A ORDEM DO SUBGRUPO UNITÁRIO DE ALGUMAS ÁLGEBRAS DE GRUPO MODULARES

Antonio Luiz Rosa

TESE APRESENTADA
AO
INSTITUTO DE MATEMÁTICA E ESTATÍSTICA
DA
UNIVERSIDADE DE SÃO PAULO
PARA
OBTENÇÃO DO GRAU
DE
DOUTOR EM MATEMÁTICA

Área de Concentração: **Álgebra**
Orientador: **Prof. Dr. Francisco César Polcino Milies**

– São Paulo, outubro de 2000 –

A ORDEM DO SUBGRUPO UNITÁRIO DE ALGUMAS ÁLGEBRAS DE GRUPO MODULARES

Antonio Luiz Rosa

Este exemplar corresponde à redação final da tese apresentada por Antonio Luiz Rosa, devidamente corrigida e aprovada pela Comissão Julgadora

São Paulo, outubro de 2000

Comissão Julgadora

- Prof. Dr. Francisco César Polcino Milies - IME-USP
- Prof. Dr. Jairo Zacarias Gonçalves - IME-USP
- Prof. Dr. Guilherme Leal - UFRJ
- Prof. Dr. Rudolf Meier - UnB
- Prof. Dr. Miguel Ferrero - UFRGS

"Ainda que eu falasse as línguas dos homens e dos anjos,
se não tiver amor,
sou como o bronze que soa,
ou como o címbalo que retine.

Mesmo que eu tivesse o dom da profecia,
e conhecesse todos os mistérios e toda a ciência;
mesmo que eu tivesse toda a fé,
a ponto de transportar montanhas,
se não tiver amor,
não sou nada."

(1 Coríntios 13-1, 2)

À minha

maravilhosa

família.

Agradecimentos

A Deus que me concedeu esta oportunidade, privilégio e alegria;

À minha família pelo apoio durante a realização deste;

Aos professores do IME-USP que muito contribuíram para a minha formação;

Aos professores e amigos da Universidade Federal de Ouro Preto que muito me encorajaram no êxito deste trabalho;

E a todos os demais que de forma direta ou indireta contribuíram para o êxito deste meu curso;

De forma especial, agradeço ao meu orientador, Prof. Dr. Francisco César Polcino Milies, pela confiança, pela paciência e sobretudo pelos ensinamentos no decorrer destes anos de saudável convívio;

E, ainda, em caráter especial, agradeço ao Prof. Dr. Victor Bovdi e ao Prof. Dr. Adalbert Bovdi, ambos da Lajos Kossuth University-Debrecen-Hungria, pela amizade, pela atenção, pelas informações e por tudo mais que foi fundamental para a realização deste trabalho.

RESUMO

Sejam K um corpo, G um grupo e $V(KG)$ o grupo das unidades normalizadas na álgebra de grupo KG. O anti-automorfismo em G, $g \mapsto g^{-1}$, estende-se linearmente ao anti-automorfismo

$$\alpha = \sum \alpha_g g \mapsto \alpha^* = \sum \alpha_g g^{-1}$$

em $V(KG)$. Define-se o subgrupo unitário de KG o seguinte:

$$V_*(KG) = \{\alpha \in V(KG) \mid \alpha^* = \alpha^{-1}\}.$$

O objetivo deste trabalho é determinar a ordem do subgrupo unitário $V_*(KG)$, onde K é um corpo finito de característica p (p um número primo) e G é um p-grupo finito.

Numa primeira etapa, determinamos a ordem do subgrupo unitário $V_*(KG)$ no caso da característica $p > 2$. No restante deste trabalho, determinamos a ordem do subgrupo unitário $V_*(KG)$, quando K é um corpo finito de característica 2 e G é um grupo finito dentre os seguintes:

(i) G é um 2-grupo extra-especial;

(ii) G é um produto central de um 2-grupo extra-especial com um grupo cíclico de ordem 4;

(iii) G é um 2-grupo contendo um subgrupo abeliano A de índice 2 e um elemento b tal que b inverte cada elemento de A.

Ressaltamos que por (iii) obtemos a ordem do subgrupo unitário $V_*(KG)$ para os 2-grupos diedrais D_{2^n} e os quatérnios generalizados Q_{2^n} ($n \geq 3$).

ABSTRACT

Let K be a field, G be a group and $V(KG)$ be the group of normalized units in the group algebra KG. The anti-automorphism in G, $g \mapsto g^{-1}$, extends linearly to an anti-automorphism

$$\alpha = \sum \alpha_g g \mapsto \alpha^* = \sum \alpha_g g^{-1}$$

of $V(KG)$. Define the unitary subgroup of KG the following

$$V_*(KG) = \{\alpha \in V(KG) \mid \alpha^* = \alpha^{-1}\}.$$

We determine in this work the order of unitary subgroup $V_*(KG)$, where K is a finite field of characteristic p (p is a number prime) and G is a finite p-group.

In a first step, we determine the order of unitary subgroup $V_*(KG)$ in the case of the characteristic $p > 2$. In the remainder of this work, we determine the order of unitary subgroup $V_*(KG)$, when K is a finite field of characteristic 2 and G is a finite p-group among the following:

(i) G is an extraspecial 2-group;

(ii) G is a central product of an extraspecial 2-group with a cyclic group of order 4;

(iii) G is a 2-group which contains an abelian subgroup A of index two and an element b such that $b^{-1}ab = a^{-1}$ for all $a \in A$.

We emphasize that by (iii), we obtain the order of unitary subgroups $V_*(KG)$ for all dihedral group D_{2^n} and for all generalized quaternion Q_{2^n} ($n \geq 3$).

Sumário

Notação

$\mathrm{char}(K)$	Característica do corpo K
K	Corpo
$G, H, \ldots$	Grupos
KG	Álgebra de grupo de um grupo G sobre um corpo K
x^y	$y^{-1}xy$
$[x, y]$	$x^{-1}y^{-1}xy$
$Z(G)$	Centro do grupo G
$G' = [G, G]$	Subgrupo comutador de um grupo G
$H \cong G$	H é isomorfo com G
$H \leq G$	H é um subgrupo do grupo G
$H \triangleleft G$	H é um subgrupo normal de G
$H_1 H_2 \cdots H_n$	Produto de subconjuntos de um grupo
$\langle x \mid x^n = 1 \rangle$	Subgrupo gerado pelo elemento x de ordem n
$\langle A_1, \ldots, A_n \rangle$	Subgrupo gerado pelo conjunto $A_1, \ldots, A_n$
G^n	Subgrupo gerado por todos g^n, onde $g \in G$
$G[n]$	Subgrupo gerado por todos $g \in G$ tal que $g^n = 1$
$\lvert K \rvert$	Ordem do corpo K
$\lvert G \rvert$	Ordem do grupo G
$[G : H]$	Índice do subgrupo H no grupo G
$\lvert x \rvert$	Ordem do elemento x
$G \times H$	Produto direto
$H \ltimes N$	Produto semidireto
$H \curlyvee N$	Produto central
$\mathrm{Frat}G$	Subgrupo de Frattini de G
D_{2^n}	Grupo diedral de ordem 2^n
Q_{2^n}	Grupo quatérnio generalizado de ordem 2^n
$\Delta(G : H)$	Ideal de KG gerado pelos elementos $h - 1$, onde $h \in H$
$\Delta(G)$	Ideal de aumento de KG
$\alpha = \sum_{g \in G} \alpha_g g$	Elemento na álgebra KG onde $\alpha_g \in K$ para todo $g \in G$
$\varepsilon(\alpha)$	Aumento do elemento $\alpha \in KG$
$U(KG)$	Grupo das unidades de KG
$V(KG)$	Grupo das unidades normalizadas de KG
$V_*(KG)$	Subgrupo unitário de KG
$Ann_{KG}(\alpha)$	Anulador do elemento α em KG
$\mathrm{supp}(\alpha)$	Suporte do elemento α em KG
$S_+(\Delta(G))$	Conjunto de elementos simétricos de aumento zero em KG
$S_-(\Delta(G))$	Conjunto de elementos anti-simétricos de aumento zero em KG
$S_*(KG)$	Conjunto das unidades normalizadas simétricas em KG

Introdução

O Subgrupo Unitário $V_*(KG)$ tornou-se um objeto de grande interesse dentro da teoria de Álgebras de Grupo Modulares, no sentido de que o conhecimento deste aproxima-nos do conhecimento do grupo das unidades normalizadas $V(KG)$ e de possíveis respostas a muitos problemas abertos nesta teoria.

Em 1995, A. Bovdi e A. Szakács [4,5] descreveram plenamente a estrutura de $V_*(KG)$, dando uma base para este grupo, quando KG é uma álgebra de grupo de um p-grupo abeliano finito G sobre um corpo finito K de p^m elementos.

Muito pouco se sabe no caso em que G é um p-grupo finito não abeliano (vide [1]). Pode-se considerar que um primeiro passo nesta direção é um resultado de V. Bovdi e L.G. Kovács [6]. Eles determinaram condições sobre a álgebra $\mathbb{F}_pG$, de um p-grupo não abeliano G, nas quais as unidades bicíclicas de $V(\mathbb{F}_pG)$ são unitárias.

Muitos problemas ainda permanecem abertos sobre $V_*(KG)$ quando G é não abeliano. Podemos citar dentre muitos os seguintes:

(i) Determinar um sistema de geradores para $V_*(KG)$.

(ii) Quando é que G tem um complemento normal em $V_*(KG)$?

(iii) Qual a classe de nilpotência de $V_*(KG)$?

(iv) Se KG é finito, qual é a ordem de $V_*(KG)$?

É claro que, para responder as questões (i), (ii) ou (iii) resulta necessário primeiro responder (iv).

Neste trabalho, vamos determinar a ordem de $V_*(KG)$ quando a característica de K é $p > 2$, p primo, para todas as famílias de p-grupos finitos não abelianos. Já no caso mais complexo da característica $p = 2$, determinamos a ordem de $V_*(KG)$ para diversas famílias de 2-grupos finitos não abelianos.

A tese é apresentada em quatro capítulos. O primeiro inclui noções preliminares que serão usadas em resultados dos capítulos seguintes. Este se divide em resultados preliminares sobre a Teoria dos Grupos, a Teoria de Anéis e em resultados preliminares sobre a Teoria de Anéis de Grupo. Nosso propósito aqui não é uma completa dissertação sobre tais assuntos, mas simplesmente recordarmos o essencial para uma completa compreensão dos resultados obtidos nos capítulos seguintes.

No segundo capítulo, determinamos a ordem do subgrupo unitário $V_*(KG)$ no caso em que a característica de K é $p > 2$. Aqui, não há restrição a nenhum p-grupo finito

não abeliano G.

No terceiro capítulo, determinamos a ordem do subgrupo unitário $V_*(KG)$ quando G é um determinado produto central. Incluímos aqui o caso em que G é um 2-grupo extra-especial.

Por fim, no quarto capítulo, determinamos a ordem de $V_*(KG)$ quando G contém um subgrupo abeliano A de índice dois e um elemento b que inverte cada elemento de A. Como casos particulares, determinamos a ordem de $V_*(KG)$ quando G é do tipo 2-grupo diedral ou um quatérnio generalizado.

Os resultados aqui contidos foram recentemente publicados no Communications in Algebra [9].

Capítulo 1

Resultados preliminares

Neste capítulo apresentamos resultados básicos que serão utilizados nos capítulos seguintes.

Começamos expondo a parte sobre grupos e anéis, recordando apenas o que for essencial para a compreensão dos mesmos. Em seguida, expomos a parte referente a Anéis de Grupos, em que recordamos os principais resultados obtidos até o momento e que serão fundamentais em nossas conclusões.

1.1 Grupos

Seja G um grupo. O *subgrupo de Frattini* de G é, por definição, a intersecção de todos os seus subgrupos maximais. Denotaremos este subgrupo por $\mathrm{Frat}G$.

Teorema 1.1.1 *(Wielandt) Seja G um grupo finito. Então G é nilpotente se e somente se $G' \leq \mathrm{Frat}G$.*

Prova: [pp.137, 11].

Teorema 1.1.2 *(Burnside) Seja G um p-grupo finito. Então $\mathrm{Frat}G = G'G^p$.*

Prova: [pp.140, 11].

Um p-grupo finito G é dito ser um *grupo extra-especial* se G' e $Z(G)$, o subgrupo comutador e o centro de G, respectivamente, coincidem e têm ordem p.

Lema 1.1.3 *Seja G um grupo e u, v elementos de G. Então vale a identidade*

$$[u^m, v] = [u, v]^{u^{m-1}+u^{m-2}+\cdots+u^2+u+1} \quad (m \in \mathbb{N}).$$

Além disso, se $[u, v]$ pertence ao centro de $\langle u, v\rangle$, então $[u^m, v] = [u, v]^m = [u, v^m]$.

Prova: Se $m = 1$, é evidente a identidade. Agora temos que

$$[u^m, v] = [u^{m-1}.u, v] = [u^{m-1}, v]^u.[u, v]$$

e o resultado segue por indução. ■

Teorema 1.1.4 *Seja G um p-grupo extraespecial. Então* Frat$G$, *$Z(G)$ e G' coincidem e têm ordem p.*

Prova: Que $Z(G)$ e G' coincidem e têm ordem p segue por definição. Agora, pelo Teorema 1.1.2, temos que Frat$G = G'G^p$, e pelo Lema 1.1.3, segue que para todos $x, g \in G$, $[x, g^p] = [x, g]^p = 1$ e disto $g^p \in Z(G) = G'$. Portanto, $G^p = \langle g^p | g \in G \rangle \subseteq G'$ e disto Frat$G = G'$. ■

Um grupo G é dito ser um *produto central* de seus subgrupos normais $G_1, \ldots, G_n$ se:

1. $G = G_1 \cdots G_n$;
2. $[G_i, G_j] = 1$, para $i \neq j$;
3. $G_i \cap \prod_{j \neq i} G_j = C \subseteq Z(G)$, para todo i.

Ao subgrupo C, chamaremos de *subgrupo fator central.*

Como $C \subseteq Z(G)$ então $C \subseteq Z(G_i)$, para todo i.

Notaremos $G = G_1 \curlyvee G_2 \curlyvee \cdots \curlyvee G_n$.

Temos,

$$|G| = \left(\prod_{i=1}^{n} |G_i|\right) / |C|.$$

Temos ainda que,

$$\bigcup_{i=1}^{n} Z(G_i) = Z(G).$$

Observamos que todo produto direto de grupos $G = H \times K$ pode ser visto como um produto central destes grupos com $C = \langle 1 \rangle$.

Exemplo 1: Sejam

$$A = \langle a, b | a^4 = 1, a^2 = b^2, a^b = a^{-1} \rangle = \{1, a, a^2, a^3, b, ab, a^2b, a^3b\}$$

e

$$B = \langle c, d | c^4 = 1, d^4 = 1, dc = c^3d \rangle$$

$$B = \{1, c, c^2, c^3, d, cd, c^2d, c^3d, d^2, cd^2, c^2d^2, c^3d^2, d^3, cd^3, c^2d^3, c^3d^3\}$$

Temos:

(i) $A = Q_8$, $|A| = 8$, $Z(A) = \{1, a^2\}$, $|Z(A)| = 2$;

(ii) $B = \langle c \rangle \rtimes \langle d \rangle$, $\langle c \rangle \triangleleft B$, $|B| = 16$, $Z(B) = \{1, c^2, d^2, c^2d^2\}$, $|Z(B)| = 4$.

Logo é possível obter 3 grupos do tipo $G = A \curlyvee B$, a saber:

1. $G_1 = A \curlyvee B$ com $C = \langle a^2 | a^2 = c^2 \rangle$, isto é,
   $G_1 = \langle a, b, c, d | a^4 = c^4 = d^4 = 1, a^2 = b^2 = c^2, dc = c^3d, [a, c] = [a, d] = [b, c] = [b, d] = 1 \rangle$;

2. $G_2 = A \curlyvee B$ com $C = \langle a^2 | a^2 = d^2 \rangle$, isto é,
   $G_2 = \langle a, b, c, d | a^4 = c^4 = d^4 = 1, a^2 = b^2 = d^2, dc = c^3d, [a, c] = [a, d] = [b, c] = [b, d] = 1 \rangle$;

3. $G_3 = A \curlyvee B$ com $C = \langle a^2 | a^2 = c^2d^2 \rangle$, isto é,
   $G_1 = \langle a, b, c, d | a^4 = c^4 = d^4 = 1, a^2 = b^2 = c^2d^2, dc = c^3d, [a, c] = [a, d] = [b, c] = [b, d] = 1 \rangle$;

Apesar de $|G_i| = (8 \times 16)/2 = 64$ para $i = 1, 2, 3$, temos que G_1, G_2 e G_3 não são isomorfos.

Exemplo 2: Sejam

$$A = H_1 \curlyvee H_2 \curlyvee \ldots \curlyvee H_n, \quad H_i = \langle a_i, b_i | a_i^4 = 1, {b_i}^2 = {a_i}^2, {a_i}^{b_i} = {a_i}^{-1} \rangle \cong Q_8,$$

um 2-grupo extra-especial , e

$$B = \langle x | x^4 = 1 \rangle, \text{um grupo cíclico de ordem } 4$$

Temos:

(i) $|A| = 2^{2n+1}$, $Z(A) = \{1, a^2\}$, $|Z(A)| = 2$;

(ii) $|B| = 4$, $Z(B) = B = \{1, x, x^2, x^3\}$, $|Z(B)| = 4$.

Logo é possível obter o seguinte grupo do tipo $G = A \curlyvee B$ com $C = \langle a^2 | a^2 = x^2 \rangle$, $|C| = 2$, $C \subseteq Z(A)$ e $C \subseteq Z(B)$, a saber:

$$G = \langle a_i, b_i, x | {a_i}^4 = x^4 = 1, a_i^2 = b_i^2 = x^2, {a_i}^{b_i} = {a_i}^{-1}, [a_i, x] = [b_i, x] = 1 \rangle.$$

Temos ainda que

$$|G| = \frac{2^{2n+1} \times 4}{2} = 2^{2n+2}.$$

Lema 1.1.5 *Se G é um grupo não abeliano de ordem p^3, então G é extra-especial.*

Prova: Sendo G não abeliano, então $G \neq Z(G)$ e $G' \neq 1$. Por outro lado, sendo $|G| = p^3$, então $Z(G) \neq 1$ e disto $|Z(G)| = p$ ou p^2. Mas se $|Z(G)| = p^2$, $G/Z(G)$ é cíclico e portanto G abeliano, o que é uma contradição. Portanto $|Z(G)| = p$.

Agora, como G é um grupo nilpotente e $1 \neq G' \triangleleft G$, então $G' \cap Z(G) \neq 1$. Mas $G' \cap Z(G) \subseteq Z(G)$ e disto $G' \cap Z(G) = Z(G)$, i.e, $Z(G) \subseteq G'$.

Por outro lado, $\left|\dfrac{G}{Z(G)}\right| = p^2$, i.e, $\dfrac{G}{Z(G)}$ é abeliano. Logo, $G' \subseteq Z(G)$. Portanto, $G' = Z(G)$ e $|G'| = |Z(G)| = p$. ■

É natural pensar um p-grupo extra-especial G como um produto direto de grupos G_i nos quais subgrupos centrais dos G_i são identificados por um subgrupo fator central C.

Teorema 1.1.6 *Um p-grupo extra-especial é um produto central de n subgrupos não abelianos de ordem p^3 e tem ordem p^{2n+1}. Reciprocamente, um produto central finito de grupos não abelianos de ordem p^3 com subgrupo fator central não trivial é um p-grupo extra-especial.*

Prova: [pp.146, 11].

Lema 1.1.7 *Sejam D_8 o grupo diedral de ordem 8 e Q_8 o grupo quatérnio de ordem 8. Então*

$$D_8 \curlyvee D_8 \cong Q_8 \curlyvee Q_8.$$

Prova: [pp.139, 12] Seja $D_8 = \langle x, y \mid x^4 = 1 = y^2,\ x^y = x^{-1} \rangle$. Deste modo, $D_8 = \{x^i y^j;\ 0 \leq i \leq 3,\ j = 0, 1\}$ e temos a regra $(x^i y^j)(x^k y^l) = x^a y^b$, onde $a \equiv i + (-1)^j k$

(mod 4) e $b \equiv j + l$ (mod 2) (isto segue da relação $xy = yx^{-1}$).

Seja $x^i y^j \in Z(D_8)$, $0 \leq i \leq 3$, $j = 0, 1$. Então, visto que $D_8 = \langle x, y \rangle$, devemos ter:

$$(x^i y^j)x = x(x^i y^j) \Rightarrow x^{i+(-1)^j}.y^j = x^{1+i}y^j \Rightarrow x^{(-1)^j - 1} = 1$$

e

$$(x^i y^j)y = y(x^i y^j) \Rightarrow x^i y^{1+j} = x^{-i}y^{1+j} \Rightarrow x^{2i} = 1.$$

Logo, devemos ter $(-1)^j \equiv 1$ (mod 4) e $2i \equiv 0$ (mod 4), com $0 \leq i \leq 3$ e $j = 0, 1$. Disto segue que $j = 0$, $i = 2$ e $x^i y^j \in Z(D_8)$ com $x^i y^j = x^2$. Portanto, temos $Z(D_8) = \langle x^2 \rangle$.

Sejam D_i $(i = 1, 2)$ grupos isomorfos a D_8. Consideramos o produto central $G = D_1 \curlyvee D_2$ identificando o centro. Isto é, $[D_1, D_2] = 1$, $G = D_1 D_2$ e $Z(D_8) = D_1 \cap D_2$.

Sejam $D_1 = \langle x_1, y_1 \rangle$ e $D_2 = \langle x_2, y_2 \rangle$. Identificando os centros, fazemos $x_1^2 = x_2^2 = c$.

Definimos agora dois subgrupos Q_1 e Q_2 por

$$Q_1 = \langle x_1, y_1 x_2 \rangle, \quad Q_2 = \langle x_1 y_2, x_2 \rangle.$$

Faça $x_3 = y_1 x_2$ e $x_4 = x_1 y_2$. Visto que $[D_1, D_2] = 1$, temos:

$$\begin{aligned}
x_3^2 &= (y_1 x_2)(y_1 x_2) = y_1^2 x_2^2 = x_2^2 = c \\
x_4^2 &= (x_1 y_2)(x_1 y_2) = x_1^2 y_2^2 = x_1^2 = c \\
x_3^{-1} x_1 x_3 &= (y_1 x_2)^{-1} x_1 (y_1 x_2) = x_2^{-1} y_1^{-1} x_1 y_1 x_2
\end{aligned}$$

$$
\begin{aligned}
&= x_2^{-1}x_1^{-1}x_2 = x_1^{-1} \\
x_4^{-1}x_2x_4 &= (x_1y_2)^{-1}x_2(x_1y_2) = y_2^{-1}x_1^{-1}x_2x_1y_2 \\
&= y_2^{-1}x_2y_2 = x_2^{-1} \\
(x_1x_3)^2 &= (x_1x_3)(x_1x_3) = (x_1y_1x_2)(x_1y_1x_2) \\
&= y_1x_1^{-1}x_2x_1y_1x_2 = y_1x_2y_1x_2 = x_3^2 = c \\
(x_2x_4)^2 &= (x_2x_4)(x_2x_4) = (x_2x_1y_2)(x_2x_1y_2) \\
&= x_2x_1x_2^{-1}y_2x_1y_2 = x_1y_2x_1y_2 = x_4^2 = c.
\end{aligned}
$$

Logo,

$$Q_1 = \langle x_1, x_3 \mid x_1^4 = 1, x_3^2 = x_1^2, x_1^{x_3} = x_1^{-1} \rangle \cong Q_8$$

e

$$Q_2 = \langle x_2, x_4 \mid x_2^4 = 1, x_4^2 = x_2^2, x_2^{x_4} = x_2^{-1} \rangle \cong Q_8.$$

Portanto, temos $|Q_1| = |Q_2| = 8$ e o único elemento de ordem 2 em Q_i, $i = 1, 2$, é c. Além do mais, valem:

$$
\begin{aligned}
x_1.x_4 &= x_1.x_1y_2 = x_1y_2x_1 = x_4.x_1 \\
x_2x_3 &= x_2y_1x_2 = y_1x_2x_2 = x_3x_2 \\
x_3x_4 &= (y_1x_2)(x_1y_2) = y_1x_1x_2y_2 = x_1^{-1}y_1y_2x_2^{-1} \\
&= x_1x_1^2y_1y_2x_2x_2^2 = x_1cy_1y_2x_2c = x_1y_1y_2x_2c^2 \\
&= x_1y_1y_2x_2 = x_1y_2y_1x_2 = x_4x_3.
\end{aligned}
$$

Assim também $G = Q_1 \curlyvee Q_2$.

Como nem D_8 e nem Q_i podem ser escritos como um produto central de subgrupos próprios, temos que $D_8 \curlyvee D_8 \cong Q_8 \curlyvee Q_8$. ■

Corolário 1.1.8 *Seja G um grupo extra-especial de ordem 2^{2n+1}. Então G é um produto central de grupos, todos eles isomorfos a D_8, ou um produto central de cópias de D_8 com um Q_8.*

Assim, se G é um grupo extra-especial de ordem 2^{2n+1}, então G pode ser visto como

$$G = G_1 \curlyvee \cdots \curlyvee G_n, \quad \text{com } G_i \cong Q_8, \quad 1 \leq i \leq n.$$

Agora, se $G_i = \langle a_i, b_i \rangle$ e $Z(G) = G' = \langle c \mid c^2 = 1 \rangle$, então cada elemento em G pode ser escrito como

$$x = c^k a_1^{\alpha_1} b_1^{\beta_1} a_2^{\alpha_2} b_2^{\beta_2} \cdots a_n^{\alpha_n} b_n^{\beta_n},$$

com $k = 0, 1$, $\alpha_i = 0, 1$ e $\beta_i = 0, 1$, $1 \leq i \leq n$, visto que $a_i^{-1} = a_i^3 = ca_i$ e $b_i^{-1} = b_i^3 = cb_i$, $1 \leq i \leq n$. Então, temos $x^2 = b_1^{2\beta_1} \cdots b_n^{2\beta_n} = c^\lambda$, com $\lambda = 0, 1$, pois $a_i^{b_i} = a_i^{-1}$ e $g^2 \in Z(G) = G'$, para todo $g \in G_i$, i qualquer. Assim, a ordem de x é 4 se $\lambda = 1$ e λ será 0 se a ordem de x é 2. De qualquer forma, cada elemento de G pode ser escrito

$$x = z_{i_1} z_{i_2} \cdots z_{i_k},$$

onde $z_{i_t} \in G_{i_t}$ tem ordem 4 e $i_1 < i_2 < \cdots < i_k$.

1.2 Anéis

Seja R um anel com unidade 1. Uma *involução* $*$ sobre R é uma aplicação $x \mapsto x^*$ que é um anti-automorfismo de período 2. Isto é, $*$ é um anti-automorfismo sobre R tal que

$$(r_1 r_2)^* = r_2^* r_1^* \quad \text{e} \quad (r_i^*)^* = r_i \qquad (r_i \in R).$$

Um elemento $u \in R$ é chamado um *elemento unitário* se $uu^* = 1 = u^*u$. Um elemento $k \in R$ é chamado *anti-simétrico* se $k^* = -k$.

Lema 1.2.1 *Seja k um elemento anti-simétrico em R tal que $1+k$ seja inversível em R. Então o elemento $u = (1-k)(1+k)^{-1}$ é unitário.*

Prova: Primeiro, observamos que

$$(1+k)(1-k) = 1 - k^2 = (1-k)(1+k).$$

Visto que $1+k$ é inversível, segue também que

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

Assim, tomando

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

obtemos

$$u(1+k) = 1 - k = (1+k)u \tag{1}$$

e

$$u(1+k) = 1-k$$

$$[u(1+k)]^* = (1-k)^*$$

$$(1+k)^* u^* = (1-k)^*$$

$$(1+k^*)u^* = (1-k^*)$$

$$(1-k)u^* = 1+k.$$

Além disso, usando (1) obtemos

$$\begin{aligned} u^*(1-k) &= u^*(1+k^*) = u^*(1+k)^* = [(1+k)u]^* \\ &= (1-k)^* = (1-k^*) = 1+k = (1-k)u^*. \end{aligned}$$

Portanto,

$$\begin{aligned} uu^* &= [(1+k)^{-1}(1-k)]u^* = (1+k)^{-1}[(1-k)u^*] \\ &= (1+k)^{-1}(1+k) = 1 \end{aligned}$$

e

$$\begin{aligned} u^*u &= u^*[(1-k)(1+k)^{-1}] = [u^*(1-k)](1+k)^{-1} \\ &= (1+k)(1+k)^{-1} = 1. \end{aligned}$$

■

Os elementos unitários da forma $u = (1-k)(1+k)^{-1}$, onde k é um elemento anti-simétrico tal que $1+k$ é inversível em R, são chamados *elementos unitários de Cayley.*

Lema 1.2.2 *Seja R um anel com involução $*$ no qual 2 é inversível. Então um elemento unitário u é um elemento unitário de Cayley se, e somente se, $1+u$ é inversível em R.*

Prova: [10] Suponha que u seja um elemento unitário de Cayley. Isto é, $u = (1-k)(1+k)^{-1}$ para algum elemento anti-simétrico k tal que $1+k$ seja inversível em R.

Assim, temos

$$(1-k) = 2-(1+k)$$

$$(1-k)(1+k)^{-1} = [2-(1+k)](1+k)^{-1}$$

$$u = 2(1+k)^{-1} - 1$$

$$u+1 = 2(1+k)^{-1}.$$

Logo, vê-se que $1+u$ é inversível em R.

Reciprocamente, suponha que u seja um elemento unitário tal que $1+u$ seja inversível em R.

Considere $k = (1-u)(1+u)^{-1}$. Vemos então

$$k(1+u) = (1-u)$$

$$[k(1+u)]^* = (1-u)^*$$

$$(1+u)^*k^* = 1-u^*$$

$$(1+u^*)k^* = 1-u^*$$

$$u[(1+u^*)k^*] = u(1-u^*)$$

$$[u(1+u^*)]k^* = u-1$$

$$(u+1)k^* = u-1$$

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

isto é, k é um elemento anti-simétrico em R. Além do mais, $1+k = 2(1+u)^{-1}$ é inversível em R.

Assim,

$$1+k = 2(1+u)^{-1}$$

$$(1+k)(1+u) = 2$$

$$(1+k)+(1+k)u = 2$$

$$(1+k)u = 2-(1+k)$$

$$(1+k)u = 1-k$$

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

isto é, u é um elemento unitário de Cayley. ■

1.3 Anéis de Grupos

Sejam K um corpo e G um grupo. A *álgebra de grupo* KG de G sobre K é definida como sendo o K-módulo livre sobre os elementos de G, com a multiplicação induzida pela multiplicação de G, i.e, KG consiste de todas as somas formais finitas da forma

$$\alpha = \sum_{g \in G} \alpha_g g, \qquad \alpha_g \in K,$$

com a soma, multiplicação e multiplicação por escalar dadas por:

(i) $\sum_{g \in G} \alpha_g g + \sum_{g \in G} \beta_g g = \sum_{g \in G} (\alpha_g + \beta_g) g;$

(ii) $\left(\sum_{g \in G} \alpha_g g\right) \cdot \left(\sum_{h \in G} \beta_h h\right) = \sum_{g,h \in G} \alpha_g \beta_h gh = \sum_{t \in G} \delta_t t,$
onde $\delta_t = \sum_{gh=t} \alpha_g \beta_h$;

(iii) $\lambda \left(\sum_{g \in G} \alpha_g g\right) = \sum_{g \in G} (\lambda \alpha_g) g,$ para todo $\lambda \in K$.

Para qualquer elemento $\alpha = \sum_{i=1}^{r} \alpha_i g_i$ em KG, define-se o *suporte* de α como sendo o conjunto $\mathrm{supp}(\alpha) = \{g_i \in G \mid \alpha_i \neq 0\}$.

Seja H um subgrupo normal de G. Definimos $\Delta(G, H)$ como sendo o *ideal* de KG gerado pelo conjunto $\{h - 1 \mid h \in H\}$. Se $H = G$, então denotamos $\Delta(G, G)$ por $\Delta(G)$ e o chamamos de *ideal de aumento de* KG. Note que $\Delta(G)$ é o núcleo do homomorfismo

$$\varepsilon : KG \to K$$

definido por $\varepsilon(\sum_{g\in G}\alpha_g g) = \sum \alpha_g$. Este homomorfismo é chamado o *homomorfismo aumento.*

O conjunto de unidades em KG forma um grupo denotado $U(KG)$, o *grupo das unidades* de KG. Se $\alpha \in U(KG)$, então $\varepsilon(\alpha) \in K^* = K\backslash\{0\}$. Definimos $V(KG)$ como sendo o conjunto

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

que, obviamente, é um subgrupo de $U(KG)$. $V(KG)$ é chamado o *grupo das unidades normalizadas* em KG.

O anti-automorfismo em G, $g \mapsto g^{-1}$, estende-se linearmente a um anti-automorfismo $\alpha \mapsto \alpha^*$ de KG, onde se $\alpha = \sum_{g\in G}\alpha_g g$, então $\alpha^* = \sum_{g\in G}\alpha_g g^{-1}$. É fácil observar que $V(KG)$ é invariante sob este anti-automorfismo. Além disso, a restrição desta aplicação a $V(KG)$ seguido por $v \mapsto v^{-1}$ dá-nos um automorfismo de $V(KG)$. Os elementos de $V(KG)$ fixados por este automorfismo são as *unidades normalizadas unitárias* de KG, e estas formam um subgrupo ao qual denotamos por $V_*(KG)$, o *subgrupo unitário* de KG. Em outras palavras, temos:

$$V_*(KG) = \{\alpha \in V(KG) \mid \alpha^* = \alpha^{-1}\}.$$

O subgrupo unitário $V_*(KG)$ será o objeto de nosso estudo neste trabalho.

Consideramos o *caso modular* em que K é um corpo finito de característica prima p e G é um p-grupo finito. É bem sabido que nestas condições temos:

(i) $|KG| = |K|^{|G|}$;

(ii) $\Delta(G) = \{\alpha \in KG \mid \varepsilon(\alpha) = 0\}$ é um ideal nilpotente;

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

(iv) $KG = U(KG) \cup \Delta(G)$;

(v) $V(KG) = 1 + \Delta(G)$;

(vi) $|V(KG)| = |K|^{|G|-1}$.

A estrutura do grupo $V_*(KG)$ de uma álgebra de grupo de um p-grupo abeliano finito G sobre um corpo finito K de p^m elementos foi plenamente determinada por A. Bovdi e A. Szakács em [4,5]. Já sobre $V_*(KG)$ quando G é não abeliano pouco se sabe (vide [1]). A. Bovdi e L. Erdei [2] descreveram o subgrupo unitário $V_*(\mathbb{F}_2G)$ para todos os grupos de ordem 8 e 16.

Um dos primeiros resultados na investigação do subgrupo unitário $V_*(KG)$ no caso não abeliano pode ser considerado o seguinte resultado devido a V. Bovdi e T. Rozgonyi [8].

Teorema 1.3.1 *Seja G um 2-grupo finito contendo um subgrupo abeliano A de índice 2. Suponha que exista um elemento $b \in G \backslash A$ de ordem 4 tal que $b^{-1}ab = a^{-1}$ para todo $a \in A$. Então o subgrupo unitário $V_*(\mathbb{F}_2G)$ é um produto semidireto de G e um subgrupo*

normal H. O subgrupo H é o produto semidireto do 2-grupo abeliano elementar normal

$$W = \{1 + (1 + b^2)zb \mid z \in \mathbb{F}_2 A\}$$

e o subgrupo abeliano L, onde $V_*(\mathbb{F}_2 A) = A \times L$. O grupo abeliano W é o produto direto de $\frac{1}{2}|A|$ cópias do grupo aditivo do corpo $\mathbb{F}_2$.

Tal resultado foi baseado no seguinte importante resultado de A. Bovdi e A.A. Szakács [4].

Teorema 1.3.2 *Sejam K um corpo de 2^m elementos e G um 2-grupo abeliano finito. Então:*

(i) $V_*(KG) = G \times L$, onde L é um subgrupo abeliano;

(ii) $|V_*(KG)| = |G^2[2]|\ |K|^{\frac{1}{2}(|G|+|G[2]|)-1}$, onde $G[2] = \{g \in G \mid g^2 = 1\}$.

Em seguida, listamos alguns resultados preliminares essenciais na obtenção de nossos novos resultados. Estes são devidos a V. Bovdi e L.G. Kovács [6].

Lema 1.3.3 *Sejam K um anel comutativo com 1 e G um grupo qualquer. Para $x \in V(KG)$ e $y \in V_*(KG)$, temos que $x^{-1}yx \in V_*(KG)$ se e somente se xx^* comuta com y.*

Prova: Basta notarmos que $(x^{-1}yx)^* = (x^{-1}yx)^{-1}$ significa que $x^*y^*(x^*)^{-1} = x^{-1}y^{-1}x$, o que é equivalente a $xx^*y^* = y^{-1}xx^*$. Visto que por hipótese $y^* = y^{-1}$, segue o resultado. ■

É fácil observarmos que, visto que $G \leq V_*(KG)$, qualquer elemento $\alpha \in KG$ que comuta com cada elemento de $V_*(KG)$ é central em KG. Deste modo, o Lema 1.2.3 nos dá o seguinte:

Corolário 1.3.4 *O subgrupo $V_*(KG)$ é normal em $V(KG)$ se e somente se todos os elementos da forma xx^* com $x \in V(KG)$ são centrais em KG.* ■

Teorema 1.3.5 *Sejam K um corpo de característica p e G um p-grupo localmente finito, não abeliano. O subgrupo $V_*(KG)$ é normal em $V(KG)$ se e somente se $p = 2$ e G é o produto direto de um grupo abeliano elementar com um grupo H para o qual vale uma das seguintes:*

(i) H não possui fator direto de ordem 2, mas ele é o produto semidireto de um grupo $\langle b \rangle$ de ordem 2 e um 2-grupo abeliano A tal que $b^{-1}ab = a^{-1}$, para todo $a \in A$.

(ii) H é um 2-grupo extra-especial ou o produto central de um tal grupo com um grupo cíclico de ordem 4.

Uma unidade $\alpha \in V(KG)$ diz-se *simétrica* se possui a propriedade que $\alpha^* = \alpha$. Ao contrário das unidades unitárias, em geral, as unidades simétricas não formam um subgrupo em $V(KG)$. V. Bovdi, L.G. Kovács e S.K. Sehgal [7] caracterizaram os grupos G e os corpos K para os quais o conjunto de unidades simétricas forma um subgrupo, com algumas hipóteses restritivas:

Teorema 1.3.6 *Sejam p um primo, K um anel comutativo de característica p, e G um p-grupo localmente finito não-abeliano. As unidades simétricas de KG formam um grupo multiplicativo se, e somente se, $p = 2$ e G é o produto direto de um grupo abeliano elementar e um grupo H para o qual vale uma das seguintes:*

(i) H possui um subgrupo abeliano A de índice 2 e um elemento b de ordem 4 tal que $b^{-1}ab = a^{-1}$, para todo $a \in A$;

(ii) H é o produto direto de um grupo quatérnio de ordem 8 e um grupo cíclico de ordem 4, ou o produto direto de dois grupos quatérnios de ordem 8;

(iii) H é o produto central do grupo

$$\langle x, y \mid x^4 = y^4 = 1,\ x^2 = [y, x] \rangle$$

com um grupo quatérnio de ordem 8, o elemento não-trivial comum aos dois grupos sendo x^2y^2;

(iv) H é isomorfo a um dos grupos

$$H_{32} = \langle x, y, u \mid x^4 = y^4 = 1, x^2 = [y, x], y^2 = u^2 = [u, x], x^2y^2 = [u, y] \rangle$$

$$H_{245} = \langle x, y, u, v \mid x^4 = y^4 = [v, u] = 1, x^2 = v^2 = [y, x] = [v, y]$$
$$y^2 = u^2 = [u, x], x^2y^2 = [u, y] = [v, x]\rangle.$$

Visto que $(\alpha^*)^* = \alpha$ e $(\alpha\beta)^* = \beta^*\alpha^*$, para todos $\alpha, \beta \in KG$, segue que todos os elementos da forma $\alpha\alpha^*$, com $\alpha \in V(KG)$, é uma unidade simétrica.

Observamos que se $V_*(KG)$ é normal em $V(KG)$, pelo Corolário 1.3.4, todo elemento da forma xx^* com $x \in V(KG)$ é central em KG. Como cada unidade em KG é um múltiplo escalar de uma unidade normalizada, a mesma conclusão é adequada se x é uma unidade qualquer em KG. Deste modo, se $x \in U(KG)$, então

$$xx^* = x^{-1}(xx^*)x = x^*x.$$

Agora, se $x \notin U(KG)$, então $x \in \Delta(G)$ e disto $1 + x$ é uma unidade e então vale

$$(1 + x)(1 + x)^* = (1 + x)^*(1 + x),$$

e, conseqüentemente, novamente temos $xx^* = x^*x$.

Uma álgebra de grupo KG na qual $xx^* = x^*x$ vale para cada elemento $x \in KG$ é chamada *normal*. A. Bovdi, P.M. Gudivok e M.S. Semirot provaram em [3] que a álgebra de grupo de um grupo não abeliano G sobre um anel comutativo K é normal se e somente se G é hamiltoniano ou a característica de K é 2 e G é um produto direto de um 2-grupo abeliano elementar com um grupo H tal que (i) ou (ii) do Teorema 1.3.5 vale.

Capítulo 2

A ordem do subgrupo unitário para característica $p > 2$

Neste capítulo determinamos a ordem do subgrupo unitário $V_*(KG)$ da álgebra de grupo KG no caso em que a característica de K é $p > 2$ e G é um p-grupo finito.

Ainda neste, determinamos a ordem do importante conjunto

$$S_*(KG) = \{\alpha \in V(KG) \mid \alpha^* = \alpha\},$$

o conjunto das unidades normalizadas simétricas da álgebra de grupo KG para a característica $p > 2$.

2.1 p-grupos finitos ($p > 2$)

Sejam K um corpo finito com $\mathrm{char}(K) = p > 2$ e G um p-grupo finito.

O conjunto

$$\left\{\alpha = \sum_{g\in G} \alpha_g g \in KG \mid \varepsilon(\alpha) = \sum_{g\in G} \alpha_g = 0\right\}$$

é um ideal na álgebra de grupo KG, denotado por $\Delta(G)$ e chamado de *ideal de aumento* da álgebra KG. Isto é, $\Delta(G)$ é o conjunto de todos os elementos em KG de aumento zero.

Considere

$$S_+(\Delta(G)) = \{\alpha \in \Delta(G) \mid \alpha^* = \alpha\}$$

o *conjunto de elementos simétricos de aumento zero* em KG e

$$S_-(\Delta(G)) = \{\alpha \in \Delta(G) \mid \alpha^* = -\alpha\}$$

o *conjunto de elementos anti-simétricos de aumento zero* em KG.

Lema 2.1.1 *Sejam K um corpo com* $\mathrm{char}(K) = p > 2$ *e G um grupo de ordem ímpar. Então,*

(i) $\Delta(G) = S_+(\Delta(G)) + S_-(\Delta(G))$;

(ii) $S_+(\Delta(G)) \cap S_-(\Delta(G)) = \{0\}$.

Assim, $\Delta(G) = S_+(\Delta(G)) \oplus S_-(\Delta(G))$ *como* K*-espaços.*

Prova: (i) Seja $\alpha \in \Delta(G)$.

Tomemos $\beta = \frac{\alpha+\alpha^*}{2}$ e $\gamma = \frac{\alpha-\alpha^*}{2}$. Facilmente, vê-se que $\beta^* = \beta$, $\gamma^* = -\gamma$ e $\alpha = \beta + \gamma$, donde de conclui que $\Delta(G) \subset S_+(\Delta(G)) + S_-(\Delta(G))$. Portanto, $\Delta(G) = S_+(\Delta(G)) + S_-(\Delta(G))$.

(ii) Seja $\alpha = \sum_{g \in G} \alpha_g g \in S_+(\Delta(G)) \cap S_-(\Delta(G))$. Então,

$$\alpha = \alpha^* = -\alpha$$

$$2\alpha = 0$$

$$\alpha_g = 0, \quad \forall g \in G,$$

visto que $\mathrm{char}(K) \neq 2$.

Portanto, $\alpha = 0$ e $S_+(\Delta(G)) \cap S_-(\Delta(G)) = \{0\}$. ■

Corolário 2.1.2 *Seja* KG *uma álgebra de grupo finita de característica* $p > 2$*, então*

$$|\Delta(G)| = |S_+(\Delta(G))| \cdot |S_-(\Delta(G))|. \qquad ■$$

Exemplo 2.1.3 Considere a álgebra de grupo $\mathbf{Z}_3 G$, onde $G = \langle a | a^3 = 1 \rangle$. Temos então:

(i) $|\mathbf{Z}_3G| = |\mathbf{Z}_3|^{|G|} = 3^3 = 27$;

(ii) $|V(\mathbf{Z}_3G)| = |\mathbf{Z}_3|^{|G|-1} = 3^2 = 9$;

(iii) $|\Delta(G)| = |V(\mathbf{Z}_3G)| = 9$.

É fácil observarmos que

$$\begin{aligned}\Delta(G) &= \left\{\alpha = \sum_{i=0}^{2} \alpha_i a^i \in \mathbf{Z}_3G \mid \varepsilon(\alpha) = \sum_{i=0}^{2} \alpha_i = 0\right\} \\ &= \{0,\ 1+2a,\ 1+2a^2,\ 2+a,\ 2+a^2, a+2a^2, \\ &\qquad 2a+a^2,\ 1+a+a^2,\ 2+2a+2a^2\}.\end{aligned}$$

Assim,

$$\begin{aligned}S_+(\Delta(G)) &= \{\alpha \in \Delta(G) \mid \alpha^* = \alpha\} \\ &= \{0,\ 1+a+a^2,\ 2+2a+2a^2\}\end{aligned}$$

e

$$\begin{aligned}S_-(\Delta(G)) &= \{\alpha \in \Delta(G) \mid \alpha^* = -\alpha\} \\ &= \{0,\ 2a+a^2,\ a+2a^2\},\end{aligned}$$

onde se vê, $|S_+(\Delta(G))| \cdot |S_-(\Delta(G))| = |\Delta(G)|$ e $\Delta(G) = S_+(\Delta(G)) \oplus S_-(\Delta(G))$.

Lema 2.1.4 *Sejam K um corpo finito de característica $p > 2$ e G um grupo finito de ordem ímpar. Então*

$$|S_+(\Delta(G))\ | = |K|^{\frac{|G|-1}{2}}.$$

Prova: Seja $x = \sum_{g \in G} \alpha_g g \in S_+(\Delta(G))$. Visto que $x^* = x$, temos que

$$\operatorname{supp}(x) = \operatorname{supp}(x^*) \ \text{ e } \ \alpha_g = \alpha_{g^{-1}}, \ \ \forall g \in \operatorname{supp}(x).$$

Logo,

$$x = \alpha_1 + \sum_{\substack{g \in G \\ g \neq 1}} \alpha_g (g + g^{-1}) \ \text{ com } \ \sum_{g \in G} \alpha_g \equiv 0 \pmod p.$$

Mas,

$$\varepsilon(x) = \alpha_1 + 2 \sum_{\substack{g \in G \\ g \neq 1}} \alpha_g = 0,$$

isto é,

$$\alpha_1 + 2 \sum_{g \neq 1} \alpha_g \equiv 0 \pmod p$$

$$\alpha_1 \equiv -2 \sum_{g \neq 1} \alpha_g \pmod p.$$

Portanto,

$$\begin{aligned} x &= \alpha_1 + \sum_{\substack{g \in G \\ g \neq 1}} \alpha_g (g + g^{-1}) \\ &= -2 \sum_{\substack{g \in G \\ g \neq 1}} \alpha_g + \sum_{\substack{g \in G \\ g \neq 1}} \alpha_g (g + g^{-1}) \\ &= \sum_{\substack{g \in G \\ g \neq 1}} \alpha_g (g + g^{-1} - 2). \end{aligned}$$

Assim,

$$S_+(\Delta(G)) = \left\{ x = \sum_{\substack{g \in G \\ g \neq 1}} \alpha_g (g + g^{-1} - 2) \mid \alpha_g \in K \right\},$$

donde se conclui que

$$|S_+(\Delta(G))| = |K|^{\frac{|G|-1}{2}}.$$

■

Exemplo 2.1.5 Considere a álgebra de grupo $\mathbf{Z}_5G$, onde $G = \langle a | a^5 = 1 \rangle$. Temos pelo Lema 2.1.4 que $|S(\Delta(G))| = 5^2 = 25$. A saber,

$$\begin{aligned} S(\Delta(G)) &= \{\alpha_1(a + a^4 - 2) + \alpha_2(a^2 + a^3 - 2) \mid \alpha_i \in \mathbf{Z}_5,\ i = 1,2\} \\ &= \{-2(\alpha_1 + \alpha_2) + \alpha_1(a + a^4) + \alpha_2(a^2 + a^3) \mid \alpha_i \in \mathbf{Z}_5,\ i = 1,2\} \\ &= \{3(\alpha_1 + \alpha_2) + \alpha_1(a + a^4) + \alpha_2(a^2 + a^3) \mid \alpha_i \in \mathbf{Z}_5,\ i = 1,2\}. \end{aligned}$$

Corolário 2.1.6 *Sejam K um corpo finito de característica $p > 2$ e G um p-grupo finito. Então*

$$|S_-(\Delta(G))| = |K|^{\frac{|G|-1}{2}}.$$

■

Corolário 2.1.7 *Sejam K um corpo finito de característica $p > 2$ e G um p-grupo finito. Então*

$$|S_*(KG)| = |K|^{\frac{|G|-1}{2}}.$$

Prova: Seja $\alpha = \sum_{g \in G} \alpha_g g \in S_*(KG)$. Logo $\alpha^* = \alpha$ e $\varepsilon(\alpha) = \sum_{g \in G} \alpha_g = 1$. Assim,

$$\mathrm{supp}(\alpha^*) = \mathrm{supp}(\alpha),$$

$$\alpha_g = \alpha_{g^{-1}}, \quad \forall g \in \mathrm{supp}(\alpha) \quad \text{e} \quad \sum_{g \in G} \alpha_g = 1.$$

Assim, $\alpha = \alpha_1 + \sum_{\substack{g \in G \\ g \neq 1}} \alpha_g (g + g^{-1})$.

Logo,

$$\begin{aligned}\varepsilon(\alpha) &= \alpha_1 + \sum_{g\neq 1} 2\alpha_g = 1\\ \alpha_1 &\equiv 1 - 2\sum_{g\neq 1}\alpha_g \pmod p.\end{aligned}$$

Deste modo,

$$\begin{aligned}\alpha &= \left(1 - 2\sum_{\substack{g\in G\\ g\neq 1}}\alpha_g\right) + \sum_{\substack{g\in G\\ g\neq 1}}\alpha_g(g+g^{-1})\\ \alpha &= 1 + \sum_{\substack{g\in G\\ g\neq 1}}\alpha_g(g+g^{-1}-2)\end{aligned}$$

e então

$$|S_*(KG)| = |K|^{\frac{|G|-1}{2}}.$$

Na realidade, observamos que

$$S_*(KG) = 1 + S_+(\Delta(G)).$$

■

Teorema 2.1.8 *Sejam K um corpo finito de característica $p > 2$ e G um p-grupo finito. Então*

$$|V_*(KG)| = |K|^{\frac{|G|-1}{2}}.$$

Prova: Observemos que, se $x \in S_-(\Delta(G))$, então visto que $U(KG) = \{\alpha \in KG | \varepsilon(\alpha) \neq 0\}$, o elemento $1 + x$ é uma unidade em KG e, pelo Lema 1.2.2, $u = (1-x)(1+x)^{-1}$ é uma unidade unitária de Cayley.

É fácil observarmos que qualquer elemento em $V_*(KG)$ é uma unidade unitária de Cayley para $\mathrm{char}(K) > 2$.

De fato, se $u \in V_*(KG)$ então $\varepsilon(u) = 1$ e $1 + u$ é uma unidade, visto que

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

Assim, $k = (1 - u)(1 + u)^{-1}$ é um elemento anti-simétrico em KG. Logo, $1 + k = 2(1 + u)^{-1}$ é uma unidade em KG, e $u = (1 - k)(1 + k)^{-1}$ é uma unidade unitária de Cayley.

Portanto,

$$|V_*(KG)| = |S_-(\Delta(G))| = |K|^{\frac{|G|-1}{2}}.$$

■

Capítulo 3

A ordem do subgrupo unitário para alguns produtos centrais

Neste capítulo determinamos a ordem do subgrupo unitário $V_*(KG)$ da álgebra de grupo KG quando K é um corpo finito de característica 2 e G é um 2-grupo extra-especial ou um produto central de um 2-grupo extra-especial com um grupo cíclico de ordem 4.

3.1 2-grupo extra-especial

Para uma álgebra de grupo KG, denotamos $S_K(G) = \{xx^* \mid x \in V(KG)\}$ que é, como já visto, um conjunto de unidades simétricas em KG.

Lema 3.1.1 *Se $V_*(KG)$ é normal em $V(KG)$, então $S_K(G)$ é um subgrupo normal em $V(KG)$.*

Prova: Sendo $V_*(KG) \triangleleft V(KG)$, segue que a álgebra KG é normal, i.e, $xx^* = x^*x$, para todo $x \in KG$, pela conclusão do capítulo 1. Pelo Corolário 1.3.4, temos também que xx^* é central em KG sempre que $x \in V(KG)$. Logo,nós temos

$$\begin{aligned}(xx^*)(yy^*)^{-1} &= xx^*(y^*)^{-1}y^{-1} = xx^*(y^{-1})^*y^{-1} \\ &= (y^{-1})^*xx^*y^{-1} = (y^{-1})^*x^*xy^{-1} = (xy^{-1})^*(xy^{-1}) \\ &= (xy^{-1})(xy^{-1})^*,\end{aligned}$$

para todos x, y em $V(KG)$, o que nos diz que $S_K(G)$ é um subgrupo em $V(KG)$. A normalidade de $S_K(G)$ segue do fato que cada elemento de $S_K(G)$ é estável por conjugação em $V(KG)$. ■

Lema 3.1.2 *Sejam K um corpo de característica 2 e G um 2-grupo extra-especial. Então a aplicação $x \mapsto xx^*$ é um epimorfismo do grupo $V(KG)$ no subgrupo $S_K(G)$. Além disso, se $V(KG)$ é finito, então a ordem do subgrupo unitário $V_*(KG)$ coincide com o índice do subgrupo $S_K(G)$ em $V(KG)$.*

Prova: Pelo Teorema 1.3.5 e Corolário 1.3.4, temos que xx^* é central em $V(KG)$ para todo $x \in V(KG)$. Fazendo $\phi(x) = xx^*$, temos

$$\phi(xy) = (xy)(xy)^* = xyy^*x^* = xx^*yy^* = \phi(x)\phi(y)$$

para todos $x, y \in V(KG)$. Portanto, ϕ é um epimorfismo. Agora, o núcleo de ϕ é

$$\{x \in V(KG) \mid xx^* = 1\},$$

facilmente visto ser $V_*(KG)$, donde segue o resto do Lema. ■

Para um 2-grupo finito G com subgrupo comutador $G' = \langle c \mid c^2 = 1\rangle$, definimos L_G como sendo um subconjunto de elementos de ordem 4 em G tal que $L_G \cap L_G c$ é vazio e $L_G \cup L_G c$ coincide com o conjunto de todos os elementos de ordem 4 em G.

Lema 3.1.3 *Seja G um 2-grupo extra-especial de ordem $|G| = 2^{2n+1}$, com $n \geq 2$. Então*

$$|L_G| = 2^{n-1}(2^n - (-1)^n).$$

Prova: Sendo G um 2-grupo extra-especial de ordem $|G| = 2^{2n+1}$, com $n \geq 2$, então, pelo Corolário 1.1.8, nós temos $G = G_1 \curlyvee \cdots \curlyvee G_n$, onde G_i é um grupo quatérnio de ordem 8. Então, $Z(G) = G' = \langle c \mid c^2 = 1\rangle$ e $G_i \cap G_j = \langle c\rangle$ para quaisquer $i \neq j$. Evidentemente cada elemento de ordem 4 de G pode ser escrito como

$$x = z_{i_1} z_{i_2} \ldots z_{i_s}, \tag{1}$$

onde $z_{i_k} \in G_{i_k}$ tem ordem 4 e $i_1 < i_2 < \cdots < i_s$. Chamamos s o comprimento de x. Pelo fato que $Z(G) = G'$ e do Lema 1.1.3, nós temos que $z_{i_k}^2 = c$ e $x^2 = z_{i_1}^2 z_{i_2}^2 \cdots z_{i_s}^2 = c^s$. Sendo a ordem de x igual a 4, devemos ter $s \equiv 1 \pmod 2$, i.e, s deve ser ímpar.

Considere $H_k = H(i_1, i_2, \ldots, i_k) = G_{i_1} \curlyvee G_{i_2} \curlyvee \cdots \curlyvee G_{i_k}$, onde k é ímpar e $i_1 < i_2 < \cdots < i_k$. Nosso objetivo aqui é mostrar que existem precisamente 3^k elementos de comprimento k em L_{H_k}. Cada L_{G_i} contém três diferentes elementos e cada elemento de comprimento k da forma (1) tem ordem 4. Portanto, o número de elementos de L_{H_k} é 3^k. Agora, o número de diferentes subgrupos H_k de G é $\binom{n}{k}$ e, então, o número de elementos de L_G é

$$|L_G| = \sum_{j=1}^{m} \binom{n}{2j-1} 3^{2j-1},$$

onde $m = \frac{n+1}{2}$ se n é ímpar e $m = \frac{n}{2}$ se n é par.

Se escrevemos

$$M_1 = 2^{2n} = (1+3)^n = \sum_{i=0}^{n} \binom{n}{i} 3^i,$$

e

$$M_2 = (-1)^n 2^n = (1-3)^n = \sum_{i=0}^{n} \binom{n}{i} (-1)^i 3^i,$$

então podemos obter

$$\begin{aligned} |L_G| &= \sum_{j=1}^{m} \binom{n}{2j-1} 3^{2j-1} = \frac{1}{2}\left(\sum_{i=0}^{n} \binom{n}{i} 3^i - \sum_{i=0}^{n} \binom{n}{i} (-1)^i 3^i\right) \\ &= \frac{1}{2}(M_1 - M_2) = 2^{n-1}(2^n - (-1)^n). \end{aligned}$$

■

Lema 3.1.4 *Sejam K um corpo finito de característica 2 e G um 2-grupo extra-especial de ordem $|G| = 2^{2n+1}$, com $n \geq 2$. Então, para todo $x \in V(KG)$,*

$$xx^* = \prod_{b \in L_G} (1 + \alpha_b b(1 + c)),$$

onde $\alpha_b \in K$.

Prova: Seja $x = \sum_{i=1}^{t} \alpha_i a_i \in V(KG)$. Então $x^* = \sum_{i=1}^{t} \alpha_i a_i^{-1}$ e

$$\begin{aligned} xx^* &= (\alpha_1 a_1 + \cdots + \alpha_t a_t)(\alpha_1 a_1^{-1} + \cdots + \alpha_t a_t^{-1}) \\ &= (\alpha_1^2 + \cdots + \alpha_t^2) + \sum_{\substack{i,j \\ i<j}} \alpha_i \alpha_j (a_i a_j^{-1} + a_j a_i^{-1}). \end{aligned}$$

Temos que analisar dois casos sobre a ordem de $a_i a_j^{-1}$:

Se a ordem de $a_i a_j^{-1}$ é 2, então $a_i a_j^{-1} = (a_i a_j^{-1})^{-1} = a_j a_i^{-1}$. Assim, o suporte de xx^* não contém elementos de ordem 2.

Portanto, a ordem de $a_i a_j^{-1}$ deve ser 4. Visto que $g^2 \in G' = \langle c \mid c^2 = 1 \rangle$, para todo $g \in G$, devemos ter $(a_i a_j^{-1})^2 = c$ e disto $a_i a_j^{-1} = c a_j a_i^{-1}$. Como $\varepsilon(x) = \sum_{i=1}^{t} \alpha_i = 1$ e característica de K é 2, segue que

$$xx^* = 1 + \sum_{\substack{i,j \\ i<j}} \alpha_{ij} a_i a_j^{-1} (1 + c),$$

com $a_i a_j^{-1} \in L_G$. Denotando $a_i a_j^{-1}$ por b e observando que $(1 + c)^2 = 0$, segue que

$$xx^* = 1 + \sum_{b \in L_G} \alpha_b b(1 + c) = \prod_{b \in L_G} (1 + \alpha_b b(1 + c)).$$

■

Teorema 3.1.5 *Sejam K um corpo finito de característica 2 e G um 2-grupo extra-especial de ordem $|G| = 2^{2n+1}$, com $n \geq 2$. Então*

$$|V_*(KG)| = |K|^{2^{n-1}(2^{n+2}-2^n+(-1)^n)-1}.$$

Prova: Vemos claramente pelo Lema 3.1.4 que a ordem de $S_K(G) = \{xx^* \mid x \in V(KG)\}$ é no máximo $|K|^{|L_G|}$. Nosso objetivo aqui é provar que $|S_K(G)|$ é exatamente $|K|^{|L_G|}$.

Tome $b \in L_G$ arbitrário e um $\alpha_b \in K$. Então existe um elemento $\omega_b \in G$ de ordem 2 tal que $[\omega_b, b] \neq 1$. De fato, sendo $b = z_{i_1} z_{i_2} \cdots z_{i_{2k+1}} \in L_G$, então escolhemos um $u_1 \in G_{i_1}$ de ordem 4 tal que $[u_1, z_{i_1}] \neq 1$ e um elemento u_2 do conjunto $\{z_{i_2}, \ldots, z_{i_{2k+1}}\}$ se $k \neq 0$, e caso $k = 0$, escolhemos u_2 de G_t para algum $t \neq i_1$ com $|u_2| = 4$. Assim, $\omega_b = u_1 u_2$ é um elemento de ordem 2 em G tal que $[\omega_b, b] \neq 1$.

Agora,

$$\begin{aligned}
(1+\alpha_b(b+\omega_b)).(1+\alpha_b(b+\omega_b))^* &= (1+\alpha_b(b+\omega_b)).(1+\alpha_b(b^{-1}+\omega_b^{-1}) \\
&= (1+\alpha_b(b+\omega_b)).(1+\alpha_b(cb+\omega_b) \\
&= 1+\alpha_b(cb+\omega_b)+\alpha_b(b+\omega_b) \\
&\quad +\alpha_b^2(b+\omega_b)(cb+\omega_b) \\
&= 1+\alpha_b b(1+c)+\alpha_b^2(1+b\omega_b+c\omega_b b+1) \\
&= 1+\alpha_b b(1+c)+\alpha_b^2(b\omega_b+b\omega_b) \\
&= 1+\alpha_b b(1+c),
\end{aligned}$$

que nos mostra que qualquer fator do produto $\prod_{b\in L_G}(1+\alpha_b b(1+c))$ pertence ao subgrupo $S_K(G)$.

Como uu^* é central em KG para qualquer $u \in V(KG)$, conforme Corolário 1.3.4, temos ainda que

$$\begin{aligned}
&\prod_{b\in L_G}(1+\alpha_b(b+\omega_b))(1+\alpha_b(b+\omega_b))^* = \\
&\quad = (1+\alpha_{b_1}(b_1+\omega_{b_1}))(1+\alpha_{b_1}(b_1+\omega_{b_1}))^*(1+\alpha_{b_2}(b_2+\omega_{b_2}))(1+\alpha_{b_2}(b_2+\omega_{b_2}))^*\cdots \\
&\qquad \cdots(1+\alpha_{b_t}(b_t+\omega_{b_t}))(1+\alpha_{b_t}(b_t+\omega_{b_t}))^* \\
&\quad = (1+\alpha_{b_1}(b_1+\omega_{b_1}))(1+\alpha_{b_2}(b_2+\omega_{b_2}))(1+\alpha_{b_2}(b_2+\omega_{b_2}))^*(1+\alpha_{b_1}(b_1+\omega_{b_1}))^*\cdots \\
&\qquad \cdots(1+\alpha_{b_t}(b_t+\omega_{b_t}))(1+\alpha_{b_t}(b_t+\omega_{b_t}))^* \\
&\quad = (1+\alpha_{b_1}(b_1+\omega_{b_1}))(1+\alpha_{b_2}(b_2+\omega_{b_2}))(1+\alpha_{b_3}(b_3+\omega_{b_3}))(1+\alpha_{b_3}(b_3+\omega_{b_3}))^*\cdots \\
&\qquad \cdots(1+\alpha_{b_t}(b_t+\omega_{b_t}))(1+\alpha_{b_t}(b_t+\omega_{b_t}))^*,
\end{aligned}$$

assim, observando que

$$(u_1u_2\cdots u_nu_n^*\cdots u_2^*u_1^*)u_{n+1}u_{n+1}^* = u_1u_2\cdots u_nu_{n+1}u_{n+1}^*u_n^*\cdots u_2^*u_1^*, \forall n$$

temos que após $(t-1)$ passos obtemos,

$$\begin{aligned}
&\prod_{b\in L_G}(1+\alpha_b(b+\omega_b))(1+\alpha_b(b+\omega_b))^* = \\
&\quad = (1+\alpha_{b_1}(b_1+\omega_{b_1}))(1+\alpha_{b_2}(b_2+\omega_{b_2}))\cdots(1+\alpha_{b_t}(b_t+\omega_{b_t}))(1+\alpha_{b_t}(b_t+\omega_{b_t}))^*\cdots \\
&\qquad \cdots(1+\alpha_{b_2}(b_2+\omega_{b_2}))^*(1+\alpha_{b_1}(b_1+\omega_{b_1}))^* \\
&\quad = (1+\alpha_{b_1}(b_1+\omega_{b_1}))(1+\alpha_{b_2}(b_2+\omega_{b_2}))\cdots(1+\alpha_{b_t}(b_t+\omega_{b_t})). \\
&\qquad .((1+\alpha_{b_1}(b_1+\omega_{b_1}))(1+\alpha_{b_2}(b_2+\omega_{b_2}))\cdots(1+\alpha_{b_t}(b_t+\omega_{b_t})))^* \\
&\quad = \prod_{b\in L_G}(1+\alpha_b(b+\omega_b)).\left(\prod_{b\in L_G}(1+\alpha_b(b+\omega_b))\right)^*,
\end{aligned}$$

o que nos mostra que $\prod_{b\in L_G}(1+\alpha_b(b+\omega_b))(1+\alpha_b(b+\omega_b))^*$ pertence ao subgrupo $S_K(G)$.

Portanto, temos que $|S_K(G)| = |K|^{|L_G|}$. Agora, pelo Lema 3.1.2, temos que $|V_*(KG)| = |V(KG)|/|S_K(G)|$. Como $|V(KG)| = |K|^{|G|-1} = |K|^{2^{2n+1}-1}$ e, pelo Lema 3.1.3, vemos que $|L_G| = 2^{n-1}(2^n - (-1)^n)$, segue que

$$\begin{aligned} |V_*(KG)| &= |K|^{2^{2n+1}-1}.|K|^{-2^{n-1}(2^n-(-1)^n)} \\ &= |K|^{2^{n-1}(2^{n+2}-2^n+(-1)^n)-1}. \end{aligned}$$

■

3.2 Produto central de um 2-grupo extra-especial com um grupo cíclico de ordem 4

Neste parágrafo determinamos a ordem do subgrupo unitário $V_*(KG)$ quando K é um corpo finito de característica 2 e $G = H\curlyvee C_4$, onde H é um 2-grupo extra-especial de ordem $|H| = 2^{2n+1}$ e $C_4 = \langle d\rangle$ é um grupo cíclico de ordem 4. Uma vez já analisado o caso em que G é um 2-grupo extra-especial, torna-se de fácil análise esta nova situação.

Lema 3.2.1 *Sejam K um corpo finito de característica 2 e G um produto central de um 2-grupo extra-especial H de ordem $|H| = 2^{2n+1}$ com um grupo cíclico $\langle d\rangle$ de ordem 4. Então a aplicação $x \mapsto xx^*$ é um epimorfismo do grupo $V(KG)$ no subgrupo $S_K(G)$. Além disso, se $V(KG)$ é finito , então a ordem do subgrupo unitário $V_*(KG)$ coincide com o índice do subgrupo $S_K(G)$ em $V(KG)$.*

Prova: É só observarmos que, pelo Teorema 1.3.5 e Corolário 1.3.4, nós temos que xx^* é central em $V(KG)$ para todo $x \in V(KG)$. A conclusão deste Lema segue análoga à do Lema 3.1.2. ■

Lema 3.2.2 *Seja G um produto central de um 2-grupo extra-especial H de ordem $|H| = 2^{2n+1}$ com um grupo cíclico $\langle d \rangle$ de ordem 4. Então*

$$|L_G| = 2^{2n}.$$

Prova: Sendo $G = H \curlyvee \langle d \rangle$ com H um 2-grupo extra-especial de ordem 2^{2n+1} e $\langle d \rangle$ de ordem 4, temos identificado que $d^2 = c$, onde $G' = Z(G) = \langle c \mid c^2 = 1 \rangle$. Logo, visto que $H = H_1 \curlyvee \cdots \curlyvee H_n$, com $H_i \cong Q_8$, $1 \leq i \leq n$, temos que cada elemento de ordem 4 em G pode ser escrito como

$$x = z_{i_1} z_{i_2} \cdots z_{i_s} d^k,$$

onde $z_{i_t} \in H_{i_t}$ tem ordem 4, com $i_1 < \cdots < i_s$ e $k = 0, 1$. Como antes observamos no Lema 3.1.3, visto que ordem de x é 4 e $x^2 = z_{i_1}^2 z_{i_2}^2 \cdots z_{i_s}^2 d^{2k} = c^{s+k}$, devemos ter $k = 0$ e s ímpar ou que $k = 1$ e s par. Deste modo, concluímos que qualquer elemento de ordem 4 em G ou pertence a H ou pode ser escrito como hd, onde $h \in H$ e $|h| \neq 4$. O número de elemento de ordem 4 exclusivamente de H é igual a $|L_H|$. Agora, o número de elementos $h \in H$ com $|h| \neq 4$ é igual a $|H| - 2|L_H|$. Portanto, concluímos que

$$|L_G| = |L_H| + \frac{|H| - 2|L_H|}{2} = \frac{|H|}{2} = 2^{2n}.$$

■

Teorema 3.2.3 *Sejam K um corpo finito de característica 2 e G um produto central de um 2-grupo extra-especial H de ordem $|H| = 2^{2n+1}$ com um grupo cíclico $\langle d \rangle$ de ordem 4. Então*

$$|V_*(KG)| = |K|^{3.2^{2^n}-1}.$$

Prova: De forma análoga à análise feita no Lema 3.1.4, vê-se que para todo $x \in V(KG)$, com $G = H \curlyvee \langle d \rangle$, temos que

$$xx^* = 1 + \sum_{b \in L_G} \alpha_b b(1+c) = \prod_{b \in L_G} (1 + \alpha_b b(1+c)).$$

Como $H = H_1 \curlyvee \cdots \curlyvee H_n$, onde $H_i \cong Q_8$ e $1 \leq i \leq n$, é um 2-grupo extra-especial de ordem $|H| = 2^{2n+1}$, pela prova do Teorema 3.1.5 vemos que $1 + \alpha_b b(1+c) \in S_K(G)$, para todo $b \in L_H$, e por conseguinte $1 + \sum_{b \in L_G} \alpha_b b(1+c) \in S_K(G)$. Portanto, nós temos que

$$|K|^{|L_H|} \leq |S_K(G)| \leq |K|^{|L_G|}.$$

Objetivamos aqui mostrar que $|S_K(G)| = |K|^{|L_G|}$. Para isto, devemos mostrar que $1 + \alpha_{hd} hd(1+c) \in S_K(G)$ com $h \in H$ e $|h| \neq 4$.

Seja dado o elemento $hd \in G$ com $h \in H$ e $|h| \neq 4$. Obviamente, temos que $hd \in L_G$.

Se $h = 1$, então tomando $x = 1 + a_i + d$ e $y = 1 + a_i + b_i d$, que são unidades evidentemente, onde $H_i = \langle a_i, b_i \rangle$ para algum $i \in \{1, 2, \ldots, n\}$, obtemos então que

$$\begin{aligned} xx^* &= (1 + a_i + d)(1 + a_i + d)^* = (1 + a_i + d)(1 + a_i^{-1} + d^{-1}) \\ &= (1 + a_i + d)(1 + a_i c + dc) \\ &= 1 + a_i c + dc + a_i + 1 + a_i dc + d + da_i c + 1 \\ &= 1 + (a_i + d)(1 + c) \end{aligned}$$

e

$$\begin{aligned} yy^* &= (1 + a_i + b_i d)(1 + a_i + b_i d)^* = (1 + a_i + b_i d)(1 + a_i^{-1} + d^{-1} b_i^{-1}) \\ &= (1 + a_i + b_i d)(1 + a_i c + b_i d) \\ &= 1 + a_i c + b_i d + a_i + 1 + a_i b_i d + b_i d + b_i a_i dc + 1 \\ &= 1 + a_i(1 + c), \end{aligned}$$

visto que $a_i^{b_i} = a_i^{-1} = a_i c$, $[H_i, \langle d \rangle] = 1$ e $g^2 \in G' = Z(G) = \langle c \mid c^2 = 1 \rangle$, para todo $g \in G$.

Portanto, obtemos que

$$\begin{aligned} 1 + d(1 + c) &= 1 + (a_i + d + a_i)(1 + c) \\ &= (1 + (a_i + d)(1 + c))(1 + a_i(1 + c)) \\ &= (xx^*)(yy^*) \\ &= xyy^*x^* = (xy)(xy)^* \in S_K(G), \end{aligned}$$

visto que, pelo Teorema 1.3.5 e Corolário 1.3.4, temos que yy^* é central em KG.

Agora, se $|h| = 2$, então h pode ser escrito como

$$h = z_{i_1} z_{i_2} \cdots z_{i_{2k}},$$

onde $z_{i_t} \in H_{i_t}$ tem ordem 4, com $i_1 < \cdots < i_{2k}$. Neste caso, basta-nos tomar $x = 1 + z_{i_1} + hd$ e $y = 1 + z_{i_1} + u_1 hd$, onde u_1 é um outro elemento de H_{i_1} de ordem 4 e tal que $[u_1, z_{i_1}] \neq 1$. É óbvio que a ordem de $u_1 hd$ é 2. Assim, temos que

$$\begin{aligned}
xx^* &= (1 + z_{i_1} + hd)(1 + z_{i_1} + hd)^* \\
&= (1 + z_{i_1} + hd)(1 + z_{i_1}^{-1} + (hd)^{-1}) \\
&= (1 + z_{i_1} + hd)(1 + z_{i_1} c + hdc) \\
&= 1 + z_{i_1} c + hdc + z_{i_1} + 1 + z_{i_1} hdc + hd + hz_{i_1} dc + 1 \\
&= 1 + (z_{i_1} + hd)(1 + c)
\end{aligned}$$

e

$$\begin{aligned}
yy^* &= (1 + z_{i_1} + u_1 hd)(1 + z_{i_1} + u_1 hd)^* \\
&= (1 + z_{i_1} + u_1 hd)(1 + z_{i_1}^{-1} + (u_1 hd)^{-1}) \\
&= (1 + z_{i_1} + u_1 hd)(1 + z_{i_1} c + u_1 hd) \\
&= 1 + z_{i_1} c + u_1 hd + z_{i_1} + 1 + z_{i_1} u_1 hd + u_1 hd + u_1 z_{i_1} hdc + 1 \\
&= 1 + z_{i_1}(1 + c),
\end{aligned}$$

visto que, se $[u_1, z_{i_1}] \neq 1$, então $[u_1, z_{i_1}] = c$, pois $G' = \langle c \mid c^2 = 1 \rangle$. Da mesma forma que acima, nós temos

$$1 + hd(1 + c) = xx^* yy^* = (xy)(xy)^* \in S_K(G).$$

Deste modo, concluímos que $|S_K(G)| = |K|^{|L_G|}$. Visto que $|V(KG)| = |K|^{|G|-1} = |K|^{2^{2n+2}-1}$, pelo Lema 3.2.1 e Lema 3.2.2 obtemos que

$$|V_*(KG)| = |K|^{2^{2n+2}-1}.|K|^{-2^{2n}} = |K|^{2^{2n}(2^2-1)-1} = |K|^{3\cdot 2^{2n}-1}.$$

■

Capítulo 4

A ordem do subgrupo unitário para os 2-grupos diedrais e para os quatérnios generalizados

Neste capítulo determinamos a ordem do subgrupo unitário $V_*(KG)$ quando K é um corpo finito de característica 2 e G é um produto semidireto de um 2-grupo abeliano A de índice 2 com um grupo $\langle b \rangle$ tal que b inverte cada elemento de A, i.e, $a^b = a^{-1}$, para todo $a \in A$.

Observamos que sendo A um subgrupo abeliano de índice 2 em G, então $G = A \cup bA$ e disto $b^2 \in A$. Logo, $b^2 = b^{-1}b^2b = b^{-2}$ e disto $b^4 = 1$. Portanto, a ordem de b só pode ser 2 ou 4.

Se ordem de b é 2, inclui-se neste caso os 2-grupos diedrais e se ordem de b é 4, inclui-se

então os quatérnios generalizados.

4.1 2-grupos diedrais

Lema 4.1.1 *Sejam K um corpo de característica 2 e G um 2-grupo contendo um subgrupo abeliano A de índice 2 e um elemento b que inverte cada elemento de A. Então a aplicação $x \mapsto xx^*$ é um epimorfismo do grupo $V(KG)$ no subgrupo $S_K(G)$. Além disso, se $V(KG)$ é finito, então a ordem do subgrupo unitário $V_*(KG)$ coincide com o índice do subgrupo $S_K(G)$ em $V(KG)$.*

Prova: Análoga à prova do Lema 3.1.2. ■

Para o grupo abeliano A, definimos $A[2] = \{a \in A \mid a^2 = 1\}$.

Lema 4.1.2 *Sejam K um corpo finito de característica 2 e G um 2-grupo contendo um subgrupo abeliano A de índice 2 e um elemento b de ordem 2 que inverte cada elemento de A. Então, para todo $x \in V(KG)$, nós temos que*

$$xx^* = 1 + \sum_{a \in L} \alpha_a (a + a^{-1}),$$

onde L é um sistema completo de representantes do subconjunto $\{a^{-1}, a \mid a \in A \backslash A[2]\}$ e $\alpha_a \in K$ para todo $a \in A$.

Prova: Qualquer elemento $x \in V(KG)$ pode ser escrito como $x = x_0 + x_1 b$, onde $x_i \in KA$, $i = 0, 1$, e $\varepsilon(x_0) + \varepsilon(x_1) = 1$. Pelo fato que $a^b = a^{-1}$, para todo $a \in A$, segue imediatamente que $x_i^b = x_i^*$, $i = 0, 1$. Logo, temos que

$$\begin{aligned} xx^* &= (x_0 + x_1 b)(x_0 + x_1 b)^* = (x_0 + x_1 b)(x_0^* + b^{-1} x_1^*) \\ &= (x_0 + x_1 b)(x_0^* + x_1 b) = x_0 x_0^* + x_0 x_1 b + x_1 b x_0^* + x_1 x_1^* \\ &= x_0 x_0^* + x_0 x_1 b + x_0 x_1 b + x_1 x_1^* \\ &= x_0 x_0^* + x_1 x_1^*. \end{aligned}$$

Agora, se $y = \alpha_1 a_1 + \cdots + \alpha_s a_s \in KA$, com $a_i \in A$, e $1 \leq i \leq s$, então

$$\begin{aligned} yy^* &= (\alpha_1 a_1 + \cdots + \alpha_s a_s)(\alpha_1 a_1^{-1} + \cdots + \alpha_s a_s^{-1}) \\ &= (\alpha_1^2 + \cdots + \alpha_s^2) + \sum_{\substack{i,j \\ i<j}} \alpha_i \alpha_j (a_i a_j^{-1} + a_j a_i^{-1}). \end{aligned}$$

Se $a_i a_j^{-1}$ é um elemento de ordem 2, então $a_i a_j^{-1} = a_j a_i^{-1}$ e, portanto, o suporte do elemento yy^* não contém elemento de ordem 2. E disto temos que

$$yy^* = (\varepsilon(y))^2 + \sum_{a \in L} \alpha_a (a + a^{-1}).$$

Como uma conseqüência, temos que para todo $x \in V(KG)$ vale

$$xx^* = 1 + \sum_{a \in L} \alpha_a (a + a^{-1}).$$

■

Teorema 4.1.3 *Sejam K um corpo finito de característica 2 e G um 2-grupo finito contendo um subgrupo abeliano A de índice 2 e um elemento b de ordem 2 que inverte cada*

elemento de A. Então

$$|V_*(KG)| = |K|^{\frac{3|A|+|A[2]|-2}{2}}.$$

Prova: Considerando L um sistema completo de representantes do subconjunto $\{a^{-1}, a | a \in A \backslash A[2]\}$, vemos que o número de elementos de L é $\ell = \frac{|A|-|A[2]|}{2}$. Logo, pelo Lema 4.1.2, a ordem do subgrupo $S_K(G)$ é no máximo $|K|^\ell$. Provaremos que esta é exatamente a ordem de $S_K(G)$. Para isto, basta-nos mostrar que para qualquer z da forma

$$z = 1 + \sum_{a \in L} \alpha_a (a + a^{-1}) \quad (\alpha_a \in K)$$

existe $x \in V(KG)$ tal que $xx^* = z$.

Se $z = 1 + \alpha_1(a_1 + a_1^{-1}) + \alpha_2(a_2 + a_2^{-1}) + \cdots + \alpha_s(a_s + a_s^{-1})$, então colocamos $x_0 = \alpha_1 a_1 + \alpha_2 a_2 + \cdots + \alpha_s a_s$ e $x_1 = 1 + x_0$. Então temos que

$$\varepsilon(x_0) + \varepsilon(x_1) = 1 + 2(\alpha_1 + \alpha_2 + \cdots + \alpha_s) = 1$$

e

$$x = x_0 + x_1 b \in V(KG).$$

Além do mais, vemos que

$$\begin{aligned} xx^* &= x_0 x_0^* + x_1 x_1^* = x_0 x_0^* + (1 + x_0)(1 + x_0^*) \\ &= x_0 x_0^* + 1 + x_0^* + x_0 + x_0 x_0^* \\ &= 1 + x_0 + x_0^*. \end{aligned}$$

Isto é,

$$\begin{aligned} xx^* &= 1 + (\alpha_1 a_1 + \cdots + \alpha_s a_s) + (\alpha_1 a_1 + \cdots + \alpha_s a_s)^* \\ &= 1 + (\alpha_1 a_1 + \cdots + \alpha_s a_s) + (\alpha_1 a_1^{-1} + \cdots + \alpha_s a_s^{-1}) \\ &= 1 + \alpha_1(a_1 + a_1^{-1}) + \cdots + \alpha_s(a_s + a_s^{-1}) = z. \end{aligned}$$

Deste modo, temos que a ordem do subgrupo $S_K(G)$ é igual a $|K|^{\ell}$. Visto que $|V(KG)| = |K|^{|G|-1} = |K|^{2|A|-1}$, pelo Lema 4.1.1, obtemos que

$$\begin{aligned} |V_*(KG)| &= |K|^{2|A|-1}.|K|^{-\frac{|A|-|A[2]|}{2}} \\ &= |K|^{\frac{3|A|+|A[2]|-2}{2}}. \end{aligned}$$

■

Corolário 4.1.4 *Sejam K um corpo finito de característica 2 e*

$$D_{2^{n+1}} = \langle a, b \mid a^{2^n} = b^2 = 1,\ a^b = a^{-1} \rangle$$

um grupo diedral de ordem 2^{n+1}. Então temos que

$$|V_*(KD_{2^{n+1}})| = |K|^{3 \cdot 2^{n-1}}.$$

Prova: Temos que $D_{2^{n+1}} = A \rtimes \langle b \rangle$, onde $A = \langle a | a^{2^n} = 1 \rangle$. Daí, temos que $|A[2]| = 2$ e $|A| = 2^n$. Portanto, segue que

$$|V_*(KD_{2^{n+1}})| = |K|^{\frac{3.2^n+2-2}{2}} = |K|^{3.2^{n-1}}.$$

■

4.2 Quatérnios generalizados

O resultado seguinte trata-se de uma mera generalização do Teorema 1.3.1. Aqui utilizamos o mesmo método lá desenvolvido com pequenas modificações. No que se segue, denotamos $A[2] = \{a \in A \mid a^2 = 1\}$ para A um grupo abeliano.

Teorema 4.2.1 *Sejam K um corpo finito de característica 2 e G um 2-grupo finito contendo um subgrupo abeliano A de índice 2 e um elemento b de ordem 4 que inverte cada elemento de A. Então o subgrupo unitário $V_*(KG)$ é o produto semidireto de G e um subgrupo normal H. O subgrupo H é o produto semidireto do 2-grupo abeliano elementar*

$$R = \{1 + (1 + b^2)zb \mid z \in KA\}$$

e o subgrupo abeliano U, onde $V_*(KA) = A \times U$.

Prova: Seja $G = A \rtimes \langle b \rangle$, onde A é um 2-grupo abeliano de índice 2 e b de ordem 4 com $a^b = a^{-1}$, para todo $a \in A$.

Sendo A um 2-grupo abeliano finito, pelo Teorema 1.3.2, temos que $V_*(KA) = A \times U$ e

$$|V_*(KA)| = |A^2[2]|.|K|^{\frac{1}{2}(|A|+|A[2]|)-1}.$$

Sendo $G = \langle A, b \rangle$, então cada elemento x em KG pode ser escrito como

$$x = x_1 + x_2 b$$

com $x_i \in KA$, $i = 1, 2$.

Em particular, se $x \in V_*(KG)$, então $x = x_1 + x_2 b$, com $x_i \in KA$, $i = 1, 2$, $\varepsilon(x) = \varepsilon(x_1) + \varepsilon(x_2) = 1$ e $xx^* = 1$.

Agora, visto que $G \leq V_*(KG)$, se $x \in V_*(KG)$, então $xb = x_1 b + x_3 \in V_*(KG)$, com $x_3 = x_2 b^2 \in KA$. Portanto, sem perda de generalidades, podemos assumir que $\varepsilon(x_1) = 1$ e $\varepsilon(x_2) = 0$. Logo, $x_1 \in V(KA)$ e disto x pode ser escrito como

$$x = x_1(1 + x_1^{-1} x_2 b).$$

Logo, todo $x \in V_*(KG)$ pode ser tomado como $x = x_1(1 + x_2 b)$ com $x_i \in KA$, $i = 1, 2$, $\varepsilon(x_1) = 1$ e $\varepsilon(x_2) = 0$. Então temos que

$$x^* = (x_1(1 + x_2 b))^* = (1 + x_2 b)^* x_1^* = (1 + b^{-1} x_2^*) x_1^*.$$

Deste modo segue que

$$\begin{aligned}
xx^* &= x_1(1 + x_2 b)(1 + b^{-1} x_2^*) x_1^* \\
&= (x_1 + x_1 x_2 b)(x_1^* + b^{-1} x_2^* x_1^*) \\
&= x_1 x_1^* + x_1 b^{-1} x_2^* x_1^* + x_1 x_2 b x_1^* + x_1 x_2 x_2^* x_1^* \\
&= x_1 x_1^* + x_1 x_1^* x_2 x_2^* + x_1 x_2 b^{-1} x_1^* + x_1 x_2 x_1 b \\
&= x_1 x_1^*(1 + x_2 x_2^*) + x_1 x_2 x_1 b^{-1} + x_1 x_2 x_1 b \\
&= x_1 x_1^*(1 + x_2 x_2^*) + x_1^2 x_2 (b^{-1} + b),
\end{aligned}$$

onde usamos o fato que $a^b = a^{-1}$, para todo $a \in A$, implica que $x_i^b = x_i^*$, $i = 1, 2$.

Assim, temos que $x \in V_*(KG)$ se e somente se

$$\begin{cases} x_1x_1^*(1+x_2x_2^*) = 1, \\ x_1^2x_2(b^{-1}+b) = 0 \end{cases}$$

o que equivale a

$$\begin{cases} x_1x_1^*(1+x_2x_2^*) = 1, \\ x_2(1+b^2) = 0 \end{cases} \tag{1}$$

Mas o anulador de $(1+b^2)$ em KA é exatamente

$$Ann_{KA}(1+b^2) = \{(1+b^2)z \mid z \in KA\},$$

e então x_2 é da forma

$$x_2 = (1+b^2)z \quad (z \in KA) \tag{2}$$

e disto segue que

$$x_2x_2^* = (1+b^2)zz^*(1+b^2) = 0.$$

Assim, de (1) temos que $x_1x_1^* = 1$ e então $x_1 \in V_*(KA)$.

Considere agora o seguinte subgrupo

$$R = \{1+(1+b^2)zb \mid z \in KA\} = \prod_{u \in T} \langle 1+\lambda u(1+b^2)b \mid \lambda \in K\rangle,$$

onde T é um transversal para $\langle b^2\rangle$ em A. Temos assim que para todo $z \in KA$,

$$\begin{aligned}
(1+(1+b^2)zb)(1+(1+b^2)zb)^* &= (1+(1+b^2)zb)(1+b^{-1}z^*(1+b^2)) \\
&= (1+(1+b^2)zb)(1+(1+b^2)b^{-1}z^*) \\
&= (1+(1+b^2)zb)(1+(1+b^2)bz^*) \\
&= (1+(1+b^2)zb)(1+(1+b^2)zb) \\
&= 1+(1+b^2)zb+(1+b^2)zb \\
&= 1,
\end{aligned}$$

pois $(1+b^2)b^{-1} = (1+b^2)b^3 = (1+b^2)b$ e $z^b = z^*$, para todo $z \in KA$.

Assim, R é um 2-grupo abeliano elementar de ordem $|K|^{\frac{1}{2}|A|}$ e $R \subseteq V_*(KG)$. Observamos, por (2), que $1 + x_2 b \in R$. Logo, vemos que $V_*(KG)$ é gerado pelos grupos G, $V_*(KA)$ e R.

Além disso, para todo $z \in KA$, nós temos que

$$b^{-1}(1+(1+b^2)zb)b = 1 + (1+b^2)b^{-1}zb^2 = 1 + (1+b^2)z^*b \in R$$

e para cada $\omega \in V_*(KA)$, temos

$$\begin{aligned} \omega^{-1}(1+(1+b^2)zb)\omega &= 1 + (1+b^2)\omega^{-1}zb\omega \\ &= 1 + (1+b^2)\omega^{-1}\omega^* zb \\ &= 1 + (1+b^2)(\omega^*)^2 zb \in R \end{aligned}$$

porque

$$b\omega = \omega^* b = \omega^{-1} b.$$

Deste modo, R é um subgrupo normal em $V_*(KG)$ e $R \cap U = \langle 1 \rangle$, onde $V_*(KA) = A \times U$.

Considere $H = \langle R, U \rangle$. Como visto acima, temos que $\omega^{-1}R\omega \subseteq R$, para todo $\omega \in V_*(KA)$, e disto segue que H é um produto semidireto do subgrupo normal R e o subgrupo abeliano U, i.e, $H = U \ltimes R$

Portanto, temos que $V_*(KG) = \langle G, H\rangle$. Das identidades acima, vemos que H é um subgrupo normal de $V_*(KG)$ e que

$$V_*(KG) = G \ltimes H = G \ltimes (U \ltimes R).$$

■

Corolário 4.2.2 *Sejam K um corpo finito de característica 2 e G um 2-grupo finito contendo um subgrupo abeliano A de índice 2 e um elemento b de ordem 4 tal que $a^b = a^{-1}$ para todo $a \in A$. Então temos que*

$$|V_*(KG)| = 2.|A^2[2]|\,|K|^{|A|+\frac{1}{2}|A[2]|-1}.$$

Prova: Pelo Teorema 4.2.1, temos que

$$V_*(KG) = G \ltimes (U \ltimes R), \quad \text{com } |R| = |K|^{\frac{1}{2}|A|}.$$

Sabemos também que $V_*(KA) = A \times U$ tem ordem

$$|V_*(KA)| = |A^2[2]|\,|K|^{\frac{1}{2}(|A|+|A[2]|)-1}.$$

Logo, $|U| = |A|^{-1}.|A^2[2]|.|K|^{\frac{1}{2}(|A|+|A[2]|)-1}$.

Portanto, segue que

$$\begin{aligned} |V_*(KG)| &= |G|.|U|.|R| \\ &= 2.|A|.|A|^{-1}.|A^2[2]|\,|K|^{\frac{1}{2}(|A|+|A[2]|)-1}.|K|^{\frac{1}{2}|A|} \\ &= 2.|A^2[2]|.|K|^{|A|+\frac{1}{2}|A[2]|-1}. \end{aligned}$$

■

Corolário 4.2.3 *Sejam K um corpo finito de característica 2 e*

$$Q_{2^{n+1}} = \langle a, b \mid a^{2^n} = 1,\ b^2 = a^{2^{n-1}},\ a^b = a^{-1} \rangle$$

um grupo quatérnio de ordem 2^{n+1}. Então temos que

$$|V_*(KQ_{2^{n+1}})| = 4.|K|^{2^n}.$$

Prova: Temos que $Q_{2^{n+1}} = A \rtimes \langle b \mid b^4 = 1 \rangle$ com $A = \langle a \mid a^{2^n} = 1 \rangle$. Logo, temos que $|A| = 2^n$, $|A[2]| = 2$ e $|A^2[2]| = 2$. Portanto, concluímos pelo Corolário 4.2.2 que

$$|V_*(KQ_{2^{n+1}})| = 4|K|^{2^n}.$$

■

Referências

[1] Bovdi, A.A., The group of units of a group algebra of characteristic p, *Publ. Math. Debrecen* **52** (**1-2**) (1998), 193–244.

[2] Bovdi, A.A., Erdei, L., Unitary units in modular group algebras of groups of order 16, *Technical Report Universitas Debrecen, Dept. of Math., L. Kossuth Univ.* **96/4** (1996), 1–16.

[3] Bovdi, A.A., Gudivok, P.M., Semirot, M.S., Normal group rings. *Ukrain Mat. Zh.*, **37**, 3-8 (1985) (Russian).

[4] Bovdi, A.A., Szakács, A., Unitary subgroup of the group of units of a modular group algebra of a finite abelian p-group, *Mat. Zametki* **45**, n.6 (1989), 23–29.

[5] Bovdi, A.A., Szakács, A., A basis for the unitary subgroup of the group of units in a finite commutative group algebra, *Publ. Math. Debrecen* **46** (**1-2**) (1995), 97–120.

[6] Bovdi, V., Kovács, L.G., Unitary units in modular group algebras,*Manuscripta Math.* **84** (1994), 57–72.

[7] Bovdi, V., Kovács, L.G., Sehgal, S.K., Symmetric units in modular group algebra, *Comm. Algebra* **24**, n.3 (1996), 803–808.

[8] Bovdi, V., Rozgonyi, T., On the unitary subgroup of modular group algebras, *Acta Acad. Paedagogicae Nyíregyháza* **13/** (1992), 13–17.

[9] Bovdi, V. e Rosa, A.L., On the order of the unitary subgroup of a modular group algebra, *Comm. Algebra*, **28** (4) (2000), 1897–1905.

[10] Chuang, C.L., Lee, P.H., Unitary elements in simple artinian rings, *J. Algebra* **176**, 449–459 (1995).

[11] Robinson, D.J.S., A course in the theory of groups, *Springer-Verlag, Berlin-Heidelberg-New York*, 1996.

[12] Suzuki, M., Group theory I, *Springer-Verlag, Berlin-Heidelberg-New York*, 1982.