UNIVERSIDADE FEDERAL DE MINAS GERAIS
INSTITUTO DE CIÊNCIAS EXATAS
Departamento de Matemática

Involuções e elementos Cayley unitários em álgebras de grupos e anéis de matrizes

Viviane Ribeiro Tomaz da Silva

Orientadora: Ana Cristina Vieira

Belo Horizonte - Dezembro de 2004

Resumo

Seja $*$ a involução canônica da álgebra de grupo KG induzida pela aplicação $x \mapsto x^{-1}$ para $x \in G$. No caso em que K é uma extensão real de $\mathbb{Q}$, consideramos elementos Cayley unitários construídos a partir de elementos anti-simétricos $k = \alpha(x - x^{-1})$ em KG tais que $1 + k$ é invertível em KG, para $\alpha \in K$ e $x \in G$. As construções envolvem uma interessante seqüência nos coeficientes de $(1+k)^{-1}$, que é a seqüência de Fibonacci quando $\alpha = 1$. Estudamos também involuções e elementos Cayley unitários no anel $M_n(D)$ de matrizes $n \times n$ sobre um anel de divisão D, baseados no artigo *Unitary elements in simple artinian rings* de C. Chuang e P. Lee.

Abstract

Let $*$ denote the canonical involution of the group algebra KG induced by the map $x \mapsto x^{-1}$ for $x \in G$. In case K is a real extension of $\mathbb{Q}$, we consider Cayley unitary elements built out of skew elements $k = \alpha(x - x^{-1})$ in KG such that $1+k$ is invertible in KG, for $\alpha \in K$ and $x \in G$. The constructions involve an interesting sequence in the coefficients of $(1 + k)^{-1}$ which is the Fibonacci sequence when $\alpha = 1$. We also study involutions and Cayley unitary elements in the ring $M_n(D)$ of $n \times n$ matrices over a division ring D, based on the article *Unitary elements in simple artinian rings* of C. Chuang and P. Lee.

Agradecimentos

À minha orientadora, professora Ana Cristina Vieira, pelos ensinamentos valiosos, acompanhamento contínuo e solícito e por sua admirável dedicação.

Ao professor Michel Spira, pela confiança e incentivo, pelo interesse e atenção para com o trabalho desenvolvido e por todas as sugestões.

Ao professor Adilson Gonçalves, pelas sugestões e considerações feitas ao trabalho.

Aos professores Antônio Giambruno (Universidade de Palermo), Vitor de Oliveira Ferreira (USP) e Jairo Zacarias Gonçalves (USP), pelo cuidado e prontidão com que responderam aos nossos questionamentos.

Aos professores e funcionários do Departamento de Matemática da UFMG, pelo estímulo, formação e convívio.

Aos amigos, pelo carinho, companheirismo e torcida.

Aos meus pais e irmãs, pelo amor diariamente manifestado em pequenos-grandes gestos, pelo apoio e compreensão.

A Deus, meu eterno e grande Amigo, por nos querer cada vez mais plenos, pelo infinito amor, pela doce e terna presença!...

Sumário

Resumo **ii**

Abstract **iii**

Agradecimentos **iv**

Introdução **1**

1 Conceitos e resultados essenciais **4**

1.1 Módulos e álgebras 4

1.2 Involuções em um anel 9

1.3 Elementos unitários e Cayley unitários 14

1.4 Funções geradoras 17

2 Elementos Cayley unitários de álgebras de grupos **21**

2.1 Exemplos de elementos Cayley unitários 21

2.2 Encontrando $(1 + x - x^{-1})^{-1}$ 26

2.3 Encontrando $(1 + \alpha(x - x^{-1}))^{-1}$ 28

2.4 Elementos Cayley unitários de KG obtidos a partir de $\alpha(x - x^{-1})$ . . 33

3 Involuções em anéis de matrizes **39**

3.1 Isomorfismos de anéis com involução 39

3.2 Caracterização de involuções 42
3.3 Produto de elementos Cayley unitários 47

Considerações Finais **56**

Referências Bibliográficas **58**

Introdução

Entendemos por involução um anti-automorfismo de ordem 2 em um anel. Um dos exemplos mais elementares é a aplicação transposta no anel de matrizes sobre um corpo. A "álgebra-multiplicação de uma superfície de Riemann" é um exemplo de uma álgebra sobre $\mathbb{Q}$ admitindo uma involução e foi a motivação para a investigação de anéis com involução iniciado por A. Albert [1] no início dos anos 30.

Em 1998, M. A. Knus, A. Merkurjev, M. Rost e J. P. Tignol publicaram o livro *The book of involutions* [8], que trata de involuções de uma maneira bem geral e apresenta resultados um tanto quanto sofisticados. Anterior a estes autores, em 1976, I. Herstein [6] também dedicou um livro a este assunto intitulado *Rings with involution*, onde tratou os resultados conhecidos até então em uma variedade de direções.

Nesta dissertação, concentrar-nos-emos principalmente em anéis de grupos e anéis de matrizes munidos de involuções específicas e desenvolveremos resultados a respeito de elementos Cayley unitários destes anéis.

Elementos unitários e Cayley unitários têm sido objetos de interesse no estudo de anéis com involução em recentes trabalhos de pesquisa. Em 1995, estes elementos foram particularmente estudados por C. Chuang e P. Lee [2] em anéis de matrizes $M_n(D)$, onde D é um anel de divisão. Eles determinaram condições para que um elemento seja o produto de dois elementos Cayley unitários de $M_n(D)$.

Em 2001, J. Gonçalves e D. Passman [5] mostraram que um par de elementos Cayley unitários em uma álgebra de grupo KG essencialmente gera um subgrupo livre do grupo dos elementos unitários de KG.

Dividiremos este trabalho em três capítulos. O primeiro, intitulado "Conceitos e resultados essenciais", possui quatro seções, sendo que as três primeiras tratam de "Módulos e álgebras", "Involuções em um anel" e "Elementos unitários e Cayley unitários" abordando estes conceitos, exemplos dos mesmos e alguns resultados a eles relacionados que serão importantes no decorrer deste texto. Já a Seção 4,

intitulada "Funções geradoras", explica resumidamente como podemos utilizá-las para tentar encontrar o termo geral de uma seqüência dada por uma relação de recorrência e as utiliza na obtenção de uma fórmula para o termo geral da seqüência (G_i) recursivamente definida por

$$G_0 = 0,\ G_1 = 1 \ \text{ e } \ G_i = \alpha^2 G_{i-2} + G_{i-1},\ \ i \geqslant 2,$$

onde α é um elemento de uma extensão real de $\mathbb{Q}$. Tal fórmula será importante na demonstração do Teorema 2.3.1.

O Capítulo 2 trata sobretudo de elementos Cayley unitários da álgebra de grupo KG sobre um corpo K, a príncipio de característica zero, munida da involução canônica induzida pela aplicação $x \mapsto x^{-1}$, $x \in G$. Este capítulo se inicia com exemplos de elementos Cayley unitários obtidos a partir dos geradores do conjunto dos elementos anti-simétricos de KG para alguns grupos finitos.

A partir da observação dos exemplos construídos, elaboramos hipóteses que são trabalhadas a partir de novos exemplos e de uma observação cada vez mais minunciosa dos mesmos. Todo este processo culmina primeiramente na obtenção do Teorema 2.2.1 que garante a existência do inverso de $1 + x - x^{-1}$ em KG, quando $x \in G$, $o(x) = n > 2$ e K é um corpo com característica zero, e além disso nos fornece uma expressão explícita para tal inverso em função da seqüência de Fibonacci (F_i) definida recursivamente por $F_0 = 0$, $F_1 = 1$ e $F_i = F_{i-2} + F_{i-1}$, para $i \geqslant 2$.

Em seguida, obtemos o Teorema 2.3.1 que consiste em uma generalização do Teorema 2.2.1, garantindo a existência do inverso de $1+\alpha(x-x^{-1})$ em KG, para $\alpha \in K$, e fornecendo uma expressão para este inverso. Neste resultado, exigimos como hipótese que K seja uma extensão real de $\mathbb{Q}$ e vemos que a expressão obtida para o inverso de $1 + \alpha(x - x^{-1})$ depende da seqüência (G_i) definida acima que, por sua vez, constitui uma generalização da seqüência de Fibonacci (F_i). Finalmente, no Teorema 2.4.1, damos uma fórmula explícita para o elemento Cayley unitário de KG obtido a partir de $\alpha(x - x^{-1})$. É feita, então, a caracterização dos elementos Cayley unitários de $\mathbb{Q}G$ para alguns grupos pequenos.

O capítulo termina com duas proposições e um exemplo que buscam responder as seguintes questões:

- ✓ "Que elementos de G são elementos Cayley unitários de KG?"
- ✓ "A partir de que elementos anti-simétricos de KG eles são obtidos?"
- ✓ "Se $x \in G$ e $o(x)$ é par, então x é um produto de elementos Cayley unitários de KG?".

O terceiro capítulo lida com involuções em um anel de matrizes $M_n(D)$, onde D é um anel de divisão. Este capítulo é baseado sobretudo no artigo *Unitary elements in simple artinian rings* de C. Chuang e P. Lee [2]. Os dois teoremas principais de tal artigo (nossos teoremas 3.3.2 e 3.3.8), junto com um corolário (nosso corolário 3.3.6), estabelecem a solução do problema anteriormente mencionado de determinar condições para que um elemento unitário seja um produto de dois elementos Cayley unitários de $M_n(D)$, quando este anel está munido de uma involução e a característica de D é diferente de 2.

Omitimos a demonstração do Teorema 3.3.8, procurando esclarecê-lo através de um exemplo, mas a prova do Teorema 3.3.2 feita por Chuang e Lee é apresentada neste trabalho e utiliza o Teorema 3.2.1. Este, por sua vez, nos permite caracterizar involuções em $M_n(D)$, a menos de isomorfismos de anéis com involução. A definição geral de isomorfismos de anéis com involução e alguns exemplos destes isomorfismos em anéis de matrizes são dados na Seção 1, enquanto a Seção 2 trata da caracterização de involuções em $M_n(D)$.

A dissertação termina com a seção "Considerações finais". Primeiramente é elaborada uma hipótese sobre a existência do inverso de

$$1 + \alpha_1(x - x^{p-1}) + \alpha_3(x^3 - x^{p-3}) + \cdots + \alpha_{p-2}(x^{p-2} - x^2)$$

em KC_p e, consequentemente, a respeito da existência do elemento Cayley unitário construído a partir de

$$k = \alpha_1(x - x^{p-1}) + \alpha_3(x^3 - x^{p-3}) + \cdots + \alpha_{p-2}(x^{p-2} - x^2),$$

quando K é uma extensão real de $\mathbb{Q}$, $C_p = \langle x \rangle$, p é um primo ímpar e $\alpha_1, \alpha_3, \cdots, \alpha_{p-2}$ pertencem a K.

A seguir são feitas considerações sobre hipóteses mais fracas para o corpo K nos Teoremas 2.3.1 e 2.4.1. Por fim, é feito um último comentário que diz respeito à generalidade das involuções e dos isomorfismos de anéis de matrizes com involução considerados na Seção 1 do Capítulo 3.

Capítulo 1

Conceitos e resultados essenciais

1.1 Módulos e álgebras

Nesta seção recordaremos alguns conceitos básicos e fixaremos notações que serão utilizadas no decorrer deste trabalho.

Dado um grupo G, denotaremos por $o(x)$ a ordem de um elemento $x \in G$. Os anéis com os quais trabalharemos serão anéis com unidade. Serão utilizadas as notações $\mathcal{U}(R)$ para o grupo das unidades (elementos invertíveis) de um anel R e $\mathrm{Int}(u)$ para o automorfismo interno induzido pelo elemento $u \in \mathcal{U}(R)$, isto é, $\mathrm{Int}(u)(x) = uxu^{-1}$ para todo $x \in R$. Vale lembrar que se $x \in \mathcal{U}(R)$, então x não é um divisor de zero.

Recordemos ainda que um anel R é denominado um **anel de divisão** se todos os seus elementos não nulos são invertíveis (isto é, se $R\backslash\{0\} = \mathcal{U}(R)$). Denotando por $\mathcal{Z}(R)$ o centro de um anel R, temos que $\mathcal{Z}(D)$ é um corpo se D é um anel de divisão.

Definição 1.1.1 *Seja R um anel. Um grupo abeliano M (aditivo) é chamado um R-**módulo** à esquerda (ou um módulo à esquerda sobre R) se, para cada elemento $x \in R$ e $m \in M$, temos definido um produto $xm \in M$ tal que:*

(i) $(x + y)m = xm + ym$,

(ii) $(x \cdot y)m = x(ym)$,

(iii) $x(m_1 + m_2) = xm_1 + xm_2$,

(iv) $1m = m$,

para todo $x, y \in R$ e $m, m_1, m_2 \in M$.

Analogamente podemos definir um R-módulo à direita. Neste trabalho utilizaremos o termo R-módulo como uma abreviação para R-módulo à esquerda. Notemos que, se K é um corpo, o conceito de K-módulo coincide com a noção de espaço vetorial sobre K. Assim, constituem exemplos de K-módulos com as operações usuais:

- K^n, o conjunto dos vetores colunas com suas n coordenadas em K;
- $M_n(K)$, o conjunto de matrizes $n \times n$ com entradas em K;
- $K[t]$, o conjunto dos polinômios na variável t com coeficientes em K.

Dado um homomorfismo φ de $M_n(K)$, então K^n é um $M_n(K)$-módulo com o produto Av definido por $\varphi(A) \cdot v$, para toda matriz $A \in M_n(K)$ e todo $v \in K^n$, onde $\cdot$ denota a muliplicação de matrizes. Neste caso, diremos que K^n é um $M_n(K)$-**módulo com o produto induzido por** φ. Em particular, se φ é a identidade, então K^n é um $M_n(K)$-módulo com o produto Av coincidindo com a multiplicação de matrizes $A \cdot v$.

Se L é um ideal à esquerda de um anel R, então L é um R-módulo. Em particular, um anel é sempre um módulo sobre si mesmo.

Dado um anel R, um exemplo importante de R-módulo que será utilizado neste trabalho é o chamado **anel de séries formais** $R[[t]]$ dado por

$$R[[t]] = \left\{ \sum_{i=0}^{\infty} a_i t^i \, ; \, a_i \in R \right\}$$

com as operações

$$\sum_{i=0}^{\infty} a_i t^i + \sum_{i=0}^{\infty} b_i t^i = \sum_{i=0}^{\infty} (a_i + b_i) t^i,$$

$$\sum_{i=0}^{\infty} a_i t^i \cdot \sum_{i=0}^{\infty} b_i t^i = \sum_{i=0}^{\infty} c_i t^i,$$

onde $c_i = \sum_{j=0}^{i} a_j b_{i-j}$.

Definição 1.1.2 *Sejam R um anel e M um R-módulo. Um subconjunto não vazio $N \subseteq M$ é chamado um R-**submódulo de** M se as seguintes propriedades são satisfeitas:*

(i) $n_1 + n_2 \in N$

(ii) $xn \in N$,

para todo $n_1, n_2, n \in N$ *e* $x \in R$.

Se V é um espaço vetorial sobre um corpo K, então os K-submódulos de V são precisamente seus subespaços. Em geral, todo módulo não nulo M contém pelos menos dois submódulos, M e $\{0\}$, os quais são chamados **triviais**.

Definição 1.1.3 *Seja R um anel. Um R-módulo M é chamado **simples** se $M \neq \{0\}$ e seus únicos R-submódulos são os triviais.*

Vale ressaltar que K^n não é um K-módulo simples quando $n > 1$, já que todo subespaço de K^n é um K-submódulo. No entanto, K^n é um $M_n(K)$-módulo simples com o produto induzido por um automorfismo φ, conforme veremos no próximo exemplo.

Exemplo 1.1.4

Seja K um corpo e φ um automorfismo de $M_n(K)$. Então K^n é um $M_n(K)$-módulo simples com o produto induzido por φ.

De fato, seja $N \neq \{0\}$ um $M_n(K)$-submódulo de K^n. Então N possui um elemento $v \neq 0$. Sejam v_i uma coordenada não nula de v e $\alpha \in K$. Como φ é um automorfismo de $M_n(K)$, para cada $j \in \{1, \cdots, n\}$, existe uma matriz A_j tal que $\varphi(A_j) = \frac{\alpha}{v_i} E_{ji}$, onde E_{ji} é a matriz com 1 na (j,i)-ésima entrada e 0 nas demais. Assim,

$$A_j v = \varphi(A_j) \cdot v = \frac{\alpha}{v_i} E_{ji} \cdot v = \alpha e_j,$$

onde e_j é o vetor com 1 na j-ésima coordenada e 0 nas demais.

Logo, como N é um $M_n(K)$-submódulo e α foi escolhido arbitrariamente, segue que $\alpha e_j \in N$ para todo $\alpha \in K$ e $j \in \{1, \cdots, n\}$. Portanto, $N = K^n$.

Exemplo 1.1.5

Sejam K um corpo e $i \in \{1, \cdots, n\}$. O ideal (à esquerda) de matrizes colunas

$$L_i = \left\{ \begin{pmatrix} 0 & \cdots & 0 & a_{1i} & 0 & \cdots & 0 \\ \vdots & \ddots & \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & \cdots & 0 & a_{ni} & 0 & \cdots & 0 \end{pmatrix} ; a_{ji} \in K, \forall\, j \in \{1, \cdots, n\} \right\}$$

é um $M_n(K)$-módulo simples com a operação usual.

Definição 1.1.6 *Sejam M e N dois módulos sobre um anel R. Uma aplicação $f : M \to N$ é um **isomorfismo de R-módulos**, se f é um isomorfismo de grupos aditivos e*

$$f(xm) = xf(m),$$

para todo $x \in R$ e $m \in M$. Neste caso, dizemos que M e N são R-módulos isomorfos.

Exemplo 1.1.7

Sejam K um corpo e L_i e L_j dois ideais de matrizes colunas com $i, j \in \{1, \cdots, n\}$. A aplicação $f : L_i \to L_j$ definida por:

$$\begin{pmatrix} 0 & \cdots & 0 & a_{1i} & 0 & \cdots & 0 \\ \vdots & \ddots & \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & \cdots & 0 & a_{ni} & 0 & \cdots & 0 \end{pmatrix} \quad \mapsto \quad \begin{pmatrix} 0 & \cdots & 0 & a_{1i} & 0 & \cdots & 0 \\ \vdots & \ddots & \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & \cdots & 0 & a_{ni} & 0 & \cdots & 0 \end{pmatrix}$$

$\hookrightarrow i$-ésima coluna $\qquad\qquad$ $\hookrightarrow j$-ésima coluna

é claramente um isomorfismo de $M_n(K)$-módulos.

Assim, L_i e L_j são $M_n(K)$-módulos simples e isomorfos para todo $i, j \in \{1, \cdots, n\}$. Em geral temos o seguinte resultado.

Proposição 1.1.8 *Se K é um corpo, então todos os $M_n(K)$-módulos simples são isomorfos.*

Demonstração: Seja N um R-módulo simples, onde $R = M_n(K)$. Segue do visto acima que basta provar que existe $i \in \{1, \cdots, n\}$ tal que N é isomorfo ao ideal de matrizes colunas L_i.

Como $N = 1N \subseteq RN \subseteq N$, temos $RN = N$. Logo, como $R = \sum_{i=1}^{n} L_i$ e $N \neq \{0\}$, existe $i \in \{1, \cdots, n\}$ tal que $L_i N \neq \{0\}$. Portanto, existe $n \in N$ tal que $\widetilde{l_i} n \neq 0$ para algum $\widetilde{l_i} \in L_i$. Consideremos, então, a aplicação

$$\begin{array}{rccc} f & : & L_i & \to & N \\ & & l_i & \mapsto & l_i n. \end{array}$$

Temos que f é um homomorfismo de grupos aditivos com conjunto imagem $f(L_i) \neq \{0\}$ e satisfaz $f(xl_i) = xf(l_i)$, para todo $x \in R$ e $l_i \in L_i$. Como $f(L_i)$ é um R-submódulo de N e N é um R-módulo simples, então $f(L_i) = N$. Por outro lado, como o núcleo $\mathrm{Ker}(f)$ é um R-submódulo de L_i tal que $\mathrm{Ker}(f) \neq L_i$ e L_i é um R-módulo simples, então $\mathrm{Ker}(f) = \{0\}$. Logo, f é um isomorfismo de R-módulos.

□

Definição 1.1.9 *Seja R um anel comutativo. Um R-módulo A é chamado uma R-**álgebra** se existe uma multiplicação definida em A tal que, com a adição dada em A e esta muliplicação, A é um anel e valem as seguintes condições:*

$$x(ab) = (xa)b = a(xb),$$

para todo $x \in R$ e $a, b \in A$.

Se R é um anel comutativo, então $M_n(R)$, $R[t]$ e $R[[t]]$ são exemplos de R-álgebras. Notemos também que se D é um anel de divisão, então $M_n(D)$ é uma $\mathcal{Z}(D)$-álgebra. Apresentaremos a seguir um exemplo de R-álgebra que será importante no desenvolvimento de nosso trabalho.

Sejam R um anel, G um grupo e RG o conjunto de todas as combinações formais $\alpha = \sum_{x \in G} \alpha_x x$, com $\alpha_x \in R$ e apenas um número finito de α_x's diferentes de zero. Definimos que $\sum_{x \in G} \alpha_x x = \sum_{x \in G} \beta_x x$ se, e somente se, $\alpha_x = \beta_x$ para todo $x \in G$. Em RG definimos, respectivamente, as operações soma e produto por:

$$\alpha + \beta = \sum_{x \in G} \alpha_x x + \sum_{x \in G} \beta_x x = \sum_{x \in G} (\alpha_x + \beta_x) x,$$

$$\alpha \cdot \beta = \sum_{x \in G} \alpha_x x \cdot \sum_{y \in G} \beta_y y = \sum_{x,y \in G} (\alpha_x \beta_y)(xy).$$

Reordenando os termos do produto, obtemos

$$\alpha \cdot \beta = \sum_{x \in G} \alpha_x x \cdot \sum_{y \in G} \beta_y y = \sum_{z \in G} \gamma_z z,$$

onde $\gamma_z = \sum_{xy=z} \alpha_x \beta_y$.

Com estas operações é fácil ver que RG é um anel com unidade $1 = \sum_{x \in G} u_x x$, onde o coeficiente de $1 \in G$ é a unidade $1 \in R$ e os coeficientes dos demais u_i's são todos iguais a zero. Temos assim a seguinte definição:

Definição 1.1.10 *Sejam R um anel e G um grupo. O conjunto RG com as operações soma e produto definidas acima é denominado o* ***anel de grupo de*** *G* ***sobre*** *R.*

Em RG podemos definir também o produto de elementos de RG por elementos $\lambda \in R$:

$$\lambda \sum_{x \in G} \alpha_x x = \sum_{x \in G} (\lambda \alpha_x) x.$$

Com esta operação, RG é um R-módulo. Ainda, no caso em que R é comutativo, RG é uma R-álgebra.

Definição 1.1.11 *Sejam R um anel comutativo e G um grupo. O anel de grupo RG com o produto de seus elementos por elementos de R definido como acima é denominado a* ***álgebra de grupo de*** *G* ***sobre*** *R.*

Observemos que, se identificarmos $x \in G$ com $1 \cdot x \in RG$, podemos considerar G contido em RG, e assim os elementos de G formam uma base de RG sobre R.

1.2 Involuções em um anel

Daremos agora a definição de involução em um anel e, em seguida, apresentaremos exemplos de involuções e veremos algumas definições e proposições relacionadas ao conceito de involução que serão utilizadas mais adiante.

Definição 1.2.1 *Seja R um anel. Dizemos que uma aplicação $* : R \to R$ é uma* ***involução em*** *R se, para todo $x, y \in R$, as seguintes propriedades são satisfeitas:*

(i) $(x + y)^* = x^* + y^*$

(ii) $(xy)^* = y^* x^*$

(iii) $(x^*)^* = x$.

Observação 1.2.2

Dada uma involução $*$ em um anel R, utilizaremos a notação exponencial x^* para denotar a imagem de x em R por $*$.

Exemplo 1.2.3 *Aplicação identidade em um anel comutativo*

Seja R um anel comutativo e consideremos a aplicação

$$\begin{array}{rccc} * & : & R & \to & R \\ & & x & \mapsto & x. \end{array}$$

Claramente valem as propriedades (i) e (iii); além disso, como R é comutativo, a propriedade (ii) é satisfeita, já que $(xy)^* = xy = yx = y^* x^*$. Logo, $*$ é uma involução em R.

Exemplo 1.2.4 *Conjugação complexa em $\mathbb{C}$*

Seja $R = \mathbb{C}$ e consideremos a aplicação

$$\begin{array}{rccc} * & : & \mathbb{C} & \to & \mathbb{C} \\ & & \alpha + \beta i & \mapsto & \alpha - \beta i. \end{array}$$

Da definição das operações em $\mathbb{C}$, seguem facilmente as propriedades (i), (ii) e (iii). Portanto, $*$ é uma involução em $\mathbb{C}$ denominada **conjugação complexa**.

Exemplo 1.2.5 *Involuções em* $\mathbb{H}$

Seja $R = \mathbb{H}$, a álgebra dos quatérnios hamiltonianos reais, e consideremos as aplicações

$$\begin{array}{rccc} \widehat{\ } : & \mathbb{H} & \to & \mathbb{H} \\ & \alpha_0 + \alpha_1 i + \alpha_2 j + \alpha_3 k & \mapsto & \alpha_0 - \alpha_1 i - \alpha_2 j - \alpha_3 k \end{array}$$

e

$$\begin{array}{rccc} {}^{-} : & \mathbb{H} & \to & \mathbb{H} \\ & \alpha_0 + \alpha_1 i + \alpha_2 j + \alpha_3 k & \mapsto & \alpha_0 + \alpha_2 i + \alpha_1 j + \alpha_3 k. \end{array}$$

Da definição das operações em $\mathbb{H}$, seguem as propriedades (i), (ii) e (iii). Portanto, $\widehat{\ }$ e ${}^{-}$ são involuções em $\mathbb{H}$, sendo que $\widehat{\ }$ será denominada **involução canônica em** $\mathbb{H}$.

Exemplo 1.2.6 *Involução em um anel de grupo RG*

Sejam R um anel com uma involução ${}^{-}$ e G um grupo. Definimos, para o anel de grupo RG, a seguinte aplicação

$$\begin{array}{rccc} * : & RG & \to & RG \\ & \alpha = \sum_{x\in G} \alpha_x x & \mapsto & \alpha^* = \sum_{x\in G} \overline{\alpha_x} x^{-1} \ . \end{array}$$

Agora

$$\begin{aligned} (\alpha+\beta)^* &= \left(\sum_{x\in G} \alpha_x x + \sum_{x\in G} \beta_x x\right)^* = \left(\sum_{x\in G} (\alpha_x + \beta_x)x\right)^* = \sum_{x\in G} (\overline{\alpha_x + \beta_x})x^{-1} \\ &= \sum_{x\in G} (\overline{\alpha_x} + \overline{\beta_x})x^{-1} = \sum_{x\in G} \overline{\alpha_x} x^{-1} + \sum_{x\in G} \overline{\beta_x} x^{-1} = \left(\sum_{x\in G} \alpha_x x\right)^* + \left(\sum_{x\in G} \beta_x x\right)^* \\ &= \alpha^* + \beta^* \end{aligned}$$

$$\begin{aligned} (\alpha\cdot\beta)^* &= \left(\sum_{x\in G} \alpha_x x \cdot \sum_{y\in G} \beta_y y\right)^* = \left(\sum_{x,y\in G} (\alpha_x\beta_y)(xy)\right)^* = \sum_{x,y\in G} (\overline{\alpha_x\beta_y})(xy)^{-1} \\ &= \sum_{x,y\in G} (\overline{\beta_y}\,\overline{\alpha_x})(y^{-1}x^{-1}) = \sum_{y\in G} \overline{\beta_y} y^{-1} \cdot \sum_{x\in G} \overline{\alpha_x} x^{-1} = \left(\sum_{y\in G} \beta_y y\right)^* \cdot \left(\sum_{x\in G} \alpha_x x\right)^* \\ &= \beta^*\alpha^* \end{aligned}$$

e

$$(\alpha^*)^* = \left(\sum_{x\in G} \overline{\alpha}_x x^{-1}\right)^* = \sum_{x\in G} \overline{\overline{\alpha_x}}(x^{-1})^{-1} = \sum_{x\in G} \alpha_x x = \alpha.$$

Assim, procedendo de modo análogo para o produto de dois elementos quaisquer de RG, verificamos que $*$ é uma involução em RG. Notemos ainda que, para todo anel R comutativo, RG possui uma involução $*$ definida como acima, já que a identidade é uma involução em R.

Exemplo 1.2.7 *Involução canônica na álgebra de grupo KG*

Seja KG uma álgebra de grupo sobre um corpo K. Do que foi visto no exemplo anterior, segue que a aplicação

$$\begin{array}{rccc} * & : & KG & \to & KG \\ & & \alpha = \displaystyle\sum_{x\in G} \alpha_x x & \mapsto & \alpha^* = \displaystyle\sum_{x\in G} \alpha_x x^{-1} \end{array}$$

é uma involução, que será denominada **involução canônica em** KG.

Exemplo 1.2.8 *Involução em $M_n(R)$ obtida a partir de uma em R*

Sejam R um anel e $^-$ uma involução em R. Então a aplicação

$$\begin{array}{rccc} * & : & M_n(R) & \to & M_n(R) \\ & & (a_{ij}) & \mapsto & (\overline{a_{ji}}) \end{array}$$

é uma involução em $M_n(R)$. De fato, como $^-$ uma involução em R, então

$$\begin{aligned} ((a_{ij}) + (b_{ij}))^* &= (a_{ij} + b_{ij})^* = (\overline{a_{ji} + b_{ji}}) = (\overline{a_{ji}} + \overline{b_{ji}}) = (\overline{a_{ji}}) + (\overline{b_{ji}}) \\ &= (a_{ij})^* + (b_{ij})^* \end{aligned}$$

$$\begin{aligned} ((a_{ik}) \cdot (b_{lj}))^* &= \left(\sum_{m=1}^{n} a_{im}b_{mj}\right)^* = \left(\overline{\sum_{m=1}^{n} a_{jm}b_{mi}}\right) = \left(\sum_{m=1}^{n} \overline{b_{mi}}\,\overline{a_{jm}}\right) \\ &= (\overline{b_{ki}}) \cdot (\overline{a_{jl}}) = (b_{ik})^* \cdot (a_{lj})^* \end{aligned}$$

$$((a_{ij})^*)^* = (\overline{a_{ji}})^* = (\overline{\overline{a_{ij}}}) = (a_{ij}).$$

Exemplo 1.2.9 *Transposta de uma matriz em $M_n(R)$*

Seja R um anel comutativo. Considerando a aplicação identidade como sendo a involução $^-$ em R, segue do exemplo anterior que

$$\begin{array}{rccc} * & : & M_n(R) & \to & M_n(R) \\ & & (a_{ij}) & \mapsto & (a_{ji}) \end{array}$$

é uma involução em $M_n(R)$ comumente chamada de **transposta**.

Proposição 1.2.10 *Seja $*$ uma involução em um anel R. Então valem as seguintes propriedades:*

(i) $1^* = 1$

(ii) Se $x \in \mathcal{U}(R)$*, então* $(x^{-1})^* = (x^*)^{-1}$

(iii) $x \in \mathcal{Z}(R)$ *se, e somente se,* $x^* \in \mathcal{Z}(R)$.

Demonstração:
(i) Temos

$$1 = (1^*)^* = (1 \cdot 1^*)^* = (1^*)^* \cdot 1^* = 1 \cdot 1^* = 1^*.$$

(ii) Se $x \in \mathcal{U}(R)$, então aplicando $*$ em $xx^{-1} = 1$ e utilizando que $1^* = 1$, obtemos $(x^{-1})^* x^* = 1^* = 1$. De modo análogo, $x^*(x^{-1})^* = 1$ e, portanto, $(x^{-1})^* = (x^*)^{-1}$.

(iii) Se $x \in \mathcal{Z}(R)$, então para todo $y \in R$ temos que

$$x^* y = x^*(y^*)^* = (y^* x)^* = (xy^*)^* = (y^*)^* x^* = yx^*$$

e portanto $x^* y = yx^*$, o que implica $x^* \in \mathcal{Z}(R)$. Reciprocamente, se $x^* \in \mathcal{Z}(R)$, então do que já foi mostrado temos que $x = (x^*)^* \in \mathcal{Z}(R)$. □

A partir de uma involução $*$ em um anel R, podemos construir novas involuções. Por exemplo, se $u \in \mathcal{U}(R)$ é tal que $u^* = \pm u$, então a composição $\sigma = \mathrm{Int}(u) \circ *$ é uma involução em R. De fato, como $\mathrm{Int}(u)$ é um automorfismo, temos:

$$(a+b)^\sigma = \mathrm{Int}(u)(a+b)^* = \mathrm{Int}(u)(a^* + b^*) = \mathrm{Int}(u)(a^*) + \mathrm{Int}(u)(b^*) = a^\sigma + b^\sigma$$

$$(ab)^\sigma = \mathrm{Int}(u)(ab)^* = \mathrm{Int}(u)(b^* a^*) = (\mathrm{Int}(u)(b^*))(\mathrm{Int}(u)(a^*)) = b^\sigma a^\sigma$$

$$\begin{aligned} (a^\sigma)^\sigma &= \mathrm{Int}(u)(\mathrm{Int}(u)(a^*))^* = u(ua^*u^{-1})^* u^{-1} = u(u^{-1})^*(a^*)^* u^* u^{-1} \\ &= u(u^*)^{-1} a u^* u^{-1} = u(\pm u)^{-1} a (\pm u) u^{-1} = a. \end{aligned}$$

Vejamos dois exemplos de involuções assim construídas que serão fundamentais no Capítulo 3.

Exemplo 1.2.11

Sejam D um anel de divisão, $^-$ uma involução em D e $C = \mathrm{diag}(c_1, \cdots, c_n)$ uma matriz diagonal invertível com $\overline{c_i} = c_i$, para $i = 1, \cdots, n$. Se τ é a involução em $M_n(D)$ dada por $(a_{ij}) \mapsto (\overline{a_{ji}})$ (veja Exemplo 1.2.8), então $C^\tau = C$ e a aplicação

$$\sigma = \mathrm{Int}(C) \circ \tau$$

é uma involução em $M_n(D)$.

Exemplo 1.2.12

Sejam K um corpo, $n = 2m$ e $S = \begin{pmatrix} 0 & I \\ -I & 0 \end{pmatrix} \in M_n(K)$, onde I é a identidade em $M_m(K)$. Então, se τ é a involução transposta em $M_n(K)$, temos que $S^\tau = -S$ e a aplicação

$$\sigma = \mathrm{Int}(S) \circ \tau$$

é uma involução em $M_n(K)$.

Definição 1.2.13 *Seja R um anel com uma involução $*$. Um elemento $k \in R$ é denominado um* ***elemento simétrico de*** *R se $k^* = k$. O conjunto dos elementos simétricos de R é*

$$R^+ = \{k \in R \,|\, k^* = k\}.$$

Definição 1.2.14 *Seja R um anel com uma involução $*$. Um elemento $k \in R$ é denominado um* ***elemento anti-simétrico de*** *R se $k^* = -k$. O conjunto dos elementos anti-simétricos de R é*

$$R^- = \{k \in R \,|\, k^* = -k\}.$$

No caso em que K é um corpo com característica diferente de 2 e $*$ é a involução canônica na álgebra de grupo KG, temos o seguinte resultado para o conjunto dos elementos anti-simétricos.

Proposição 1.2.15 *Sejam K um corpo com característica diferente de 2 e $*$ a involução canônica em KG. Então KG^-, como K-módulo, é gerado por $x - x^{-1}$, $x \in G$.*

Demonstração: Se $\alpha = \sum_{x\in G} \alpha_x x \in KG^-$, então $\sum_{x\in G} \alpha_x x = -\sum_{x\in G} \alpha_x x^{-1}$. Logo $\alpha_x = -\alpha_{x^{-1}}$, para todo $x \in G$. Portanto, $\alpha = \sum_{x\in G} \frac{1}{2}\alpha_x(x - x^{-1})$. □

Proposição 1.2.16 *Seja $k \in R^-$. Então $1 + k$ é invertível em R se, e somente se, $1 - k$ é invertível em R.*

Demonstração: Se $1 + k$ é invertível em R, então existe $x \in R$ tal que $x(1 + k) = 1$. Assim,

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

□

Definição 1.2.17 *Uma involução $*$ em um anel R é denominada uma **involução do primeiro tipo** se todo elemento do centro de R é simétrico. Caso contrário, ela é dita ser do **segundo tipo**.*

A aplicação identidade em qualquer anel comutativo, a involução canônica em $\mathbb{H}$ e a transposta em $M_n(R)$, onde R é um anel comutativo, são exemplos de involuções do primeiro tipo. Já a conjugação complexa em $\mathbb{C}$ e a involução canônica na álgebra de grupo KG, onde G é um grupo abeliano contendo elementos de ordem maior que 2 e K é um corpo, são exemplos de involuções do segundo tipo.

1.3 Elementos unitários e Cayley unitários

Introduziremos nesta seção dois subconjuntos de $\mathcal{U}(R)$, onde R é um anel munido de uma involução, que serão parte essencial no desenvolvimento desta dissertação.

Definição 1.3.1 *Seja R um anel com uma involução $*$. Um elemento $u \in \mathcal{U}(R)$ é denominado um **elemento unitário de** R se $uu^* = 1$. O conjunto dos elementos unitários de R é um subgrupo de $\mathcal{U}(R)$ denotado por $\mathcal{U}n(R)$.*

Proposição 1.3.2 *Se $k \in R^-$ e $1+k \in \mathcal{U}(R)$, então $u = (1-k)(1+k)^{-1} \in \mathcal{U}n(R)$.*

Demonstração: Como $k^* = -k$, segue imediatamente que

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

Logo

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

Portanto, u é um elemento unitário de R. □

Definição 1.3.3 *Um elemento $u \in \mathcal{U}n(R)$ é chamado um **elemento Cayley unitário de** R se existe $k \in R^-$ com $1+k$ invertível em R tal que $u = (1-k)(1+k)^{-1}$. Neste caso, dizemos que u é o elemento Cayley unitário obtido a partir de k, denotado, quando conveniente, por $u_{[k]}$. O conjunto dos elementos Cayley unitários de R será denotado por $\mathcal{U}n^C(R)$.*

Se R é um anel com involução no qual 2 é invertível e $u \in \mathcal{U}n^C(R)$, então a próxima proposição nos diz que existe um único $k \in R^-$ com $1+k$ invertível em R tal que $u = u_{[k]}$.

Proposição 1.3.4 *Sejam R um anel com involução $*$ no qual 2 é invertível e $u \in \mathcal{U}n(R)$. Se $u = u_{[k]} = u_{[h]}$, então $k = h$.*

Demonstração: Suponhamos que $u_{[k]} = u_{[h]}$. Então

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

o que implica

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

Logo, $2(1+k)^{-1} = 2(1+h)^{-1}$ e, como 2 é invertível em R, segue que

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

Assim, $1+k = 1+h$ e, portanto, $k = h$. □

Se $k \in R^-$ é tal que $1+k$ é invertível em R, então da Proposição 1.2.16 segue que $1-k$ também é invertível em R. Além disso,

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

Assim temos a seguinte proposição.

Proposição 1.3.5 *Sejam R um anel com involução e $u_{[k]} \in \mathcal{U}n^C(R)$. Então $(u_{[k]})^{-1} = u_{[-k]}$.*

Nos próximos dois lemas, encontrados em [2], R é um anel com involução $*$ no qual 2 é invertível. Estes lemas nos dão condições necessárias e suficientes para que $u \in \mathcal{U}n(R)$ seja, respectivamente, um elemento Cayley unitário e um produto de dois elementos Cayley unitários de R.

Proposição 1.3.6 ([2], Lema 1) *Seja $u \in \mathcal{U}n(R)$. Então $u \in \mathcal{U}n^C(R)$ se, e somente se, $1+u$ é invertível em R.*

Demonstração:
($\Rightarrow$) Se $u \in \mathcal{U}n^C(R)$, então $u = (1-k)(1+k)^{-1}$ para algum elemento anti-simétrico k tal que $1+k$ é invertível em R. Logo

$$\begin{aligned} 1+u &= 1+(1-k)(1+k)^{-1} \\ &= (1+k)(1+k)^{-1}+(1-k)(1+k)^{-1} \\ &= 2(1+k)^{-1}. \end{aligned}$$

Portanto, como 2 é invertível em R, então $1+u$ é invertível em R.

($\Leftarrow$) Se u é um elemento unitário tal que $1+u$ é invertível em R, então $k = (1-u)(1+u)^{-1}$ é anti-simétrico. De fato, como $*$ é uma involução e $u \in \mathcal{U}n(R)$,

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

Como $(1-u)(1+u) = (1+u)(1-u)$, então $(1+u)^{-1}(1-u) = (1-u)(1+u)^{-1}$. Logo

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

Agora, como 2 é invertível em R, então $1+k = 2(1+u)^{-1}$ é invertível em R. Assim, como $1-k = 2u(1+u)^{-1}$, temos que

$$(1-k)(1+k)^{-1} = 2u(1+u)^{-1}(2(1+u)^{-1})^{-1} = 2u(1+u)^{-1}(1+u)2^{-1} = 2u2^{-1} = u.$$

Logo, $u = (1-k)(1+k)^{-1} = u_{[k]} \in \mathcal{U}n^C(R)$. □

Proposição 1.3.7 ([2], Lema 2) *Se $u \in \mathcal{U}n(R)$, então u é um produto de dois elementos Cayley unitários de R se, e somente se, $(1+u)-(1-u)k$ é invertível em R, para algum elemento $k \in R^-$ com $1+k$ invertível em R.*

Demonstração:
($\Rightarrow$) Suponha que $u \in \mathcal{U}n(R)$ é um produto de dois elementos Cayley unitários de R, isto é, $u = u_{[h]}u_{[k]}$. Então $uu_{[-k]} = u(u_{[k]})^{-1} = u_{[h]}$, ou seja, $uu_{[-k]} \in \mathcal{U}n^C(R)$. Da Proposição 1.3.6 segue que $1+uu_{[-k]}$ é invertível em R. Agora

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

Logo, $(1+u)-(1-u)k = (1+uu_{[-k]})(1-k)$ é invertível em R.

($\Leftarrow$) Se $(1+u)-(1-u)k$ é invertível em R, para algum elemento $k \in R^-$ com $1+k$ invertível em R, então $1+uu_{[-k]} = [(1+u)-(1-u)k](1-k)^{-1}$ é invertível em R. Logo, pela Proposição 1.3.6, $uu_{[-k]} \in \mathcal{U}n^C(R)$, isto é, $uu_{[-k]} = u_{[h]}$, $h \in R$. Assim, $u = u_{[h]}u_{[k]}$ é um produto de dois elementos Cayley unitários. □

1.4 Funções geradoras

Nesta seção explicaremos brevemente como, utilizando funções geradoras, podemos encontrar o termo geral de uma seqüência dada por uma relação de recorrência. A seguir encontraremos o termo geral da seqüência (G_i) que será utilizada no Capítulo 2.

Definição 1.4.1 *A **função geradora** de uma seqüência $A_0, A_1, A_2, \cdots$ é definida como a série formal* $A(t) = \sum_{i \geq 0} A_i t^i$.

Dada uma relação de recorrência que define uma seqüência $A_0, A_1, A_2, \cdots$ cujo termo geral A_i é desconhecido, podemos tentar obter uma fórmula para este termo geral encontrando uma forma fechada para a função geradora $A(t)$ e então obtendo o coeficiente de t^i em $A(t)$. Mais precisamente, conforme mencionado em [11], uma fórmula para A_i pode ser obtida seguindo-se os seguintes passos:

1. Descreva os valores de i para os quais a relação de recorrência é válida.
2. Escreva a função geradora a ser procurada $A(t) = \sum_{i \geq 0} A_i t^i$ em termos da seqüência desconhecida (A_i).
3. Multiplique ambos os lados da relação de recorrência por t^i e some sobre todos os valores de i para os quais a recorrência é válida.
4. Expresse ambos os lados da equação resultante explicitamente em termos de $A(t)$.
5. Resolva a equação resultante para a desconhecida função geradora $A(t)$.
6. Tente obter a fórmula para A_i expandindo $A(t)$ em uma série de potências e tomando então o coeficiente de t^i nesta série.

Exemplo 1.4.2 *Fórmula para o termo geral da seqüência* (G_i)

Sejam K uma extensão real de $\mathbb{Q}$ e $0 \neq \alpha \in K$. Usando funções geradoras, encontraremos uma fórmula para o termo geral da seqüência (G_i) dada por

$$G_0 = 0,\ G_1 = 1 \ \text{ e } \ G_i = \alpha^2 G_{i-2} + G_{i-1},\ i \geq 2. \tag{1.1}$$

Seja $G(t) = \sum_{i=0}^{\infty} G_i t^i$ a função geradora de (G_i). Multiplicando por t^i cada termo da relação de recorrência de (1.1) e somando sobre $i \geq 2$, obtemos

$$\sum_{i \geq 2} G_i t^i = \alpha^2 \sum_{i \geq 2} G_{i-2} t^i + \sum_{i \geq 2} G_{i-1} t^i,$$

o que implica

$$\sum_{i\geq 2} G_i t^i = \alpha^2 t^2 \sum_{i\geq 2} G_{i-2} t^{i-2} + t \sum_{i\geq 2} G_{i-1} t^{i-1},$$

ou seja,

$$\sum_{i\geq 0} G_i t^i - G_1 t - G_0 = \alpha^2 t^2 \sum_{i\geq 0} G_i t^i + t\left(\sum_{i\geq 0} G_i t^i - G_0\right).$$

Logo, desde que $G_0 = 0$ e $G_1 = 1$, da definição de $G(t)$, segue

$$G(t) - t = \alpha^2 t^2 G(t) + tG(t),$$

assim,

$$G(t) = \frac{t}{1 - t - \alpha^2 t^2}.$$

Sejam $r' = \frac{1+\sqrt{1+4\alpha^2}}{2\alpha^2}$ e $r'' = \frac{1-\sqrt{1+4\alpha^2}}{2\alpha^2}$. Como as raízes de $1 - t - \alpha^2 t^2$ são $-r'$ e $-r''$, então $r'r'' = -\frac{1}{\alpha^2}$ e

$$\begin{aligned} 1 - t - \alpha^2 t^2 &= -\alpha^2 (t + r'')(t + r') \\ &= (1 - \alpha^2 r' t)(1 - \alpha^2 r'' t). \end{aligned}$$

Expandindo $\frac{t}{1-t-\alpha^2 t^2}$ em frações parciais, temos

$$\begin{aligned} \frac{t}{1 - t - \alpha^2 t^2} &= \frac{t}{(1 - \alpha^2 r' t)(1 - \alpha^2 r'' t)} \\ &= \frac{1}{\alpha^2 (r' - r'')} \left(\frac{1}{1 - \alpha^2 r' t} - \frac{1}{1 - \alpha^2 r'' t}\right). \end{aligned}$$

Como $\alpha^2 (r' - r'') = \sqrt{1 + 4\alpha^2}$, segue que

$$G(t) = \frac{1}{\sqrt{1 + 4\alpha^2}} \left(\frac{1}{1 - \alpha^2 r' t} - \frac{1}{1 - \alpha^2 r'' t}\right).$$

Agora, no anel de séries formais $K[[t]]$,

$$\frac{1}{1 - \lambda t} = \sum_{i=0}^{\infty} \lambda^i t^i,\ \lambda \in K.$$

Logo

$$G(t) = \frac{1}{\sqrt{1+4\alpha^2}} \left(\sum_{i=0}^{\infty} (\alpha^2 r')^i t^i - \sum_{i=0}^{\infty} (\alpha^2 r'')^i t^i \right) \cdot$$

Como G_i é o coeficiente de t^i em $G(t)$, segue que

$$G_i = \frac{1}{\sqrt{1+4\alpha^2}} \left((\alpha^2 r')^i - (\alpha^2 r'')^i \right) \cdot$$

Portanto, da definição de r' e r'', temos

$$G_i = \frac{(1+\sqrt{1+4\alpha^2})^i - (1-\sqrt{1+4\alpha^2})^i}{2^i(\sqrt{1+4\alpha^2})}, i = 0, 1, \cdots, n, \cdots \tag{1.2}$$

Agora, observemos:

$$(1+\sqrt{1+4\alpha^2})^i - (1-\sqrt{1+4\alpha^2})^i =$$

$$= \sum_m \binom{i}{m} (\sqrt{1+4\alpha^2})^m - \sum_m \binom{i}{m} (-1)^m (\sqrt{1+4\alpha^2})^m$$

$$= \sum_m \binom{i}{m} (1-(-1)^m)(\sqrt{1+4\alpha^2})^m$$

$$= 2 \sum_{m \text{ ímpar}} \binom{i}{m} (\sqrt{1+4\alpha^2})^m$$

$$= 2\sqrt{1+4\alpha^2} \sum_{m \text{ ímpar}} \binom{i}{m} (1+4\alpha^2)^{\frac{m-1}{2}}.$$

Logo, a fórmula geral para G_i é:

$$G_i = \frac{1}{2^{i-1}} \sum_{m \text{ ímpar}} \binom{i}{m} (1+4\alpha^2)^{\frac{m-1}{2}}, \ i \geq 1. \tag{1.3}$$

Capítulo 2

Elementos Cayley unitários de álgebras de grupos

Neste capítulo estudaremos elementos Cayley unitários da álgebra de grupo KG, onde K é um corpo, a princípio de característica zero, G é um grupo e a involução $*$ é a canônica em KG.

2.1 Exemplos de elementos Cayley unitários

O nosso objetivo inicial é estudar alguns grupos finitos tentando obter exemplos de elementos Cayley unitários nas álgebras destes grupos sobre corpos de característica zero. Mais precisamente procuraremos, num primeiro momento, encontrar elementos Cayley unitários obtidos a partir dos geradores de KG^- para alguns grupos finitos. Neste sentido, nossa preocupação se encontra em verificar se um gerador $x - x^{-1} \in KG^-$ é tal que $1 + x - x^{-1}$ é invertível em KG.

Vejamos alguns exemplos:

Exemplo 2.1.1 KS_3

$S_3 = \langle x, y \,|\, x^2 = 1, y^3 = 1, xy = y^{-1}x \rangle$, ${KS_3}^-$ é gerado por $y - y^{-1}$ e $1 + y - y^{-1}$ é invertível, pois $(1 + y - y^{-1})(\frac{1}{2} + \frac{1}{2}y^2) = 1$. Assim, da Proposição 1.3.2, obtemos o elemento Cayley unitário

$$\begin{aligned} u &= (1 - y + y^{-1})\left(\frac{1}{2} + \frac{1}{2}y^2\right) \\ &= y^2. \end{aligned}$$

Exemplo 2.1.2 KD_4

$D_4 = \langle x, y \,|\, x^2 = 1, y^4 = 1, xy = y^{-1}x \rangle$, $y - y^{-1} \in KD_4{}^-$ e $1 + y - y^{-1}$ é invertível, pois $(1 + y - y^{-1})(\frac{3}{5} - \frac{1}{5}y + \frac{2}{5}y^2 + \frac{1}{5}y^3) = 1$. Assim, da Proposição 1.3.2, obtemos

$$u = \frac{1}{5} - \frac{2}{5}y + \frac{4}{5}y^2 + \frac{2}{5}y^3$$

um elemento Cayley unitário de KD_4.

Exemplo 2.1.3 KQ_8

$Q_8 = \langle x, y \,|\, x^4 = 1, x^2 = y^2, xy = y^{-1}x \rangle$ e $1 + x - x^{-1}$ e $1 + y - y^{-1}$ são invertíveis, pois $(1 + x - x^{-1})(\frac{3}{5} - \frac{1}{5}x + \frac{2}{5}x^2 + \frac{1}{5}x^3) = 1$ e $(1 + y - y^{-1})(\frac{3}{5} - \frac{1}{5}y + \frac{2}{5}y^2 + \frac{1}{5}y^3) = 1$. Assim

$$u_1 = \frac{1}{5} - \frac{2}{5}x + \frac{4}{5}x^2 + \frac{2}{5}x^3$$

e

$$u_2 = \frac{1}{5} - \frac{2}{5}y + \frac{4}{5}y^2 + \frac{2}{5}y^3$$

são elementos Cayley unitários de KQ_8.

Observemos que, embora D_4 e Q_8 sejam grupos distintos, se x é um elemento de ordem 4 em um destes grupos, então $1 + x - x^{-1}$ é invertível, sendo seu inverso dado por $\frac{3}{5} - \frac{1}{5}x + \frac{2}{5}x^2 + \frac{1}{5}x^3$ e o elemento Cayley unitário obtido a partir de $x - x^{-1}$ dado por $\frac{1}{5} - \frac{2}{5}x + \frac{4}{5}x^2 + \frac{2}{5}x^3$. Assim, se $x \in G$ e $o(x) = n$, pelo que temos observado, $(1 + x - x^{-1})^{-1}$ e $u_{[x-x^{-1}]}$, caso existam, parecem não depender de G, mas apenas da ordem de x. Portanto, trabalharemos a partir de agora com os grupos cíclicos $C_n = \langle x \rangle$, $o(x) = n > 2$.

Trabalhando com $3 \leq n \leq 7$, encontramos:

n	$(1+x-x^{-1})^{-1}$
3	$\frac{1}{2}+\frac{1}{2}x^2$
4	$\frac{3}{5}-\frac{1}{5}x+\frac{2}{5}x^2+\frac{1}{5}x^3$
5	$\frac{5}{11}-\frac{2}{11}x+\frac{3}{11}x^2+\frac{1}{11}x^3+\frac{4}{11}x^4$
6	$\frac{1}{2}-\frac{1}{4}x+\frac{1}{4}x^2+\frac{1}{4}x^4+\frac{1}{4}x^5$
7	$\frac{13}{29}-\frac{7}{29}x+\frac{6}{29}x^2-\frac{1}{29}x^3+\frac{5}{29}x^4+\frac{4}{29}x^5+\frac{9}{29}x^6$

n	$u=(1-x+x^{-1})(1+x-x^{-1})^{-1}$
3	x^2
4	$\frac{1}{5}-\frac{2}{5}x+\frac{4}{5}x^2+\frac{2}{5}x^3$
5	$-\frac{1}{11}-\frac{4}{11}x+\frac{6}{11}x^2+\frac{2}{11}x^3+\frac{8}{11}x^4$
6	$-\frac{1}{2}x+\frac{1}{2}x^2+\frac{1}{2}x^4+\frac{1}{2}x^5$
7	$-\frac{3}{29}-\frac{14}{29}x+\frac{12}{29}x^2-\frac{2}{29}x^3+\frac{10}{29}x^4+\frac{8}{29}x^5+\frac{18}{29}x^6$

Os resultados acima sugerem que se $C_n = \langle x \rangle$, então $1 + x - x^{-1}$ é invertível em KC_n, quando K é um corpo de característica zero. Na tentativa de mostrar que isto de fato ocorre e de encontrar alguma regularidade que nos ajude a obter uma fórmula geral para $(1 + x - x^{-1})^{-1}$, podemos resolver de uma forma padrão, para $3 \leq n \leq 7$, os sistemas lineares

$$\begin{cases} a_0 - a_{n-1} + a_1 &= 1 \\ a_1 - a_0 + a_2 &= 0 \\ a_2 - a_1 + a_3 &= 0 \\ \vdots & \vdots \ \vdots \\ a_{n-1} - a_{n-2} + a_0 &= 0 \end{cases}$$

que fornecem o inverso de $1 + x - x^{-1}$, onde $o(x) = n$. Como exemplo, vejamos a obtenção de $(1 + x - x^{-1})^{-1}$ no caso em que $n = 7$.

Exemplo 2.1.4 *Obtenção de* $(1 + x - x^{-1})^{-1}$ *no caso em que* $o(x) = 7$.

Sejam $C_7 = \langle x \rangle$ e K um corpo com característica zero. Queremos encontrar a_0, a_1, a_2, a_3, a_4, a_5, $a_6 \in K$ tais que

$$(1 + x - x^{-1})(a_0 + a_1x + a_2x^2 + a_3x^3 + a_4x^4 + a_5x^5 + a_6x^6) = 1.$$

Isto é equivalente a encontrar uma solução do sistema linear

$$\begin{cases} a_0 + a_6 - a_1 &= 1 \\ a_1 + a_0 - a_2 &= 0 \\ a_2 + a_1 - a_3 &= 0 \\ a_3 + a_2 - a_4 &= 0 \\ a_4 + a_3 - a_5 &= 0 \\ a_5 + a_4 - a_6 &= 0 \\ a_6 + a_5 - a_0 &= 0. \end{cases}$$

Resolveremos o sistema acima seguindo os seguintes passos:

1^o **passo:** Isolaremos a_6 na 7^a equação e o substituiremos na 6^a equação; isolaremos, então, a_5 na 6^a equação e o substituiremos na 5^a equação e assim sucessivamente.

Logo

$$\begin{cases} a_6 = a_0 - a_5 \\ a_5 = \frac{a_0 - a_4}{2} \\ a_4 = \frac{a_0 - 2a_3}{3} \\ a_3 = \frac{a_0 - 3a_2}{5} \\ a_2 = \frac{a_0 - 5a_1}{8} \\ a_1 = \frac{a_0 - 8a_0}{13} \\ a_0 = \frac{13 - 13a_6}{20}. \end{cases}$$

2^o **passo:** Escreveremos todos os a_i's em função de a_6, substituindo a_0 em a_1, e, então, a_0 e a_1 em a_2, e assim sucessivamente. Obtendo

$$\begin{cases} a_0 = \frac{13}{20}(1 - a_6) \\ a_1 = \frac{-7}{20}(1 - a_6) \\ a_2 = \frac{6}{20}(1 - a_6) \\ a_3 = \frac{-1}{20}(1 - a_6) \\ a_4 = \frac{5}{20}(1 - a_6) \\ a_5 = \frac{4}{20}(1 - a_6) \\ a_6 = \frac{9}{20}(1 - a_6). \end{cases}$$

3^o **passo:** Encontraremos o valor de a_6 e então, por substituição, os dos demais a_i's. Assim,

$$a_6 = \frac{9}{29},\ a_5 = \frac{4}{29},\ a_4 = \frac{5}{29},\ a_3 = \frac{-1}{29},\ a_2 = \frac{6}{29},\ a_1 = \frac{-7}{29} \text{ e } a_0 = \frac{13}{29}.$$

Portanto,

$$(1 + x - x^{-1})^{-1} = \frac{13}{29} - \frac{7}{29}x + \frac{6}{29}x^2 - \frac{1}{29}x^3 + \frac{5}{29}x^4 + \frac{4}{29}x^5 + \frac{9}{29}x^6.$$

Observando cuidadosamente os a_i's obtidos nos dois primeiros passos da resolução de nosso sistema linear, podemos encontrar uma fórmula para $(1+x-x^{-1})^{-1}$, onde $o(x) = n > 2$. É o que faremos na próxima seção.

2.2 Encontrando $(1 + x - x^{-1})^{-1}$

Sejam $x \in G$ tal que $o(x) = n > 2$ e K um corpo de característica zero. No Exemplo 2.1.4, obtivemos o inverso de $1 + x - x^{-1}$, para $n = 7$, resolvendo em 'três passos' um sistema linear nas variáveis $a_0, \cdots, a_6$. Observando os a_i's obtidos no 1^o passo da resolução de nosso sistema linear, vemos que os denominadores de a_6, a_5, a_4, a_3, a_2 e a_1 são os seis primeiros termos da seqüência de Fibonacci $1, 2, 3, 5, 8, 13, ...$ Já os numeradores dos a_i's obtidos no 2^o passo são os sete primeiros termos da seqüência de Fibonacci $13, -7, 6, -1, 5, 4, 9, ...$

Uma pergunta natural e importante é a seguinte: "É possível escrever os a_i's obtidos nestes dois passos em função de uma mesma seqüência de Fibonacci?". A resposta é afirmativa e tal seqüência pode ser encontrada a partir da observação de que os a_i's obtidos no 2^o passo podem ser reescritos da seguinte forma:

$$\begin{cases} a_0 = \frac{0+13}{21-1}(1 - a_6) \\ a_1 = \frac{1-8}{21-1}(1 - a_6) \\ a_2 = \frac{1+5}{21-1}(1 - a_6) \\ a_3 = \frac{2-3}{21-1}(1 - a_6) \\ a_4 = \frac{3+2}{21-1}(1 - a_6) \\ a_5 = \frac{5-1}{21-1}(1 - a_6) \\ a_6 = \frac{8+1}{21-1}(1 - a_6)\cdot \end{cases}$$

Assim, vamos considerar (F_i) a seqüência de Fibonacci

$$0, 1, 1, 2, 3, 5, 8, 13, 21, \cdots$$

dada pela relação de recorrência

$$F_0 = 0,\ F_1 = 1 \ \text{ e } \ F_i = F_{i-1} + F_{i-2},\ i \geqslant 2. \tag{2.1}$$

Reescrevendo os a_i's em função dos F_i's temos

$$\begin{cases} a_0 = \frac{F_0+F_7}{F_8-1}(1-a_6) \\ a_1 = \frac{F_1-F_6}{F_8-1}(1-a_6) \\ a_2 = \frac{F_2+F_5}{F_8-1}(1-a_6) \\ a_3 = \frac{F_3-F_4}{F_8-1}(1-a_6) \\ a_4 = \frac{F_4+F_3}{F_8-1}(1-a_6) \\ a_5 = \frac{F_5-F_2}{F_8-1}(1-a_6) \\ a_6 = \frac{F_6+F_1}{F_8-1}(1-a_6). \end{cases}$$

Logo, podemos escrever para $n = 7$:

$$a_i = \frac{F_i + (-1)^i F_{n-i}}{F_{n+1} - 1}(1 - a_{n-1}),\ i = 0, 1, \cdots, n-1,$$

e então encontrando a expressão para a_{n-1} e, por substituição, a dos demais a_i's, obtemos

$$a_i = \frac{F_i + (-1)^i F_{n-i}}{F_{n+1} + F_{n-1} - (1 + (-1)^n)},\ i = 0, 1, \cdots, n-1.$$

Formulamos então o seguinte.

Teorema 2.2.1 *Consideremos (F_i) a seqüência de Fibonacci definida em (2.1). Se $x \in G$ é tal que $o(x) = n > 2$ e K é um corpo com característica zero, então $1 + x - x^{-1}$ é invertível em KG e seu inverso é dado por $a_0 + a_1 x + \cdots + a_{n-1}x^{n-1}$, onde*

$$a_i = \frac{F_i + (-1)^i F_{n-i}}{F_{n+1} + F_{n-1} - (1 + (-1)^n)},\ i = 0, 1, \cdots, n-1.$$

Vamos nos preparar para, na próxima seção, demonstrarmos este teorema em uma situação mais geral, considerando elementos $1+\alpha(x-x^{-1}) \in KG$, onde $\alpha \in K$ e $x \in G$ com $o(x) = n > 2$. Para este fim vamos considerar, a partir de agora, K uma extensão real de $\mathbb{Q}$.

2.3 Encontrando $(1+\alpha(x-x^{-1}))^{-1}$

Sejam $C_n = \langle x \rangle$ tal que $n > 2$ e α um elemento não nulo de K. Queremos encontrar $(1+\alpha(x-x^{-1}))^{-1}$ em KC_n para posteriormente obtermos o elemento Cayley unitário proveniente do elemento anti-simétrico $\alpha(x-x^{-1})$. A fim de encontrarmos uma fórmula geral para tal inverso, estudaremos inicialmente o caso particular em que $o(x) = 7$.

Sejam $C_7 = \langle x \rangle$ e α um elemento não nulo de K. Queremos encontrar a_0, a_1, a_2, a_3, a_4, a_5, $a_6 \in K$ tais que

$$(1+\alpha(x-x^{-1}))(a_0+a_1x+a_2x^2+a_3x^3+a_4x^4+a_5x^5+a_6x^6) = 1.$$

Isto é equivalente a encontrarmos uma solução do sistema linear

$$\begin{cases} a_0+\alpha a_6-\alpha a_1 &= 1 \\ a_1+\alpha a_0-\alpha a_2 &= 0 \\ a_2+\alpha a_1-\alpha a_3 &= 0 \\ a_3+\alpha a_2-\alpha a_4 &= 0 \\ a_4+\alpha a_3-\alpha a_5 &= 0 \\ a_5+\alpha a_4-\alpha a_6 &= 0 \\ a_6+\alpha a_5-\alpha a_0 &= 0. \end{cases}$$

Resolvendo o sistema acima seguindo os passos descritos no Exemplo 2.1.4, obtemos

1^o **passo:**

$$\begin{cases} a_6 = \alpha(a_0-a_5) \\ a_5 = \frac{\alpha(\alpha a_0-a_4)}{1+\alpha^2} \\ a_4 = \frac{\alpha(\alpha^2 a_0-(1+\alpha^2)a_3)}{1+2\alpha^2} \\ a_3 = \frac{\alpha(\alpha^3 a_0-(1+2\alpha^2)a_2)}{1+3\alpha^2+\alpha^4} \\ a_2 = \frac{\alpha(\alpha^4 a_0-(1+3\alpha^2+\alpha^4)a_1)}{1+4\alpha^2+3\alpha^4} \\ a_1 = \frac{\alpha(\alpha^5 a_0-(1+4\alpha^2+3\alpha^4)a_0)}{1+5\alpha^2+6\alpha^4+\alpha^6} \\ a_0 = \frac{(1+5\alpha^2+6\alpha^4+\alpha^6)(1-\alpha a_6)}{1+6\alpha^2+10\alpha^4+4\alpha^6-\alpha^7}. \end{cases}$$

Notemos que nos denominadores dos a_i's, $1 \leq i \leq 6$, aparece uma interessante seqüência $1, 1+\alpha^2, 1+2\alpha^2, 1+3\alpha^2+\alpha^4, 1+4\alpha^2+3\alpha^4, 1+5\alpha^2+6\alpha^4+\alpha^6$ muito parecida com a seqüência de Fibonacci, já que satisfaz a relação de recorrência $G_i = \alpha^2 G_{i-2} + G_{i-1}$.

2^o **passo:**

$$\begin{cases} a_0 = \frac{1+5\alpha^2+6\alpha^4+\alpha^6}{1+6\alpha^2+10\alpha^4+4\alpha^6-\alpha^7}(1-\alpha a_6) \\ a_1 = \frac{\alpha(\alpha^5-(1+4\alpha^2+3\alpha^4))}{1+6\alpha^2+10\alpha^4+4\alpha^6-\alpha^7}(1-\alpha a_6) \\ a_2 = \frac{\alpha^2(\alpha^3+1+3\alpha^2+\alpha^4)}{1+6\alpha^2+10\alpha^4+4\alpha^6-\alpha^7}(1-\alpha a_6) \\ a_3 = \frac{\alpha^3(\alpha+\alpha^3-(1+2\alpha^2))}{1+6\alpha^2+10\alpha^4+4\alpha^6-\alpha^7}(1-\alpha a_6) \\ a_4 = \frac{\alpha^3(\alpha+\alpha^3+1+2\alpha^2)}{1+6\alpha^2+10\alpha^4+4\alpha^6-\alpha^7}(1-\alpha a_6) \\ a_5 = \frac{\alpha^2(1+3\alpha^2+\alpha^4-\alpha^3)}{1+6\alpha^2+10\alpha^4+4\alpha^6-\alpha^7}(1-\alpha a_6) \\ a_6 = \frac{\alpha(1+4\alpha^2+3\alpha^4+\alpha^5)}{1+6\alpha^2+10\alpha^4+4\alpha^6-\alpha^7}(1-\alpha a_6). \end{cases}$$

Observemos que os a_i's podem ser reescritos da seguinte forma:

$$\begin{cases} a_0 = \frac{\alpha^7.0+\alpha^0(1+5\alpha^2+6\alpha^4+\alpha^6)}{1+6\alpha^2+10\alpha^4+4\alpha^6-\alpha^7}(1-\alpha a_6) \\ a_1 = \frac{\alpha^6.1-\alpha^1(1+4\alpha^2+3\alpha^4)}{1+6\alpha^2+10\alpha^4+4\alpha^6-\alpha^7}(1-\alpha a_6) \\ a_2 = \frac{\alpha^5.1+\alpha^2(1+3\alpha^2+\alpha^4)}{1+6\alpha^2+10\alpha^4+4\alpha^6-\alpha^7}(1-\alpha a_6) \\ a_3 = \frac{\alpha^4(1+\alpha^2)-\alpha^3(1+2\alpha^2)}{1+6\alpha^2+10\alpha^4+4\alpha^6-\alpha^7}(1-\alpha a_6) \\ a_4 = \frac{\alpha^3(1+2\alpha^2)+\alpha^4(1+\alpha^2)}{1+6\alpha^2+10\alpha^4+4\alpha^6-\alpha^7}(1-\alpha a_6) \\ a_5 = \frac{\alpha^2(1+3\alpha^2+\alpha^3)-\alpha^5.1}{1+6\alpha^2+10\alpha^4+4\alpha^6-\alpha^7}(1-\alpha a_6) \\ a_6 = \frac{\alpha(1+4\alpha^2+3\alpha^4)+\alpha^6.1}{1+6\alpha^2+10\alpha^4+4\alpha^6-\alpha^7}(1-\alpha a_6). \end{cases}$$

Assim, seja (G_i) a seqüência

$$0, 1, 1, 1+\alpha^2, 1+2\alpha^2, 1+3\alpha^2+\alpha^4, 1+4\alpha^2+3\alpha^4, 1+5\alpha^2+6\alpha^4+\alpha^6, \cdots$$

(G_i) é dada pela relação de recorrência

$$G_0 = 0,\ G_1 = 1 \ \text{ e } \ G_i = \alpha^2 G_{i-2} + G_{i-1},\ \ i \geqslant 2,$$

ou seja, (G_i) é a seqüência de Fibonacci (F_i) quando $\alpha = 1$.

Reescrevendo os a_i's em função dos G_i's temos

$$\begin{cases} a_0 = \frac{\alpha^7 G_0 + (-\alpha)^0 G_7}{G_8 - \alpha^7}(1 - \alpha a_6) \\ a_1 = \frac{\alpha^6 G_1 + (-\alpha)^1 G_6}{G_8 - \alpha^7}(1 - \alpha a_6) \\ a_2 = \frac{\alpha^5 G_2 + (-\alpha)^2 G_5}{G_8 - \alpha^7}(1 - \alpha a_6) \\ a_3 = \frac{\alpha^4 G_3 + (-\alpha)^3 G_4}{G_8 - \alpha^7}(1 - \alpha a_6) \\ a_4 = \frac{\alpha^3 G_4 + (-\alpha)^4 G_3}{G_8 - \alpha^7}(1 - \alpha a_6) \\ a_5 = \frac{\alpha^2 G_5 + (-\alpha)^5 G_2}{G_8 - \alpha^7}(1 - \alpha a_6) \\ a_6 = \frac{\alpha^1 G_6 + (-\alpha)^6 G_1}{G_8 - \alpha^7}(1 - \alpha a_6). \end{cases}$$

Logo, para $n = 7$,

$$a_i = \frac{\alpha^{n-i} G_i + (-\alpha)^i G_{n-i}}{G_{n+1} - \alpha^n}(1 - \alpha a_{n-1}), i = 0, 1, \cdots, n-1,$$

e assim

$$a_i = \frac{\alpha^{n-i} G_i + (-\alpha)^i G_{n-i}}{G_{n+1} + \alpha^2 G_{n-1} - \alpha^n (1 + (-1)^n)},\ i = 0, 1, \cdots, n-1.$$

Em geral, vale a seguinte generalização do Teorema 2.2.1:

Teorema 2.3.1 *Sejam $x \in G$ tal que $o(x) = n > 2$ e $\alpha \in K$, onde K é uma extensão real de $\mathbb{Q}$. Então, o elemento $1 + \alpha(x - x^{-1})$ é invertível em KG e seu inverso é dado por $a_0 + a_1x + \cdots + a_{n-1}x^{n-1}$, onde*

$$a_i = \frac{\alpha^{n-i}G_i + (-\alpha)^i G_{n-i}}{G_{n+1} + \alpha^2 G_{n-1} - \alpha^n(1 + (-1)^n)}, \tag{2.2}$$

para $0 \leq i \leq n-1$, e G_j é dado pela relação (1.1), para $0 \leq j \leq n$.

Demonstração: Para que $a_0 + a_1x + \cdots + a_{n-1}x^{n-1}$ definido no enunciado de nosso teorema seja um elemento de KG, basta que $G_{n+1} + \alpha^2 G_{n-1} - \alpha^n(1 + (-1)^n)$ seja diferente de zero. Para garantir este fato, vamos utilizar a fórmula geral para a seqüencia (G_i) encontrada no Exemplo 1.4.2, analisando o que ocorre nos dois casos possíveis: n ímpar e n par.

Se n é ímpar, então

$$G_{n+1} + \alpha^2 G_{n-1} - \alpha^n(1 + (-1)^n) = G_{n+1} + \alpha^2 G_{n-1}$$

e, como $\alpha^2 \geq 0$, segue de (1.3) que

$$G_{n+1} + \alpha^2 G_{n-1} > 0.$$

Se n é par, então

$$G_{n+1} + \alpha^2 G_{n-1} - \alpha^n(1 + (-1)^n) = G_{n+1} + \alpha^2 G_{n-1} - 2\alpha^n.$$

Segue de (1.3) que

$$G_{n+1} = \frac{1}{2^n} \sum_{m \text{ ímpar}} \binom{n+1}{m} (1 + 4\alpha^2)^{\frac{m-1}{2}}$$

e

$$G_{n-1} = \frac{1}{2^{n-2}} \sum_{m \text{ ímpar}} \binom{n-1}{m} (1 + 4\alpha^2)^{\frac{m-1}{2}}.$$

Agora, como $n+1$ e $n-1$ são ímpares e K é uma extensão real de $\mathbb{Q}$, então

$$G_{n+1} > \frac{1}{2^n}\binom{n+1}{n+1}(1 + 4\alpha^2)^{\frac{(n+1)-1}{2}} > \frac{1}{2^n}(4\alpha^2)^{\frac{n}{2}} = \frac{(2\alpha)^n}{2^n} = \alpha^n$$

e

$$G_{n-1} \geq \frac{1}{2^{n-2}}\binom{n-1}{n-1}(1 + 4\alpha^2)^{\frac{(n-1)-1}{2}} \geq \frac{1}{2^{n-2}}(4\alpha^2)^{\frac{n-2}{2}} = \frac{(2\alpha)^{n-2}}{2^{n-2}} = \alpha^{n-2}.$$

Logo,

$$G_{n+1} + \alpha^2 G_{n-1} - 2\alpha^n > \alpha^n + \alpha^2\alpha^{n-2} - 2\alpha^n.$$

Portanto,

$$G_{n+1} + \alpha^2 G_{n-1} - 2\alpha^n > 0.$$

Agora, consideremos os a_i's dados em (2.2). Vamos mostrar que $a_0 + \cdots + a_{n-1}x^{n-1}$ é o inverso de $1 + \alpha(x - x^{-1})$ quando $x \in G$ é um elemento de ordem $n > 2$.

$(1 + \alpha(x - x^{-1}))(a_0 + a_1x + a_2x^2 + \cdots + a_{n-1}x^{n-1}) =$

$= (a_0 + \alpha a_{n-1} - \alpha a_1) + \cdots + (a_i + \alpha a_{i-1} - \alpha a_{i+1})x^i + \cdots + (a_{n-1} + \alpha a_{n-2} - \alpha a_0)x^{n-1}.$

Assim, basta mostrar que $a_0 + \alpha a_{n-1} - \alpha a_1 = 1$, $a_{n-1} + \alpha a_{n-2} - \alpha a_0 = 0$ e, para todo $i \in \{1, \cdots, n-2\}$, $a_i + \alpha a_{i-1} - \alpha a_{i+1} = 0$. Da definição dos a_i's e da relação (1.1), temos

$a_0 + \alpha a_{n-1} - \alpha a_1 =$

$$= \frac{\alpha^n G_0 + (-\alpha)^0 G_n + \alpha(\alpha^1 G_{n-1} + (-\alpha)^{n-1} G_1) - \alpha(\alpha^{n-1} G_1 + (-\alpha)^1 G_{n-1})}{G_{n+1} + \alpha^2 G_{n-1} - \alpha^n(1 + (-1)^n)}$$

$$= \frac{(G_n + \alpha^2 G_{n-1}) + \alpha^2 G_{n-1} - \alpha^n(1 + (-1)^n)}{G_{n+1} + \alpha^2 G_{n-1} - \alpha^n(1 + (-1)^n)}$$

$$= \frac{G_{n+1} + \alpha^2 G_{n-1} - \alpha^n(1 + (-1)^n)}{G_{n+1} + \alpha^2 G_{n-1} - \alpha^n(1 + (-1)^n)} = 1$$

$a_i + \alpha a_{i-1} - \alpha a_{i+1} =$

$$= \frac{\alpha^{n-i}(G_i + \alpha^2 G_{i-1} - G_{i+1}) + (-\alpha)^i(G_{n-i} - G_{n-i+1} + \alpha^2 G_{n-i-1})}{G_{n+1} + \alpha^2 G_{n-1} - \alpha^n(1 + (-1)^n)}$$

$$= \frac{\alpha^{n-i}.0 + (-\alpha)^i.0}{G_{n+1} + \alpha^2 G_{n-1} - \alpha^n(1 + (-1)^n)} = 0$$

$a_{n-1} + \alpha a_{n-2} - \alpha a_0 =$

$$= \frac{\alpha G_{n-1} + (-\alpha)^{n-1} G_1 + \alpha(\alpha^2 G_{n-2} + (-\alpha)^{n-2} G_2) - \alpha(\alpha^n G_0 + (-\alpha)^0 G_n)}{G_{n+1} + \alpha^2 G_{n-1} - \alpha^n(1 + (-1)^n)}$$

$$= \frac{\alpha(G_{n-1} + \alpha^2 G_{n-2} - G_n)}{G_{n+1} + \alpha^2 G_{n-1} - \alpha^n(1 + (-1)^n)} = 0$$

e o teorema está demonstrado. □

2.4 Elementos Cayley unitários de KG obtidos a partir de $\alpha(x - x^{-1})$

Sejam $x \in G$ tal que $o(x) = n > 2$ e $\alpha \in K$, onde K é uma extensão real de $\mathbb{Q}$. O elemento Cayley unitário obtido a partir de $\alpha(x - x^{-1})$ é dado por

$$(1 - \alpha(x - x^{-1}))(1 + \alpha(x - x^{-1}))^{-1}.$$

Agora, $(1 + \alpha(x - x^{-1}))^{-1} = a_0 + a_1 x + \cdots + a_{n-1} x^{n-1}$, onde os a_i's são dados por (2.2). Logo

$(1 - \alpha(x - x^{-1}))(1 + \alpha(x - x^{-1}))^{-1} =$

$= (1 - \alpha x + \alpha x^{-1})(a_0 + a_1 x + a_2 x^2 + \cdots + a_{n-1} x^{n-1})$

$= (a_0 - \alpha a_{n-1} + \alpha a_1) + \cdots + (a_i - \alpha a_{i-1} + \alpha a_{i+1}) x^i + \cdots + (a_{n-1} - \alpha a_{n-2} + \alpha a_0) x^{n-1}.$

Substituindo os a_i's por suas respectivas expressões e utilizando a relação (1.1), obtemos o seguinte resultado.

Teorema 2.4.1 *Sejam $x \in G$ tal que $o(x) = n > 2$ e $\alpha \in K$, onde K é uma extensão real de $\mathbb{Q}$. O elemento Cayley unitário de KG obtido a partir de $\alpha(x - x^{-1})$ é dado por $b_0 + b_1 x + \cdots + b_{n-1} x^{n-1}$, onde*

$$b_0 = \frac{G_n - 2\alpha^2 G_{n-1} + \alpha^n(1 + (-1)^n)}{G_{n+1} + \alpha^2 G_{n-1} - \alpha^n(1 + (-1)^n)},$$

$$b_i = 2a_i, i = 1, \cdots, n-1,$$

e os a_i's são dados por (2.2).

Exemplo 2.4.2 *Caracterização dos elementos Cayley unitários de* $\mathbb{Q}C_3$

Seja $C_3 = \langle x \rangle$, então $\mathbb{Q}C_3{}^- = \{\alpha(x - x^{-1}); \alpha \in \mathbb{Q}\}$ e, conseqüentemente, todo elemento Cayley unitário de $\mathbb{Q}C_3$ é obtido a partir de $\alpha(x - x^{-1})$, para algum $\alpha \in \mathbb{Q}$. Agora, do Teorema 2.4.1 segue que, se $\alpha \in \mathbb{Q}$, então $u_{[\alpha(x-x^{-1})]}$ é dado por $b_0 + b_1 x + b_2 x^2$, onde

$$\begin{aligned} b_0 &= \frac{G_3 - 2\alpha^2 G_2 + \alpha^3(1 + (-1)^3)}{G_4 + \alpha^2 G_2 + \alpha^3(1 + (-1)^3)} \\ &= \frac{(1 + \alpha^2) - 2\alpha^2}{(1 + 2\alpha^2) + \alpha^2} \\ &= \frac{1 - \alpha^2}{1 + 3\alpha^2} \end{aligned}$$

$$\begin{aligned} b_1 &= 2\frac{\alpha^2 G_1 + (-\alpha)^1 G_2}{G_4 + \alpha^2 G_2 + \alpha^3(1 + (-1)^3)} \\ &= 2\frac{\alpha^2 - \alpha}{(1 + 2\alpha^2) + \alpha^2} \\ &= \frac{2\alpha(\alpha - 1)}{1 + 3\alpha^2} \end{aligned}$$

$$\begin{aligned} b_2 &= 2\frac{\alpha^1 G_2 + (-\alpha)^2 G_1}{G_4 + \alpha^2 G_2 \alpha^3(1 + (-1)^3)} \\ &= 2\frac{\alpha^2 + \alpha}{(1 + 2\alpha^2) + \alpha^2} \\ &= \frac{2\alpha(\alpha + 1)}{1 + 3\alpha^2}. \end{aligned}$$

Assim, todo elemento Cayley unitário de $\mathbb{Q}C_3$ é da forma

$$\frac{1}{1 + 3\alpha^2}\left(1 - \alpha^2 + 2\alpha(\alpha - 1)x + 2\alpha(\alpha + 1)x^2\right),$$

para algum $\alpha \in \mathbb{Q}$, e então

$$\mathcal{U}n^C(\mathbb{Q}C_3) = \left\{\frac{1}{1 + 3\alpha^2}\left(1 - \alpha^2 + 2\alpha(\alpha - 1)x + 2\alpha(\alpha + 1)x^2\right); \alpha \in \mathbb{Q}\right\} \subseteq \mathcal{U}n(\mathbb{Q}C_3).$$

Notemos que $\mathcal{U}n^C(\mathbb{Q}C_3)$ não é subgrupo de $\mathcal{U}n(\mathbb{Q}C_3)$, já que o produto de dois elementos Cayley unitários não é necessariamente um elemento Cayley unitário. De fato, sejam $k_1 = -(x - x^{-1})$ e $k_2 = -\frac{1}{3}(x - x^{-1})$, então

$$u_{[k_1]} = x \text{ e } u_{[k_2]} = \frac{2}{3} + \frac{2}{3}x - \frac{1}{3}x^2,$$

o que implica

$$u_{[k_1]}u_{[k_2]} = -\frac{1}{3} + \frac{2}{3}x + \frac{2}{3}x^2.$$

Agora

$$1 + u_{[k_1]}u_{[k_2]} = \frac{2}{3}(1 + x + x^2)$$

e $\frac{2}{3}(1 + x + x^2)$ é divisor de zero, pois

$$\frac{2}{3}(1 + x + x^2)(1 - x) = \frac{2}{3}(1 - x^3) = 0,$$

já que $x^3 = 1$. Logo, $1 + u_{[k_1]}u_{[k_2]}$ não é invertível e da Proposição 1.3.6 concluímos que $u_{[k_1]}u_{[k_2]}$ não é um elemento Cayley unitário.

Notemos também que x e x^2 são elementos Cayley unitários de $\mathbb{Q}C_3$ já que $u_{[-(x-x^{-1})]} = x$ e $u_{[x-x^{-1}]} = x^2$.

Exemplo 2.4.3 *Caracterização dos elementos Cayley unitários de* $\mathbb{Q}S_3$

Seja $S_3 = \langle x, y \,|\, x^2 = 1, y^3 = 1, xy = y^{-1}x\rangle$, então $\mathbb{Q}S_3{}^- = \{\alpha(y - y^{-1}); \alpha \in \mathbb{Q}\} = \mathbb{Q}C_3{}^-$, onde $C_3 = \langle y\rangle$. Logo

$$\begin{aligned}\mathcal{U}n^C(\mathbb{Q}S_3) &= \mathcal{U}n^C(\mathbb{Q}C_3)\\ &= \left\{\frac{1}{1+3\alpha^2}\left(1 - \alpha^2 + 2\alpha(\alpha-1)y + 2\alpha(\alpha+1)y^2\right); \alpha \in \mathbb{Q}\right\}.\end{aligned}$$

Exemplo 2.4.4 *Caracterização dos elementos Cayley unitários de* $\mathbb{Q}C_4$

Seja $C_4 = \langle x\rangle$, então $\mathbb{Q}C_4{}^- = \{\alpha(x - x^{-1}); \alpha \in \mathbb{Q}\}$ e, conseqüentemente, todo elemento Cayley unitário de $\mathbb{Q}C_4$ é obtido a partir de $\alpha(x - x^{-1})$, para algum $\alpha \in \mathbb{Q}$. De modo análogo ao que foi feito para $\mathbb{Q}C_3$, temos que, se $\alpha \in \mathbb{Q}$, então $u_{[\alpha(x-x^{-1})]} = b_0 + b_1x + b_2x^2 + b_3x^3$, onde

$$b_0 = \frac{1}{1+4\alpha^2},\ b_1 = -\frac{2\alpha}{1+4\alpha^2},\ b_2 = \frac{4\alpha^2}{1+4\alpha^2} \text{ e } b_3 = \frac{2\alpha}{1+4\alpha^2}.$$

Logo

$$\mathcal{U}n^C(\mathbb{Q}C_4) = \left\{ \frac{1}{1+4\alpha^2}\left(1 - 2\alpha x + 4\alpha^2 x^2 + 2\alpha x^3\right); \alpha \in \mathbb{Q} \right\} \subseteq \mathcal{U}n(\mathbb{Q}C_4).$$

Notemos que x, x^2 e x^3 não são elementos Cayley unitários de $\mathbb{Q}C_4$, já que todo elemento Cayley unitário de $\mathbb{Q}C_4$ possui termo independente não nulo.

Exemplo 2.4.5 *Caracterização dos elementos Cayley unitários de* $\mathbb{Q}D_4$

Seja $D_4 = \langle x, y \,|\, x^2 = 1, y^4 = 1, xy = y^{-1}x \rangle$, então $\mathbb{Q}D_4{}^- = \{\alpha(y - y^{-1}); \alpha \in \mathbb{Q}\}$ $= \mathbb{Q}C_4{}^-$, onde $C_4 = \langle y \rangle$. Logo

$$\begin{aligned} \mathcal{U}n^C(\mathbb{Q}D_4) &= \mathcal{U}n^C(\mathbb{Q}C_4) \\ &= \left\{ \frac{1}{1+4\alpha^2}\left(1 - 2\alpha y + 4\alpha^2 y^2 + 2\alpha y^3\right); \alpha \in \mathbb{Q} \right\}. \end{aligned}$$

Exemplo 2.4.6 *Caracterização dos elementos Cayley unitários de* $\mathbb{Q}C_5$

Sejam $C_5 = \langle x \rangle$ e $\alpha, \beta \in \mathbb{Q}$. Então $1 + \alpha(x - x^4) + \beta(x^3 - x^2)$ é invertível em $\mathbb{Q}C_5$ e seu inverso é dado por $a_0 + a_1x + a_2x^2 + a_3x^3 + a_4x^4$, onde

$$a_0 = \frac{\alpha^4 + 2\beta\alpha^3 - \beta^2\alpha^2 + 3\alpha^2 - 2\alpha\beta^3 + 1 + \beta^4 + 3\beta^2}{5\alpha^4 + 10\beta\alpha^3 - 5\beta^2\alpha^2 + 5\alpha^2 - 10\alpha\beta^3 + 1 + 5\beta^2 + 5\beta^4}$$

$$a_1 = \frac{\alpha^4 - 2\alpha^3 + 2\beta\alpha^3 - \beta^2\alpha^2 - 3\beta\alpha^2 + \alpha\beta^2 - \alpha - 2\alpha\beta^3 + 2\alpha\beta + \beta^2 + \beta^4 + \beta^3}{5\alpha^4 + 10\beta\alpha^3 - 5\beta^2\alpha^2 + 5\alpha^2 - 10\alpha\beta^3 + 1 + 5\beta^2 + 5\beta^4}$$

$$a_2 = \frac{\alpha^4 + 2\beta\alpha^3 + \alpha^3 + \alpha^2 - \beta\alpha^2 - \beta^2\alpha^2 - 2\alpha\beta - 3\alpha\beta^2 - 2\alpha\beta^3 + \beta + \beta^4 + 2\beta^3}{5\alpha^4 + 10\beta\alpha^3 - 5\beta^2\alpha^2 + 5\alpha^2 - 10\alpha\beta^3 + 1 + 5\beta^2 + 5\beta^4}$$

$$a_3 = \frac{\alpha^4 - \alpha^3 + 2\beta\alpha^3 + \beta\alpha^2 - \beta^2\alpha^2 + \alpha^2 - 2\alpha\beta + 3\alpha\beta^2 - 2\alpha\beta^3 - \beta + \beta^4 - 2\beta^3}{5\alpha^4 + 10\beta\alpha^3 - 5\beta^2\alpha^2 + 5\alpha^2 - 10\alpha\beta^3 + 1 + 5\beta^2 + 5\beta^4}$$

$$a_4 = \frac{\alpha^4 + 2\alpha^3 + 2\beta\alpha^3 - \beta^2\alpha^2 + 3\beta\alpha^2 - 2\alpha\beta^3 + \alpha + 2\alpha\beta - \alpha\beta^2 - \beta^3 + \beta^2 + \beta^4}{5\alpha^4 + 10\beta\alpha^3 - 5\beta^2\alpha^2 + 5\alpha^2 - 10\alpha\beta^3 + 1 + 5\beta^2 + 5\beta^4}.$$

Além disso, o elemento Cayley unitário obtido a partir de $\alpha(x - x^4) + \beta(x^3 - x^2)$ é dado por $b_0 + b_1x + b_2x^2 + b_3x^3 + b_4x^4$, onde

$$b_0 = \frac{1-3\beta^4+6\alpha\beta^3-6\beta\alpha^3+3\alpha^2\beta^2+\alpha^2-3\alpha^4+\beta^2}{5\alpha^4+10\beta\alpha^3-5\beta^2\alpha^2+5\alpha^2-10\alpha\beta^3+1+5\beta^2+5\beta^4}$$

$$b_1 = \frac{2(\alpha^4+2\beta\alpha^3-2\alpha^3-3\beta\alpha^2-\alpha^2\beta^2+\alpha\beta^2-\alpha-2\alpha\beta^3+2\alpha\beta+\beta^4+\beta^2+\beta^3)}{5\alpha^4+10\beta\alpha^3-5\beta^2\alpha^2+5\alpha^2-10\alpha\beta^3+1+5\beta^2+5\beta^4}$$

$$b_2 = \frac{2(\alpha^4+\alpha^3+2\beta\alpha^3+\alpha^2-\beta\alpha^2-\alpha^2\beta^2-2\alpha\beta-2\alpha\beta^3-3\alpha\beta^2+2\beta^3+\beta^4+\beta)}{5\alpha^4+10\beta\alpha^3-5\beta^2\alpha^2+5\alpha^2-10\alpha\beta^3+1+5\beta^2+5\beta^4}$$

$$b_3 = \frac{2(\alpha^4-\alpha^3+2\beta\alpha^3+\alpha^2-\alpha^2\beta^2+\beta\alpha^2-2\alpha\beta-2\alpha\beta^3+3\alpha\beta^2-2\beta^3+\beta^4-\beta)}{5\alpha^4+10\beta\alpha^3-5\beta^2\alpha^2+5\alpha^2-10\alpha\beta^3+1+5\beta^2+5\beta^4}$$

$$b_4 = \frac{2(\alpha^4+2\beta\alpha^3+2\alpha^3+3\beta\alpha^2-\alpha^2\beta^2-\alpha\beta^2+\alpha-2\alpha\beta^3+2\alpha\beta+\beta^4+\beta^2-\beta^3)}{5\alpha^4+10\beta\alpha^3-5\beta^2\alpha^2+5\alpha^2-10\alpha\beta^3+1+5\beta^2+5\beta^4}.$$

Notemos que os denominadores dos a_i's são iguais a $5(\alpha^2+\alpha\beta-\beta^2)^2+5(\alpha^2+\beta^2)+1$ e, portanto, são sempre maiores que zero, o que nos garante que $a_i, b_i \in \mathbb{Q}$ para todo i. Quando α e β percorrem todo o conjunto $\mathbb{Q}$ obtemos $\mathcal{U}n^C(\mathbb{Q}C_5)$. Além disso,

$$C_5 \subseteq \mathcal{U}n^C(\mathbb{Q}C_5),$$

já que $u_{[0]} = 1$, $u_{[-(x-x^4)-(x^3-x^2)]} = x$, $u_{[-(x-x^4)+(x^3-x^2)]} = x^2$, $u_{[(x-x^4)-(x^3-x^2)]} = x^3$ e $u_{[(x-x^4)+(x^3-x^2)]} = x^4$.

Segue do que foi visto nos exemplos acima que, se x é um elemento de um grupo G e $o(x) = 3$ ou $o(x) = 5$, então $x \in \mathcal{U}n^C(\mathbb{Q}G)$, enquanto que se $o(x) = 4$, então $x \notin \mathcal{U}n^C(\mathbb{Q}G)$. Em geral, vale o seguinte resultado.

Proposição 2.4.7 *Sejam $x \in G$ tal que $o(x) = n$ e K um corpo de característica diferente de 2. Então x é um elemento Cayley unitário de KG se, e somente se, n é ímpar.*

Demonstração: Como $x \in G$, então x é um elemento unitário de KG. Logo, segue da Proposição 1.3.6, que x é um elemento Cayley unitário se, e somente se, $1+x$ é invertível em KG. Agora,

$$(1+x)\frac{1}{2}(1-x+x^2-x^3+\cdots+(-1)^{n-1}x^{n-1}) = \frac{1}{2}(1+(-1)^{n-1}x^n).$$

Como $o(x) = n$, temos

$$(1+x)\frac{1}{2}(1-x+x^2-x^3+\cdots+(-1)^{n-1}x^{n-1}) = \frac{1}{2}(1+(-1)^{n-1}). \tag{2.3}$$

Assim, se n é ímpar, então $1+x$ é invertível em KG, o que implica x é um elemento Cayley unitário. Se n é par, então $1+x$ é divisor de zero e, portanto, não é invertível em KG, o que faz com que x não seja um elemento Cayley unitário. □

Concluímos que se G é um grupo com ordem ímpar e K é um corpo de característica diferente de 2, então todo elemento de G é um elemento Cayley unitário de KG. Mais do que isto, se $x \in G$ tem ordem ímpar $n > 1$, então o elemento antisimétrico k tal que $x = u_{[k]}$ é conhecido. É o que veremos na próxima proposição.

Proposição 2.4.8 *Sejam $x \in G$ um elemento não trivial de ordem ímpar n e K um corpo de característica diferente de 2. Então $x = u_{[k]}$, onde*

$$k = -(x - x^{n-1}) - (x^3 - x^{n-3}) - \cdots - (x^{n-2} - x^2).$$

Demonstração: Como x tem ordem ímpar $n > 1$, então $x = u_{[k]}$ e $1+x = 2(1+k)^{-1}$. Agora, de (2.3) temos que $1+x = 2[1-(x-x^{n-1})-(x^3-x^{n-3})-\cdots-(x^{n-2}-x^2)]^{-1}$. Logo, da unicidade de k, segue que $k = -(x-x^{n-1})-(x^3-x^{n-3})-\cdots-(x^{n-2}-x^2)$. □

Se a ordem de G é par, então $G \not\subseteq \mathcal{U}n^C(KG)$, já que G possui elementos de ordem 2, que por sua vez não são elementos Cayley unitários. Uma pergunta que poderíamos fazer é: "Se $x \in G$ e $o(x)$ é par, então x é um produto de elementos Cayley unitários de KG?". Vamos responder esta questão através do seguinte exemplo.

Exemplo 2.4.9

Se $D_4 = \langle x, y \,|\, x^2 = 1, y^4 = 1, xy = y^{-1}x \rangle$, então

$$\mathcal{U}n^C(\mathbb{Q}D_4) \;=\; \left\{ \frac{1}{1+4\alpha^2} \left(1 - 2\alpha y + 4\alpha^2 y^2 + 2\alpha y^3\right) ; \alpha \in \mathbb{Q} \right\}.$$

Assim, x e y^2 são dois elementos de D_4 de ordem par, mas x não é um produto de elementos Cayley unitários de $\mathbb{Q}D_4$, enquanto y^2 o é (note que $y^2 = (u_{[k]})^2$, onde $k = \frac{1}{2}(y - y^3)$).

Capítulo 3

Involuções em anéis de matrizes

Sejam D um anel de divisão e $^-$ uma involução em D. Neste capítulo, denotaremos por τ a involução no anel de matrizes $M_n(D)$, vista no Exemplo 1.2.8, dada por

$$\begin{array}{rccc} \tau & : & M_n(D) & \to & M_n(D) \\ & & (a_{ij}) & \mapsto & (\overline{a_{ji}}). \end{array}$$

Conforme veremos, τ será usado no Teorema 3.2.1, o qual nos permite caracterizar involuções em $M_n(D)$ e será utilizado na demonstração do Teorema 3.3.2. Este, por sua vez, trata de elementos unitários que são produtos de dois elementos Cayley unitários de $M_n(D)$, quando este anel está munido de uma involução $*$ que induz uma involução diferente da identidade em D e a característica de D é diferente de 2.

3.1 Isomorfismos de anéis com involução

Definição 3.1.1 *Sejam σ_1 e σ_2 involuções nos anéis R_1 e R_2, respectivamente. Um* ***isomorfismo de anéis com involução*** *$(R_1, \sigma_1) \to (R_2, \sigma_2)$ é um isomorfismo de anéis $\psi : R_1 \to R_2$ tal que $\psi(x^{\sigma_1}) = (\psi(x))^{\sigma_2}$ para todo $x \in R_1$. Neste caso, denotamos $(R_1, \sigma_1) \cong (R_2, \sigma_2)$.*

Considerando uma involução $^-$ no anel de divisão D e U e V matrizes invertíveis em $M_n(D)$ tais que $U^\tau = \pm U$ e $V^\tau = \pm V$, vimos na Seção 2 do Capítulo 1 que as aplicações $* = \mathrm{Int}(U) \circ \tau$ e $\sigma = \mathrm{Int}(V) \circ \tau$ são involuções em $M_n(D)$.

Agora, se P é um elemento invertível de $M_n(D)$ temos que $\psi : M_n(D) \to M_n(D)$, dado por $\psi(A) = PAP^{-1}$, é um isomorfismo de anéis. Assim, munindo $M_n(D)$ com as involuções $*$ e σ, podemos nos perguntar quando

$$\begin{array}{rccc} \psi & : & (M_n(D), *) & \to & (M_n(D), \sigma) \\ & & A & \mapsto & PAP^{-1} \end{array}$$

é um isomorfismo de anéis com involução. Temos,

$$\psi(A^*) = \psi(\mathrm{Int}(U)(A^\tau)) = \psi(UA^\tau U^{-1}) = P(UA^\tau U^{-1})P^{-1} = (PU)A^\tau(PU)^{-1}$$

e

$$(\psi(A))^\sigma = \mathrm{Int}(V)(\psi(A))^\tau = V(PAP^{-1})^\tau V^{-1} = (V(P^{-1})^\tau)A^\tau(P^\tau V^{-1}),$$

para toda matriz $A \in M_n(D)$. Logo, se $PU = V(P^{-1})^\tau$, nossa aplicação ψ é um isomorfismo de anéis com involução.

Vejamos agora alguns exemplos.

Exemplo 3.1.2

Seja $^-$ a involução em $\mathbb{H}$, vista no Exemplo 1.2.5, dada por

$$\overline{a_0 + a_1 i + a_2 j + a_3 k} = a_0 + a_2 i + a_1 j + a_3 k$$

e consideremos

$$U = \begin{pmatrix} 0 & j \\ i & 0 \end{pmatrix} \in \mathcal{U}(M_2(\mathbb{H})) \quad \text{e} \quad * = \mathrm{Int}(U) \circ \tau.$$

Então $U^\tau = U$ e $*$ é uma involução em $M_2(\mathbb{H})$.

Se $P = \frac{1}{2}\begin{pmatrix} 1 & -2i \\ -k & -2j \end{pmatrix} \in \mathcal{U}(M_2(\mathbb{H}))$, então a aplicação

$$\begin{array}{rccc} \psi & : & (M_2(\mathbb{H}), *) & \to & (M_2(\mathbb{H}), \tau) \\ & & A & \mapsto & PAP^{-1} \end{array}$$

é um isomorfismo de anéis com involução, já que neste caso $\sigma = \mathrm{Int}(V) \circ \tau$, onde V é a identidade,

$$P^{-1} = \frac{1}{2}\begin{pmatrix} 2 & 2k \\ i & j \end{pmatrix} \quad \text{e} \quad PU = \frac{1}{2}\begin{pmatrix} 2 & j \\ 2k & i \end{pmatrix} = (P^{-1})^\tau = V(P^{-1})^\tau.$$

Exemplo 3.1.3

Sejam $^-$ a conjugação complexa em $\mathbb{C}$, $* = \mathrm{Int}(U) \circ \tau$ e $\sigma = \mathrm{Int}(C) \circ \tau$, onde

$$U = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix} \text{ e } C = \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix}.$$

Então $*$ e σ são involuções em $M_2(\mathbb{C})$, pois $U^\tau = U$ e $C^\tau = C$.

Se $P = \frac{\sqrt{2}}{2} \begin{pmatrix} 1 & i \\ i & 1 \end{pmatrix} \in \mathcal{U}(M_2(\mathbb{C}))$, então a aplicação

$$\begin{array}{rccc} \psi & : & (M_2(\mathbb{C}), *) & \to & (M_2(\mathbb{C}), \sigma) \\ & & A & \mapsto & PAP^{-1} \end{array}$$

é um isomorfismo de anéis com involução, já que

$$PU = \frac{\sqrt{2}}{2} \begin{pmatrix} -1 & -i \\ i & 1 \end{pmatrix} = C(P^{-1})^\tau.$$

Exemplo 3.1.4

Sejam $^-$ a identidade em $\mathbb{C}$, $* = \mathrm{Int}(U) \circ \tau$ e $\sigma = \mathrm{Int}(S) \circ \tau$, onde

$$U = \begin{pmatrix} 0 & 0 & 1 & 0 \\ 0 & 0 & -1 & 1 \\ -1 & 1 & 0 & -2 \\ 0 & -1 & 2 & 0 \end{pmatrix} \text{ e } S = \begin{pmatrix} 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ -1 & 0 & 0 & 0 \\ 0 & -1 & 0 & 0 \end{pmatrix}.$$

Então $*$ e σ são involuções em $M_4(\mathbb{C})$, já que $U^\tau = -U$ e $S^\tau = -S$.

Se $P = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 \\ 1 & 1 & 1 & 0 \\ 0 & 1 & 0 & 1 \end{pmatrix} \in \mathcal{U}(M_4(\mathbb{C}))$, então

$$PU = \begin{pmatrix} 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ -1 & 1 & 0 & -1 \\ 0 & -1 & 1 & 1 \end{pmatrix} = S(P^{-1})^\tau.$$

E, portanto, a aplicação

$$\begin{array}{rccc} \psi & : & (M_4(\mathbb{C}), *) & \to & (M_4(\mathbb{C}), \sigma) \\ & & A & \mapsto & PAP^{-1} \end{array}$$

é um isomorfismo de anéis com involução.

Proposição 3.1.5 *Seja $\psi : (R_1, \sigma_1) \to (R_2, \sigma_2)$ um isomorfismo de anéis com involução. Então valem as seguintes propriedades:*

(i) $k \in {R_1}^-$ se, e somente se, $\psi(k) \in {R_2}^-$.

(ii) $u \in \mathcal{U}n(R_1)$ se, e somente se, $\psi(u) \in \mathcal{U}n(R_2)$.

(iii) $u \in \mathcal{U}n^C(R_1)$ se, e somente se, $\psi(u) \in \mathcal{U}n^C(R_2)$.

Demonstração: Para cada item provaremos apenas uma das implicações, a outra se obtém aplicando a inversa de ψ.

(i) Seja $k \in {R_1}^-$. Temos $k^{\sigma_1} = -k$ e, portanto, $\psi(k^{\sigma_1}) = \psi(-k)$. Assim, como ψ é uma isomorfismo de anéis com involução, segue que

$$(\psi(k))^{\sigma_2} = \psi(k^{\sigma_1}) = -\psi(k),$$

ou seja, $\psi(k) \in {R_2}^-$.

(ii) Se $u \in \mathcal{U}n(R_1)$, então $uu^{\sigma_1} = 1$ e assim

$$\psi(u)(\psi(u))^{\sigma_2} = \psi(u)\psi(u^{\sigma_1}) = \psi(uu^{\sigma_1}) = \psi(1) = 1.$$

Logo, $\psi(u) \in \mathcal{U}n(R_2)$.

(iii) Se $u \in \mathcal{U}n^C(R_1)$, então $u = u_{[k]}$ com $k \in {R_1}^-$. Logo $\psi(k) \in {R_2}^-$ e

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

Portanto, $\psi(u) \in \mathcal{U}n^C(R_2)$. □

3.2 Caracterização de involuções

Iniciaremos esta seção com alguns exemplos de involuções em anéis de matrizes que nos permitirão entender melhor o comportamento de involuções em anéis $M_n(D)$, onde D é um anel de divisão.

Sejam σ_1 a involução em $M_2(\mathbb{H})$ dada por

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix}^{\sigma_1} = \begin{pmatrix} \widehat{a} & \frac{3}{5}\widehat{c} \\ \frac{5}{3}\widehat{b} & \widehat{d} \end{pmatrix}$$

e σ_2, σ_3, σ_4 e σ_5 involuções em $M_2(\mathbb{C})$ dadas por

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix}^{\sigma_2} = \begin{pmatrix} a & \frac{c}{2} \\ 2b & d \end{pmatrix}, \quad \begin{pmatrix} a & b \\ c & d \end{pmatrix}^{\sigma_3} = \begin{pmatrix} a & -c \\ -b & d \end{pmatrix},$$

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix}^{\sigma_4} = \begin{pmatrix} \widetilde{a} & -\widetilde{c} \\ -\widetilde{b} & \widetilde{d} \end{pmatrix} \quad \text{e} \quad \begin{pmatrix} a & b \\ c & d \end{pmatrix}^{\sigma_5} = \begin{pmatrix} d & -b \\ -c & a \end{pmatrix},$$

onde $\widehat{\ }$ e $\widetilde{\ }$ denotam, respectivamente, a involução canônica em $\mathbb{H}$ e a conjugação complexa em $\mathbb{C}$.

Então σ_1 induz em $\mathbb{H}$ uma involução $^-$ que coincide com a involução canônica $\widehat{\ }$ em $\mathbb{H}$ e cada σ_m, com $m = 2, 3, 4$ e 5, induz em $\mathbb{C}$ uma involução $^-$, que é a identidade quando $m = 2, 3$ e 5 e coincide com a conjugação complexa $\widetilde{\ }$ no caso em que $m = 4$. Além disso, para cada $^-$ assim definido, temos uma aplicação τ_m (com $\tau_2 = \tau_3 = \tau_5$) e podemos escrever:

$$\sigma_m = \mathrm{Int}(C_m) \circ \tau_m, \text{ para } m = 1, 2, 3 \text{ e } 4, \quad \text{e} \quad \sigma_5 = \mathrm{Int}(S) \circ \tau_5,$$

$$\text{onde } C_1 = \begin{pmatrix} 3 & 0 \\ 0 & 5 \end{pmatrix}, C_2 = \begin{pmatrix} i & 0 \\ 0 & 2i \end{pmatrix}, C_3 = C_4 = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \text{ e } S = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}.$$

Ainda, os elementos da diagonal de C_1 são fixados pela involução canônica em $\mathbb{H}$ (que é a involução $^-$ induzida por σ_1), os elementos da diagonal de C_2 e C_3 são fixados pela identidade (que é a involução $^-$ induzida por σ_2 e σ_3) e os da diagonal de C_4 são fixados pela conjugação complexa (que é a involução $^-$ induzida por σ_4).

Assim, σ_1, σ_2, σ_3 e σ_4 se enquadram no Exemplo 1.2.11 e σ_5 é a involução do Exemplo 1.2.12 quando $K = \mathbb{C}$ e $n = 2$. Em geral, a menos de isomorfismo de anéis com involução, toda involução em $M_n(D)$ se enquadra em um destes dois exemplos. Isto é o que nos informa o próximo resultado, cuja demonstração pode ser encontrada em [3].

Teorema 3.2.1 ([4], Lema 2.1) *Sejam D um anel de divisão com centro $\mathcal{Z}(D)$ e n um inteiro positivo. Suponhamos que $M_n(D)$ tenha uma involução $*$. Então uma, e somente uma, das alternativas abaixo ocorre:*

(i) D tem uma involução $^-$ induzida por $*$ e existe uma matriz diagonal invertível $C = \mathrm{diag}(c_1, \cdots, c_n) \in M_n(D)$, com $\overline{c_i} = c_i$ para todo i, tal que $(M_n(D), *) \cong (M_n(D), \mathrm{Int}(C) \circ \tau)$.

(ii) $D = \mathcal{Z}(D)$ é comutativo, $n = 2m$ e $(M_n(D), *) \cong (M_n(D), \mathrm{Int}(S) \circ \tau)$, onde a involução $^-$ induzida por $*$ é a involução identidade em D, $S = \begin{pmatrix} 0 & I \\ -I & 0 \end{pmatrix}$ e I é a identidade em $M_m(D)$.

Observação 3.2.2

Segue da demonstração do teorema acima que existe $P \in M_n(D)$ invertível tal que o automorfismo interno $\mathrm{Int}(P)$ é um isomorfismo de anéis com involução de $(M_n(D), *)$ sobre $(M_n(D), \mathrm{Int}(C) \circ \tau)$, no caso do item (i), e de $(M_n(D), *)$ sobre $(M_n(D), \mathrm{Int}(S) \circ \tau)$, quando $*$ se enquadra no item (ii).

Observação 3.2.3

Se $*$ induz uma involução em D diferente da identidade ou se $D \neq \mathcal{Z}(D)$, então $*$ se enquadra necessariamente no item (i) do Teorema 3.2.1.

Exemplo 3.2.4

Seja $*$ a involução em $M_2(\mathbb{H})$ dada por

$$\begin{pmatrix} a_0 + a_1 i + a_2 j + a_3 k & b_0 + b_1 i + b_2 j + b_3 k \\ c_0 + c_1 i + c_2 j + c_3 k & d_0 + d_1 i + d_2 j + d_3 k \end{pmatrix}^* =$$

$$= \begin{pmatrix} d_0 - d_2 i + d_1 j - d_3 k & b_3 + b_1 i + b_2 j + b_0 k \\ -c_3 + c_1 i + c_2 j - c_0 k & a_0 + a_2 i - a_1 j - a_3 k \end{pmatrix},$$

para todo $a_r, b_r, c_r, d_r \in \mathbb{R}$ com $1 \leq r \leq 4$.

Como $\mathbb{H} \neq \mathcal{Z}(\mathbb{H})$, segue da Observação 3.2.3 que $*$ se enquadra no item (i) do Teorema 3.2.1. Agora, $* = \mathrm{Int}(U) \circ \tau$, onde $U = \begin{pmatrix} 0 & j \\ i & 0 \end{pmatrix}$ e $^-$ é a involução em $\mathbb{H}$ dada por

$$\overline{a_0 + a_1 i + a_2 j + a_3 k} = a_0 + a_2 i + a_1 j + a_3 k.$$

Logo, $*$ coincide com a involução de mesmo nome vista no Exemplo 3.1.2 e, portanto,

$$(M_2(\mathbb{H}), *) \cong (M_2(\mathbb{H}), \mathrm{Int}(C) \circ \tau),$$

onde C é a matriz identidade em $M_2(\mathbb{H})$.

Exemplo 3.2.5

Sejam $^-$ a conjugação complexa em $\mathbb{C}$ e $*$ a involução em $M_2(\mathbb{C})$ dada por

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix}^* = \begin{pmatrix} \overline{d} & -\overline{b} \\ -\overline{c} & \overline{a} \end{pmatrix}$$

para todo $a, b, c, d \in \mathbb{C}$.

Então $*$ se enquadra no item (i) do Teorema 3.2.1. De fato, $*$ é a involução de mesmo nome vista no Exemplo 3.1.3, já que $* = \mathrm{Int}(U) \circ \tau$, onde $U = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}$. Assim,

$$(M_2(\mathbb{C}), *) \cong (M_2(\mathbb{C}), \mathrm{Int}(C) \circ \tau),$$

onde $C = \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix}$.

Exemplo 3.2.6

Seja $*$ a involução em $M_4(\mathbb{C})$ dada por

$$\begin{pmatrix} a_{11} & a_{12} & a_{13} & a_{14} \\ a_{21} & a_{22} & a_{23} & a_{24} \\ a_{31} & a_{32} & a_{33} & a_{34} \\ a_{41} & a_{42} & a_{43} & a_{44} \end{pmatrix}^* = \begin{pmatrix} b_{11} & b_{12} & b_{13} & b_{14} \\ b_{21} & b_{22} & b_{23} & b_{24} \\ b_{31} & b_{32} & b_{33} & b_{34} \\ b_{41} & b_{42} & b_{43} & b_{44} \end{pmatrix},$$

onde

j	b_{1j}	b_{3j}
1	$2a_{23} + a_{33} + a_{43}$	$-2a_{21} + 2a_{22} - 4a_{24} - a_{31} + a_{32} - 2a_{34} - a_{41} + a_{42} - 2a_{44}$
2	$-2a_{13} + a_{43}$	$2a_{11} - 2a_{12} + 4a_{14} - a_{41} + a_{42} - 2a_{44}$
3	$-a_{13}$	$a_{11} - a_{12} + 2a_{14}$
4	$-a_{13} - a_{23}$	$a_{11} - a_{12} + 2a_{14} + a_{21} - a_{22} + 2a_{24}$

j	b_{2j}	b_{4j}
1	$-2a_{23} + 2a_{24} - a_{33} + a_{34} - a_{43} + a_{44}$	$-2a_{22} + 4a_{23} - a_{32} + 2a_{33} - a_{42} + 2a_{43}$
2	$2a_{13} - 2a_{14} - a_{43} + a_{44}$	$2a_{12} - 4a_{13} - a_{42} + 2a_{43}$
3	$a_{13} - a_{14}$	$a_{12} - 2a_{13}$
4	$a_{13} - a_{14} + a_{23} - a_{24}$	$a_{12} - 2a_{13} + a_{22} - 2a_{23}$

Temos que $*$ se enquadra no item (ii) do Teorema 3.2.1. Com efeito, $*$ é a involução de mesmo nome vista no Exemplo 3.1.4, já que $* = \mathrm{Int}(U) \circ \tau$, onde $U = \begin{pmatrix} 0 & 0 & 1 & 0 \\ 0 & 0 & -1 & 1 \\ -1 & 1 & 0 & -2 \\ 0 & -1 & 2 & 0 \end{pmatrix}$ e $^-$ é a identidade em $\mathbb{C}$. Logo,

$$(M_4(\mathbb{C}), *) \cong (M_4(\mathbb{C}), \mathrm{Int}(S) \circ \tau),$$

onde $S = \begin{pmatrix} 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ -1 & 0 & 0 & 0 \\ 0 & -1 & 0 & 0 \end{pmatrix}$.

O fato de termos trabalhado no exemplo anterior com $n = 4$ (e não com $n = 2$, como nos Exemplos 3.2.4 e 3.2.5) não foi ao acaso. De fato, se K é um corpo, para se obter uma involução em $M_n(K)$ que se enquadre no item (ii) do Teorema 3.2.1 e não coincida com $\mathrm{Int}(S) \circ \tau$, precisamos trabalhar com n par e maior que 2.

Proposição 3.2.7 *Sejam K um corpo e $*$ uma involução em $M_2(K)$ que se enquadra no item (ii) do Teorema 3.2.1. Então $* = \mathrm{Int}(S) \circ \tau$.*

Demonstração: Segue da Observação 3.2.2 que existe $P \in M_2(K)$ invertível tal que

$$\begin{array}{rccc} \psi & : & (M_2(K), *) & \to & (M_2(K), \mathrm{Int}(S) \circ \tau) \\ & & A & \mapsto & PAP^{-1} \end{array}$$

é um isomorfismo de anéis com involução. Assim, como ψ preserva involução, temos

$$PA^*P^{-1} = \psi(A^*) = \mathrm{Int}(S)(\psi(A))^\tau = S(PAP^{-1})^\tau S^{-1} = S(P^{-1})^\tau A^\tau P^\tau S^{-1},$$

para toda matriz $A \in M_2(K)$. Logo,

$$A^* = P^{-1}S(P^{-1})^\tau A^\tau P^\tau S^{-1}P = (P^{-1}S(P^{-1})^\tau)A^\tau(P^{-1}S(P^{-1})^\tau)^{-1}.$$

Como τ é a involução transposta em $M_2(K)$, então $BSB^\tau = (\det B)S$, para toda matriz $B \in M_2(K)$. Assim,

$$A^* = (\det(P^{-1})S)A^\tau(\det(P^{-1})S)^{-1} = \det(P^{-1})SA^\tau\frac{1}{\det(P^{-1})}S^{-1} = SA^\tau S^{-1},$$

para toda matriz $A \in M_2(K)$. E, portanto, $* = \mathrm{Int}(S) \circ \tau$. □

Como toda involução em um corpo K é um automorfismo, podemos, uma vez conhecidos os automorfismos de K, caracterizar todas as involuções em $M_n(K)$.

Exemplo 3.2.8 *Caracterização das involuções em $M_n(\mathbb{R})$*

Lembrando que a identidade é o único automorfismo de $\mathbb{R}$, vemos que a única involução em $\mathbb{R}$ é a identidade. Portanto, se $*$ é uma involução em $M_n(\mathbb{R})$, então a involução $^-$ induzida por $*$ é a identidade. Logo nossa involução τ é a aplicação transposta e segue do Teorema 3.2.1 que, a menos de isomorfismo de anéis com involução, $*$ é da forma $\mathrm{Int}(S) \circ \tau$ ou $\mathrm{Int}(C) \circ \tau$, onde C é uma matriz diagonal invertível em $M_n(\mathbb{R})$.

Exemplo 3.2.9 *Caracterização das involuções em* $M_n(\mathbb{Q}(\sqrt{d}))$

Seja d um inteiro positivo livre de quadrados. As únicas involuções em $\mathbb{Q}(\sqrt{d})$ são:

$$\begin{array}{rccc} \xi_1 & : & \mathbb{Q}(\sqrt{d}) & \to & \mathbb{Q}(\sqrt{d}) \\ & & a+b\sqrt{d} & \mapsto & a+b\sqrt{d} \end{array} \quad \text{e} \quad \begin{array}{rccc} \xi_2 & : & \mathbb{Q}(\sqrt{d}) & \to & \mathbb{Q}(\sqrt{d}) \\ & & a+b\sqrt{d} & \mapsto & a-b\sqrt{d}, \end{array}$$

pois todo automorfismo de $\mathbb{Q}(\sqrt{d})$ é a identidade em $\mathbb{Q}$ e leva $\sqrt{d}$ em $\pm\sqrt{d}$.

Se $*$ é uma involução em $M_n(\mathbb{Q}(\sqrt{d}))$, então $*$ induz em $\mathbb{Q}(\sqrt{d})$ uma involução $^-$ que coincide com ξ_1 ou ξ_2.

• Se $^-$ é a involução ξ_1, então τ é a involução transposta e, a menos de isomorfismo de anéis com involução, $*$ é da forma $\mathrm{Int}(S)\circ\tau$ ou $\mathrm{Int}(C)\circ\tau$, onde C é uma matriz diagonal invertível em $M_n(\mathbb{Q}(\sqrt{d}))$.

• Se $^-$ é a involução ξ_2, então τ é dada por $(a_{ij}+b_{ij}\sqrt{d})^\tau = (a_{ji}-b_{ji}\sqrt{d})$ e, a menos de isomorfismo de anéis com involução, $*$ é da forma $\mathrm{Int}(C)\circ\tau$, onde C é uma matriz diagonal invertível em $M_n(\mathbb{Q}(\sqrt{d}))$ cujas entradas são fixadas por ξ_2, isto é, pertencem a $\mathbb{Q}$.

3.3 Produto de elementos Cayley unitários

No capítulo anterior trabalhamos com elementos Cayley unitários em uma álgebra de grupo KG munida da involução canônica e vimos que em $\mathbb{Q}D_4$ existe um elemento unitário que não é Cayley unitário (Proposição 2.4.7), nem o produto de dois elementos Cayley unitários de $\mathbb{Q}D_4$ (Exemplo 2.4.9).

Nesta seção veremos que o problema de determinar quando um elemento unitário é um produto de dois elementos Cayley unitários de $M_n(D)$ está completamente resolvido, quando este anel está munido de uma involução $*$ e D é um anel de divisão com característica diferente de 2.

Observemos inicialmente que se $*$ induz a identidade em D, então D é um corpo, já que $ab = (ab)^* = b^*a^* = ba$, para todo $a, b \in D$. Assim, temos dois casos possíveis para nossa involução $*$ em $M_n(D)$:

1^o **caso:** $*$ não induz a identidade em D

2^o **caso:** $*$ induz a identidade em D e assim $D = \mathcal{Z}(D)$.

Com o objetivo de demonstrar o Teorema 3.3.2, que trata do caso em que $*$ induz uma involução em D diferente da identidade, consideremos o seguinte lema.

Lema 3.3.1 ([2], Lema 3) *Seja D um anel de divisão e consideremos $H_1, \cdots, H_n$ subconjuntos de D, cada qual contendo pelo menos dois elementos. Então para qualquer $A \in M_n(D)$, existe uma matriz diagonal $H = \mathrm{diag}(h_1, \cdots, h_n)$, com $h_i \in H_i$ para $i = 1, \cdots, n$, tal que $I - A - AH$ é invertível em $M_n(D)$, onde I é a identidade em $M_n(D)$.*

Demonstração: Nossa prova será por indução sobre n. Primeiramente, consideremos o caso $n = 1$.

• Se $A = 0$, então $I - A - AH = I$ para qualquer $H \in H_1$ e a afirmação vale trivialmente.

• Se $A \neq 0$, então $I - A - AH = 0$ apenas se $H = A^{-1} - I$. Como H_1 contém pelo menos dois elementos, existe $H \in H_1$ com $H \neq A^{-1} - I$ e para este H temos que $I - A - AH \neq 0$, isto é, $I - A - AH$ é invertível em $M_n(D)$.

Agora assumamos que $n > 1$ e que a afirmação vale para $n - 1$. Consideremos $A = (a_{ij})_{1 \leq i,j \leq n} \in M_n(D)$ e seja $A' \in M_{n-1}(D)$ a submatriz de A formada pelas primeiras $n - 1$ linhas e $n - 1$ colunas de A, isto é, $A' = (a_{ij})_{1 \leq i,j \leq n-1}$.

$$A = \left(\begin{array}{c|c} & a_{1n} \\ A' & \vdots \\ & a_{n-1,n} \\ \hline a_{n1} \cdots a_{n,n-1} & a_{n,n} \end{array}\right)$$

Da hipótese de indução segue que existe $H' = \mathrm{diag}(h_1, \cdots, h_{n-1})$, com $h_i \in H_i$, $i = 1, \cdots, n-1$, tal que $I' - A' - A'H'$ é invertível em $M_{n-1}(D)$, onde I' denota a identidade em $M_{n-1}(D)$. Mostraremos que $I - A - AH$ é singular para no máximo um elemento $h_n \in H_n$, onde $H = \mathrm{diag}(h_1, \cdots, h_n)$.

Suponhamos que $h_n \in H_n$ seja tal que

$$I - A - AH = \left(\begin{array}{c|c} I' - A' - A'H' & \begin{array}{c} -a_{1n}(1+h_n) \\ \vdots \\ -a_{n-1,n}(1+h_n) \end{array} \\ \hline -a_{n1}(1+h_1) \cdots -a_{n,n-1}(1+h_{n-1}) & 1 - a_{n,n}(1+h_n) \end{array}\right)$$

seja singular.

Então existe um vetor não nulo $v = (v_1, \cdots, v_n)$ com entradas em D tal que $v(I - A - AH) = 0$. Seja $v' = (v_1, \cdots, v_{n-1})$. Mostraremos que, como $v \neq 0$, então $v_n \neq 0$.

Suponhamos por absurdo que $v_n = 0$. A multiplicação de v pelas primeiras $n-1$ colunas de $I-A-AH$ nos dá $v'(I'-A'-A'H') = 0$ e, como a matriz $I'-A'-A'H'$ é invertível em $M_{n-1}(D)$, temos que $v' = 0$ e portanto $v = 0$, uma contradição. Assim $v_n \neq 0$.

O produto de v pelas primeiras $n-1$ colunas de $I - A - AH$ é

$$v'(I' - A' - A'H') - v_n(a_{n1}(1+h_1), \cdots, a_{n,n-1}(1+h_{n-1})) = 0.$$

Logo

$$({v_n}^{-1}v_1, \cdots, {v_n}^{-1}v_{n-1}) = (a_{n1}(1+h_1), \cdots, a_{n,n-1}(1+h_{n-1}))(I' - A' - A'H')^{-1}$$

é determinado por $h_1, \cdots, h_{n-1}$ e as entradas de A.

O produto de v pela n-ésima coluna de $I - A - AH$ é

$$v_n - \sum_{i=1}^{n} v_i a_{in}(1+h_n) = 0.$$

Como $v_n \neq 0$, então $\sum_{i=1}^{n} v_i a_{in} \neq 0$ e portanto

$$h_n = \left(\sum_{i=1}^{n} v_i a_{in}\right)^{-1} \cdot v_n - 1 = \left(\sum_{i=1}^{n} ({v_n}^{-1}v_i) a_{in}\right)^{-1} - 1.$$

Assim, como $({v_n}^{-1}v_1, \cdots, {v_n}^{-1}v_{n-1})$ é determinado por $h_1, \cdots, h_{n-1}$ e as entradas de A, então h_n também o é. Portanto, $I - A - AH$ é singular para no máximo um elemento $h_n \in H_n$, onde $H = \text{diag}(h_1, \cdots, h_n)$. Logo, como H_n contém mais de um elemento, podemos escolher $h_n \in H_n$ tal que $H = \text{diag}(h_1, \cdots, h_n)$ torna $I-A-AH$ invertível em $M_n(D)$. □

Teorema 3.3.2 ([2], Teorema 1) *Seja D um anel de divisão com característica diferente de 2. Suponhamos que $R = M_n(D)$ tenha uma involução $*$ que induz uma involução em D diferente da identidade. Então todo elemento unitário de R é um produto de dois elementos Cayley unitários.*

Demonstração: Seja $^-$ a involução induzida por $*$ em D. Então $^-$ é diferente da identidade e segue da Observação 3.2.3 que $*$ se enquadra no item (i) do Teorema 3.2.1. Em virtude da Proposição 3.1.5, podemos supor que existem n elementos π_i's em D, com $\overline{\pi_i} = \pi_i \neq 0$, tais que

$$(a_{ij})^* = (\pi_i \overline{a_{ji}} {\pi_j}^{-1})$$

para toda matriz $(a_{ij}) \in R$.

Seja U uma matriz unitária de R. Como a característica de D é diferente de 2, podemos definir a matriz

$$A = \frac{1}{2}(I - U).$$

Para $i = 1, \cdots, n$, seja

$$H_i = \{\pi_i a \in D \,|\, \overline{a} = -a\}.$$

Como $^-$ não é a identidade em D, existe $b \in D$ tal que $\overline{b} = c \neq b$. Assim, seja $a = b - c \neq 0$. Temos que

$$\overline{a} = \overline{b - c} = \overline{b} - \overline{c} = c - b = -(b - c) = -a.$$

Como $\overline{-a} = -\overline{a} = -(-a)$, $\pi_i \neq 0$ para todo $i = 1, \cdots, n$ e a característica de D é diferente de 2, então $\pi_i a$ e $\pi_i(-a)$ são dois elementos distintos em H_i. Portanto H_i contém pelo menos dois elementos e do Lema 3.3.1 segue que existe uma matriz diagonal $H = \text{diag}(h_1, \cdots, h_n)$, com $h_i \in H_i$ para $i = 1, \cdots, n$, tal que $I - A - AH$ é invertível em R.

Temos que $H = (h_{ij}) \in R^-$. De fato, para cada $i = 1, \cdots, n$, existe $a_i \in D$ tal que $\overline{a_i} = -a_i$ e $h_i = \pi_i a_i$. Assim,

$$(h_{ij})^* = (\pi_i \overline{h_{ji}} {\pi_j}^{-1}) = \begin{cases} \pi_i \overline{h_i} {\pi_i}^{-1}, & \text{se } j = i \\ \pi_i \overline{0} {\pi_j}^{-1}, & \text{se } j \neq i. \end{cases}$$

Agora,

$$\pi_i\overline{h_i}{\pi_i}^{-1} = \pi_i\overline{\pi_i a_i}{\pi_i}^{-1} = \pi_i\overline{a_i}\,\overline{\pi_i}{\pi_i}^{-1} = \pi_i(-a_i)\pi_i{\pi_i}^{-1} = -\pi_i a_i = -h_i.$$

Logo $(h_{ij})^* = -(h_{ij})$.

Além disso, temos que $I + H$ é invertível em R, pois

$$I + H = \mathrm{diag}(1 + h_1, \cdots, 1 + h_n)$$

e $1 + h_i = 1 + \pi_i a_i \neq 0$ para todo $i = 1, \cdots, n$ (já que $\overline{a_i} = -a_i$ e $\overline{\pi_i} = \pi_i \neq 0$). Como

$$I - A - AH = \frac{1}{2}[(I + U) - (I - U)H]$$

é invertível em R, então $(I+U)-(I-U)H$ é invertível. Assim, como $H \in R^-$ com $I + H$ invertível em R e $U \in \mathcal{U}n(R)$, segue da Proposição 1.3.7 que U é um produto de dois elementos Cayley unitários de R. □

Trataremos agora do caso em que $*$ induz a identidade em D e portanto D é um corpo K.

Primeiramente notemos que se K é um corpo e $*$ é uma involução em $M_n(K)$, desde que $\mathcal{Z}(M_n(K)) \cong K$, então $*$ induz a identidade em K se, e somente se, $*$ é do primeiro tipo.

A fim de provarmos a próxima proposição, consideremos o seguinte lema.

Lema 3.3.3 *Sejam K um corpo e φ um automorfismo de $M_n(K)$ que fixa os elementos de K. Então φ é um automorfismo interno.*

Demonstração: Segue dos comentários feitos na primeira seção do Capítulo 1 que K^n pode ser visto como um $M_n(K)$-módulo com o produto induzido tanto pela identidade (que é um automorfismo de $M_n(K)$), como por φ. Em ambos os casos concluímos do Exemplo 1.1.4 que o respectivo $M_n(K)$-módulo é simples. Pela Proposição 1.1.8, esses dois $M_n(K)$-módulos são isomorfos e, assim, existe um isomorfismo de $M_n(K)$-módulos $f : K^n \to K^n$ tal que

$$f(A \cdot v) = \varphi(A) \cdot f(v),$$

para todo $v \in K^n$ e $A \in M_n(K)$.

Agora, como φ fixa os elementos de K e $\varphi(I) = I$, então

$$f(\alpha v) = f((\alpha I) \cdot v) = \varphi(\alpha I) \cdot f(v) = \alpha\varphi(I) \cdot f(v) = \alpha I \cdot f(v) = \alpha f(v),$$

para todo $\alpha \in K$ e $v \in K^n$.

Assim, f é uma transformação linear bijetiva e, portanto, existe uma matriz C invertível tal que $f(v) = C \cdot v$, para todo $v \in K^n$. Logo,

$$C \cdot (A \cdot v) = \varphi(A) \cdot (C \cdot v),$$

para todo $v \in K^n$ e $A \in M_n(K)$, o que implica que $C \cdot A = \varphi(A) \cdot C$, para toda matriz $A \in M_n(K)$. Portanto,

$$\varphi(A) = C \cdot A \cdot C^{-1},$$

para toda matriz $A \in M_n(K)$, isto é, $\varphi = \mathrm{Int}(C)$. □

Na próxima proposição e nos dois corolários subseqüentes, estaremos considerando R o anel de matrizes $M_n(K)$ sobre um corpo K munido de uma involução $*$ do primeiro tipo.

Proposição 3.3.4 ([2], Lema 4) *Para todo $A \in R$ temos que* $\det A^* = \det A$.

Demonstração: Sejam A^t a transposta da matriz A em R e φ a aplicação de R em R tal que $\varphi(A) = (A^*)^t$. Se $A, B \in R$ então, como $*$ e t são involuções em R, temos que φ é uma bijeção com $\varphi(A + B) = \varphi(A) + \varphi(B)$. Ainda,

$$\varphi(AB) = ((AB)^*)^t = (B^*A^*)^t = (A^*)^t(B^*)^t = \varphi(A)\varphi(B).$$

Logo φ é um automorfismo de R. Além disso, como $*$ e t são do primeiro tipo, então φ deixa os elementos centrais de R fixados. Desta forma, φ é um automorfismo de R que fixa os elementos de K e, portanto, pelo lema anterior, existe uma matriz invertível $C \in R$ tal que, para todo $A \in R$, $\varphi(A) = CAC^{-1}$, isto é,

$$(A^*)^t = CAC^{-1}.$$

Assim, $A^* = (C^t)^{-1}A^tC^t$ e, portanto,

$$\det A^* = (\det C^t)^{-1}(\det A^t)(\det C^t) = \det A^t = \det A.$$

□

Corolário 3.3.5 ([2], Corolário 1) *Se $U \in \mathcal{U}n(R)$ então* $\det U = \pm 1$.

Demonstração: Seja $U \in \mathcal{U}n(R)$. Como $UU^* = 1$, então segue da proposição anterior que $(\det U)^2 = (\det U)(\det U^*) = 1$ e portanto $\det U = \pm 1$. □

Corolário 3.3.6 ([2], Corolário 2) *Se $U \in R$ é um produto de elementos Cayley unitários então* $\det U = 1$.

Demonstração: Suponhamos que $V \in \mathcal{U}n^C(R)$, digamos $V = (I-H)(I+H)^{-1}$ para algum $H \in R^-$ com $I+H$ invertível em R. Desde que $H = -H^*$, usando a Proposição 3.3.4, obtemos

$$\begin{aligned} \det V &= [\det(I-H)][\det(I+H)]^{-1} = [\det(I-H)][\det(I-H)^*]^{-1} \\ &= [\det(I-H)][\det(I-H)]^{-1} = 1. \end{aligned}$$

Assim, todo elemento Cayley unitário de R possui determinante 1. Se $U = U_1 \cdots U_r$, com $U_i \in \mathcal{U}n^C(R)$ para $i = 1, \cdots, r$, então

$$\det U = (\det U_1) \cdots (\det U_r) = 1.$$

□

O corolário anterior nos permite concluir que se $*$ é uma involução do primeiro tipo em $M_n(K)$, então apenas as matrizes unitárias de determinante 1 podem ser expressas como um produto de elementos Cayley unitários. O próximo exemplo mostra que nem toda matriz unitária de determinante 1 pode ser assim expressa.

Exemplo 3.3.7 *Matriz unitária de determinante 1 que não pode ser expressa como um produto de elementos Cayley unitários*

Sejam $K = \{-1, 0, 1\}$ um corpo com três elementos e $R = M_2(K)$ com uma involução $*$ definida por

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix}^* = \begin{pmatrix} a & -c \\ -b & d \end{pmatrix}.$$

Os elementos anti-simétricos de R são todos da forma $\begin{pmatrix} 0 & \alpha \\ \alpha & 0 \end{pmatrix}$, onde $\alpha \in K$. Logo

$$R^- = \left\{ \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} 0 & -1 \\ -1 & 0 \end{pmatrix} \right\}.$$

O único elemento de R^- com a propriedade de ser invertível quando somado à identidade é $\begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$. Logo, $\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ é o único elemento Cayley unitário de R.

Agora, $\begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix} \in \mathcal{U}n(R)$ não é um produto de elementos Cayley unitários de R, embora tenha determinante 1.

Na verdade, este é o único exemplo de matriz unitária de determinante 1 que não é um produto de elementos Cayley unitários, conforme garante o seguinte resultado de C. Chuang e P. Lee.

Teorema 3.3.8 ([2], Teorema 2) *Seja K um corpo de característica diferente de 2. Suponhamos que $R = M_n(K)$ tenha uma involução $*$ do primeiro tipo. Então qualquer elemento unitário de R com determinante 1 é um produto de dois elementos Cayley unitários, exceto quando K é um corpo com três elementos, $n = 2$ e $*$ é a involução dada por $\begin{pmatrix} a & b \\ c & d \end{pmatrix}^* = \begin{pmatrix} a & -c \\ -b & d \end{pmatrix}$.*

Exemplo 3.3.9 *Elementos Cayley unitários de $M_2(K)$*

Sejam K um corpo de característica diferente de 2 e $*$ a involução transposta em $R = M_2(K)$, isto é,

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix}^* = \begin{pmatrix} a & c \\ b & d \end{pmatrix}.$$

Então

$$R^- = \left\{ \begin{pmatrix} 0 & \alpha \\ -\alpha & 0 \end{pmatrix} ; \alpha \in K \right\} \quad \text{e} \quad \mathcal{U}n(R) = \mathcal{A}_1 \cup \mathcal{A}_2,$$

onde

$$\mathcal{A}_1 = \left\{ \begin{pmatrix} a & b \\ -b & a \end{pmatrix} ; a^2 + b^2 = 1 \right\} \text{ e } \mathcal{A}_2 = \left\{ \begin{pmatrix} a & b \\ b & -a \end{pmatrix} ; a^2 + b^2 = -1 \right\}.$$

Seja $\alpha \in K$ tal que $1 + \alpha^2 \neq 0$. O elemento Cayley unitário obtido a partir de $H = \begin{pmatrix} 0 & \alpha \\ -\alpha & 0 \end{pmatrix}$ é

$$\begin{aligned} U_{[H]} &= \left[\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} - \begin{pmatrix} 0 & \alpha \\ -\alpha & 0 \end{pmatrix} \right] \left[\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} + \begin{pmatrix} 0 & \alpha \\ -\alpha & 0 \end{pmatrix} \right]^{-1} \\ &= \begin{pmatrix} 1 & -\alpha \\ \alpha & 1 \end{pmatrix} \begin{pmatrix} 1 & \alpha \\ -\alpha & 1 \end{pmatrix}^{-1} = \frac{1}{1+\alpha^2} \begin{pmatrix} 1 & -\alpha \\ \alpha & 1 \end{pmatrix} \begin{pmatrix} 1 & -\alpha \\ \alpha & 1 \end{pmatrix} \\ &= \frac{1}{1+\alpha^2} \begin{pmatrix} 1-\alpha^2 & -2\alpha \\ 2\alpha & 1-\alpha^2 \end{pmatrix}. \end{aligned}$$

Logo

$$\mathcal{U}n^C(R) = \left\{ \frac{1}{1+\alpha^2} \begin{pmatrix} 1-\alpha^2 & -2\alpha \\ 2\alpha & 1-\alpha^2 \end{pmatrix} ; 1 + \alpha^2 \neq 0 \right\}.$$

Segue do Corolário 3.3.6 que os elementos de $\mathcal{U}n(R)$ que são produtos de Cayley unitários estão todos contidos em $\mathcal{A}_1$ e do Teorema 3.3.8 concluímos que, na verdade, todos os elementos de $\mathcal{A}_1$ são produtos de dois elementos Cayley unitários.

Se $A = \begin{pmatrix} a & b \\ -b & a \end{pmatrix} \in \mathcal{A}_1$, então $A = U_{[H]}U_{[H']}$, com

$$\begin{cases} H = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \text{ e } H' = \begin{pmatrix} 0 & -\frac{a}{1-b} \\ \frac{a}{1-b} & 0 \end{pmatrix}, & \text{se } b \neq 1 \\ \\ H = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \text{ e } H' = \begin{pmatrix} 0 & \frac{a}{1+b} \\ -\frac{a}{1+b} & 0 \end{pmatrix}, & \text{se } b \neq -1. \end{cases}$$

De fato, se $b \neq 1$, então

$$U_{[H]} = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \text{ e } U_{[H']} = \frac{1}{(1-b)^2 + a^2} \begin{pmatrix} (1-b)^2 - a^2 & 2a(1-b) \\ -2a(1-b) & (1-b)^2 + a^2 \end{pmatrix}.$$

Como $a^2 + b^2 = 1$, então $(1-b)^2 - a^2 = -2b(1-b)$ e $(1-b)^2 + a^2 = 2(1-b)$. Logo $U_{[H']} = \begin{pmatrix} -b & a \\ -a & -b \end{pmatrix}$ e, portanto,

$$U_{[H]}U_{[H']} = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} -b & a \\ -a & -b \end{pmatrix} = \begin{pmatrix} a & b \\ -b & a \end{pmatrix} = A.$$

Analogamente temos o caso em que $b \neq -1$.

Considerações Finais

Considerando K uma extensão real de $\mathbb{Q}$, $\alpha \in K$ e x um elemento de ordem finita de um grupo G, o Teorema 2.4.1 nos permite caracterizar todos os elementos Cayley unitários da álgebra de grupo KG, munida da involução canônica, obtidos a partir de um elemento anti-simétrico da forma $\alpha(x-x^{-1})$. Assim, quando G é um grupo tal que o K-módulo KG^- possui um único gerador, podemos utilizar este teorema para caracterizar todo o conjunto $\mathcal{U}n^C(KG)$. Essencialmente fizemos isto para $K = \mathbb{Q}$ nos Exemplos 2.4.2, 2.4.3 e 2.4.4, quando $G = C_3$, S_3 e C_4, respectivamente.

Agora, para $G = C_5 = \langle x \rangle$, temos que

$$KC_5{}^- = \left\{ \alpha_1(x - x^4) + \alpha_3(x^3 - x^2) \,;\, \alpha_1, \alpha_3 \in K \right\}$$

e assim o Teorema 2.4.1 caracteriza apenas os elementos Cayley unitários de KC_5 tais que $\alpha_1 = 0$ ou $\alpha_3 = 0$. Cálculos computacionais nos permitem concluir, conforme visto no Exemplo 2.4.6, que existe o inverso de $1 + \alpha_1(x - x^4) + \alpha_3(x^3 - x^2)$ em KC_5 para todo $\alpha_1, \alpha_3 \in K$ e ainda nos dão o elemento Cayley unitário $u_{[k]}$ para $k = \alpha_1(x - x^4) + \alpha_3(x^3 - x^2)$. Ou seja, caracterizamos completamente o conjunto $\mathcal{U}n^C(KC_5)$.

Cálculos semelhantes podem ser feitos para $C_7 = \langle x \rangle$ e obtemos uma expressão geral para o inverso de $1+\alpha_1(x-x^6)+\alpha_3(x^3-x^4)+\alpha_5(x^5-x^2)$ em KC_7 em função de parâmetros $\alpha_1, \alpha_3, \alpha_5 \in K$.

Isto sugere que em geral para $C_p = \langle x \rangle$, com p primo ímpar, temos que

$$1 + \alpha_1(x - x^{p-1}) + \alpha_3(x^3 - x^{p-3}) + \cdots + \alpha_{p-2}(x^{p-2} - x^2)$$

é invertível em KC_p. E assim, o elemento Cayley unitário $u_{[k]}$ pode ser construído para

$$k = \alpha_1(x - x^{p-1}) + \alpha_3(x^3 - x^{p-3}) + \cdots + \alpha_{p-2}(x^{p-2} - x^2).$$

É importante salientar que, embora os Teoremas 2.3.1 e 2.4.1 tenham sido enunciados e provados no caso em que K é uma extensão real de $\mathbb{Q}$, eles são verdadeiros para qualquer corpo K tal que $G_{n+1} + \alpha^2 G_{n-1} - \alpha^n(1 + (-1)^n)$ seja diferente de zero para todo $n > 2$ e $\alpha \in K$. Em particular, se G é um grupo finito de ordem $m > 2$, basta observar se $G_{n+1} + \alpha^2 G_{n-1} - \alpha^n(1 + (-1)^n)$ é diferente de zero para todo $\alpha \in K$ e para todo n tal que $2 < n \leq m$ e n divide m.

Por exemplo, se G é um grupo de ordem 20, então, conforme veremos a seguir, os Teoremas 2.3.1 e 2.4.1 são verdadeiros também para a extensão não real de $\mathbb{Q}$ dada por $\mathbb{Q}(i\sqrt{d})$, onde $d > 1$ é um inteiro positivo livre de quadrados.

Exemplo

Seja G um grupo de ordem $m = 20$. Então os divisores de m maiores que 2 são 4, 5, 10 e 20. Agora,

n	$G_{n+1} + \alpha^2 G_{n-1} - \alpha^n(1 + (-1)^n)$
4	$1 + 4\alpha^2$
5	$1 + 5\alpha^2 + 5\alpha^4$
10	$(1 + 5\alpha^2 + 5\alpha^4)^2$
20	$(1 + 4\alpha^2)(1 + 3\alpha^2 + \alpha^4)^2(1 + 5\alpha^2 + 5\alpha^4)^2$

Consideremos, então, os polinômios na variável α dados por $1+4\alpha^2$, $1+5\alpha^2+5\alpha^4$ e $1 + 3\alpha^2 + \alpha^4$. Temos:

Polinômio	Raízes em $\mathbb{C}$
$1 + 4\alpha^2$	$\pm\frac{i}{2}$
$1 + 5\alpha^2 + 5\alpha^4$	$\pm i\sqrt{\frac{1}{10}(5 \pm \sqrt{5})}$
$1 + 3\alpha^2 + \alpha^4$	$\pm i\sqrt{\frac{1}{2}(3 \pm \sqrt{5})}$

Assim, se $K = \mathbb{Q}(i\sqrt{d})$ onde $d > 1$ é um inteiro positivo livre de quadrados, segue que $G_{n+1} + \alpha^2 G_{n-1} - \alpha^n(1 + (-1)^n)$ é diferente de zero para todo $\alpha \in K$ e para todo n tal que $2 < n \leq 20$ e n divide 20. Logo, valem os Teoremas 2.3.1 e 2.4.1 para tal grupo G e tal corpo K.

Antes de finalizar, observemos que, na Seção 1 do Capítulo 3, vimos três exemplos de isomorfismos de anéis de matrizes com involução. Em todos eles consideramos uma involução $^-$ em um anel de divisão D e duas involuções em $M_n(D)$, a saber

$$* = \mathrm{Int}(U) \circ \tau \ \text{ e } \ \sigma = \mathrm{Int}(V) \circ \tau,$$

onde U é uma matriz invertível em $M_n(D)$ tal que $U^\tau = \pm U$ e

- No Exemplo 3.1.2, V é a matriz identidade
- No Exemplo 3.1.3, V é uma matriz C diagonal invertível cujas entradas são fixadas pela involução $^-$
- No Exemplo 3.1.4, V é a matriz $S = \begin{pmatrix} 0 & I \\ -I & 0 \end{pmatrix}$, onde I é a identidade em $M_2(\mathbb{C})$.

Além disso, o isomorfismo considerado era sempre um automorfismo interno $\mathrm{Int}(P)$, onde P é uma matriz invertível em $M_n(D)$ tal que $PU = V(P^{-1})^\tau$.

Embora possa parecer que as involuções $*$ e σ e os isomorfismos de anéis de matrizes com involução definidos como acima são um tanto quanto particulares, eles na verdade dão conta de toda a caracterização feita no Teorema 3.2.1.

De fato, conforme podemos verificar em [3], dada uma involução $*$ em $M_n(D)$, existe uma matriz invertível $U \in M_n(D)$ e uma involução $^-$ induzida por $*$ em D tal que

$$* = \mathrm{Int}(U) \circ \tau \ \text{ e } \ U^\tau = \pm U,$$

sendo que a alternativa $U^\tau = -U$ é considerada apenas no caso em que n é par, $^-$ é a identidade e D é um corpo.

Ainda, o isomorfismo de anéis com involução que nos permite caracterizar $*$ é na verdade um automorfismo interno $\mathrm{Int}(P)$, onde P é uma matriz invertível em $M_n(D)$ tal que

- *No caso em que $U^\tau = U$:* $PU = C(P^{-1})^\tau$ para alguma matriz C diagonal invertível cujas entradas são fixadas pela involução $^-$
- *No caso em que $n = 2m$, $^-$ é a identidade, D é um corpo e $U^\tau = -U$:* $PU = S(P^{-1})^\tau$ com $S = \begin{pmatrix} 0 & I \\ -I & 0 \end{pmatrix}$, onde I é a identidade em $M_m(D)$.

Referências Bibliográficas

[1] Albert. A. *Involutorial simple algebras and real Riemann matrices.* Ann. of Math., **36** (1935), 886 - 964.

[2] Chuang, C. L. e Lee, P. H. *Unitary elements in simple artinian rings.* Journal of Algebra, **176** (1995), 449 - 459.

[3] Ferreira, V. O. *Notas: Involuções em anéis artinianos simples*, IME-USP (2004).

[4] Ferreira, V. O., Gonçalves, J. Z. e Mandel, A. *Free symmetric and unitary pairs in division ring with involution.* A aparecer em International Journal of Algebra and Computation, Vol. 5, **1** (2005).

[5] Gonçalves, J. Z. e Passman, D. S. *Unitary units in group algebras.* Israel Journal of Mathematics, **125** (2001), 131 - 155.

[6] Herstein, I. N. *Rings with involution.* Lectures in Math. (1976).

[7] Jacobson, N. *Basic Algebra I.* W. H. Freeman and Company (1974).

[8] Knus, M. A., Merkurjev, A., Rost, M. e Tignol, J. P. *The book of involutions.* Colloquium Publications, Vol.44, Amer. Math. Society (1998).

[9] Lam, T. Y. *A First Course in Noncommutative Rings.* Springer-Verlag (1991).

[10] Milies, C. P. e Sehgal, S. K. *An introduction to group rings.* Kluwer Academic Publishers (2002).

[11] Wilf, H. S. *Generatingfunctionology.* Academic Press, 2^a edição (1994).