MONOGRAFIAS DE MATEMÁTICA Nº 58

UNIDADES EM ANEIS DE GRUPOS

CESAR POLCINO MILIES
IME-USP

INSTITUTO DE MATEMÁTICA PURA E APLICADA

RIO DE JANEIRO
1998

Impresso no Brasil / *Printed in Brazil*

Distribuição:
Instituto de Matemática Pura e Aplicada
Estrada Dona Castorina, 110
22460-320 - Rio de Janeiro-RJ
Tel. (021)529-5276
Fax (021)529-5005
e-mail: sic@impa.br

ISBN 85-244-0140-0

1 Prefácio

A estrutura algébrica dos anéis de grupo é particularmente rica. Para explorá-la é necessário recorrer não somente a técnicas da teoria dos grupos e da teoria dos anéis como também à teoria dos números algébricos, das representações de grupos e álgebras e, às vezes até, à álgebra homológica.

Esta é uma das principais razões que nos levaram a oferecer o presente curso, uma vez que acreditamos que o jovem estudante se beneficiará grandemente de abordar um assunto que mostra a integração entre os diversos ramos da álgebra.

Nestas notas demos especial atenção ao estudo do grupo das unidades. Os principais resultados aqui incluidos podem ser considerados já clássicos. Porém, optamos por adotar uma abordagem recente que se apóia em técnicas que estão sendo utilizadas na pesquisa atual.

O primeiro capítulo é inteiramente dedicado a motivar o estudo. Na primeira seção damos uma visão histórica das razões que levaram à introdução de prório conceito de anel de grupo para mostrar que sua definição é inteiramente natural e surgiu como consequência de determinadas circunstâncias históricas. Na segunda, mostramos porque o chamado Problema do Isomorfismo é talvez o problema central da área e como ele leva naturalmente o pesquisador a se intere grupo dos elementos inversíveis deste anel.

O segundo capítulo é dedicado a estudar alguns aspectos concretos do grupo das unidades. Finalmente, no terceiro capítulo damos rapidamente uma visão do estado atual da pesquisa em relação a dois problemas intimamente relacionados com a determinação da estrutura do grupo das unidades.

Agradecemos à Comissão organizadora da XIV Escola de Álgebra pelo convite para ministrar este curso e à Profa. Sônia P. Coelho pela leitura atenta dos originais.

Conteúdo

Parte I
Anéis de Grupo

2 Antecedentes históricos

Em 1833, Sir William Rowan Hamilton formulou a primeira teoria formal dos números complexos definindo-os, tal como é frequente fazer hoje em dia, como pares ordenados de números reais, acabando assim com quase trezentos anos de dúvidas quanto à real existência destes números. Ele já conhecia a interpretação geométrica dos complexos como vetores do plano, formulada poucos anos antes por autores como Wessel, Argand e Gauss, de modo que percebia que o que tinha feito, na verda onstruir uma álgebra que permitia trabalhar com os vetores do plano. Tinha também total consciência de que o maior desafio para a matemática da época era construir uma linguagem apropriada para desenvolver a dinâmica; algo semelhante ao que tinha sido feito antes por Newton ao criar o cálculo, dando condições para o desenvolvimento da cinemática. Para isso, seria necessário criar uma álgebra que permitisse trabalhar com os vetores do espaço.

Após muitos esforços, ele percebeu que não era possível criar uma tal estrutura e, por considerações essencialmente geométricas, chegou à conclusão de que poderia descrever operadores que agem sobre os vetores do espaço, trabalhando com uma álgebra de dimensão quatro.

Passou então a considerar elementos da forma $\alpha = a + bi + cj + dk$, que chamou *quatérnios*, onde os coeficientes a, b, c, d representam números reais. Era claro para ele que a soma de dois elementos desta forma devia ser definida somando coeficiente a coeficiente; isto é, na forma:

$$(a+bi+cj+dk)+(a'+b'i+c'j+d'k) = (a+a)+(b+b')i+(c+c')j+(d+d')k.$$

A grande dificuldade era definir adequadamente o produto de dois destes elementos. É claro que, se era de se esperar que esse produto tivesse as propriedades usuais das operações, como a propriedade distributiva, então seria suficiente definir apenas os produtos dos símbolos i, j, k, dois a dois e estender depois a definição de forma natural, usando a distributividade. Isto levou ainda muito tempo porque, de início, Hamilton assumiu que esse produto seria comutativo (o qu feitamente razoável, uma vez que ele não sabia que estava por descobrir a primeira álgebra não comutativa na história

da matemática). Finalmente, em outubro de 1843 ele descobriu as fórmulas fundamentais para a multiplicação de quatérnios:

$$i^2 = j^2 = k^2 = ijk = -1.$$

No dia seguinte, ele apresentou uma extensa memória sobre o cálculo de quatérnios à Acadêmia Real da Irlanda. A descoberta destes números causou um grande impacto na época, por diversas razões. Entre outras coisas, porque abria as possibilidades para novas extensões dos campos de números, justamente num momento em que a descoberta relativamente recente do Teorema Fundamental da Álgebra parecia indicar que todos os campos numéricos realmente necessários se esgotavam com o os complexos.

Em dezembro desse mesmo ano, numa resposta a uma carta do próprio Hamilton, o matemático inglês John T. Graves introduz ainda um outro conjunto, os *octônios*, que podem ser definidos como elementos da forma $a_0 + a_1e_1 + a_2e_2 + \cdots + a_7e_7$, onde os coeficientes a_i, $1 \leq i \leq 7$, são números reais e os símbolos e_i, $1 \leq i \leq 7$, são chamados unidades básicas. Novamente, a soma se define coeficiente a coeficiente e o produto se define nas unidades básicas, uanto vale o produto de unidades, tomadas duas a duas. Graves não chegou a publicar esta descoberta e este números foram redescobertos por Arthur Cayley em 1845, razão pela qual eles são chamados, às vezes, de *números de Cayley.*

O próprio Hamilton percebeu as possibilidades de generalização e definiu primeiro os chamados *biquatérnios*, que são elementos da forma $\alpha = a + bi + cj + dk$, onde os coeficientes a, b, c, d se tomam agora nos números complexos. Mais adiante, ele deu uma definição geral: introduziu os *números hipercomplexos*, que são elementos da forma $\alpha = a_1e_1 + a_2e_2 + \cdots + a_ne_n$. Novamente, dois destes elementos se somam coeficiente a coeficiente e se multiplicam defini odutos das unidades básicas duas a duas, e extendendo distributivamente. Como o produto de duas unidades básicas deve ser novamente um elemento do mesmo conjunto, deve ser da forma:

$$e_ie_j = \sum_{k=1}^{n} \gamma_k(i,j)e_k.$$

Resulta assim que para dar a estrutura de álgebra a este conjunto basta escolher adequadamente os valores dos coeficientes $\gamma_k(i,j)$. Por causa disso, estes coeficientes são chamados de *constantes estruturais.*

Os fatos que relatamos até aqui constituem os primeiros passos no desenvolvimento da teoria de anéis. Paralelamente, outros desenvolvimentos es-

tavam sendo feitos no continente. Na sua célebre memória sobre a resolução de equações algébricas de 1771, Joseph Louis Lagrange tinha ressaltado a importância singular do estudo das permutações. Após as contribuições de Niels Heinrich Abel e Paolo Ruffini, coube a Evariste Galois, em 1832, no trabalho que deu origem à t hoje leva seu nome, introduzir efetivamente o conceito de *grupo de permutações* e definir algumas das noções fundamentais da área. Posteriormente, no período entre 1844 e 1846, Agustin Cauchy publicou uma sequência de trabalhos sobre grupos de permutações que deram a esta área uma vida independente da teoria das equações.

Finalmente, inspirado por estes trabalhos, e seguindo a tendência à abstração que era mais marcada na Inglaterra, Arthur Cayley publicou em 1854 un trabalho com o título *On the theory of groups as depending on the symbolic equation* $\theta^n = 1$ [7] que é considerado hoje como o artigo que deu origem à teoria *abstrata* de grupos. Trata-se de um trabalho relativamente curto, mas que introduz uma série de fatos fundamentais:

- Dá uma definição abstrata de grupo, utilizando uma notação multiplicativa.
- Introduz as *tabelas* da operação.
- Mostra que existem dois grupos não isomorfos de ordem quatro, e dá exemplos explícitos dos mesmos.
- Mostra que existem dois grupos não isomorfos de ordem seis, um deles comutativo e o outro não, provando que este último é isomorfo a S_3, o grupo das permutações de três elementos.
- Prova que a ordem de todo elemento é um divisor da ordem do grupo.

No início do artigo, quando está enfatizando que num grupo se trabalha com uma única operação, ele observa que, como está utilizando a notação multiplicativa, símbolos tais como 0 ou + não tem sentido neste contexto. Já no fim do artigo ele retoma esta questão e mostra como, a partir de um grupo, é possível construir um outro conjunto onde estes símbolos têm sentido. Para isso, ele imita, de certa forma, a construção dos sistemas hipercomplexos.

Vamos examinar sua idéia empregando uma notação atualizada. Dado o grupo G, enumera os seus elementos indexando-os: $g_1, g_2, \ldots, g_n$. Depois considera *combinações lineares formais* destes elementos; isto é, algo semelhante a "polinômios", não em potências de uma variável mas usando

os elementos do grupo: $a_1g_1 + a_2g_2 + \cdots + a_ng_n$. Note que se trata essencialmente da mesma construção dos sistemas hipercomplexos, com a única diferença que, em vez lizar símbolos quaisquer para as unidades básicas, ele se utiliza dos elementos de um dado grupo. Trata-se da primeira construção concreta de um *anel de grupo*. Claro que, como a teoria de anéis não estava ainda adequadamente desenvolvida, a noção de anel de grupo não tinha uma utilidade visível e caiu, por um tempo, no esquecimento. Vamos dar agora a definição explícita.

Definição 2.1 *Dados um grupo finito*[1] $G = \{g_1, g_2, \ldots, g_n\}$ *e um anel com unidade* R, *o* anel de grupo *de* G *sobre* R *é o conjunto*

$$RG = \{\sum_{i=1}^{n} r_i g_i \mid r_i \in R\},$$

com as operações definidas por:

$$\sum_{i=1}^{n} r_i g_i + \sum_{i=1}^{n} s_i g_i = \sum_{i=1}^{n} (r_i + s_i) g_i,$$

$$(\sum_{i=1}^{n} r_i g_i)(\sum_{i=1}^{n} s_j h_j) = \sum_{i,j} (r_i s_j)(g_i h_j).$$

verifica-se facilmente que, com estas operações, RG resulta um anel, com unidade.

Podemos definir ainda o produto de um elemento de RG por um escalar $\lambda \in R$ Por:

$$\lambda(\sum_{i=1}^{n} r_i g_i) = \sum_{i=1}^{n} (\lambda r_i) g_i.$$

Também é facil verificar que, com a soma definida acima e este produto por escalares, define-se em RG uma estrutura de R-módulo.

Note que a função $\varphi; G \to RG$ definida por:

$$g \in G \mapsto \varphi(g) = \sum_{i=1}^{n} r_i g_i \in RG$$

[1]Esta noção pode-se definir também no caso geral dos grupos infinitos, apenas nos restringimos ao caso finito para simplificar a exposição.

onde $r_i = 0$ se $g_i \neq g$ e $r_i = 1$ se $g_i = g$ é um monomorfismo. Identificando G com sua imagem $\varphi(G)$, nossas definições implicam imediatamente que G é uma base de RG quando considerado como módulo sobre R.

Dado um elemento $\alpha = \sum_{i=1}^{n} r_i g_i \in RG$, chama-se *suporte* de α ao conjunto de elementos de G que comparecem efetivamente na expressão de α; i.e.:

$$sup(\alpha) = \{g_i \in G \mid a_i \neq 0\}.$$

O conceito de anel de grupo reaparece nos trabalhos de Theodor Molien que, em 1898, dá um critério para decidir quando um sistema hipercomplexo pode se decompor como a soma direta de sistemas simples. Ao buscar aplicações para seu critério, ele redefine anéis de grupo e aplica esta noção para desenvolver a teoria de representações de grupos, chegando a descobrir inclusive as relações de ortogonalidade de caracteres por esta via. Mais uma vez, estas descobertas não ti nde impacto na coletividade matemática pois foram eclipsadas pelas descobertas simultâneas de resultados importantes na teoria das representações por William Burnside e Georg Frobenius cujos trabalhos tiveram ampla aceitação.

Finalmente, entre os anos de 1927 e 1929, numa série de três trabalhos [31], [6], [5] (sendo um deles em conjunto) Emmy Noether e Richard Brauer revolucionaram a teoria das representações ao descobrir sua íntima relação com a teoria de estrutura de álgebras. Justamente a conexão fundamental entre ambas as teorias é feita através do conceito de anel de grupo. A partir deste momento, esta noção veio a se tornar de grande importância na álgebra.

Cabe mencionar ainda que, em 1963, Ian G. Connell [9] publicou um trabalho em que trata de propriedades dos anéis de grupo do ponto de vista específico da teoria de anéis. A partir dali, esta noção adquiriu também importância como fonte de exemplos - e também de problemas - para a teoria de anéis.

3 O Problema do Isomorfismo

Fundamentalmente por causa da conexão com a teoria das representações, é muito natural se perguntar até que ponto o conhecimento da estrutura e propriedades de um dado anel de grupo pode determinar a estrutura do grupo dado. Mais formalmente, podemos nos colocar a seguinte pergunta:

Dados dois grupos G e H e um anel R, será que a existência de um isomorfismo $RG \cong RH$ implica que $G \cong H$?.

Esta questão tem, em geral, uma resposta negativa. Mostraremos, por exemplo, que se $R = \mathbb{C}$, o corpo dos números complexos e G e H são dois grupos abelianos de ordem n, mesmo que não isomorfos, tem-se que $\mathbb{C}G \cong \mathbb{C}H$.

Consideremos primeiro o caso em que $G =< a \mid a^n = 1 >$ é um grupo cíclico e seja K um corpo tal que $car(K) \nmid |G|$. Considere a função $\phi : K[X] \to KG$ dada por:

$$f \in K[X] \mapsto f(a) \in KG.$$

É muito fácil verificar que ϕ é um epimorfismo de anéis. Logo,

$$KG \cong \frac{K[X]}{Ker(\phi)}$$

onde $Ker(\phi) = \{f \in K[X] | f(a) = 0\}$.

Como $K[X]$ é um domínio principal, $Ker(\phi)$ é o ideal gerado pelo polinômio mônico f_0, de mínimo grau, tal que $f_0(a) = 0$. É importante notar que, neste isomorfismo, o elemento a corresponde com a classe $X + (f_0) \in \frac{K[X]}{(f_0)}$.

Como $a^n = 1$, segue que $X^n - 1 \in Ker(\phi)$. Note também que, se $f = \sum_{i=1}^{r} k_i X^i$ é um polinônio de grau $r < n$ temos que $f(a) = \sum_{i=1}^{r} k_i a^i \neq 0$ porque os elementos $\{1, a, a^2, \ldots, a^r\}$ são linearmente independentes sobre K. Logo $Ker(\phi) = (X^n - 1)$, donde:

$$KG \cong \frac{K[X]}{(X^n - 1)}.$$

Seja $X^n - 1 = f_1 f_2 \ldots f_t$ a decomposição de $X^n - 1$ como produto de polinômios irredutíveis em $K[X]$. Como estamos assumindo que $car(K) \nmid n$, este polinômio é separável em $K[X]$ portanto, $f_i \neq f_j$ se $i \neq j$. Usando o Teorema Chinês do Resto, podemos escrever:

$$KG \cong \frac{K[X]}{(f_1)} \oplus \frac{K[X]}{(f_2)} \oplus \cdots \oplus \frac{K[X]}{(f_t)}.$$

Neste isomorfismo, o elemeto a corresponde com a t-upla

$$(X + (f_1), \ldots, X + (f_t))$$

Agora, seja ζ_i uma raiz de f_i,$1 \leq i \leq t$. Então, temos que: $\frac{K[X]}{(f_i)} \cong K(\zeta_i)$. Consequentemente:

$$KG \cong K(\zeta_1) \oplus K(\zeta_2) \oplus \cdots \oplus K(\zeta_t.)$$

Como todos os elementos ζ_i , $1 \leq i \leq t$, são raízes de $X^n - 1$, provamos que *KG é isomorfo a uma soma direta de extensões de K por raízes da unidade.* Neste isomorfismo final, o elemento a corresponde com o elemento $(\zeta_1, \zeta_2, \ldots, \zeta_t)$.

Lembramos que, no caso particular em que $K = \mathbf{Q}$, o corpo dos números racionais, a decomposição em fatores irredutíveis de $X^n - 1$ é $X^n - 1 = \Pi_{d|n}\phi_d(X)$ onde o produto se toma sobre todos os divisores positivos d de n e $\phi_d(X)$ indica o *polinômio ciclotômico* de índice d que é o polinômio cujas raízes complexas são todas as raízes primitivas d-ésimas da unidade. Como cada quociente da forma $\mathbf{Q}[X]/(\phi_d(x))$ é isomorfo ao corpo $\mathbf{Q}(\zeta_d)$, onde ζ_d indica uma raiz primitiva d-ésima da unidade, provamos a seguinte.

Proposição 3.1 *Seja $G =< a \mid a^n = 1 >$ um grupo cíclico de ordem finita n. Então tem-se que:*

$$\mathbf{Q}G \cong \oplus_{d|n} \frac{\mathbf{Q}[X]}{(\phi_d(X))} \cong \oplus_{d|n} \mathbf{Q}(\zeta_d).$$

onde ζ_d indica uma raiz primitiva d-ésima da unidade, para cada divisor d de n. Neste isomorfismo, o elemento a corresponde ao elemento $\{\xi_d\}_{d|n} \in \oplus_{d|n}\mathbf{Q}(\zeta_d)$.

Antes de explorar mais um pouco estas observações, vamos computar alguns exemplos concretos.

Exemplos 3.2 $G =< a \mid a^7 = 1 >, K = \mathbf{Q}$.

Neste caso, a decomposição de $X^7 - 1$ em $\mathbf{Q}[X]$ é

$$X^7 - 1 = (X - 1)(X^6 + X^5 + X^4 + X^3 + X^2 + X + 1).$$

Logo, se ζ denota uma raiz primitiva da unidade de ordem 7, temos que:

$$\mathbf{Q}G \cong \mathbf{Q} \oplus \mathbf{Q}(\zeta).$$

Exemplos 3.3 $G =< a \mid a^6 = 1 >, K = \mathbf{Q}$.

A decomposição de $X^6 - 1$ como produto de polinômios irredutíveis de $\mathbf{Q}[X]$ é:

$$X^6 - 1 = (X-1)(X+1)(X^2+X+1)(X^2-X+1).$$

Logo:

$$\mathbf{Q}G \cong \mathbf{Q} \oplus \mathbf{Q} \oplus \mathbf{Q}(\frac{-1+i\sqrt{3}}{2}) \oplus \mathbf{Q}(\frac{1+i\sqrt{3}}{2}).$$

Aqui, $\frac{-1+i\sqrt{3}}{2}$ é uma raiz de X^2+X+1 e $\frac{1+i\sqrt{3}}{2}$ é uma raiz de X^2-X+1. O leitor deverá notar que, na verdade, os dois últimos somandos são iguais.

Note agora que, se $K = \mathbf{C}$, o corpo dos números complexos, então todo polinômio irredutível de $\mathbf{C}[X]$ é de primeiro grau e todos os quocientes da forma $\mathbf{C}[X]/(f_i)$ são isomorfos a $\mathbf{C}$ donde, se G é cíclico e $|G| = n$, temos que:

$$\mathbf{C}G \cong \underbrace{\mathbf{C} \oplus \cdots \oplus \mathbf{C}}_{n \text{ vezes}}.$$

Para estender este resultado para os grupos abelianos finitos em geral, precisamos de mais uma observação. Seja G um grupo que pode se escrever como produto direto de dois subgrupos $G = H \times N$ e seja K um corpo qualquer. Dado um elemento $\alpha \in KG$, enumerando os elementos de cada um destes subgrupos na forma $H = \{h_1, h_2, \ldots h_r\}$ e $N = \{n_1, n_2, \ldots, n_t\}$, podemos escrever α na forma $\alpha = \sum_{j=1}^{t} (\sum_{i=1}^{r} x_{ij} h_i)\, n_j$, com $x_{ij} \in K$. Chamando $\alpha_j = \sum_{i=1}^{r} x_{ij} h_i$ temos que $\alpha = \sum_{j=1}^{t} \alpha_j n_j$, com $\alpha_j \in KH$. A partir desta observação é facil demonstrar que:

$$K(H \times N) \cong (KH)N.$$

Em outras palavras, o anel de grupo sobre K do produto direto $H \times N$ é isomorfo ao anel de grupo do grupo N com coeficientes no anel KH.

Uma outra observação de que iremos necessitar e que decorre diretamente da definição de anel de grupo é a seguinte: se R é um anel que é soma direta de uma família de anéis $R = \oplus_{i \in \mathcal{I}} R_i$ tem-se que:

$$RG \cong \oplus_{i \in \mathcal{I}} (R_i G).$$

Finalmente estamos em condições de demonstrar a seguinte.

Proposição 3.4 *Seja G um grupo abeliano de ordem finita n. Então:*

$$\mathbf{C}G \cong \underbrace{\mathbf{C} \oplus \cdots \oplus \mathbf{C}}_{n \text{ vezes}}$$

Demonstração. De acordo com o teorema de estrutura para grupos abelianos finitos, podemos escrever G na forma $G = G_1 \times \cdots \times G_t$ onde G_i é um grupo cíclico, $1 \leq i \leq t$. Faremos a demonstração por indução em t.

Se $t = 1$ então G é cíclico e o resultado já foi demonstrado nesse caso. Suponha então que o resultado vale para um grupo que é um produto direto de $t-1$ grupos cíclicos. Escrevendo $G = G_1 \times \cdots \times G_{t-1} \times G_t$ temos que:

$$\begin{aligned} \mathbf{C}G &\cong (\mathbf{C}(G_1 \times \cdots \times G_{t-1}))\, G_t \cong (\mathbf{C} \oplus \cdots \oplus \mathbf{C})\, G_t \\ &\cong \mathbf{C}G_t \oplus \cdots \oplus \mathbf{C}G_t. \end{aligned}$$

Isto mostra que $\mathbf{C}G$ é isomorfo a uma soma direta de cópias de $\mathbf{C}$. Como a dimensão de $\mathbf{C}G$ como espaço vetorial sobre $\mathbf{C}$ é precisamente $n = |G|$, segue imediatamente que o número de somandos diretos é igual a n. $\diamondsuit$

Corolario 3.5 *Sejam G e H dois grupos abelianos da mesma ordem finita n. Então $\mathbf{C}G \cong \mathbf{C}H$.*

Demonstração. Com efeito, basta observar que:

$$\mathbf{C}G \cong \underbrace{\mathbf{C} \oplus \cdots \oplus \mathbf{C}}_{n \text{ vezes}}.$$

Como é fácil determinar grupos abelianos da mesma ordem, que não são isomorfos, o corolário acima mostra que o problema do isomorfismo tem resposta negativa quando se trabalha sobre $\mathbf{C}$.

Em 1950 S. Perlis e C. Walker [32] provaram que grupos abelianos finitos estão de fato determinados pelo seu anel de grupo sobre o corpo dos números racionais. Pouco depois, em 1956, W.E. Deskins [11] demonstrou que p-grupos abelianos finitos estavam determinados pelos seus anéis de grupo sobre quaisquer corpos de característica p. Houve também alguns resultados parciais sobre grupos não comutativos devidos a D.B. Coleman [8] e D.S. Passman [34] e [35].

Isto parecia sugerir que, para famílias específicas de grupos poder-se-ia determinar algum corpo adequado onde a resposta a questão tivesse sempre uma resposta positiva. Porém, em 1972, E. Dade [10] publicou um exemplo de dois grupos (que têm uma estrutura razoavelmente simples, já que são

grupos metacíclicos) não isomorfos, mas que têm anéis de grupo isomorfos sobre qualquer corpo K!

Isto levou a centralizar as atenções sobre os anéis de grupo sobre os inteiros, formulando-se a seguinte conjectura para grupos finitos quaisquer:

(ISO) $\qquad \mathbf{Z}G \cong \mathbf{Z}H \Longrightarrow G \cong H.$

Uma razão fundamental para voltar as atenções para esta questão é que pode-se demonstrar facilmente que se para dois grupos G e H tem-se que $\mathbf{Z}G \cong \mathbf{Z}H$, então também tem-se que $RG \cong RH$ para todo outro anel com unidade R. Resulta assim que esta hipótese é a mais forte que se pode formular, neste contexto.

Em apoio a esta conjectura sabia-se que em 1940, Graham Higman [17] tinha demonstrado que ela é verdadeira no caso dos grupos abelianos finitos e também no caso dos 2-grupos que são Hamiltonianos (isto é, quando todo subgrupo é normal). Até agora a conjectura, em todo sua generalidade, continua em aberto, mas ela já foi demonstrada numa série de casos particulares:

- Os grupos metabelianos finitos [49].
- Grupos simétricos e grupos alternados.
- Grupos finitos que são grupos de unidades de algum anel, por exemplo, os grupos do tipo $GL(n, F)$, onde F indica um corpo finito [47].
- Grupos nilpotentes finitos [50].

Parte II

O Grupo das Unidades

4 Introdução

Para motivar adequadamente a necessidade de estudar o grupo das unidades de um anel de grupo vamos fazer primeiro algumas considerações. Para isso, precisamos definir novos conceitos.

Definição 4.1 *A aplicação* $\varepsilon : \mathbf{Z}G \to \mathbf{Z}$ *dada por* $\sum_{i=1}^{n} r_i g_i \mapsto \sum_{i=1}^{n} r_i$ *(que é um homomorfismo) chama-se a* função de aumento *de* $\mathbf{Z}G$.

Definição 4.2 *Um isomorfismo* $\varphi : \mathbf{Z}G \to \mathbf{Z}H$ *diz-se um* isomorfismo normalizado *se, para todo elemento* $\alpha \in \mathbf{Z}G$ *tem-se que* $\varphi(\alpha) = \varepsilon(\varphi(\alpha))$ *(ou, equivalentemente, se para todo elemento* $g \in G$ *tem-se que* $\varepsilon(\varphi(g)) = 1$*).*

Se existe algum isomorfismo $\varphi : \mathbf{Z}G \to \mathbf{Z}H$ então também existe um isomorfismo normalizado entre estes anéis. De fato, basta definir uma nova aplicação $\psi : \mathbf{Z}G \to \mathbf{Z}H$ da seguinte forma: para cada elemento $\alpha = \sum_{i=1}^{n} r_i g_i \in \mathbf{Z}G$ definimos $\psi(\alpha) = \sum_{i=1}^{n} \varepsilon \circ \varphi(g_i)^{-1} r_i g_i$. (Note que, como $g \in G$ é inversível e como ε é um epimorfismo, tem-se que $\varepsilon \circ \varphi(g)$ é inversível em $\mathbf{Z}$: i.e., $\varphi(g) = \pm 1$). É fácil verificar que ψ é, de fato, um isomorfismo normalizado. Assim, toda vez que consideramos o problema do isomorfismo, não perdemos generalidade se supomos que o isomorfismo com que estamos trabalhando é normalizado.

Seja então $\varphi : \mathbf{Z}H \to \mathbf{Z}G$ um isomorfismo normalizado. Note que se $\varphi(g) \in H$, para todo elemento $g \in G$, então o próprio φ dá, por restrição, um isomorfismo entre os grupos H e G. Aliás, esta foi justamente a técnica empregada por Higman para demonstrar seus resultados que mencionamos na seção anterior. A grande dificuldade consiste precisamente em que, em geral, não temos maiores informações sobre os elementos da forma $\varphi(h)$, $h \in H$, porém, afirmar algumas coisas. Note que, como $|H| = n$, temos que $h^n = 1$ para todo $h \in H$ e, como φ é um morfismo, segue que também $\varphi(h)^n = 1$. Isto significa que $\varphi(h)$, $h \in H$, é sempre um elemento inversível, de ordem finita em $\mathbf{Z}G$. Isto justifica nossa próxima definição.

Definição 4.3 *Seja* G *um grupo finito. Definimos então:*

$$\mathcal{U}(\mathbf{Z}G) = \{\alpha \in \mathbf{Z}G \mid \alpha \text{ é inversível}\},$$

$$\mathcal{U}_1(\mathbf{Z}G) = \{\alpha \in \mathcal{U}\mathbf{Z}G) \mid \varepsilon(\alpha) = 1\}.$$

O primeiro conjunto é chamado de *grupo das unidades* de $\mathbf{Z}G$ e o segundo, que é um subgrupo normal do primeiro, de *grupo das unidades normalizadas* de $\mathbf{Z}G$.

É natural se perguntar então que informações podemos obter sobre o grupo das unidades normalizadas de $\mathbf{Z}G$ uma vez que um conhecimento adequado deste grupo poderia nos levar a soluções do problema do isomorfismo.

5 Unidades de ordem finita

Começaremos nosso estudo com um resultado, publicado em 1955 por S.D. Berman [3], que permite dar uma demonstração muito simples do teorema de G. Higman sobre isomorfismos de anéis de grupo abelianos e que tem também outras aplicações importantes.

Teorema 5.1 *Seja* $G = \{g_1 = 1, g_2, \ldots g_n\}$ *um grupo finito e seja* $\mu = \sum_{i=1}^{n} a_i g_i \in \mathcal{U}(\mathbf{Z}G)$ *uma unidade de ordem finita. Se* $a_1 \neq 1$ *então* $\mu = \pm 1$.

Demonstração. Vamos considerar $\mathbf{Z}G$ incluido em $\mathbf{C}G$. Para cada elemento $\alpha \in \mathbf{Z}G$, consideramos a função $T_\alpha : \mathbf{C}G \to \mathbf{C}G$ definida por $T_\alpha(x) = \alpha x$, $\forall x \in \mathbf{C}G$. Claramente, esta é uma função linear; i.e., ela verifica que $T_\alpha(rx + sy) = rT_\alpha(x) + rT_\alpha(y), \forall r, s \in \mathbf{C}$, $\forall x, y \in \mathbf{C}G$.

Vamos calcular o traço de T_μ a partir de sua matriz na base G de $\mathbf{C}G$. Para isso, devemos estudar a ação de T_μ em cada um dos elementos da base. Note que $T_\mu(1) = \mu 1 = \mu = \sum_{i=1}^{n} a_i g_i$. Logo, o elemento que está na posição $1,1$ da matriz de T_μ é precisamente o coeficiente a_1. Em geral, se consideramos um elemento $g_j \neq 1$ temos que $T_\mu(g_j) = \mu g_j = \sum_{i=1}^{n} a_i(g_i g_j)$. Para conhecer o elemento que está na posição j, j precisamos determinar o coeficiente de g_j na expressão de $T_\mu(g_j)$. Note que $g_i g_j = g_j$ só quando $g_i = 1$; logo o elemento procurado é novamente a_1. Este argumento mostra que todos os elementos da diagonal desta matriz são iguais a a_1 donde $tr(T_\mu) = na_1$.

Agora, vamos calcular o mesmo valor $tr(T_\mu)$ de outra forma. Note que como μ é de ordem finita, existe um inteiro positivo m tal que $\mu^m = 1$; logo $(T_m)^m = T_{\mu^m} = I$. Resulta assim que T_μ é raiz do polinômio $X^m - 1 = (X - \xi_1)(x - \xi_2) \cdot \cdots \cdot (X - \xi_m)$, onde $\xi_1, \xi_2, \ldots \xi_m$ denotam as raízes m-ésimas da unidade. Isto implica que T_μ é diagonalizável e que existe uma base de $\mathbf{C}G$ onde a matriz de T_μ é da forma:

$$A = \begin{bmatrix} \xi_1 & & & \\ & \xi_2 & & \\ & & \cdots & \\ & & & \xi_n \end{bmatrix}$$

Logo, comparando ambos os valores obtidos para $tr(T_\mu)$, temos que:

$$n\alpha_1 = \sum_{i=1}^{n} \xi_i,$$

donde

$$|n\alpha_1| = \left|\sum_{i=1}^{n} \xi_i\right| \leq \sum_{i=1}^{n} |\xi_i| = n.$$

Como $|na_1| = n|a_1| \geq n$ deve ser $|a_1| = 1$ e ainda, deve-se ter que $|\sum_{i=1}^{n} \xi_i| = \sum_{i=i}^{n} |\xi_i|$, o que só acontece se $\xi_1 = \xi_2 = \cdots = \xi_n$. Neste caso, temos que $A = \xi_1 I$ é uma matriz diagonal e, consequentemente, a matriz de T_μ na base G também é essa matriz diagonal.

Finalmente, é facil ver que se fosse $a_i \neq 0$ para algum índice $i \neq 1$, na i-ésima coluna da matriz de T_μ ter-se-ia um elemento não nulo fora da diagonal, o que é uma contradição. Logo, deve ser $a_i = 0$ para todo $i \neq 1$ e segue que $\mu = a_1 g_1 = a_1 1$. Como $|a_1| = 1$ temos que $a_1 = \pm 1$. ◇

Corolario 5.2 *Seja G um grupo finito. Se $\mu = \sum_{i=1}^{n} a_i g_i \in \mathcal{U}(\mathbf{Z}G)$ é tal que, para algúm elemento $g_i \in \mathcal{Z}(G)$ onde $\mathcal{Z}(G)$ denota o centro de G, tem-se que $a_i \neq 0$, então $\mu = \pm g_i$.*

Demonstração. Basta observar que μg_i^{-1} é ainda uma unidade de ordem finita cujo coeficiente de 1 é $a_i \neq 0$ e aplicar o Teorema acima. ◇

Em geral, as unidade da forma $\pm g$, $g \in G$ chamam-se *unidades triviais* de $\mathbf{Z}G$. No caso particular em que G é abeliano, todo elemento de G é central; isto nos permite concluir imediatamente o seguinte.

Corolario 5.3 *Seja G um grupo finito, abeliano. Então, toda unidade de ordem finita de $\mathbf{Z}G$ é trivial.*

Em outras palavras, se G é um grupo finito, temos que:

$$\mathcal{U}(\mathbf{Z}G) = \{\pm 1\} \times G,$$

$$\mathcal{U}_1(\mathbf{Z}G) = G.$$

Podemos dar agora uma demonstração muito simples do Teorema de Higman sobre isomorfismos de anéis de grupos abelianos.

Teorema 5.4 *Seja G um grupo finito e seja H um outro grupo tal que $\mathbf{Z}G \cong \mathbf{Z}H$. Então $G \cong H$.*

Demonstração. É claro que, se G é um grupo abeliano, então o anel $\mathbf{Z}G$ é comutativo, portante o anel $\mathbf{Z}H$ é comutativo e segue que H também é um grupo abeliano. Devido à invariância da dimensão dos módulos livres sobre $\mathbf{Z}$, segue imediatamente que H também é finito e que $|G| = |H|$.

Se $\mathbf{Z}G \cong \mathbf{Z}H$, tal como observamos anteriormente, podemos supor que existe um isomorfismo normalizado $\varphi : \mathbf{Z}G \to \mathbf{Z}H$. Para cada elemeto $g \in G$ temos que $\varphi(g)$ é uma unidade normalizada, de ordem finita, de $\mathbf{Z}H$. Pelo lema anterior, segue que $\varphi(g) \in \pm H$ e como φ é normalizado, segue que $\varphi(g) \in H$. Isto mostra que $\varphi(G) \subset H$ e como $|G| = |H|$ temos que $\varphi(G) = H$. Em outras palavras, a restrição de φ a G estabelece um isomorfismo de grupos entre G e H. ◇

6 Unidade cíclicas e bicíclicas

Tendo em vista os resultados da seção anterior e suas aplicações ao problema do isomorfismo, é natural se perguntar também quais são os grupos G tais que *todas* as unidades de $\mathbf{Z}G$ são triviais. A resposta a esta pergunta também é devida a G. Higman [17]. Os métodos que ele emprega na sua demonstração precisam de sofisticados resultados da teoria dos números e, em particular, do Teorema das Unidades de Dirichlet. Existe uma demonstração mais recente, devida a E. Jespers, M. Parmenter e P. Smith [25] que tem a vantagem adicional de utilizar um certo tipo de unidades especiais que têm sido de utilidade no estudo de muitos outros problemas da área. Na seção §3.2 mencionamos a mais importante destas aplicações. Vamos introduzir agora essas unidades e estudar algumas de sus prorpiedades.

Seja g um elemento de um grupo G, de ordem n. Denotaremos por $\widehat{g}$ o elemento:

$$\widehat{g} = 1 + g + g^2 + \cdots g^{n-1} \in \mathbf{Z}G.$$

Definição 6.1 *Seja G um grupo finito. Uma* unidade bicíclica *do anel de grupo $\mathbf{Z}G$ é um elemento da forma:*

$$\mu_{g,h} = 1 + (1-g)h\widehat{g}$$

onde g, h são elementos de G.

Note que $\widehat{g}(1-g) = 0$. Isto permite demonstrar facilmente, mediante um cálculo direto, que $\mu_{g,h}$ é de fato uma unidade, cujo inverso é:

$$\mu_{g,h}^{-1} = 1 - (1-g)h\widehat{g}.$$

Estas unidades desempenharam um papel fundamental no estudo de subgrupos de índice finito nos grupos de unidades de anéis de grupo. Veja, por exemplo, [39], [20] e [21].

Será muito importante saber quando estas unidades são triviais.

Lema 6.2 *Sejam g, h elementos de um grupo finito G. Então a unidade bicíclica $\mu_{g,h}$ é trivial se e somente se existe um inteiro positivo j tal que $h^{-1}gh = g^j$.*

Demonstração. Suponhamos que $h^{-1}gh = g^j$, para algum j. Note que $g^j\widehat{g} = \widehat{g}$. Como temos que $gh = hg^j$ resulta que $gh\widehat{g} = h\widehat{g}$. Substituindo na expressão de $\mu_{g,h}$ vem diretamente que $\mu_{g,h} = 1$.

Reciprocamente, suponhamos que $\mu_{g,h}$ é trivial. Como esta é uma unidade normalizada, deve existir um elemento $x \in G$ tal que $\mu_{g,h} = x$. Temos então que:

$$1 + (1-g)h\widehat{g} = x,$$

donde

$$1 + h(1 + g + g^2 + \cdots + g^{n-1}) = x + gh(1 + g + g^2 + \cdots + g^{n-1}).$$

Como o elemento 1 comparece no primeiro membro desta igualdade, ele deve aparecer também no segundo membro; logo, deve existir um inteiro positivo i tal que $1 = ghg^i$. Isto implica que $h = g^{-(i+1)}$ e segue que $h^{-1}gh$ é uma potência de g. ◇

Para introduzir mais um tipo de unidades, lembramos que o símbolo ϕ denota a chamada função *phi* de Euler; i.e., para um inteiro positivo n

define-se $\phi(n)$ como sendo o número de inteiros positivos menores que n e relativamente primos com ele. Lembramos que para calcular o valor de ϕ num inteiro positivo n basta decompor n como produto de fatores primos: $n = p_1^{n_1}.\cdots.p_t^{n_t}$. então, tem-se que:

$$\phi(n) = p_1^{n_1-1}(p_1-1).\cdots.p_t^{n_t-1}(p_t-1).$$

Uma propriedade interessante desta função é dada pelo chamado *Teorema de Euler*: se i e n são inteiros relativamente primos então $i^{\phi(n)} \equiv 1 \pmod{n}$.

Definição 6.3 *Seja g um elemento de ordem n de um grupo finito G. Uma* unidade cíclica de Bass *é um elemento do anel de grupo $\mathbf{Z}G$ da forma:*

$$\mu_i = (1 + g + \cdots + g^{i-1})^{\phi(n)} + \frac{1 - i^{\phi(n)}}{n}\widehat{g},$$

onde i é um inteiro tal que $1 < i < n$ e $mdc(i,n) = 1$.

Naturalmente, deve-se mostrar que uma unidade cíclica de Bass é, de fato, uma unidade. Isto pode ser feito diretamente exibindo sua inversa, que é da forma:

$$\mu = (1 + g + \cdots + g^{i(k-1)})^{\phi(n)} + \frac{1 - k^{\phi(n)}}{n}\widehat{g},$$

onde k é um inteiro tal que $1 < k < n$ e $n|(1-ik)$. Damos a seguir uma outra demonstração que é mais informativa e mostra a relação destas unidades com unidades de anéis de inteiros ciclotômicos. Para isso, vamos introduzir mais alguns conceitos e demonstrar alguns fatos razoavelmente elementares.

Definição 6.4 *Seja A uma $\mathbf{Q}$-álgebra. Um subanel unitário R de A diz-se uma* $\mathbf{Z}$-ordem, *ou simplesmente uma* ordem *em A se R é finitamente gerado como $\mathbf{Z}$-módulo e $\mathbf{Q}R = A$.*

Exemplos

- Se G é um grupo finito, então $\mathbf{Z}G$ é uma ordem em $\mathbf{Q}G$.
- Se $\mathcal{O}$ é o anel dos inteiros de um corpo de números algébricos K, então $\mathcal{O}$ é uma ordem em K e $M_2(\mathcal{O})$ é uma ordem em $M_2(K)$.

Lema 6.5 *Sejam $R_1 \subset R_2$ ordens de uma $\mathbf{Q}$-álgebra A. Então, existe um inteiro d tal que $dR_2 \subset R_1$. Ainda, considerando R_1 e dR_2 como grupos aditivos, tem se que o índice $[R_1 : dR_2]$ é finito.*

Demonstração. De acordo com a definição, R_2 é finitamente gerado como $\mathbf{Z}$-módulo; seja $\{\gamma_1, \ldots, \gamma_t\}$ um conjunto de geradores. Como $A = \mathbf{Q}R_1$ podemos escrever cada elemento γ_i na forma:

$$\gamma_i = \sum_j \frac{x_{ij}}{y_{ij}} r_j,$$

onde $r_j \in R_1$. Chamando $d_i = \Pi_j y_{ij}$ temos que $\gamma_i = \frac{1}{d_i} \sum_{i,j} \frac{d_i x_{ij}}{y_{ij}} r_j$ onde $\frac{d_i x_{ij}}{y_{ij}} \in \mathbf{Z}$. Assim, se denotamos $\alpha_i = \sum_{i,j} \frac{d_i x_{ij}}{y_{ij}} r_j$, resulta que $\gamma_i = \frac{1}{d_i} \alpha_i$ com $\alpha_i \in R_1$.

Seja agora $d = \Pi_i d_i$. Temos então que $d\gamma_i \in R_1$, $1 \leq i \leq t$. Finalmente, note que dado um elemento arbitrário $\alpha \in R_2$, ele pode-se escrever na forma $\alpha = \sum_{i=1}^t x_i \gamma_i$, onde $x_i \in \mathbf{Z}$, $1 \leq i \leq t$. Desta forma tem-se que $d\alpha = \sum_{i=1}^t x_i d\gamma_i \in R_1$; isto é, $dR_2 \subset R_1$.

Como R_2 é um $\mathbf{Z}$-módulo finitamente gerado, considerado como grupo aditivo ele é da forma $R_2 = F \oplus T$ onde F é um $\mathbf{Z}$-módulo livre de posto finito e T um grupo abeliano finito; logo, podemos escrever:

$$R_2 \cong \mathbf{Z} \oplus \cdots \oplus \mathbf{Z} \oplus T,$$

onde os somandos diretos isomorfos a $\mathbf{Z}$ estão em número finito. Temos então que:

$$dR_2 \cong d\mathbf{Z} \oplus \cdots \oplus d\mathbf{Z} \oplus dT,$$

donde

$$\frac{R_2}{dR_2} \cong \frac{\mathbf{Z}}{d\mathbf{Z}} \oplus \cdots \oplus \frac{\mathbf{Z}}{d\mathbf{Z}} \oplus \frac{T}{dT}.$$

Isto mostra que $[R_2 : dR_2] = |R_2/dR_2|$ é finito. Finalmente, como $R_1 \subset R_2$ temos que $[R_1 : dR_2] \leq [R_2 : dR_2]$ também é finito. $\diamondsuit$

Vamos resumir uma série de fatos bem conhecidos sobre as ordens no nosso próximo lema. Como antes, dado um anel R, o símbolo $\mathcal{U}(R)$ denotará o grupo das unidades de R; i.e., o conjunto de todos os elementos inversíveis de R.

Lema 6.6 *Sejam R_1 e R_2 duas ordens de uma* $\mathbf{Q}$*-álgebra A. Então:*

1. *$R_1 \cap R_2$ é uma ordem em A.*
2. *O índice $[\mathcal{U}(R_1) : \mathcal{U}(R_1 \cap R_2)]$ é finito.*
3. *Se um subanel unitário R de A é finitamente gerado como* $\mathbf{Z}$*-módulo e $R_1 \subset R$, então R é uma ordem em A.*
4. *Se $R_2 \subset R_1$ e $u \in R_2$ é inversível em R_1, então $u^{-1} \in R_2$.*

Demonstração. A demonstração dos itens (1) e (3) é imediata.

Para demonstrar (2) vamos denotar $R_1 \cap R_2 = R$. De acordo com o lema 6.5, existe um inteiro d tal que $dR_1 \subset R$ e, quando tomamos R e dR_1 como grupos aditivos, temos que $[R : dR_1]$ é finito. Consideremos então os grupos multiplicativos $\mathcal{U}(R_1)$ e $\mathcal{U}(R)$. Para demonstrar que o índice $[\mathcal{U}(R_1) : \mathcal{U}(R)]$ é finito, vamos provar que ele é limitado pelo índice $[R : dR_1]$. Com efeito, sejam $x, y \in \mathcal{U}(R_1)$ tais que $x + dR_1 = y + dR_1$. Então temos que $x - 1 \in dR_1 \subset R$ e portanto $y^{-1}x \in \mathcal{U}(R)$ o que implica que $x \in y\mathcal{U}(R)$. Este argumento mostra que se dois elementos estão na mesma classe aditiva módulo dR_1 então também estão na mesma classe multiplicativa módulo $\mathcal{U}(R)$; portanto, as classes laterais de $\mathcal{U}(R)$ estão formadas por reunião de classes aditivas módulo dR_1, o que prova nossa afirmação.

Finalmente, vamos demonstrar (4). Note que, se $u \in R_2$ é inversível em R_1 então temos que $R_1 = uR_1$. Considerando estas álgebras com sua estrutura aditiva, temos que $[R_1 : uR_2] = [uR_1 : uR_2]$. Agora, dados $x, y \in R_1$, se $ux \in uy + uR_2$, já que u é inversível em R_1 segue que $x \in y + R_2$. Isto mostra que, se $x_1, \ldots, x_r$ são todos os representantes de classes de R_2 em R_1, os elementos $ux_1, \ldots, ux_r$ certamente representam classes diferentes de uR_2 em uR_1, donde

$$[R_1 : R_2] \leq [R_1 : uR_2].$$

A desigualdade de sentido contrário é imediata, logo $uR_2 = R_2$. Como $1 \in R_2$ segue facilmente que u é inversível em R_2. ◇

Seja agora g um elemento de ordem n num grupo finito G. Sejam ainda i um inteiro tal que $1 < i < n$ com $mdc(i, n) = 1$ e ξ_n uma raiz primitiva n-ésima da unidade. Como antes, vamos denotar por $\mathbf{Q}(\xi_n)$ a extensão de $\mathbf{Q}$ pelo elemento ξ_n e vamos indicar por $\mathbf{Z}[\xi_n]$ o subanel de $\mathbf{Q}(\xi_n)$ gerado por ξ_n. Note que o elemento

$$\frac{\xi_n^i - 1}{\xi_n - 1} = 1 + \xi_n + \cdots + \xi_n^{i-1}$$

pertence a $\mathbf{Z}[\xi_n]$ e é inversível nesse anel, já que seu inverso é:

$$\frac{\xi_n - 1}{\xi_n^i - 1} = \frac{\xi_n^{ik} - 1}{\xi_n^i - 1} = 1 + \xi_n^i + \cdots + \xi_n^{i(k-1)},$$

onde k é um inteiro tal que $ik \equiv 1 \pmod{n}$.

De acordo com a Proposição 3.1 podemos escrever:

$$\mathbf{Q} < g > \cong \oplus_{d|n} \mathbf{Q}(\xi_n^d).$$

(Note que ξ_n^d é uma raiz primitiva da unidade de ordem n/d; assim, quando d percorre o conjunto de todos os divisores positivos de n tem-se que ξ_n^d também percorre o conjunto de todas as raízes primitivas da unidade de ordens divisores de n). No isomorfismo acima, o elemento g corresponde ao elemento:

$$\{\xi_n^d\}_{d|n} \in \oplus_{d|n} \mathbf{Q}(\xi_n^d).$$

Vamos denotar $R = \oplus_{d|n} \mathbf{Z}[\xi_n^d]$. Seja $v = 1 + g + \cdots + g^i \in \mathbf{Z}G$. Então a projeção de v em cada componente de R é uma unidade, exceto no caso em que $d = n$ quando vale precisamente i. Como $mdc(i, n) = 1$, do Teorema de Euler segue que $i^{\phi(n)} = 1 + tn$ para algum $t \in \mathbf{Z}$. Consideramos então

$$u = (1 + g + \cdots + g^{i-1})^{\phi(n)} - t\widehat{g}.$$

Note que a projeção de $\widehat{g}$ em qualquer componente $\mathbf{Q}(\xi_n^d)$, com $d \neq n$, é 0, logo a projeção de u continua sendo uma unidade. Ainda, a projeção de $\widehat{g}$ no caso $d = n$ é precisamente n donde a projeção de u é $i^{\phi(n)} - tn = 1$. Assim, a projeção de $u \in \mathbf{Z} < g >$ em *todas* as componentes de $\mathbf{Q} < g >$ é uma unidade; logo $u \in \mathbf{Z} < g >$ é uma unidade em $\mathbf{Q} < g >$ e, de acordo com o lema 6.6 também é uma unidade de $\mathbf{Z} < g > zG$.

Como $t = (1 - i^{\phi(n)})/n$, este argumento prova que, de fato, as unidades cíclicas de Bass são unidades de $\mathbf{Z}G$.

Vamos dar agora um critério para decidir quando as unidades cíclicas de Bass são não triviais.

Lema 6.7 *Seja g um elemento de ordem n num grupo finito G e seja i um inteiro tal que $1 < i < n$ e $mdc(i, n) = 1$. Se $i \not\equiv \pm 1 \pmod{n}$ então a unidade cíclica de Bass*

$$u = (1 + g + \cdots + g^{i-1})^{\phi(n)} - \frac{1 - i^{\phi(n)}}{n}\widehat{g}.$$

não é trivial.

Demonstração. Suponhamos, por absurdo, que u é trivial. Como o suporte de u só contém potências de g, se u é trivial deve existir um inteiro positivo j tal que $u = g^j$. Seja $m = \phi(n)$. Se

$$(1 + g + \cdots + g^{i-1})^m - \frac{1 - i^m}{n}\widehat{g} = g^j$$

multiplicando por $(1-g^m)$ temos que $(1-g^m)(1+g+\cdots+g^{i-1})^m = (1+g^i)^m$ e $(1-g^m)\widehat{g} = 0$, obtemos que $(1-g^i)^m = (1-g^i)g^j$ donde segue a igualdade:

$$1 - mg^i + \binom{m}{2}g^{2i} + \cdots + (-1)^i g^{im} = g^j - mg^{j+1} + \binom{m}{2}g^{j+2} + \cdots + (-1)^m g^{j+m}.$$

Como $1 < i < n$ claramente temos que $n > 2$ donde $m = \phi(n)$ é par. Ainda, note que a hipótese $i \not\equiv \pm 1 \pmod{m}$ implica que $n > 4$ e portanto $m > 2$.

Como as potências de g no primeiro membro desta igualdade são todas diferentes, resulta que o elemento 1 aparece efetivamente nesse primeiro membro, com coeficiente igual a 1. Logo, deve comparecer também no segundo membro e também com coeficiente igual a 1. Temos portanto duas possibilidades: ou $g^j = 1$ ou $g^{j+m} = 1$.

Consideremos primeiro o caso em que $g^j = 1$. Comparando então os elementos de ambos os membros que têm coeficiente igual a m segue que $g^i = g$ ou $g^i = g^{m-1}$. Porém, nossa hipótese sobre i implica que a primeira possibilidade não pode acontecer; logo, deve ser $g^i = g^{m-1}$. Nesse caso, temos que $g^{2i} = g^{2m-2}$. Comparando agora somandos com coeficiente igual a $\binom{m}{2}$, e lembrando que $g^{2m-2} \neq g^{m-2}$ (pois $n \nmid m$), conclui-se que $g^{2m-2} = g^{2i} = g^2$. Isto que $n \mid (2m-4)$. Como $2 < m < n$ deve ser $n = 2m - 4$; logo n é par e tem-se que $m = \phi(n) \leq \frac{n}{2}$. Como $m = \frac{n-4}{2} > \frac{n}{2}$ temos uma contradição.

No caso em que $g^{j+m} = 1$, comparando novamente termos com coeficiente igual a m em ambos membros da igualdade, temos que $g^i = g^{j+1} = g^{j+m+1-m} = g^{1-m}$ ou $g^i = g^{j+m-1} = g^{-1}$. Como nossa hipótese sobre i implica que este último caso não pode acontecer, deve-se ter que $g^i = g^{1-m}$ o que implica que $g^2 i = g^{2-2m} \neq g^{2-m}$. Logo, comparando agora os termos que têm coeficiente igual a $\binom{m}{2}$ segue que $g^{2i} = g^{-2}$. Novamente isto implica que $n \mid \frac{n}{2}$ o que leva à mesma contradição. ◊

7 Unidades triviais

Com os elementos introduzidos na seção anterior, estamos agora em condições de caracterizar os grupos finitos G tais que o anel de grupo $\mathbf{Z}G$ tem apenas unidades triviais. O primeiro passo nesse sentido tem agora uma demonstração muito simples.

Lema 7.1 *Seja G um grupo finito tal que $\mathcal{U}_1(\mathbf{Z}G) = G$. Então todo subgrupo de G é normal.*

Demonstração. Para demonstrar a afirmação bastará provar que todo subgrupo cíclico de G é normal. Suponhamos, por absurdo, que existe um subgrupo cíclico $< g >$ que não é normal .Então existe $h \in G$ tal que $h^{-1}gh \notin < g >$ e segue do Lema 6.2 que a unidade bicíclica $u = 1+(1-g)h\widehat{g}$ não é trivial. $\diamondsuit$

Obviamente, se um grupo é abeliano então todos os seus subgrupos são normais. Lembramos que um grupo não abeliano tal que todo subgrupo é normal chama-se um *grupo Hamiltoniano* e que estes grupos são bem conhecidos. Em particular, sabe-se que se G é um grupo finito Hamiltoniano então ele é da forma:

$$G = \mathcal{Q}_8 \times A \times B,$$

onde A é um grupo abeliano 2-elementar (i.e., todo elemento $a \neq 1$ de A é de ordem 2), B é um grupo abeliano de ordem ímpar e $\mathcal{Q}_8$ é o *grupo quatérnio de ordem* 8; isto é, o grupo

$$\mathcal{Q}_8 = < a, b \mid a^4 = 1, a^2 = b^2, bab^{-1} = a^{-1} > .$$

Note que um grupo Hamiltoniano é um 2-grupo se e somente se $B = \{1\}$, ou seja, se é da forma $G = \mathcal{Q}_8 \times A$.

Proposição 7.2 *Seja G um grupo finito tal que $\mathcal{U}_1(\mathbf{Z}G) = G$. Então G é um grupo abelano de expoente igual a $1, 2, 3, 4$ ou 6 ou um 2-grupo Hamiltoniano.*

Demonstração. Do lema anterior segue que G é abeliano ou Hamiltoniano. Suponhamos inicialmente que G é abeliano. Se o seu expoente é diferente de $1, 2, 3, 4$ ou 6 então G contem um elemento de ordem n tal que $n = 5$ ou $n > 6$. em ambos os casos tem-se que $\phi(n) > 2$ e o Lema 6.7 mostra que G contém uma unidade cíclica de Bass que não é trivial.

Da mesma forma, se G é Hamiltoniano mas não é um 2-grupo então G contém um elemento $x \in B$ de ordem $p \neq 2$. Então o elemento $g = ax$ tem ordem $n = 4p$ e novamente temos que $\phi(n) > 2$, logo também neste caso G contém uma unidade cíclica de Bass que não é trivial. $\diamondsuit$

Na verdade, a condição obtida na proposição acima também é suficiente. Isso será demonstrado numa série de passos.

Lema 7.3 *Seja G um grupo finito tal que as unidades de $\mathbf{Z}G$ são triviais e seja C_2 um grupo cíclico. Então as unidades de $\mathbf{Z}(G \times C_2)$ também são triviais.*

Demonstração. Seja $C_2 =< a \mid a^2 = 1 >$. Como $\mathbf{Z}(G \times C_2) \cong (\mathbf{Z}G)C_2$, um elemento $u \in \mathbf{Z}(G \times C_2)$ pode-se escrever na forma $u = \alpha + \beta a$ onde $\alpha, \beta \in \mathbf{Z}G$.

Se u é uma unidade, existe um outro elemento $u^{-1} = \gamma + \delta a$ tal que

$$(\alpha + \beta a)(\gamma + \delta a) = (\alpha\gamma + \beta\delta) + (\alpha\delta + \beta\gamma)a = 1,$$

logo,

$$\begin{aligned} \alpha\gamma + \beta\delta &= 1 \\ \alpha\delta + \beta\gamma &= 0 \end{aligned}$$

Então, temos que:

$$\begin{aligned} (\alpha + \beta)(\gamma + \delta) &= \alpha\gamma + \beta\delta + \alpha\delta + \beta\gamma = 1 \\ (\alpha - \beta)(\gamma - \delta) &= \alpha\gamma + \beta\delta - (\alpha\delta + \beta\gamma) = 1 \end{aligned}$$

o que mostra que $\alpha + \beta$ e $\gamma + \delta$ são unidades de $\mathbf{Z}G$ e consequentemente são triviais. Devem existir então dois elementos $g_1, g_2 \in G$ tais que:

$$\alpha + \beta = \pm g_1, \quad \alpha - \beta = \pm g_2.$$

Portanto temos que $\alpha = \frac{1}{2}(\pm g_1 \pm g_2)$ e como os coeficientes de α devem ser inteiros, segue que $g_1 = g_2$ e $\alpha = \pm g_1$.

Assim, temos que:

$$\alpha + \beta = \alpha - \beta = \pm g_1,$$

ou

$$\alpha + \beta = -(\alpha - \beta) = \pm g_1.$$

No primeiro caso vem que $\alpha = \pm g_1$ e $\beta = 0$ e no segundo que $\alpha = 0$ e $\beta = \pm g_1$. Em ambos os casos temos que u é trivial. $\Diamond$

Lema 7.4 *As unidades do anel de grupo* $\mathbf{Z}\mathcal{Q}_8$ *são triviais.*

Demonstração. Podemos escrever explicitamente todos os elementos de $\mathcal{Q}_8$:

$$\mathcal{Q}_8 = \{1, a, b, ab, a^2, a^3, a^2b, ab^3\}.$$

Logo, todo elemento α de $\mathbf{Z}\mathcal{Q}_8$ é da forma:

$$\alpha = x_0 + x_1a + x_2b + x_3ab + y_0a^2 + y_1a^3 + y_2a^2b + y_3a^3\beta.$$

Consideremos agora o anel dos quatérnios inteiros; isto é, o anel:

$$\mathbf{H} = \{m_o + m_ii + m_2j + m_3k \mid m_0, m_1, m_2, m_3 \in \mathbf{Z}\}.$$

É facil demonstrar que as únicas unidades de $\mathbf{H}$ são ± 1, $\pm i$, $\pm j$, $\pm k$ (veja por exemplo [16, Lema 7.12]).

Pode-se definir um epimorfismo $\varphi : \mathbf{Z}\mathcal{Q}_8 \to \mathbf{H}$ por

$$\alpha \mapsto (x_0 - y_0) + (x_1 - y_1)i + (x_2 - y_2)j + (x_3 - y_3)k.$$

Se α é uma unidade de $\mathbf{Z}\mathcal{Q}_8$ então $\varphi(\alpha)$ é uma unidade de $\mathbf{H}$; logo, para algúm índice i, $0 \leq i \leq 3$, deve ser:

$$\begin{aligned} x_i - y_i &= \pm 1, \\ x_j - y_j &= 0 \quad \text{se} \quad i \neq j. \end{aligned}$$

Por outro lado, é fácil ver que a^2 é central e que $\mathcal{Q}_8/ < a^2 > \cong C_2 \times C_2$. Se denotamos por $\overline{g}$ a classe de um elemento $g \in \mathcal{Q}_8$ no quociente e por $\varphi : \mathbf{Z}\mathcal{Q}_8 \to \mathbf{Z}(\mathcal{Q}_8/ < a^2 >)$ a extensão da projeção canônica $\mathcal{Q}_8 \to \mathcal{Q}_8/ < a^2 >$ a todo $\mathbf{Z}\mathcal{Q}_8$, por linearidade, temos que:

$$\varphi(\alpha) = (x_0 + y_0) + (x_1 + y_1)i + (x_2 + y_2)j + (x_3 + y_3)k.$$

Do lema anterior temos que as unidades de $\mathbf{Z}(C_2 \times C_2)$ são triviais, logo, para algum índice h, $0 \leq h \leq 3$, deve ser:

$$\begin{aligned} x_h + y_h &= \pm 1 \\ x_k + y_k &= 0 \quad \text{se} \quad h \neq k \end{aligned}$$

Como os coeficientes são números inteiros, comparando os sistemas de equações obtidos acima é facil ver que deve ser $i = h$ e

$$x_i = \pm 1, \quad y_i = 0, \quad x_j = y_j = 0 \text{ se } j \neq i,$$

ou

$$x_i = 0, \quad y_i = \pm 1, \quad x_j = y_j = 0 \text{ se } j \neq i.$$

Em ambos os casos temos que α é uma unidade trivial de $\mathbf{Z}Q_8$. $\Diamond$

Note que os lemas 7.3 e 7.4 já mostram que se G é um 2-grupo Hamiltoniano ou um 2-grupo abeliano elementar então as unidades de $\mathbf{Z}G$ são triviais.

Lema 7.5 *Seja* $G =< a \mid a^3 = 1 >$ *um grupo cíclico de ordem* 3. *Então* $\mathcal{U}_1(\mathbf{Z}G) = G$.

Demonstração. Mostraremos inicialmente que se ξ denota uma raiz cúbica da unidade, então as únicas unidades do anel $\mathbf{Z}[\xi]$ são $\pm 1, \pm\xi, \pm\xi^2$.

Note que o polinômio minimal de ξ é $X^2 + X + 1$; logo todo elemento $\alpha \in \mathbf{Z}[\xi]$ é da forma $\alpha = a + b\xi$, com $a, b \in \mathbf{Z}$. Suponhamos que α é uma unidade de $\mathbf{Z}[\xi]$. Como a função $f : \mathbf{Z}[\xi] \to \mathbf{Z}[\xi]$ definida por $f(x + y\xi) = x + y\xi^2$ é um automorfismo, segue que $\alpha' = a + b\xi^2$ também é uma unidade e portanto

$$\begin{aligned} \alpha\alpha' &= (a + b\xi)(a + b\xi^2) = a^2 + b^2 + ab(\xi + \xi^2) \\ &= a^2 + b^2 - ab \end{aligned}$$

é uma unidade. Como $\alpha\alpha' \in \mathbf{Z}$ deve ser $a^2 + b^2 - ab = \pm 1$. Suponhamos que $a \geq b$. Se $b \neq 0, 1$ tem-se que $a^2 + b^2 > ab \pm 1$. Se $b = 0$ segue que $\alpha = a \in \mathbf{Z}$ é uma unidade, logo $\alpha = \pm 1$. Se $b = 1$ temos $a^2 + 1 = a \pm 1$ o que implica $a^2 = a$ ou $a^2 - a + 2 = 0$. No primeiro caso temos que $a = 0$

ou $a = 1$ e no segundo caso a equação não tem soluções inteiras. Se $a = 0$ temos que $\alpha = b\xi$ e como $|\alpha| = 1$, segue que $\alpha = \pm\xi$. Se $a = b = 1$ temos que $\alpha = 1 + \xi = -\xi^2$. O caso leva a um resultado semelhante.

Agora consideremos o epimorfismo $\varphi : \mathbf{Z}G \to \mathbf{Z}[\xi]$ definido por $x_0 + x_1a + x_2a^2 \mapsto x_0 + x_1\xi + x_2\xi^2$.

Seja $v = x_0+x_1a+x_2a^2$ uma unidade de G. Como $\varepsilon(v) = x_0+x_1+x_2 = 1$, temos que:

$$\begin{aligned} v - 1 &= x_0 + x_1a + x_2a^2 - (x_0 + x_1 + x_2) = x_1(a-1) + x_2(a^2-1) \\ &= x_1(a-1) + x_2(a-1)(a+1) = (a-1)(x_1 + x_2 + x_2a) \end{aligned}$$

Assim, chamando $y_0 = x_1 + x_2$, $y_1 = x_2$ podemos escrever v na forma:

$$v = 1 + (a-1)(y_0 + y_1a).$$

Agora calculamos:

$$\varphi(v) = 1 + (1-\xi)(y_0 + y_1\xi) = \pm 1 + (y_0 + y_1) + (2y_1 - y_0)\xi.$$

Como $\varphi(v)$ deve coincidir com uma das unidades de $\mathbf{Z}[\xi]$, a saber $\pm 1, \pm\xi, \pm\xi^2 = \pm(-\xi - 1)$ temos três possibilidades:

Caso(i)

$$\begin{aligned} 1 + (y_0 + y_1) &= \pm 1, \\ (2y_1 - y_0) &= 0. \end{aligned}$$

Somando ambas as equações temos que $3y_1 = -2$ ou $3y_1 = 0$. A primeira equação não tem solução em $\mathbf{Z}$ e a segunda implica $y_1 = 0$, donde $y_2 = 0$ e portanto $x_1 = x_2 = 0$, consequentemente $v = 1$.

Caso(ii)

$$\begin{aligned} \pm 1 + (y_0 + y_1) &= 0, \\ (2y_1 - y_0) &= \pm 1. \end{aligned}$$

Neste caso, uma análise semalhante mostra que $v = a$.

Caso(iii)

$$\begin{aligned} \pm 1 + (y_0 + y_1) &= (2y_1 - y_0). \\ (2y_1 - y_0) &= \pm 1. \end{aligned}$$

Da primeira equação vem que $y_1 - 2y_0 = 1$ e, somando com a segunda, temos que $3(y_1 - y_0) = 2$ ou $y_1 - y_0 = 0$. Novamente, a primeira equação não tem solução em $\mathbf{Z}$, a segunda implica que $y_1 = y_0$ e, voltando ao sistema inicial, segue que $y_1 = -1$; donde $x_1 = 0$ e $x_2 = -1$. Isto implica que $v = a^2$, o que completa nossa demonstração. $\diamondsuit$

Lema 7.6 *Seja $G = C_3 \times \cdots \times C_3$, onde C_3 denota um grupo cíclico de ordem 3. Então $\mathcal{U}_1(\mathbf{Z}G) = G$.*

Demonstração. Faremos a demonstração por indução no número de fatores diretos de G, que denotaremos por t. Se $t = 1$ a afirmação é verdadeira, pois foi provada no lema anterior.

Suponhamos então que o resultado vale para grupos que podem se escrever como o produto direto de no máximo $t-1$ grupos cíclicos de ordem 3. Vamos escrever G na forma $G = A \times < a > \times < b >$ onde $a^3 = b^3 = 1$ e A é um produto direto de $t-2$ grupos cíclicos de ordem 3 (ou, eventualmente, $A = \{1\}$).

Seja $v \in \mathbf{Z}G$ uma unidade. Como no lema anterior, podemos escrever v na forma

$$v = 1 + (1 - b)(y_0 + y_1 b),$$

onde $y_0, y_1 \in \mathbf{Z}A \times < a > \cong (\mathbf{Z}A) < a >$. Consequentemente, existem $\gamma_i, \delta_j \in \mathbf{Z}A$, $0 \leq i, j \leq 2$, tais que:

$$v = 1 + (1 - b)[(\gamma_0 + \gamma_i a + \gamma_2 a^2) + (\delta_0 + \delta_1 a + \delta_2 a^2 0).$$

O grupo $G/ < a, b >$ tem posto $t - 1$, logo a imagem de v em $\mathbf{Z}(G/ < a, b >)$ deve ser trivial. Como $b = a^2 ab$, essa imagem é:

$$\begin{aligned} \overline{v} &= 1 + (1 - b)[(\gamma_0 + \gamma_1 a + \gamma_2 a^2) + (\delta_0 + \delta_1 a + \delta_2 a^2)a^2] \\ &= 1 + \gamma_0 + \gamma_1 + \delta_1 - \delta_2 + (\gamma_1 - \gamma_2 + \delta_2 + \delta_0)a + (\gamma_2 - \gamma_0 + \delta_o - \delta_1)a^2. \end{aligned}$$

Consequentemente, dois destes coeficientes devem ser iguais a 0. Temos que considerar então três casos possíveis.

Caso (i): $\gamma_1 - \gamma_2 + \delta_2 - \delta_0 = \gamma_2 - \gamma_0 + \delta_0 - \delta_1 = 0$.

Como $G/ < a^2 b >$ também tem posto $t - 1$, a imagem de v em $\mathbf{Z}(G/ < a^2 b >)$ também deve ser uma unidade trivial. Essa imagem é

$$\begin{aligned}\tilde{v} &= 1+(1-a)[\gamma_0+\gamma_1 a+\gamma_2 a^2+(\delta_0+\delta_1 a+\delta_2 a^2)a] \\ &= 1+\gamma_0-\gamma_2+\delta_2-\delta_1+(\gamma_1=\gamma_0+\delta_0-\delta_2)a+(\gamma_2-\gamma_1+\delta_1-\delta_0)a^2 \\ &= (1+\delta_0-2\delta_1+\delta_2)+(\gamma_0+\gamma_1-2\delta_2)a+(-2\gamma_o+\gamma_1+\gamma_2)a^2.\end{aligned}$$

Como só um destes três coeficientes pode ser diferente de 0 sabemos que ou o segundo ou o terceiro coeficiente seguramente é 0. Note que ambas as situações implicam que o primeiro coeficiente é congruente a 1, módulo 3. Logo tanto o segundo como o terceiro coeficientes devem ser iguais a 0 e isto implica que $\gamma_0=\gamma_1=\gamma_2$ donde segue também que $\delta_0=\delta_1=\delta_2$. Finalmente, notamos que a imagem de v em $\mathbf{Z}(G/<a>)$ é $1+(1-b)(3\gamma_0+3\delta_0 b)$ e, como nos casos a , deve ser trivial. Segue então que $\gamma_0=\delta_0=0$, o que implica $v=1$.

Caso (ii): $1+\gamma_0-\gamma_1+\delta_1-\delta_2=\gamma_1-\gamma_2+\delta_2-\delta_0$

Neste caso, a imagem de v em $\mathbf{Z}(G/<a^2b>)$ é

$$\tilde{v}=\gamma_0-2\gamma_1+\gamma-2+(1+g_0+\gamma_1-2g_2)a+(-2g_0+g_1+g_2)a^2.$$

Como no caso anterior, concluimos que $\gamma_0-2\gamma_1+\gamma_2=0=-2\gamma_0+\gamma_1+\gamma_2$. Segue que $\gamma_0=\gamma_1=\gamma_2$ e que $\delta_1=\delta_2=1+\delta_0$. A imagem de v em $\mathbf{Z}(G/<a>)$ é agora $1+(1-b)(2+3\gamma_0+3\delta_0 b)$; concluimos então que $\delta_0=-1$, $\gamma_0=0$ e $v=b$.

Caso (iii): $1+\gamma_0-\gamma_1+\delta_1-\delta_2=\gamma_2-\gamma_0+\delta_0-\delta_1=0$.

Agora, a imagem de v em $\mathbf{Z}(G/<a^2b>)$ é

$$\tilde{v}=1+\gamma_0-2\gamma_1+\gamma_2+(1+\gamma_0+\gamma_1-2\gamma_2)a=(-1-2\gamma_0+\gamma_1+\gamma_2)a^2.$$

Novamente, como no primeiro caso, temos que $1+\gamma_0+2\gamma_1+\gamma_2=0=1+\gamma_0+\gamma_1-2\gamma_2$ e assim obtemos $\gamma_2-\gamma_1=1+\gamma_0$ e $\delta_2=\delta_1=1+\delta_0$. Finalmente, a imagem de v em $\mathbf{Z}(G/<a>)$ é $1+(1-b)[2+3\gamma_0+(2+3\gamma_0)b]$, de modo que concluimos que $\gamma_0=\delta_0=-1$, o que implica que $v=b^2$.

Em todos os casos temos provado que v é uma unidade trivial, o que completa nossa demonstração. $\diamond$

Lema 7.7 *Seja C_4 um grupo cíclico de ordem 4 e $G=C_4\times\cdots\times C_4$. Então $\mathcal{U}_1(\mathbf{Z}G)=G$.*

Demonstração. Mais uma vez, vamos proceder por indução no número de fatores diretos de G, que denotaremos por t. Se $t = 1$, então G é um grupo cíclico de ordem 4. Como o elemento $a \in \mathcal{Q}_8$ é de ordem 4, o anel de grupo $\mathbf{Z}G$ é isomorfo ao anel $\mathbf{Z} < a > \subset \mathbf{Z}\mathcal{Q}_8$. Como este último tem só unidades triviais, segue nossa afirmação neste caso.

Suponhamos agora que o resultado vale para grupos que são produto de $t-1$ fatores diretos iguais a C_4. Vamos escrever $G = A\times < x > \times < y >$, onde $x^4 = y^4 = 1$. Seja v uma unidade de $\mathbf{Z}G$. Podemos escrevere v na forma $v = \gamma_0 + \gamma_1 y + \gamma_2 y^2 + \gamma_3 y^3$, com $\gamma_i \in \mathbf{Z}A\times < x >$, $0 \leq i \leq 3$. Se denotamos por $\overline{y}$ a classe de y em $< y > / < y^2 >$ temos que $\overline{y}$ é um elemento de ordem 2 e a projeção de v em $\mathbf{Z}A\times < x > \times(< y > / < y^2 >)$ é:

$$\overline{v} = (\gamma_0 + \gamma_2) + (\gamma_1) + \gamma_3)\overline{y}$$

Pela hipótese de indução, toda unidade de $\mathbf{Z}(A\times < x >)$ é trivial e, pelo Lema 7.3, temos que também as unidades de $\mathbf{Z}(A\times < x > \times(< y > / < y^2 >))$ são triviais. Portanto temos dois casos possíveis:

Ou temos que $\gamma_0 + \gamma_2 = 0$ e $\gamma_1 + \gamma_3 = 1$ ou $\gamma_0 + \gamma_2 = 1$ e $\gamma_1 + \gamma_3 = 1$.

No primeiro caso, escrevendo $\gamma_2 = -\gamma_0$ e $\gamma_3 = 1 - \gamma - 1$ temos que v é da forma $v = y^3 + (\gamma_0 + \gamma_1 y)(1 - y^2)$; no segundo, procedendo de forma análoga obtemos que $v = y^2 + (\gamma_0 + \gamma_1 y)(1 - y^2)$, de modo que, em ambos os casos, multiplicando v por uma potência conveniente de y temos outro unidade v' que é da forma $v' = y^2 + (\gamma_0 + \gamma_1 y)(1 - y^2)$. Isto implica que v' pode se escrever também na forma:

$$v' = 1 + (\alpha_0 + \alpha_1 x + \alpha_2 x^2 + \alpha_3 x_3 + \beta_0 y + \alpha_1 xy + \beta_2 x^2 y + \beta_3 x^3 y)(1 - y^2),$$

onde $\alpha_i, \beta_j \in \mathbf{Z}A$, $0 \leq i, j \leq 3$. Como a projeção de v' em $\mathbf{Z}(G/ < x^2 >)$ também deve ser trivial, obtemos que $\alpha_1 + \alpha_3 = \beta_0 + \beta_2 = \beta_1 + \beta_3 = 0$ e $\alpha_0 + \alpha_2 = 0$ ou $\alpha_0 + \alpha_2 = -1$.

De forma análoga, a projeção de v' em $\mathbf{Z}(G/ < x^2 y^2 >)$ deve ser trivial, e obtemos assim que $\alpha_1 - \alpha_3 = \beta_0 - \beta_2 = \beta_1 - \beta_3 = 0$ e $\alpha_0 - \alpha_2 = 0$ ou $\alpha_0 - \alpha_2 = -1$.

Combinando ambos resultados obtemos que $\alpha_1 = \alpha_3 = \beta_0 = \beta_2 = \beta_1 = \beta_3 = \alpha_2 = 0$ e $\alpha_o = 0$ ou $\alpha_0 = -1$. Isto implica que $v' = 1$ ou $v' = b^2$. Em ambos os casos v' é trivial, o que implica que v também é trivial. $\diamondsuit$

Finalmente estamos em condições de enunciar o resultado principal desta seção.

Teorema 7.8 *Seja G um grupo finito. Então todas as unidades de $\mathbf{Z}G$ são triviais se e somente se G e um grupo abeliano de expoente igual a $1, 2, 3, 4$ ou 6 ou um 2-grupo Hamiltoniano.*

Demonstração. Em uma direção a afirmação já foi provada na Proposição 7.2. Para demonstrar a recíproca, note que, se G é um 2-grupo Hamiltoniano, o resultado é uma consequência dos lemas 7.3 e 7.4. Finalmente, se G é abeliano e seu expoente é um $1, 2, 3, 4$ ou 6, sua decomposição como produto direto de grupos cíclicos deve ser de uma das seguintes formas:

$$G \cong C_2 \times \cdots \times C_2,$$
$$G \cong C_3 \times \cdots \times C_3,$$
$$G \cong C_4 \times \cdots \times C_4,$$
$$G \cong C_2 \times \cdots \times C_2 \times C_3 \times \cdots \times C_3.$$

Em todos os casos, os lemas acima mostram que as unidades de $\mathbf{Z}G$ são triviais. $\diamondsuit$.

Parte III
Alguns problemas

8 A conjectura de Zassenhaus

No início da década de setenta, H.J. Zassenhaus formulou diversas conjecturas sobre as unidades e os isomorfismos normalizados de um anel de grupo. Nós as listamos a seguir, junto com o nome com que elas são conhecidas na atualidade.

- **(Aut)** Seja $\theta : \mathbf{Z}G \to \mathbf{Z}G$ um automorfismo normalizado. Então existem uma unidade $\alpha \in \mathbf{Q}G$ e um automorfismo $\sigma \in Aut(G)$ tais que $\theta(g) = \alpha^{-1}\sigma(g)\alpha$, $\forall g \in G$.
- **(ZC1)** Seja $u \in \mathcal{U}(\mathbf{Z}G)$ um elemento de ordem finita. Então existe uma unidade $\alpha \in \mathbf{Q}G$ tal que $\alpha^{-1}u\alpha \in G$ (neste caso, dizemos que u é *racionalmente conjugado* a um elemento de G).
- **(ZC2)** Seja $\mathcal{H}$ um subgrupo finito de $\mathcal{U}_1\mathbf{Z}G)$ tal que $|\mathcal{H}| = |G|$. Então existe uma unidade $\alpha \in \mathbf{Q}G$ tal que $\alpha^{-1}\mathcal{H}\alpha = G$.
- **(ZC3)** Seja $\mathcal{H}$ um subgrupo finito de $\mathcal{U}_1\mathbf{Z}G)$. Então existe uma unidade $\alpha \in \mathbf{Q}G$ tal que $\alpha^{-1}\mathcal{H}\alpha \subset G$.

Note que **(ZC2)** é obviamente um caso particular de **(ZC3)**. Também **(ZC1)** é **(ZC3)** no caso particular dos grupos cíclicos. Infelizmente, esta conjectura não é verdadeira, como foi recentemente demonstrado por K.W. Roggenkamp e L. Scott. O contraexemplo destes autores é particularmente difícil e foi simplificado por L. Klinger em 1993 [27]. Mesmo assim, o contraexemplo apresentado é de dois grupos de ordens iguais a $2^6.3.5.7$.

Damos, a seguir, uma lista dos grupos para os quais vale **(ZC1)**.

- S_3 (I. Hughes e K.R. Pearson [18]).
- D_4 (C. Polcino Milies [36]).
- Grupos metacíclicos da forma $G =< x > \rtimes < y >$ onde $o(x) = p$, $o(y) = q$ com p, q primos diferentes (A.K, Bhandari e I.S. Luthar [4]).

- Grupos metacíclicos da forma $G =< x > \rtimes < y >$ onde $mdc(o(x), o(y)) = 1$ (C. Polcino Milies, J. Ritter e S.K. Sehgal [37], [37], [39].)
- S_4 (N.A. Fernandes [31]).
- A_5 (I.S. Luthar e I.B.S. Passi [28]).
- S_5 (I.S. Luthar e P. Trama [29]).
- Grupos da forma $G =< x > \rtimes H$ onde H é um grupo abeliano tal que $mdc(o(x), |H|) = 1$ (I.S. Luthar e P. Trama [30]).

Já a validade da conjectura **(ZC3)** foi estabelecida para os seguintes grupos.

- Grupos nilpotentes (A. Weiss [50]).
- Grupos metacíclicos da forma $G =< x > \rtimes < y >$ onde $mdc(o(x), o(y)) = 1$ (A. Valenti [48]).
- S_5, A_5 e $SL(2,5)$ (M. Dokuchaev, S.O. Juriaans e C. Polcino Milies [13]).

Finalmente, cabe mencionar que recentemente foi formulada uma versão mais fraca da conjectura:

- **(p-ZC)** Seja $\mathcal{H}$ um p-subgrupo finito de $\mathcal{U}_1\mathbf{Z}G)$. Então existe uma unidade $\alpha \in \mathbf{Q}G$ tal que $\alpha^{-1}\mathcal{H}\alpha \subset G$.

Note que esta conjectura é, em certo sentido, semelhante ao Teorema de Sylow. Esta versão da conjectura, até a presente data, foi estabelecida para as seguintes famílias de grupos.

- Grupos nilpotentes-por-nilpotentes.
- Grupos solúveis tais que todo p-subgrupo de Sylow é abeliano ou quatérnio generalizado.
- Grupos solúveis cujas ordens não são divisíveis pela quarta potência de um primo.
- Grupos de Frobenius em geral para $p > 2$ e grupos de Frobenius que não têm imagem homomorfa a S_5, no caso $p = 2$.

Os primeiros três resultados foram estabelecidos por M. Dokuchaev e S.O. Juriaans [12] e o último por M. Dokuchaev, S.O. Juriaans e C. Polcino Milies [13].

9 Subgrupos de índice finito

No caso geral, resulta muito difícil descrever completamente o grupo das unidades de um anel de grupo sobre os inteiros. Uma tentativa recente tem sido a de determinar, mediante famílias de geradores, pelo menos um subgrupo "grande", isto é, um subgrupo que seja de índice finito em $\mathcal{U}(\mathbf{Z}G)$.

As unidades cíclicas de Bass, que definimos na seção anterior, foram intruduzidas por esse autor em [1] e utilizadas por H. Bass e J. Milnor em [2] para mostrar que elas geram um subgrupo de índice finito no anel $\mathcal{U}(\mathbf{Z}A)$, onde A é um grupo abeliano.

No caso não abeliano é necessário introduzir novas unidades, as unidades bicíclicas que também definimos na seção anterior e que foram assim denominadas por J. Ritter e S.K. Sehgal em [41], embora nem sempre estas duas famílias de unidades sejam suficientes para gerar subgrupos de índice finito. Nós daremos aqui uma idéia dos resultados obtidos em torno deste problema, seguindo essencialmente a primeira parte de [26]. O leitor interessado nestas questîs geralmente, na estrutura e propriedades dos grupos das unidades, pode consultar os surveys recentes de J. Ritter [44] e S.K. Sehgal [45]. Uma visão mais abrangente sobre o assunto pode-se obter em [46]

A pesquisa sobre este problema foi iniciada numa série de artigos por J. Ritter e S.K. Sehgal, [40], [41], [42] e [43]. Muitos dos resultados por eles obtidos seguem agora do seguinte resultado recente de E. Jespers e G. Leal [21].

Teorema 9.1 *Seja G um grupo finito tal que a algebra de grupo $\mathbf{Q}G$ não tem componentes simples de nenhum dos seguintes tipos:*

1. *uma álgebra com divisão não comutativa, diferente da álgebra de quaternios totalmente definida.*
2. *o anel $M_2(\mathbf{Q})$.*
3. *um anel da forma $M_2(F)$, onde F é uma extensão quadrática imaginária dos racionais.*
4. *um anel da forma $M_2(D)$, onde D é uma álgebra com divisão, não comutativa.*

Para cada idempotente primitivo central e_i tal que a componente $(\mathbf{Q}G)e_i$ não é um anel com divisão, seja f_i um idempotente não central de $(\mathbf{Q}G)e_i$

e n_i um inteiro positivo tal que $n_i f_i \in \mathbf{Z}G$. Então, o subgrupo gerado pelas unidades cíclicas de Bass e as unidades da forma :

$$1 + n_i^2 f_i h(1 - f_i) \quad e \quad 1 + n_i^2 (1 - f_i) h f_i,$$

$h \in G$, é de índice finito em $\mathcal{U}(\mathbf{Z}G)$.

Lembramos que um grupo diz-se *livre de pontos fixos*, se existe uma representação complexa irredutível ρ tal que para todo elemento $x \neq 1$ em G tem-se que $\rho(x)$ tem todos seus valores próprios diferentes de 1. Estes grupos são precisamente os complementos de Frobenius e são bem conhecidos. Veja, por exemplo [33]. Como consequência deste resultado pode-se provar o seguinte.

Corolario 9.2 *Seja G um grupo finito tal que $\mathbf{Q}G$ satisfaz as condições (2), (3), e (4) do teorema acima. Se G tem uma imagem homomorfa não abeliana que é livre de pontos fixos então o subgrupo gerado pelas unidades cíclicas de Bass e as unidades da forma:*

$$1 + \widehat{g} h(1 - g) \quad e \quad 1 + (1 - g) h \widehat{g},$$

$g, h \in G$, é de índice finito em $\mathcal{U}(\mathbf{Z}G)$. Se ainda $\mathbf{Q}G$ não contém componentes simples que seja álgebras com divisão não comutativas, então vale também a recíproca.

Um resultado análogo já tinha aparecido em [40].
Alguns exemplos que satisfazem as condições deste corolário são os seguintes:

- Grupos simétricos S_n, $n \geq 5$. Neste caso pode-se demonstrar que as unidades dadas no corolário, junto com uma transposição geram um subgrupo de índice finito.
- Grupos metacíclicos da forma : $< a, b \mid a^m = b^s = 1, b^{-1}ab = a^r >$, onde s é ímpar, $mdc(s, m) = 1$ e

  $$r^j i \equiv i \text{ (mod m) implica } ri \equiv i \text{ (mod m)},$$

  para cada $1 \leq i \leq m$, $1 \leq j \leq s - 1$.

Numa série de artigos, E. Jespers, G. Leal e M.M. Parmenter [19], [20], [22], [23], [24] caracterizaram completamente o grupo das unidades de $\mathcal{U}(\mathbf{Z}G)$, quando G é um grupo não abeliano de ordem menor o igual a 16. Destes resultados segue, em particular, que se denotamos por D_{2n} o grupo dihedral de ordem $2n$, então D_{16} e $D_8 \times C_2$ são os únicos grupos de ordem 16 para os quais as unidades cíclicas de Bass junto com as unidades bi cas geram um subgrupo de índice finito. Eles mostraram também que essas unidades geram subgrupos de índice finito em S_3 e S_4.

Ainda, em [19] se prova que as unidades cíclicas de Bass junto com as unidades bicíclicas geram um subgrupo de índice finito en $\mathcal{U}(\mathbf{Z}D_{2n})$.

Finalmente, em [26] se prova que estas unidades também são suficientes para gerar um subgrupo de índice finito em $\mathcal{U}(\mathbf{Z}G)$, quando G é um p-grupo finito tal que $G/\mathcal{Z}(G) \cong C_p \times C_p$.

Bibliografia

[1] Bass, H., The Dirichlet unit theorem, induced characters and Whitehead groups of finite groups, *Topology*, 4 (1966), 391-340.

[2] Bass, H. and Milnor, and Serre J.P. Solution of the congruence subgroup problem for SL_n $N \geq 3$ and Sp_2n, ; $n \geq 2$, *Publ. Math. I.H.E.S.*, 33 (1967), 59-137.

[3] Berman, S.D., On the equation $X^n = 1$ in an integral group ring, *Ukrain. Math. Zh.*, 7 (1955), 253-261.

[4] Bhandari, A.K. and Luthar, I.S., Torsion units of integral group rings of metacyclic groups, *J. Number Theory*, 17 (1983), 170-183.

[5] Brauer, R. Über Systeme Hypercomplexer Zahlen *Math. Z.*, 30 (1929), 79-107.

[6] Brauer, R. and Noether, E., Über minimale Zerfällungskörper irreduzibler Darstellungen, *Sitz. Preuss. Akad. Wiss.* (1927), 221-228.

[7] Cayley, A. On the theory of groups as depending on the symbolic equation $\theta^n = 1$, *Phillos. Mag.*, 7 (1854), 40-47.

[8] Coleman, D.B., Finite groups with isomorphic group algebras, *Trans. Amer. Math. Soc.*, 105 (1962), 1-8.

[9] Connell, I.G., On the group ring, *Canad. J. Math.*, 15 (1963), 650-685.

[10] Dade, E.C., Deux groups finis ayant la même algebre de group sur tout corps, *Math. Z.*, 119 (1971), 345-348.

[11] Deskins, W.E., Finite abelian groups with isomorphic group algebras, *Duke Math. J.* 23 (1956), 35-40.

[12] Dokuchaev, M.A., Juriaans, S.O., Finite Subgroups in Integral Group Rings, *Canad. J. Math.* (a aparecer).

[13] Dokuchaev, M.A., Juriaans, S.O. and Polcino Milies, C., Integral Group Rings of Frobenius groups and the Conjectures of H.J. Zassenhaus, preprint.

[14] Fernandes N.A., Torsion Units in the Integral Group Ring of S_4, *Bol. Soc. Brasileira de Mat.*, **18**, 1 (1987), 1-10.

[15] Goodaire, E.G., Jespers and Polcino Milies, C., *Alternative Loop Rings*, North Holland Math. Series, a aparecer.

[16] Herstein, I.N., *Topics in Algebra*, Blaisdell, New York, 1964.

[17] Higman, G. The units of group rings, *Proc. London Math. Soc*, 2, 46 (1940), 231-248.

[18] Hughes, I. and Pearson, K.R., The group of units of the integral group ring $\mathbf{Z}S_3$, *Canad. Math, Bull.*, 15 (1972), 529-534.

[19] Jespers, E., Bicyclic units in some integral group rings, *Canad. Math. Bull.*, 38 (1995), 80-86.

[20] Jespers, E. and Leal, G., Describing units in integral group rings of some 2-groups, *Comm. Algebra*, 19, 6 (1991) 1808-1827.

[21] Jespers, E. and Leal, G., Generators of large subgroups of the unit group of integral group rings, *Manuscripta Math.* 78 (1993), 303-315.

[22] Jespers, E., Leal, G. and Parmenter, M.M Bicyclic and Bass cyclic units in group rings, *Canad. Math. Bull.*, 36, 2 (1993), 178-182.

[23] Jespers, E. and Parmenter, M., Bicyclic units in $\mathbf{Z}S_3$, *Bull. Soc. Math. Belg.*, ser. B, 44, 2 (1992), 141-146.

[24] Jespers, E. and Parmenter, M., Units of group rings of groups of order 16, *Glasgow Math. J.*, 35 (1993), 367-379.

[25] Jespers, E., Parmenter, M. and Smith, P., *Revisiting a Theorem of Higman*, in *Proceedings, Groups' 93*, ed. by C.M. Campbell, T.C. Hurley, E.F. Robertson,S.J. Tobin and J.J. Ward, London Math. Soc. Lecture Notes 212, London, 1995, pp. 269-273.

[26] Jepers,E. and Polcino Milies, C., Units of group rings *J. Pure and Appl. Algebra*, 107 (1996), 233-251.

[27] Klinger, L., Construction of a counterexample to a conjecture of Zassenhaus, *Commun. Algebra* **19** (1993), 2303-2330.

[28] Luthar, I.S., Passi, I.B.S., Zassenhaus conjecture for A_5, *Proc. Indian Acad. Sci* **99** (1) (1989), 1-5.

[29] Luthar, I.S. and Trama, P., Zassenhaus conjecture for S_5, (preprint).

[30] Luthar, I.S. and Trama, P., Zassenhaus conjecture for certain integral group rings, *J. Indian Math. Soc.*, 55 (1990), 199-212.

[31] Noether, E., Hypercomplexe Grössen und Darstellungstheorie, *Math. Z.*, 30 (1929), 641-692.

[32] Perlis, S. and Walker, G.L., Abelian Group Algebras of Finite Order, *Trans. Amer. Math. Soc. 68* (1950), 420-426.

[33] Passman, D.S., *Permutation Groups*, Benjamin, New York, 1968.

[34] Passman, D.S., The group algebras of groups of order p^4 over a modular field, *Michigan Math. J.*, 12 (1965), 405-415.

[35] Passman, D.S., Isomorphic groups and group rings, *Pacific J. Math.*, 14 (1965), 561-583.

[36] Polcino Milies, C., The units of the integral grouop ring $\mathbf{Z}D_4$, *Bol. Soc. Brasileira de Mat.*, 4 (1972), 85-92.

[37] Polcino Milies, C., Ritter, J., Sehgal, S. K., On a conjecture of Zassenhaus on torsion units in integral group rings II, *Proc. Amer. Math. Soc.* **97** (2) (1986), 206-210.

[38] Ritter, J, and Sehgal, S.K., Integral group rings of some p-groups, *Canad. J. Math.*, 34, 1 (1982), 233-246.

[39] Ritter, J. and Sehgal, S.K., On a conjecture of Zassenhaus on torsion units in integral group rings, *Math. Ann.*, 264 (1983), 257-270.

[40] Ritter, J. and Sehgal, S.K., Generators of subgroups of $\mathcal{U}(\mathbf{Z}G)$, *Contemp. Math.*, 93 (1989), 331-347.

[41] Ritter, J. and Sehgal, S.K., Construction of units in integral group rings of finite nilpotent groups, *Trans. Amer. Math Soc.*, 324, 2 (1991), 602-621.

[42] Ritter, J. and Sehgal, S.K., Construction of units in group rings of monomial and symmetric groups, *J. Algebra*, 142 (1991), 511-526.

[43] Ritter, J. and Sehgal, S.K., Units of group rings of solvable and Frobenius groups over large rings of cyclotomic integers, *J. Algebra*,158 (1993), 116-129.

[44] Ritter, J. Large subgroups in the unit groups of group rings, (a survey), *Bayreuther Math. Schrift.*, 33 (1990), 153-171.

[45] Sehgal, S.K., Units of integral group rings - a survey, in *Proc. First Symposium in Algebra and Number Theory*, Hong Kong, World Scientific, 1990, pp. 255-268.

[46] Sehgal, S.K. *Units in Integral Group Rings*, Longman, Essex, 1993.

[47] Sandling, R., Group rings of circle and unit groups, *Math. Z.*, 140 (1974), 195-202.

[48] Valenti, A., Torsion Units in Integral Group Rings, *Proc. Amer. Math. Soc.* **120** (1) (1994), 1-4.

[49] Whitcomb, A., The group ring problem. Ph.D. Thesis, University of Chicago, 1968.

[50] Weiss, A., Rigidity of p-adic torsion, *Ann. Math.* **127** (1988), 317-332.

MONOGRAFIAS DE MATEMÁTICA

(títulos já publicados)

01) Azevedo, Alberto / Piccinini, Renzo – INTRODUÇÃO À TEORIA DOS GRUPOS (1970) / reprodução (1984)
02) Santos, Nathan M. – VETORES E MATRIZES (1970) – esgotada
03) Carmo, Manfredo P. do – INTRODUÇÃO À GEOMETRIA DIFERENCIAL GLOBAL (1970) – esgotada
04) Palis Junior, Jacob – SEMINÁRIO DE SISTEMAS DINÂMICOS (1971) – esgotada
05) Carvalho, João Pitombeira de – INTRODUÇÃO À ÁLGEBRA LINEAR (1971) – esgotada
06) Fernandez, Pedro Jesus – INTRODUÇÃO À TEORIA DAS PROBABILIDADES (1971) – esgotada
07) Robinson, R.C. – LECTURES ON HAMILTONIAN SYSTEMS (1972) – esgotada
08) Carmo, Manfredo P. de – NOTAS DE GEOMETRIA RIEMANNIANA (1972) – esgotada
09) Hönig, Chaim S. – ANÁLISE FUNCIONAL E O PROBLEMA DE STURM- LIOUVILLE (1972) – esgotada
10) Melo, Welington de – ESTABILIDADE ESTRUTURAL EM VARIEDADES DE DIMENSÃO 2 (1972) – esgotada
11) Lesmes, Jaime – TEORIA DAS DISTRIBUIÇÕES E EQUAÇÕES DIFERENCIAIS (1972) – esgotada
12) Vilanova, Clóvis – ELEMENTOS DA TEORIA DOS GRUPOS E DA TEORIA DOS ANÉIS (1972) – esgotada
13) Douai, Jean Claude – COHOMOLOGIE DES GROUPES (1973) – esgotada
14) Lawson Jr. / H. Blaine – LECTURES ON MINIMAL SUBMANIFOLDS, Vol. I (1973) – esgotada
15) Lima, Elon Lages – VARIEDADES DIFERENCIÁVEIS (1973) – esgotada
16) Mendes, Pedro – TEOREMAS DE Ω-ESTABILIDADE E ESTABILIDADES ESTRUTURAL EM VARIEDADES ABERTAS (1973) – esgotada
17) Amann, Herbert – LECTURES ON SOME FIXED POINT THEOREMS (1974) – esgotada
18) – EXERCÍCIOS DE MATEMÁTICA / IMPA (1974) – esgotada
19) Figueiredo, Djairo Guedes de – NÚMEROS IRRACIONAIS E TRANSCEDENTES (1975) – esgotada
20) Zeeman, C.E. – UMA INTRODUÇÃO INFORMAL À TOPOLOGIA DAS SUPERFÍCIES (1975) – esgotada
21) Carmo, Mandredo P. do – NOTAS DE UM CURSO DE GRUPOS DE LIE (1975) – esgotada
22) Prestel, Alexander – LECTURES ON FORMALLY REAL FIELDS (1975) – esgotada
23) Simis, Aron – INTRODUÇÃO À ÁLGEBRA (1976) – esgotada
24) Lesmes, Jaime – SEMINÁRIO DE ANÁLISE FUNCIONAL (1976) – esgotada
25) Brauer, Fred – SOME STABILITY AND PERTURBATION PROBLEM FOR DIFFERENTIAL AND INTEGRAL EQUATIONS (1976) – esgotada
26) Rodríguez, Lúcio – GEOMETRIA DAS SUBVARIEDADES (1976)
27) Miranda, Mário – FRONTIÈRE MINIME (1976)
28) Cardoso, Fernando – RESOLUBILIDADE LOCAL DE EQUAÇÕES DIFERENCIAIS PARCIAIS (1977) – esgotada
29) Becker, Eberhard – HEREDITARILY-PYTHAGOREAN FIELDS AND ORDERINGS OF HIGHER LEVEL (1978)
30) Bass, Hyman – PROJECTIVE MODULES AND SYMMETRIC ALGEBRAS (1978)
31) Neyman, J. – PROBABILIDADE FREQÜENTISTA E ESTATÍSTICA FREQÜENTISTA (1978)
32) Dumortier, Freddy – SINGULARITIES OF VECTOR FIELDS (1978)
33) Viswanathan, T.M. – INTRODUÇÃO À ÁLGEBRA E ARITMÉTICA (1979) – esgotada
34) Thayer, F. Javier – NOTES ON PARTIAL DIFFERENTIAL EQUATIONS (1980)
35) Bierstone, Edward – THE STRUCTURE OF ORBIT SPACES AND THE SINGULARITIES OF EQUIVARIANT MAPPINGS (1980)
36) Thayer, F. Javier – THÉORIE SPECTRALE (1982)
37) Carmo, Manfredo P. de – FORMAS DIFERENCIAIS E APLICAÇÕES (1983)
38) Prestel, Alexander / Roquette, Peter – LECTURES ON FORMALLY p-ADIC FIELDS (1983)
39) Lequain, Yves / Garcia, Arnaldo – ÁLGEBRA: UMA INTRODUÇÃO (1983) – esgotada
40) Barbosa, J. Lucas / Colares, A. Gervásio – MINIMAL SURFACES IN R^3 (1986)
41) Bérard, Pierre H. – SPECTRAL GEOMETRY; DIRECT AND INVERSE PROBLEMS (1986)
42) Bérard, Pierre H. - ANALYSIS ON RIEMANNIAN MANIFOLDS AND GEOMETRIC APPLICATIONS: AN INTRODUCTION (1987)
43) Torres, Felipe Cano - DESINGULARIZATION STRATEGIES FOR THREE-DIMENSIONAL VECTOR FIELDS (1988)
44) Endler, Otto - TEORIA DOS CORPOS (1988)
45) Bruns, Winfried / Vetter, Udo - DETERMINANTAL RINGS (1968)
46) Hefez, Abramo - INTRODUÇÃO À GEOMETRIA PROJETIVA (1990)
47) Gouvêa, Fernando Quadros – FORMAS MODULARES: UMA INTRODUÇÃO (1990)
48) JØrgensen, Bent – EXPONENTIAL DISPERSION MODELS (1991)
49) Bustos, Oscar H. / Frery, Alejandro C. - SIMULAÇÃO ESTOCÁSTICA: TEORIA E ALGORITMOS (Versão Completa) (1992)
50) Létac, Gérard - LECTURES ON NATURAL EXPONENTIAL FAMILIES AND THEIR VARIANCE FUNCTIONS (1992)
51) JØrgensen, Bent - THE THEORY OF EXPONENTIAL DISPERSION MODELS AND ANALYSIS OF DEVIANCE (1992)
52) JØrgensen, Bent / Labouriau Rodrigo S. / Colaboração: Martinez, José R. – FAMÍLIAS EXPONENCIAIS E INFERÊNCIA TEÓRICA (1992)
53) Gomes, Jonas de Miranda / Velho, Luiz – IMPLICIT OBJECTS IN COMPUTER GRAPHICS (1992)
54) Fontes, Luiz Renato G. – NOTAS EM PERCOLAÇÃO (1996)
55) Lopes, Helena J.N. / Lopes, Milton C.F. – UMA INTRODUÇÃO A SOLUÇÕES DE VISCOSIDADE PARA EQUAÇÕES DE HAMILTON-JACOBI (1997)
56) Viana, Paulo – TOPOLOGIA ÉTALE (1998)
57) Sidki, Said - REGULAR TREES AND THEIR AUTOMORPHISMS (1998)
58) Milies, Cesar - UNIDADES EM ANEIS DE GRUPOS (1998)

Impresso na Gráfica do

pelo Sistema Xerox / 5390