Sobre uma classificação dos anéis de inteiros, dos semigrupos finitos e dos RA-loops com a propriedade hiperbólica

ANTÔNIO CALIXTO DE SOUZA FILHO

TESE APRESENTADA
AO
INSTITUTO DE MATEMÁTICA E ESTATÍSTICA
DA
UNIVERSIDADE DE SÃO PAULO
PARA
OBTENÇÃO DO TÍTULO DE DOUTOR
EM
CIÊNCIAS
Área de Concentração: Matemática
Orientador: Prof. Dr. Orlando Stanley Juriaans

São Paulo, 16 de novembro de 2006

Sobre uma classificação
dos anéis de inteiros,
dos semigrupos finitos
e dos RA-loops
com a propriedade hiperbólica

Este exemplar corresponde à redação
final da tese devidamente corrigida,
defendida por Antônio Calixto de Souza Filho
e aprovada pela comissão julgadora.

–São Paulo, 16 novembro de 2006–

BANCA EXAMINADORA

-Prof. Dr. Orlando Stanley Juriaans (IME-USP)- Presidente

-Prof. Dr. Francisco César Polcino Milies (IME-USP)

-Prof. Dr. Paulo Brumatti (IMECC-UNICAMP)

-Prof. Dr. Pavel Zalesski(UnB)

-Prof. Dr. Wagner de Oliveira Cortes(UFRGS)

Agradecimentos

O agradecimento é um momento especial. Bom em si mesmo. Acima de tudo, agradeço a Deus. Agradeço a meus pais, Terezinha Costa de Souza e Antônio Calixto de Souza(in memorium) pela educação e conduta que me ajudam a construir. As minhas irmãs, Liliane Cristina de Souza e Sônia Regina Vieira pela compreensão por minha ausência A minha sobrinha, Patrícia Regina Vieira por sua confiança e estima e pessoa singular. Agradeço a minhas tias, tios, primas e primos que participaram comigo dessa etapa. Agradeço ao amigo e colega Édson Iwaki, pela sua contribuição constante, pelo apoio enquanto estive no Mato Grosso, e pelas discuções durante a elaboração da tese. Ao Ronaldo pelo seu incentivo e suas inestimáveis acessorias com o Linux, Latex e Beamer. Agradeço a meu amigo Antônio Sérgio Munhoz, pela sua atenção detalhada. Aos meus amigos e colegas do instituto: Wálter Martins, Ronaldo Garcia, Jose Domingo, Sandra, entre outros, cuja diversidade de relação é grande, são pessoas de valorosa participação nestes anos. Agradeço à Ângela por sua presença e à Regina e sua irmã Cida, pela paciência, zelo e energia nas correções do texto. Agradeço aos colegas da UNEMAT, amigos e professores. Agradeço a Luciana, Viviani e Raul, pela amizade contínua. Agradeço à professora Iracema Bund por sua orientação inicial, a minha orientadora da especialização, professora Elza Gomide, aos professores Shestakov, Dokuchaev, Piotri, Cláudio Gorodski, Polcino Milies, às professoras Ofélia, Lúcia Junqueira e Myrian. Agradeço aos membros da banca pela participação e pelas importantes sugestões. Agradeço ao professor I. B. Passi, pela sua participação na gênese deste trabalho, quando de sua visita ou IME-USP, em 2002. Agradeço aos colegas, funcionários, alunos, e professores, do Instituto de Matemática e Estatística e da Universidade de São Paulo, pelo apoio e à estrutura, possíveis pelo trabalho destes. Agradeço a meu orientador Stanley Orlando Juriaans, por sua orientação e sua imparcialidade comprometida com a excelência, a coerência e a dedicação.

Antônio Calixto de Souza Filho

"Pois eu sou e sempre tenho sido uma daquelas naturezas que deve ser guiada pela razão; não importa o que a razão possa ser, sobre a reflexão ela surge como a melhor." (Platão)

Dedicatória

Dedico a meu pai, em sua memória, e a minha mãe, em sua presença.

Conteúdo

Resumo

Apresentamos duas construções para unidades de uma ordem em uma classe de álgebras de quatérnios que é anel de divisão: as unidades de Pell e as unidades de Gauss. Classificamos os anéis de inteiros de extensões quadráticas racionais, R, cujo grupo de unidades $\mathcal{U}(RG)$ é hiperbólico para um certo grupo G fixado. Também classificamos os semigrupos finitos S, tal que, para a álgebra unitária $\mathbb{Q}S$ e para toda $\mathbb{Z}$-ordem Γ de $\mathbb{Q}S$, o grupo de unidades $\mathcal{U}(\Gamma)$ é hiperbólico. Nesse mesmo contexto, classificamos os RA-loops L cujo loop de unidades $\mathcal{U}(\mathbb{Z}L)$ não contém um subgrupo abeliano livre de posto dois.

abstract

For a given division algebra of a quaternion algebra, we construct and define two types of units of its $\mathbb{Z}$-orders: Pell units and Gauss units. Also, for the quadratic imaginary extensions over the racionals and some fixed group G, we classify the algebraic integral rings for which the unit group ring is a hyperbolic group. We also classify the finite semigroups S, for which all integral orders Γ of $\mathbb{Q}S$ have hyperbolic unit group $\mathcal{U}(\Gamma)$. We conclude with the classification of the RA-loops L for which the unit loop of its integral loop ring does not contain a free abelian subgroup of rank two.

Introdução

Uma excelente referência histórico-matemática sobre os Anéis de Grupo pode ser encontrada no Capítulo 3, [27]. Esse texto apresenta diversos resultados da Matemática que contribuíram, a partir do século XIX, para o desenvolvimento da teoria de Anéis de Grupo, com apresentação de extensa referência bibliográfica. Nesse contexto, interessa-nos destacar o artigo *THE UNITS OF GROUP RINGS* de G. Higman, no qual aparecem os primeiros resultados para as unidades do anel de grupo sobre os inteiros de grupos abelianos finitos. Entre estes resultados destacamos o Teorema 11 sobre as unidades de torção de $\mathbb{Z}A$, sendo A um grupo abeliano finito, e em que condições o grupo $\mathcal{U}(\mathbb{Z}A)$ é trivial, isto é, $\mathcal{U}(\mathbb{Z}A) = \mathcal{U}(\mathbb{Z})A$. Nessa direção, Herman, Li e Parmenter em [19], formulam e respondem a questão: "Para quais grupos G e anéis R, que são G-adaptado, RG tem somente unidades triviais? "É suficiente estudar os casos para os grupos classificados por Higman.

Nesta tese, vamos além, pois nos interessa, também, classificar os anéis R, mais especificamente, os anéis de inteiros de extensões quadráticas racionais, cujo grupo $\mathcal{U}_1(RG)$, nesse caso com G abeliano, tenha o posto livre maior que um. Tal necessidade surge porque o problema considerado no capítulo 1, como veremos a seguir, está ligado a este fato.

Dado um grupo G que satisfaz uma propriedade $\mathcal{P}$, é natural perguntar em quais grupos G verifica-se tal propriedade, ou seja, classificar os grupos que satisfazem $\mathcal{P}$. Para R um anel comutativo e com unidade, podemos classificar os grupos G, tal que, o grupo de unidades $\mathcal{U}(RG)$ satisfaz a propriedade $\mathcal{P}$. O teorema de Berman-Higman, por exemplo, classifica os grupos abelianos finitos cujo grupo $\mathcal{U}(\mathbb{Z}A)$ é finito.

Os grupos hiperbólicos foram inicialmente definidos por Gromov em [17] a partir do conceito de espaço métrico hiperbólico. Dado um grupo finitamente gerado, é possível construir uma métrica que, associada ao grafo de Cayley desse mesmo grupo, define um espaço métrico. Um grupo é hiperbólico se seu grafo de Cayley for um espaço métrico hiperbólico.

De acordo com um resultado de Gromov, se Γ é um grupo hiperbólico, então Γ não contém um grupo abeliano livre de posto dois, isto é, $\mathbb{Z}^2 \not\rightarrow \Gamma$. É fato conhecido que, neste caso, para um subgrupo finito $G \subset \Gamma$, a $\mathbb{Q}$-álgebra $\mathbb{Q}G$ tem no máximo uma componente de Wedderburn que não é um anel de divisão e esta deve ser $M_2(\mathbb{Q})$, fato inicialmente provado por E. Jespers em [22]. Neste artigo, Jespers classifica os grupos finitos G que têm complemento normal livre não abeliano em $\mathcal{U}(\mathbb{Z}G)$. Inicialmente é considerado o caso em que existe um complemento normal livre de G em $\mathcal{U}(\mathbb{Z}G)$, e, portanto, $\mathcal{U}(\mathbb{Z}G)$ não contém um subgrupo isomorfo a $\mathbb{Z}^2$.

Recentemente, Juriaans, Passi e Prasad [24] classificaram os grupos finitos G para o qual o grupo $\mathcal{U}_1(\mathbb{Z}G)$ é hiperbólico. Para o caso abeliano, cujo grupo de unidades é trivial, G é um grupo abeliano de expoente que divide 4 ou 6; para o caso abeliano, cujo posto de $\mathcal{U}_1(\mathbb{Z}G)$ é um, $G \in \{C_5, C_8, C_{12}\}$; para G não abeliano, cujo grupo de unidades é trivial, G é um 2-grupo Hamiltoniano e, para G não abeliano, cujo grupo de unidades não é trivial, $G \in \{S_3, D_4, Q_{12}, C_4 \ltimes C_4\}$.

No primeiro capítulo estendemos este resultado, classificando certos anéis R e os grupos finitos G, cujo grupo de unidades $\mathcal{U}_1(RG)$ é hiperbólico, sendo R o anel de inteiros de uma extensão quadrática racional K.

Para o caso em que o grupo G é cíclico, utilizamos uma técnica semelhante à aplicada em ([30],§1.2). Porém, para o caso C_2, um grupo cíclico de ordem 2, seguimos o artigo [19]. Nesse capítulo, determinamos o grupo $\mathcal{U}_1(RC_2)$.

Para o caso em que G não é abeliano, e não é 2-hamiltoniano, a álgebra KG possui em sua decomposição de Wedderburn componentes de matrizes. O anel de inteiros de K, diferente do caso racional, é um $\mathbb{Z}$-módulo livre de posto dois, o que permite a imersão de $\mathbb{Z}^2$ nas $\mathbb{Z}$-ordens das matrizes sobre K que aparecem na decomposição de Wedderburn. Com este fato, mostramos que $\mathcal{U}_1(RG)$ não é hiperbólico para os anéis de inteiros $R \neq \mathbb{Z}$.

Quanto aos 2-grupos Hamiltonianos G, mostramos que apenas os anéis R de extensões imaginárias, que chamamos de anéis imaginários, podem ser tais que $\mathcal{U}_1(RG)$ seja um grupo hiperbólico. Além disso, K_8 é o único grupo Hamiltoniano para o qual isso é possível. Por um resultado de Teoria dos Números, se $K = \mathbb{Q}(\sqrt{d})$, somente para os casos $-d \equiv 7 \pmod 8$, ocorre que $\mathbf{H}(K)$ é uma álgebra de divisão. Isso permite concluir que somente para estes casos o grupo $\mathcal{U}_1(RG)$ pode ser hiperbólico. A demonstração que este grupo é hiperbólico não é imediata. Para tanto, utilizamos uma apropriada ação sobre o espaço hiperbólico de dimensão 3.

Os grupos hiperbólicos, não finitos, Γ estudados em [24], têm a fronteira hiperbólica $\partial\Gamma$ homeomorfa ao conjunto de Cantor, e, portanto, têm infinitos fins. Mostramos que a fronteira hiperbólica de $\mathcal{U}(RK_8)$ é homeomorfa à esfera S^2, um conjunto conexo, portanto, o número de fins é 1, se R é o anel de inteiros de K, $R = I_K$, para $K = \mathbb{Q}(\sqrt{-d})$ e $d \equiv 7 \pmod 8$. De acordo com a bibliografia sobre o assunto, esta é a primeira classe de grupos hiperbólicos construída com essa propriedade, isto é, grupos hiperbólicos infinitos que não são virtualmente livres.

Finalizamos o primeiro capítulo, apresentando um resultado inédito sobre como obter unidades em anéis de divisão. Em 2004, num artigo publicado na revista *Advanced in Mathematics*, Corrales *et alli* determinaram os geradores do grupo de unidades $\mathbf{H}(\mathbb{Z}(\frac{1+\sqrt{-7}}{2}))$. Aqui construímos algumas unidades do anel de inteiros para qualquer álgebra de divisão $\mathbf{H}(\mathbb{Q}(\sqrt{d}))$. Determinamos uma equação de Pell, cuja solução gera unidades que passamos a denominar **unidades de Pell**.

As unidades de Pell são unidades de norma 1. Para as unidades de norma -1, obtemos uma solução que depende da condição de um dado número inteiro n poder ser escrito como a soma de três inteiros quadrados. Este problema tem uma solução clássica dada por um teorema de Gauss, que caracteriza os números inteiros positivos que podem ser obtidos pela soma de três quadrados. Apresentamos uma condição necessária para que a soma entre 1, ou -1, e o quadrado do coeficiente não inteiro de uma unidade em $\mathbf{H}(R)$ esteja nas condições do teorema de Gauss. Unidades que passamos a denominar **unidades de Gauss**.

Para 2-unidades de Pell e, mais geralmente, para as 2-unidades de Gauss, isto é, unidades cuja cardinalidade do suporte é dois, e cuja interseção dos suportes é $\{1\}$, ocorre

que para alguma potência m, o subgrupo gerado pelas potências dessas duas unidades é um grupo livre de posto dois.

Mostramos que 2-unidades de Gauss de norma 1 são exatamente as 2-unidades de Pell.

No capítulo 2 classificamos os semigrupos finitos S, cuja $\mathbb{Q}$-álgebra unitária $\mathbb{Q}S$ é, tal que, para toda $\mathbb{Z}$-ordem Γ de $\mathbb{Q}S$ o grupo de unidades $\mathcal{U}(\Gamma)$ não contém um grupo abeliano livre de posto 2. A esta propriedade referimo-nos por propriedade hiperbólica.

Inicialmente, consideramos o caso geral para as álgebras de dimensão finita não semi-simples que têm a propriedade hiperbólica. Mostramos, nessas condições, que o radical da álgebra é 2-nilpotente. Portanto, como um $\mathbb{Q}$-espaço vetorial, o radical tem dimensão, sobre $\mathbb{Q}$, no máximo 1.

Caso o radical seja não central, é possível decompor a álgebra como soma direta de dois ideais: a sub-álgebra das matrizes triangulares superiores dois por dois sobre $\mathbb{Q}$ e seu anulador.

Obtemos um resultado fundamental para o desenvolvimento do capítulo sobre as álgebras de dimensão finita com a propriedade hiperbólica. Para o caso semi-simples, consideramos a existência ou não de elementos nilpotentes. Para o caso não semi-simples, consideramos a centralidade ou não do radical.

Apresentamos alguns resultados clássicos de semigrupos, e exemplos que ilustram o desenvolvimento da teoria. Nossa principal referência é o livro *The Algebraic Theory of Semigroups*.

Enfatizamos os resultados que estão ligados com a estrutura do semigrupo, como, por exemplo, os fatores principais e os subgrupos maximais. Os semigrupos de matrizes de Rees e as álgebras Munn são definições que relacionam de modo natural a estrutura da álgebra de semigrupos com a estrutura dos semigrupos. Dessa forma, é possível determinar propriedades da álgebra de um certo semigrupo finito S, a partir da álgebra de seus fatores principais. Nesse sentido, os semigrupos cujos fatores principais são isomorfos a grupos tem especial interesse.

A teoria para as álgebras de semigrupo semi-simples foi contruída a partir da teoria de álgebras de grupo semi-simples. O Teorema de Rees, que estabelece a equivalência entre os semigrupos de Rees e os semigrupos completamente 0-simples, permite relacionar as álgebras de semigrupos dos fatores principais às álgebras de Munn. Dessa forma, temos uma estrutura semelhante àquela obtida quando os fatores principais são grupos, porém, neste caso, ao invés de álgebras de grupo, surgem matrizes sobre álgebras de grupo.

No artigo [23] são classificados os semigrupos Σ cujo grupo de unidades $\mathcal{U}(\mathbb{Z}\Sigma)$ é finito. Sendo $\mathbb{Z}\Sigma$ uma $\mathbb{Z}$-ordem da álgebra $\mathbb{Q}\Sigma$, estas álgebras, que são semi-simples, têm a propriedade hiperbólica. Ocorre que existem semigrupos S, com $\mathcal{U}(\mathbb{Z}S)$ infinito, cuja álgebra $\mathbb{Q}S$ satisfaz a propriedade hiperbólica.

Inicialmente, abordamos o caso em que $\mathbb{Q}S$ é semi-simples e livre de elementos nilpotentes. Nessas condições é possível determinar uma classe de semigrupos S, cujo grupo $\mathcal{U}(\mathbb{Z}S)$ é infinito: são os semigrupos inversos, dados pela união disjunta de grupos abelianos de expoente dividindo 4 ou 6, 2-grupos hamiltonianos e somente um dos grupos cíclicos C_5, C_8 e C_{12}.

Para o caso semi-simples com elementos nilpotentes há uma obstrução devido às matrizes. Há duas possibilidades: S não contém elementos nilpotentes, ou o contrário. No primeiro caso, S é a união de grupos, mas os grupos cíclicos do caso anterior dão lugar aos grupos não abelianos S_3, D_4, Q_{12} ou $C_4 \rtimes C_4$, com a mesma condição de aparecer apenas um deles na união. Já no segundo caso, S não é a união de grupos, pois existem elementos nilpotentes. Porém, no lugar dos grupos que não são abelianos, S é a união disjunta de um semigrupo de ordem 5 com os demais grupos.

Para o caso não semi-simples, a obstrução é a existência de um radical não trivial. Inicialmente provamos a existência e unicidade de um elemento j_0 do semigrupo S que é nilpotente. Este elemento é o gerador do radical.

Na primeira seção do Capítulo 2, apresentamos os resultados gerais da ação do radical, no caso não central, sobre a álgebra. Estes resultados permitem classificar os semigrupos cuja $\mathbb{Q}$-álgebra tem a propriedade hiperbólica.

Provamos que para o caso não semi-simples, com radical não central, o semigrupo S contém, ou tem uma cópia isomorfa de, pelo menos, um dos seguintes semigrupos: ou

o semigrupo T_2 das matrizes elementares, e_{ij} triangulares superiores de ordem 2, ou um semigrupo T_2' de ordem 5, cuja álgebra $\mathbb{Q}S \supset \mathbb{Q}T_2' \cong \mathbb{Q} \oplus \mathbb{Q} \oplus \mathbb{Q}T_2$, ou o semigrupo $\hat{T}_2$, de cardinalidade 4, não isomorfo a T_2. Porém, a álgebra $\mathbb{Q}\hat{T}_2$ é isomorfa à álgebra das matrizes triangulares superiores dois por dois sobre os racionais, $T_2(\mathbb{Q})$.

Para a condição não semi-simples com radical central, o semigrupo S é a união disjunta de grupos, os quais são precisamente descritos na condição de $\mathbb{Q}S$ ser semi-simples, com um subsemigrupo nulo que é central.

O terceiro capítulo trata do problema da hiperbolicidade do loop das unidades $\mathcal{U}(\mathbb{Z}L)$ para anéis de RA-loops. Nossa referência principal é o livro *Alternative Loop Rings*. Esse capítulo originou a idéia principal desta tese: classificar estruturas a partir de uma certa propriedade.

Uma propriedade importante de um grupo hiperbólico G é que este não contém um grupo abeliano livre de posto 2, ou seja,

$$\mathbb{Z}^2 \not\hookrightarrow G.$$

Diante dessa propriedade, referimo-nos à hiperbolicidade de um loop através de sua propriedade de conter ou não um grupo abeliano livre de posto 2. Dizemos que um loop L satisfaz a propriedade hiperbólica se $\mathbb{Z}^2 \not\hookrightarrow \mathcal{U}(\mathbb{Z}L)$.

Nesse contexto é natural perguntar-se sobre os loops L cujo loop das unidades $\mathcal{U}(\mathbb{Z}L)$ tem a propriedade hiperbólica. Obtemos tal classificação para os RA-loops.

Os RA-loops foram inicialmente considerados por O. Chein e E.G. Goodaire no artigo *Loops Whose Loop Rings are Alternative*. Neste artigo prova-se que os RA-loops são loops de Moufang, os quais são quase grupos e quase comutativos.

Os RA-loops têm uma estrutura bem definida, ou seja, são determinados por um grupo não abeliano, uma involução e uma indeterminada u, de modo que certas propriedades podem ser conhecidas a partir do grupo ou da involução.

Para a classificação dos RA-loops finitos L cujo loop de unidades $\mathcal{U}(\mathbb{Z}L)$ é hiperbólico,

utilizamos, como ponto de partida, um resultado recente sobre os grupos não abelianos que são hiperbólicos.

A $\mathbb{Q}$-álgebra do RA-loop, determinado por um desses grupos, contém uma cópia isomorfa às matrizes de Zorn, que por sua vez, contém uma $\mathbb{Z}$-ordem Γ, tal que, $\mathbb{Z}^2 \hookrightarrow \mathcal{U}(\Gamma)$, e, portanto, não é hiperbólica. Estes fatos, entre outros que provamos naquele capítulo, reduzem o caso para os 2-grupos hamiltonianos que, pelo teorema de Norton, geram 2-loops Hamiltonianos, cujo loop de unidades é trivial, e, portanto, tem a propriedade hiperbólica.

Para o caso de um RA-loop infinito algumas técnicas utilizadas em [15] permitem reduzir esta condição para um RA-loop finitamente gerado e, este último, para o caso de torção, que é finito, permite a classificação desses RA-loops.

Apresentamos nossos resultados em três capítulos independentes, dentro de certos limites; à exceção do primeiro capítulo, cujas primeiras seções tratam do assunto mais geral da tese que será utilizado ao longo do trabalho.

Preferimos inserir os resultados conhecidos na literatura a simplemente citá-los nas demonstrações. Com isso, esperamos apresentar um texto mais completo.

Capítulo 1

Anéis R de Grupo $\mathcal{U}_1(RG)$ Hiperbólico

1.1 Anéis de grupo

Definição 1.1.1. *O anel de grupo de um grupo G sobre um anel R, com identidade, é o anel RG de todas as somas formais*

$$\sum_{g\in G} \lambda_g g, \quad \lambda_g \in R,$$

tal que,

$$supp(\lambda) = \{g : \lambda_g \neq 0\},$$

o suporte de λ, é finito; com as seguintes operações:

(1) $\sum_{g\in G} \lambda_g g = \sum_{g\in G} \mu_g g \Longleftrightarrow \lambda_g = \mu_g$, *para todo* $g \in G$;

(2) $\sum_{g\in G} \lambda_g g + \sum_{g\in G} \mu_g g = \sum_{g\in G} (\lambda_g + \mu_g) g$;

(3) $(\sum_{g\in G} \lambda_g g)(\sum_{g\in G} \mu_g g) = \sum_{g\in G} \nu_g g$, *em que* $\nu_g = \sum_{xy=g} \lambda_x \mu_y$.

Definição 1.1.2. *Um elemento r de um anel R é denominado uma unidade se existe um elemento inverso s, tal que, $rs = 1 = sr$. O conjunto de todas as unidades de R é denominado o grupo das unidades de R, $\mathcal{U}(R)$.*

Seja RG um anel de grupo. Definimos o aumento de RG, pela aplicação $\epsilon : RG \to R$, que a cada elemento $RG \ni \lambda = \sum_{g\in G} \lambda_g g$ associa $\epsilon(\lambda) = \sum_{g\in G} \lambda_g \in R$.

Diz-se que o conjunto $\mathcal{U}_1 = \{u \in \mathcal{U}(RG) : \epsilon(u) = 1\}$ é o grupo de unidades de aumento 1. Se $\mathcal{U}(RG) = \mathcal{U}(R)G$, dizemos que o grupo $\mathcal{U}(RG)$ é trivial.

Obviamente $\mathcal{U}(RG) \cong \mathcal{U}(R) \times \mathcal{U}_1(RG)$.

Definição 1.1.3. *Seja RG um anel de grupo. Uma unidade $u \in \mathcal{U}(RG)$ é denominada unidade de torção se existe um inteiro n, não nulo, tal que, $u^n = 1$.*

Teorema 1.1.4 (Teorema de Higman)**.** *Para um grupo finito G, $\mathcal{U}(\mathbb{Z}G) = \pm G$ se, e somente se, G é um grupo abeliano de expoente que divide 4 ou 6, ou $G = E \times K_8$, um 2-grupo Hamiltoniano, em que K_8 é o grupo dos quatérnios de ordem 8, e E é um 2-grupo abeliano elementar.*

Seja G um grupo. Poucas das propriedades de G são preservadas pelo anel de grupo RG ou pelo grupo de unidades $\mathcal{U}(RG)$. Por exemplo, não é verdade que se G é um grupo solúvel, então $\mathcal{U}(RG)$ seja solúvel, ver [18]; de igual maneira, a finitude de G não implica a de $\mathcal{U}(RG)$. Sabemos que se $\mathcal{U}(\mathbb{Z}G)$ é um grupo solúvel, então G é um grupo abeliano ou um 2-grupo Hamiltoniano. Uma demonstração elementar pode ser encontrada em [13]. Também são conhecidos os grupos G, tal que, $\mathcal{U}(\mathbb{Z}G)$ é trivial.

Um tipo de questão são os problemas de classificação de grupos G cujo grupo de unidades $\mathcal{U}(\mathbb{Z}G)$ tenha uma determinada propriedade.

Nesse sentido, dado um grupo G, podemos, então, colocar o seguinte problema: determinar os anéis R cujo grupo de unidades $\mathcal{U}(RG)$ satisfaça uma certa propriedade $\mathcal{P}$. Isso foi feito em [19], com R sendo o anel de inteiros de extensões quadráticas racionais, e com $\mathcal{P}$ sendo a propriedade que $\mathcal{U}(RG)$ seja trivial. Nesse caso os grupos G fixados são aqueles classificados no Teorema de Higman.

Este primeiro capítulo trata deste tipo de problema, qual seja: classificar os anéis R, quando R é o anel de inteiros de uma extensão quadrática racional cujo grupo de unidades

$\mathcal{U}(RG)$ satisfaz uma propriedade $\mathcal{P}$ para G fixado. A propriedade que iremos estudar é a hiperbolicidade de um grupo. A seguir, definimos um grupo hiperbólico.

1.2 Grupos hiperbólicos

Definição 1.2.1. *Seja Γ um grupo finitamente gerado, e, S um sistema de geradores finito, simétrico , isto é, $S = S^{-1}$, e que não contém o elemento neutro de G. Se $\gamma \in \Gamma$, denotamos por $l_S(\gamma)$, que chamamos o comprimento de γ relativo a S, o menor número de geradores de S, necessários para escrever o elemento γ. Se $\gamma_1, \gamma_2 \in \Gamma, d_S(\gamma_1, \gamma_2) := l_S(\gamma_1^{-1}\gamma_2)$ é a distância entre γ_1 e γ_2.*

Nessas condições, podemos associar a Γ um espaço métrico, pois a distância acima definida é uma métrica.

Definição 1.2.2 (Grafo de Cayley $\mathcal{G}(\Gamma, S)$)**.** *O conjunto de vértices de $\mathcal{G}(\Gamma, S)$ é o grupo Γ, e para cada $s \in S, \gamma \in \Gamma$ existe uma aresta do vértice γ ao vértice γs. Tornamos $\mathcal{G}(\Gamma, S)$ um espaço métrico, considerando cada aresta isométrica ao intervalo unitário, e a métrica de caminho induzida.*

Os Espaços Métricos Hiperbólicos foram inicialmente estudados por Gromov [17].

Definição 1.2.3 (Produto de Gromov)**.** *Seja $\{X, d\}$ um espaço métrico, e, $x \in X$. O produto de Gromov de $y, z \in X$, relativamente a x, é definido por*

$$(y \cdot z)_x = \frac{1}{2}(d(y, x) + d(z, x) - d(y, z)).$$

Definição 1.2.4 (Espaço métrico δ-hiperbólico)**.** *Seja $\delta > 0$. Um espaço métrico X é δ-hiperbólico se, para qualquer $w, x, y, z \in X$,*

$$(x.y)_w \geq min\{(x.z)_w, (y.z)_w\} - \delta.$$

Definição 1.2.5. *Um espaço métrico (X, d) é um espaço geodésico se todos $x, y \in X$ podem ser unidos por uma geodésica, isto é, uma aplicação $c : [0, D] \longrightarrow X$, sendo $[0, D]$ um intervalo real, tal que, $c(0) = x; c(D) = y$ e para todo $t, t' \in [0, D]$, $d(c(t), c(t')) = |t - t'|$.*

Geometricamente, um espaço métrico geodésico $\{X, d\}$ é hiperbólico se existe $\delta \geq 0$, tal que, para cada $x, y, z \in X$, que são os vértices de um triângulo geodésico, a união das δ-vizinhanças, de quaisquer dois lados do triângulo, contém o terceiro, isto é,

$$[x_1, x_3] \subset \bigcup_{i \in \{1,2\}} V_\delta([x_i, x_{i+1}]), x_i \in \{x, y, z\}, 1 \leq i \leq 3,$$

em que $[x_i, x_{i+1}]$ denota o lado do triângulo definido por estes dois vértices.

Definição 1.2.6 (Grupo Hiperbólico)**.** *Um grupo Γ, finitamente gerado, é hiperbólico se, para algum sistema de geradores S de Γ, o Grafo de Cayley $\mathcal{G}(\Gamma, S)$ é um espaço métrico δ-hiperbólico, para algum $\delta \geq 0$.*

Definição 1.2.7 (Fronteira hiperbólica ∂X)**.** *Seja X um espaço métrico. Uma seqüência $x_i \in X, i = 1, 2, \ldots,$ é dita convergente no infinito se*

$$(x_i \cdot y_j) \longrightarrow \infty \text{ para } i, j \longrightarrow \infty.$$

Se X é hiperbólico, então a igualdade

$$\lim_{i,j \longrightarrow \infty} inf(x_i \cdot y_j) = \infty$$

define uma relação de equivalência sobre o conjunto de seqüências em X que convergem no infinito. A fronteira hiperbólica ∂X, de um espaço hiperbólico, é o conjunto das classes de equivalência das seqüências em X que convergem no infinito. Defini-se por número de fins a cardinalidade de ∂X que é o número de componentes conexas de ∂X

Essa definição é devida a Gromov. Ocorre que a definição de número de fins pode ser estendida para espaços topológicos, o que permite, portanto, definir o número de fins para grupos, a partir de seu grafo de Cayley. Tal definição é devida a Freudenthal.

Lembrando que uma aplicação $f : X \longrightarrow Y$ entre espaços topológicos é *própria* se $f^{-1}(C) \subseteq X$ é compacto, para cada subconjunto compacto $C \subseteq Y$.

Definição 1.2.8. *Seja X um espaço topológico. Um raio em X é uma aplicação*

$$r : [0, \infty[\longrightarrow X.$$

Sejam r_1, r_2 dois raios próprios. Diz-se que r_1, r_2 convergem para o mesmo fim se a cada compacto $C \subset X$ existe $N \in \mathbb{N}$, tal que, $r_1([N, \infty[)$ e $r_1([N, \infty[)$ estão contidos na mesma componente de caminho de $X \setminus C$. Isto define uma relação de equivalência sobre os raios próprios contínuos; a classe de equivalência de r é denotada por $fim(r)$, e $fins(X)$ denota o conjunto de classes de equivalência. A cardinalidade $|fins(X)|$ é o número de fins de X.

Definição 1.2.9 (Fins de um Grupo)**.** *Seja Γ um grupo finitamente gerado, S um sistema de geradores finito, e seja $\mathcal{G} = \mathcal{G}(\Gamma, S)$ seu grafo de Cayley. Definimos $Fins(\Gamma) := Fins(\mathcal{G})$.*

Denotamos por $\mathbb{Z}^2 \doteq \mathbb{Z} \times \mathbb{Z}$ um grupo abeliano livre de posto dois.

Um resultado fundamental é:

Teorema 1.2.10 ([5], Corolário $III.\Gamma.3.10(2)$)**.** *Se Γ é um grupo hiperbólico, então $\mathbb{Z}^2 \not\hookrightarrow \Gamma$.*

Corolário 1.2.11. *Se G é um grupo abeliano livre de posto maior que um, então G não é um grupo hiperbólico.*

Teorema 1.2.12 ([5], Proposição $III.\Gamma.2.22$)**.** *Se um grupo hiperbólico é infinito, então ele contém um elemento de ordem infinita.*

Corolário 1.2.13. *Seja Γ um grupo hiperbólico. Se G é um subgrupo de torção de Γ, então G é finito.*

Definição 1.2.14. *Seja $\mathbb{H}$ o espaço hiperbólico tri-dimensional, e seja $Iso(\mathbb{H})$ seu grupo de isometrias. Denomina-se o grupo $\Gamma < Iso(\mathbb{H})$ um grupo descontínuo se, para todo $P \in \mathbb{H}$ e toda seqüência $(T_n)_{n\leq 1}$ de elementos distintos de Γ, a seqüência $(T_nP)_{n\leq 1}$ não tem ponto de acumulação em $\mathbb{H}$. Neste caso, também, diz-se que Γ age descontinuamente sobre $\mathbb{H}$. Seja $PSL(2,\mathbb{C})$ o grupo de matrizes dois por dois sobre $\mathbb{C}$ cujo determinante é 1, módulo seu centro $\{-I, I\}$. Um subgrupo $\Gamma < PSL(2,\mathbb{C})$ é discreto se sua imagem inversa em $SL(2,\mathbb{C}) \subset \mathbb{C}^4$ é discreta na topologia do espaço vetorial.*

Definição 1.2.15. *Seja $\Gamma < Iso(\mathbb{H})$ um subgrupo descontínuo, Γ é co-compacto se tem um domínio fundamental compacto.*

Recentemente, foram classificados os grupos finitos cujo grupo de unidades de um anel de grupo integral, $\mathcal{U}(\mathbb{Z}G)$, é um grupo hiperbólico.

Teorema 1.2.16 ([24], Teorema 3)**.** *Se um grupo de torção G imerge em um grupo de unidade hiperbólico, então G deve ser finito e isomorfo a um dos seguintes grupos:*

(1) *C_5, C_8, C_{12}, um grupo Abeliano de expoente que divide 4 ou 6;*

(2) *um 2-grupo hamiltoniano;*

(3) *$S_3, D_4, Q_{12}, C_4 \rtimes C_4$.*

Reciprocamente, o grupo de unidades do anel de grupo inteiro de todos os grupos listados acima é hiperbólico.

Neste capítulo, apresentamos uma classificação dos anéis de inteiros de uma extensão quadrática racional K, que denotamos por R, cujo grupo $\mathcal{U}_1(RG)$ é um grupo hiperbólico. Ocorre que $\mathcal{U}(\mathbb{Z}G) \hookrightarrow \mathcal{U}(RG)$. Portanto, a partir dos grupos obtidos em [24] é que classificamos estes anéis.

Lembramos que se $\theta \in \mathbb{Z}G$ é um elemento nilpotente não nulo, então $u = 1 + \theta$ é uma unidade de ordem infinita de $\mathcal{U}(\mathbb{Z}G)$.

Lema 1.2.17. *Seja A um anel cujo grupo aditivo é livre de torção, e sejam $\theta_1, \theta_2 \in A$, elementos nilpotentes de índice 2, que comutam, tal que, $\{\theta_1, \theta_2\}$ seja $\mathbb{Z}$-LI. Então $\mathbb{Z}^2$ está imerso em $\mathcal{U}(A)$.*

Demonstração.

Para $u = 1+\theta_1$ e $v = 1+\theta_2$ temos que $u, v \in \mathcal{U}(A)$ são unidades de ordem infinita. Se supomos que $1 \neq w \in \langle u\rangle \cap \langle v\rangle$, então existem $i, j \in \mathbb{Z}^*$, tal que, $u^i = w = v^j$. Portanto, $u^i = 1 + i\theta_1 = 1 + j\theta_2 = v^j$. Daí, $i\theta_1 - j\theta_2 = 0$, e, logo, $\{\theta_1, \theta_2\}$ é $\mathbb{Z}$-LD, um absurdo. Assim $\langle u\rangle \cap \langle v\rangle = 1$, $uv = vu$ e $o(u) = o(v) = \infty$ implicam que $\langle u, v\rangle \cong \mathbb{Z}^2 \hookrightarrow \mathcal{U}(A)$. □

Definição 1.2.18. *Seja K um corpo de números algébricos, e, R seu anel de inteiros. Para $a, b \in K$, denotamos por $\mathbf{H}(K) = (\frac{a,b}{K})$ a álgebra de quatérnios generalizada, induzida por a, b, i.e., $\mathbf{H}(K)$ é a K-álgebra dada por:*

$$\mathbf{H}(K) = K[i, j : i^2 = a, j^2 = b, ji = -ij =: k].$$

Temos que o conjunto $\{1, i, j, k\}$ é uma K-base de $\mathbf{H}(K)$. Dizemos que $\mathbf{H}(K)$ é uma álgebra de quatérnios totalmente definida se K é um corpo numérico totalmente real, e a e b são totalmente positivos.

Se $a, b \in R$, então o conjunto

$$\mathbf{H}(R) = R[i, j : i^2 = a, j^2 = b, -ji = ij =: k]$$

é a R-álgebra que consiste das combinações R-lineares de $\{1, i, j, k\}$. A aplicação

$$\begin{array}{rccc} \eta: & \mathbf{H}(K) & \longrightarrow & K \\ & x = x_1 + x_i i + x_j j + x_k k & \mapsto & x_1^2 - a x_i^2 - b x_j^2 + ab x_k^2 \end{array}$$

é denominada norma.

Para $a = b = -1$, $\mathbf{H}(K)$ denota a álgebra dos quatérnios.

1.3 Classificação dos anéis R com $\mathcal{U}_1(RG)$ hiperbólico

Seja $K = \mathbb{Q}\sqrt{d}$, com $d \in \mathbb{Z} \setminus \{0, 1\}$ livre de quadrados. Neste capítulo, vamos abordar o problema da hiperbolicidade de anéis de grupo sobre o anel de inteiros algébricos, I_K, de

uma extensão quadrática do corpo dos racionais, isto é, se o grupo de unidades do anel de grupo sobre I_k é um grupo hiperbólico . Denotamos por $R \doteq I_K$ e C_n o grupo cíclico de ordem $n \in \mathbb{Z}^+$. Se G é um grupo abeliano, denotamos $\rho(\mathcal{U}(RG))$ o posto livre de $\mathcal{U}(RG)$.

Definição 1.3.1. *Seja G um grupo. Diz-se que dois subgrupos $U_1, U_2 < G$ são comensuráveis se os índices $[U_1 : U_1 \cap U_2]$ e $[U_2 : U_1 \cap U_2]$ são ambos finitos.*

Se P é um sub-anel de $\mathbb{Q}G$, que contém $\mathbb{Z}G$, e é finitamente gerado, então $[\mathcal{U}(P) : \mathcal{U}(\mathbb{Z}G)] < \infty$. Neste caso, estes grupos são comensuráveis. Em geral, dois grupos são comensuráveis se eles têm subgrupos isomorfos de índice finito, isto é, se G e H são comensuráveis, então existem subgrupos $G_1 < G$ e $H_1 < H$, isomorfos $G_1 \cong H_1$, tal que, $[G : G_1] < \infty$ e $[H : H_1] < \infty$.

A partir da classificação dos grupos cujo grupo de unidades $\mathcal{U}_1(\mathbb{Z}G)$ é hiperbólico [24], estendemos tal resultado, classificando os anéis R, e, portanto, a extensão K, cujo grupo de unidades $\mathcal{U}_1(RG)$ é hiperbólico.

Ao longo do capítulo, ϵ denota o invertível fundamental ou, como na proposição seguinte, um elemento invertível, isto é, $\epsilon \in \mathcal{U}(R)$. Lembramos que o anel de inteiros R é um $\mathbb{Z}$-módulo livre de posto 2, isto é, R admite uma base integral de cardinalidade 2.

Se $d \equiv 2 \pmod 4$ ou $d \equiv 3 \pmod 4$ (respectivamente $d \equiv 1 \pmod 4$), então $\{1, \sqrt{d}\}$, (respectivamente $\{1, \frac{1+\sqrt{d}}{2}\}$) é uma base integral de R. Nessas condições, $\epsilon = x + y\sqrt{d}$, (respectivamente $\epsilon = x + y(\frac{1+\sqrt{d}}{2})$) se $d \equiv i \pmod 4, i = 2, 3$, (respectivamente $d \equiv 1 \pmod 4$).

Uma propriedade importante do invertível fundamental é que, a norma $\eta(\epsilon) = \epsilon\overline{\epsilon} = \pm 1$, sendo os coeficientes $x, y \in \mathbb{Z}$, os menores inteiros positivos com essa propriedade. A equação correspondente, quando a norma é 1, é a **Equação de Pell**:

$$x^2 - y^2 d = 1.$$

Uma propriedade importante, da equação de Pell, é a existência de sua solução. Na última seção deste capítulo construímos unidades, para anéis de divisão, a partir dessa equação.

Proposição 1.3.2. *Seja $d \equiv 1 \pmod 4$. Se $\epsilon = x + y(\frac{1+\sqrt{d}}{2})$ é um invertível, então as seguintes afirmações são verdadeiras:*

(1) x e y não são ambos pares;

(2) $8 \nmid (d+3)$ se, e somente se, $x \equiv 1 \pmod 2$ e $y \equiv 0 \pmod 2$.

(3) Se $8 \mid d-1$, então $x \equiv 1 \pmod 2$ e $y \equiv 0 \pmod 2$;

Demonstração.

Sendo $\epsilon = x+y(\frac{1+\sqrt{d}}{2}) = \frac{2x+y}{2} + y\frac{\sqrt{d}}{2}$, um invertível, obtemos $(2x+y)^2 - y^2d = \pm 4$. Se x, y são ambos pares, então $x = 2m; y = 2n$, logo, $(2m+n)^2 - n^2d = \pm 1$. Consideramos $z = m + n\frac{1+\sqrt{d}}{2}$, de modo que $z\overline{z} = \frac{(2m+n)^2 - n^2d}{4} = \pm\frac{1}{4} \notin R$. Logo, isso é um absurdo.

A congruência $d \equiv 1 \pmod 4$ implica que se $d \equiv a \pmod 8$, então $a \in \{1, 5\}$. Se $d \equiv 5 \pmod 8$, então $8 \mid (d+3)$. Da relação $(2x+y)^2 - y^2d = \pm 4$, obtemos que $4x(x+y) - y^2(d-1) = \pm 4$. Se $8 \nmid d+3$, então, pela condição anterior, $d \equiv 1 \pmod 8$. Logo, $4x(x+y) - y^2(d-1) \equiv 4x(x+y) \pmod 8$ e, portanto, $4x(x+y) \equiv \pm 4 \pmod 8$. Segue-se que $8 \nmid 4x(x+y)$ e, conseqüentemente, $x \equiv 1 \pmod 2$ e $y \equiv 0 \pmod 2$. A recíproca é imediata!

Se $8 \mid d-1$, então $d - 1 = 8k$. Sendo ϵ invertível, obtemos a equação $4x(x+y) - y^2(d-1) = \pm 4$, substituindo pelo valor de $d - 1 = 8k$, e tomando-se a congruência módulo 8, obtemos: $(4x(x+y)) \equiv \pm 4 \pmod 8$. Como no caso anterior, $x \equiv 1 \pmod 2$, e $y \equiv 0 \pmod 2$. □

Nosso principal resultado, neste capítulo, é o seguinte teorema:

Teorema 1.3.3. *Seja R o anel de inteiros de uma extensão quadrática racional $K = \mathbb{Q}(\sqrt{d})$, e seja $d \in \mathbb{Z} \setminus \{1\}$ livre de quadrados. O grupo de unidades $\mathcal{U}_1(RG)$ é hiperbólico para os seguintes casos:*

(1) $G \in \{C_2, C_3\}$, e d é qualquer.

(2) G é um grupo abeliano de expoente dividindo n para:
$n = 2$ e $d < 0$; ou $n = 6$ e $d = -3$; ou $n = 4$ e $d = -1$.

(3) $G = C_4$, e $d < 0$.

(4) $G = C_8$ *e* $d = -1$.

(5) $G = K_8$, *e* $d < 0$, $-d \equiv 7 \pmod 8$.

Reciprocamente, em cada caso, o grupo $\mathcal{U}_1(RG)$ *é hiperbólico.*

1.4 G como 2-grupo Abeliano elementar

Em [20], Proposição 1, é estabelecido em quais condições o grupo $\mathcal{U}_1(RC_2)$ é não-trivial. Apresentamos a seguir uma demonstração elementar para este resultado, utilizando a representação regular de C_2.

Proposição 1.4.1. *Seja* R *um anel comutativo com unidade. O grupo* $\mathcal{U}_1(RC_2)$ *é não-trivial se, e somente se, existe* $a \in R \setminus \{0,1\}$, *tal que,* $2a-1 \in \mathcal{U}(R)$. *Além disso, se* $2a-1 = e \in \mathcal{U}(R)$, *então* $\frac{1+e}{2} + (\frac{1-e}{2})g$ *é uma unidade do grupo* $\mathcal{U}_1(RC_2)$.

Demonstração.

Seja $C_2 = \langle g \rangle$, e suponha $\mathcal{U}_1(RC_2)$ não-trivial. Seja $u \in \mathcal{U}_1(RC_2), u = a + (1-a)g, a \notin \{0,1\}$. A representação regular de u é dada pela matriz $[u] = \begin{bmatrix} a & 1-a \\ 1-a & a \end{bmatrix}$. Sendo u uma unidade, temos que $det(u) = 2a-1 \in \mathcal{U}(R)$. Reciprocamente, seja $a \in R \setminus \{0,1\}$, tal que, $e = 2a-1 \in \mathcal{U}(R)$. Afirmamos que $u = \frac{1+e}{2} + \frac{1-e}{2}g$ é um elemento de R. Com efeito, $\frac{e+1}{2} = a \in R$ e $\frac{e-1}{2} = 1-a \in R$. Sendo $e = 2a-1$ uma unidade, temos que $e^{-1} \in R$. Além do mais, $\frac{1+e^{-1}}{2} + \frac{1-e^{-1}}{2}g \in RG$. De fato, $1 + e^{-1} = e^{-1}e + e^{-1} = e^{-1}(e+1) = e^{-1}(2a)$; logo, $\frac{1+e^{-1}}{2} = e^{-1}a \in R$, e, analogamente, $\frac{1-e^{-1}}{2} \in R$. O elemento $\frac{1+e^{-1}}{2} + (\frac{1-e^{-1}}{2})g$ é o inverso de u, pois $u(\frac{1+e^{-1}}{2} + (\frac{1-e^{-1}}{2})g) = 1$; logo, $u \in U_1(RC_2)$. □

Como conseqüência da proposição anterior, se $K = \mathbb{Q}(\sqrt{d})$, então $\mathcal{U}_1(RC_2)$ é trivial se, e somente se, K é uma extensão imaginária, ou $K = \mathbb{Q}$ ([19], Teorema 2.2).

Inicialmente, provamos que se $d > 0$, e ϵ é o invertível fundamental de R, então existe $n \in \mathbb{N}$, e, $a \in R$, tal que, $\epsilon^n = 2a - 1$ e, portanto, de acordo com o teorema anterior, $\mathcal{U}(RC_2)$ é não-trivial.

Lema 1.4.2. *Seja K uma extensão quadrática real. Existe $a \in R$, e, $n \in \{1,2,3\}$, tal que, a equação $2a-1=\epsilon^n$ admite solução em R. Conseqüentemente, $\mathcal{U}_1(RC_2)$ não é trivial.*

Demonstração.

Seja $K=\mathbb{Q}(\sqrt{d})$. Inicialmente consideremos os casos $d \equiv i \pmod 4, i \in \{2,3\}$. Nessa condição, $\{1,\sqrt{d}\}$ é base integral de R. Se $\epsilon = x+y\sqrt{d}$ é o invertível fundamental, então

$$x^2-dy^2=\pm 1. \quad (\star)$$

Afirmamos que existe $a \in R$, tal que,

$$2a-1=\begin{cases} \epsilon & \text{se } 2 \mid y \\ \epsilon^2, & \text{caso contrário} \end{cases}.$$

De fato, se $d \equiv 2 \pmod 4$, então $d \equiv 0 \pmod 2$, por $(\star)$, $x \equiv 1 \pmod 2$. Portanto, $x+1 \equiv 0 \pmod 2$. Se y é par, então $a := \frac{x+1}{2}+\frac{y}{2}\sqrt{d} \in R$; se y é ímpar, consideramos $\epsilon^2=(x^2+dy^2)+(2xy)\sqrt{d}$, sendo x ímpar, $x^2+dy^2 \equiv 1 \pmod 2$, daí $a := \frac{\epsilon^2+1}{2} \in R$.

Se $d \equiv 3 \pmod 4$, então $d \equiv 1 \pmod 2$. Logo, por $(\star)$, $x^2-y^2 \equiv 1 \pmod 2$, e, portanto, x e y não têm a mesma paridade. Desse modo, se $x \equiv 1 \pmod 2$, então $y \equiv 0 \pmod 2$; portanto, $a := \frac{x+1}{2}+\frac{y}{2}\sqrt{d} \in R$. Se $x \equiv 0 \pmod 2$, então y é ímpar e, sendo d ímpar, $x^2+dy^2 \equiv 1 \pmod 2$, portanto, $a := \frac{\epsilon^2+1}{2} \in R$.

Se $d \equiv 1 \pmod 4$, então $\{1,\frac{1+\sqrt{d}}{2}\}$ é base integral de R. Seja $\epsilon = x+y(\frac{1+\sqrt{d}}{2}) = \frac{2x+y}{2}+\frac{y\sqrt{d}}{2}$. Pela proposição 1.3.2, x e y não são ambos números pares. Se $x \equiv 1 \pmod 2$ e $y \equiv 0 \pmod 2$, então $a := \frac{x+1}{2}+\frac{y}{2}(\frac{1+\sqrt{d}}{2}) = \frac{\epsilon+1}{2} \in R$ é, tal que, $2a-1=\epsilon$.

Se $y \equiv 1 \pmod 2$, então, para a equação $2a-1=\epsilon^2$, não existe solução em R, pois $\epsilon^2 = \frac{4x^2+y^2(d-1)}{4}+y(2x+y)(\frac{1+\sqrt{d}}{2})$ e $2 \nmid y(2x+y)$. Nesse caso, afirmamos que $2a-1=\epsilon^3$ tem solução em R. De fato, utilizando que $4\epsilon^2=(4x(x+y)+y^2(d+1))+2y(2x+y)\sqrt{d}$, e $2\epsilon=(2x+y)+y\sqrt{d}$, obtemos

$$8\epsilon^3=[(2x+y)(4x(x+y)+y^2(3d+1))]+[y(12x(x+y)+y^2(d+3))]\sqrt{d}$$

que, convenientemente representado, fica:

$$8\epsilon^3=[8x(x^2-y^2)+2xy^2(3d+1)+2y^3(d-1)]+[y(12x(x+y)+y^2(d+3))](1+\sqrt{d}) =: r+s(1+\sqrt{d}).$$

Obviamente, $\epsilon^3=\frac{r}{8}+\frac{s}{4}(\frac{1+\sqrt{d}}{2}) \in R$, pois $\epsilon \in R$.

Afirmamos que $\frac{r}{8}$ é um inteiro ímpar. Com efeito, sendo $d \equiv 1 \pmod 4$, temos que $3d+1 \equiv 4 \pmod 4$, e $4 \mid 3d+1$. Se $x \equiv 0 \pmod 2$, então $16 \mid 8x(x^2-y^2)+2xy^2(3d+1)$, porém $16 \nmid 2y^3(d-1)$, uma vez que y é ímpar e, pela proposicão 1.3.2, $8 \nmid d-1$. Logo, o inteiro $\frac{r}{8}$ é ímpar. Como $y \equiv 1 \pmod 2$, pela proposição 1.3.2, $8 \mid d+3$; portanto, o coeficiente $s = y(12x(x+y)+y^2(d+3))$ é um múltiplo de 8; logo, $\frac{s}{4}$ é um inteiro par, e $a := \frac{\frac{r}{8}+1}{2} + \frac{\frac{s}{4}}{2}\left(\frac{1+\sqrt{d}}{2}\right) = \frac{\epsilon^3+1}{2} \in R$, ou seja, $2a-1 = \epsilon^3$. Se ocorre que $x \equiv 1 \pmod 2$, como $\frac{s}{4}$ é um inteiro par, que é coeficiente de um invertível, pela proposição 1.3.2, o outro coeficiente $\frac{r}{8}$ é ímpar, portanto, o mesmo caso anterior.

Pelo Teorema de Dirichlet, se R é o anel de inteiros de uma extensão real, então $\mathcal{U}(R) \cong \{-1,1\} \times \langle \epsilon \rangle$. Assim, existe $a \in R \setminus \{0,1\}$, tal que, $2a-1 \in \mathcal{U}(R)$. Logo, pela proposição 1.4.1, $\mathcal{U}_1(RC_2)$ é não-trivial. □

Estamos em condições de enunciar nosso primeiro resultado relativo à hiperbolicidade de $\mathcal{U}_1(RC_2)$.

Teorema 1.4.3. *O grupo de unidades $\mathcal{U}_1(RC_2)$ é hiperbólico. Em particular, se R é o anel de inteiros de uma extensão real, $\mathcal{U}(R) = \langle \epsilon \rangle$, e $C_2 = \langle g \rangle$, então existe $n \in \{1,2,3\}$, tal que, $\mathcal{U}_1(RC_2) \cong \langle g \rangle \times \langle \frac{1+\epsilon^n}{2} + (\frac{1-\epsilon^n}{2})g \rangle \cong C_2 \times \mathbb{Z}$.*

Demonstração.

Se R é imaginário, então, pela Proposição 1.4.1, $\mathcal{U}_1(RC_2)$ é trivial. Com efeito, se $K = \mathbb{Q}(\sqrt{-1})$, então $\mathcal{U}(R) = \{-1,-i,i,1\}$ e, nas condições da Proposição 1.4.1, $a \in R$, $2a-1 \in \mathcal{U}(R)$ somente se $a \in \{0,1\}$. Analogamente, se $K = \mathbb{Q}(\sqrt{-3})$. Para as demais extensões imaginárias, $\mathcal{U}(R) = \{-1,1\}$ e ocorre o mesmo fato. Logo, $\mathcal{U}_1(RC_2)$ é finito, portanto, hiperbólico.

Seja $K = \mathbb{Q}(\sqrt{d})$, com $d \in \mathbb{Z}, d > 1$. Obviamente, $C_2 \subset \mathcal{U}_1(RC_2)$. Pelo lema anterior, $\mathcal{U}_1(RC_2)$ é não-trivial, e existe $a \in R$, e, $n \in \{1,2,3\}$, tal que, $2a-1 = \epsilon^n$. Pela Proposição 1.4.1, $u = \frac{1+\epsilon^n}{2} + (\frac{1-\epsilon^n}{2})g$ é uma unidade de $\mathcal{U}_1(RC_2)$. Sendo ϵ de ordem infinita, e $u^k = \frac{1+\epsilon^{nk}}{2} + \frac{1-\epsilon^{nk}}{2}g$, temos que $\langle u \rangle \cong \mathbb{Z}$.

Se tomarmos para n a menor potência positiva possível, tal que, $u \in \mathcal{U}_1(RC_2)$, afirmamos que $\mathcal{U}_1(RC_2) \cong C_2 \times \langle u \rangle$. Com efeito, seja $v \in \mathcal{U}_1(RC_2)$ uma unidade não trivial. Repetindo-se os argumentos anteriores, existe um inteiro positivo $m \geq n$, tal que, $v = \frac{1+\epsilon^m}{2} + (\frac{1-\epsilon^m}{2})g$. Afirmamos que $v = u^q$. De fato, $m = qn + r$; então

$v^m = (\frac{1+\epsilon^m}{2} + (\frac{1-\epsilon^m}{2})g)^q((\frac{1+\epsilon^r}{2} + (\frac{1-\epsilon^r}{2})g)$ e, logo, $(\frac{1+\epsilon^r}{2} + (\frac{1-\epsilon^r}{2})g) \in \mathcal{U}_1(RC_2)$. Segue que a equação $2a-1 = \epsilon^r$ tem solução em $\mathcal{U}(R)$, e $r < n$, o que contraria a minimalidade de n. Portanto, $m = qn$ e $v = u^q \in \langle u \rangle$. Concluímos, então que

$$\mathcal{U}_1(RC_2) \cong C_2 \times \mathbb{Z} \cong \langle g \rangle \times \langle \frac{1+\epsilon^n}{2} + (\frac{1-\epsilon^n}{2})g \rangle$$

é um grupo virtualmente cíclico, logo, é hiperbólico. □

Corolário 1.4.4. *Seja G um 2-grupo abeliano elementar que não é cíclico. O grupo $\mathcal{U}_1(RG)$ é hiperbólico se, e somente se, R é imaginário.*

Demonstração.

Suponha que R é real. Sendo G não cíclico, temos que existem $g, h \in G, g \neq h, o(g) = o(h) = 2$. Pelo teorema, $\mathcal{U}_1(R\langle g \rangle) \cong C_2 \times \mathbb{Z} \cong \mathcal{U}_1(R\langle h \rangle)$. Sendo $\langle g \rangle \cap \langle h \rangle = \{1\}$, então $\mathcal{U}_1(R\langle g \rangle) \cap \mathcal{U}_1(R\langle h \rangle) = \{1\}$; logo, $\mathcal{U}_1(RG)$ contém um grupo abeliano livre de posto 2. Portanto, não é hiperbólico. Reciprocamente, se R é imaginário, por indução sobre a ordem de G, concluímos que $\mathcal{U}_1(RG)$ é trivial, portanto, hiperbólico, porque G é um grupo finito. □

Estamos interessados em determinar o posto $\rho(\mathcal{U}_1(RG))$. Sendo $\mathcal{U}(RG) \cong \mathcal{U}(R) \times \mathcal{U}_1(RG)$, se G é abeliano, então $\rho(\mathcal{U}_1(RG)) = \rho(\mathcal{U}(RG)) - \rho(\mathcal{U}(R))$. Sempre ocorre que $\rho(\mathcal{U}(\mathbb{Z}G)) = \rho(\mathcal{U}_1(\mathbb{Z}G))$, pois $\mathcal{U}(\mathbb{Z}) = \{-1, 1\}$ tem posto livre nulo. E ocorre o mesmo para as extensões imaginárias. Porém, se a extensão é real, o Teorema das unidades de Dirichlet garante que $\rho(\mathcal{U}(R)) = 1$, portanto, $\rho(\mathcal{U}_1(RG)) = \rho(\mathcal{U}(RG)) - 1$.

Os exemplos a seguir mostram que, de fato, a equação $2a-1 \in \mathcal{U}(R)$ apresenta soluções dos três tipos:

tipo 1 ou $2a - 1 = \epsilon$;

tipo 2 ou $2a - 1 = \epsilon^2$, e $2a - 1 = \epsilon$ não admite solução;

tipo 3 ou $2a - 1 = \epsilon^3$, e não há solução para a potências 1 e 2 de ϵ.

Exemplo 1.4.5. *Finalizamos a seção, mostrando que no Teorema 1.4.3, de fato, n pode assumir os três valores. Seja $C_2 = R\langle g\rangle$, o último exemplo mostra, também, que $\rho(\mathcal{U}(RC_2)) > \rho(\mathcal{U}_1(RC_2))$.*

tipo 1 *Seja $d = 73$, $73 \equiv 1 \pmod 4$; $\{1, \frac{1+\sqrt{73}}{2}\}$ é uma base integral; $\epsilon = 1068 + 125\sqrt{73}$ é o invertível fundamental. A equação $2a - 1 = 1068 + 125\sqrt{73}$ tem solução em R, sendo $a = 472 + 125(\frac{1+\sqrt{73}}{2})$*

tipo 2 *Seja $d = 7$, $7 \equiv 3 \pmod 4$; $\{1, \sqrt{7}\}$ é uma base integral de R, e $\epsilon = 8 + 3\sqrt{7}$; logo, $2a-1 = 8+3\sqrt{7}$ não tem solução, mas $2a-1 = \epsilon^2 = 127+48\sqrt{7}$ tem solução, e $a = 64 + 24\sqrt{7}$*

tipo 3 *Seja $d = 61$, $61 \equiv 1 \pmod 4$; $\{1, \frac{1+\sqrt{61}}{2}\}$ é uma base integral de R cujo invertível fundamental $\epsilon = 17+5(\frac{1+\sqrt{61}}{2})$ não é solução da equação, pois o coeficiente da parte irracional é ímpar, $\epsilon^2 = 664 + 195(\frac{1+\sqrt{61}}{2})$ não é solução, pois ainda ocorre o mesmo caso anterior. Nas condições do lema anterior*
$2a - 1 = \epsilon^3 = 25913 + 7610(\frac{1+\sqrt{61}}{2}) = 29718 + 3085\sqrt{61}$, logo, o grupo

$$\mathcal{U}(RC_2) = \langle g\rangle \times \langle 29718 + 3085\sqrt{61}\rangle \times \langle \frac{29719 + 3085\sqrt{61}}{2} + (\frac{-29717 - 3085\sqrt{61}}{2})g\rangle$$

tem posto livre 2, enquanto que $\rho(\mathcal{U}_1(RC_2)) = 1$.

1.5 G como grupo cíclico de ordem $3, 4, 5, 6$ ou 8

Em [19] e [20] são determinados os anéis R cujo grupo $\mathcal{U}_1(RC_3)$ é trivial. Interessa-nos, porém, se este grupo é hiperbólico, o que requer, entre outras coisas, a determinação do posto desse grupo de unidades.

Seja $\mathbb{L}$ uma extensão algébrica de índice $[\mathbb{L} : \mathbb{Q}] = n$. Existem exatamente n isomorfismos de $\mathbb{L}$ sobre $\mathbb{C}$. Uma imersão $\sigma : \mathbb{L} \longrightarrow \mathbb{C}$ é denominada imersão real (respectivamente complexa) se $\sigma(\mathbb{L}) \subseteq \mathbb{R}$ (respectivamente $\sigma(\mathbb{L}) \nsubseteq \mathbb{R}$).

Seguindo a notação de [12], em que s denota o número de imersões reais do corpo $\mathbb{L}$ e $2t$ o número de imersões complexas, então $[\mathbb{L} : \mathbb{Q}] = s + 2t$.

Se $R = I_{\mathbb{L}}$ é o anel de inteiros da extensão $\mathbb{L}$, então R é um $\mathbb{Z}$ módulo livre. Lembrando que $\rho(\mathcal{U}(R))$ é o posto de $\mathcal{U}(R)$, temos, pelo Teorema de Dirichlet, que

$$\rho(\mathcal{U}(R)) = s + t - 1.$$

Seja K um corpo, e, $K[x]$ o anel de polinômios sobre K na indeterminada x. Definimos a aplicação

$$\begin{array}{rccc} \psi: & K[x] & \longrightarrow & KC_n \\ & f & \mapsto & f(g) \end{array},$$

que é um epimorfismo cujo núcleo, $ker(\psi) = (x^n - 1))$, é o ideal de $K[x]$ gerado pelo polinômio $x^n - 1$. Portanto,

$$K[x]/(x^n - 1) \cong KC_n.$$

Seja $f := x^n - 1 = f_1 f_2 \cdots f_t$ a decomposição do polinômio f como produto de polinômios irredutíveis em $K[x]$. Utilizando o teorema Chinês de Restos, obtemos:

$$KC_n \cong K[x]/(f_1) \oplus \cdots \oplus K[x]/(f_t),$$

e temos a decomposição da álgebra KC_n em componentes simples que são isomorfas a corpos. A partir do Teorema de Dirichlet, determinamos o posto livre de $\mathcal{U}_1(RC_n)$.

Proposição 1.5.1. *Seja $d \in \mathbb{Z}^* \setminus \{1\}$ um inteiro livre de quadrados, tal que, $K = \mathbb{Q}(\sqrt{d})$. A tabela abaixo fornece o posto do grupo $\mathcal{U}_1(RC_n), n \in \{2, 3, 4, 5, 6, 8\}$.*

n	$\rho(\mathcal{U}_1(RC_n))$	n	$\rho(\mathcal{U}_1(RC_n))$
2	0 *se* $d < 0$ 1 *se* $d > 1$	3	1 *se* $d < 0, d \neq -3$ 0 *se* $d = -3$ 1 *se* $d > 1$
4	1 *se* $d < -1$ 0 *se* $d = -1$ 2 *se* $d > 1$	5	6 *se* $d < 0$ 2 *se* $d = 5$ 6 *se* $d \in \mathbb{Z}^+ \setminus \{1, 5\}$
6	2 *se* $d < -3$ 0 *se* $d = -3$ 3 *se* $d > 1$	8	4 *se* $d < -1$ 1 *se* $d = -1$ 4 *se* $d = 2$ 5 *se* $d > 2$

Demonstração.

(1) Se $n = 2$, o resultado é conseqüência do Teorema 1.4.3.

(2) Se $n = 3$, considerando o epimorfismo anterior, então

$$KC_3 \cong K[x]/(x^3 - 1) \cong K/(x - 1) \oplus K[x]/(x^2 + x + 1),$$

sendo $K[x]/(x-1) \cong K$, há as seguintes possibilidades para o polinômio quadrático:

- Se $x^2 + x + 1$ é redutível sobre K, então $K = \mathbb{Q}(\sqrt{-3})$. Nesse caso $KC_3 \cong K \oplus K \oplus K$. Portanto, $RC_3 \hookrightarrow R \oplus R \oplus R =: \Lambda$, e $\mathcal{U}(R) = \mathcal{U}(Z(\sqrt{-3})) \cong \langle \zeta_6 \rangle$, a raiz primitiva da unidade de ordem 6. Logo, $\mathcal{U}(R) \cong C_6$ e $\mathcal{U}(\Lambda) \cong C_6 \times C_6 \times C_6$, portanto, $\rho(\mathcal{U}(\Lambda)) = 0$. Sendo $\mathcal{U}(RC_3)$ e $\mathcal{U}(\Lambda)$ grupos comensuráveis, temos que $\rho(\mathcal{U}(RC_3)) = 0$.
- Se $x^2 + x + 1$ é irredutível sobre K, então $d \neq -3$, e $K[x]/x^2 + x + 1 \cong K(\zeta_3) = K(\sqrt{-3})$, nesse caso $KC_3 \cong K \oplus \mathbb{Q}(\sqrt{-3} + \sqrt{d})$. Seja $\mathbb{L} = \mathbb{Q}(\sqrt{-3} + \sqrt{d})$, temos que $[\mathbb{L} : \mathbb{Q}] = 4$. Se supomos que $\mathbb{L}$ admite alguma extensão real σ, então $\sigma(\sqrt{-3}) = a \in \mathbb{R}$ e, portanto, $a^2 = -3$, um absurdo. Logo, $s = 0, t = 2$, e $\rho(\mathcal{U}(I_{\mathbb{L}})) = s + t - 1 = 1$; $RC_3 \hookrightarrow R \oplus I_{\mathbb{L}} =: \Lambda$. Sendo $\mathcal{U}(\Lambda)$ e $\mathcal{U}(RC_3)$ comensuráveis. Há duas possibilidades:
  - •• $d < 0, d \neq -3$: sendo K uma extensão quadrática imaginária, $|\mathcal{U}(R)| < \infty$, logo, $\rho(\mathcal{U}(R)) = 0$, assim $\rho(\mathcal{U}(RC_3)) = 1$;
  - •• $d > 1$: pelo Teorema de Dirichlet, $\rho(\mathcal{U}(R)) = 1$, portanto $\rho(\mathcal{U}(RC_3)) = 2$.

(3) Se $n = 4$, então

$$KC_4 \cong K[x]/(x + 1) \oplus K[x]/(x - 1) \oplus K[x]/(x^2 + 1).$$

Há duas possibilidades para o polinômico quadrático:

- $x^2 + 1$ é redutível sobre K. Neste caso $K = \mathbb{Q}(\sqrt{-1})$, portanto, $KC_4 \cong K^4$, e $\rho(\mathcal{U}(RC_4)) = 0$;
- x^2+1 é irredutível sobre K, portanto, $d \neq -1$, e $K[x]/(x^2+1) \cong K(\sqrt{-1})$; $KC_4 \cong K \oplus K \oplus K(\sqrt{-1})$, onde $K(\sqrt{-1}) = \mathbb{Q}(\sqrt{d})(\sqrt{-1}) = \mathbb{Q}(\sqrt{-1}+\sqrt{d}) = \mathbb{L}$. Logo, $[\mathbb{L} : \mathbb{Q}] = 4$, e a extensão $\mathbb{L}$ admite somente imersões complexas, portanto, $s = 0$. Logo, $\rho(\mathcal{U}(I_{\mathbb{L}})) = 1$, $RC_4 \hookrightarrow R \oplus R \oplus I_{\mathbb{L}} =: \Lambda$, e $\mathcal{U}(\Lambda)$ e $\mathcal{U}(RC_4)$ são comensuráveis. Há duas possibilidades para d:

•• $d < -1$: sendo K um extensão quadrática imaginária, $\mathcal{U}(R)$ é finito, portanto, $\rho(\mathcal{U}(RC_4)) = 1$;

•• $d > 1$: $\mathcal{U}(R)$ é um grupo cíclico infinito, portanto $\rho(\mathcal{U}(RC_4)) = 3$.

(4) Se $n = 5$, então

$$KC_5 \cong K[x]/(x^5 - 1) \cong K/(x - 1) \oplus K[x]/(x^4 + x^3 + x^2 + x + 1).$$

O polinômio $f(x) = x^4 + x^3 + x^2 + x + 1$ é redutível sobre $\mathbb{Q}(\sqrt{5})$ e irredutível sobre $\mathbb{Q}(\sqrt{d})$, se $d \neq 5$. Analisemos os casos abaixo:

- Se $d = 5$, então $f(x) = (x^2 + \frac{1+\sqrt{5}}{2}x + 1)(x^2 + \frac{1-\sqrt{5}}{2}x + 1)$, portanto, $KC_5 \cong K \oplus K[x]/(x^2 + \frac{1+\sqrt{5}}{2}x + 1) \oplus K[x]/(x^2 + \frac{1-\sqrt{5}}{2}x + 1)$, e $K[x]/(x^2 + \frac{1+\sqrt{5}}{2}x + 1) \cong \mathbb{Q}(\sqrt{2\sqrt{5} - 10}) =: \mathbb{L}$ é uma extensão de grau 4 sobre $\mathbb{Q}$, não admitindo imersão real. Portanto, $t = 2$, e $\rho(\mathcal{U}(I_{\mathbb{L}})) = 1$. O mesmo ocorre para $K[x]/(x^2 + \frac{1-\sqrt{5}}{2}x + 1) = \mathbb{L}_1$. Sendo K uma extensão quadrática real, $\mathcal{U}(R)$ é cíclico infinito; $RC_5 \hookrightarrow R \oplus I_{\mathbb{L}} \oplus I_{\mathbb{L}_1} =: \Lambda$, e $\mathcal{U}(RC_5)$ e $\mathcal{U}(\Lambda)$ são comensuráveis. Logo $\rho(\mathcal{U}(RC_5)) = 1 + 1 + 1 = 3$.
- Se $d \neq 5$, então $f(x)$ é irredutível sobre K; $K[x]/(f(x)) \cong K(\zeta_5)$, nesse caso $KC_5 \cong K \oplus \mathbb{L}$, onde $\mathbb{L} = \mathbb{Q}(\sqrt{d} + \zeta_5)$. Assim $[\mathbb{L} : \mathbb{Q}] = 8$, e $\mathbb{L}$ não admite imersão real. Consideramos as duas possibilidades:
  - •• Se $d < 0$, então $t = 4$, e $\rho(\mathcal{U}(I_{\mathbb{L}})) = s + t - 1 = 3$. Temos que $RC_5 \hookrightarrow R \oplus I_{\mathbb{L}} \oplus I_{\mathbb{L}_1} =: \Lambda$. Daí $|\mathcal{U}(R)| < \infty$, $\rho(\mathcal{U}(R)) = 0$, e $\rho(\mathcal{U}(RC_5)) = 0 + 3 + 3 = 6$.
  - •• Se $d > 1$, então $\rho(\mathcal{U}(R)) = 1$; além disso $d \neq 5$, implica $t = 4$, logo, $\rho(\mathcal{U}(RC_5)) = 1 + 3 + 3 = 7$.

(5) Se $n = 6$, então

$$KC_6 \cong K[x]/(x + 1) \oplus K[x]/(x - 1) \oplus K[x]/(x^2 + x + 1) \oplus K[x]/(x^2 - x + 1).$$

Os polinômios $x^2 + x + 1$ e $x^2 - x + 1$ são redutíveis sobre $\mathbb{Q}(\sqrt{-3})$ e são irredutíveis sobre $\mathbb{Q}(\sqrt{d})$, quando $d \neq -3$. Há dois casos há analisar:

- Se $x^2 + x + 1$ e $x^2 - x + 1$ são redutíveis sobre K, então $K = \mathbb{Q}(\sqrt{-3})$. Portanto $KC_6 \cong K \oplus K \oplus K \oplus K$. Assim $\rho(\mathcal{U}(RC_6)) = 0$.

- Se x^2+x+1 e x^2-x+1 são irredutíveis sobre K então $d \neq 3$ e $K[x]/(x^2+x+1) \cong K[x]/(x^2-x+1) \cong K(\sqrt{-3}) = \mathbb{Q}(\sqrt{-3}+\sqrt{d}) := \mathbb{L}$. Desse modo, $KC_6 \cong K \oplus K \oplus \mathbb{L} \oplus \mathbb{L}$, sendo $[\mathbb{L} : \mathbb{Q}] = 4$. A extensão $\mathbb{L}$ admite somente imersões complexas, portanto, $\rho(\mathcal{U}(I_{\mathbb{L}})) = 1$; $RC_6 \hookrightarrow R \oplus R \oplus I_{\mathbb{L}} \oplus I_{\mathbb{L}} =: \Lambda$, e $\mathcal{U}(\Lambda)$ é comensurável a $\mathcal{U}(RC_6)$. Existem duas possibilidades:
  - ••Se $d < 0$, então $\rho(\mathcal{U}(RC_6)) = 2$;
  - ••Se $d > 1$, então $\rho(\mathcal{U}(RC_6)) = 4$.

(6) Se $n = 8$, então

$$KC_8 \cong K[x]/(x-1) \oplus K[x]/(x+1) \oplus K[x]/(x^2+1) \oplus K[x]/(x^4+1).$$

Se $d = -1$ ou $d = 2$, então o polinômio x^4+1 é redutível sobre K. As possibilidades para d são:

- Se $d = -1$, então x^2+1 e x^4+1 são redutíveis sobre K e os polinômios $x^2+\sqrt{-1}$ e $x^2-\sqrt{-1}$ são fatores de x^4+1. além disso,
  $x^2+\sqrt{-1} = (x+(\frac{\sqrt{2}+\sqrt{-2}}{2}))(x-(\frac{\sqrt{2}+\sqrt{-2}}{2}))$. Portanto $K[x]/(x^4+1) \cong K(\sqrt{2}) = \mathbb{Q}(\sqrt{-1}+\sqrt{2}) = \mathbb{L}$, e $KC_8 \cong K \oplus K \oplus K \oplus K \oplus \mathbb{L}$. Sendo $[\mathbb{L} : \mathbb{Q}] = 4$, temos que $t = 2$, e $\rho(\mathcal{U}(I_{\mathbb{L}})) = 1$; $RC_8 \hookrightarrow R \oplus R \oplus R \oplus R \oplus I_{\mathbb{L}} =: \Lambda$. Sendo K uma extensão imaginária, temos que $\rho(\mathcal{U}(R)) = 0$, logo, $\rho(\mathcal{U}(RC_8)) = 0+1 = 1$;
- Se $d = 2$, então x^2+1 é irredutível sobre K, porém
  $x^4+1 = (x^2+\sqrt{2}x+1)(x^2-\sqrt{2}x+1)$ é redutível em fatores quadráticos sobre K. Logo $K[x]/(x^2+1) \cong K(\sqrt{-1}) = \mathbb{Q}(\sqrt{-1}+\sqrt{2}) = \mathbb{L}$, ocorrendo o mesmo para $K[x]/(x^2+\sqrt{2}x+1) \cong K[x]/(x^2-\sqrt{2}x+1) \cong \mathbb{L}$. Portanto, $KC_8 \cong K \oplus K \oplus \mathbb{L} \oplus \mathbb{L} \oplus \mathbb{L}$, e $RC_8 \hookrightarrow R \oplus R \oplus I_{\mathbb{L}} \oplus I_{\mathbb{L}} \oplus I_{\mathbb{L}} =: \Lambda$. Como no caso anterior $\rho(\mathcal{U}(I_{\mathbb{L}})) = 1$, porém K é uma extensão real, portanto, $\rho(\mathcal{U}(R)) = 1$. Logo $\rho(\mathcal{U}(RC_8)) = 1+1+1+1+1+1 = 5$;
- Se $d < -1$, então x^2+1 e x^4+1 são polinômios irredutíveis sobre K, logo, $K[x]/(x^2+1) \cong K(\sqrt{-1}) = \mathbb{Q}(\sqrt{d}+\sqrt{-1}) = \mathbb{L}$, e
  $K[x]/(x^4+1) \cong K(\sqrt{-1}+\sqrt{2}) = \mathbb{Q}(\sqrt{d}+\sqrt{-1}+\sqrt{2}) = \mathbb{L}_1$. Daí $KC_8 \cong K \oplus K \oplus \mathbb{L} \oplus \mathbb{L}_1$, em que os graus são $[\mathbb{L} : \mathbb{Q}] = 4$ e $[\mathbb{L}_1 : \mathbb{Q}] = 8$. Para a extensão $\mathbb{L}$(respectivamente $\mathbb{L}_1$) há 2(respectivamente 4) pares de imersões complexas de modo que $\rho(\mathcal{U}(I_{\mathbb{L}})) = 1$ e $\rho(\mathcal{U}(I_{\mathbb{L}_1})) = 3$. Assim $RC_8 \hookrightarrow R \oplus R \oplus I_{\mathbb{L}} \oplus I_{\mathbb{L}_1} =: \Lambda$. Sendo K uma extensão imaginária, temos que $\rho(\mathcal{U}(\Lambda)) = 0+0+1+3 = 4 = \rho(\mathcal{U}(RC_8))$, pois são grupos comensuráveis;

- O caso $d > 2$ é análogo ao anterior, porém o posto $\rho(\mathcal{U}(R)) = 1$, pois, neste caso, K é uma extensão real, logo, $\rho(\mathcal{U}(RC_8)) = 1 + 1 + 1 + 3 = 6$.

Para os casos onde K é uma extensão real, temos que $\rho(\mathcal{U}_1(RC_n)) = \rho(\mathcal{U}(RC_n)) - 1$ e completamos a tabela. □

Quando o posto livre de $\mathcal{U}_1(RG)$ é nulo, então $\mathcal{U}_1(R(G \times G))$ também é hiperbólico. Também, se $\mathcal{U}_1(RH)$ tem posto nulo, então $\mathcal{U}_1(R(G \times H))$ também tem posto nulo, e, portanto, é hiperbólico. Segundo o corolário acima, este é o caso para $d = -3$, pois o posto $\mathcal{U}_1(RG)$ é nulo quando $G \in \{C_2, C_3, C_6\}$, e para $d = -1$, quando $G = C_2$ e C_4.

Para os casos em que $\rho(\mathcal{U}_1(RG)) = 1$ e $\rho(\mathcal{U}_1(RH)) = 0$, na Proposição 1.5.1, não obtemos $\rho(\mathcal{U}_1(R(G \times H))) = 1$ e, portanto, $\mathcal{U}_1(R(G \times H))$ não é um grupo hiperbólico. O teorema e a proposição a seguir exprimem estes resultados.

Teorema 1.5.2. *Seja $K = \mathbb{Q}(\sqrt{d})$. Se $d \neq 1$ então as seguintes afirmações são verdadeiras:*

(1) O grupo $\mathcal{U}_1(RC_3)$ é hiperbólico.

(2) O grupo $\mathcal{U}_1(RC_4)$ é hiperbólico se, e somente se, $d < 0$.

(3) Para G um grupo abeliano de expoente dividindo n, o grupo $\mathcal{U}_1(RG)$ é hiperbólico se, e somente se: $n = 6$ e $d = -3$, ou $n = 4$ e $d = -1$.

(4) O grupo $\mathcal{U}_1(RC_8)$ é hiperbólico se, e somente se, $d = -1$.

(5) O grupo $\mathcal{U}_1(RC_5)$ não é hiperbólico.

Demonstração.

Segundo a Proposição 1.5.1, obtemos o posto livre para cada grupo de unidades. Pelo Corolário 1.2.11, são hiperbólicos os grupos cujo posto livre é no máximo 1. O resultado é direto. □

Proposição 1.5.3. *Nas condições do teorema anterior, o grupo $\mathcal{U}_1(RC_{12})$ não é hiperbólico.*

Demonstração.

$KC_{12} \cong K\bigotimes_{\mathbb{Q}}(\mathbb{Q}C_{12}) \cong K\bigotimes_{\mathbb{Q}}(\mathbb{Q}(C_3 \times C_4)) \cong K(C_3 \times C_4)$, então $RC_3 \hookrightarrow KC_{12}$ e $RC_4 \hookrightarrow KC_{12}$, portanto $\rho(\mathcal{U}_1(RC_{12})) \geq \rho(\mathcal{U}_1(RC_3)) + \rho(\mathcal{U}_1(RC_4))$, suponha que $\mathcal{U}_1(RC_{12})$ hiperbólico, pelo Corolário 1.2.11, $\rho(\mathcal{U}_1(RC_{12})) < 2$, então, pela Proposição 1.5.1, $d \in \{-3, -1\}$.

$K(C_3 \times C_4) \cong (KC_3)C_4 \cong (K \oplus K(\sqrt{-3}))C_4 \cong KC_4 \oplus K(\sqrt{-3})C_4 \cong 2K \oplus K(\sqrt{-1}) \oplus 2K(\sqrt{-3}) \oplus K(\sqrt{-3} + \sqrt{-1})$, seja $\mathbb{L} = \mathbb{Q}(\sqrt{-3} + \sqrt{-1})$. Basta verificar a decomposição acima para $d = -3$ e $d = -1$. Segundo a demonstração da Proposição 1.5.1, se $d = -3$, então $RC_{12} \hookrightarrow 4R \oplus 2I_{\mathbb{L}}$, e $\rho(\mathcal{U}(I_{\mathbb{L}})) = 1$. Portanto, $\rho(\mathcal{U}(RC_{12})) = 2$. Analogamente para $d = -1$, $RC_{12} \hookrightarrow 3R \oplus 3I_{\mathbb{L}}$, logo, $\rho(\mathcal{U}(RC_{12})) = 3$. As extensões são complexas, portanto, $\rho(\mathcal{U}_1(RC_{12})) = \rho(\mathcal{U}(RC_{12})) - 0 \geq 2$ daí, pelo Corolário 1.2.11, os grupos não são hiperbólicos. □

1.6 G não abeliano

Pelo Teorema 1.2.16, estão determinados os grupos finitos não abelianos G cujo grupo de unidades $\mathcal{U}_1(\mathbb{Z}G)$ é hiperbólico; são eles os grupos:

$$G \in \{S_3, D_4, Q_{12}, C_4 \rtimes C_4\} \cup \{\text{2-grupo hamiltoniano}\}.$$

Um subgrupo H, de um grupo G, tem um complemento normal N, se N é um subgrupo normal de G, tal que, $HN = G$ e $H \cap N = \{1\}$. Nesse caso, dizemos que N é o complemento normal de H em G. Se N é um grupo livre, então dizemos que H tem complemento normal livre em G.

Em [22], são classificados os grupos finitos G que têm um complemento normal livre não abeliano em $\mathcal{U}(\mathbb{Z}G)$, e portanto virtualmente livres. É conhecido que a álgebra $\mathbb{Q}G$, desses grupos, tem uma componente simples de Wedderburn que é isomorfa a $M_2(\mathbb{Q})$. Estes grupos, a menos dos 2-grupos Hamiltonianos, são os únicos grupos não abelianos cujo grupo de unidades $\mathcal{U}(\mathbb{Z}G)$ é hiperbólico, [24].

Lema 1.6.1. *Seja G um grupo, e seja K uma extensão quadrática. Se $M_2(K)$ é uma componente de Wedderburn de KG, então $\mathbb{Z}^2 \hookrightarrow \mathcal{U}_1(RG)$, isto é, $\mathcal{U}_1(RG)$ não é um grupo hiperbólico.*

Demonstração.

$\Gamma = M_2(R)$ é uma $\mathbb{Z}$-ordem em $M_2(K)$, e $X = \{e_{12}, e_{12}\sqrt{d}\} \subset \Gamma$ tem elementos nilpotentes de índice 2 que comutam. Além disso, o conjunto $\{1, \sqrt{d}\}$ é linearmente independente sobre $\mathbb{Q}$, logo, $\{e_{12}, e_{12}\sqrt{d}\}$ também é $\mathbb{Q} - LI$. Portanto, pelo Lema 1.2.17, $\mathbb{Z}^2 \hookrightarrow \mathcal{U}_1(\Gamma)$. Por hipótese, $M_2(K)$ é componente de Wedderburn de KG, portanto, $\mathbb{Z}^2 \hookrightarrow \mathcal{U}_1(RG)$ e, logo, este não é um grupo hiperbólico. □

Corolário 1.6.2. *Seja $G \in \{S_3, D_4, Q_{12}, C_4 \rtimes C_4\}$, então $\mathcal{U}_1(RG)$ não é hiperbólico.*

Demonstração.

Sendo $KG \cong K \bigotimes_{\mathbb{Q}} (\mathbb{Q}G)$, para os grupos listados, e $M_2(\mathbb{Q})$ uma componente de Wedderburn de $\mathbb{Q}G$, temos que $M_2(K)$ é uma componente de Wedderburn de KG. Portanto, pelo lema anterior, $\mathcal{U}_1(RG)$ não é um grupo hiperbólico. □

Recordamos que se H é um 2-grupo Hamiltoniano, então $H = E \times K_8$, sendo E um 2-grupo abeliano elementar e K_8 o grupo dos quatérnios. Do fato de K_8 conter um subgrupo cíclico de ordem 4, pelo Teorema 1.5.2, $\mathcal{U}_1(RK_8)$ é hiperbólico somente se R é imaginário, pois, caso contrário, como $\mathbb{Z}^2 \hookrightarrow \mathcal{U}_1(RC_4) \hookrightarrow \mathcal{U}_1(RK_8)$, temos que $\mathcal{U}_1(RK_8)$ não seria hiperbólico.

Proposição 1.6.3. *Se G é um 2-grupo hamiltoniano, de ordem $|G|$ maior que 8. Então o grupo de unidades $\mathcal{U}_1(RG)$ não é hiperbólico.*

Demonstração.

Seja $G = E \times K_8$, tal que, $|E| = 2^n$; $KG = K(E \times K_8) \cong K \bigotimes_{\mathbb{Q}} (\mathbb{Q}(E \times K_8)$. Sendo $\mathbb{Q}(E \times K_8) \cong (\mathbb{Q}E)K_8 \cong (2^n\mathbb{Q})K_8$, temos que $KG \cong (2^nK)K_8$. Se $|G| > 8$, então $n \geq 1$. Pela Proposição 1.5.1, $\rho(\mathcal{U}_1(RC_4)) = 1$, e C_4 é subgrupo de K_8, portanto $A = \mathcal{U}_1((2^nK)C_4)$ é um subgrupo de $\mathcal{U}(RG)$, de posto $\rho(A) \geq 2^n \geq 2$, logo, $\mathcal{U}_1(RG)$ não é um grupo hiperbólico. □

Provamos, portanto, que o grupo dos quatérnios K_8 é único 2-grupo hamiltoniano cujo grupo $\mathcal{U}_1(RG)$ pode ser hiperbólico, e neste caso R é o anel de inteiros de uma extensão

imaginária.

Se ocorre que $\mathcal{U}_1(KK_8)$ contém alguma cópia de matrizes de ordem 2 sobre o corpo K, sendo a dimensão do anel de inteiros R igual 2, como $\mathbb{Z}$-módulo, temos que, pelo Lema 1.6.1, este grupo não é hiperbólico.

O seguinte teorema elucida essa condição, pois, sendo $\mathbb{Q}K_8 \cong 4\mathbb{Q} \oplus \mathbf{H}(\mathbb{Q})$, obtemos

$$KK_8 \cong K\bigoplus_{\mathbb{Q}}(4\mathbb{Q} \oplus \mathbf{H}(\mathbb{Q})) \cong 4K \oplus \mathbf{H}(K).$$

Teorema 1.6.4 ([27], Teorema 7.4.6)**.** *Se K é um corpo de característica diferente de dois. Então a álgebra de quatérnios $\mathbf{H}(K)$ é ou um anel de divisão, ou é isomorfa a álgebra de matrizes $M_2(K)$. A segunda possibilidade ocorre se, e somente se, a equação $X^2 + Y^2 = -1$ admite solução em K.*

Definição 1.6.5 ([28])**.** *O menor número natural s para o qual a equação*

$$-1 = a_1^2 + a_2^2 + \cdots + a_s^2, a_j \in K, 1 \leq j \leq s$$

*é solúvel, é denominado o nível(*Stufe*) de K, $s(K)$. Se a equação não admite solução, definimos $s := \infty$, e K é chamado formalmente real.*

Teorema 1.6.6 ([28],Teorema 3.2)**.** *Se $d < 0$ é um inteiro livre de quadrados, e $K = \mathbb{Q}(\sqrt{d})$, então*

$$s(K) = \begin{cases} 1 & se \ -d = 1, \\ 2 & se \ -d \neq 8b + 7, \\ 4 & se \ -d = 8b + 7. \end{cases}$$

Se $d > 0$, então K é formalmente real.

Corolário 1.6.7. *Seja $K = \mathbb{Q}(\sqrt{d})$ uma extensão imaginária. A álgebra de quatérnios sobre K, $\mathbf{H}(K)$, é um anel de divisão se, e somente se, $-d \equiv 7 \pmod 8$.*

Demonstração.

Se $\mathbf{H}(K)$ é um anel de divisão, então, pelo Teorema 1.6.4, a equação $x^2 + y^2 = -1$ não admite solução em K. Portanto, $s(K) \notin \{1, 2\}$. Logo, pelo teorema anterior $s(K) = 4$, portanto, $-d \equiv 7 \pmod 8$. Reciprocamente, se $-d \equiv 7 \pmod 8$, então $s(k) = 4$, ou seja, o número mínimo de quadrados cuja soma é -1 deve ser 4. Portanto, $x^2 + y^2 = -1$ não tem solução em K. Pelo Teorema 1.6.4, temos que $\mathbf{H}(K)$ é um anel de divisão. □

Proposição 1.6.8. *Seja $K = \mathbb{Q}(\sqrt{d})$ uma extensão imaginária. Se $-d \not\equiv 7 \pmod 8$, então o grupo $\mathcal{U}_1(RK_8)$ não é hiperbólico.*

Demonstração.

Pelo corolário anterior, KK_8 não é uma álgebra de divisão. Logo, pelo Teorema 1.6.4, KK_8 tem $M_2(K)$ como componente de Wedderburn. Portanto, pelo Lema 1.6.1, o grupo $\mathcal{U}_1(RK_8)$ não é hiperbólico. □

1.7 A hiperbolicidade de $\mathcal{U}(RK_8)$

O espaço hiperbólico tri-dimensional, que denotamos por $\mathbb{H}$, é a única variedade riemanniana conexa e simplesmente conexa, de curvatura constante -1.

Um modelo adequado para $\mathbb{H}$ é o espaço $\mathbb{C}\times]0,\infty[$. Seja $\mathbf{H} := \mathbf{H}(-1,-1)$, segundo a definição 1.2.18, a álgebra dos quatérnios sobre os reais, com a base usual $\{1,i,j,k\}$. Podemos identificar o espaço $\mathbb{H}$ com um subconjunto de $\mathbf{H}$:

$$\mathbb{H} = \{z + rj : z \in \mathbb{C}, r \in \mathbb{R}^+\}.$$

Seja $PSL(2,\mathbb{C}) \doteq \{M \in M_2(\mathbb{C}) : det(M) = 1\}/\{\pm I\}$, em que $det(M)$ denota o determinante da matriz M, e I a matriz identidade.

O grupo $PSL(2,\mathbb{C})$ age sobre $\mathbb{H}$ da seguinte forma:

$$\begin{array}{rccc} \varphi: & PSL(2,\mathbb{C}) \times \mathbb{H} & \longrightarrow & \mathbb{H} \\ & (M,P) & \mapsto & \begin{pmatrix} a & b \\ c & d \end{pmatrix} P \doteq (aP+b)(cP+d)^{-1} \end{array},$$

onde $(cP+d)^{-1}$ é obtido em $\mathbf{H}$, com a coordenada de k nula. Explicitamente, $MP = M(z+rj) = z^* + r^* j$, com $z^* = \frac{(az+b)(\overline{cz}+\overline{d})+a\overline{c}r^2}{|cz+d|^2+|c|^2r^2}$ e $r^* = \frac{r}{|cz+d|^2+|c|^2r^2}$.

Para o que segue, consideramos K uma extensão quadrática imaginária, e R o anel de inteiros de K e $\mathbf{H}$ a álgebra dos quaténios sobre K ou R, conforme seja indicado.

Lembramos que

$$RK_8 \cong 4R \oplus \mathbf{H}(R).$$

Sendo η a norma em $\mathbf{H}$, definimos o grupo $SL_1(\mathbf{H}(R)) = \{x \in \mathbf{H}(R) : \eta(x) = 1\}$.

O grupo de unidades $\mathcal{U}(\mathbf{H}(R))$ é comensurável ao grupo $\mathcal{U}(R) \times SL_1(\mathbf{H}(R))$. Portanto investigamos as propriedades de $\mathcal{U}(\mathbf{H}(R))$, a partir do grupo $SL_1(\mathbf{H}(R))$.

Seja $\mathcal{I}nn(\mathbf{H}(K))$ o grupo dos automorfismos internos do grupo $SL_1(\mathbf{H}(R))$. Consideramos o subcorpo $F = K[i] \subset \mathbf{H}(K)$, que é um corpo maximal na álgebra $\mathbf{H}(K)$. O automorfismo $\sigma \in \mathcal{I}nn(\mathbf{H}(K))$,

$$\begin{array}{rccc} \sigma: & \mathbf{H}(K) & \longrightarrow & \mathbf{H}(K) \\ & x & \mapsto & jxj^{-1} \end{array},$$

fixa F. Podemos considerar $\mathbf{H}(K) \cong F \oplus Fj$, o produto cruzado entre estes K-espaços vetoriais.

Temos a seguinte imersão de $\mathbf{H}(K)$ em $M_2(\mathbb{C})$:

$$\begin{array}{rccc} \Psi: & \mathbf{H}(K) & \hookrightarrow & M_2(\mathbb{C}) \\ & x + yj & \mapsto & \begin{pmatrix} x & y \\ -\sigma(y) & \sigma(x) \end{pmatrix}. \end{array} \qquad 1.7$$

Esta imersão associa os grupos $SL_1(\mathbf{H}(R))$ e $SL_1(\mathbf{H}(K))$ a subgrupos de $SL(2, \mathbb{C})$.

Via essa imersão, o grupo $SL_1(\mathbf{H}(K))$ age sobre o espaço $\mathbb{H}$, e utilizamos esta ação para estudar o grupo $\mathcal{U}(\mathbf{H}(R))$.

Teorema 1.7.1 ([11], Teorema 2.1.2)**.** *Um subgrupo $\Gamma < PSL(2, \mathbb{C})$ é um grupo descontínuo se, e somente se, Γ é discreto em $PSL(2, \mathbb{C})$.*

O teorema a seguir, mostra que o subgrupo $SL_1(\mathbf{H}(R))$, em alguns casos, é discreto. Portanto, segundo o teorema anterior, o grupo $SL_1(\mathbf{H}(R))$ age descontinuamente sobre o espaço $\mathbb{H}$.

Teorema 1.7.2 ([11],Teorema 10.1.2)**.** *Se* $\mathbf{H}(K)$ *é a álgebra de quatérnios generalizada, sobre um corpo numérico* K*, e as seguintes condições são satisfeitas:*

- K *tem exatamente um par de imersões complexas (também conhecido como place Arquimediano Complexo);*
- $\mathbf{H}(K)$ *é ramificado em todos os places reais, isto é,* $\mathbf{H}(\sigma(K)) \bigotimes_K \mathbb{R})$ *é um anel de divisão (necessariamente o anel dos quatérnios hamiltonianos* $\mathbf{H}(\mathbb{R})$*), para toda imersão real* σ *de* K*.*

Então, para toda ordem Γ *em* $\mathbf{H}(K)$*:*

(1) $SL_1(\Gamma)$ *é discreto.*

(2) $SL_1(\Gamma)$ *tem covolume finito(i.e., os domínios fundamentais têm volume finito), e portanto ([11], Teorema* 7.1.1 *item* 7*), é geometricamente finito (i.e., todos os poliedros normais de Dirichlet, ou Poincaré, têm número finito de faces).*

(3) $SL_1(\Gamma)$ *é co-compacto (i.e., tem um domínio fundamental compacto) se, e somente se,* $\mathbf{H}(K)$ *é um anel de divisão.*

O seguinte teorema permite concluir nossa principal investigação desta seção:

Teorema 1.7.3 ([3], Teorema 2.24))**.** *Seja* G *um grupo. Então* G *é hiperbólico se, e somente se,* G *admite uma ação geométrica sobre um espaço métrico hiperbólico e próprio* (X, d)*.*

Corolário 1.7.4 ([3], Exemplo 2.22.5))**.** *Seja* M *uma variedade riemanniana fechada* n*-dimensional de curvatura seccional constante negativa, e seja* $G = \pi_1(M)$*. Então* G *é um grupo hiperbólico e* $\partial(G)$*(a fronteira hiperbólica de* G*) é homeomorfa à esfera* S^{n-1}*.*

Estamos em condições de provar o teorema principal para os anéis de inteiros de uma extensão quadrática racional, cujo grupo de unidades $\mathcal{U}_1(RG)$ é um grupo hiperbólico.

Teorema 1.7.5. *Seja R o anel de inteiros de uma extensão quadrática racional $K = \mathbb{Q}(\sqrt{d})$, e, $d \in \mathbb{Z}\setminus\{1\}$ livre de quadrados. O grupo de unidades $\mathcal{U}_1(RG)$ é hiperbólico se, e somente se, G é um dos grupos listados abaixo, e R determinado pelo respectivo valor de d:*

(1) $G \in \{C_2, C_3\}$, e d é qualquer.

(2) G é um grupo abeliano de expoente dividindo n para:
$n = 2$ e $d < 0$; ou $n = 6$ e $d = -3$; ou $n = 4$ e $d = -1$.

(3) $G = C_4$, e $d < 0$.

(4) $G = C_8$ e $d = -1$.

(5) $G = K_8$, e $s(K) = 4$, ou seja, $d < 0$, e $-d \equiv 7 \pmod 8$.

Demonstração.

Os casos abelianos foram provados nas seções 1.4 e 1.5.

Se $\mathcal{U}_1(RK_8)$ é hiperbólico, então $KK_8 \hookleftarrow \mathbf{H}(K) \ncong M_2(K)$, caso contrário, pelo Lema 1.6.1, $\mathbb{Z}^2 \hookrightarrow \mathcal{U}_1(RK_8)$. Portanto, pelo Teorema 1.6.4, $\mathbf{H}(K)$ é anel de divisão. Logo, pelo Corolário 1.6.7, $-d \equiv 7 \pmod 8$.

Reciprocamente, pelo Teorema 1.7.2, $SL_1((\mathbf{H}(R)))$ age sobre o espaço $\mathbb{H}$ e é um subgrupo discreto de $SL_2(\mathbb{C})$. Temos, portanto, que o espaço quociente $Y := \mathbb{H}/SL_1((\mathbf{H}(R))$ é uma variedade riemanniana de curvatura constante -1. Além disso, sendo $\mathbb{H}$ simplesmente conexo, temos que $SL_1((\mathbf{H}(R))) \cong \pi_1(Y)$.

Sendo $-d \equiv 7 \pmod 8$, segue-se, pelo Corolário 1.6.7, que $\mathbf{H}(K)$ é um anel de divisão. Logo, pelo item 3 do Teorema 1.7.2, $SL_1((\mathbf{H}(R))$ é co-compacto, portanto Y é compacto. Assim, pelo corolário 1.7.4, $SL_1((\mathbf{H}(R)))$ é hiperbólico. Sendo $\mathcal{U}(\mathbf{H}(R))$ comensurável ao grupo $\mathcal{U}(R) \times SL_1(\mathbf{H}(R))$, e $\mathcal{U}(R) = \{-1, 1\}$, segue-se que $\mathcal{U}(\mathbf{H}(R))$ é um grupo hiperbólico.

Sendo $\mathcal{U}(RK_8) \cong \mathcal{U}(R)\times\mathcal{U}(R)\times\mathcal{U}(R)\times\mathcal{U}(R)\times\mathcal{U}(\mathbf{H}(R))$ e $\mathcal{U}(R) \cong C_2$, então $\mathcal{U}(RK_8)$ e $\mathcal{U}(\mathbf{H}(R))$ são comensuráveis, e, logo, $\mathcal{U}(RK_8)$ é um grupo hiperbólico. □

Corolário 1.7.6. *Nas condições do teorema anterior, $\mathcal{U}(RK_8)$ é hiperbólico se, e somente se, $-d \equiv 7 \pmod 8$. Nesse caso, a fronteira hiperbólica $\partial(\mathcal{U}(RK_8)) \cong S^2$, a esfera euclideana de dimensão 2, e o número de fins é 1.*

Demonstração.

Pelo Corolário 1.7.4, a fronteira $\partial(\mathcal{U}(RK_8)) \cong S^2$. Que é um conjunto conexo, portanto, o resultado. □

Note que no caso em que $\mathcal{U}(\mathbb{Z}G)$ é hiperbólico, $\partial(\mathcal{U}(\mathbb{Z}G))$ é totalmente desconexo e isomorfo ao conjunto de Cantor. Nesse caso, o grupo $\mathcal{U}(\mathbb{Z}G)$ tem infinitos fins. Tais grupos, que são virtualmente livres, são exemplos clássicos de grupos hiperbólicos infinitos. Ocorre que o grupo $\mathcal{U}(RK_8)$ não é virtualmente livre e é hiperbólico. Este fato, exibe esse grupo como um dos primeiros exemplos de um grupo hiperbólico infinito nessas condições, isto é, não virtualmente livre.

Teorema 1.7.7. *Seja $K = \mathbb{Q}(\sqrt{-d})$, $d \in \mathbb{Z}^+$, livre de quadrados, e seja R o anel de inteiros de K. O grupo $\mathcal{U}(\mathbf{H}(R))$ é hiperbólico se, e somente se, $d \equiv 7 \pmod 8$.*

Teorema 1.7.8 ([5], Proposição $III.\Gamma.3.2$)**.** *Se Γ é um grupo hiperbólico, então para todo conjunto finito de elementos $h_1, \cdots, h_r \in \Gamma$, existe um inteiro $n > 0$, tal que, o conjunto $\{h_1^n, \cdots, h_r^n\}$ gera um subgrupo livre de posto máximo r em Γ.*

Teorema 1.7.9. *Seja R o anel de inteiros da extensão imaginária $K = \mathbb{Q}(\sqrt{-d})$, e, $d \equiv 7 \pmod 8$. Se $u_1 \cdots u_r \in \mathcal{U}_1(RK_8)$, então existe $n \in \mathbb{N}$, tal que, $\langle u_1^n, \cdots, u_r^n \rangle$ é um grupo livre de posto menor ou igual a r.*

Em [8], determina-se uma apresentação (*presentation*), para o grupo de unidades $\mathcal{U}(\mathbf{H}(\mathbb{Z}(\frac{1+\sqrt{-7}}{2})))$, bem como mostra-se um algorítmo para determinar um conjunto finito de geradores do grupo de unidades de uma ordem em uma álgebra de quatérnios que não cinde (*non split*), sobre uma extensão K.

Na seção seguinte, construímos unidades $u \in \mathcal{U}(\mathbf{H}(R))$: a partir de unidades do anel de inteiros de uma extensão real ou a partir da solução do problema dos três quadrados, isto é, quando um número inteiro é a soma de três inteiros quadrados.

1.8 As unidades de Pell e as unidades de Gauss

Seja $u \in \mathcal{U}(\mathbf{H}(R))$. Se a álgebra $\mathbf{H}(K)$ não é anel de divisão, podemos obter unidades u, de uma $\mathbb{Z}$-ordem de $\mathbf{H}(K)$, a partir da álgebra de matrizes $M_2(K)$, pois neste caso as álgebras são isomorfas. No entanto, se $\mathbf{H}(K)$ é um anel de divisão, isto foi feito apenas para o caso $\mathcal{U}(\mathbf{H}(\mathbb{Z}(\frac{1+\sqrt{-7}}{2})))$, por C. Corrales, E. Jespers, G. Leal e A. del Río, no artigo *Presentations of the unit group of an order in a non-split quaternion algebra*, publicado em (2004), na Advances in Mathematics.

Aqui construímos explicitamente unidades de $\mathcal{U}(\mathbf{H}(R))$, quando a álgebra $\mathbf{H}(K)$ é um anel de divisão, resolvendo assim um problema antigo.

Para o que apresentamos a seguir, $K = \mathbb{Q}(\sqrt{-d})$ é uma extensão quadrática imaginária e $d \equiv 7 \pmod 8$.

Considerando a base usual dos quatérnios, para $u \in \mathcal{U}(\mathbf{H}(R))$, $u = u_1 + u_i i + u_j j + u_k k$, e u_1, denominado coeficiente livre, denota o coeficiente do elemento 1, para a unidade u.

Uma condição para que $u \in \mathbf{H}(R)$ seja uma unidade, é que sua norma

$$\eta(u) = u_1^2 + u_i^2 + u_j^2 + u_k^2 = \pm 1.$$

Para K uma extensão imaginária, existem unidades não triviais, às quais apresentamos uma construção.

Seja $u = u_1 + u_i i + u_j j + u_k k \in \mathbf{H}(K)$, escrevendo $u = u_1 + u_i i + (u_j + u_k i)j$ a representação de u dada por 1.7, é:

$$[u] := \begin{pmatrix} u_1 + u_i i & u_j + u_k i \\ -u_j + u_k i & u_1 - u_i i \end{pmatrix},$$

o produto uv é dado por:

$$[uv] = \begin{pmatrix} u_1 + u_i i & u_j + u_k i \\ -u_j + u_k i & u_1 - u_i i \end{pmatrix} \begin{pmatrix} v_1 + v_i i & v_j + v_k i \\ -v_j + v_k i & v_1 - v_i i \end{pmatrix} = \begin{pmatrix} A + Bi & C + Di \\ -C + Di & A - Bi \end{pmatrix}.$$

Sendo $\begin{array}{ll} A = u_1v_1 - u_iv_i - u_jv_j - u_kv_k & B = u_1v_i + u_iv_1 + u_jv_k - u_kv_j \\ C = u_1v_j - u_iv_k + u_jv_1 + u_kv_i & D = u_1v_k + u_iv_j - u_jv_i + u_kv_1 \end{array}$.

Se $\Psi(u) = [u]$ denota a matriz associada a u, seja χ_u o polinômio característico de $[u]$, e, m_u o polinômio minimal de $[u]$. O grau de χ_u, $\partial(\chi_u) = 2$, e, portanto $\partial(m_u) \leq 2$. Se $\partial(m_u) = 1$, então $m_u(X) = X - z_0, z_0 \in \mathbb{C}$. Nessas condições $u = z_0$, pois $m_u([u]) = m_u(\Psi(u)) = \Psi(m_u(u))$, e sendo Ψ um monomorfismo, obtemos $m_u(u) = 0 = u - z_0$. Portanto, $u = z_0$.

O polinômio característico é

$$\chi_u(X) = X^2 - \text{traço}([u])X + det([u]),$$

sendo traço$([u]) = u_1 + u_ii + \sigma(u_1 + u_ii) = 2u_1$. Se u é uma unidade, então $det([u]) = \pm 1$;

$$\chi_u(X) = X^2 - 2u_1X \pm 1$$

é o polinômio característico de $\Psi(u)$. Se $u_1 \neq 1$ ou $u_1 \neq -1$, então o polinômio característico é irredutível sobre K, portanto $m_u = \chi_u$.

Proposição 1.8.1. *Seja $u = u_1 + u_ii + u_jj + u_kk \in \mathcal{U}(\mathbf{H}(K))$, e, $\eta(u)$ a norma de u. As seguintes afirmações são verdadeiras :*

(1) $u^2 = 2u_1u - \eta(u)$

(2) Se $d \equiv 7 \pmod 8$ *e* $\eta(u) = 1$*, então u é de torção se, e somente se,* $u_1 \in \{-1, 0, 1\}$*, e nesse caso a ordem de u,* $o(u) = 4, 2,$ *ou* 1.

(3) Se $d \equiv 7 \pmod 8$*, e* $\eta(u) = -1$ *então u tem ordem infinita,* $o(u) = \infty$.

Demonstração. A primeira parte é uma aplicação direta do polinômio característico: $\chi_u[u] = u^2 - 2u_1u + \eta(u) = 0$ implica $u^2 = 2u_1u - \eta(u)$

Se u é de torção, então existe $n \in Z^+$, tal que, $u^n = 1$.
Seja $\Psi_u(X) = X^2 - 2u_1X + \eta(u) = (X - \zeta_1)(X - \zeta_2)$ a decomposição do polinômio característico em $\mathbb{C}$. Afirmamos que u_1 é um número real. De fato $\zeta_1\zeta_2 = \eta(u) = \pm 1$. Ou ocorre que $u_1 \in \{-1, 1\}$, e nesse caso $m_u(X) = X - u_1$, ou χ_u é irredutível sobre K, e, portanto, $m_u = \chi_u$. Em qualquer caso, $m_u(u) \mid u^n - 1$, então $\zeta_l^n = 1$, e $\zeta_l, l = 1, 2$ é uma raiz da unidade. Portanto $\zeta_1 = \overline{\zeta_2}$, sendo $2u_1 = \zeta_1 + \zeta_2 = 2\Re(\zeta_1)$, em que $\Re(\zeta)$ denota a

parte real de ζ, obtemos $u_1 \in \mathbb{R}$. Sendo $u \in \mathbf{H}(R)$, e, $\{1, \frac{\sqrt{-d}+1}{2}\}$ uma base integral de R, obtemos $u_1 = a \in \mathbb{Z}$. Da igualdade $2u_1 = \zeta_1 + \zeta_2$, temos que $2|u_1| = |\zeta_l + \zeta_2| \leq 2$, e, portanto, $u_1 \in \{-1, 0, 1\}$.

Na condição da norma $\eta(u) = 1$, reciprocamente, para $u_1 = 0$, a primeira parte da proposição mostra que $u^2 = -1$, portanto $o(u) = 4$. Se $u_1 = \pm 1$, então $m_u(X) = X^2 \mp 2X + 1 = (X \mp 1)^2$, sendo $m_u(u) = 0 = (u \mp 1)^2 \in \mathbf{H}(K)$ um anel de divisão, então $u = \pm 1$, e, logo, $u = 1$ ou $u = -1$.

Na condição da norma $\eta(u) = -1$, temos que $\eta(u^2) = 1$. Suponhamos que u é de torção, pelo item anterior, obtemos $o(u) \in \{2, 4\}$. Logo, no máximo, $o(u) = 8$. Se $u_1 = 0$, então, pelo primeiro item , $u^2 = -\eta(u) = 1$, assim $u = 1$ ou $u = -1$, um absurdo com a hipótese de $\eta(u) = -1$. Se $u_1 = 1$ ou $u_1 = -1$, então $m_u(X) = \chi_u(X) = X^2 - 2u_1X - 1$. Desse modo, $m_u(u) \mid u^8 - 1$, e $m_u = u^2 \mp 2u - 1$ tem $\pm 1 \pm \sqrt{2}$ como raízes. Isso é um absurdo, porque essas raízes não são raízes da unidade, o que refuta a divisibilidade. Portanto, se $\eta(u) = -1$, então $o(u) = \infty$. □

A seguir, as unidades consideradas, a menos que se mencione o contrário, são de norma 1.

Sejam $\xi \neq \psi \in \{1, i, j, k\}$ e $u := m\sqrt{-d}\xi + p\psi \in \mathcal{U}(\mathbf{H}(K))$, então $u\overline{u} = 1 = p^2 - m^2d$. Estamos interessados no caso em que $\mathbf{H}(K)$ é um anel de divisão, portanto, $d \equiv 7 \pmod 8$. Nessas condições, $8 \mid d+1$, portanto $d \equiv 3 \pmod 4$. Se $\mathbb{L} = \mathbb{Q}(\sqrt{d})$, então $\{1, \sqrt{d}\}$ é uma base integral de $I_{\mathbb{L}}$ e a equação $1 = p^2 - m^2d$ sempre tem solução em $\mathbb{Z}$. Denotamos por $u_{(\epsilon)}$, a unidade construída pelo invertível $\epsilon = p + m\sqrt{d} \in \mathcal{U}(I_{\mathbb{L}})$, definindo $u_{(1)} := 1$.

Proposição 1.8.2. *Seja $d \equiv i \pmod 4, i \in \{2, 3\}$, e sejam $\xi \neq \psi \in \{1, i, j, k\}$. As seguintes afirmações são verdadeiras:*

(1) $u_{(\epsilon)} \in \mathcal{U}(\mathbf{H}(R))$ se, e somente se, $\epsilon = p + m\sqrt{d}$ é invertível em $I_{\mathbb{L}}$.

(2) Se $1 \notin supp(u)$, o suporte de u, então u é de torção.

(3) Se μ e ν são invertíveis em $I_{\mathbb{L}}$, e $1 \in supp(u_{(\mu)}) = supp(u_{(\nu)})$, então $u_{(\mu)}u_{(\nu)} = u_{(\mu\nu)}$.

(4) Seja $\epsilon = p + m\sqrt{d}$ um invertível. Se $1 \in supp(u_{(\epsilon)})$, então

$$\langle u_{(\epsilon)} \rangle = \{u_{(\epsilon^n)}, n \in \mathbb{Z}\}.$$

Demonstração.

Sendo d livre de quadrados, $\{1, \sqrt{d}\}$ é base integral de $I_{\mathbb{L}}$, portanto, se u é unidade, então a norma de u, $\eta(u) = 1 = p^2 - m^2 d$. Logo, $p + m\sqrt{d} \in \mathcal{U}(I_{\mathbb{L}})$. Reciprocamente, se $\epsilon = p + m\sqrt{d} \in \mathcal{U}(I_{\mathbb{L}})$, então $p^2 - m^2 d = 1 = (m\sqrt{-d}\xi + p\psi)(m\sqrt{-d}\xi - p\psi)$, e $m\sqrt{-d}\xi + p\psi \in \mathbf{H}(R)$ é uma unidade.

Se $1 \notin supp(u)$, então $u_1 = 0$, portanto, pela Proposição 1.8.1, u é de torção.

Seja $\epsilon = x + y\sqrt{d}$ o invertível fundamental. Pelo Teorema de Dirichlet, $\mu, \nu \in \langle\epsilon\rangle$. Portanto, $\mu = \epsilon^m = A + B\sqrt{d}$, e $m \in \mathbb{Z}$, e $A, B \in \mathbb{Z}$ coeficientes que dependem somente se x, y, d, m, e mesmo ocorre com $\nu = \epsilon^n = C + D\sqrt{d}$. Assim, $u_{(\mu)} = A\xi + B\sqrt{-d}\psi$, $u_{(\nu)} = C\xi + D\sqrt{-d}\psi$, como $1 \in supp(u)$, consideramos, sem perda de generalidade, $\xi = 1$. Por um lado, o produto $\mu\nu = AC + dBD + (AD + BC)\sqrt{d} = \epsilon^{m+n}$. Por outro lado, o produto $u_{(\mu)}u_{(\nu)} = (AC + dBD) - (AD + BC)\sqrt{-d}\psi = u_{(\mu\nu)}$. Como conseqüência disso, obtemos que $\langle u_{(\epsilon)}\rangle = \{u_{(\epsilon^n)}, n \in \mathbb{Z}\}$ □

As unidades construídas dessa forma vamos denominá-las de 2-unidades de Pell, e o grupo cíclico

$$\langle u_{(\epsilon)}\rangle = \{u_{(\epsilon^n)}, n \in \mathbb{Z}\} := \langle u_{\langle\epsilon\rangle}\rangle$$

De modo semelhante à construção anterior, para $\xi, \psi, \phi \in \{1, i, j, k\}$, distintos dois a dois, construímos unidades do seguinte tipo:

$$u = m\sqrt{-d}\xi + p\psi + (1 - p)\phi.$$

Proposição 1.8.3. *Seja $d \equiv 3 \pmod 4$, e, $\mathbb{L} = \mathbb{Q}(\sqrt{2d})$, e, $I_{\mathbb{L}}$ o anel de inteiros de $\mathbb{L}$. Se $\xi, \psi, \phi \in \{1, i, j, k\}$, são distintos dois a dois, então*

$$u = m\sqrt{-d}\xi + p\psi + (1 - p)\phi \in \mathcal{U}(\mathbf{H}(R)) \Leftrightarrow \epsilon = (2p - 1) + m\sqrt{2d} \in \mathcal{U}(I_{\mathbb{L}})$$

Demonstração.

Se u é uma unidade, então $1 = u\overline{u} = -m^2 d + p^2 + (1 - p)^2$ determina a equação: $2p^2 - 2p - m^2 d = 0$, multiplicamos por 2 e obtemos $(2p - 1)^2 - m^2 2d = 1$. Sendo $d \equiv 3 \pmod 4$, temos que $2d \equiv 2 \pmod 4$, logo, $\{1, \sqrt{2d}\}$ é uma base integral de $I_{\mathbb{L}}$. Portanto $\epsilon = (2p-1) + m\sqrt{2d}$ é um invertível de $I_{\mathbb{L}}$. Reciprocamente, se ϵ é um invertível, então $(2p-1)^2 - m^2 2d = 1$, implica que $2p^2 - 2p - m^2 d = 0$. Seja $u = m\sqrt{-d}\xi + p\psi + (1-p)\phi$,

a norma de u é $u\overline{u} = -m^2d + p^2 + (1-p)^2 = -m^2d + 2p^2 - 2p + 1 = 1$, então $\overline{u}$ é o inverso de u. Se $\epsilon = x + y\sqrt{2d}$, sendo $\epsilon\overline{\epsilon} = 1 = x^2 - 2dy^2$, necessariamente $x \equiv 1 \pmod 2$. Portanto, se $2p - 1 = x$, então $p \in \mathbb{Z}$, logo $u \in \mathcal{U}(\mathbf{H}(R))$. □

As unidades construídas desse modo serão denominadas 3-unidades de Pell.

Vamos procurar as unidades do tipo $u = m\sqrt{-d} + (m\sqrt{-d})i + pj + qk$, com $m, p, q \in \mathbb{Z}$.

A condição sobre a norma de u, resulta na equação:

$$-2m^2d + p^2 + q^2 = 1.$$

Seja $p + q = r$, então obtemos uma equação quadrática em p, parametrizada pelo inteiros m e r, ou seja: $2p^2 - 2pr - 2m^2d + r^2 - 1 = 0$

Proposição 1.8.4. *A equação $2p^2 - 2pr - 2m^2d + r^2 - 1 = 0$, com coeficientes inteiros, $d > 0$ e $d \equiv 7 \pmod 8$, tem solução em $\mathbb{Z}$ quando $r := p + q = 1$.*

Demonstração.

Seja $r = 1$. A solução da equação, em p, é $p = \frac{1 \pm \sqrt{1+4m^2d}}{2}$. Considerando a solução em $\mathbb{Z}$, o termo do radical necessariamente é um quadrado e $1 + 4m^2d = z^2$, portanto,

$$z^2 - 4m^2d = 1 \quad 1.8.$$

Sendo $d \equiv 7 \pmod 8$, temos que $d \equiv 3 \pmod 4$. Portanto, $\{1, \sqrt{d}\}$ é base integral do anel de inteiros de $\mathbb{Q}(\sqrt{d})$. Seja $\epsilon = x + y\sqrt{d}$ um invertível, então
$x^2 - y^2d = 1 = (x + y\sqrt{d})(x - y\sqrt{d})$. Rescrevendo a equação 1.8, convenientemente, obtemos $(z + 2m\sqrt{d})(z - 2m\sqrt{d}) = 1$. Se y é um inteiro ímpar, consideramos
$\epsilon^2 = (x^2 + y^2d) + 2xy\sqrt{d}$ que é invertível. Logo, escrevendo

$$m = \begin{cases} \frac{y}{2} & \text{se } y \equiv 0 \pmod 2 \\ xy & \text{se } y \equiv 1 \pmod 2 \end{cases},$$

temos que $1 + 4m^2d = z^2$ é um quadrado ímpar. Portanto, $p = \frac{1 \pm z}{2} \in \mathbb{Z}$ é solução em $\mathbb{Z}$ da equação quadrática.

□

Estamos interessados na condição $d \equiv 7 \pmod 8$, onde $\mathbf{H}(\mathbb{Q}(\sqrt{-d}))$ é um anel de divisão. O lema, a seguir, é válido para extensões $\mathbb{L} := \mathbb{Q}(\sqrt{d})$ com $I_{\mathbb{L}}$ o anel de inteiros e base integral $\{1, \sqrt{d}\}$, ou seja, $d \equiv 2 \pmod 4$ ou $d \equiv 3 \pmod 4$.

Lema 1.8.5. *Seja $K = \mathbb{Q}(\sqrt{-d})$ uma extensão imaginária, com $d \equiv 2 \pmod 4$ ou $d \equiv 3 \pmod 4$ e $\mathbf{H}(K)$ a álgebra de quatérnios sobre K. Se $x + y\sqrt{d} \in \mathcal{U}(I_{\mathbb{L}})$, um invertível do anel de inteiros da extensão $\mathbb{L} = \mathbb{Q}(\sqrt{d})$, então*

$$u = \begin{cases} \frac{y}{2}\sqrt{-d} + (\frac{y}{2}\sqrt{-d})i + (\frac{1\pm x}{2})j + (\frac{1\mp x}{2})k & \text{se } y \equiv 0 \pmod 2 \\ xy\sqrt{-d} + (xy\sqrt{-d})i + (\frac{1\pm(x^2+y^2d)}{2})j + (\frac{1\mp(x^2+y^2d)}{2}k) & \text{se } y \equiv 1 \pmod 2 \end{cases}$$

são unidades em $\mathbf{H}(K)$. Se permutarmos os coeficientes de $\{1, i, j, k\}$, obtemos outras unidades.

Teorema 1.8.6. *Seja $K = \mathbb{Q}(\sqrt{-d})$ uma extensão imaginária, cuja álgebra de quatérnios $\mathbf{H}(K)$, sobre K, é um anel de divisão, e, $\mathbb{L} = \mathbb{Q}(\sqrt{d})$. Se $x + y\sqrt{d} \in \mathcal{U}(I_{\mathbb{L}})$, então*

$$u = \begin{cases} \frac{y}{2}\sqrt{-d} + (\frac{y}{2}\sqrt{-d})i + (\frac{1\pm x}{2})j + (\frac{1\mp x}{2})k & \text{se } y \equiv 0 \pmod 2 \\ xy\sqrt{-d} + (xy\sqrt{-d})i + (\frac{1\pm(x^2+y^2d)}{2})j + (\frac{1\mp(x^2+y^2d)}{2}k) & \text{se } y \equiv 1 \pmod 2 \end{cases}$$

são unidades em $\mathbf{H}(R)$.

Definição 1.8.7. *As unidades, acima, obtidas pela equação de Pell, equação [1.8], vamos denominar **Unidades de Pell**. A unidade $u = m\sqrt{-d} + (m\sqrt{-d})i + pj + (1-p)k$ é denominada unidade primária. Uma unidade de Pell u cuja cardinalidade do suporte $l := |supp(u)| \in \{2, 3\}$ e $m\sqrt{-d}$ é o único coeficiente não inteiro de u é denominada l-unidade de Pell.*

Proposição 1.8.8. *Sejam $K = \mathbb{Q}(\sqrt{-d})$ uma extensão imaginária, com $d \equiv 2 \pmod 4$ ou $d \equiv 3 \pmod 4$ e $\mathbf{H}(K)$ a álgebra de quatérnios sobre K. Se $u \in \mathcal{U}(\mathbf{H}(R))$ é uma unidade primária de Pell, e $m\sqrt{-d}$ é o fator de Pell, então u^2 não é uma unidade de Pell.*

Demonstração. Seja u a unidade primária, $u = m\sqrt{-d} + (m\sqrt{-d})i + pj + (1-p)k$, utilizando que $u^2 = 2u_1u - 1 = (2m^2d - 1) + (2m^2d)i + (2m\sqrt{d}p)j + (2m\sqrt{d}(1-p))k$, os coeficientes $(u^2)_j$ e $(u^2)_k$, de u^2, são distintos, portanto u^2 não é unidade de Pell. □

As unidades de Pell, assim construídas, são unidades de norma 1. As unidades de norma -1, portanto não são geradas a partir das unidades de Pell, pois a norma é um homomorfismo multiplicativo.

Seja $u = m\sqrt{-d} + pi + qj + rk \in \mathcal{U}(\mathbf{H}(R))$ uma unidade de norma -1. Nesse caso, $p^2 + q^2 + r^2 = m^2d - 1$.

Para o que discutiremos a seguir, estamos supondo que $\mathbf{H}(K)$ seja um anel de divisão, ou equivalentemente, que $d \equiv 7 \pmod 8$.

Teorema 1.8.9 (Gauss, [29], Teorema 1)**.** *Seja n um inteiro positivo. Se $n = 4^a n'$, $4 \nmid n'$ e $a \geq 0$. Então n é a soma de três inteiros quadrados se, e somente se,*
$n' \not\equiv 7 \pmod 8$.

Proposição 1.8.10. *Seja $d \equiv 7 \pmod 8$. Se $m \equiv 2 \pmod 4$, então $m^2d - 1$ e $m^2d + 1$ são soma de três quadrados.*

Demonstração.

Por hipótese, $m \equiv 2 \pmod 4$, logo, m é par: $4 \mid m^2$, mas $8 \nmid m^2$, sendo $d \equiv 7 \pmod 8$, $d \equiv 1 \pmod 2$, portanto $m^2d \not\equiv 0 \pmod 8$, e, logo, $m^2d - 1 \not\equiv 7 \pmod 8$. Seja $m^2d \equiv z \pmod 8$, temos que $z = m^2d - 8q = 4q'$. Logo, $m^2d \equiv 4 \pmod 8$, assim, $m^2d + 1 \equiv 5 \pmod 8$. Pelo Teorema de Gauss, em cada caso os inteiros são soma de três inteiros quadrados.

□

Teorema 1.8.11. *Seja $K = \mathbb{Q}(\sqrt{-d})$, tal que, a álgebra de quatérnios $\mathbf{H}(K)$ é um anel de divisão. Se $m \equiv 2 \pmod 4$, então existem $p, q, r \in \mathbb{Z}$, tal que,*

$$u = m\sqrt{-d} + pi + qj + rk \in \mathcal{U}(\mathbf{H}(R)).$$

Demonstração.

A álgebra $\mathbf{H}(K)$ é um anel de divisão, portanto, pelo corolário 1.6.7, $d \equiv 7 \pmod 8$. Se $m \equiv 2 \pmod 4$, então, pela Proposição 1.8.10, $m^2d \pm 1$ é soma de três inteiros quadrados.

Sejam $p, q, r \in Z$, estes quadrados, assim $m^2d \pm 1 = p^2+q^2+r^2$. Se $u = m\sqrt{-d}+pi+qj+rk$, então a norma de u, $\eta(u) = -m^2d+p^2+q^2+r^2 = \pm 1$, logo, u é uma unidade de $\mathbf{H}(R)$. □

Definição 1.8.12. *Uma unidade u de $\mathbf{H}(R)$ cuja cardinalidade do suporte $l := |supp(u)| > 1$, $m\sqrt{-d}$ é o único coeficiente não inteiro de u, e $(m^2d \pm 1)$ é a soma de três quadrados, é denominada* ***unidade de Gauss****, ou l-****unidade de Gauss****.*

O seguinte resultado é evidente:

Proposição 1.8.13. *Seja $l = 2$ ou $l = 3$, u uma unidade de norma 1, e seja $d \equiv 7 \pmod 8$.*

u é uma l-unidade de Pell se, e somente se, u é uma l-unidade de Gauss.

Demonstração. Se u é uma 3-unidade de Pell, cujos coeficientes são $m\sqrt{-d}, p, q$, então $p^2 + q^2 + 0^2 = m^2d + 1$, logo $m^2d + 1$ é soma de três quadrados e u uma 3-unidade de Gauss. Analogamente, ocorre para uma 2-unidade de Pell, pois estamos no caso em que $d \equiv 7 \pmod 8$. A recíproca é imediata. □

Exemplo 1.8.14. *No artigo [8], as unidades obtidas para $\mathbf{H}(\mathbb{Z}(\frac{1+\sqrt{-7}}{2}))$, são de norma 1, apresentamos algumas unidades de norma -1. Segundo o teorema anterior, existem inteiros p, q, r, de modo que, $u = 6\sqrt{-7} + pi + qj + rk$ seja uma unidade. De fato, $\{(p, q, r) : (15, 5, 1), (13, 9, 1), (11, 11, 9)\}$, são todas as soluções inteiras, a menos de permutação de sinais e coordenadas, possíveis. Para $\mathbf{H}(\frac{1+\sqrt{-23}}{2})$, $u = 5\sqrt{-23} + 23i + 6j + 3k$ é uma unidade de norma -1.*

Também exibimos algumas unidades de Gauss, de norma $\eta(u) = 1$. Para $\mathbf{H}(\mathbb{Z}(\frac{\sqrt{-15}+1}{2}))$, existem inteiros p, q, r, de modo que, $u = 10\sqrt{-15} + pi + qj + rk$ seja uma unidade de norma 1. Com efeito, $(36, 14, 3), (36, 13, 6), (32, 21, 6), (30, 24, 5)$ são alguns dos valores de (p, q, r). Para $\mathbf{H}(\frac{1+\sqrt{-23}}{2})$, $u = 2\sqrt{-23}+8i+5j+2k$ é uma unidade de norma 1. Observe que $u = 3588\sqrt{-23} + 12168i + 12167j$ é uma unidade de Gauss, embora $4 \mid 3588$. Tal unidade é mais facilmente obtida como uma 3-unidade de Pell.

Se consideramos o anel de inteiros $R = \mathbb{Z}(\frac{1+\sqrt{-7}}{2})$, sua base integral é $\{1, \frac{1+\sqrt{-7}}{2}\}$. A unidade $\frac{m+\sqrt{-d}}{2} \pm (\frac{m-\sqrt{-d}}{2})i + pj$ é um tipo que não está na classe das unidades de Pell, ou de Gauss. Para aquelas de norma $\eta(u) = 1$, a solução da equação

$$m^2 + 2p^2 = 2 + d \qquad 1.8$$

em $\mathbb{Z}$, permite obter essas unidades. Para o caso $d = -7$, o conjunto S das unidades obtidas a partir dessas soluções, juntamente com as unidades triviais i e j, geram o grupo $SL_1(\mathbf{H}(R))$, como provado em [8]. Se v é uma unidade de $\mathbf{H}(R)$, de norma -1, então o grupo $\langle v, S\rangle = \mathcal{U}(\mathbf{H}(R))$ é o grupo de unidades de $\mathbf{H}(R)$. De fato, se $w \in \mathcal{U}(\mathbf{H}(R))$ e $\eta(w) = -1$, então $\eta(vw) = \eta(v)\eta(w) = 1$, logo $vw \in SL_1(\mathbf{H}(R))$, portanto $w \in \langle v, S\rangle$. Assim se $v = 5\sqrt{-23} + 23i + 6j + 3k$ é uma unidade de $\eta(v) = -1$, então, temos que, $\mathcal{U}(\mathbf{H}(\mathbb{Z}(\frac{1+\sqrt{-7}}{2}))) = \langle v, S\rangle = \mathcal{U}(\mathbf{H}(R))$.

No caso $d \neq 7$, temos unidades do tipo $\frac{m+\sqrt{-d}}{2} \pm (\frac{m-\sqrt{-d}}{2})i + pj$, que exemplificamos para $d = 15$ e $d = 31$.

Exemplo 1.8.15. *Se $d = 15$, a equação 1.8 escreve-se como $m^2 + 2p^2 = 17$, cuja soluções em $\mathbb{Z}$ são: $(m, p) \in \{(3, 2), (3, -2), (-3, 2), (-3, -2)\}$. Fixado $m = 3$, obtemos $p = 2$ ou $p = -2$, portanto, há 4 unidades possíveis. Cada coeficiente de u é distinto, logo há $6 \cdot 3!$, possibilidades para u, para um mesmo suporte. Sendo $d \equiv 7 \pmod 8$, pela proposição 1.8.1, se $u_1 \notin \{-1, 0, 1\}$, então u é de ordem infinita. Logo, para $1 \in supp(u)$, deve ocorrer que $\{i, j\} \subset supp(u)$, ou $\{i, k\} \subset supp(u)$, ou $\{j, k\} \subset supp(u)$, portanto há $3.36 = 108$ unidades dessa forma, que são de ordem infinita. A unidade*

$$\frac{3 + \sqrt{-15}}{2} + (\frac{3 - \sqrt{-15}}{2})j - 2k$$

é uma delas.

Se $1 \notin supp(u)$, então u é de torção, logo há 36 unidades deste tipo que são de torção. Uma delas é a unidade

$$(\frac{-3 - \sqrt{-15}}{2})i + (\frac{-3 + \sqrt{-15}}{2})j + 2k,$$

que é de ordem 4.

Exemplo 1.8.16. *Se $d = 31$, a equação 1.8 escreve-se como $m^2+2p^2 = 33$, cuja soluções em $\mathbb{Z}$ são: $(m, p) \in \{(1, 4), (1, -4), (-1, 4), (-1, -4)\}$. Analogamente, há 108 unidades que são de ordem infinita, e 36 unidades de torção.*

A equação $m^2 + 2p^2 = -2 + d$, para $d \equiv 7 \pmod 8$, não tem solução em $\mathbb{Z}$, pois suponha $(\overline{m}, \overline{p})$ uma solução em $\mathbb{Z}_8$. Teríamos $\overline{m}^2 - \overline{6}\overline{p}^2 = \overline{-3}$, portanto $3\overline{m}^2 = 2\overline{p}^2 - 1$, porém $2\overline{p}^2 - 1 \in \{\overline{1}, \overline{7}\}$, um absurdo. Portanto, as unidades u do tipo acima não são de norma $\eta(u) = -1$.

O seguinte resultado mostra uma aplicação para as unidades de Gauss.

Se u e v são 2-unidades de Gauss, cuja interseção entre os suportes é não vazia, e $supp(u) \cap supp(v) = \{1\}$, então $\langle u\rangle \cap \langle v\rangle = \{1\}$.

Teorema 1.8.17. *Sejam $K = \mathbb{Q}(\sqrt{-d})$, $d \equiv 7 \pmod 8$, e R o anel de inteiros de K. Se $u, v \in \mathcal{U}(\mathbf{H}(R))$ são 2-unidades de Gauss, e $supp(u) \cap supp(v) = \{1\}$. Então existe $m \in \mathbb{N}$, tal que, $\langle u^m, v^m\rangle$ é um grupo livre de posto 2.*

Demonstração.

Sendo $d \equiv 7 \pmod 8$, então, pelo Corolário 1.7.7, $\mathcal{U}(\mathbf{H}(R))$ é hiperbólico. Pelo Teorema 1.7.9, existe um natural m, tal que, $\langle u^m, v^m\rangle$ é um grupo livre de posto, no máximo, 2. Sendo u, v 2-unidades de Gauss, estas são 2-unidades de Pell, logo existem ϵ, ν invertíveis em $I_{\mathbb{L}}$, de modo que, $u = u_{(\epsilon)}$ e $v = v_{(\nu)}$. Por hipótese, $supp(u) \cap supp(v) = \{1\}$, e, pela Proposição 1.8.2 item (4), $\langle u_{(\epsilon)}\rangle = \langle u_{\langle\epsilon\rangle}\rangle$, logo $\langle u\rangle \cap \langle v\rangle = \{1\}$. Portanto, o posto de $\langle u^m, v^m\rangle$ é maior que 1, logo $\langle u^m, v^m\rangle$ é um grupo livre de posto 2. □

Capítulo 2

Álgebras de Semigrupos

No capítulo anterior, descrevemos uma certa classe de anéis R cujo grupo $\mathcal{U}_1(RG)$ é hiperbólico. Seja $\mathcal{A}$ uma álgebra finitamente gerada, e $\Gamma_0 \subset \mathcal{A}$ uma $\mathbb{Z}$-ordem. Se $\mathcal{U}(\Gamma_0)$ é um grupo hiperbólico, então $\mathcal{U}(\Gamma)$ é hiperbólico, para toda $\mathbb{Z}$-ordem $\Gamma \subset \mathcal{A}$. Isso ocorre, porque $\mathcal{U}(\Gamma_0)$ e $\mathcal{U}(\Gamma)$ são comensuráveis, e, pelo Teorema de Borel-Chandra ([4]), toda $\mathbb{Z}$-ordem de $\mathcal{A}$ é finitamente gerada.

Neste capítulo, classificamos os semigrupos S, tais que, para uma (portanto para toda) $\mathbb{Z}$-ordem Γ_0 de $\mathbb{Q}S$, uma $\mathbb{Q}$-álgebra unitária, ocorre que $\mathbb{Z}^2 \not\hookrightarrow \mathcal{U}(\Gamma_0)$, sendo $\mathcal{U}(\Gamma_0)$ o grupo de unidades de Γ.

2.1 A propriedade hiperbólica

Definição 2.1.1. *Seja $\mathcal{A}$ uma $\mathbb{Q}$-álgebra finitamente gerada, e seja Γ uma $\mathbb{Z}$-ordem de $\mathcal{A}$. Dizemos que a álgebra $\mathcal{A}$ satisfaz a propriedade hiperbólica quando*

$$\mathbb{Z}^2 \not\hookrightarrow \mathcal{U}(\Gamma).$$

Note que esta definição independe da ordem Γ, já que o grupo de unidades de duas ordens de $\mathcal{A}$ são comensuráveis. Vide $VIII.2.6$ de [15].

Inicialmente, apresentamos alguns resultados sobre uma $\mathbb{Q}$-Álgebra unitária $\mathcal{A}$ de dimensão finita sobre $\mathbb{Q}$. Denotamos por $\mathcal{S}(\mathcal{A})$, respectivamente $J(\mathcal{A})$, a sub-álgebra semi-simples, respectivamente o radical de $\mathcal{A}$, e $E(\mathcal{A}) = \{ E_1, \cdots, E_N\}, N \in \mathbb{Z}^+$ o conjunto completo de idempotentes centrais primitivos da sub-álgebra semi-simples $\mathcal{S}(\mathcal{A})$.

Um resultado clássico, devido a Wedderburn-Malĉev, garante-nos que

$$\mathcal{A} \cong \mathcal{S}(\mathcal{A}) \oplus J(\mathcal{A}).$$

Uma soma como espaços vetoriais. Nessas condições, temos que $\mathcal{A}$ é uma álgebra artiniana, e, logo, o seu radical $J(\mathcal{A})$ é um ideal nilpotente.

A seguir, mostramos que o radical de uma $\mathbb{Q}$-álgebra de dimensão finita e com a propriedade hiperbólica é 2-nilpotente.

Lema 2.1.2. *Seja $\mathcal{A}$ uma $\mathbb{Q}$-álgebra com a propriedade hiperbólica. Se J é o radical de $\mathcal{A}$, então $J^2 = 0$.*

Demonstração.

Inicialmente, provamos que se o radical é i-nilpotente, $i \in \mathbb{Z}^+$, então $i < 4$. Supomos, por absurdo, que $i \geq 4$. Sejam $x, y \in \mathcal{A}$, de modo que $x \in J^{i-2} \setminus J^{i-1}, y \in J^{i-1}$, e $\Gamma \subset A$ é uma $\mathbb{Z}$-ordem de A, tal que, existem $\alpha, \beta \in \mathbb{Z}$, e $\alpha x, \beta y \in \Gamma \cap J$. Como $x^2 \in J^{2i-4} = J^i J^{i-4}$, temos $x^2 = 0$. Analogamente, sendo $y^2 \in J^{2i-2} = J^i J^{i-2}$, temos $y^2 = 0$; como $xy \in J^{2i-3} = J^i J^{i-3}$ obtemos $xy = yx = 0$. Assim $\alpha x, \beta y$ são elementos nilpotentes, logo $(1 + \alpha x), (1 + \beta y) \in \mathcal{U}(\Gamma)$, de modo que $\langle 1 + \alpha x, 1 + \beta y \rangle \cong \mathbb{Z}^2$. Com efeito, $\forall n \in \mathbb{Z}$

$$\begin{cases} (1 + \alpha x)^n = 1 + n\alpha x, \text{ se } n > 0 \\ (1 + \alpha x)^n = 1 - n\alpha x, \text{ se } n < 0 \end{cases},$$

e, analogamente, para $(1 + \beta y)$, sendo portanto elementos de ordem infinita. Além disso $\langle 1 + \alpha x \rangle \cap \langle 1 + \beta y \rangle = \{1\}$, pois caso contrário existiriam $m, n \in \mathbb{Z}$, tal que, $(1 + \alpha x)^m = (1 + \beta y)^n \Rightarrow x = \frac{n\beta}{m\alpha} y \in J^{i-1}$, contrário à condição inicial sobre x. Porém, tais condições implicam que $\mathbb{Z}^2 \hookrightarrow \mathcal{U}(\Gamma)$, um absurdo. Portanto, $i < 4$. O mesmo argumento prova que $i \neq 3$. De fato, sejam $x \in J \setminus J^2$, $y \in J^2$, α, e β como acima, e suponha que $i = 3$.

$$\begin{cases} (1 + \alpha x)^n = 1 + n\alpha x + kx^2\alpha^2, \text{ com } k = \binom{n}{2}, \text{ se } n > 0 \\ (1 + \alpha x)^n = 1 - n\alpha x + kx^2\alpha^2, \text{ com } k = (n + \binom{|n|}{2}), \text{ se } n < 0 \end{cases},$$

logo, $1+\alpha x, 1+\beta y$ são livres de torção. Se existem inteiros positivos, tal que, $(1+\alpha x)^m = (1+\beta y)^n$, então $\pm m\alpha x + k(\alpha x)^2 = \pm n\beta y$. Multiplicamos a igualdade por y, $(\pm m\alpha x)y + (k\alpha^2 x^2)y = \pm n\beta y^2 = 0$, portanto, a condição $(k\alpha^2 y)x^2 = 0$ implica que $x^2 = 0$, e o resultado segue análogo. □

Corolário 2.1.3. *Seja $\mathcal{A}$ uma $\mathbb{Q}$-álgebra com a propriedade hiperbólica.*
Se $\mathcal{A} = \mathcal{S}(\mathcal{A}) \oplus J(\mathcal{A})$, então $dim_{\mathbb{Q}}(J(\mathcal{A})) \leq 1$, isto é, como sub-espaço vetorial de $\mathcal{A}$, $J(\mathcal{A}) = J$ tem, no máximo, dimensão igual a 1. Ademais, se $J \neq 0$, existe $j_0 \in \mathcal{A}$, e $J = \langle j_0, j_0^2 = 0\rangle_{\mathbb{Q}}$, e $1+J$ é isomorfo a $\mathbb{Q}$, como grupo multiplicativo.

Demonstração.

Pelo lema anterior, $J^2 = 0$. Se $J \neq 0$, e Γ é uma $\mathbb{Z}$-ordem em $\mathcal{A}$, sejam $x, y \in J \cap \Gamma$. Então o grupo $\langle 1+x, 1+y\rangle < \mathcal{U}(\Gamma)$ e $1+x, 1+y$ são elementos de ordem infinita. Sendo $\mathcal{U}(\Gamma)$ hiperbólico, temos que $\langle 1+x, 1+y\rangle \cong \mathbb{Z}$. Caso contrário, $\mathcal{U}(\Gamma)$ teria uma cópia de $\mathbb{Z}^2$. Portanto, a intersecção $\langle 1+x\rangle \cap \langle 1+y\rangle$ deve ser não trivial, isto é, existem m, n, tal que, $(1+x)^m = (1+y)^n$. Sendo x, y 2-nilpotentes, temos que $1+mx = 1+ny$, e, logo, $x = \frac{n}{m}y$. Assim o conjunto $\{x, y\}$ é $\mathbb{Q}$-linearmente dependente, portanto $dim_{\mathbb{Q}}(J) = 1$. Escreva $J = \mathbb{Q}j_0$, assim $1+J \cong \mathbb{Q}$. Com efeito, $\phi : 1+J \to \mathbb{Q}, \phi(1+qj_0) =: q$ é, tal que, $\phi(xy) = \phi((1+qj_0)(1+kj_0)) = \phi(1+(q+k)j_0) = q+k = \phi(x)+\phi(y)$. Portanto, ϕ é um homomorfismo que é bijetor. □

Se $\mathcal{A}$ é uma $\mathbb{Q}$-álgebra de dimensão finita e $\mathcal{A} = \mathcal{S}(\mathcal{A}) \oplus J(\mathcal{A})$, a decomposição de Wedderburn-Malĉev, então

$$\mathcal{A} = (\bigoplus_{E_i \in E(\mathcal{A})} \mathcal{S}(\mathcal{A})E_i) \oplus J(\mathcal{A}).$$

Suponha ainda que $J(\mathcal{A})$ tenha dimensão um sobre $\mathbb{Q}$. Se E é um idempotente da decomposição acima, sendo $J(\mathcal{A}) = \langle j_0\rangle$ um ideal de $\mathcal{A}$, então $j_0E \in J(\mathcal{A})$. Logo existe $\lambda \in \mathbb{Q}$, tal que, $j_0E = \lambda j_0$. Analogamente, existe $\mu \in \mathbb{Q}$, tal que, $Ej_0 = \mu j_0$.

Proposição 2.1.4. *Seja $\mathcal{A}$ uma $\mathbb{Q}$-álgebra não semi-simples com $dim(J(\mathcal{A})_{\mathbb{Q}}) = 1$, $J(\mathcal{A}) = \langle j_0 \rangle$ e $N = |E(\mathcal{A})|$. As seguintes afirmações são verdadeiras:*

(1) Para todo $x \in \mathcal{A}$, existem $\lambda_x, \mu_x \in \mathbb{Q}$, tal que, $xj_0 = \lambda_x j_0$ e $j_0 x = \mu_x j_0$.

(2) Se x é um idempotente, então $\lambda_x, \mu_x \in \{0, 1\}$.

(3) Se $J(\mathcal{A}) = \langle j_0 \rangle$, então existem únicos $E, F \in E(\mathcal{A})$, tal que $Ej_0 \neq 0$ e $j_0 F \neq 0$.

(4) Se $E = F$, então J é central.

(5) Se J é não-central, a menos de uma reordenação de índices, podemos supor que $E = E_1$, e $F = E_N$. Então $E_1 j_0 = j_0 E_N = j_0$.

Demonstração.

Se $x \in \mathcal{A}$, o radical J é um ideal bilateral de $\mathcal{A}$, logo, $xj_0 \in \langle j_0 \rangle_{\mathbb{Q}}$, e, portanto, existe $\lambda_x \in \mathbb{Q}$, tal que, $xj_0 = \lambda_x j_0$. Da mesma forma, $j_0 x = \mu_x j_0$.

Se x é um idempotente, e $xj_0 = \lambda_x j_0 = x^2 j_0 = x(xj_0) = x(\lambda_x j_0) = \lambda_x^2 j_0 x$, implica $(\lambda_x^2 - \lambda_x) j_0 = 0$, portanto, $\lambda_x^2 - \lambda_x = 0$. Logo, $\lambda_x \in \{0, 1\}$.

Sendo $1 = \sum_{1 \leq i \leq N} E_i$, então $1 \cdot j_0 = \sum_{1 \leq i \leq N} (E_i \cdot j_0) = \sum_{1 \leq i \leq N} (\lambda_i j_0) = (\sum_{1 \leq i \leq N} \lambda_i) j_0$, e, logo, $\sum_{1 \leq i \leq N} \lambda_i = 1$. Sendo cada E_i um idempotente, assim $\lambda_i \in \{0, 1\}$, que juntamente com a primeira condição: $\sum_{1 \leq i \leq N} \lambda_i = 1$, implica a existência de um único índice, m, $1 \leq m \leq N$, tal que, $\lambda_m = 1$, e os demais são todos nulos. Logo $E = E_m$ é único. A mesma técnica pode ser aplicada para a multiplicação à direita de j_0 por um idempotente $F \in E(\mathcal{A})$. Concluímos, de forma análoga, que existe um único $k, 1 \leq k \leq N$, tal que, $j_0 E_k = j_0$, e para os demais idempotentes $j_0 E_i = 0$ com $i \neq k$.

Se $E = F$, $E_m j_0 = E_k j_0$, pela unicidade, $m = k$, então $j_0 E_m = E_m j_0 = j_0$. Por outro lado, para $i \neq k$, temos $j_0 E_i = E_i j_0 = 0$. Portanto, J comuta com $\mathcal{S}(\mathcal{A})$ e, portanto, é central. O último item é imediato. □

Como conseqüência desse resultado:

Corolário 2.1.5. *Seja $\mathcal{A}$ uma $\mathbb{Q}$-álgebra não semi-simples com a propriedade hiperbólica. Então $J(\mathcal{A}) = \langle j_0 \rangle$ é central em $\mathcal{A}$ se, e somente se, existe um único $E \in E(\mathcal{A})$, e $Ej_0 = j_0E \neq 0$. Neste caso $Ej_0 = j_0 = j_0E$.*

Seja $\mathcal{A}$ uma $\mathbb{Q}$-álgebra com a propriedade hiperbólica, $N = |E(\mathcal{A})|$, e $E_1, E_N \in E(\mathcal{A})$, os idempotentes satisfazendo a relação $E_1j_0 = j_0E_N = j_0$. Podemos escrever, convenientemente a componente semi-simples $\mathcal{S}(\mathcal{A})$:

$$\mathcal{S}(\mathcal{A}) = \underbrace{(\bigoplus_{1<i<N} \mathcal{S}(\mathcal{A})E_i)}_{B} \oplus \underbrace{(\mathcal{S}(\mathcal{A})E_1 \oplus \mathcal{S}(\mathcal{A})E_N)}_{C} = B \oplus C.$$

Denotando-se $\mathcal{S}(\mathcal{A})E_i = \mathcal{A}_i, 1 \leq i \leq N$, escrevemos: $\mathcal{A} \cong B \oplus \mathcal{A}_1 \oplus \mathcal{A}_N \oplus J(\mathcal{A})$.

Vamos denotar Γ_0 uma $\mathbb{Z}$-ordem em $\mathcal{A}$, $\Gamma_0 \cong \Gamma_1 \oplus \cdots \oplus \Gamma_N \oplus j_0\mathbb{Z}$, onde cada Γ_i é uma $\mathbb{Z}$-ordem em $\mathcal{A}_i$ com $E_i \in \Gamma_i$.

Definimos uma aplicação

$$\begin{aligned} \varphi: \ \mathcal{A}_1 \oplus \mathcal{A}_N \oplus J(\mathcal{A}) &\to \begin{pmatrix} \mathcal{A}_1 & \mathbb{Q} \\ 0 & \mathcal{A}_N \end{pmatrix} \\ a_1E_1 + a_NE_N + qj_0 &\mapsto \begin{pmatrix} a_1 & q \\ 0 & a_N \end{pmatrix} \end{aligned}.$$

Desse modo φ é um isomorfismo, pois $\varphi(x+y) = \varphi(x) + \varphi(y)$, e sendo os idempotentes centrais e ortogonais, e verificadas as relações $E_Nj_0 = j_0E_1 = 0$ e $E_1j_0 = j_0E_N = j_0$, temos que
$\varphi(xy) = \begin{pmatrix} x_1y_1 & q_xy_N + q_yx_1 \\ 0 & x_Ny_N \end{pmatrix} = \varphi(x)\varphi(y)$. Portanto, φ é um homomorfismo, que é bijetor. Concluímos, portanto, que

$$\mathcal{A}_1 \oplus \mathcal{A}_N \oplus J(\mathcal{A}) \cong \begin{pmatrix} \mathcal{A}_1 & \mathbb{Q} \\ 0 & \mathcal{A}_N \end{pmatrix}.$$

Denote por M o anulador à esquerda de J em $\mathcal{A}_1$. Sendo $dim_{\mathbb{Q}}(J) = 1$, segue-se que M é um ideal próprio de $\mathcal{A}_1$: de fato seja $\{j_0\}$ uma $\mathbb{Q}$-base de J então, claramente, temos que

$M = Ann(j_0)$. Que M é fechado em relação à soma, é obvio. Agora, se $x \in M$ e $y \in \mathcal{A}_1$, então $yx \cdot j_0 = y \cdot (x \cdot j_0) = 0$. Sendo $dim_{\mathbb{Q}}(J) = 1$, existe $\lambda \in \mathbb{Q}$, tal que, $y \cdot j_0 = \lambda j_0$, então $xy \cdot j_0 = x \cdot \lambda j_0 = \lambda(x \cdot j_0) = 0$, e, portanto xy e $yx \in M$. Se $x \in \mathcal{A}_1$, então existe $\lambda_x \in \mathbb{Q}$, tal que $x \cdot j = \lambda_x j_0$, daí $x = (x - \lambda_x E_1) + \lambda_x E_1$ implica que $\mathcal{A}_1 = M \oplus \mathbb{Q}E_1$. Desse modo, $dim_{\mathbb{Q}}(M) + 1 = dim_{\mathbb{Q}}(\mathcal{A}_1)$. Sendo $\mathcal{A}$ uma $\mathbb{Q}$-álgebra simples devemos, portanto, ter que $M = \{0\}$ e $dim_{\mathbb{Q}}(\mathcal{A}_1) = 1$. Analogamente, obtemos que $\mathcal{A}_N \cong \mathbb{Q}$. Provamos assim o seguinte

Teorema 2.1.6. *Seja $\mathcal{A}$ uma $\mathbb{Q}$-álgebra não semi-simples com a propriedade hiperbólica. Se $J(\mathcal{A}) = \langle j_0 \rangle$ é não-central, então, a menos de uma reordenação, tem-se que $E_1 j_0 = j_0 E_N = j_0$, e $E_N j_0 = j_0 E_1 = 0$. Para os demais idempotentes $E_i, i \notin \{1, N\}$ temos que $E_i j_0 = j_0 E_i = 0$. Mais ainda $\mathcal{A}_1 \oplus \mathcal{A}_N \oplus J(\mathcal{A}) \cong \begin{pmatrix} \mathcal{A}_1 & J(\mathcal{A}) \\ 0 & \mathcal{A}_N \end{pmatrix} \cong \begin{pmatrix} \mathbb{Q} & \mathbb{Q} \\ 0 & \mathbb{Q} \end{pmatrix}$ é um ideal de $\mathcal{A}$.*

Denotamos por $T_2(\mathbb{Q}) := \begin{pmatrix} \mathbb{Q} & \mathbb{Q} \\ 0 & \mathbb{Q} \end{pmatrix}$, com a multiplicação usual de matrizes, que também denominamos a álgebra das matrizes triangulares superiores dois por dois sobre $\mathbb{Q}$.

Corolário 2.1.7. *Seja $\mathcal{A}$ uma $\mathbb{Q}$-álgebra com a propriedade hiperbólica, e, $|E(\mathcal{A})| = N$. Se J não é central, então temos que*

$$\mathcal{A} \cong B \oplus T_2(\mathbb{Q}) \cong \begin{pmatrix} \mathcal{A}_2 & 0 & 0 & \cdots & 0 \\ 0 & \mathcal{A}_3 & 0 & \cdots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \cdots & \mathcal{A}_{N-1} \end{pmatrix} \oplus \begin{pmatrix} \mathbb{Q} & \mathbb{Q} \\ 0 & \mathbb{Q} \end{pmatrix} \cong \begin{pmatrix} \mathbb{Q} & 0 & 0 & \cdots & \mathbb{Q} \\ 0 & \mathcal{A}_2 & 0 & \cdots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \cdots & \mathbb{Q} \end{pmatrix}.$$

Mais ainda, para cada $1 \leq i \leq N$, $\mathcal{A}_i$ é um corpo quadrático imaginário, ou $\mathcal{A}_i$ é uma álgebra de quatérnios totalmente definida cujo corpo maximal é um corpo quadrático.

Demonstração.

Pelo teorema anterior, B e $T_2(\mathbb{Q})$ são ideais, cuja soma direta resulta em $\mathcal{A}$. Considere

a aplicação

$$\varphi : \begin{pmatrix} \mathcal{A}_2 & 0 & 0 & \cdots & 0 \\ 0 & \mathcal{A}_3 & 0 & \cdots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \cdots & \mathcal{A}_{N-1} \end{pmatrix} \oplus \begin{pmatrix} \mathbb{Q} & \mathbb{Q} \\ 0 & \mathbb{Q} \end{pmatrix} \longrightarrow \begin{pmatrix} \mathbb{Q} & 0 & 0 & \cdots & \mathbb{Q} \\ 0 & \mathcal{A}_2 & 0 & \cdots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \cdots & \mathbb{Q} \end{pmatrix}.$$

$$\begin{pmatrix} a_2 & 0 & 0 & \cdots & 0 \\ 0 & a_3 & 0 & \cdots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \cdots & a_{N-1} \end{pmatrix} \oplus \begin{pmatrix} q_1 & q \\ 0 & q_N \end{pmatrix} \mapsto \begin{pmatrix} q_1 & 0 & 0 & \cdots & q \\ 0 & a_2 & 0 & \cdots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \cdots & q_N \end{pmatrix}.$$

;

de modo análogo à demonstração do Teorema 2.1.6, φ é um isomorfismo.

Seja Γ_0 a $\mathbb{Z}$-ordem em $\mathcal{A}$, e $E_1 + E_2 + \cdots E_N + j_0 = 1 + j_0 \in \mathcal{U}(\Gamma_0)$. Pelo Lema 2.1.2, $(1 + j_0)^n = 1 + nj_0$. Portanto, $\langle 1 + j_0 \rangle \cong \mathbb{Z}$.

Suponha que $\gamma_i \in \Gamma_i$ é um elemento de ordem infinita, e seja $\gamma = E_1 + \cdots + \gamma_i E_i + \cdots + E_N$, $1 < i < N$. Temos que $o(\gamma^n) = \infty$, $\langle 1 + j_0 \rangle \cong \mathbb{Z}$, e $\langle 1 + j_0 \rangle \cap \langle \gamma \rangle = \{1\}$. Sendo $\mathcal{A}_i \subset C_{\mathcal{A}}(J)$, o centralizador de J em $\mathcal{A}$, temos que $\langle 1+j_0 \rangle \times \langle \gamma_i \rangle \cong \mathbb{Z}^2$ é um subgrupo de $\mathcal{U}(\Gamma_0)$, o que contraria o fato de $\mathcal{A}$ ter a propriedade hiperbólica. Portanto $\mathcal{U}(\Gamma_i)$ é um grupo linear de torção, logo, é finito. Obviamente $|\mathcal{U}(\Gamma_1) \cong \mathcal{U}(\Gamma_N)| \leq 2$, pois, pelo teorema anterior $\mathcal{A}_1 \cong \mathcal{A}_N \cong \mathbb{Q}$. Portanto, pelo Lema 21.3 de [30], cada $\mathcal{A}_i$ é um corpo quadrático imaginário, ou uma álgebra de quatérnios totalmente definida cujo corpo maximal é um corpo quadrático. □

Se $\mathcal{A}$ tem a propriedade hiperbólica, e o radical $J \neq \{0\}$ é central, então a parte semi-simples de $\mathcal{A}$ é uma soma direta de anéis de divisão, porque se alguma componente não fosse anel de divisão, então teria componente de matrizes, mas $\mathbb{Z}$-ordens de matrizes têm sempre elementos de ordem infinita. Logo teríamos que $\mathbb{Z}^2 \hookrightarrow \mathcal{U}(\Gamma)$, para alguma $\mathbb{Z}$-ordem Γ de $\mathcal{A}$. Portanto, em qualquer caso, as componentes simples $\mathcal{A}_i, 1 \leq i \leq N$, da parte semi-simples de $\mathcal{A}$ são todas anéis de divisão.

Corolário 2.1.8. *Nas condições do corolário anterior, $\mathcal{U}(\Gamma_i)$ é um subgrupo finito. Além disso, se Γ é uma $\mathbb{Z}$-ordem de $\mathcal{A}$, então $\mathcal{U}(\Gamma)$ é comensurável com $\mathbb{Z} \times C_2 \times C_2 \times \prod H_i$, onde os H_i são grupos finitos. Em particular, $\mathcal{U}(\Gamma) = \Delta(\mathcal{U}(\Gamma))$, o FC-centro de $\mathcal{U}(\Gamma)$ (grupo de conjugação finita).*

Demonstração.

Tem-se pelo Teorema de Borel-Harishandra que $\mathcal{U}(\Gamma)$ é finitamente gerado. O resultado segue agora dos comentários anteriores. □

Provamos até aqui alguns resultados para álgebras não semi-simples de dimensão finita que satisfazem a propriedade hiperbólica. Um resultado semelhante ocorre para as álgebras semi-simples. O teorema seguinte exprime nosso resultado fundamental para as álgebras de dimensão finita com a propriedade hiperbólica.

Teorema 2.1.9. *Seja $\mathcal{A}$ uma $\mathbb{Q}$-álgebra de dimensão finita. Se $\mathcal{A}_i$ é uma componente semi-simples de $\mathcal{A}$, denote por F_i um subcorpo maximal de $\mathcal{A}_i$ e $\Gamma_i \subset \mathcal{A}_i$ uma $\mathbb{Z}$-ordem. As seguintes proposições são verdadeiras:*

(1) A álgebra $\mathcal{A}$ tem a propriedade hiperbólica, é semi-simples e livre de elementos nilpotentes se, e somente se,

$$\mathcal{A} \cong \oplus \mathcal{A}_i,$$

com $\mathcal{A}_i$ anel de divisão, e existe, no máximo, um índice i_0, tal que, $\mathcal{U}(\Gamma_{i_0})$ é um grupo infinito e hiperbólico.

(2) A álgebra $\mathcal{A}$ tem a propriedade hiperbólica, é semi-simples com elementos nilpotentes se, e somente se,

$$\mathcal{A} \cong (\oplus \mathcal{A}_i) \oplus M_2(\mathbb{Q}).$$

(3) A álgebra $\mathcal{A}$ tem propriedade hiperbólica, é não-semi-simples, com $J(\mathcal{A})$ central se, e somente se,

$$\mathcal{A} \cong (\oplus \mathcal{A}_i) \oplus J,$$

e $dim_{\mathbb{Q}}(J) = 1$.

(4) A álgebra $\mathcal{A}$ tem a propriedade hiperbólica, é não-semi-simples, com $J(\mathcal{A})$ não central se, e somente se,

$$\mathcal{A} \cong (\oplus \mathcal{A}_i) \oplus T_2(\mathbb{Q}),$$

e $dim_{\mathbb{Q}}(J) = 1$.

Em cada caso, ou $\mathcal{A} = F_i$ é um corpo quadrático imaginário, ou $\mathcal{A}_i$ é uma álgebra de quatérnios totalmente definida, e os somandos são ideais.

Demonstração.

Provaremos primeiro (2), pois (1) é conseqüência de (2). Os itens (3) e (4) são conseqüência direta dos resultados anteriores.

A álgebra $\mathcal{A}$ é semi-simples com elementos nilpotentes, logo $\mathcal{A} \cong \bigoplus M_{n_i}(D_i)$, sendo D_i anéis de divisão. Cada $n_i \leq 2$, porque se $n_i \geq 3$ os elementos $\theta_1 = e_{13}$ e $\theta_2 = e_{23}$, formam um conjunto $\mathbb{Q}$-LI, e, pelo Lema 1.2.17, $\mathbb{Z}^2 \hookrightarrow \mathcal{U}(\Gamma)$ que contraria a propriedade hiperbólica de $\mathcal{A}$.

Há no máximo uma componente $n_i = 2$. Caso contrário, existem $\mathcal{A}_1 = M_2(D_1)$ e $\mathcal{A}_2 = M_2(D_2)$, sendo D_1, D_2 anéis de divisão. Portanto, se $\Gamma_j \subset \mathcal{A}_j$ é uma $\mathbb{Z}$-ordem, existem nilpotentes $\theta_j \in \Gamma_j$, e analogamente teríamos que $\mathbb{Z}^2 \hookrightarrow \mathcal{U}(\Gamma_1) \times \mathcal{U}(\Gamma_2)$. Logo, a componente de $\mathcal{A}$ que não é um anel de divisão deve ser $M_2(D)$, se $D \neq \mathbb{Q}$, existem $u, v \in D$, tal que, o conjunto $\{ue_{12}, ve_{12}\}$ é $\mathbb{Q}$-LI. Logo, pelo lema 1.2.17, temos uma contradição. Portanto, $M_2(D) = M_2(\mathbb{Q})$.

Se Γ_0 é a $\mathbb{Z}$-ordem $\Gamma_0 = M_2(\mathbb{Z}) \oplus (\oplus\Gamma_i)$, então $\mathcal{U}(\Gamma_0) \cong GL_2(\mathbb{Z}) \times (\prod \mathcal{U}(\Gamma_i))$. Logo, $\mathcal{U}(\Gamma_i)$ é um subgrupo de torção de um grupo hiperbólico, portanto, pelo Corolário 1.2.13, cada $\mathcal{U}(\Gamma_i)$ é finito.

A recíproca é imediata.

Se $\mathcal{A}$ é semi-simples, livre de elementos nilpotentes, então $M_2(\mathbb{Q})$ não é uma componente de wedderburn na decomposição da álgebra. Podemos substituir esta componente por $\mathcal{A}_j$. Se uma $\mathbb{Z}$-ordem $\Gamma_j \subset \mathcal{A}_j$ é, tal que, $\mathcal{U}(\Gamma_j) = \infty$, então, de modo análogo ao anterior concluímos que para as demais $\mathbb{Z}$-ordens $\Gamma_i \subset \mathcal{A}_i, i \neq j, \mathcal{U}(\Gamma_i) < \infty$, isto prova (1). □

Proposição 2.1.10. *Seja $\mathcal{A}$ uma álgebra com a propriedade hiperbólica cujo radical J é não-trivial. Se $a \in \mathcal{A}$ é um elemento nilpotente, não nulo, então $a \in J$.*

Demonstração.

Pelo teorema anterior, $\mathcal{A} \cong B \oplus T_2(\mathbb{Q})$ (respectivamente $\mathcal{A} \cong B \oplus J$) se J é não-central, (respectivamente se J é central). Se $a \in \mathcal{A}$ e $a^2 = 0$, então $a \notin B$, pois cada $\mathcal{A}_i, 1 < i < N$, é anel de divisão, logo, $a \in T_2(\mathbb{Q})$, (respectivamente $a \in J$). É suficiente, portanto, considerar o caso onde J não é central. Seja $a = \begin{pmatrix} x & y \\ 0 & z \end{pmatrix}$; $a^2 = 0$ implica $x = z = 0$, e $y \in \mathbb{Q}$. Portanto, $a = \begin{pmatrix} 0 & y \\ 0 & 0 \end{pmatrix} \in J$. □

2.2 Semigrupos finitos

Definição 2.2.1. *Um semigrupo é um conjunto não vazio S, juntamente com uma operação binária associativa $* : S^2 \to S$. O conjunto $S^1 \doteq S \cup \{1\}$, tal que $\forall s \in S, s * 1 = 1 * s = s$, é um monóide, ou seja, um semigrupo com uma identidade. O conjunto $S^\theta \doteq S \cup \{\theta\}$, tal que, $\forall s \in S, s * \theta = \theta * s = \theta$, um elemento zero, é um semigrupo com um elemento zero.*

Para o que segue, S^θ é um semigrupo cujo elemento θ é um zero de S.

Um subconjunto $T \subseteq S$ é um subsemigrupo se a operação $*$ do semigrupo, restrita a T, é uma operação binária. Um semigrupo é nulo à direita se, para todo $x, y \in S$, $x \cdot y = y$. Um semigrupo S^θ é um semigrupo nulo se, para todo $x, y \in S$, $x \cdot y = \theta$.

Diz-se que um elemento $e \in S$, tal que, $e^2 = e$ é um idempotente. Denotamos por $E(S)$ o conjunto de idempotentes de S. Sejam $e, f \in E(S)$; dizemos que $e \leq f$ se $ef = fe = e$. Um idempotente $f \in E(S)$ é um idempotente primitivo se $f \neq 0$ e se $e \leq f$, implicar que $e = 0$ ou $e = f$. Seja T um subsemigrupo de S que, segundo a operação binária de S, é um grupo. Nesse caso, T é um subgrupo do semigrupo S. Se T é um subgrupo de S, o elemento neutro de T é um idempotente de S.

Seja S um semigrupo finito, e, $s \in S$. O semigrupo cíclico gerado por s é o subconjunto de S:

$$\langle s \rangle = \{s^n : n = 1, 2, \cdots\}.$$

Sendo S finito, existem inteiros positivos, n e k, tal que, $s^{n+k} = s^n$. Daí $s^{n+vk} = s^n$, para todo inteiro positivo v. Em particular $s^{n(1+k)} = s^n$. Assim, o subsemigrupo $\langle s \rangle$, contém um elemento a, tal que, $a^m = a$, para algum inteiro $m \geq 2$. Se $m \neq 2$, então $(a^{m-1})^2 = a^{m-1}a^{m-1} = aa^{m-1}a^{m-2} = a^{m-1}$, e, portanto temos o seguinte resultado:

Lema 2.2.2 ([7], §1.6)**.** *Todo subsemigrupo cíclico $\langle s \rangle$ de um semigrupo finito S contém um idempotente.*

Definição 2.2.3. *Seja S um semigrupo. Um elemento $a \in S$ é regular se $a \in aSa$; S é regular se todos os elementos de S são regulares.*

Por exemplo, todo idempotente é regular. Além disso, se a é regular em S, isto é, existe $x \in S$, tal que $a = axa$, então $\{ax, xa\} \subset E(S)$, e $aS^1 = aS$.

Definição 2.2.4. *Seja S um semigrupo, e sejam $x, y \in S$; x e y são inversos um do outro se*

$$xyx = x \quad e \quad yxy = y.$$

Um semigrupo inverso é um semigrupo em que todo elemento, exceto um zero, tem um único inverso.

Sejam $A, B \subseteq S$, e o produto $AB \doteq \{ab : a \in A, b \in B\}$. Um ideal à esquerda(direita), de um semigrupo S, é um subconjunto não vazio $A \subseteq S$, tal que, $SA \subseteq A (AS \subseteq A)$. Um conjunto A, que é um ideal à esquerda e à direita de S, é um ideal bilateral de S, que também nos referimos por ideal.

Definição 2.2.5 ([7], Seção 2.5)**.** *Seja S um semigrupo. Se K é um ideal minimal de S, então K é denominado o núcleo de S.*

Definição 2.2.6. *Seja I um ideal de S. O semigrupo de fatores de Rees, S/I, é o conjunto $(S \setminus I) \cup \{\theta\}$ sujeito à operação $\circ$ definida por*

$$s \circ t := \begin{cases} st, & \text{se } st \notin I \\ \theta, & \text{se } st \in I \end{cases}$$

Uma importante classe de ideais de S é aquela formada por ideais do tipo $J_s = S^1 s S^1, s \in S$, o ideal principal de S gerado por s.

O conjunto $I_s \doteq \{x : x \in J_s, J_s \neq J_x\}$ ou é um ideal de J_s, ou é vazio. Neste caso J_s é um ideal minimal de S.

Definição 2.2.7. *Seja S um semigrupo, $s \in S$, e, J_s o ideal gerado por s. O fator $S_s \doteq J_s/I_s$ é o fator principal de S determinado por $s \in S$, convencionando-se que se $I_s = \emptyset$, então $S_s = J_s$.*

Definição 2.2.8. *Um semigrupo S é simples, se não possui ideais próprios, S é 0-simples se não contém ideais próprios não nulos e não é um semigrupo nulo de cardinalidade 2. Um semigrupo 0-simples é completamente 0-simples se contém idempotentes primitivos. Um semigrupo S é semi-simples, se todo fator de S é simples ou 0-simples, e S é completamente semi-simples se seus fatores principais são semigrupos completamente simples ou 0-simples.*

Lema 2.2.9 ([7], Lema 2.39)**.** *Um fator principal de um semigrupo S é ou 0-simples, ou simples ou nulo. Somente se S tem um núcleo, existe um fator principal simples, e neste caso, o núcleo é o único fator principal simples.*

Definição 2.2.10. *Uma série principal de um semigrupo S é uma cadeia*

$$S = S_1 \supset S_2 \supset \cdots \supset S_n \supset S_{n+1} = \emptyset$$

de ideais S_i de S, tal que S_{i+1} é um ideal maximal de S_i, $1 \leq i \leq n$. Os semigrupos de fatores de Rees S_i/S_{i+1} são denominados fatores da série principal de S.

Proposição 2.2.11. *Cada fator S_i/S_{i+1} de uma série principal é isomorfo a algum fator principal de S.*

Demonstração.

Teorema 2.40, [7]. □

Os semigrupos S que são união de grupos aparecem, naturalmente, no contexto em que trabalhamos.

Teorema 2.2.12 ([7], Teorema 1.11)**.** *Seja S um semigrupo, $e = e^2 \in S$ um idempotente, e, H_e o grupo de unidades de SeS. Se G é um subgrupo de S, tal que, $H_e \cap G \neq \emptyset$, então $G \subseteq H_e$.*

Definição 2.2.13. *Um subgrupo G de um semigrupo S é denominado subgrupo maximal de S se não está propriamente contido em qualquer outro subgrupo de S.*

Segundo o teorema anterior, se e é um idempotente de S, então o grupo H_e é maximal. Pelo mesmo teorema os subgrupos maximais de um semigrupo S são dois a dois disjuntos.

Em [7], é indicado que os semigrupos S, que são união de subgrupos, são a união de subgrupos disjuntos. Diante deste fato, não há ambigüidade em referir-se a semigrupos que são união de subgrupos, ou união disjunta de subgrupos, indistintivamente. Demonstramos esta propriedade com o seguinte lema:

Lema 2.2.14 ([7], Clifford(1941))**.** *Se um semigrupo S é a união de grupos, então S é a união de disjunta de seus subgrupos maximais.*

Demonstração.

Seja I um conjunto de índices, tal que, $S = \bigcup_{i\in I} G_i$. Para cada $s \in S$, existe um índice $j \in I$, de modo que, $s \in G_j$. Seja $e_j \in G_j$ o elemento neutro deste grupo, portanto, um idempotente de S, e seja H_{e_j} o grupo de unidades de Se_jS. Pelo Teorema 2.2.12, H_{e_j} é um subgrupo maximal de S. Além disso $e_j \in G_j \cap H_{e_j}$, e, logo, segundo o mesmo teorema, $G_j \subseteq H_{e_j}$. Portanto $s \in H_{e_j}$, logo, $S = \bigcup_{j\in J\subseteq I} H_{e_j}$. □

Proposição 2.2.15. *Seja S^θ um semigrupo finito cujos fatores principais são isomorfos a grupos adjuntados com o zero θ, isto é, $S_i/S_{i+1} \cong G_i^\theta$. Então S^θ é a união disjunta de grupos.*

Demonstração.

Por indução sobre o número de fatores principais. Se $n = 1$ é óbvio; supondo verdadeiro para $n = k$, seja $n = k + 1$, e, $S = S_1 \supset S_2 \supset \cdots \supset S_{k+1}$, por hipótese $S_2 = \bigcup_{i=1}^{k-1} G_i$; $S_1/S_2 = S_1 \setminus S_2 \cup \{\theta\} \cong G_1^\theta$, portanto, $S^\theta = \bigcup G_i$. O lema anterior nos dá o resultado desejado. □

2.3 Semigrupo de matrizes de Rees e álgebras de Munn

Dado um grupo G, e $m, n \in \mathbb{N}$, consideramos o semigrupo G^θ e M o conjunto de matrizes $n \times m$, sobre G^θ. Existe um modo natural de definir, para um subconjunto adequado $\mathcal{M}^0 \subset M$, uma operação binária $\circ$, de modo que $\{\mathcal{M}^0, \circ\}$ seja um semigrupo. O semigrupo assim construído será denominado semigrupo de matrizes de Rees.

Definição 2.3.1. *Seja G um grupo, e I, Λ conjuntos arbitrários. Por uma matriz de Rees $I \times \Lambda$, entendemos uma matriz $I \times \Lambda$ sobre G^θ com no máximo uma única entrada não nula. Para $a \in G, i \in I$ e $\lambda \in \Lambda$, $(a)_{i\lambda}$ denota uma matriz de Rees $I \times \Lambda$ sobre G^θ, em que a é a entrada da matriz correspondente à linha i e à coluna λ e as demais entradas são todas nulas. Para qualquer $i \in I$ e $\lambda \in \Lambda$, a expressão $(\theta)_{i\lambda}$ denota a matriz nula $I \times \Lambda$, que também se denota por θ. Fixamos $P = (p_{\lambda i})_{\lambda i}$ uma matriz $\Lambda \times I$ sobre G^θ, denominada matriz sanduíche, e seja $\mathcal{M}^0$ o conjunto das matrizes de Rees $I \times \Lambda$ sobre G^θ. Em $\mathcal{M}^0$ definimos a seguinte operação:*

$$A \circ B = APB.$$

É imediato verificar que $\circ$ é uma operação binária associativa, portanto o conjunto $\{\mathcal{M}^0, \circ\}$ é um semigrupo. Denotamos este semigrupo por $\mathcal{M}^0(G; I, \Lambda; P)$. Sendo G denominado o grupo estrutural do semigrupo.

Um aspecto importante do semigrupo de matrizes de Rees, é a possibilidade de caracterizar os semigrupos completamente 0-simples. Seja S o semigrupo de matrizes de Rees $S = \mathcal{M}^0(G; I, \Lambda; P)$. O semigrupo S é regular se, e somente se, cada linha e cada coluna da matriz P tem uma entrada não nula, veja ([7], Lema 3.1).

Teorema 2.3.2 (Teorema de Rees)**.** *([7], Teorema 3.5) Um semigrupo é completamente 0-simples se, e somente se, é isomorfo a um semigrupo de matrizes de Rees, sobre um grupo com zero, que é regular.*

De modo análogo às matrizes de Rees, definimos as álgebras de matrizes de Munn:

Definição 2.3.3. *Seja R uma anel, e m, n inteiros positivos. Considere $\mathcal{M}(R, m, n, P)$ o conjunto de matrizes $m \times n$ sobre R. Para cada $A = (a_{ij}), B = (b_{ij}) \in \mathcal{M}(R, m, n, P)$ a adição é definida por $A + B = (a_{ij} + b_{ij})$, e a multiplicação por $AB = A \circ P \circ B$. Sendo P uma matriz $n \times m$, fixada, com entradas em R, e $\circ$ a operação usual de matrizes. O anel $\mathcal{M}(R, m, n, P)$ é chamado uma álgebra de tipo matriz sobre R ou uma álgebra de matriz sobre R. Se cada linha e cada coluna de P contém uma unidade de R, então a álgebra $\mathcal{M}(R, m, n, P)$ é chamada uma álgebra de Munn sobre R.*

2.4 Álgebras de semigrupos

Definição 2.4.1. *Seja K um corpo, e S um semigrupo. Pela álgebra KS de S sobre K, denominamos uma álgebra $\mathcal{A}$ sobre K que contém um subconjunto $\overline{S}$, que é tanto uma base de $\mathcal{A}$ quanto um semigrupo multiplicativo de $\mathcal{A}$ isomorfo a S. Seja S um semigrupo com um zero. Por álgebra contráctil K_0S de S sobre K, denominamos uma álgebra sobre K que contém uma base B, tal que, $B \cup \{0\}$ é um subsemigrupo de K_0S isomorfo a S.*

Lema 2.4.2. *([7], Lema 5.17) Seja S um semigrupo de matrizes de Rees $S = \mathcal{M}^0(G; m, n; P)$. A álgebra contráctil $K_0S \cong \mathcal{M}(KG; m, n; P)$.*

Exemplo 2.4.3. *Seja $\mathcal{M}^0(G; m, n; P)$ o semigrupo de Rees, para $G = \{1\}$ um grupo trivial, $n = m = 2$ e $P = \begin{pmatrix} x & y \\ z & w \end{pmatrix}$ a matriz sanduíche, com $\{x, y, z, w\} \subset \{1, 0\}$. Se considerarmos a restrição $xw - yz = \pm 1$, então: ou $x = w = 1$ e $yz = 0$; ou $xw = 0$ e $y = z = 1$. Logo existem quatro casos possíveis para o semigrupo $\mathcal{M}^0(\{1\}; 2, 2; P)$ cujos elementos são as matrizes elementares $e_{11}, e_{12}, e_{21}, e_{22}$ e θ, a matriz nula.*

- *O semigrupo M das matrizes elementares, quando P é a matriz identidade, e a operação $e_{ij} \circ e_{kl} = e_{ij}Pe_{kl} = e_{ij}e_{kl} = e_{il}\delta_{jk}$ é o produto usual das matrizes e_{ij} e e_{kl}.*
- *O semigrupo M' quando $x = w = 0$. A matriz sanduíche P é a matriz diagonal secundária. Se $\circ$ é a operação de M': $e_{ij} \circ e_{kl} := e_{ij}Pe_{kl}$, e σ é o ciclo (12), é imediato que $e_{ij}P = e_{i\sigma(j)}$ e $Pe_{ij} = e_{\sigma(i)j}$.*

- *O semigrupo M_{12}, quando, ou $y = 1$ e $z = 0$; ou $x = 1$ e $w = 0$. Com a operação $e_{i1} \circ e_{2j} = e_{ij}$, e o produto usual para os demais elementos.*

- *O semigrupo M_{21}, quando, ou $y = 0$ e $z = 1$; ou $x = 0$ e $w = 1$. Com a operação $e_{i2} \circ e_{1j} = e_{ij}$, e o produto é o usual para os demais elementos.*

Os semigrupos M e M' são isomorfos. De fato, a aplicação

$$\begin{array}{rccc} \varphi: & M & \longrightarrow & M' \\ & e_{ij} & \mapsto & e_{i\sigma(j)} \end{array},$$

é uma bijeção. Além disso,

$$\varphi(e_{ij}e_{kl}) = \varphi(e_{il}\delta_{jk}) = \varphi(e_{il})\delta_{jk} = \varphi(e_{il})\delta_{\sigma(j)\sigma(k)},\ \textit{pois, } \delta_{jk} = \delta_{\sigma(j)\sigma(k)};\ \textit{e}$$
$$\varphi(e_{ij}) \circ \varphi(e_{kl}) = e_{i\sigma(j)}Pe_{k\sigma(l)} = e_{i\sigma(j)}e_{\sigma(k)\sigma(l)} = e_{i\sigma(l)}\delta_{\sigma(j)\sigma(k)} = \varphi(e_{ij}e_{kl}).$$

Portanto, φ é um isomorfismo, ou seja, $M \cong M'$.

Os semigrupos M_{12}, M_{21} são isomorfos. Com efeito, para o ciclo $\sigma = (12)$,

$$\begin{array}{rccc} \varphi: & M_{12} & \longrightarrow & M_{21} \\ & (e_{ij}) & \mapsto & e_{\sigma(i)\sigma(j)} \end{array},$$

é, obviamente, uma aplicação bijetora. Também é um homomorfismo, porque se $j = k$, então $\varphi(e_{ij}e_{kl}) = \varphi(e_{il}) = e_{\sigma(i)\sigma(l)} = e_{\sigma(i)\sigma(j)}e_{\sigma(k)\sigma(l)} = \varphi(e_{ij})\varphi(e_{kl})$. Caso contrário, se $j = 1$ e $k = 2$, então $\varphi(e_{ij}e_{kl}) = \varphi(e_{il}) = e_{\sigma(i)\sigma(l)} = e_{\sigma(i)2}e_{1\sigma(l)} = e_{\sigma(i)\sigma(j)}e_{\sigma(k)\sigma(l)} = \varphi(e_{ij})\varphi(e_{kl})$. Se $j = 2$ e $k = 1$, então $\varphi(e_{ij}e_{kl}) = 0 = e_{\sigma(i)\sigma(j)}e_{\sigma(k)\sigma(l)} = \varphi(e_{ij})\varphi(e_{kl})$. Logo φ é um isomorfismo. Porém M_{12} e M_{21} não são isomorfos ao semigrupo M.

Obviamente, os elementos nilpotentes e_{12}, e_{21}, geram o semigrupo M, portanto, se considerarmos a álgebra contrátil $\mathbb{Q}_0M \cong \mathcal{M}(\mathbb{Q}, 2, P) \cong M_2(\mathbb{Q})$, os elementos nilpotentes de M geram $\mathbb{Q}_0M$, e, portanto, $\mathbb{Q}M$.

Lema 2.4.4. *Seja $\mathcal{M}^0(\{1\}, 2, P)$ um semigrupo de Rees, $M = \mathcal{M}^0(\{1\}, 2, P)$ quando $P = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$, e $M_{12} = \mathcal{M}^0(\{1\}, 2, P)$ quando $P = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$. As álgebra $\mathbb{Q}M$ e $\mathbb{Q}M_{12}$ são geradas por elementos nilpotentes.*

Demonstração.

Para o semigrupo M isso é óbvio. Os seguintes elementos de $\mathbb{Q}M_{12}$ são nilpotentes: $t_1 := \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}$ e $t_2 := \begin{pmatrix} 0 & 0 \\ -1 & 1 \end{pmatrix}$, pois

$$t_1^2 = [t_1]P[t_1] = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}\begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} = 0,$$

e $t_2^2 = [t_2]P[t_2] = 0$. Os demais elementos são: $t_1t_2 = \begin{pmatrix} -1 & 1 \\ 0 & 0 \end{pmatrix}$ e $t_2t_1 = \begin{pmatrix} 0 & 0 \\ 0 & -1 \end{pmatrix}$. O conjunto $S = \{t_1, t_2, t_1t_2, t_2t_1\}$ é $\mathbb{Q}$-LI e, portanto,

$$\mathbb{Q}S = \langle\{t_1, t_2, t_1t_2, t_2t_1\}\rangle$$

é uma álgebra gerada por nilpotentes. □

Se T é um ideal de um semigrupo S, então $\mathbb{Q}S/\mathbb{Q}T \cong \mathbb{Q}_0(S/T)$. Sendo $\{\theta\}$ um ideal de S, então $\mathbb{Q}S/\mathbb{Q}\theta \cong \mathbb{Q}_0S$. Segue-se que $\mathbb{Q}S \cong \mathbb{Q}_0S \oplus \theta\mathbb{Q}$. Portanto, a álgebra $\mathbb{Q}S$ é semi-simples se, somente se, $\mathbb{Q}_0S$ é semi-simples, ([7], Lema 5.13).

Proposição 2.4.5 ([7], Corolário 5.15)**.** *Se KS é semi-simples, então S é semi-simples.*

Exemplo 2.4.6. *Seja $N = \{e_{33}, e_{12}\}$. O semigrupo $S = N \cup \{\theta\}$ admite a série principal*

$$S \supset \{e_{12}, \theta\} \supset \{\theta\} \supset \emptyset.$$

Observe que o fator principal $\{e_{12}, \theta\}/\{\theta\} = \{e_{12}, \theta\}$ é um subsemigrupo nulo de S, logo $\mathbb{Q}S$ é não-semi-simples.

Seja S um semigrupo finito. Pela proposição anterior, se a álgebra $\mathbb{Q}S$ é semi-simples, então o semigrupo S é semi-simples, isto é, cada fator principal de S é simples ou 0-simples.

Para o que segue, supomos que $\mathbb{Q}S$ tem unidade.

Lema 2.4.7 ([7], Corolário 2.56)**.** *Todo semigrupo periódico (em particular, qualquer semigrupo finito) 0-simples é completamente 0-simples.*

Assim, pelo Teorema de Rees, Teorema 2.3.2, os semigrupos 0-simples são isomorfos a um semigrupo de Rees.

Proposição 2.4.8 ([7], Corolário 5.24)**.** *Seja S um semigrupo simples finito. Se a álgebra KS é semi-simples, então S é um grupo.*

Teorema 2.4.9 ([7], Teorema 5.14)**.** *A álgebra $\mathbb{Q}S$ é semi-simples se, e somente se, a $\mathbb{Q}$-álgebra $\mathbb{Q}(S_i/S_{i+1})$, de cada fator principal de S, é semi-simples.*

Lema 2.4.10. *Seja $\mathbb{Q}S$ uma álgebra semi-simples. Se S_i/S_{i+1} é um fator principal de S, então S_i/S_{i+1} é isomorfo a um semigrupo de matrizes de Rees.*

Demonstração.

Sendo $\mathbb{Q}S$ semi-simples, pelo Teorema 2.4.9, $\mathbb{Q}(S_i/S_{i+1})$ é semi-simples, isto é, S_i/S_{i+1} é um semigrupo simples ou 0-simples:

- Se o fator S_i/S_{i+1} é simples, pela Proposição 2.4.8, então este fator é um grupo, logo um semigrupo de matrizes de Rees;
- Se o fator S_i/S_{i+1} é 0-simples, sendo S_i/S_{i+1} finito, pelo Lema 2.4.7, S_i/S_{i+1} é completamente 0-simples, portanto pelo Teorema de Rees, 2.3.2, S_i/S_{i+1} é isomorfo a um semigrupo de matrizes de Rees.

□

Proposição 2.4.11 ([25], Corolário 5.26)**.** *Seja $S = \mathcal{M}^0(G; m, n; P)$ um semigrupo de matrizes de Rees. As seguintes condições são equivalentes:*

(1) A Álgebra $\mathbb{Q}_0S$ é unitária;

(2) $m = n$ e P é uma matriz invertível em $M_n(\mathbb{Q}G)$.

Teorema 2.4.12 ([23],6.1)**.** *Seja S um semigrupo finito, tal que, $\mathbb{Z}S$ contém uma identidade. Então $\mathcal{U}(\mathbb{Z}S)$ é finito se, e somente se, S é um semigrupo inverso, que é a união disjunta de grupos, que são ou abelianos de expoente $1, 2, 3, 4$ ou 6 ou são 2-grupos Hamiltonianos.*

Neste caso, a álgebra $\mathbb{Q}S$ é livre de elementos nilpotentes, isto é, se $|\mathcal{U}(\mathbb{Z}S)| < \infty$ então a álgebra $\mathbb{Q}S$ não contém elementos nilpotentes. Logo, o teorema não se aplica quando $\mathbb{Q}S$ é não-semi-simples, pois $J = \langle j_0 \rangle$ e $1 + \mathbb{Z}j_0 \cong \mathbb{Z}$.

Na classificação dos grupos G, cujo grupo $\mathcal{U}(\mathbb{Z}G)$ é hiperbólico (Ver Teorema 1.2.16.), existem grupos G cuja álgebra $\mathbb{Q}G$ não contém elementos nilpotentes, e $\mathcal{U}(\mathbb{Z}G)$ é um grupo infinito. Portanto, mesmo para a condição semi-simples o teorema acima não descreve este caso.

A seguir determinamos a estrutura do semigrupo S finito cuja álgebra $\mathbb{Q}S$ tenha a propriedade hiperbólica. Um resultado que auxilia nessa direção é o seguinte teorema. (Veja [9].)

Teorema 2.4.13. *Seja $\mathbb{Q}S$ uma álgebra semi-simples. Se*

$$S = S_1 \supset S_2 \supset \cdots \supset S_n \supset S_{n+1} = \emptyset$$

é uma séria principal de S. Então cada fator principal é um semigrupo simples ou completamente 0-simples, e $S_i/S_{i+i} \cong \mathcal{M}^0(G_i; n_i, n_i; P_i)$,$1 \leq i \leq n$, P_i é uma matriz invertível em $M_{n_i}(\mathbb{Q}G_i)$, sendo cada G_i um subgrupo maximal de S. Além do mais,

$$\mathbb{Q}_0 S \cong \bigoplus_i M_{n_i}(\mathbb{Q}G_i).$$

é uma decomposição da álgebra $\mathbb{Q}_0 S$ cujos fatores $M_{n_i}(\mathbb{Q}G_i)$ são isomorfos a ideais de $\mathbb{Q}S$.

Demonstração.

A série principal de S define uma cadeia de ideais da $\mathbb{Q}$-álgebra $\mathbb{Q}S$;

$$\mathbb{Q}S = \mathbb{Q}S_1 \supset \mathbb{Q}S_2 \supset \cdots \supset \mathbb{Q}S_n \supset \mathbb{Q}S_{n+1} = \{0\}.$$

Sendo cada S_i um ideal de S, temos que $\mathbb{Q}S_i/\mathbb{Q}S_{i+i} \cong \mathbb{Q}_0(S_i/S_{i+i})$. Pelo Lema 2.4.10, cada fator principal $S_i/S_{i+1} \cong \mathcal{M}^0(G_i; m_i, n_i; P_i)$, portanto, pelo Lema 2.4.2, $\mathbb{Q}_0(S_i/S_{i+i}) \cong \mathbb{Q}\mathcal{M}^0(G_i; m_i, n_i; P_i) \cong \mathcal{M}(\mathbb{Q}G_i; m_i, n_i; P_i)$. Sendo a álgebra unitária, pela Proposição 2.4.11, $\mathcal{M}(\mathbb{Q}G_i; m_i, n_i; P_i) \cong M_{n_i}(\mathbb{Q}G_i)$, a álgebra usual de matrizes sobre $\mathbb{Q}G_i$. Cada fator $\mathbb{Q}_0(S_i/S_{i+1})$ é simples, logo,

$$\mathbb{Q}_0 S \cong \bigoplus_i \mathbb{Q}_0(S_i/S_{i+1}) \cong \bigoplus_i M_{n_i}(\mathbb{Q}G_i).$$

□

Sendo $\mathbb{Q}S \cong \mathbb{Q}_0 S \oplus \theta\mathbb{Q}$, os resultados do teorema são válidos para $\mathbb{Q}S$.

Definição 2.4.14 ([25], págs. 82,83)**.** *Sejam $x, y, w_1, w_2, \cdots$ elementos de um semigrupo S. Considere a seqüência de elementos definida, indutivamente, como segue:*

$$\begin{array}{ll} x_0 = x & y_0 = y; \\ x_{n+1} = x_n w_{n+1} y_n & y_{n+1} = y_n w_{n+1} x_n, \text{ para } n \geq 0 \end{array}.$$

Dizemos que a identidade $X_n = Y_n$ é satisfeita em S se $x_n = y_n, \forall x, y, w_1, w_2, \cdots \in S$. Um semigrupo é chamado fracamente nilpotente de classe n, se satisfaz a identidade $X_n = Y_n$ e n é o menor inteiro positivo com esta propriedade. Um semigrupo S^θ é nilpotente se existe $n \in \mathbb{Z}^+$, tal que, $S^n = \{\theta\}$. Se $s \in S$ e $s^n = \theta$, então dizemos que s é n-nilpotente, ou simplesmente nilpotente.

Inicialmente vamos estudar o caso em que a álgebra $\mathbb{Q}S$ é semi-simples e não possui elementos nilpotentes. Neste caso, a ordem das matrizes do teorema anterior é $n_i = 1, 1 \leq i \leq n$, sendo n o número de componentes dadas pelo Teorema 2.4.13.

Lema 2.4.15. *Seja S um semigrupo finito. A álgebra $\mathbb{Q}S$ é livre de elementos nilpotentes se, e somente se, S admite uma série principal, tal que, cada fator principal é isomorfo a um subgrupo maximal G de S, e $\mathbb{Q}G$ é livre de elementos nilpotentes. Em particular, S é a união disjunta de seus subgrupos maximais.*

Demonstração.

Seja

$$S = S_1 \supset S_2 \supset \cdots \supset S_n \supset S_{n+1} = \emptyset,$$

uma série principal de S, e seja

$$\mathbb{Q}S = \mathbb{Q}S_1 \supset \mathbb{Q}S_2 \supset \cdots \supset \mathbb{Q}S_n \supset \mathbb{Q}S_{n+1} = \{0\},$$

a cadeia de ideais da álgebra $\mathbb{Q}S$ originada pela série. Pelo Teorema 2.4.13, $\mathbb{Q}_0(S_i/S_{i+1}) \cong M_{n_i}(\mathbb{Q}G_i)$. Sendo $\mathbb{Q}S$ livre de elementos nilpotentes, $n_i = 1$, e, $\mathbb{Q}_0(S_i/S_{i+1}) \cong \mathbb{Q}G_i$. Como $\mathbb{Q}S$ é semi-simples, a Proposicao 2.4.5 permite-nos distingüir dois casos:

- S_i/S_{i+1} é simples. Portanto, $S_i/S_{i+1} \cong H_i$ é um grupo;
- S_i/S_{i+1} é 0-simples. Logo $S_i/S_{i+1} \cong \mathcal{M}^0(G_i, n_i, P_i)$ com P_i invertível em $M_{n_i}(\mathbb{Q}G_i)$. Sendo $n_i = 1$, então $S_i/S_{i+1} \cong G_i$ é um grupo.

Assim, cada fator principal de S é isomorfo a um grupo. Logo, pelo Corolário 2.2.15, concluímos que S é a união disjunta de seus grupos maximais.

Reciprocamente, se S é um semigrupo com uma série principal cujos fatores principais são $S_i/S_{i+1} \cong G_i$. Então, pelo Teorema de Maschke, $\mathbb{Q}_0(S_i/S_{i+1}) \cong \mathbb{Q}G_i$ é semi-simples, logo, pelo Teorema 2.4.9, $\mathbb{Q}S$ é semi-simples, e, pelo teorema 2.4.13, cada $\mathbb{Q}G_i$ é isomorfo a um ideal de $\mathbb{Q}S$. Sendo $\mathbb{Q}G_i$ livre de elementos nilpotentes, para cada G_i, concluímos que a álgebra $\mathbb{Q}S$ é livre de nilpotência.

□

O problema do isomorfismo, para as álgebras de semigrupos sobre $\mathbb{Q}$, tem resposta negativa mesmo para o caso abeliano, como ilustra o seguinte exemplo:

Exemplo 2.4.16. *Sejam f, g elementos de ordem 2 e os semigrupos $S = \langle f \rangle \cup \langle g \rangle \cup \{\theta\}$ e $S' = \{e_{11}, e_{22}, e_{33}, e_{44}\} \cup \{\theta\}$, sendo e_{ii} matrizes 4 por 4 com entrada 1 na posição ii e 0, nas demais. A operação, em S, é a usual, se os elementos estão no mesmo grupo, e θ caso contrário. Para S', a operação é o produto usual de matrizes. Nessas condições, $\mathbb{Q}S \cong \mathbb{Q} \oplus \mathbb{Q} \oplus \mathbb{Q} \oplus \mathbb{Q} \oplus \mathbb{Q} \cong \mathbb{Q}S'$, porém os semigrupos não são isomorfos, pois todo elemento de S' é idempotente, enquanto S não tem tal propriedade.*

No entanto, pode ocorrer que alguma propriedade do semigrupo seja preservada. É o que ocorre, para um semigrupo finito S, com relação a união de seus grupos maximais, quando a álgebra $\mathbb{Q}S$ é livre de elementos nilpotentes.

Corolário 2.4.17. *Seja S' um semigrupo que é a união disjunta de grupos, cuja álgebra $\mathbb{Q}S'$ é livre de elementos nilpotentes. Se $\mathbb{Q}S \cong \mathbb{Q}S'$, então S é a união disjunta de grupos.*

Demonstração.

Sendo $\mathbb{Q}S'$ livre de nilpotência, $\mathbb{Q}S$ também é livre de nilpotentes, pelo teorema anterior S é a união disjunta de grupos. □

2.5 Álgebras de semigrupos com a propriedade hiperbólica

Os teoremas seguintes classificam os semigrupos finitos S cuja álgebra $\mathbb{Q}S$ tem a propriedade hiperbólica. Inicialmente supomos que $\mathbb{Q}S$ é livre de elementos nilpotentes. Com os resultados obtidos, prosseguimos com a caracterização de S, para os casos mais gerais.

Teorema 2.5.1. *A álgebra $\mathbb{Q}S$ é livre de elementos nilpotentes e satisfaz a propriedade hiperbólica se, e somente se, S admite uma série principal, onde cada fator é isomorfo a quaisquer dos grupos abaixo:*

(1) um grupo abeliano de expoente dividindo 4 ou 6;

(2) um 2-grupo hamiltoniano;

(3) um dos grupos cíclicos C_5, C_8 ou C_{12}.

Além disso, S deve conter, no máximo, um dos grupos do item (3). Ademais, S é um semigrupo inverso e é a união disjunta de grupos do tipo (1),(2) ou (3).

Demonstração.

Sendo $\mathbb{Q}S$ livre de elementos nilpotentes, a álgebra é semi-simples. A álgebra $\mathbb{Q}S$ tem a propriedade hiperbólica, pelo Lema 2.4.15, $\mathbb{Q}_0S = \bigoplus_i \mathbb{Q}G_i$, onde cada $\mathbb{Q}G_i$ é isomorfo a um ideal de $\mathbb{Q}S$. Se $\Gamma_0 = \bigoplus \Gamma_i \cong \bigoplus \mathbb{Z}G_i$, então, pelo Teorema 2.1.9 item (1), existe, no máximo, uma componente j, tal que, $|\mathcal{U}(\Gamma_j)| = \infty$. Há duas possibilidades:

- No primeiro caso, cada componente $\mathcal{U}(\mathbb{Z}G_i)$ é um grupo finito, e, pelo Teorema 1.1.4, G_i é um grupo abeliano de expoente dividindo 4 ou 6, ou G_i é um 2-grupo hamiltoniano.
- No segundo caso, $\mathcal{U}(\Gamma_j) = \mathcal{U}(\mathbb{Z}G_j)$ é infinito e $\mathcal{U}(\Gamma_j) \hookrightarrow \mathcal{U}(\Gamma_0)$ que é hiperbólico, logo, $\mathcal{U}(\Gamma_j)$ é hiperbólico. Pelo Teorema 1.2.16, $G_j \in \{C_5, C_8, C_{12}\}$.

Portanto, cada G_i é abeliano de expoente dividindo 4 ou 6, ou um 2-grupo hamiltoniano, e, para um único j, G_j é um dos grupos cíclicos C_5, C_8 ou C_{12}. Sendo cada grupo isomorfo a um fator principal de S. Pela Proposição 2.2.15, $S = (\dot{\bigcup} G_i) \dot{\cup} G_j$. Logo, todo elemento de $s \in S$ admite inverso e, sendo $\mathcal{U}(\mathbb{Z}S) \subset \mathcal{U}(\Gamma_0)$, temos que s tem um único inverso. Portanto, S é um semigrupo inverso.

Reciprocamente, seja S um semigrupo com uma série principal em que cada fator principal $S_i/S_{i+1} \cong G_i$. Pelo Teorema 2.4.13, $\mathbb{Q}_0S \cong \bigoplus \mathbb{Q}_0(S_i/S_{i+1}) \cong \bigoplus \mathbb{Q}G_i$. Portanto $\mathcal{U}(\Gamma_0) \cong \prod \mathcal{U}(\mathbb{Z}G_i)$. Por hipótese, no máximo um grupo G_j é cíclico de ordem $5, 8$ ou 12, e, para os demais, $\mathcal{U}(\mathbb{Z}G_i)$ é trivial. Assim, no máximo uma componente Γ_j é, tal que, $\mathcal{U}(\Gamma_j)$ é infinito e hiperbólico. Portanto, pelo Teorema 2.1.9 item (1), a álgebra $\mathbb{Q}S$ tem a propriedade hiperbólica. □

Se uma álgebra $\mathcal{A}$, com a propriedade hiperbólica, admitir elementos nilpotentes, pode, ou não, ocorrer que ela seja semi-simples. Neste último caso, pelo Teorema 2.1.9, a decomposição de Wedderburn-Malĉev deve ter uma única componente isomorfa a $M_2(\mathbb{Q})$. Para as demais componentes, o grupo de unidades de toda $\mathbb{Z}$-ordem, de alguma dessas componentes, deve ser um grupo finito. O teorema a seguir classifica os semigrupos finitos cuja álgebra $\mathbb{Q}S$ tem estas propriedades.

Teorema 2.5.2. *Seja $\mathbb{Q}S$ uma álgebra com elementos nilpotentes. A álgebra $\mathbb{Q}S$ é semi-simples e tem a propriedade hiperbólica se, e somente se, S admite uma série principal, onde cada fator é isomorfo a grupos G, e um único semigrupo K determinado por uma das seguintes condições:*

(1) G é um grupo abeliano de expoente dividindo 4 ou 6

(2) G é um 2-grupo hamiltoniano.

(3) K é um grupo do conjunto $\{S_3, D_4, Q_{12}, C_4 \ltimes C_4\}$;

(4) K é um ideal de S, dado por:

$$\mathcal{M}^0(\{1\}, 2, I_d) = M \qquad ou \qquad \mathcal{M}^0(\{1\}, 2, \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}) = M_{12}$$

Em particular S é a união disjunta dos grupos do item (1) e 2, e o semigrupo K.

Demonstração.

Se $\mathbb{Q}S$ é semi-simples, então, pelo Teorema 2.4.13, $\mathbb{Q}_0(S_i/S_{i+1}) \cong M_{n_i}(\mathbb{Q}G_i)$. Se $\mathbb{Q}S$ tem elementos nilpotentes, então existem duas possibilidades para S: ou S é livre de elementos nilpotentes ou S contém elementos nilpotentes.

Se S é livre de elementos nilpotentes, então $n_i = 1$, para todo i. Com efeito, suponha que $n_i > 1$, para algum i. Pelo Teorema 2.1.9 item (2),

$$\mathbb{Q}S \cong M_2(\mathbb{Q}) \oplus \mathcal{A}_i, \qquad 2.5$$

sendo cada $\mathcal{A}_i$ um anel de divisão. Logo, existe um único $n_j = 2$, e $M_2(\mathbb{Q}G_j) \cong M_2(\mathbb{Q})$, e, portanto, $G_j = \{1\}$ é um grupo trivial. Pelo Teorema 2.4.13, o fator principal $S_j/S_{j+1} \cong \mathcal{M}^0(\{1\}, 2, P)$, sendo P uma matriz invertível. Se $P = \begin{pmatrix} x & y \\ z & w \end{pmatrix}$, e $x, y, z, w \in \{0, 1\}$, para $xw - yz = \pm 1$, então

$$P \in \left\{ I_d, \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \right\} \bigcup \left\{ \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix} \right\}.$$

Desse modo $\mathcal{M}^0(\{1\}, 2, P)$ é isomorfo a um dos semigrupos do Exemplo 2.4.3: $M = \{e_{11}, e_{12}, e_{21}, e_{22}\} \cup \{\theta\}$ ou M_{12}. Como ambos contêm elementos nilpotentes, e o subsemigrupo S não contém elementos nilpotentes, temos um absurdo.

Logo, se S é livre de nilpotentes, então $n_i = 1$, para todo i. Assim cada fator principal é isomorfo a um grupo, e deve existir um único $G_j = K$, tal que, $M_2(\mathbb{Q})$ seja a única componente de Wedderburn da álgebra $\mathbb{Q}K$. Por hipótese, a $\mathbb{Z}$-ordem $\Gamma_0 = \mathbb{Z}S = \oplus\mathbb{Z}G_i \oplus \mathbb{Z}K \subset \mathbb{Q}S$ é tal que $\mathcal{U}(\Gamma_0)$ é hiperbólico, logo $\mathbb{Z}^2 \not\hookrightarrow \mathcal{U}(\mathbb{Z}K)$. Logo, pelo teorema 1.2.16, $K \in \{S_3, D_4, Q_{12}, C_4 \ltimes C_4\}$.

Se S contém elementos nilpotentes, então existe um único j, tal que, $n_j = 2$ e, como já visto, $S_i/S_{i+1} \cong G_i, i \neq j$ e $S_j/S_{j+1} \cong \mathcal{M}^0(\{1\}, 2, P)$. Afirmamos que S_j/S_{j+1} é um ideal de S. De fato, se $P = I_d$, então $\mathcal{M}^0(\{1\}, 2, P) = M$. Como na expressão 2.5, cada componente $\mathcal{A}_i$ é anel de divisão, os elementos nilpotentes de $\mathbb{Q}S$ estão em $M_2(\mathbb{Q})$. Pelo Lema 2.4.4, $\mathbb{Q}M$ é gerado por elementos nilpotentes. Portanto, $\mathbb{Q}_0M \subset M_2(\mathbb{Q})$. Mas $M \setminus \{\theta\}$ é uma $\mathbb{Q}$-base de $M_2(\mathbb{Q})$, logo, $\mathbb{Q}_0M = M_2(\mathbb{Q})$ e $\mathbb{Q}M = \mathbb{Q}\theta \oplus M_2(\mathbb{Q})$. Se $s \in S$ e $m \in M$, então $sm \in s\mathbb{Q}M \subseteq \mathbb{Q}M$, de modo que $sm = \lambda\theta + x_1t_1 + x_2t_2 + x_3t_1t_2 + x_4t_2t_1$. Se $sm \notin M$, então $\{sm\} \cup M$ é um subconjunto L.I. de $\mathbb{Q}M$, um absurdo. Portanto, $SM \subset M$, e da mesma forma, $MS \subset M$. Portanto, $K := M$ é um ideal de S.

No outro caso, $P = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$, e temos que $\mathcal{M}^0(\{1\}, 2, P) = M_{12}$. Pelo Lema 2.4.4, a álgebra $\mathbb{Q}M_{12}$ é gerada por elementos nilpotentes. Analogamente, $K := M_{12}$ é um ideal de S.

Sendo K ideal de S, temos $\mathbb{Q}S/\mathbb{Q}K \cong \mathbb{Q}_0(S/K) \cong (\oplus\mathbb{Q}G_i)$ e, pelo Teorema 2.5.1, cada fator principal de S/K, é isomorfo a G_i, que são grupos abelianos de expoente dividindo 4 ou 6, ou 2-grupo hamiltoniano. Portanto, os fatores S_i/S_{i+1} são os grupos G_i e o semigrupo K. Além disso, pela Proposição 2.2.15, $S/K \cong \dot{\bigcup} G_i$, e, portanto, $S \cong (\dot{\bigcup} G_i)\dot{\cup} K$.

Reciprocamente, cada fator principal $S_i/S_{i+1} \cong G_i$, portanto, $\mathbb{Q}_0(S_i/S_{i+1})$ é semi-simples, logo, $\mathbb{Q}S$ é semi-simples. Pois, pelo Teorema 2.4.13, cada fator principal é isomorfo a um semigrupo de matrizes de Rees.

Analisamos o 1^o caso, onde K é um grupo. Por hipótese, S é um semigrupo que admite uma série principal, onde cada fator $S_i/S_{i+1} \cong G_i$, isto é, $G_i \cong S_i/S_{i+1} \cong \mathcal{M}^0(G_i, n_i, P)$, logo $n_i = 1$ para todo i. Portanto $\mathbb{Q}_0S \cong \oplus\mathbb{Q}G_i$. Se Γ_0 é a $\mathbb{Z}$-ordem $\oplus\mathbb{Z}G_i \subset \oplus\mathbb{Q}G_i$, então $\mathcal{U}(\Gamma_0) = \prod \mathcal{U}(\mathbb{Z}G_i)$. Por hipótese, no máximo um fator principal $S_j/S_{j+1} \cong K \in \{S_3, D_4, Q_{12}, C_4 \ltimes C_4\}$, e $\mathcal{U}(\mathbb{Z}K)$ é um grupo hiperbólico, logo, pelo teorema 2.1.9, $\mathbb{Q}K$ contém uma única componente de Wedderburn que é $M_2(\mathbb{Q})$ e as demais são anéis de divisão $\mathcal{A}_{k_i}$ cuja $\mathbb{Z}$-ordem Γ_{k_i} é, tal que, $\mathcal{U}(\Gamma_{k_i})$ é finito. Para $G_i \neq K$, sendo $\mathcal{U}(\mathbb{Z}G_i)$ trivial, então $\mathbb{Q}S$ está nas condições da recíproca do Teorema 2.1.9 item

(2), e, portanto, $\mathbb{Q}S$ tem a propriedade hiperbólica.

No 2^o caso, em que algum fator $S_j/S_{j+1} = K$ não é um grupo, então $K = M$ ou M_{12}, e $S = (\cup G_i \cup K)$. Para cada fator principal, de S, S_i/S_{i+1}, com $i \neq j$, definimos $\overline{S}_i/\overline{S}_{i+1} := (S_i/K)/(S_{i+1}/K)$. Afirmamos que estes são os fatores principais do semigrupo S/K. Com efeito, seja

$$S = S_1 \supset S_2 \supset \cdots \supset S_j \supset S_{j+1} \supset \cdots \supset S_n \supset \{\theta\} \supset \emptyset,$$

a série principal de S, cujos fatores são os grupos G_i, para $i \neq j$ e K, para $i = j$. Se $i \neq j$, então $\overline{S}_i/\overline{S}_{i+1} \cong S_i/S_{i+1} \cong G_i$. Se $i = j$, então $\overline{S}_j/\overline{S}_{j+1} = \emptyset$, portanto $S_j/K = S_{j+1}/K$ e

$$S = S_1/K \supset S_2/K \supset \cdots \supset S_{j-1}/K \supset S_{j+1}/K \supset \cdots \supset S_n/K \supset \{\theta\} \supset \emptyset,$$

é uma série principal de S/K.

Logo, cada fator principal de S/K é isomorfo a G_i, portanto, $S/K \cong \cup G_i$. Nas condições dos grupos G_i, $\mathbb{Q}(S/K)$ é livre de elementos nilpotentes, e, pelo Lema 2.4.15, $\mathbb{Q}(S/K)$ tem a propriedade hiperbólica, logo, pelo Teorema 2.1.9 item (1), $\mathbb{Q}(S/K) \cong \oplus\mathcal{A}_i$. Portanto, $\mathbb{Q}S \cong \mathbb{Q}K \oplus \mathcal{A}_i \cong M_2(\mathbb{Q}) \oplus (\oplus\mathcal{A}_i)$. Ocorre que $\mathcal{A}_i \cong \mathbb{Q}G_i$ é, tal que, $\mathcal{U}(\mathbb{Z}G_i)$ é finito, portanto, pela recíproca do Teorema 2.1.9 item (2), a álgebra $\mathbb{Q}S$ tem a propriedade hiperbólica. □

Exemplo 2.5.3. *Sejam $S' = D_4 \cup \{\theta\}$ e $S = C_2 \times C_2 \cup \{e_{11}, e_{12}, e_{21}, e_{22}, \theta\}$, com a operação: $x, y \in S$, $x \circ y = \theta$ se $x, y \notin C_2 \times C_2$, e $x \circ y = xy$, caso contrário. As álgebras $\mathbb{Q}S$ e $\mathbb{Q}S'$ são isomorfas, mas S não é a união de grupos, pois S não é um semigrupo inverso.*

Consideremos agora, um semigrupo finito S que não é semi-simples. Pelo Corolário 2.4.5, a série principal de S admite fator principal nulo. O exemplo a seguir é uma ocorrência deste fato.

Exemplo 2.5.4. *Considere o semigrupo $T_2 = \{e_{11}, e_{22}, e_{12}, \theta\}$ sendo e_{ij} as matrizes elementares 2×2 e θ o zero de T_2;*

$$T_2 \supset \{e_{11}, e_{12}, \theta\} \supset \{e_{12}, \theta\} \supset \{\theta\} \supset \emptyset$$

é uma série principal cujos fatores $\langle e_{11}\rangle$ e $\langle e_{22}\rangle$ são semigrupos completamente 0-simples e $\{e_{12}, \theta\}$ é um semigrupo nulo, portanto, pelo Corolário 2.4.5, $\mathbb{Q}S$ não é semi-simples. Com efeito, o radical de $J(\mathbb{Q}S) \cong \mathbb{Q}e_{12}$ é não-trivial.

Lema 2.5.5. *Seja S um semigrupo finito, tal que, $J(\mathbb{Q}S) = \mathbb{Q}j_0$ para algum $j_0 \in \mathbb{Q}S$, e $j_0^2 = 0$. Então, para cada $s \in S$, $s \cdot j_0 = \lambda_s j_0$, $j_0 \cdot s = \rho_s j_0$, com $\lambda_s, \rho_s \in \{-1, 0, 1\}$*

Demonstração.

Sendo $J(\mathbb{Q}S) := J = \langle j_0 \rangle$ um ideal, para $s \in S$ temos $J \ni x := s \cdot j_0$. Logo, existe $\lambda_s \in \mathbb{Q}$, tal que, $x = \lambda_s j_0$. Seja $\langle s \rangle$ o semigrupo cíclico gerado por s. Pelo Lema 2.2.2, existe $n \in \mathbb{N}$, tal que, s^n é um idempotente. Indutivamente, obtemos que $s^n \cdot j_0 = \lambda_s^n j_0$. Seja $e := s^n$, temos que $e^2 = s^{2n} = s^n = e$, logo, $\lambda_s^{2n} j_0 = e^2 \cdot j_0 = e \cdot j_0 = \lambda_s^n j_0$. Daí $(\lambda_s^n - 1)\lambda_s^n j_0 = 0$, portanto $\lambda_s \in \{-1, 0, 1\}$. Analogamente, $\rho_s \in \{-1, 0, 1\}$. □

Proposição 2.5.6. *Seja S^θ um semigrupo finito não semi-simples, tal que, $\mathbb{Q}S$ tem a propriedade hiperbólica. Então existe um único elemento nilpotente $j_0 \in S$. Além do mais, $\mathfrak{I} := \{\theta, j_0\}$ é um semigrupo nulo que é um ideal de S, e $J = \mathbb{Q}j_0$.*

Demonstração.

Suponha que existam elementos nilpotentes $r, s \in S$. Pela Proposição 2.1.10, $r, s \in J$, portanto, $\{s, r\}$ é um conjunto $\mathbb{Q} - LD$, um absurdo, pois pelo corolário 2.1.3, $dim_{\mathbb{Q}}(J) = 1$. Logo S admite, no máximo, um elemento nilpotente.

Sendo S um semigrupo não semi-simples finito, a série principal de S admite algum fator principal $\{\theta, j_0\}$ que é um semigrupo nulo, e, logo, j_0 é nilpotente. Portanto pela unicidade, este fator principal nulo é único. Logo, j_0 é o único nilpotente de S. Portanto, pela Proposição 2.1.10, $j_0 \in J$, e $J = \mathbb{Q}j_0$. Se $s \in S$, então $sj_0 \in J$, portanto, pelo lema anterior, $sj_0 = \theta$ ou $sj_0 = j_0$, portanto, $sj_0 \in \{\theta, j_0\}$. Analogamente, $j_0 s \in \{\theta, j_0\}$, logo, $\mathfrak{I} := \{\theta, j_0\}$ é um ideal de S. □

Quando a álgebra $\mathbb{Q}S$ é não-semi-simples, pode ocorrer ou não que $J(\mathbb{Q}S)$ seja central. Se $J(\mathbb{Q}S)$ é não-central, vide exemplo 2.5.3, S contém o subsemigrupo das matrizes triangulares superiores e um semigrupo nulo não central. No caso central, vide exemplo 2.4.6, S contém um subsemigrupo nulo que é central.

Teorema 2.5.7. *Seja S^θ um semigrupo finito. A álgebra $\mathbb{Q}S$ é não-semi-simples e satisfaz a propriedade hiperbólica se, e somente se, existe um único elemento nilpotente $j_0 \in S$, tal que, o subsemigrupo $\mathfrak{I} = \{\theta, j_0\}$ é um ideal de S, e $S/\mathfrak{I}$ admite uma série principal, onde cada fator principal é isomorfo a grupos abelianos de expoente dividindo 4 ou 6, ou a $2-$grupos hamiltonianos. Em particular, $S/\mathfrak{I}$ é a união disjunta de seus subgrupos maximais.*

Demonstração.

Se $\mathbb{Q}S$ é não-semi-simples, então $\mathbb{Q}S \cong \mathcal{S}(\mathbb{Q}S) \oplus J$. Tendo $\mathbb{Q}S$ a propriedade hiperbólica, temos, pelo Teorema 2.1.9, que $\mathbb{Q}S \cong (\oplus \mathcal{A}_i) \oplus X$, em que $X \in \{J, T_2(\mathbb{Q})\}$ depende da centralidade do radical. Em ambos os casos, se Γ é uma $\mathbb{Z}$-ordem em $\mathbb{Q}S/J$, então $\mathcal{U}(\Gamma)$ é finito. Portanto, $\mathbb{Q}S/J$ tem a propriedade hiperbólica e é livre de elementos nilpotentes.

Pela Proposição 2.5.6, existe um único elemento nilpotente $j_0 \in S$, $\mathfrak{I} = \{j_0, \theta\}$ é um ideal de S, e $J = \mathbb{Q}j_0$. Pelas condições de $\mathfrak{I}$, $\mathbb{Q}_0\mathfrak{I} \cong \mathbb{Q}j_0$, portanto $\mathbb{Q}S/J \cong \mathbb{Q}S/\mathbb{Q}\mathfrak{I} \cong \mathbb{Q}_0(S/\mathfrak{I})$ tem a propriedade hiperbólica e é livre de nilpotentes. Pelo Teorema 2.4.15, $S/\mathfrak{I}$ admite uma série cujos fatores principais são grupos abelianos de expoente dividindo 4 ou 6 ou 2-grupos hamiltonianos, como, pelo parágrafo anterior $\mathcal{U}(\Gamma)$ é finito, os grupos cíclicos C_5, C_8 e C_{12} não ocorrem.

Reciprocamente, se S tem um único elemento nilpotente j_0, tal que, $\mathfrak{I} = \{j_0, \theta\}$ é um ideal de S, e $S/\mathfrak{I}$ admite uma série cujos fatores são os grupos acima, pelo Lema 2.4.15, $\mathbb{Q}_0(S/\mathfrak{I}) \cong \bigoplus_{i=1}^{N} \mathbb{Q}G_i$, logo, $\mathbb{Q}S/\mathbb{Q}\mathfrak{I} \cong \bigoplus_{i=1}^{N} \mathbb{Q}G_i$. Sendo $\mathbb{Q}_0\mathfrak{I} \cong \langle j_0 \rangle_{\mathbb{Q}} = J$, temos a decomposição de Wedderburn-Mal*čev*:

$$\mathbb{Q}_0 S \cong (\oplus \mathbb{Q}G_i) \oplus \langle j_0 \rangle_{\mathbb{Q}}. \qquad 2.5$$

Pela proposição 2.1.4, se J é não-central, então existem únicos $E_1, E_N \in E(\mathbb{Q}S)$, idempotentes centrais e ortogonais, tal que, $E_1 j_0 = j_0 E_N = j_0$ e $j_0 E_1 = E_N j_0 = 0$. Portanto, $\{E_1, E_N, j_0, \theta\} \cong T_2$, o semigrupo das matrizes triangulares superiores de ordem 2. Seja $E = E_1 + E_2$, $E^2 = E$ um idempotente central, e $(\mathbb{Q}_0 S)E = \mathbb{Q}\langle E_1, E_2, j_0 \rangle \cong \mathbb{Q}T_2 \cong T_2(\mathbb{Q})$. Logo, $\mathbb{Q}S \cong \bigoplus_{1<i<N} \mathcal{S}(\mathbb{Q}S)E_i \oplus T_2(\mathbb{Q}) \cong B \oplus T_2(\mathbb{Q})$, sendo B o anulador de $\langle j_0 \rangle$. Além disso, para $\mathcal{A}_i := \mathcal{S}(\mathbb{Q}S)E_i$, temos $\bigoplus_{1<i<N} \mathcal{A}_i = \bigoplus_{1<i<N} \mathcal{S}(\mathbb{Q}S)E_i \subset \oplus \mathbb{Q}G_i$, e nas condições de cada G_i, $\mathcal{U}(\mathbb{Z}G_i)$ é finito. Portanto, $\mathbb{Q}S \cong (\bigoplus_{1<i<N} \mathcal{A}_i) \oplus T_2(\mathbb{Q})$. Caso J seja

central $\mathbb{Q}S \cong (\oplus \mathcal{A}_i) \oplus J$.

Em ambos os casos, $\mathcal{A}_i$ é anel de divisão, e $|\mathcal{U}(\Gamma_i)| < \infty$, para toda $\mathbb{Z}$-ordem $\Gamma_i \subset \mathcal{A}_i$. Assim $\mathbb{Q}S$ está nas condições do Teorema 2.1.9, itens (c) ou (d), e, logo, $\mathbb{Q}S$ satisfaz a propriedade hiperbólica.

□

Corolário 2.5.8. *O radical de $\mathbb{Q}S$ é central se, e somente se, S é a união disjunta de grupos, listados no teorema anterior, com um subsemigrupo nulo central em S.*

Este corolário caracteriza os semigrupo finitos $\{S, \circ\}$, cuja álgebra $\mathbb{Q}S$ não é semi-simples e o radical é central.

Como exemplo, construímos alguns semigrupos finitos S para visualizar sua estrutura e a álgebra $\mathbb{Q}S$. Garantimos que os conjuntos são semigrupos, verificando que a operação é associativa.

Em [7], é apresentado o *Teste de Light* que verifica, de modo sistemático, se a operação do semigrupo é associativa. A seguir apresentamos esse teste, e na seqüência, o aplicamos nos exemplos considerados.

Por linha indicial da tabela de Cayley, consideramos a linha do extremo superior da tabela, cuja primeira entrada é o símbolo correspondente à operação binária. Por coluna indicial, a coluna do extremo esquerdo da tabela, cuja primeira entrada é a operação binária.

Seja $\{S, \cdot\}$ um semigrupo finito. O teste de Light considera para cada gerador $g \in S$ duas operações, $\circ$ e $\star$, assim definidas:

$$\begin{array}{rccc} \star: & S \times S & \longrightarrow & S \\ & (ab) & \mapsto & a \cdot (g \cdot b) \end{array} \qquad \begin{array}{rccc} \circ: & S \times S & \longrightarrow & S \\ & (ab) & \mapsto & (a \cdot g) \cdot b \end{array}$$

De modo que a operação $\cdot$ é associativa se as operações $\star$ e $\circ$ são iguais.

Verificamos essa igualdade, construindo, para cada gerador, a tabela de Cayley das operações binárias $\star$ e $\circ$.

Pode-se, em uma mesma tábua, construir a tabela para uma das operações, e inspecionar a outra operação, verificando se são as mesmas. Mas não é necessário realizar as operações novamente, se procedermos do seguinte modo.

Construímos a tabela da operação $\star_g$. Os valores $(g \cdot b)$ correspondem à linha de g na tabela da operação $\cdot$, como vamos computar estes valores com $a \in S$, interessam somente os resultados da linha de g em $\cdot$, esta linha compõe a linha indicial da tabela de $\star$. A coluna indicial da tabela é a mesma coluna indicial da tabela $\cdot$. Se x é um dos resultados $g \cdot b$, os valores $a \cdot x$, que compõem a parte interna da tabela de $\star$, correspondem à coluna de x na tabela de $\cdot$. Com isso obtemos a tábua da operação $\star$.

A tábua da operação $\circ$ é feita de modo análogo, porém a coluna indicial desta tabela é formada pela coluna de g da tabela de $\cdot$, a linha indicial é a linha indicial da tabela $\cdot$ e, para cada elemento da coluna indicial, $y = a \cdot g$, copiamos a linha de y da tabela de $\cdot$.

Obtemos, portanto, as tabelas das operações $\star$ e $\circ$.

Porém, o teste de light pode ser feito com apenas uma tabela, para cada gerador. De fato! Como a tábua de $\star$, assim construída, tem a mesma coluna indicial da tabela de $\cdot$, nesta coluna copiamos a coluna de g da tabela indicial, e para cada elemento desta coluna, que é a indicial, comparamos a linha da tabela de $\cdot$ com a linha da tabela, que foi construída para $\star$.

Exemplo 2.5.9. *Seja $S = \{a, b, c, d, e\}$ e $\cdot$ a operação binária.*

Primeiro construímos a tabela original de S:

$\cdot$	a	b	c	d	e
a	a	a	a	d	d
b	a	b	c	d	d
c	a	c	b	d	d
d	d	d	d	a	a
e	d	e	e	a	a

.

Identificamos os geradores do semigrupo: $\{c, e\}$.

Para cada gerador, g, contruímos uma tabela da seguinte forma: a linha indicial da

tabela é formada pela linha do gerador g; a coluna indicial da tabela é formada pela coluna do gerador g; para cada elemento da linha indicial, sua coluna será formada pela coluna da tabela original para este elemento.

Teste para o gerador c:

c	a	c	b	d	d
a	a	a	a	d	d
c	a	c	b	d	d
b	a	b	c	d	d
d	d	d	d	a	a
e	d	e	e	a	a

.

A associatividade é verificada se para cada elemento da coluna indicial, sua linha é a mesma da tabela original, para este elemento. Isto ocorre para a tabela acima. Para o gerador "e", procedemos da mesma forma.

O teste de Light, para o elemento em que falha a associatividade, permite obter diretamente qualquer caso em que esta a não ocorre.

Exemplo 2.5.10. *O teste de Light mostra que $S = \{a, b, c, d\}$, com a operação $\cdot$ abaixo, não é um semigrupo. Porque a operação de S não é associativa:*

$\cdot$	a	b	c	d
a	a	b	a	a
b	b	a	a	a
c	b	b	c	d
d	b	b	d	d

.

Os geradores são $\{b, d\}$. O teste para b é:

b	b	a	a	a
b	b	a	a	a
a	a	b	b	b
b	b	b	b	b
b	b	b	b	b

, observe que as duas últimas linhas não correspondem à linha de b, na tabela original, falha, por exemplo, o último elemento. De fato, na linha 5, coluna 5, da tabela de b, o valor $(d \cdot b) \cdot d = b$, foi calculado pela tabela. Porém o valor que checamos, pela linha, é $d(b \cdot d) = a$. Portanto falha a associatividade nesse produto.

Recordamos que T_2 é o semigrupo das matrizes elementares triangulares superiores de ordem dois e $T_2(\mathbb{Q})$ a álgebra das matrizes triangulares superiores de ordem dois sobre $\mathbb{Q}$. Por $\mathfrak{I}$, denotamos o ideal nulo $\{\theta, j_0\}$. O seguinte exemplo é de um semigrupo que contém um subsemigrupo isomorfo a T_2.

Exemplo 2.5.11. *Seja $S = \{e, g, f, h, j_0\} \cup \{\theta\}$, com a operação $\circ$ dada pela tabela de Cayley:*

$\circ$	e	g	f	h	j_0	θ
e	e	g	θ	θ	j_0	θ
g	g	e	θ	θ	j_0	θ
f	θ	θ	f	h	θ	θ
h	θ	θ	h	f	θ	θ
j_0	θ	θ	j_0	j_0	θ	θ
θ	θ	θ	θ	θ	θ	θ

A associatividade da operação $\circ$ pode ser verificada usando o teste de associatividade de Light ([7], §1.2), a partir dos geradores de S, que são: $\{g, h, j_0\}$, que resulta nas seguintes tábuas:

g	g	e	θ	θ	j_0	θ
g	g	e	θ	θ	j_0	θ
e	e	g	θ	θ	j_0	θ
θ	θ	θ	θ	θ	θ	θ
θ	θ	θ	θ	θ	θ	θ
θ	θ	θ	θ	θ	θ	θ
θ	θ	θ	θ	θ	θ	θ

h	θ	θ	h	f	θ	θ
θ	θ	θ	θ	θ	θ	θ
θ	θ	θ	θ	θ	θ	θ
h	θ	θ	h	f	θ	θ
f	θ	θ	f	h	θ	θ
j_0	θ	θ	j_0	j_0	θ	θ
θ	θ	θ	θ	θ	θ	θ

j_0	θ	θ	j_0	j_0	θ	θ
j_0	θ	θ	j_0	j_0	θ	θ
j_0	θ	θ	j_0	j_0	θ	θ
θ	θ	θ	θ	θ	θ	θ
θ	θ	θ	θ	θ	θ	θ
θ	θ	θ	θ	θ	θ	θ
θ	θ	θ	θ	θ	θ	θ

Usando estas tabelas e o teste de Light, concluímos que $\{S, \circ\}$ é um semigrupo.

As relações entre e, f, j_0, a partir da tabela acima, mostram que o subsemigrupo $\{e, f, j_0, \theta\} \cong T_2$.

Observamos, também, as seguintes propriedades de $\mathbb{Q}S$:

$g \in S\{e, f, j_0, \theta\}S$, portanto, o subsemigrupo não é um ideal de S.

O conjunto $E = \{\frac{e+g}{2}, \frac{e-g}{2}, \frac{f+h}{2}, \frac{f-h}{2}\}$ *é um sistema completo de idempotentes centrais, ortogonais e primitivos da álgebra* $\mathcal{S}(\mathbb{Q}S) \cong \mathbb{Q}(S/\mathfrak{I})$. *Ademais,* $e+f$ *é a unidade de* $\mathbb{Q}S$.

A decomposição de $\mathbb{Q}S$ *em componentes de Wedderburn-Malĉev é:*

$$\mathbb{Q}S \cong \mathbb{Q}S(\frac{e-g}{2}) \oplus \mathbb{Q}S(\frac{f-h}{2}) \oplus \mathbb{Q}S(\frac{e+g}{2}) \oplus \mathbb{Q}S(\frac{f+h}{2}) \oplus \mathbb{Q}\mathfrak{I},$$

$S(\frac{e-g}{2}) = \{\pm\frac{e-g}{2}\}$ *e* $S(\frac{f-h}{2}) = \{\pm\frac{f-h}{2}\}$, *e, portanto as duas componentes iniciais são ideais de* $\mathbb{Q}S$. *Para as demais componentes, como,* $S(\frac{e+g}{2}) = \{\frac{e+g}{2}, j_0\}$, *isso não ocorre. Porém o conjunto* $I_2 = \{\frac{e+g}{2}, \frac{f+h}{2}, j_0, \theta\} \cong T_2$. *Nesse caso* $\mathbb{Q}S(\frac{e+g}{2}) \oplus \mathbb{Q}S(\frac{f+h}{2}) \oplus \underbrace{\mathbb{Q}j_0 \oplus \mathbb{Q}\theta}_{\mathbb{Q}\mathfrak{I}} = \mathbb{Q}I_2$ *e* $\mathbb{Q}_0 I_2 \cong T_2(\mathbb{Q})$ *é um ideal de* $\mathbb{Q}S$.

A decomposição de $\mathbb{Q}_0 S$, *como soma de ideais, fica:*

$$\mathbb{Q}_0 S \cong \mathbb{Q}(\frac{e-g}{2}) \oplus \mathbb{Q}(\frac{f-h}{2}) \oplus T_2(\mathbb{Q}).$$

Aqui temos uma situação bastante peculiar: embora $S' = \{e, f, j_0, \theta\}$ *não seja ideal de* S, *portanto* $\mathbb{Q}S'$ *não é ideal de* $\mathbb{Q}S$, *ocorre que* $\mathbb{Q}S'$ *é isomorfo ao ideal* $T_2(\mathbb{Q})$ *de* $\mathbb{Q}S$.

Definição 2.5.12. *Denotamos por* T_2' *o semigrupo* $\{e_1, e_2, e_3, j_0, \theta\}$, *com a tabela de Cayley:*

$\cdot$	e_1	e_2	e_3	j_0	θ
e_1	e_1	θ	e_3	j_0	θ
e_2	θ	e_2	e_3	θ	θ
e_3	e_3	e_3	e_3	θ	θ
j_0	θ	j_0	θ	θ	θ
θ	θ	θ	θ	θ	θ

.

O semigrupo $H = \{e_1 - e_3, e_2 - e_3, j_0, \theta\} \subset \mathbb{Q}T_2'$ é, tal que, $H \cong T_2$ e $\mathbb{Q}T_2' \cong \mathbb{Q} \oplus \mathbb{Q} \oplus T_2(\mathbb{Q})$, cuja unidade é $e_1 + e_2 - e_3$. Além disso, $\mathbb{Q}T_2'(e_1 + e_2 - 2e_3) \cong T_2(\mathbb{Q})$.

Definição 2.5.13. *Denotamos por $\hat{T}_2$ o semigrupo $\{e_1, e_2, j_0, \theta\}$, com a tabela de Cayley:*

$\circ$	e_1	e_2	j_0	θ
e_1	e_1	j_0	j_0	θ
e_2	θ	e_2	θ	θ
j_0	θ	j_0	θ	θ
θ	θ	θ	θ	θ

.

Nesse caso, temos que $H = \{e_1 - j_0, e_2, j_0, \theta\} \subset \mathbb{Q}T_2$ é um subsemigrupo $\mathbb{Q}$-L.I. e isomorfo a T_2. Logo $\mathbb{Q}_0\hat{T}_2 \cong \mathbb{Q}_0T_2 \cong T_2(\mathbb{Q})$. A unidade de $\mathbb{Q}_0\hat{T}_2$ é $e_1 + e_2 - j_0$.

Os semigrupos T_2, T_2' e $\hat{T}_2$ são os blocos básicos dos semigrupos S, tal que $\mathbb{Q}S$ é não-semi-simples e tem a propriedade hiperbólica. (Vide Teorema 2.5.20.)

Observamos que se S é um semigrupo, tal que, $\mathbb{Q}_0S \supset T_2(\mathbb{Q})$, como somando direto, então existe $S' \subset S$ e S' é isomorfo a um dos semigrupos do conjunto $\{T_2, T_2', \hat{T}_2\}$.

Os exemplos, a seguir, são de semigrupos S, cuja álgebra $\mathbb{Q}S$ não é central. No primeiro, existe um semigrupo $T_2' \subseteq S$. No outro, um semigrupo $\hat{T}_2 \subset S$.

No exemplo anterior, o grupos $G = \{e, g\}$ e $H = \{f, h\}$ são ortogonais, e a ação de e, f sobre j_0 é trivial. O próximo exemplo, trata de um caso não ortogonal, isto é, $ef = fe \neq 0$.

Exemplo 2.5.14. *Seja $S = \{e, g, f, h, x, y, j_0\} \cup \{\theta\}$, com a operação $\circ$ dada pela tabela de Cayley:*

$\circ$	e	g	f	h	x	y	j_0	θ
e	e	g	x	x	x	y	j_0	θ
g	g	e	x	x	x	y	j_0	θ
f	x	x	f	h	x	y	θ	θ
h	x	x	h	f	x	y	θ	θ
x	x	x	x	x	x	y	θ	θ
y	y	y	y	y	y	x	θ	θ
j_0	θ	θ	j_0	j_0	θ	θ	θ	θ
θ	θ	θ	θ	θ	θ	θ	θ	θ

A associatividade da operação $\circ$ pode ser verificada usando o teste de associatividade de Light ([7], §1.2), a partir dos geradores de S, que são: $\{g, h, y, j_0\}$, que resulta nas seguintes tábuas:

g	g	e	x	x	x	y	j_0	θ
g	g	e	x	x	x	y	j_0	θ
e	e	g	x	x	x	y	j_0	θ
x	x	x	x	x	x	y	θ	θ
x	x	x	x	x	x	y	θ	θ
x	x	x	x	x	x	y	θ	θ
y	y	y	y	y	y	x	θ	θ
θ	θ	θ	θ	θ	θ	θ	θ	θ
θ	θ	θ	θ	θ	θ	θ	θ	θ

h	x	x	h	f	x	y	θ	θ
x	x	x	x	x	x	y	θ	θ
x	x	x	x	x	x	y	θ	θ
h	x	x	h	f	x	y	θ	θ
f	x	x	f	h	x	y	θ	θ
x	x	x	x	x	x	y	θ	θ
y	y	y	y	y	y	x	θ	θ
j_0	θ	θ	j_0	j_0	θ	θ	θ	θ
θ	θ	θ	θ	θ	θ	θ	θ	θ

y	y	y	y	y	y	x	θ	θ
y	y	y	y	y	y	x	θ	θ
y	y	y	y	y	y	x	θ	θ
y	y	y	y	y	y	x	θ	θ
y	y	y	y	y	y	x	θ	θ
y	y	y	y	y	y	x	θ	θ
x	x	x	x	x	x	y	θ	θ
θ	θ	θ	θ	θ	θ	θ	θ	θ
θ	θ	θ	θ	θ	θ	θ	θ	θ

j_0	θ	θ	j_0	j_0	θ	θ	θ	θ
j_0	θ	θ	j_0	j_0	θ	θ	θ	θ
j_0	θ	θ	j_0	j_0	θ	θ	θ	θ
θ	θ	θ	θ	θ	θ	θ	θ	θ
θ	θ	θ	θ	θ	θ	θ	θ	θ
θ	θ	θ	θ	θ	θ	θ	θ	θ
θ	θ	θ	θ	θ	θ	θ	θ	θ
θ	θ	θ	θ	θ	θ	θ	θ	θ
θ	θ	θ	θ	θ	θ	θ	θ	θ

Usando estas tabelas e o teste de Light, concluímos que $\{S, \circ\}$ é um semigrupo.

Pela definição de S, $ef = fe = x \neq 0$, e o semigrupo $\{e, f, x, j_0, \theta\} \cong T_2'$.

Os elementos $e_{11} = \frac{e+g}{2} - x$ e $e_{22} = \frac{f+h}{2} - x$ são tais, que $\mathbb{Q}S \supset I_2 = \{e_{11}, e_{22}, j_0, 0\} \cong T_2$, e $\mathbb{Q}I_2$ é ideal de $\mathbb{Q}S$.

O conjunto

$$\{\frac{e-g}{2}, \frac{f-h}{2}, \frac{x+y}{2}, \frac{x-y}{2}, e_{11}+e_{22}\}$$

é um sistema completo de idempotentes centrais, ortogonais e primitivos da álgebra $\mathcal{S}(\mathbb{Q}S) \cong \mathbb{Q}(S/\mathfrak{J})$. *Além disso,* $d = e + f - x$ *é a unidade da álgebra* $\mathbb{Q}S$.

A decomposição de $\mathbb{Q}S$ *em soma de ideais é:*

$$\mathbb{Q}_0 S \cong B \oplus T_2(\mathbb{Q})$$

$$B \cong \mathbb{Q}(\frac{e-g}{2}) \oplus \mathbb{Q}(\frac{f-h}{2}) \oplus \mathbb{Q}(\frac{x+y}{2}) \oplus \mathbb{Q}(\frac{x-y}{2})$$

$$T_2(\mathbb{Q}) \cong \mathbb{Q}(\frac{e+g}{2} - x) \oplus \mathbb{Q}(\frac{f+h}{2} - x) \oplus \mathbb{Q}j_0,$$

em que B *é o anulador de* j_0.

O exemplo seguinte considera o caso $e_1e_2 \neq e_2e_1$, mostrando inclusive que é possível outros grupos maximais de S, além de G_1 e G_N, agir não trivialmente sobre $\{j_0, \theta\}$.

Exemplo 2.5.15. *Seja* $S = \{e_1, e_2, e_3, j_0\} \cup \{\theta\}$, *com a operação* $\circ$ *dada pela tabela de Cayley:*

$\circ$	e_1	e_2	e_3	j_0	θ
e_1	e_1	j_0	e_3	j_0	θ
e_2	θ	e_2	θ	θ	θ
e_3	e_3	j_0	e_3	j_0	θ
j_0	θ	j_0	θ	θ	θ
θ	θ	θ	θ	θ	θ

A associatividade da operação $\circ$ *pode ser verificada usando o teste de associatividade de Light ([7], §1.2), a partir dos geradores de* S, *que são:* $\{e_1, e_2, e_3, j_0\}$, *que resulta nas seguintes tábuas:*

e_1	e_1	j_0	e_3	j_0	θ
e_1	e_1	j_0	e_3	j_0	θ
θ	θ	θ	θ	θ	θ
e_3	e_3	j_0	e_3	j_0	θ
θ	θ	θ	θ	θ	θ
θ	θ	θ	θ	θ	θ

e_2	θ	e_2	θ	θ	θ
j_0	θ	j_0	θ	θ	θ
e_2	θ	e_2	θ	θ	θ
j_0	θ	j_0	θ	θ	θ
j_0	θ	j_0	θ	θ	θ
θ	θ	θ	θ	θ	θ

e_3	e_3	j_0	e_3	j_0	θ
e_3	e_3	j_0	e_3	j_0	θ
θ	θ	θ	θ	θ	θ
e_3	e_3	j_0	e_3	j_0	θ
θ	θ	θ	θ	θ	θ
θ	θ	θ	θ	θ	θ

j_0	θ	j_0	θ	θ	θ
j_0	θ	j_0	θ	θ	θ
θ	θ	θ	θ	θ	θ
j_0	θ	j_0	θ	θ	θ
θ	θ	θ	θ	θ	θ
θ	θ	θ	θ	θ	θ

Usando estas tabelas e o teste de Light, concluímos que $\{S, \circ\}$ é um semigrupo.

Temos que $\{e_1, e_2, j_0, \theta\} \cong \hat{T}_2$.

Destacamos, além disso, algumas propriedades de álgebra $\mathbb{Q}S$:

Para $I_2 = \{e_2 - j_0, e_3, j_0\} \subset \mathbb{Q}S$, $\mathbb{Q}I_2$ é ideal de $\mathbb{Q}S$, e $\mathbb{Q}I_2 \cong T_2(\mathbb{Q})$.

A unidade da álgebra $\mathbb{Q}S$ é $e_1 + e_2 - j_0$, e $\{e_2 + e_3 - j_0, e_1 - e_3\}$ é o sistema completo de idempotentes centrais, ortogonais e primitivos de $\mathcal{S}(\mathbb{Q}S) \cong \mathbb{Q}(S/\mathfrak{I})$.

A decomposição de Wedderburn-Malĉev de $\mathbb{Q}S$ é:

$$\mathbb{Q}S \cong \mathbb{Q}S(e_1 - e_3) \oplus \mathbb{Q}S(e_2 + e_3 - j_0) \oplus \mathbb{Q}\mathfrak{I}.$$

Sendo $S(e_2 + e_3 - j_0) \cup \{\theta\} = \{e_2, e_3, j_0\} \cup \{\theta\} \cong T_2$, obtemos a decomposição de $\mathbb{Q}_0 S$ como soma de ideais:

$$\mathbb{Q}_0 S \cong \mathbb{Q}(e_1 - e_3) \oplus T_2(\mathbb{Q}).$$

2.5.1 Idempotentes dos grupos maximais

Concluímos a primeira seção com um teorema que dá a estrutura de uma álgebra finitamente gerada com a propriedade hiperbólica. Recordamos a decomposição dos idempotentes da proposição 2.1.4, para a álgebra não semi-simples $\mathbb{Q}S$:

$$1 = \sum_{1<i<N} E_i + E, \text{ sendo } E = E_1 + E_N.$$

Seja $e \in \mathbb{Q}S$ um idempotente. Então $e = \sum_{1<i<N} eE_i + eE$, cada $(eE_i)^2 = eE_i$ é um idempotente de $\mathbb{Q}S$, e $eE_i = E_ie \in \mathcal{A}_i$, que é um anel de divisão. Portanto $eE_i \in \{E_i, 0\}$, logo, $e = \sum E_{i_l} + eE$.

Proposição 2.5.16. *Seja $S = \cup G_i \cup \{\theta, j_0\}$. Se $e_i \in G_i$ é o elemento neutro do grupo. Então e_i tem uma das seguintes expressões:*

$$\begin{array}{l} \sum E_{i_l} + E_1 + \lambda j_0 \\ \sum E_{i_l} + E_N + \mu j_0 \\ \sum E_{i_l} + E_1 + E_N \\ \sum E_{i_l} \end{array} .$$

Sendo que as duas últimas são centrais em $\mathbb{Q}S$.

Demonstração.

Como elemento da álgebra $\mathbb{Q}S$, $e_i = \sum E_{i_l} + uE_1 + vE_N + wj_0$, sendo cada E_{i_l} central, ortogonal e anulador de j_0; $E_1j_0 = j_0E_N = j_0$ e $E_Nj_0 = j_0E_1 = 0$, obtemos:
$e_i^2 = \sum E_{i_l} + u^2E_1 + v^2E_N + w(u+v)j_0 = e_i$, portanto, $u, v \in \{1, 0\}$, e $w(u+v) = w$. Se $u = v = 1$, então $w = 0$, portanto, $e_i = \sum E_{i_l} + E_1 + E_N$, e as demais possibilidades:
$u = 1, v = 0, w = 1$, $u = 0, v = 1, w = 1$, e $u = v = w = 0$, determinam as outras expresssões de e_i.

□

Lema 2.5.17. *Seja $\mathbb{Q}S \cong \mathcal{A}_i \oplus \mathbb{Q}j_0$, $\mathcal{A}_i = E_i\mathbb{Q}S$, $E_1j_0 = j_0E_N = j_0$, e G, H subgrupos maximais de S. Se $\mathcal{A}_1 \subseteq \mathbb{Q}G$, então, para todo $g \in G$, $gj_0 = j_0$, e $j_0g = 0$. Se $\mathcal{A}_N \subseteq \mathbb{Q}H$, então, para todo $h \in H$, $j_0h = j_0$, e $hj_0 = 0$.*

Demonstração.

Seja $E_1 \in \mathcal{A}_1 \subset \mathbb{Q}G$, e $E_1 = \sum_{g\in G} \alpha_g g$. Pela propriedade de E_1, $j_0 = E_1j_0 = (\sum \alpha_g)\lambda_g j_0 \neq 0$, e $\lambda_g \in \{0, 1\}$. Existe $g \in G$, tal que, $\lambda_g = 1$. Portanto, $gj_0 = j_0$, sendo $gj_0 = ge_1j_0 = j_0$, temos que $e_1j_0 \neq 0$, e, portanto, $e_1j_0 = j_0$. Analogamente, $j_0e_N = j_0$.

Sendo $\mathbb{Q}j_0$ um ideal, $j_0e_1 = \rho j_0$, e $\rho \in \{0, 1\}$. Suponhamos que $\rho = 1$, isto é, $e_1j_0 = j_0 = j_0e_1$, então e_1 centraliza j_0, logo, $e_1 \in \mathcal{A}_i, 1 < i < N$, absurdo. Com os mesmos argumentos, provamos que $e_Nj_0 = 0$.

Afirmação: se $g \in G$, então $gj_0 = j_0$, com efeito, sendo $gj_0 = \lambda j_0$, indutivamente obtemos $g^m j_0 = \lambda^m j_0$. O grupo G é finito, portanto, $g^{|G|} j_0 = e_1 j_0 = \lambda^{|G|} j_0$, pelo Lema 2.5.5, $\lambda \in \{-1, 1, 0\}$, ademais $e_1 j_0 \neq 0$, portanto, $\lambda \neq 0$, logo, $gj_0 = j_0$, para todo $g \in G$. De modo análogo ao que fizemos para provar que $j_0 e_1 = 0$, obtemos que $j_0 g = 0$, para todo $g \in G$. Do mesmo modo, obtemos o resultado para H. □

Corolário 2.5.18. *Nas condições do lema anterior, se $\Delta(G)$ é o ideal de aumento, e $\mathbb{Q}G \cong \mathbb{Q}\hat{G} \oplus \Delta(G)$. Então $\mathcal{A}_i = \mathbb{Q}\hat{G}$.*

Proposição 2.5.19. *Seja G um subgrupo maximal de S. Se $e = \sum E_l + E_1 + \lambda j_0$, então, para todo $g \in G, g = \sum gE_l + E_1 + \lambda j_0$. Da mesma forma, se $e = \sum E_l + E_N + \mu j_0$, então, para todo $g \in G, g = \sum gE_l + E_N + \mu j_0$*

Demonstração.

Seja $g \in G$,

$$g = ge = \sum gE_l + gE_1 + g\lambda j_0 \qquad (\star).$$

Pela expressão de $e = \sum E_l + E_1 + \lambda j_0$, multiplicando por j_0 à direita, $ej_0 = j_0$. Pelo Lema 2.5.17, $gj_0 = j_0$, e multiplicando a equação $(\star)$ à esquerda por g, obtemos: $g = \sum gE_l + gE_1 + \lambda j_0$. Para determinarmos gE_1, seja $gE_1 = tE_1 + sE_N + rj_0$. Existe $l \in \mathbb{Z}$, tal que, $g^l = e$, portanto, sendo E_1 ortogonal a cada $E_i, i \neq 1$ e $E_1 j_0 = j_0$, obtemos $E_1 g^l = E_1 + \lambda j_0$. Comparando com a equação $(gE_1)^l = (tE_1 + sE_N + rj_0)^l = t^l E_1 + s^l E_n + r' j_0$, obtemos: $t^l = 0, s^l = 1$, e $r' = \lambda$. Desse modo $g = \sum gE_l \pm E_1 + \lambda j_0$, e multiplicando por j_0, utilizando o Lema 2.5.17:$j_0 = gj_0 = \pm E_1 j_0$, determinamos $g = \sum gE_l + E_1 + \lambda j_0$.

Para o outro caso: $e = \sum E_l + E_N + \mu j_0$, ocorre que $j_0 e = j_0$. Se $g \in G$, repetindo-se o procedimento, obtemos que $g = \sum gE_l + E_N + \mu_g j_0$. □

Teorema 2.5.20. *Seja S um semigrupo que é a união de grupos com um ideal $\mathfrak{I} = \{\theta, j_0\}$, $S = \cup G_i \cup \mathfrak{I}$, tal que, $\mathbb{Q}S$ tem a propriedade hiperbólica. Se $e_1 \in G_1$, e $e_N \in G_N$ são os elementos neutros dos grupos, e $e_1 j_0 = j_0 e_N = j_0$, escrevendo*

$$\begin{aligned} e_1 &= \sum E_{1_l} + E_1 + \lambda j_0 \\ e_N &= \sum E_{N_l} + E_N + \mu j_0. \end{aligned}$$

Então apenas uma das sequintes condições é satisfeita:

(1)

$$e_1 e_N = 0 \Leftrightarrow e_N e_1 = 0 \text{ e } \lambda + \mu = 0.$$

Neste caso, $\{e_1, e_N, j_0, \theta\} \cong T_2$.

(2)

$$\text{Se } e_N e_1 \neq 0 \text{ então } e_1 e_N = e_N e_1 =: e_3 \text{ e } \lambda + \mu = 0.$$

Neste caso, $\{e_1, e_N, e_3, j_0, \theta\} \cong T_2'$.

(3)

$$e_N e_1 = 0 \Leftrightarrow e_1 e_N = j_0 \Leftrightarrow \lambda + \mu = 1$$

Neste caso, $\{e_1, e_N, j_0, \theta\} \cong \hat{T}_2$.

Demonstração.

Utilizando o fato que $E_i \in E(\mathbb{Q}S)$ são ortogonais, $j_0 e_1 = j_0 E_1 = e_n j_0 = E_N j_0 = 0$, e $e_1 j_0 = E_1 j_0 = j_0 e_n = j_0 E_N = j_0$, obtemos:

$$\begin{aligned} e_1 e_N &= \sum E_{1_l} E_{N_l} + (\lambda + \mu) j_0 \\ e_N e_1 &= \sum E_{N_l} E_{1_l} \\ e_1 e_N &= e_N e_1 + (\lambda + \mu) j_0 \end{aligned} \quad .$$

Se $e_1 e_N = 0$, então $-(\lambda + \mu) j_0 = \sum E_{1_l} E_{N_l} = \sum E_{N_l} E_{1_l} = e_N e_1 \in \mathcal{S}(\mathbb{Q}S) \cap J = \{0\}$, logo $e_N e_1 = 0$. Portanto, $\sum E_{N_l} E_{1_l} = 0$ e $\lambda + \mu = 0$. Reciprocamente, se $0 = e_N e_1 = \sum E_{N_l} E_{1_l} = 0$ e $\lambda + \mu = 0$, então $e_1 e_N = 0$. A relação $e_1 \mapsto e_{11}$, $e_N \mapsto e_{22}$, e $j_0 \mapsto e_{12}$, define um isomorfismo entre os semigrupos $\{e_1, e_N, j_0, \theta\}$ e T_2.

Suponha que $e_N e_1 \neq 0$, da equação $e_1 e_N = e_N e_1 + (\lambda + \mu) j_0$, se $(\lambda + \mu) \neq 0$, então o conjunto $\{e_1 e_N, e_N e_1, j_0\} \subseteq S$ é $\mathbb{Q}-$linearmente dependente, um absurdo. Logo $(\lambda + \mu) = 0$ e $e_1 e_N = e_N e_1$. A recíproca é imediata.

Nas condições acima, seja $e_3 := e_1 e_N$. O conjunto $\{e_1, e_2, e_3, j_0, \theta\} \subseteq S$ é isomorfo a T_2'.

Se $e_N e_1 = 0$, então $e_1 e_N = (\lambda + \mu) j_0$. Sendo $e_1, e_N \in S$, temos $e_1 e_N \in S$. Se $e_1 e_N = 0$, então estamos na condição do item (1). Se $e_1 e_N = s \neq \theta$, então, pela Proposição 2.5.6, S contém um único elemento nilpotente, portanto, $\lambda + \mu = 1$. Reciprocamente, se $\lambda + \mu = 1$, então $e_1 e_N = \sum E_{1_l} E_{N_l} + j_0$, e $e_N e_1 \in S$, logo, o conjunto $\{e_1 e_N, e_N e_1, j_0\} \subseteq S$ é $\mathbb{Q}$ linearmente dependente. Portanto, se $e_1 e_N \neq 0$, então $e_N e_1 = 0$ e $e_1 e_N = j_0$. Neste caso o semigrupo $\{e_1, e_N, j_0, \theta\}$ é isomorfo à $\hat{T}_2$,

□

Capítulo 3

Hiperbolicidade do Loop de Unidades de RA-Loops

Os anéis R que vamos considerar são anéis associativos, comutativos e com unidade, a menos que seja mencionado o contrário. As referências básicas para este capítulo são o livro *Alternative Loop Rings* [15] e o artigo *Hyperbolic Unit Groups* [24].

3.1 Anéis Alternativos

Definição 3.1.1. *Seja A um anel, não necessariamente associativo. Para elementos $x, y, z \in A$, define-se o associador deles por $[x, y, z] = (xy)z - x(yz)$.*

Se ocorre que $[x, y, z] = 0, \forall x, y, z \in A$, então A é um anel associativo.

Definição 3.1.2. *Um anel A é alternativo se, para todo $x, y \in A$, satisfaz as seguintes identidades:*

[x,x,y]=0 a identidade alternativa à esquerda
[y,x,x]=0 a identidade alternativa à direita.

Observe que todo anel associativo é alternativo. O anel dos Números de Cayley, porém é um exemplo de um anel alternativo que não é associativo. O Teorema de Artin mostra uma importante relação entre os anéis alternativos e seus subanéis.

Teorema 3.1.3 (Artin)**.** *Um anel R é alternativo se, e somente se, o subanel gerado por quaisquer 2 elementos de R é um anel associativo.*

Corolário 3.1.4 ([15], I.1.6)**.** *Em um anel alternativo A valem as seguintes identidades, $\forall x, y, z \in A$,*

(1) $((xy)x)z = x(y(xz))$ *a identidade de Moufang à esquerda;*

(2) $((xy)z)y = x(y(zy))$ *a identidade de Moufang à direita;*

(3) $(xy)(zx) = (x(yz))x$ *a identidade de Moufang interna(middle);*

Definição 3.1.5. *Um quasigrupo é um par $(L, \cdot)$, em que L é um conjunto não vazio e $(a, b) \mapsto a \cdot b$ é uma operação binária fechada sobre L, com a propriedade que a equação $a \cdot b = c$ determine um único elemento $b \in L$, quando são dados $a, c \in L$ e um único elemento $a \in L$, quando são dados $b, c \in L$. Um loop é um quasigrupo com um elemento identidade bi-lateral* 1*.*

Teorema 3.1.6 ([15],II.3.1)**.** *Em um loop, as identidades de Moufang são equivalentes.*

Definição 3.1.7. *Um loop é de Moufang se satisfaz quaisquer uma das identidades de Moufang*

Definição 3.1.8. *Seja G um grupo não abeliano, $g_0 \in \mathcal{Z}(G)$, um elemento central, $\star : G \longrightarrow G$, uma involução, tal que, $g_0^\star = g_0$ e $gg^\star \in \mathcal{Z}(G), \forall g \in G$ e u uma indeterminada. O conjunto*

$$L = G \dot{\cup} Gu,$$

com as seguintes operações:

1. $(g)(hu) = (hg)u$;
2. $(gu)h = (gh^\star)u$;
3. $(gu)(hu) = g_0 h^\star g$.

é denotado por $M(G, \star, g_0)$

A seguinte proposição mostra que a classe de loops de Moufang é de fato não trivial.

Proposição 3.1.9 ([15],II.5.2)**.** *O conjunto $L = M(G, \star, g_0)$ é um loop de Moufang*

Observamos que o fato de um loop L ser de Moufang, não garante que existem, respectivamente, G e u, um grupo não abeliano e uma indeterminada, tal que,

$$L = M(G, \star, g_0),$$

isso ocorre porém para uma classe especial de loops, denominados RA-loops, que será definida ainda neste capítulo.

Analogamente aos grupos Hamiltonianos, um loop não associativo cujos subloops são todos normais é dito um loop Hamiltoniano. Há também uma caracterização para estes loops.

Teorema 3.1.10 ([Norton]([15],II.4.8))**.** *Seja L um loop de Moufang. Então L é hamiltoniano se, e somente se:*

(1) L é um grupo abeliano, ou

(2) $L \cong Q_8 \times E \times A$, onde Q_8 é o grupo dos quatérnions de ordem 8, E é um 2-grupo abeliano e A(eventualmente trivial) é um $2'$-grupo abeliano, ou

(3) $L \cong M_{16}(Q_8) \times E \times A$, em que $M_{16}(Q_8)$ é o loop de Cayley e E e A como definidos em 2.

Definição 3.1.11. *Seja L um loop e R um anel. O anel de loop de L com coeficientes em R, denotado por RL, é o R-módulo livre com base L e cuja multiplicação é obtida extendendo-se a de L via as leis distributivas, ou seja RL é o conjunto das somas finitas*

$$\sum_{l \in P, r_l \in R} r_l l.$$

Com as operações definidas por:

$$\sum_{l \in L} r_l l + \sum_{l \in L} s_l l = \sum_{l \in L} (r_l + s_l) l;$$

$$(\sum_{l\in L} r_l l)(\sum_{l\in L} s_l l) = \sum_{l\in L}(\sum_{hk=l} r_h s_k)l.$$

Definição 3.1.12. *Se $\alpha = \sum \alpha_l l \in RL$, então o suporte de α, denotado por $supp(\alpha)$, é o conjunto dos $l \in L$, para o qual $\alpha_l \neq 0$:*

$$supp(\sum \alpha_l l) = \{l \in \mathcal{L} : \alpha_l \neq 0\}.$$

Definição 3.1.13. *O conjunto $\mathcal{U}(RL) = \{u \in RL : \exists u^{-1} \in RL, uu^{-1} = u^{-1}u = 1\}$ é denominado conjunto de unidades de RL.*

Definição 3.1.14. *Um RA-loop (Ring Alternative loop), é um loop cujo anel de loop RL, sobre um anel R de característica diferente de 2, é alternativo mas não associativo*

Lema 3.1.15 ([15], Lema $VIII.4.1$)**.** *Seja T o conjunto dos elementos de torção de um loop L. Se L é um RA-loop, então T é um subloop normal localmente finito de L. Se L é finitamente gerado, então T é finito.*

Veremos adiante que se G é um 2-grupo Hamiltoniano e $L = M(G, \star, g_0)$ é um RA-loop, então L é um 2-loop Hamiltoniano.

Estes loops têm sido objeto de estudo desde a década de oitenta. O livro de Goodaire-Jespers-Polcino Milies, [15], é uma excelente referência para a teoria relativa a esta classe de loops.

Recentemente, Juriaans, Passi e Prasad, em [24], classificaram os grupos finitos para o qual o grupo das unidades do anel de grupo sobre o anel dos inteiros $\mathbb{Z}G$ é um grupo hiperbólico.

Muitos dos problemas clássicos da Teoria de Anéis de Grupo têm uma generalização natural para os RA-loops. Polcino Milies, Jespers e Goodaire, entre outros, têm discutido, e resolvido muitos destes problemas neste contexto, veja [15].

Aqui continuamos esta tendência classificando os RA-loops L, tal que, o loop $U(\mathbb{Z}L)$ não contém um grupo abeliano livre de posto 2.

Definição 3.1.16. *Seja L um loop tal que $\mathbb{Z}^2 \not\hookrightarrow L$, nessas condições dizemos que L tem a propriedade hiperbólica.*

Obviamente, para os *RA*-loops finitos, se o loop das unidades $\mathcal{U}(\mathbb{Z}L)$ é trivial, então $\mathcal{U}(\mathbb{Z}L)$ tem a propriedade hiperbólica.

3.2 Álgebras de Cayley Dickson e matrizes de Zorn

As álgebras de Cayley Dickson que serão consideradas aqui são todas álgebras de dimensão 8 sobre um corpo F, obtidas pelo processo de duplicação de Cayley-Dickson, e serão representadas por $A(F, \alpha, \beta, \gamma)$, sendo $char(F) \neq 2$ e $\alpha, \beta, \gamma \in F$. A Proposição 1.3.2, de [15], prova que toda álgebra de Cayley-Dickson é simples. No entanto uma álgebra obtida desta forma pode ou não conter divisores de zero, não triviais. Se contém divisores de zero, não triviais, então dizemos que a álgebra cinde(*split*), caso contrário dizemos que é uma álgebra com divisão.

Definição 3.2.1. *Seja R um anel, R^3 o conjunto de ternas ordenadas sobre R e considere o conjunto de matrizes de ordem 2 da forma:*

$$\begin{pmatrix} a & \mathbf{x} \\ \mathbf{y} & b \end{pmatrix},$$

com $\boldsymbol{x,y} \in R^3$, $a, b \in R$, com a soma usual para cada entrada da matriz e com o produto seguindo a seguinte regra:

$$\begin{pmatrix} a_1 & \mathbf{x_1} \\ \mathbf{y_1} & b_1 \end{pmatrix} \begin{pmatrix} a_2 & \mathbf{x_2} \\ \mathbf{y_2} & b_2 \end{pmatrix} = \begin{pmatrix} a_1a_2 + \mathbf{x_1} \cdot \mathbf{y_2} & a_1\mathbf{x_2} + b_2\mathbf{x_1} - \mathbf{y_1} \times \mathbf{y_2} \\ a_2\mathbf{y_1} + b_1\mathbf{y_2} + \mathbf{x_1} \times \mathbf{x_2} & b_1b_2 + \mathbf{y_1} \cdot \mathbf{x_2}, \end{pmatrix}$$

em que $\cdot$ e $\times$, denotam o produto escalar e vetorial respectivamente, em R^3. Esta construção nos fornece uma álgebra alternativa que denotamos por $\mathfrak{Z}(R)$, denominada álgebra de matriz vetorial de Zorn.

Um aspecto importante das álgebras de Cayley-Dickson que cindem é o isomorfismo entre a álgebra $A(\mathbb{R}, 1, -1, -1)$ e a álgebra alternativa $\mathfrak{Z}(\mathbb{R})$.

Proposição 3.2.2. *Seja $\mathfrak{Z}(\mathbb{Q})$ a álgebra alternativa das matrizes de Zorn sobre $\mathbb{Q}$ e Γ uma $\mathbb{Z}$-ordem em $\mathfrak{Z}(\mathbb{Q})$. Então*

$$\mathbb{Z}^2 \hookrightarrow \mathcal{U}(\Gamma)$$

Demonstração.

Seja $\Lambda = \mathfrak{Z}(\mathbb{Z})$, uma $\mathbb{Z}$-ordem de $\Lambda = \mathfrak{Z}(\mathbb{Q})$. Considere os elementos $(0) = (0,0,0)$,$e_1 = (1,0,0)$, $e_2 = (0,1,0)$ e defina

$$\theta_1 = \begin{pmatrix} 0 & e_1 \\ (0) & 0 \end{pmatrix} \quad e \quad \theta_2 = \begin{pmatrix} 0 & e_2 \\ (0) & 0 \end{pmatrix}.$$

É imediata a verificação que $\theta_1^2 = \theta_2^2 = 0$ são dois elementos nilpotentes, que comutam e $\{\theta_1, \theta_2\}$ é $\mathbb{Q}$-LI. Logo, pelo Lema 1.2.17, $\mathbb{Z}^2 \hookrightarrow \mathcal{U}(\Lambda)$. Sendo $\mathcal{U}(\Lambda)$ e $\mathcal{U}(\Gamma)$ comensuráveis, temos que $\mathbb{Z}^2 \hookrightarrow \mathcal{U}(\Gamma)$. □

Um loop L tem a propriedade LC, se não é comutativo e se, para todo $x, y \in L$, $xy = yx$ se, e somente se, $x \in \mathcal{Z}(L)$ ou $y \in \mathcal{Z}(L)$ ou $xy \in \mathcal{Z}(L)$.

Um processo similar ao de Cayley-Dickson pode ser usado para obter loops a partir de um grupo prefixado G, uma involução $\star$ de G e um elemento $g_0 \in G$. A notação utilizada para um loop obtido desta forma é $L = M(G, \star, g_0)$, como apresentado na Definição 3.1.8, e descrito em detalhes em [15], Seção $II.5$; é comum usar uma notação especial em alguns casos. Esta notação foi introduzida por M. Hall Jr. e J.K. Senior. Como ela não interfere diretamente com os nossos resultados referimos à Seção $V.3$ de [15], caso seja preciso. O resultado, que citamos a seguir, é um dos mais importantes na teoria dos RA-loops. (Veja [6], [15] Teorema $IV.3.1$ e [1] Teorema 3.1)

Teorema 3.2.3. *Seja L um RA-loop. Existe um subgrupo $G \subset L$, uma involução $\star$ de G e um elemento central $g_0 \in G$, tal que, G tem a propriedade LC, $L' = G' = \{1, s\} \cong C_2$, $g_0^\star = g_0$ e $L = M(G, \star, g_0)$. Além do mais, se $l \in T(L)$ tiver ordem ímpar, então l é um elemento central.*

Se L é um RA-loop finito, então $\mathbb{Q}L \cong \bigoplus_{i=1}^{n} \mathcal{A}_i, n \in \mathbb{Z}^+$. Cada $\mathcal{A}_i$ é isomorfo a um corpo, ou uma álgebra de Cayley Dickson, ou uma álgebra de quatérnions ou uma álgebra de matrizes de Zorn, ([15], Corolário $VI.4.8$). Desse modo, se $\mathbb{Q}L$ contém algum elemento nilpotente, então alguma componente $\mathcal{A}_i$ é, a menos de isomorfismo, uma álgebra de matrizes de Zorn, como demonstrado no seguinte lema.

Lema 3.2.4. *Seja L um RA-loop finito cuja álgebra $\mathbb{Q}L$ contém elementos nilpotentes. Então $\mathbb{Q}L$ contém um somando direto isomorfo às matrizes de Zorn sobre $\mathbb{Q}$.*

Demonstração.

Sendo L um RA-loop finito, pelo Corolário $VI.4.3$ de [15], $\mathbb{Q}L \cong \bigoplus_{i=1}^{n} \mathcal{A}_i, n \in \mathbb{Z}^+$. Pela Proposição $VI.4.6$, $\mathcal{A}_j$ é associativo se, e somente se, A_j é comutativo. Se $\mathcal{A}_j$ é uma álgebra de Cayley Dickson, para algum $1 \leq j \leq n$, então A_j ou é uma álgebra de divisão, ou é uma matriz de Zorn $\mathcal{A}_j \cong \mathfrak{Z}(\mathbb{Q})$. Como $\mathbb{Q}L$ tem elementos nilpotentes e, tanto a álgebra de quatérnios, quanto a álgebra de Cayley-Dickson com divisão, não têm elementos nilpotentes, existe j, tal que, $\mathcal{A}_j \cong \mathfrak{Z}(\mathbb{Q})$. □

3.3 Unidades de um anel de loop alternativo

Um marco para a Teoria de Anéis de Grupos são os resultados de Berman e Higman para unidades de torção. Muitos desses resultados, inicialmente provados para grupos finitos, foram estendidos para todos os grupos. Apresentamos agora versões análogas para a classe dos loops alternativos. Começamos com o análogo do Teorem de Berman que foi provado por de Barros-Juriaans, veja ([2], Teorema 3.2). Este resultado foi inicialmente provado para RA-loops finitos por Goodaire-Polcino Milies.

Teorema 3.3.1. *Seja L um RA-loop e $\alpha = \sum_{\lambda \in L} \alpha_\lambda \lambda$ uma unidade de torção em $\mathbb{Z}L$. Se $\alpha_1 \neq 0$, então $\alpha = \pm 1$.*

Como mencionado anteriormente, os grupos 2-hamiltonianos têm uma estrutura bem definida. São isomorfos ao loop $\mathbb{Q}_8 \times E$, onde $\mathbb{Q}_8$ é o grupo de quatérnios de ordem 8 e E é um 2-grupo abeliano elementar.

Teorema 3.3.2 (Higman, [16], Teorema 2.3)**.** *Seja L um* RA*-loop com subloop de torção T. Então todas as unidades de $\mathbb{Z}L$ são triviais se, e somente se, todo subloop de T é normal em L, e T é um grupo abeliano de expoente dividindo 4 ou 6, ou um 2-grupo Hamiltoniano ou um 2-loop Hamiltoniano de Moufang.*

Proposição 3.3.3. *Se G é um 2-grupo hamiltoniano, e $L = M(G, *, g_0)$ é um RA-loop, então L é um 2-loop hamiltoniano de Moufang, e $\mathcal{U}_1(\mathbb{Z}L) = L$.*

Demonstração.

Obviamente L é um 2-loop de Moufang. Sendo G um 2-grupo hamiltoniano, temos que $G = Q_8 \times E$, em que E é um 2-grupo abeliano elementar e, portanto, $L = (Q_8 \times E) \dot{\cup} (Q_8 \times E)u$. Pelo Teorema (V.1.6,[15]), $L = M(Q_8 \times E, \star, g_0) \cong M(Q_8, \star, g_0) \times E = M_{16}(Q_8) \times E$ que, pelo Teorema de Norton, é um loop hamiltoniano. Logo é um 2-loop hamiltoniano.

A prova de que $\mathcal{U}_1(\mathbb{Z}L) = L$ é conhecida e pode, por exemplo, ser encontrada na página 280 de [2]. □

Se L é um RA-loop, então o anel $\mathbb{Z}L$ é alternativo e, portanto, verifica as leis de Moufang. Assim o loop de unidades $\mathcal{U}(\mathbb{Z}L)$ é um loop de Moufang.

Proposição 3.3.4 ([15], Proposição $XII.1.3$)**.** *Seja L um RA-loop com subloop de torção T. Se T é ou um grupo abeliano, ou um 2-loop hamiltoniano e todo subloop de T é normal em L, então*

$$\mathcal{U}(\mathbb{Z}L) = [\mathcal{U}(\mathbb{Z}T)]L = L[\mathcal{U}(\mathbb{Z}T)].$$

Se L é um loop alternativo finito, e G é um grupo, tal que, $L = G \dot{\cup} Gu$. Então, obviamente, temos que $\mathcal{U}(\mathbb{Z}G) \hookrightarrow \mathcal{U}(\mathbb{Z}L)$.

Lema 3.3.5. *Seja L um* RA*-loop finito. O loop $\mathcal{U}(\mathbb{Z}L)$ tem a propriedade hiperbólica se, e somente se, $\mathcal{U}(\mathbb{Z}L)$ é trivial.*

Demonstração.

Sendo L um loop alternativo temos, pelo Teorema 3.2.3, que existe G, um grupo não abeliano, tal que, $L = M(G, *, g_0) = G \dot{\cup} Gu$, e, portanto, $\mathbb{Z}^2$ não imerge em $\mathcal{U}(\mathbb{Z}G)$.

Sendo G um grupo finito não abeliano, pelo Teorema 1.2.16,

$$G \in \{S_3, D_4, C_3 \rtimes C_4, C_4 \rtimes C_4\} \cup \{K : K \text{ é um 2-grupo hamiltoniano}\}.$$

Pelo Teorema 3.2.3, temos que o conjunto $G' \cong C_2$. Portanto, $G \notin \{S_3, C_3 \rtimes C_4\}$. Além disso, $G \notin \{D_4, C_4 \rtimes C_4\}$, porque se supomos o contrário, a álgebra $\mathbb{Q}G$ contém elementos nilpotentes e, portanto, pelo Lema 3.2.4, $\mathbb{Q}L$ contém uma cópia da matriz de Zorn que, por sua vez, contém uma cópia de $\mathbb{Z}^2$ em alguma $\mathbb{Z}-$ordem de $\mathbb{Q}L$, um absurdo.

Finalmente se G é um 2-grupo hamiltoniano, a Proposição 3.3.3, garante que $\mathcal{U}(\mathbb{Z}L)$ é trivial. □

Podemos agora provar o resultado principal deste capítulo. Observe que este resultado resolve por completo o problema da hiperbolicidade para anéis de RA-loops. O equivalente para grupos ainda é um problema em aberto.

Teorema 3.3.6. *Seja L um RA-loop. O loop $\mathcal{U}(\mathbb{Z}L)$ tem a propriedade hiperbólica se, e somente se, L é um loop finito ou um loop cujo centro é virtualmente cíclico, o subloop de torção $T(L)$ de L é, tal que, caso $T(L)$ seja um grupo, será um grupo abeliano de expoente dividindo 4 ou 6, ou um 2-grupo hamiltoniano. Caso contrário, $T(L)$ é um 2-loop hamiltoniano de Moufang e, em ambos os casos, todo subloop de $T(L)$ é normal em L. Nessas condições o loop $\mathcal{U}_1(\mathbb{Z}L) = L$.*

Demonstração.

O caso em que L é finito, está provado no lema anterior. Seja L infinito, pelo Lema 2.1 de [2], o centro $\mathcal{Z}(L)$ é um grupo abeliano finitamente gerado, logo $\mathcal{Z}(L) \cong T(\mathcal{Z}(L)) \times F$, sendo $T(\mathcal{Z}(L))$ um grupo de torção e F um grupo abeliano livre de torção. Segundo a hiperbolicidade de L, $F = \langle z_0 \rangle$ é um grupo cíclico, cuja ordem $o(z_0) = \infty$. Caso contrário, ou L seria finito e, portanto, F seria trivial, ou o posto livre de F seria maior que 1, e L teria um grupo abeliano livre de posto 2, contrariando a propriedade hiperbólica de L. Logo $\mathcal{Z}(L)$ é virtualmente cíclico.

Suponha que $\mathcal{U}(\mathbb{Z}L)$ satisfaça a propriedade hiperbólica e $\alpha \in \mathcal{U}_1(\mathbb{Z}L) \setminus L$.

Podemos, sem perda de generalidade, considerar L um loop finitamente gerado, porque, fixado α, sendo L não associativo, existem $x, y, z \in L$, tal que $[x, y, z] \neq 0$. De modo que, $L_0 = \langle supp(\alpha), x, y, z \rangle$ é um RA-loop finitamente gerado. Sendo L um RA-loop

finitamente gerado, pelo Lema 3.1.15, o subloop de torção $T(L)$ é finito e normal em L. Tendo L a propriedade hiperbólica, então $T(L)$ tem a propriedade hiperbólica. Consideramos os dois casos possíveis: $T(L)$ é um grupo ou $T(L)$ é um loop. Se ocorre este último caso, pelo lema anterior, $\mathcal{U}(\mathbb{Z}(T(L)))$ é trivial. Afirmamos que todo subloop $H < T(L)$ é normal em L. De fato, suponha o contrário, seja $t \in T(L)$, tal que, $\langle t\rangle$ não é normal em L. Existe $l \in L$, tal que, $l^{-1}tl \notin \langle t\rangle$. Para $\hat{t} = 1+t+\cdots+t^{n-1}$, sendo $n = o(t)$, o elemento $\theta = (1-t)l\hat{t}$ é nilpotente, portanto, $u_{t,l} := 1+\theta$ é uma unidade livre de torção e $u_{t,l}^n \notin L$, para todo inteiro não nulo n. Nessas condições, $\langle u_{t,l}\rangle \times \langle z_0\rangle \cong \mathbb{Z}^2$, pois $z_0u_{t,l} = u_{t,l}z_0$ e $\langle u_{t,l}\rangle \cap \langle z_0\rangle = \{1\}$. Um absurdo, pois L satisfaz a propriedade hiperbólica. Assim todo subloop de $T(L)$ é normal em L. Também da condição que $\mathcal{U}(\mathbb{Z}(T(L)))$ é trivial, obtemos, pelo Teorema de Higman 3.3.2, que $T(L)$ é um 2-loop Hamiltoniano de Moufang. Segundo as condições de L: um RA-loop finitamente gerado, cujo subloop de torção é um 2-loop hamiltoniano e todo subloop de $T(L)$ é normal em L, pela Proposição 3.3.4, temos que $\mathcal{U}(\mathbb{Z}L) = L[\mathcal{U}(\mathbb{Z}(T(L)))]$. Sendo $\mathcal{U}(\mathbb{Z}(T(L)))$ trivial, concluímos que $\mathcal{U}(\mathbb{Z}L)$ é trivial, um absurdo, pois consideramos α não trivial.

Se $T(L)$ é um grupo, como $\mathcal{U}(\mathbb{Z}L)$ satisfaz a propriedade hiperbólica, obtemos que $\mathcal{U}(\mathbb{Z}T(L))$ é hiperbólico. Sendo $\langle z_0\rangle$ subgrupo de $\mathcal{Z}(L)$, então, segundo a classificação de [24], $\mathcal{U}(\mathbb{Z}T(L))$ deve ser trivial, logo, $T(L)$ é um grupo abeliano de expoente dividindo 4 ou 6, ou um $2-grupo$ hamiltoniano. Nesse caso, as condições satisfeitas no caso anterior ocorrem de modo idêntico, isto é, todo grupo, portanto, todo subloop de $T(L)$ é normal em L. Logo, pela Proposição 3.3.4, temos que $\mathcal{U}(\mathbb{Z}L) = L[\mathcal{U}(\mathbb{Z}(T(L)))]$. Sendo $\mathcal{U}(\mathbb{Z}(T(L)))$ trivial, concluímos que $\mathcal{U}(\mathbb{Z}L)$ é trivial, um absurdo, pois consideramos α não trivial.

Reciprocamente, por um lado, quando L é finito o lema anterior considera este caso. Por outro lado, seja L um RA-loop, cujo centro $\mathcal{Z}(L)$ é virtualmente cíclico, e $T(L)$ é um 2-loop Hamiltoniano de Moufang ou $T(L)$ é um grupo abeliano de expoente dividindo 4 ou 6 ou um 2-grupo hamiltoniano, tal que, todo subloop de $T(L)$ é normal em L. Pelo Teorema de Higman 3.3.2, $\mathcal{U}(\mathbb{Z}T(L))$ é trivial, e, logo, pela Proposição 3.3.4, $\mathcal{U}_1(\mathbb{Z}L) = L$. Podemos considerar L um RA-loop finitamente gerado, portanto, temos que $L/\mathcal{Z}(L) \cong C_2\times C_2\times C_2$. Logo $[L : \mathcal{Z}(L)] = [\mathcal{U}_1(\mathbb{Z}L) : \mathcal{Z}(L)] = 8$, e, portanto, $\mathcal{U}_1(\mathbb{Z}L)$ e $\mathcal{Z}(L)$ são comensuráveis. Sendo $\mathcal{Z}(L)$ virtualmente cíclico, ele é hiperbólico. Portanto $\mathcal{U}_1(\mathbb{Z}L)$ é hiperbólico. □

Referências Bibliográficas

[1] L. G. X. de Barros, S. O. Juriaans, *Units in Integral Loop Rings*, Journal of Algebra 183(1996), 637-648.

[2] L. G. X. de Barros, S. O. Juriaans, *Units in Alternative Integral Loop Rings*, Result. Math., 31 (1997), 266-281.

[3] I. Kapovich, N. Benakli, *Boundaries of hyperbolic groups*. Combinatorial and geometric group theory (New York, 2000/Hoboken, NJ, 2001), 39–93, Contemp. Math., 296, Amer. Math. Soc., Providence, RI, 2002.

[4] A. Borel, H. Chandra,*Arithmetic Subgroups of Algebraic Groups*, Annals of Mathematics, 75(3), 1962.

[5] M. R. Bridson, A. Haefliger, *Metric Spaces of Non-Positive Curvature*, Springer, Berlin, 1999.

[6] O. Chein; E. G. Goodaire, *Loops whose loop rings are alternative*, Comm. Algebra 14 (1986), no. 2, 293-310.

[7] A. H. Clifford, G. B. Preston, *The Algebraic Theory of Semigroups*, American Mathematical Society, Mathematical Surveys number 7, hode Island, 1961.

[8] C. Corrales, E. Jespers, G. Leal, A. del Río, *Presentations of the unit group of an order in a non-split quaternion algebra*, Advances in Mathematics 186(2004), 498-524.

[9] A. Dooms, E. Jespers, *Generators for a subgroup of finite index in the unit group of an integral semigroup ring*, J. Group Theory 7(2004), 543-553.

[10] A. Dooms,E. Jespers, S. O. Juriaans,*On group identities for the unit group of algebras and semigroup algebras over an infinite field*, J. Algebra 284 (2005), no. 1, 273-283.

[11] J. Elstrodt, F. Grunewald, J. Menniche, *Groups Acting on Hyperbolic Space*, Springer Monographs in Mathematics, Berlim, 1998.

[12] O. Endler, *Números Algébricos*, sexta edição, IMPA, Rio de Janeiro, 1986.

[13] J. Z. Gonçalves, *Integral Group Rings Whose Group of Units is Solvable, an Elementary Proof*, Bol. Soc. Bras. Mat., vol 16 n^0 2(985), 1-9.

[14] E. G. Goodaire, *A Brief History of Loop Rings*,15th School of Algebra (Portuguese) (Canela, 1998). Mat. Contemp. 16 (1999), 93-109.

[15] E. G. Goodaire, E. Jespers, F. C. Polcino Milies, *Alternative Loop Rings*, Elsevier, Oxford, 1996.

[16] E. G. Goodaire, F. C. Polcino Milies, *When is a unit loop f-unitary?*, Proccedings of the Edinburgh Mathematical Society (2005) 48, 125-142.

[17] M. Gromov, *Hyperbolic Groups, in Essays in Group Theory*, M. S. R. I. publ. 8, Springer, 1987, 75-263.

[18] B. Hartley, P. F. Pickel, *Free Subgroups in the Unit Groups of Integral Group Rings*, Can. J. Math, vol XXXII, n^0 6, 1980, 1342-1352.

[19] A. Herman, Y. Li, M. M. Parmenter, *Trivial Units for Group Rings with G-adapted Coefficient Rings*, Canad. Math. Bull., vol. 48(1), (2005), 80-89.

[20] A. Herman, Y. Li,*Trivial Units for Group Rings Over Rings of algebraic Integers*, Proccedings of the American Mathematical Society, volume 134, nunber 3, 631-635.

[21] G. Higman, *The Units of Group-Rings*, Proc. London Math. Soc., (2)46, (1940), 231-248.

[22] E. Jespers, *Free Normal Complements and the Unit Group of Integral Group Rings*, Proceedings of the American Mathematical Society, vol 122, number 1, 1994.

[23] E. Jespers, D. Wang, *Units of Integral Semigroup Rings*, Journal of Algebra, vol 181, 395-413,1996.

[24] S. O. Juriaans, I. B. S. Passi, D. Prasad, *Hyperbolic Unit Groups*, Proceedings of the American Mathematical Society, vol 133(2), 2005, 415-423.

[25] J. Okniński, *Semigroup Algebras*, Pure and Applied Mathematics, Dekker, USA, 1991.

[26] A. Pfister, *Zur Darstellung Von -1 als Summe von Quadraten in Einem Körper*, Journal London Math. Soc., 40(1965), 150-165.

[27] F. C. Polcino-Milies, S. K. Sehgal, *An introduction to Group Rings*, Kluwer Academic Publishers, Dordrecht, 2002.

[28] A. R. Rajwade, *A note on the Stufe of quadratic fields*, Indian J. Pure and App. Maths, 6 (1975), pages 725-726.

[29] C.Small, *Sums of three squares and levels of quadratic number fields*, Amer. Math. Monthly 93 (1986), no. 4, 276-279.

[30] S. K. Sehgal, *Units in Integral Group Rings*, Longman, Harlon, 1994.

Índice Remissivo