C})$ tal que

(i) para cada $j = 1, 2$, os valores absolutos dos autovalores de A_j são distintos.

(ii) os elementos A_j , $j = 1, 2$ não tem auto-espacos comuns. Então existe um inteiro positivo m tal que A_1^m e A_2^m geram livremente um grupo livre de posto 2.

Demonstração: Veja [22], Proposição 3.12.

Lema 2.4 Se R contém uma raiz complexa da unidade então $U(RK_g)$ contém um grupo livre de posto 2.

Demonstração: Vamos considerar dois casos:

(1) R contém θ , uma raiz primitiva p -ésima da unidade, onde p é um primo impar.

Coloquemos $IH_\theta = \mathbb{Q}(\theta) \otimes_{\mathbb{Q}} IH_{\mathbb{Q}}$, onde $IH_{\mathbb{Q}}$ é a álgebra dos quatérnios racionais. Então existe um isomorfismo de $\mathbb{Q}(\theta)$ -álgebras.

$$\vartheta: \mathbb{Q}(\theta)K_g \longrightarrow \mathbb{Q}(\theta) \oplus \mathbb{Q}(\theta) \oplus \mathbb{Q}(\theta) \oplus \mathbb{Q}(\theta) \oplus IH_\theta \quad \text{tal}$$

que:

$$\emptyset(a) = (1, 1, -1, -1, i) \quad , \quad \emptyset(b) = (1, -1, 1, -1, j).$$

Então é fácil verificar que $\emptyset^{-1}(0, 0, 0, 0, 1) = \frac{1}{2}(1-a^2) = e$ é um idempotente central de $\mathbb{Q}(\theta)K_8$ e que:

$$(\mathbb{Z}[\theta]K_8)e = \left\{ \frac{1}{2}(x_0 + x_1 a - x_0 a^2 - x_1 a^3 + y_0 b + y_1 ab - y_0 a^2 b - y_1 a^3 b) / x_0, x_1, y_0, y_1 \in \mathbb{Z}[\theta] \right\}.$$

$$\text{Coloquemos } S = \{x_0 + x_1 i + y_0 j + y_1 k / x_0, x_1, y_0, y_1 \in \mathbb{Z}[\theta]\}.$$

Então, utilizando as fórmulas explícitas da função $\emptyset$ descritas na Proposição I.1.2 verificamos que $\emptyset : \mathbb{Z}[\theta]K_8 e \longrightarrow S$ é um isomorfismo. Afirmamos que existe um inteiro $n > 0$ tal que $(1 + \theta i)^n$ e $(1 + \theta j)^n$ geram um grupo livre de posto 2 em $U(S)$.

Em primeiro lugar, observamos que $1 + \theta i$ é uma unidade de S pois $(1 + \theta i)(1 - \theta i) = 1 + \theta^2$ e colocando $X = 1$ na identidade

$$X^p + 1 = \prod_{m=0}^{p-1} (X - \theta^m) = (X + 1) \prod_{m=1}^{p-1} (X + \theta^m)$$

vemos que $1 + \theta^2$ é uma unidade de $\mathbb{Z}[\theta]$. Logo

$(1 + \theta i)^{-1} = (1 - \theta i)(1 + \theta^2)^{-1}$. Por razões análogas $1 + \theta j$ é uma unidade de S .

Seja agora L o subcorpo de $\mathbb{H}_\theta$ gerado por θ e i . Então $\mathbb{H}_\theta = L \oplus Lj$ e a representação regular à direita

determina um monomorfismo da subálgebra gerada por $1 + \theta i$ e $1 + \theta j$ em $GL(2, L)$. Por este monomorfismo temos

$$1 + \theta i \mapsto \begin{bmatrix} 1 + \theta i & 0 \\ 0 & 1 - \theta i \end{bmatrix} = A$$

$$1 + \theta j \mapsto \begin{bmatrix} 1 & \theta \\ -\theta & 1 \end{bmatrix} = B$$

Os autovalores de A são $1 + \theta i$ e $1 - \theta i$ com auto-espacos correspondentes gerados por $(1,0)$ e $(0,1)$.

Os autovalores de B são também $1 + \theta i$ e $1 - \theta i$ com auto-espacos correspondentes gerados por $(i,1)$ e $(1,i)$, respectivamente. Notemos também que $|1 + \theta i| \neq |1 - \theta i|$.

De fato, se $|1 + \theta i| = |1 - \theta i|$, então

$$2 + \theta i - \bar{\theta} i = (1 + \theta i)(1 - \bar{\theta} i) = |1 + \theta i|^2 = |1 - \theta i|^2 = (1 - \theta i)(1 + \bar{\theta} i) = 2 - \theta i + \bar{\theta} i \text{ e portanto } \theta = \bar{\theta}, \text{ uma contradição.}$$

Agora, pelo Lema 2.3 existe $n > 0$ tal que A^n e B^n geram livremente um grupo livre. Basta agora aplicar a Proposição 2.1.

(2) R contém $i = \sqrt{-1}$

Seja $M_2(\mathbb{Q}(i))$ o anel das matrizes 2×2 sobre $\mathbb{Q}(i)$. Então existe um isomorfismo.

$$\emptyset : \mathbb{Q}(i)K_8 \longrightarrow \mathbb{Q}(i) \oplus \mathbb{Q}(i) \oplus \mathbb{Q}(i) \oplus \mathbb{Q}(i) \oplus M_2(\mathbb{Q}(i))$$

de $\mathbb{Q}(i)$ -álgebras tal que:

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

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

Outra vez, temos que:

$$\emptyset^{-1}(0, 0, 0, 0, \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}) = \frac{1}{2}(1 - a^2) = e \text{ é um}$$

idempotente central de $\mathbb{Q}(i)K_8$, e $\mathbb{Z}[i]K_8e$ é igual ao seu análogo de (1). Se $M_2(\mathbb{Z}[i])$ representa o anel das matrizes 2×2 sobre $\mathbb{Z}[i]$, então:

$$\emptyset : \mathbb{Z}[i]K_8e \longrightarrow M_2(\mathbb{Z}[i]) \text{ é um monomorfismo e}$$

$$\emptyset\left(\frac{1}{2}(1 - a^2 \pm b \pm iab \mp a^2b \mp ia^3b)\right) = \begin{bmatrix} 1 & 0 \\ \pm 2 & 1 \end{bmatrix}$$

$$\emptyset\left(\frac{1}{2}(1 - a^2 \mp b \pm iab \pm a^2b \mp ia^3b)\right) = \begin{bmatrix} 1 & \pm 2 \\ 0 & 1 \end{bmatrix}$$

Pela Proposição 2.1 existe um inteiro $n > 0$ tal que $\emptyset^{-1}\left(\begin{bmatrix} 1 & 0 \\ 2n & 1 \end{bmatrix}\right)$ e $\emptyset^{-1}\left(\begin{bmatrix} 1 & 2n \\ 0 & 1 \end{bmatrix}\right)$ pertencem a $U(\mathbb{Z}[i]K_8e)$. Como pelo

Lema 2.2, $\left\langle \begin{bmatrix} 1 & 0 \\ 2n & 1 \end{bmatrix}, \begin{bmatrix} 1 & 2n \\ 0 & 1 \end{bmatrix} \right\rangle$ é um grupo livre de posto

2 a prova está completa.

Teorema 2.5 Seja G um grupo de torção e suponhamos que R contém uma raiz complexa da unidade. Então $U(RG)$ é solúvel se e só se G é abeliano.

Demonstração: Se $U(RG)$ é solúvel, então pelo resultado de Sehgal (19), Teorema VI 4.8, G é abeliano ou um 2-grupo Hamiltoniano. Mas se G fosse um 2-grupo Hamiltoniano $U(RK_8)$ seria solúvel, em contradição com o Lema 2.4.

Vamos considerar, agora, dois exemplos que sugerem que a situação mais geral em que podemos esperar que $U(RK_8)$ seja solúvel é, de fato, no caso em que K é totalmente real.

Exemplo 2.6: Seja $K = \mathbb{Q}(\sqrt[6]{2})$. Então $\mathbb{Z}(\sqrt[6]{2}) \subseteq R$ e se consideramos $x = \sqrt[3]{2}$, então o elemento $\omega = 1 + x + x^2$ é uma unidade de R .

De fato, $1 + x + x^2 = \frac{x^3 - 1}{x - 1} = \frac{1}{\sqrt[3]{2} - 1}$, i.e.,
 $(1 + x + x^2)(\sqrt[3]{2} - 1) = 1$.

Sejam $\alpha = 1 + \sqrt[6]{2} i + \sqrt[3]{2} j$ e
 $\beta = 1 + \sqrt[3]{2} i + \sqrt[6]{2} k$ elementos de $\mathbb{H}_R \subseteq \mathbb{H}_K = K \otimes_{\mathbb{Q}} \mathbb{H}_{\mathbb{Q}}$.

Afirmamos que existe um inteiro $n > 0$ tal que α^n e β^n geram um grupo livre de posto 2 em $U(\mathbb{H}_R)$.

De fato, argumentando como no Lema 2.4, parte (1), as imagens de α e β em $M_2(K(i))$ pela representação regular à direita de $I\mathbb{H}_K$ são, respectivamente:

$$A = \begin{bmatrix} 1 + \frac{6}{\sqrt{2}} i & \frac{3}{\sqrt{2}} \\ -\frac{3}{\sqrt{2}} & 1 - \frac{6}{\sqrt{2}} i \end{bmatrix} \quad \text{e} \quad B = \begin{bmatrix} 1 + \frac{3}{\sqrt{2}} i & \frac{6}{\sqrt{2}} i \\ \frac{6}{\sqrt{2}} i & 1 - \frac{3}{\sqrt{2}} i \end{bmatrix}$$

As matrizes A e B têm o mesmo polinômio característico, igual a $Y^2 - 2Y + \omega$, cujas raízes são $1 \pm \sqrt{1 - \omega}$.

Portanto, os autovalores de A e B são, aproximadamente, $1 + 1,687 i$ e $1 - 1,687 i$, com os correspondentes auto-espacos gerados por $(1; 0,448 i)$ e $(1; -2,229 i)$ para A , e $(1; 0,380)$ e $(1; -2,625)$ para B , respectivamente. Basta agora aplicar o Lema 2.3.

Exemplo 2.7: Seja $d \in \mathbb{Z}$, positivo, diferente de 1 e 3, livre de quadrados e consideremos a extensão $K = \mathbb{Q}(\sqrt{-d})$. Afirma-mos que $U(I\mathbb{H}_R)$ contém um grupo livre de posto 2.

De fato, por (16), Proposição 5.6.1 a equação de Pell-Fermat $x^2 - dy^2 = \pm 1$ tem uma solução (a,b) que corresponde a uma unidade não trivial de $\mathbb{Z}(\sqrt{d})$. Sejam

$\alpha = a + (b\sqrt{-d})i$ e $\beta = a + (b\sqrt{-d})j$ elementos de $\mathbb{H}_R$. Então $\alpha, \beta \in U(\mathbb{H}_R)$, e as imagens de α e β pela representação regular à direita são, respectivamente:

$$A = \begin{bmatrix} a - b\sqrt{d} & 0 \\ 0 & a + b\sqrt{d} \end{bmatrix} \quad \text{e} \quad B = \begin{bmatrix} a & b\sqrt{d}i \\ -b\sqrt{d}i & a \end{bmatrix}$$

As matrizes A e B têm o mesmo polinômio característico, igual a $Y^2 - 2aY + a^2 - b^2d$, cujas raízes são $a - b\sqrt{d}$ e $a + b\sqrt{d}$.

Portanto, os autovalores de A e B são $a - b\sqrt{d}$ e $a + b\sqrt{d}$, com os correspondentes auto-espacos gerados por $(1; 0)$ e $(0; 1)$ para A e $(1; i)$ e $(1; -i)$ para B , respectivamente. Basta agora aplicar o Lema 2.3.

C A P Í T U L O I I I

SUBGRUPOS DE UNIDADES LIVRES EM ANÉIS DE GRUPOS

Sejam K um corpo de característica $p \gg 0$, $K^* = K - \{0\}$, $GF(p)$ o corpo de Galois com p elementos, G um grupo e KG seu anel de grupo. Neste capítulo estudaremos condições sob as quais $U(KG)$, o grupo das unidades de KG , não contém grupos livre de posto 2, no caso em que G é finito e também para certas classes de grupos infinitos.

1. O caso $p = 0$

Seja $IH_{\mathbb{Q}}$ a álgebra dos quatérnios usual sobre $\mathbb{Q}$, i.e.,

$$IH_{\mathbb{Q}} = \{a + bi + cj + dk / a, b, c, d \in \mathbb{Q}, i^2 = j^2 = -1, ij = -ji = k\}$$

Definição: Dizemos que G é um grupo linear sobre K se G é isomorfo a um subgrupo do grupo geral linear $GL(n, K)$.

Lema 1.1 : Sobre um corpo de característica zero, um grupo linear ou contém um subgrupo livre não abeliano ou contém um subgrupo solúvel de índice finito.

Demonstração: Veja (22), Teorema 1.

Lema 1.2 : Seja D um anel com divisão, Z o seu centro, $D^* = D - \{0\}$ e $Z^* = Z - \{0\}$. Então D^* / Z^* não possui subgrupos abelianos, normais, não triviais.

Demonstração: Veja (17), Teorema 2.

Lema 1.3 : $U(IH_{\mathbb{Q}})$, o grupo multiplicativo de $IH_{\mathbb{Q}}$, contém um grupo livre de posto 2.

Demonstração: Suponhamos que isto não acontece. Então, pelo Lema 1.1, $U(IH_{\mathbb{Q}})$ contém um subgrupo normal, solúvel, γ de índice finito. Entretanto, pelo Lema 1.2, sabemos que $U(IH_{\mathbb{Q}}) / \mathbb{Q}^*$ não contém subgrupos normais, abelianos, não triviais. Portanto $\gamma \subseteq \mathbb{Q}^*$ e $U(IH_{\mathbb{Q}}) / \mathbb{Q}^*$ é finito, um contradição.

Teorema 1.4 Seja G um grupo finito. Então $U(KG)$ não contém um grupo livre de posto 2 se e só se G é abeliano.

Demonstração: Suponhamos inicialmente que $U(KG)$ não contém subgrupos livres de posto 2.

Como K tem característica zero, podemos assumir que K contém $\mathbb{Q}$.

Agora, $QG \cong \bigoplus_{i=1}^r M_{n_i}(D_i)$, onde $M_{n_i}(D_i)$ denota o anel das matrizes quadradas $n_i \times n_i$ sobre um anel com divisão D_i .

Se, para algum i , $n_i > 1$, tomamos $A = \begin{bmatrix} 1 & 2 \\ 0 & 1 \end{bmatrix}$ e $B = \begin{bmatrix} 1 & 0 \\ 2 & 1 \end{bmatrix}$. Então, pelo Lema II, A e B geram livremente um grupo livre, que pode ser incluído de forma óbvia em $M_{n_i}(D)$. Portanto, devemos ter $QG \cong \bigoplus_{i=1}^r D_i$.

Isto significa que todo idempotente de QG é central em QG . Logo, por (18), 2.6, G é um grupo abeliano ou Hamiltoniano.

Vamos supor que G contém K_8 , o grupo quaternio de ordem 8. Então

$$QK_8 \cong \left(\bigoplus_{i=1}^4 \mathbb{Q} \right) \oplus H_{\mathbb{Q}} \quad \text{e} \quad U(QK_8) \cong \left(\bigoplus_{i=1}^4 \mathbb{Q}^* \right) \oplus U(H_{\mathbb{Q}}), \quad \text{em}$$

contradição com o Lema 1.3.

A recíproca é trivial.

Corolário 1.5: Seja G um grupo nilpotente ou FC. Se $U(KG)$ não contém um subgrupo livre de posto 2, então:

- (i) T , o subgrupo de torção de G , é um subgrupo abeliano.
- (ii) todo subgrupo de T é normal em G .

Como uma recíproca parcial temos que se valem (i) e (ii), então $U(QG)$ não contém subgrupos livres de posto 2.

Demonstração: Como T é localmente finito, o Teorema 1.4 implica que T é abeliano. Agora, seja $x \in G \setminus T$, $a \in T$ e consideremos $H = \langle a, x \rangle$. Se algum idempotente de $K \langle a \rangle$ não é central em KH , por (19), Lema VI 3.12, $U(KH)$ contém uma cópia isomorfa de grupo geral linear $GL(m, F)$, sobre um corpo $F \supseteq K$ e para algum $m > 1$. Isto é impossível. Logo, todo idempotente de $K \langle a \rangle$ é central em KH e portanto x normaliza $\langle a \rangle$.

Reciprocamente, se valem (i) e (ii), então (19), Proposição VI 1.16, implica diretamente que todo idempotente de QT é central em QG , e argumentando como na prova da suficiência do Teorema I 1.5, segue que $U(QG)$ é solúvel. Portanto $U(QG)$ não contém um subgrupo livre de posto 2.

2. O caso $p > 0$

Seja E um corpo de característica $p \geq 3$, localmente compacto, com uma valorização que denotaremos por $||$, não trivial e seja

$H_E = \{a + bi + cj + dk / a, b, c, d \in E, i^2 = j^2 = -1, ij = -ji = k\}$ a álgebra de quatérnios sobre E .

Lema 2.1 : Seja G um grupo linear sobre um corpo K de característica diferente de zero. Então, são equivalentes:

- (i) G não contém um subgrupo livre não abeliano.
- (ii) G contém um subgrupo normal solúvel H tal que G/H é localmente finito.

Demonstração: Veja (22), Teorema 2.

Lema 2.2 : Se $\mathbb{H}_E$ é um anel com divisão, então $U(\mathbb{H}_E)$ contém um subgrupo livre de posto 2.

Demonstração: Suponhamos que não. Então pelo Lema 2.1

$U(\mathbb{H}_E)$ contém um subgrupo normal, solúvel Y tal que $U(\mathbb{H}_E)/Y$ é localmente finito. Mas pelo Lema 1.2 $U(\mathbb{H}_E)/E^*$ não contém subgrupos normais, abelianos, não triviais. Portanto $Y \subseteq E^* = Z(U(\mathbb{H}_E))$, o centro de $U(\mathbb{H}_E)$, e $U(\mathbb{H}_E)/E^*$ é um grupo isomorfo a $U(\mathbb{H}_E)/Y/E^*/Y$, e portanto é localmente finito.

Agora, vamos exibir um elemento de ordem in finita em $U(\mathbb{H}_E)/E^*$.

Seja $\lambda \in E$ tal que $\lambda \neq 1$, coloquemos $\tau = 1 + \lambda i$ e suponhamos que para algum n inteiro, $n > 0$, $\tau^n = \omega \in E^*$. Como estamos em característica p podemos supor que $p \nmid n$.

Portanto

$$(1 + \lambda i)^n = \sum_{l=0}^n \binom{n}{l} \lambda^{l_1} i^{l_2} = \sum_{\substack{l \text{ par} \\ l_2=0}} \binom{n}{l} \lambda^{l_1} i^{l_2} + \sum_{\substack{l \text{ ímpar} \\ l_2=1}} \binom{n}{l} \lambda^{l_1} i^{l_2} = \\ \sum_j \binom{n}{2j} \lambda^{2j} (-1)^j + \lambda i \sum_j \binom{n}{2j+1} \lambda^{2j} (-1)^j, \text{ o qual não pertence a } E$$

pois o coeficiente de λ_i é diferente de zero, uma contradição.

Teorema 2.3 : Seja G um grupo finito e K um corpo de característica $p > 0$. Então $U(KG)$ não contém um subgrupo livre de posto 2 se e só se uma das seguintes condições está verificada:

- (i) K é algébrico sobre $GF(p)$
- ou
- (ii) $S_p(G)$, o p -subgrupo de Sylow de G , é normal em G e $G/S_p(G)$ é abeliano.

Demonstração: Primeiro, observamos que se K é algébrico sobre $GF(p)$, então para qualquer elemento inversível $\alpha \in U(KG)$, existe uma extensão finita E de $GF(p)$ tal que $\alpha \in U(EG)$ é de ordem finita; portanto $U(KG)$ é um grupo de torção.

Agora, suponhamos que K não seja algébrico sobre $GF(p)$. Então existe um elemento λ em K que é transcendente sobre $GF(p)$. Por (22), Lema 4.1, podemos construir um corpo valorizado E , localmente compacto, com uma valorização $||$, tal que $|\lambda| \neq 1$.

Seja $\mathcal{O}_p(G)$ o p -subgrupo normal máximo de G e $J(EG)$ o radical de Jacobson de EG . Vamos denotar por

$\psi: EG \longrightarrow EG / J(EG)$ a projeção natural. Como $J(EG)$ é um ideal nilpotente, sabemos que ψ induz um epimorfismo

$$\psi: U(EG) \longrightarrow U(EG / J(EG)) \cong \bigoplus_{i=1}^r U(M_{n_i}(D_i)).$$

Mas se $n_i > 1$ para algum índice i , podemos produzir um subgrupo livre de posto dois em $U(M_{n_i}(E))$ por exemplo, coloquemos:

$$A = \begin{bmatrix} \lambda & 0 \\ 0 & \lambda^{-1} \end{bmatrix} \quad \text{e} \quad B = P \begin{bmatrix} \lambda & 0 \\ 0 & \lambda^{-1} \end{bmatrix} P^{-1}, \quad \text{onde} \quad P = \begin{bmatrix} 1 + \lambda & \lambda \\ -\lambda & 1 - \lambda \end{bmatrix}$$

Então por (22), Proposição 3.12, existe um inteiro $m > 0$ tal que A^m e B^m geram livremente um grupo livre de posto 2, que pode ser incluído de forma óbvia em $U(M_{n_i}(E))$. Portanto

$$U(EG / J(EG)) \cong \bigoplus_{i=1}^r U(D_i).$$

Afirmamos que $G / \mathcal{O}_p(G)$ não tem p -elementos.

De fato, se $x \in S_p(G) / \mathcal{O}_p(G)$ for um elemento de ordem potência de p , então existe $n \in \mathbb{N} - \{0\}$ tal que $x^{p^n} \in \mathcal{O}_p(G)$. Como $\mathcal{O}_p(G) \subseteq 1 + J(EG)$ temos que:

$$\psi(x^{p^n}) = (1, 1, \dots, 1) \quad \text{e}$$

$$(\psi(x) - (1, 1, \dots, 1))^{p^n} = (0, 0, \dots, 0). \quad \text{Portanto}$$

$$\psi(x) = (1, 1, \dots, 1) \quad \text{e} \quad x \in \mathcal{O}_p(G).$$

Agora, seja $\varphi : EG \longrightarrow E(G/S_p(G))$ o epimorfismo natural. Usando os mesmos argumentos anteriores concluímos que

$$\varphi : EG \longrightarrow E(G/S_p(G)) = \bigoplus_{i=1}^r D_i.$$

Como $H = G/S_p(G)$ não possui p -elementos e todo idempotente de EH é central, por (18), 2.6, segue diretamente que H é abeliano ou Hamiltoniano.

Se $p = 2$ vemos facilmente que H deve ser abeliano de ordem ímpar.

Resta estudar o caso $p > 2$.

Vamos supor que H contém o grupo quatérnio K_8 de ordem 8. Então $EK_8 \cong (\bigoplus_{i=1}^4 E) \oplus IH_E$ e

$$U(EK_8) \cong (\bigoplus_{i=1}^4 E^*) \oplus U(IH_E), \text{ em contradição com o Lema 2.2}$$

Proposição 2.4: Seja G um grupo nilpotente, não de torção, T o subgrupo de torção de G e $S_p(T)$ o p -subgrupo de Sylow de T . Se $U(KG)$ não contém subgrupos livres de posto 2 então:

- (i) $T/S_p(T)$ é abeliano, tal que todo subgrupo de $T/S_p(T)$ é normal em $G/S_p(T)$.

Como uma recíproca parcial, se vale (i) e, ademais, $T/S_p(T)$ está contido no centro de $G/S_p(T)$, então $U(KG)$ não contém subgrupos livres de posto 2.

Prova: Observemos que podemos assumir que G é finitamente gerado, pois apenas propriedades locais estão envolvidas. Porém, neste caso, T é de ordem finita, $S_p(T)$ é normal em G e podemos assumir também, considerando $G/S_p(T)$, que G não tem p -elementos.

Agora, por (14), Teorema 2.24, G contém um elemento central x de ordem infinita. Então, consideramos

$$GF(p)\langle x, T \rangle = GF(p) \langle \langle x \rangle \times T \rangle \cong GF(p)\langle x \rangle \otimes_{GF(p)} GF(p)T \cong GF(p)\langle x \rangle \otimes_{GF(p)} \left[\bigoplus_{i=1}^r M_{n_i}(E_i) \right] \cong \bigoplus_{i=1}^r M_{n_i} \left(GF(p)\langle x \rangle \otimes_{GF(p)} E_i \right).$$

Se, para algum i , $n_i > 1$ então, em $U(M_{n_i}(GF(p) \otimes_{GF(p)} E_i))$ temos matrizes A e B , como na demonstração do Teorema 2.3, uma contradição. Portanto, para todo i , $n_i = 1$ e T é abeliano.

Seja, agora, h um elemento de T e vamos assumir que $y \in G$ não normaliza $\langle h \rangle$. Sejam $n = |\langle h \rangle|$.

$$e = \frac{1}{n} \sum_{i=1}^n h^i \quad e \quad f = e(1 - e^y).$$

O suporte de ee^y é $\langle h \rangle \langle h \rangle^y$, que não está contido em $\langle h \rangle$. Logo $e \neq ee^y$ e $f \neq 0$. Temos também que $f^2 = f$ e como KT é abeliano $f^y f = f f^y$.

Sejam

$$e_{12} = fy, \quad e_{21} = y^{-1}f, \quad e_{11} = e_{12}e_{21} = f, \quad e_{22} = e_{21}e_{12} = f^y.$$

Então podemos verificar através de um cálculo direto que

$e_{ij}e_{kl} = \delta_{jk}e_{il}$, onde δ_{jk} é o delta de Kronecker para $1 \leq i, j, k, l \leq 2$. Como nenhum e_{ij} é zero, segue que

$L = \sum_{i,j=1}^2 GF(p)\langle x \rangle e_{ij} \cong M_2(GF(p)\langle x \rangle)$, o anel das matrizes 2×2 sobre $GF(p)\langle x \rangle$.

$$\text{Seja agora } \xi = \begin{matrix} e_{11} & e_{22} \end{matrix} \text{ e } R = GF(p)\langle x \rangle (1-\xi) \oplus L.$$

Nestas condições a aplicação:

$$\Psi : U(M_2(GF(p)\langle x \rangle)) \longrightarrow U(KG)$$

$$\Psi(\alpha) = 1 - \xi + \alpha \xi$$

é um monomorfismo de grupos, uma contradição.

Reciprocamente, se $\bar{T} = T/S_p(T)$ está no centro de $\bar{G} = G/S_p(T)$, então todo idempotente de $K\bar{T}$ é central em $K\bar{G}$ e argumentando como na prova da suficiência do Teorema I 1.5 segue que $U(K\bar{G})$ é solúvel. Portanto $U(KG)$ não contém subgrupos livres de posto 2.

R E F E R Ê N C I A S

- 1 - Bateman, J.M. e Coleman, D.B. Group algebras with nilpotent unit groups. Proc. Amer. Math. Soc. 19(1968), 448-449
- 2 - Brenner, J.L. Quelques groupes libres de matrices. C.R. Acad. Sci. Paris 241 (1955), 1689-1691
- 3 - Fisher, J.L., Parmenter, M.M., Sehgal, S.K. Group rings with solvable n-Engel unit groups. Proc. Amer. Math. Soc. 59(1976), 195-200.
- 4 - Hartley, B. e Pickel, P.F. Free subgroups in the unit groups of integral group rings. Can. J. of Math. 32, 6 (1980), 1342-1352.
- 5 - Janusz, G.J. Algebraic number fields. Academic Press, New York, 1973.
- 6 - Khripta, I.I. On the multiplicative group of a group ring. Thesis, Uzgorod, 1971.

- 7 - Khripta, I.I. On the nilpotence of the multiplicative group of a group ring. Mat. Zametki, 11 (1972), 191-200; Math. Notes 11 (1972), 119-124.
- 8 - Merklen, H. e Polcino Milies, C. Group rings over $\mathbb{Z}_{(p)}$ with FC unit groups. Can. J. of Math., 32, 5 (1980), 1266-1269.
- 9 - Parmenter, M.M. e Polcino Milies, C. Group rings whose units form a nilpotent of FC group. Proc. Amer. Math. Soc. 68 (1978), 247-248.
- 10 - Polcino Milies, C. Integral group rings with nilpotent unit groups. Can. J. of Math. 28 (1976) , 954-960.
- 11 - Polcino Milies, C. Group rings whose torsion units form a subgroup I . Proc. Amer. Math. Soc. 81, 2 (1981), 172-174.
- 12 - Pollard, H. The theory of algebraic numbers. Math. Assoc. of America. Buffalo, 1950.
- 12a- Reiner, I. Topics in integral representation theory. IV Escola de Álgebra. S. Paulo, 1976.

- 13 - Ribenboin, P. Algebraic numbers. Wiley -
Interscience, New York, 1972.

- 14 - Robinson, D.J.S. Finiteness conditions and
generalized soluble groups. Part I, Springer
Verlag, Berlin - Heidelberg - New York, 1972

- 15 - Rotman, J.J. The theory of groups. Allyn and Bacon,
Boston, 1965.

- 16 - Samuel, P. Théorie algébrique des nombres. Herman,
Paris, 1967.

- 17 - Scott, W.R. On the multiplicative group of a
division ring. Proc. Amer. Math. Soc.
8 (1957), 303-305.

- 18 - Sehgal, S.K. Nilpotent elements in group rings.
Manuscripta Math. 15(1975), 65-80.

- 19 - Sehgal, S.K. Topics in group rings. Marcel Dekker,
New York, 1978.

- 20 - Sehgal, S.K. e Zassenhaus, H.J. Group rings
whose units form an FC group. Math. Z.
153 (1977) , 29-35.

- 21 - Sehgal, S.K. e Zassenhaus , H.J. Integral
group rings with nilpotent unit groups.
Commun Algebra 5 (1977), 101-111.
- 22 - Tits, J. Free subgroups in linear groups. J. of
Algebra, 20 (1972), 250-270.
- 23 - Vigneras, M.F. Simplification pour les ordres
des corps de quaternions totalement
définis. J.R. Angew. Math. 286-287(1976),
257-277.

A B S T R A C T

S.K. Sehgal (19), Theorem VI 4.8 proved the following:

Theorem: Let Z be the ring of rational integers and G be a group. Suppose that $U(ZG)$, the group of units of the group ring ZG , is solvable. Then:

(*) The torsion elements T , of G form a group which is abelian or a Hamiltonian 2-group, with every subgroup normal in G .

Conversely, if G is a solvable group satisfying (*) and G/T is nilpotent then $U(ZG)$ is solvable.

In (4), Hartley and Pickel generalized the result above when G is a finite group proving:

Theorem: Let G be a finite group. Then exactly one of the following occurs:

- (i) G is abelian (and so is $U(ZG)$)
- (ii) G is a Hamiltonian 2-group, and $U(ZG) = (\pm g / g \in G)$
- (iii) $U(ZG)$ contains a free subgroup of rank two.

The goals of this thesis are the following:

- (i) to study the solvability of $U(RG)$ when R is $\mathbb{Z}_{(p)}$, the localization of $\mathbb{Z}$ at a prime ideal (p) , $\mathbb{Z}_{\hat{p}}$, the ring of p -adic integers, $\mathbb{Q}_{\hat{p}}$, the p -adic completion of the field of rational numbers and when R is the ring of integers of an algebraic number field
- (ii) if K is a field, to study when $U(KG)$ does not contains a free subgroup of rank two.

Our main results are:

Theorem I 1.5 : Let $R = \mathbb{Z}_{(p)}$ or $\mathbb{Z}_{\hat{p}}$ and suppose that $U(RG)$ is solvable. Then the following condition holds:

- (*) The set of torsion elements T , of G form a abelian group, such that every subgroup of T is normal in G .

Conversely, if G is a group satisfying (*) and

- (i) T is an Abelian p -subgroup
- (ii) G/T is nilpotent

then $U(\mathbb{Q}_{\hat{p}}G)$ is solvable.

Theorem II 1.6 : Let R be the ring of integers of a totally real algebraic number field and G be a finite group. Then the following conditions are equivalent:

- (i) $U(RG)$ is solvable
- (ii) $U(RG)$ is nilpotent
- (iii) $U(RG)$ is FC
- (iv) $T(U(RG))$, the set of torsion elements of $U(RG)$, is equal to $\pm G$
- (v) $T(U(RG))$ is a subgroup of $U(RG)$.
- (vi) G is an abelian or Hamiltonian 2-group.

Theorem II 1.9 Let G be an extension of a torsion group T by a torsion-free nilpotent group, and let R be the ring of integers of a totally real algebraic number field K , which satisfies the following property: for every rational prime p which is the order of an element $g \in T$, p is inert in K .

Then, are equivalent:

- (i) $U(RG)$ is solvable
- (ii) T is an abelian or Hamiltonian 2-group such that every subgroup of T is normal in G
- (iii) $T(U(RG)) = \pm T$
- (iv) $T(U(RG))$ is a subgroup of $U(RG)$

Theorem II 2.5 : Let R be the ring of integers of an algebraic number field, containing a complex root of the unity and G be a torsion group. Then $U(RG)$ is solvable if and only if G is abelian.

Theorem III 1.4 : Let G be a finite group and K a field of characteristic zero. Then $U(KG)$ does not contains a free group of rank two if and only if G is abelian.

Theorem III 2.3 : Let G be a finite group and K a field of characteristic $p > 0$. Then $U(KG)$ does not contains a free group of rank two if and only if either:

- (i) K is algebraic over its prime field $GF(p)$ or
- (ii) $S_p(G)$, the p -Sylow subgroup of G , is normal in G and $G/S_p(G)$ is abelian.