O Problema do Isomorfismo para Álgebras de Loops

Luiz Gonzaga Xavier de Barros

Tese apresentada ao
INSTITUTO DE MATEMÁTICA E ESTATÍSTICA
DA
UNIVERSIDADE DE SÃO PAULO
para a obtenção do grau de Doutor em Matemática

Área de Concentração: Álgebra

Orientador: Prof. Dr. Francisco César Polcino Milies

São Paulo, junho de 1992.

ABSTRACT

Given a loop L and a ring R , the definition of the loop algebra RL is very similar to the definition of a group algebra. If the characteristic of R is not 2 and the loop algebra RL is alternative, we say that L is an R.A. loop.

We have considered the following problem: "Given the R.A. loops L and M and an associative ring R , when will the algebra isomorphism $RL \cong RM$ imply the loop isomorphism $L \cong M$?"

We have studied the case when R is a field.

First, we consider the case $R = \mathbb{Q}$, the rational number field and we study a class of R.A. loops which is determined by $\mathbb{Q}$.

Then, we extend this result to fields whose characteristic does not divide the order of the loop.

“... cantar (e cantar, e cantar, e cantar)
a alegria de ser um eterno aprendiz ...”
Luiz Gonzaga Jr.

Para
Neide,
esposa,
amiga,
companheira.

ÍNDICE

CAPÍTULO 1 : PRÉ-REQUISITOS

Seção 1.1. R.A. Loops	5
Seção 1.2. Álgebras de Composição	9
Seção 1.3. Álgebras de Loops Alternativas Semisimples	16

CAPÍTULO 2 : O PROBLEMA DO ISOMORFISMO PARA ÁLGEBRAS DE LOOPS RACIONAIS

Seção 2.1. Alguns Resultados	25
Seção 2.2. As Álgebras dos R.A. Loops Indecomponíveis cujo Centro é de expoente 2	29
Seção 2.3. O Problema do Isomorfismo para os R.A. Loops do Tipo II	45

CAPÍTULO 3: CORPOS EQUIVALENTES SOBRE CLASSES DE R.A. LOOPS

Seção 3.1. Introdução	59
Seção 3.2. Álgebras de R.A. 2-Loops Semisimples	62
Seção 3.3. O Problema da Equivalência	66

Introdução

A noção de loop é conhecida há várias décadas, [1], [2] e [19]. Trata-se de um conjunto munido de uma operação que admite um elemento neutro e tal que as funções multiplicação à direita e multiplicação à esquerda por um elemento fixo são bijeções. Obviamente todo grupo é um loop. Para suavizar um pouco a notação escreveremos $x.yz$ no lugar de $x(yz)$ para indicar a ordem de associação de três elementos x, y e z de um loop L .

Dizemos que um loop L é um *loop de Moufang* se para todos x, y e z de L é verificada uma das seguintes identidades de Moufang:

$$\begin{aligned}xy.zx &= (x.yz)x \\(zx.y)x &= z(x.yx) \\(xy.x)z &= x(y.xz) \quad .\end{aligned}$$

Um anel A diz-se *alternativo* se para todos x e y de A valem

$$x.xy = x^2.y \quad e \quad xy.y = x.y^2 \quad .$$

Dados um anel associativo e comutativo R e um loop L , definimos a *álgebra de loop* RL considerando o R -módulo (à esquerda) livre que admite L como base e definindo a multiplicação de elementos de RL através da operação de L e da propriedade distributiva.

Se $\text{car} R \neq 2$ e RL é uma álgebra alternativa não associativa dizemos que L é um *R.A. loop*. Esta noção foi introduzida por E. G. Goodaire [9] em 1983 e explicitamente formalizada num artigo subsequente por O. Chein e E. G. Goodaire [5] em 1986.

É conhecido [25] que todo anel alternativo verifica as identidades de Moufang. Desse modo, se L é um R.A. loop então o anel de loop RL verifica essas identidades, e, em particular o próprio loop L as verifica. Assim, todo R.A. loop é necessariamente um loop de Moufang.

No artigo [5], O. Chein e E. G. Goodaire mostraram que os R.A. loops são quase grupos (eles admitem um subgrupo normal de índice 2) e são quase comutativos (o subloop comutador é de ordem 2). Uma descrição um pouco mais detalhada daremos na seção 1.1.

O estudos das álgebras de loops interessa no sentido de que se generalizam conceitos em várias direções. Além disso, essas álgebras tem significado na Teoria dos Códigos.

As álgebras dos R.A. loops, sendo álgebras alternativas, despertam um particular interesse pelo seu caráter quase associativo, o que permite adaptar, em muitos casos, técnicas usadas em álgebras de grupos.

O conhecido “problema do isomorfismo” foi colocado formalmente por R. M. Thrall em 1947 na Conferência de Álgebra de Michigan. Trata-se do seguinte: “Dados um anel R e os grupos G e H , dar condições sobre R , G e H para que o isomorfismo de anéis $RG \cong RH$ implique no isomorfismo de grupos $G \cong H$ ”. Quando essa implicação é verdadeira para um anel R e para todos grupos de uma

certa classe $\mathcal{G}$, dizemos que R determina a classe $\mathcal{G}$.

Em 1940, G. Higman [13] já tinha provado que o anel dos inteiros determina a classe dos grupos abelianos finitos.

Em 1950, S. Perlis e G. L. Walker [17] trabalharam com grupos abelianos e corpos cuja característica não divide a ordem dos grupos, o chamado caso semisimples abeliano. Eles conseguiram caracterizar completamente a decomposição da álgebra de grupo como soma de ideais simples, e, em particular, eles provaram que o corpo dos números racionais determina a classe dos grupos abelianos. No caso não abeliano tal fato não se verifica, mas muito se conseguiu descobrir sobre os grupos quando se verifica o isomorfismo entre as álgebras.

Quando a característica do corpo divide a ordem do grupo temos o chamado caso modular. Em 1956, W. E. Deskins resolveu o caso modular abeliano, provando que um corpo de característica p determina a classe dos p -grupos abelianos. O caso não abeliano é ainda hoje objeto de pesquisa. No artigo [18] de R. Sandling pode-se encontrar uma vasta literatura sobre o problema do isomorfismo para álgebras de grupos.

Um caminho natural é, portanto, estudar o problema do isomorfismo para álgebras de loops, e é nesse contexto que se inserem os R.A. loops, já que eles vão originar álgebras alternativas.

E. G. Goodaire e C. Polcino Milies [12] em 1988 provaram que o anel dos inteiros determina a classe dos R.A. loops.

Em 1990, G. Leal e C. Polcino Milies [15] trabalharam com o corpo dos

números racionais e resolveram o problema para uma subclasse dos R.A. loops, que aqui denominamos de tipo **I**.

No Capítulo 2 deste trabalho resolvemos completamente o problema para as álgebras de R.A. loops racionais. Uma surpresa agradável foi descobrir que uma subclasse de R.A. loops, aqui denominados de tipo **II**, é determinada pelos racionais.

No Capítulo 3, adaptando técnicas que E. Spiegel e A. Trojan ([22], [23]) usaram para álgebras de grupos, conseguimos estender os resultados de G. Leal e C. Polcino Milies [15] e os resultados do Capítulo 2 para os corpos, cuja característica não divida a ordem do R.A. loop, que, como veremos, é o caso semisimples. Em particular, conseguimos caracterizar todos os corpos que determinam a classe dos R.A. loops de tipo **II**.

Finalizando, gostaríamos de agradecer ao Prof. Francisco Cesar Polcino Milies pela sugestão do problema, pelo encorajamento e apoio durante todo o programa de doutorado e pela paciência com que ouviu e comentou as nossas exposições de resultados. Agradecemos também aos colegas dos cursos do doutorado, aos colegas do Seminário de Anéis de Grupos e Anéis não Comutativos e aos colegas do Seminário de Álgebras não Associativas.

Capítulo 1

Pré-requisitos

1.1 R.A. Loops

Até 1974 não eram conhecidos muitos exemplos de loops de Moufang. Nesse ano, O. Chein [3] apresentou um método para se construir loops desse tipo a partir de certos grupos não abelianos. Ele demonstrou o seguinte:

Teorema 1.1.1 *Seja G um grupo não abeliano com uma involução $*$ tal que gg^* está no centro de G para todo $g \in G$, e seja $g_o \in G$ um elemento central tal que $g_o = g_o^*$. Seja u uma indeterminada e consideremos $L = G \cup Gu$. Se definimos:*

$$g.hu = hg.u,$$

$$gu.h = gh^*.u,$$

$$gu.hu = g_o h^* g$$

para todos $g, h \in G$ então L é um loop de Moufang que não é um grupo.

É fácil ver que o loop L assim construído não tem a propriedade associativa. Para isso basta tomar dois elementos x e y em G tais que $xy \neq yx$. Então

$$(uy^*)x^* = yu.x^* = yx.u \quad e \quad u(y^*x^*) = u(xy)^* = xy.u$$

É costume escrever $L = L(G, *, g_o)$ para denotar o loop construído pelo método de Chein.

Em 1986, O. Chein e E. Goodaire [5] caracterizaram os R.A. loops intrinsicamente. São deles os seguintes resultados:

Teorema 1.1.2 *Seja L um R.A. loop. Então*

- (i) *O centro, $Z(L)$, e o núcleo, $N(L)$, coincidem.*
- (ii) *$g^2 \in Z(L)$ para todo $g \in L$.*
- (iii) *Existe um elemento $e \in Z(L)$ de ordem 2 tal que para todos g e h em L tem-se que ou $hg = gh$ ou $hg = egh$, e para todos g, h e k em L tem-se que ou $g(hk) = (gh)k$ ou $g(hk) = e(gh)k$.*
- (iv) *$L' = \{1, e\}$, onde L' é o subloop comutador.*
- (v) *$\frac{L}{Z(L)} \cong C_2 \times C_2 \times C_2$, onde C_2 indica o grupo cíclico de ordem 2.*

Teorema 1.1.3 *Seja L um R.A. loop. Então existe um grupo $G \subset L$ e um elemento $u \in L$ tal que $L = G \cup Gu$, $G' = L' = \{1, e\} \subseteq Z(G) = Z(L)$. Além disso, a função $*$: $L \rightarrow L$ dada por*

$$g^* = \begin{cases} g & \text{se } g \in Z(G) \\ eg & \text{se } g \notin Z(G) \end{cases}$$

é uma involução de L . Colocando $u^2 = g_o$, nós temos que $g_o \in Z(G)$ e a multiplicação em L é dada por

$$g.hu = hg.u,$$

$$gu.h = gh^*.u,$$

$$gu.hu = g_o h^* g$$

para todos $g, h \in G$, isto é, $L = L(G, *, g_o)$. Reciprocamente, dado um grupo G e uma involução $*$: $G \longrightarrow G$ como acima, o loop $L = L(G, *, g_o)$ é um R.A. loop.

Como consequência desse teorema, o grupo G é tal que $\frac{G}{Z(G)} \cong C_2 \times C_2$.

Os grupos G com a propriedade de que $\frac{G}{Z(G)} \cong C_p \times C_p$, para um p primo, foram estudados por G. Leal e C. Polcino Milies [15]. Enunciamos aqui dois de seus resultados particularizados para o caso $p = 2$.

Proposição 1.1.4 *Seja G um grupo tal que $\frac{G}{Z(G)} \cong C_2 \times C_2$. Então $G' = \{1, e\} \subseteq Z(G)$ é cíclico de ordem 2.*

Teorema 1.1.5 *Seja G um grupo. Então $\frac{G}{Z(G)} \cong C_2 \times C_2$ se e somente se G pode ser escrito na forma $G = D \times E \times A$, onde E é um 2-grupo abeliano, A é um grupo abeliano de ordem ímpar e D é um 2-grupo indecomponível tal que $D = \langle x, y, Z(D) \rangle$ com $x^2, y^2 \in Z(D)$. Além disso, $Z(D)$ pode ser escrito na forma $Z(D) = C_{2^{n_1}} \times C_{2^{n_2}} \times C_{2^{n_3}}$ com $n_1 \geq 1$ e $n_2, n_3 \geq 0$ e podemos assumir que $e \in C_{2^{n_1}}$.*

Dessa forma se tem facilmente que se L é um R.A. loop então $Z(L) = C_{2^{n_1}} \times C_{2^{n_2}} \times \cdots \times C_{2^{n_t}} \times A$, com $n_1 \geq 1$ $n_i \geq 0$ para $i = 2, \dots, t$ e A um grupo abeliano de ordem ímpar.

Num artigo subsequente[14], G. Leal, E. Jespers e C. Polcino Milies classificaram todos os grupos indecomponíveis não isomorfos com aquela propriedade e como consequência todos os R.A. loops indecomponíveis não isomorfos.

Nesse artigo eles demonstraram o seguinte:

Teorema 1.1.6 *Seja $L = L(G, *, g_o)$ um R.A. loop indecomponível. Então $G = D \times C$, onde D é um 2-grupo indecomponível e C é um grupo cíclico de ordem 2^n , $n \geq 0$.*

Segundo os resultados de [14], existem 5 tipos de grupos indecomponíveis com aquela propriedade, denominados lá por $D_1, D_2, \dots, D_5$. Eles são obtidos na forma $D_i = \langle Z(D_i), x, y \rangle$, como no teorema 1.1.5, e a escolha de x^2 e y^2 se dá conforme a tabela 1.1.1.

	$Z(G)$	x^2	y^2
D_1	$\langle t_1 \rangle$	1	1
D_2	$\langle t_1 \rangle$	t_1	t_1
D_3	$\langle t_1 \rangle \times \langle t_2 \rangle$	1	t_2
D_4	$\langle t_1 \rangle \times \langle t_2 \rangle$	t_1	t_2
D_5	$\langle t_1 \rangle \times \langle t_2 \rangle \times \langle t_3 \rangle$	t_2	t_3

Tabela 1.1.1

Ainda segundo o mesmo artigo [14], existem 7 tipos de R.A. loops indecomponíveis, denotados por $L_1, L_2, \dots, L_7$. Eles podem ser obtidos na forma $L(G, *, g_o)$, com $G = \langle Z(G), x, y \rangle$, escolhendo-se G, x^2, y^2 e g_o conforme a tabela 1.1.2, e sendo a involução $*$ de L definida como no teorema 1.1.3.

	$Z(L_i) = Z(G)$	x^2	y^2	G	$u^2 = g_0$
L₁	$\langle t_1 \rangle$	1	1	D₁	1
L₂	$\langle t_1 \rangle$	t_1	t_1	D₂	t_1
L₃	$\langle t_1 \rangle \times \langle t_2 \rangle$	1	t_2	D₃	1
L₄	$\langle t_1 \rangle \times \langle t_2 \rangle$	t_1	t_2	D₄	t_1
L₅	$\langle t_1 \rangle \times \langle t_2 \rangle \times \langle t_3 \rangle$	t_2	t_3	D₅	1
L₆	$\langle t_1 \rangle \times \langle t_2 \rangle \times \langle t_3 \rangle$	t_2	t_3	D₅	t_1
L₇	$\langle t_1 \rangle \times \langle t_2 \rangle \times \langle t_3 \rangle \times \langle w \rangle$	t_2	t_3	D₅ $\times$ $\langle w \rangle$	w

Tabela 1.1.2

1.2 Álgebras de composição

Sejam K um corpo e $\mathcal{A}$ uma álgebra sobre K com elemento unidade. Seja n uma forma quadrática definida em $\mathcal{A}$ com valores em K . Dizemos que a álgebra $\mathcal{A}$ é uma *álgebra de composição* se

- (i) $n(xy) = n(x).n(y)$ para todos x e y em $\mathcal{A}$,
- (ii) n é estritamente não-degenerada,

Se uma álgebra $\mathcal{A}$ admite uma involução $*$ tal que $a + a^*, a.a^* \in K$ para todo $a \in \mathcal{A}$, podemos construir uma nova álgebra com involução, que contém $\mathcal{A}$ como subálgebra, através do processo que passaremos a descrever.

Fixamos um elemento não-nulo $\alpha \in K$ e denotamos por $(\mathcal{A}, \alpha)$ o conjunto de todos os pares ordenados (a_1, a_2) com $a_1, a_2 \in \mathcal{A}$. Em $(\mathcal{A}, \alpha)$ definimos as operações de adição e multiplicação por escalar da maneira usual e a multiplicação de dois elementos desse conjunto definimos por

$$(a_1, a_2) \cdot (a_3, a_4) = (a_1 a_3 + \alpha . a_4 a_2^*, a_1^* a_4 + a_3 a_2).$$

É fácil ver que $(\mathcal{A}, \alpha)$ com essas operações é uma álgebra sobre K , que admite $(1, 0)$ como elemento unidade. O conjunto $\mathcal{A}' = \{(a, 0) \mid a \in \mathcal{A}\}$ é uma subálgebra de $(\mathcal{A}, \alpha)$, que é isomorfa à álgebra $\mathcal{A}$. Denotando $v = (0, 1)$ temos que $v^2 = \alpha(1, 0)$ e que $(\mathcal{A}, \alpha)$ é uma soma direta dos espaços vetoriais $\mathcal{A}'$ e $v\mathcal{A}'$. Se identificarmos $\mathcal{A}'$ com $\mathcal{A}$, todo elemento $x = (a_1, a_2) \in (\mathcal{A}, \alpha)$ pode ser escrito na forma $x = a_1 + va_2$. Definindo-se $x^* = a_1^* - va_2$ é fácil demonstrar que $*$ é uma involução em $(\mathcal{A}, \alpha)$.

Esse processo de duplicação de álgebras é conhecido pelo nome de *processo de duplicação de Cayley-Dickson*.

A álgebra dos quatérnios generalizados $\mathcal{Q}(K, \alpha, \beta) = ((K, \alpha), \beta)$ sobre K é uma álgebra simples de dimensão 4 sobre K , que admite uma base canônica $\{1, e_1, e_2, e_3\}$ tal que $e_1^2 = \alpha$, $e_2^2 = \beta$, $e_1.e_2 = e_3 = -e_2.e_1$, $e_2.e_3 = e_1 = -e_3.e_2$ e $e_3.e_1 = e_2 = -e_1.e_3$.

A álgebra de Cayley-Dickson $\mathcal{C}(K, \alpha, \beta, \gamma) = (((K, \alpha), \beta), \gamma)$ é uma álgebra simples de dimensão 8 sobre K , que admite uma base canônica $\{1, e_1, e_2, \dots, e_7\}$, cuja tabela de multiplicação é a seguinte:

	1	e_1	e_2	e_3	e_4	e_5	e_6	e_7
1	1	e_1	e_2	e_3	e_4	e_5	e_6	e_7
e_1	e_1	α	e_3	αe_2	e_5	αe_4	$-e_7$	$-\alpha e_6$
e_2	e_2	$-e_3$	β	$-\beta e_1$	e_6	e_7	βe_4	βe_5
e_3	e_3	$-\alpha e_2$	βe_1	$-\alpha \beta$	e_7	αe_6	$-\beta e_5$	$-\alpha \beta e_4$
e_4	e_4	$-e_5$	$-e_6$	$-e_7$	γ	$-\gamma e_1$	$-\gamma e_2$	$-\gamma e_3$
e_5	e_5	$-\alpha e_4$	$-e_7$	$-\alpha e_6$	γe_1	$-\alpha \gamma$	γe_3	$\alpha \gamma e_2$
e_6	e_6	e_7	$-\beta e_4$	βe_5	γe_2	$-\gamma e_3$	$-\beta \gamma$	$-\beta \gamma e_1$
e_7	e_7	αe_6	$-\beta e_5$	$\alpha \beta e_4$	γe_3	$-\alpha \gamma e_2$	$\beta \gamma e_1$	$\alpha \beta \gamma$

Tabela 1.2.1

Observemos que na Tabela 1.2.1, o conjunto $\{1, e_1, e_2, e_3\}$ é uma base de $\mathcal{Q}(K, \alpha, \beta)$ sobre K .

A álgebra dos quatérnios generalizados $\mathcal{Q}(K, \alpha, \beta)$ é associativa e não-comutativa, enquanto que a álgebra de Cayley-Dickson $\mathcal{C}(K, \alpha, \beta, \gamma)$ é alternativa, não-associativa e não-comutativa.

No estudo das álgebras de loops alternativas semisimples as álgebras de composição simples desempenham um papel importante.

Suponhamos que $\mathcal{A}$ seja uma álgebra de composição simples. Em [25] está demonstrado que $\mathcal{A}$ pode ser apenas de um dos seguintes tipos:

- (I) $\mathcal{A} = K$, um corpo.
- (II) $\mathcal{A} = (K, \alpha)$, uma duplicação do corpo K pelo processo de Cayley-Dickson, que pode resultar numa extensão de grau 2 do corpo K ou numa soma direta de duas cópias de K .
- (III) $\mathcal{A} = \mathcal{Q}(K, \alpha, \beta)$, uma álgebra de quatérnios generalizados sobre K .
- (IV) $\mathcal{A} = \mathcal{C}(K, \alpha, \beta, \gamma)$, uma álgebra de Cayley-Dickson sobre K .

As Tabelas 1.2.2 e 1.2.3 na página seguinte destacam as tábuas das álgebras $\mathcal{C}(K, -1, -1, -1)$ e $\mathcal{C}(K, -1 - 1, 1)$, respectivamente, para um futuro uso.

$$\mathcal{C}(K, -1, -1, -1)$$

	1	e_1	e_2	e_3	e_4	e_5	e_6	e_7
1	1	e_1	e_2	e_3	e_4	e_5	e_6	e_7
e_1	e_1	-1	e_3	$-e_2$	e_5	$-e_4$	$-e_7$	e_6
e_2	e_2	$-e_3$	-1	e_1	e_6	e_7	$-e_4$	$-e_5$
e_3	e_3	e_2	$-e_1$	-1	e_7	$-e_6$	e_5	$-e_4$
e_4	e_4	$-e_5$	$-e_6$	$-e_7$	-1	e_1	e_2	e_3
e_5	e_5	e_4	$-e_7$	e_6	$-e_1$	-1	$-e_3$	e_2
e_6	e_6	e_7	e_4	$-e_5$	$-e_2$	e_3	-1	$-e_1$
e_7	e_7	$-e_6$	e_5	e_4	$-e_3$	$-e_2$	e_1	-1

Tabela 1.2.2

$$\mathcal{C}(K, -1, -1, 1)$$

	1	e_1	e_2	e_3	e_4	e_5	e_6	e_7
1	1	e_1	e_2	e_3	e_4	e_5	e_6	e_7
e_1	e_1	-1	e_3	$-e_2$	e_5	$-e_4$	$-e_7$	e_6
e_2	e_2	$-e_3$	-1	e_1	e_6	e_7	$-e_4$	$-e_5$
e_3	e_3	e_2	$-e_1$	-1	e_7	$-e_6$	e_5	$-e_4$
e_4	e_4	$-e_5$	$-e_6$	$-e_7$	1	$-e_1$	$-e_2$	$-e_3$
e_5	e_5	e_4	$-e_7$	e_6	e_1	1	e_3	$-e_2$
e_6	e_6	e_7	e_4	$-e_5$	e_2	$-e_3$	1	e_1
e_7	e_7	$-e_6$	e_5	e_4	e_3	e_2	$-e_1$	1

Tabela 1.2.3

Se uma álgebra não possui divisores de zero dizemos que essa álgebra é uma *álgebra com divisão*. Caso contrário, ela é chamada uma *álgebra “split”*.

Usando a Tabela 1.2.3, o produto

$$(1 + e_5).(1 - e_5) = 0$$

mostra que a álgebra $\mathcal{C}(K, -1, -1, 1)$ é “split” qualquer que seja o corpo K .

Tomando $r = \sum_{i=0}^7 a_i.e_i \neq 0$ em $\mathcal{C}(K, -1, -1, -1)$, o elemento $\bar{r} = a_0 - \sum_{i=1}^7 a_i.e_i$ é tal que $r.\bar{r} = \sum_{i=0}^7 a_i^2 \in K$. Se tomamos, por exemplo, $K = \mathbb{Q}$, o corpo dos números racionais, então o elemento r é inversível e $r^{-1} = \frac{1}{r.\bar{r}}.\bar{r}$. Dessa forma $\mathcal{C}(\mathbb{Q}, -1, -1, -1)$ é uma álgebra com divisão.

É conhecido, ([8], [20]), que a álgebra de quatérnios generalizados $\mathcal{Q}(K, \alpha, \beta)$ é uma álgebra com divisão se e somente se a equação $X^2 - \alpha Y^2 = \beta$ não admite solução em K . Vamos estabelecer um resultado análogo para a álgebra de Cayley-Dickson $\mathcal{C}(K, \alpha, \beta, \gamma)$.

Proposição 1.2.1 *Suponhamos que $\mathcal{Q}(K, \alpha, \beta) = \mathcal{Q}$ seja uma álgebra com divisão. Então $\mathcal{C}(K, \alpha, \beta, \gamma) = \mathcal{C}$ é uma álgebra com divisão se e somente se a equação $X^2 - \alpha Y^2 - \beta Z^2 + \alpha\beta W^2 = \gamma$ não admite solução em K .*

Demonstração: Seja $\{e_0 = 1, e_1, \dots, e_7\}$ uma K -base para $\mathcal{C}$ como acima. Suponhamos que existam $a, b, c, d \in K$ tais que $a^2 - \alpha b^2 - \beta c^2 + \alpha\beta d^2 = \gamma$. Então para

$$q = ae_0 + be_1 + ce_2 + de_3 + e_4 \quad e$$

$$q^* = ae_0 - be_1 - ce_2 - de_3 - e_4$$

nós temos $q.q^* = a^2 - \alpha b^2 - \beta c^2 + \alpha\beta d^2 - \gamma = 0$. Portanto em $\mathcal{C}$ há divisores de zero.

Reciprocamente, suponhamos que a equação $X^2 - \alpha Y^2 - \beta Z^2 + \alpha\beta W^2 = \gamma$ não é solúvel em K . Primeiro observamos que os elementos em $\mathcal{C}$ da forma $q = a_0e_0 + a_1e_1 + a_2e_2 + a_3e_3 + e_4$ são inversíveis com $q^{-1} = \frac{1}{m}(a_0e_0 - a_1e_1 - a_2e_2 - a_3e_3 - e_4)$, onde $m = a_0^2 - \alpha a_1^2 - \beta a_2^2 + \alpha\beta a_3^2 - \gamma \neq 0$.

Seja $q = \sum_{i=0}^7 a_i e_i \neq 0$ em $\mathcal{C}$. Escreva $q = r + s.e_4$ com $r = a_0e_0 + a_1e_1 + a_2e_2 + a_3e_3$ e $s = a_4e_0 + a_5e_1 + a_6e_2 + a_7e_3$. Se $s = 0$ então $q = r \neq 0$ é inversível em $\mathcal{Q}$. Se $s \neq 0$ então s é inversível em $\mathcal{Q}$ e podemos escrever $s^{-1}q = b_0e_0 + b_1e_1 + b_2e_2 + b_3e_3 + e_4$ com b_0, b_1, b_2 e b_3 em K . Logo $s^{-1}q$ é inversível em $\mathcal{C}$ e segue que q é inversível em $\mathcal{C}$. $\square$

Como veremos adiante, as álgebras de Cayley-Dickson que estão relacionadas com as álgebras de loops são álgebras da forma $\mathcal{C}(K, -1, -1, -1)$ e $\mathcal{C}(K, -1, -1, 1)$. Porisso estabelecemos os seguintes corolários:

Corolário 1.2.2

- i) A álgebra $\mathcal{C}(K, -1, -1, 1)$ é “split” para todo K .
- ii) A álgebra de Cayley-Dickson $\mathcal{C}(K, -1, -1, -1)$ é uma álgebra com divisão se e somente se a equação $X^2 + Y^2 + Z^2 + W^2 = -1$ não admite solução em K .

Para o caso $K = \mathbb{Q}$, explicitamos

Corolário 1.2.3

A álgebra $\mathcal{C}(\mathbb{Q}, -1, -1, -1)$ é uma álgebra com divisão e a álgebra $\mathcal{C}(\mathbb{Q}, -1, -1, 1)$ é uma álgebra “split”.

A álgebra com divisão $\mathcal{C}(\mathbb{Q}, -1, -1, -1)$, que denotaremos por $\mathcal{C}(\mathbb{Q})$, pode ser obtida pela duplicação da álgebra dos quatérnios clássicos sobre os racionais, $\mathcal{Q}(\mathbb{Q}, -1, -1)$, que denotaremos simplesmente por $\mathcal{Q}$. Isto é, $\mathcal{C}(\mathbb{Q}) \cong (\mathcal{Q}, -1)$. Na decomposição das álgebras de loops racionais como soma direta de componentes simples, $\mathcal{C}(\mathbb{Q})$ desempenha papel análogo ao que $\mathcal{Q}$ desempenha na decomposição das álgebras de grupos sobre os racionais.

Em [25], está demonstrado que duas álgebras de composição “split” de mesma dimensão sobre um mesmo corpo são isomorfas. Portanto todas álgebras de composição “split”, cuja dimensão sobre $\mathbb{Q}$ seja 8, são isomorfas a $\mathcal{C}(\mathbb{Q}, -1 - 1, 1)$, a qual denotaremos simplesmente por $\mathcal{C}_S(\mathbb{Q})$. Esta álgebra pode ser obtida pela duplicação da álgebra das matrizes 2×2 sobre $\mathbb{Q}$, $M_2(\mathbb{Q})$, pelo processo de duplicação de Cayley-Dickson, isto é, $\mathcal{C}_S(\mathbb{Q}) = (M_2(\mathbb{Q}), -1)$. Ela também pode ser obtida pela duplicação da álgebra dos quatérnios clássicos sobre os racionais na forma $\mathcal{C}_S(\mathbb{Q}) = (\mathcal{Q}, 1)$. Em [25] está feita essa construção, que origina a chamada *álgebra matricial de Cayley-Dickson*. Na decomposição de uma álgebra de loop sobre os racionais como soma direta de componentes simples, essa álgebra vai desempenhar um papel análogo àquele que $M_2(\mathbb{Q})$ desempenha na decomposição das álgebras de grupos sobre os racionais.

Corolário 1.2.4

Seja K um corpo finito. Então as álgebras $\mathcal{C}(K, -1, -1, -1)$ e $\mathcal{C}(K, -1, -1, 1)$ são “split”.

Demonstração: Em [23] está demonstrado que a equação $X^2 + Y^2 = -1$ tem solução num corpo finito K . Dessa forma, a equação $X^2 + Y^2 + Z^2 + W^2 = -1$ também tem solução em K . Pelo corolário 1.2.2, ii) segue que $\mathcal{C}(K, -1 - 1 - 1)$ é uma álgebra “split”. A outra álgebra é “split” para todo corpo K . $\square$

1.3 Álgebras de Loops Alternativas Semisimples

Seja L um R.A. loop que é determinado pelo grupo G . Seja R um anel cuja característica não divide a ordem de L . Observamos, de início, que esta condição implica que $\text{car} R \neq 2$. Denotemos por $\mathcal{J}(RL)$ e $\mathcal{J}(RG)$ respectivamente os radicais de Jacobson de RL e RG . Em 1987, E. G. Goodaire e M. M. Parmenter [11] provaram que $\mathcal{J}(RL) = 0$ se e somente se $\mathcal{J}(RG) = 0$.

Aqui vamos considerar um corpo K tal que $\text{car} K \nmid |L|$. Então $\text{car} K \nmid |G|$, o que implica $\mathcal{J}(KG) = 0$. Logo $\mathcal{J}(KL) = 0$ e portanto KL é uma álgebra semiprima.

Existe um resultado, devido a Dieudonné, cuja demonstração se encontra em [19], que se aplica a este caso:

Teorema 1.3.1 *Seja A uma álgebra (não necessariamente associativa) sobre um corpo K que é semiprima e de dimensão finita. Suponha que esteja definida em A uma forma bilinear não degenerada que é simétrica e associativa. Então A é soma direta de ideais simples.*

O teorema seguinte é devido a E. G. Goodaire [10].

Teorema 1.3.2 *Seja L um R.A. loop e seja K um corpo tal que $\text{car} K \nmid |L|$. Então $KL \cong \bigoplus \mathcal{A}_i$, onde cada componente $\mathcal{A}_i$ é uma álgebra de composição simples.*

Demonstração: Todo loop de Moufang tem a propriedade de que, se g , h e k são elementos desse loop, então

$$gh.k = 1 \iff g.hk = 1.$$

Portanto L tem essa propriedade.

Se $r = \sum \alpha_g.g \in KL$, seja $r(1)$ o coeficiente de 1 nessa expansão. Para r e s em KL definamos $\varphi(r, s) = (rs)(1)$. Então φ é uma forma bilinear em KL . Vamos mostrar que φ é como no teorema anterior.

Considere $s = \sum \beta_h.h$ e $t = \sum \gamma_k.k$ em KL . Como

$$\varphi(rs, t) = (rs.t)(1) = \sum_{lm.n=1} \alpha_l \beta_m \gamma_n = \sum_{l.mn=1} \alpha_l \beta_m \gamma_n = (r.st)(1) = \varphi(r, st),$$

temos que φ é associativa.

Como $rs(1) = \sum_{l \in L} \alpha_l \beta_{l^{-1}} = sr(1)$, temos que φ é simétrica.

Para mostrar que φ é não degenerada, suponhamos que exista $r = \sum \alpha_g.g \in KL$ tal que $\varphi(r, KL) = 0$. Então $\varphi(r, g^{-1}) = 0$ para todo $g \in L$. Mas, $\varphi(r, g^{-1}) = \alpha_g$. Logo $r = \sum \alpha_g.g = 0$.

Pelo teorema 1.3.1 concluímos que $KL \cong \bigoplus \mathcal{A}_i$, onde cada $\mathcal{A}_i$ é uma álgebra simples. Vamos mostrar que são álgebras de composição.

Consideremos o grupo G que determina L e a involução $*$: $G \longrightarrow G$ tal que $L = L(G, *, g_o)$. Essa involução se estende para $*$: $KG \longrightarrow KG$, definindo $(\sum \alpha_g.g)^* = \sum \alpha_g.g^*$, e é fácil ver que $\alpha.\alpha^* \in Z(KG)$ para todo $\alpha \in KG$.

Essa involução também se estende para KL da seguinte maneira: cada $r \in KL$ pode ser escrito na forma $r = \alpha + \beta.u$ com α e β em KG e u como

no teorema 1.1.2. Defina então $r^* = \alpha^* + e.\beta.u$, onde e é o único comutador em L distinto da unidade. Neste caso, conforme [11], demonstra-se também que $r.r^* \in Z(KL)$.

Definimos agora $n(r) = r.r^*$ e consideramos sua restrição $n_i = n|_{\mathcal{A}_i} : \mathcal{A}_i \longrightarrow Z(\mathcal{A}_i)$. Observando, conforme [25], que $Z(\mathcal{A}_i) = K_i$ é um corpo, temos que n_i é uma forma quadrática com valores nesse corpo.

Para $r, s \in KL$ demonstra-se [10] que $n(rs) = (rs).(rs)^* = rs.s^*r^* = rr^*.ss^* = n(r).n(s)$. Portanto n e n_i admitem composição.

Resta provar que n_i é estritamente não degenerada, isto é, que a forma bilinear $f(a, b) = n_i(a + b) - n_i(a) - n_i(b)$ é não degenerada em $\mathcal{A}_i$. Consideremos então o conjunto $B = \{a \in \mathcal{A}_i \mid f(a, \mathcal{A}_i) = 0\}$ e mostremos que $B = \{0\}$. Para isso vamos mostrar primeiro que B é um ideal bilateral de $\mathcal{A}_i$. Linearizando f , obtemos

$$f(a, b).f(c, d) = f(ac, bd) + f(ad, bc)$$

Tomemos, $a \in B$, $d = 1$ e $b, c \in \mathcal{A}_i$. Como $f(a, b) = 0$, obtemos $f(ac, b) = 0$ e concluímos que $ac \in B$. Logo B é um ideal à direita de $\mathcal{A}_i$. Analogamente se mostra que B é um ideal à esquerda.

Como $f(1, 1) = 2$, temos que $B \neq \mathcal{A}_i$. Como $\mathcal{A}_i$ é um anel simples, segue que $B = 0$. Portanto f é não degenerada e podemos afirmar que cada componente simples $\mathcal{A}_i$ na decomposição de KL é uma álgebra de composição. $\square$

Se G é um grupo que determina L , a demonstração acima se aplica também à álgebra associativa KG e podemos escrever $KG \cong \bigoplus \mathcal{B}_i$, onde cada $\mathcal{B}_i$ é uma

álgebra de composição simples.

Uma outra abordagem foi feita por G. Leal e C. P. Milies [15] em 1990 para $K = \mathbb{Q}$, o corpo dos números racionais, usando técnicas de anéis de grupos devidas a D. B. Coleman [6]. Essa abordagem se generaliza facilmente para um corpo K tal $\text{car}K \nmid |L|$.

Como $L' \triangleleft L$, consideramos o quociente $\frac{L}{L'}$, que é um grupo abeliano. Neste momento é bom destacar um clássico resultado de S. Perlis e G. L. Walker [17] para álgebras de grupos abelianos e que utilizaremos muitas vezes no decorrer deste trabalho.

Teorema 1.3.3 *Seja A um grupo abeliano de ordem n , K um corpo tal que $\text{car}K \nmid n$, ξ_d uma raiz d -ésima primitiva da unidade e n_d o número de elementos de ordem d em A . Então $KA \cong \bigoplus_{d|n} v_d K(\xi_d)$, onde $v_d = \frac{n_d}{[K(\xi_d) : K]}$ e $v_d K(\xi_d)$ denota a soma direta de v_d cópias of $K(\xi_d)$.*

Voltando aos R.A. loops, consideramos a projeção natural $\omega : L \longrightarrow \frac{L}{L'}$. Essa projeção se estende de modo natural para $\omega : KL \longrightarrow K \left[\frac{L}{L'} \right]$, que é um epimorfismo de álgebras. Chamando $\text{Ker}\omega = \Delta_K(L : L')$, como KL é semisimples, segue que

$$KL \cong K \left[\frac{L}{L'} \right] \oplus \Delta_K(L : L')$$

O elemento $\hat{L}' = \frac{1+e}{2}$ é um idempotente central em KL . Portanto

$$KL = KL.\hat{L}' \oplus KL.(1 - \hat{L}').$$

Vale o seguinte resultado análogo ao de [15]:

Proposição 1.3.4 *Seja L um R.A. loop e K um corpo tal que $\text{car} K \nmid |L|$. Seja $\hat{L}'$ como acima. Então*

- (i) $KL.\hat{L}' \cong K \left[\frac{L}{L'} \right]$
- (ii) $KL.(1 - \hat{L}') = \Delta_K(L : L')$.

Demonstração: Notemos que basta provar (ii) pois

$$KL.\hat{L}' \cong \frac{KL}{KL.(1 - \hat{L}')} = \frac{KL}{\Delta_K(L : L')} \cong K \left[\frac{L}{L'} \right]$$

Seja então $\alpha \in KL.(1 - \hat{L}')$. Então $\omega(\alpha) = 0$, isto é, $\alpha \in \Delta_K(L : L')$. Por outro lado, $\Delta_K(L : L')$ é gerado pelo conjunto $\{1 - x \mid x \in L'\}$. Como $(1 - x).(1 - \hat{L}') = 1 - \hat{L}' - x + x.\hat{L}' = 1 - x$, concluímos que $1 - x \in KL.(1 - \hat{L}')$. Logo $\Delta_K(L : L') \subset KL.(1 - \hat{L}')$. $\square$

Destacamos então o seguinte resultado, que é análogo ao de D. B. Coleman [6] para anéis de grupos:

Proposição 1.3.5 *Seja L um R.A. loop e K um corpo tal $\text{car} K \nmid |L|$ e escrevamos $KL = \mathcal{I} \oplus \mathcal{J}$, onde $\mathcal{I}$ e $\mathcal{J}$ são ideais bilaterais. Então $\mathcal{I}$ é comutativo se e somente se $\mathcal{J} \supset \Delta_K(L : L')$.*

Demonstração: Sabemos que $\Delta(L : L') = KL.(1 - \hat{L}') = KL.\left(\frac{1 - e}{2}\right) = KL.(1 - e)$. Suponhamos que $\mathcal{J} \supset \Delta_K(L : L')$. Então $(1 - e) \in \mathcal{J}$.

Sejam $l, m \in L$. Se $lm = ml$ então $lm - ml \in \mathcal{J}$. Se $lm \neq ml$ então $ml = e.lm$ e $lm - ml = lm.(1 - e) \in KL.(1 - e) \subset \mathcal{J}$. Portanto $lm - ml \in \mathcal{J}$ para todos $l, m \in L$, o que implica que $\mathcal{I} \cong \frac{KL}{\mathcal{J}}$ é comutativo.

Reciprocamente, se $\mathcal{I} \cong \frac{KL}{\mathcal{J}}$ é comutativo então $lm - ml \in \mathcal{J}$ para todos $l, m \in L$. Sejam $l, m \in L$ tais que $lm \neq ml$. Então $ml = lme$. Logo $lm - ml = lm - lme = lm.(1 - e) \in \mathcal{J}$, donde concluímos que $(1 - e) \in \mathcal{J}$. Dessa forma $KL.(1 - e) \subset \mathcal{J}$, isto é, $\Delta_K(L : L') \subset \mathcal{J}$. $\square$

Como consequência dessa proposição temos o seguinte resultado, que será fundamental para o nosso trabalho.

Teorema 1.3.6 *Sejam K um corpo e L e M R.A. loops tais que $\text{car} K \nmid |L|$. Então $KL \cong KM$ se e somente se $K \left[\frac{L}{L'} \right] \cong K \left[\frac{M}{M'} \right]$ e $\Delta_K(L : L') \cong \Delta_K(M : M')$.*

Pretendemos agora analisar com mais detalhe a estrutura da álgebra KL .

Como $\frac{L}{L'}$ é um grupo abeliano, utilizando o teorema 1.3.3 obtemos

$$K \left[\frac{L}{L'} \right] \cong \bigoplus_i K(\xi_{d_i}),$$

onde ξ_{d_i} são raízes d_i -ésimas da unidade. Resta explicitar $\Delta_K(L : L')$.

Como $Z(KL) = K \left[\frac{L}{L'} \right] \oplus Z(\Delta_K(L : L'))$, obtemos outro resultado análogo ao de [15] que é

Proposição 1.3.7 *Seja L um R.A. loop e K um corpo tal $\text{car} K \nmid |L|$. Então $Z(\Delta_K(L : L')) = Z(KL.(1 - \hat{L}')) = K[Z(L)].(1 - \hat{L}')$.*

Demonstração: A primeira igualdade segue da proposição 1.3.4. Vamos à segunda igualdade. É fácil ver que $K[Z(L)].(1 - \hat{L}') \subset Z(KL.(1 - \hat{L}'))$. Vamos à inclusão contrária.

Seja $\alpha \in Z(KL.(1 - \hat{L}')) = Z(KL) \cap KL.(1 - \hat{L}')$. Como $\alpha \in KL.(1 - \hat{L}')$ temos que $\alpha = \beta.(1 - \hat{L}')$ com $\beta \in KL$. Então $\alpha.(1 - \hat{L}') = \beta.(1 - \hat{L}')^2 = \beta.(1 - \hat{L}') = \alpha$.

Além disso, as classes de conjugação de L são da forma $\{l\}$ se $l \in Z(L)$ ou $\{l, el\}$ se $l \notin Z(L)$. Assim podemos escrever

$$\alpha = \sum_{l \in Z(L)} \alpha_l.l + \sum_{l \notin Z(L)} \alpha_l.l.(1 + e) = \sum_{l \in Z(L)} \alpha_l.l + \sum_{l \notin Z(L)} \alpha_l.2l.\hat{L}'.$$

Logo $\alpha.(1 - \hat{L}') = \sum_{l \in Z(L)} \alpha_l.l.(1 - \hat{L}') \in K[Z(L)].(1 - \hat{L}')$. Como $\alpha = \alpha.(1 - \hat{L}')$, concluímos que $\alpha \in K[Z(L)].(1 - \hat{L}')$. $\square$

Como consequência dos resultados anteriores, estabelecemos a seguinte:

Proposição 1.3.8 *Sejam L e K como antes. Então $Z(\Delta_K(L : L')) \cong \bigoplus_{i=1}^m K(\xi_{d_i})$, onde ξ_{d_i} é uma raiz d_i -ésima primitiva da unidade.*

Demonstração: Suponha $Z(L) \cong C_{2^{n_1}} \times C_{2^{n_2}} \times \dots \times C_{2^{n_t}} \times A$, onde $n_1 \geq 1$, $n_i \geq 0$ for $i = 2, 3, \dots, t$, $L' \subset C_{2^{n_1}}$ e A é um grupo abeliano de ordem ímpar.

Notemos que

$$Z(\Delta_K(L : L')) \cong K[Z(L)].(1 - \hat{L}') = [(KC_{2^{n_1}}).(1 - \hat{L}')] [C_{2^{n_2}} \times \dots \times C_{2^{n_t}}] \times A.$$

Pelo teorema 1.3.3, sabemos que $KC_{2^{n_1}} \cong \bigoplus_{i=0}^{n_1} \frac{v_i}{[K(\xi_{2^i}) : K]} \cdot K(\xi_{2^i})$, onde v_i é o

número de elementos de ordem 2^i em $C_{2^{n_1}}$. Logo

$$KC_{2^{n_1}} \cong \bigoplus_{i=0}^{n_1} \frac{2^{i-1}}{[K(\xi_{2^i}) : K]} \cdot K(\xi_{2^i}) .$$

Por outro lado, nós temos que $KC_{2^{n_1}} \cong K \left[\frac{C_{2^{n_1}}}{L'} \right] \oplus \Delta_K(C_{2^{n_1}} : L')$ e
 $K \left[\frac{C_{2^{n_1}}}{L'} \right] \cong K[C_{2^{n_1-1}}] \cong \bigoplus_{i=1}^{n_1-1} \frac{2^{i-1}}{[K(\xi_{2^i}) : K]} K(\xi_{2^i}) .$

Comparando, obtemos

$$(KC_{2^{n_1}}) \cdot (1 - \hat{L}') = \Delta(C_{2^{n_1}} : L') \cong \frac{2^{n_1-1}}{[K(\xi_{2^{n_1}}) : K]} \cdot K(\xi_{2^i}) .$$

Aplicando novamente o teorema 1.3.3, concluimos que

$$\begin{aligned} Z(\Delta_K(L : L')) &\cong \left[\frac{2^{n_1-1}}{[K(\xi_{2^{n_1-1}}) : K]} \cdot K(\xi_{2^i}) \right] [C_{2^{n_2}} \times \cdots \times C_{2^{n_t}} \times A] \cong \\ &\cong \bigoplus_{i=1}^m K(\xi_{d_i}) . \end{aligned}$$

□

Seja G é um grupo que determina L . Então $Z(L) = Z(G)$, $L' = G'$ e segue facilmente que

$$Z(\Delta_K(G : G')) = K[Z(G)] \cdot \left(\frac{1-e}{2} \right) = K[Z(L)] \cdot \left(\frac{1-e}{2} \right) = Z(\Delta_K(L : L')) .$$

Escrevamos $Z(\Delta_K(L : L')) \cong Z(\Delta_K(G : G')) \cong \bigoplus_{i=1}^m K_i$. Assim temos que

$$KG \cong K \left[\frac{G}{G'} \right] \oplus \bigoplus_{i=1}^m \mathcal{B}_i(K_i) ,$$

onde cada $\mathcal{B}_i(K_i)$ é uma álgebra de composição simples sobre seu centro K_i e

$$KL \cong K \left[\frac{L}{L'} \right] \oplus \bigoplus_{i=1}^m \mathcal{A}_i(K_i) ,$$

onde cada $\mathcal{A}_i(K_i)$ é uma álgebra de composição simples sobre seu centro K_i .

Como cada $\mathcal{B}_i(K_i)$ é uma álgebra de composição simples associativa e não comutativa, concluímos que cada uma delas é uma álgebra de quatérnios generalizados sobre seu centro K_i .

Como $|L| = 2 \cdot |G|$, $\left| \frac{L}{L'} \right| = 2 \cdot \left| \frac{G}{G'} \right|$ e como $\Delta_K(L : L')$ e $\Delta_K(G : G')$ tem o mesmo número de somandos simples, concluímos que cada $\mathcal{A}_i$ é uma álgebra de composição simples de dimensão 8 sobre seu centro K_i e, portanto, cada uma delas é uma álgebra de Cayley-Dickson sobre seu centro.

Resumimos essas considerações no seguinte teorema, que é análogo a um resultado existente para álgebras de grupos:

Teorema 1.3.9 *Seja L uma R.A. loop e K um corpo tal que $\text{car} K \nmid |L|$. Então a álgebra de loop KL se decompõe como uma soma direta de componentes simples, que são ou extensões de K por raízes da unidade ou álgebras de Cayley-Dickson sobre extensões de K por raízes da unidade.*

Capítulo 2

O Problema do Isomorfismo para Álgebras de Loops Racionais

Neste capítulo estudaremos a seguinte questão: dados os R.A. loops L e M tais que suas álgebras de loops sobre os racionais, $\mathbb{Q}L$ e $\mathbb{Q}M$, são isomorfas, o que podemos afirmar sobre L e M ?

2.1 Alguns resultados

Seja L um R.A. loop e consideremos sua álgebra de loop $\mathbb{Q}L$ sobre os racionais. Como $\text{car}\mathbb{Q} = 0$, a álgebra $\mathbb{Q}L$ é semisimples e podemos aplicar todos os resultados da seção 1.3. Assim temos que

$$\mathbb{Q}L \cong \mathbb{Q} \left[\frac{L}{L'} \right] \oplus \Delta_{\mathbb{Q}}(L : L') \quad .$$

Para facilitar a notação, neste capítulo escreveremos apenas $\Delta(L : L')$ no lugar de $\Delta_{\mathbf{Q}}(L : L')$.

A nossa grande ferramenta aqui será o teorema 1.3.6. Observando que o quociente $\frac{L}{L'}$ é um grupo abeliano e lembrando o clássico resultado de S. Perlis e G. L. Walker [17] para álgebras de grupos abelianos, o enunciado desse teorema na situação em que o corpo é $\mathbf{Q}$, pode ser reescrito assim

Teorema 2.1.1 *Sejam L e M R.A. loops. Então $\mathbf{Q}L \cong \mathbf{Q}M$ se e somente se $\frac{L}{L'} \cong \frac{M}{M'}$ e $\Delta(L : L') \cong \Delta(M : M')$.*

Em 1990, G. Leal e C. Polcino Milies, [15], abordaram pela primeira vez o problema do isomorfismo para álgebras de loops racionais e obtiveram o seguinte resultado:

Teorema 2.1.2 *Seja L um R.A. loop e suponhamos que existe um elemento $\alpha \in Z(L)$ talque $\alpha^2 = e \in L'$. Seja M outro loop. Então $\mathbf{Q}L \cong \mathbf{Q}M$ se e somente se $\frac{L}{L'} \cong \frac{M}{M'}$ e $Z(\mathbf{Q}L) \cong Z(\mathbf{Q}M)$.*

Como $Z(\mathbf{Q}L) \cong \mathbf{Q} \left[\frac{L}{L'} \right] \oplus Z(\Delta(L : L'))$, este teorema mostra que nesse caso $\Delta(L : L') \cong \Delta(M : M')$ se e somente se $Z(\Delta(L : L')) \cong Z(\Delta(M : M'))$.

É nossa intenção neste capítulo tratar do problema no caso em que o R.A. loop L não contem um elemento α com aquela propriedade.

Sabemos que $Z(L) = C_{2^{n_1}} \times C_{2^{n_2}} \times \cdots \times C_{2^{n_t}} \times A$, onde A é um grupo abeliano de ordem ímpar, e que podemos sempre considerar $L' \subset C_{2^{n_1}}$. Um tal

elemento α existe se e somente se $n_1 > 1$. Para diferenciar uma situação da outra diremos que L é um R.A. loop do tipo I se $n_1 > 1$ e que L é um R.A. loop do tipo II se $n_1 = 1$.

Como se percebe pelo teorema 2.1.1, no decorrer do trabalho precisaremos de informações sobre a estrutura do quociente $\frac{L}{L'}$, principalmente quando L é um R.A. loop indecomponível. É isso que vamos fazer agora.

Proposição 2.1.3 *Seja L um R.A. loop indecomponível e escrevamos*

$Z(L) = \langle t_1 \rangle \times \langle t_2 \rangle \times \langle t_3 \rangle \times \langle w \rangle \cong C_{2^a} \times C_{2^b} \times C_{2^c} \times C_{2^d}$,
com $a \geq 1$, $b, c, d \geq 0$ e $L' \subset \langle t_1 \rangle$. Então $\frac{L}{L'}$ é isomorfo a um dos seguintes grupos:

$$(I) C_{2^{a-1}} \times C_{2^{b+1}} \times C_{2^{c+1}} \times C_{2^{d+1}}$$

$$(II) C_{2^a} \times C_{2^{b+1}} \times C_{2^{c+1}} \times C_{2^d}$$

Demonstração: Denotemos por $\overline{m}$ a classe de um elemento $m \in L$ no quociente $\frac{L}{L'}$. Usando a classificação da tabela 1.1.2, temos os seguintes casos a considerar:

(i) L é da família L_1 , L_3 ou L_5 .

Neste caso vamos provar que

$$\frac{L}{L'} = \langle \overline{t_1} \rangle \times \langle \overline{x} \rangle \times \langle \overline{y} \rangle \times \langle \overline{u} \rangle \cong C_{2^{a-1}} \times C_{2^{b+1}} \times C_{2^{c+1}} \times C_2.$$

Notemos que $o(\overline{t_1}) = 2^{a-1}$, $o(\overline{x}) = 2^{b+1}$, $o(\overline{y}) = 2^{c+1}$ e $o(\overline{u}) = 2$. Basta mostrar que esses elementos são independentes em $\frac{L}{L'}$. Suponhamos que $\overline{t_1}^\alpha \cdot \overline{x}^\beta \cdot \overline{y}^\gamma \cdot \overline{u}^\delta = \overline{1}$ (*).

Temos que mostrar que $\overline{t_1}^\alpha = \overline{x}^\beta = \overline{y}^\gamma = \overline{u}^\delta = \overline{1}$.

Da igualdade (*), tiramos que $t_1^\alpha . x^\beta . y^\gamma . u^\delta \in L' \subset Z(L)$, o que implica $x^\beta . y^\gamma . u^\delta \in Z(L)$. Como x, y e u não associam, concluímos que β, γ e δ são pares. Escrevamos $\alpha = 2\alpha_1$, $\beta = 2\beta_1$ e $\gamma = 2\gamma_1$. Então $\overline{x}^\beta = (\overline{x}^2)^{\beta_1} = \overline{t_2}^{\beta_1}$, $\overline{y}^\gamma = (\overline{y}^2)^{\gamma_1} = \overline{t_3}^{\gamma_1}$ e $\overline{u}^\delta = (\overline{u}^2)^{\delta_1} = \overline{1}$. Substituindo em (*), segue que $\overline{t_1}^\alpha . \overline{t_2}^{\beta_1} . \overline{t_3}^{\gamma_1} = \overline{1}$, o que implica $t_1^\alpha . t_2^{\beta_1} . t_3^{\gamma_1} \in L' \subset \langle t_1 \rangle$. Logo, $t_2^{\beta_1} = t_3^{\gamma_1} = 1$, isto é, $\overline{x}^\beta = \overline{1}$ e $\overline{y}^\gamma = \overline{1}$. Voltando em (*), tiramos $\overline{t_1}^\alpha = \overline{1}$.

(ii) L é da família L_2 .

Neste caso, denotando por $u_1 = uy . t_1^{(2^a-1-1)}$ e $x_1 = xy . t_1^{(2^a-1-1)}$, vamos provar que

$$\frac{L}{L'} = \langle \overline{y} \rangle \times \langle \overline{u_1} \rangle \times \langle \overline{x_1} \rangle \cong C_{2^a} \times C_2 \times C_2 .$$

Basta verificar que $o(\overline{y}) = 2^a$, $o(\overline{u_1}) = 2$ e $o(\overline{x_1}) = 2$ e mostrar que são independentes em $\frac{L}{L'}$. A demonstração é idêntica à anterior.

iii) L é da família L_4 .

De forma análoga, provamos que

$$\frac{L}{L'} = \langle \overline{x} \rangle \times \langle \overline{y} \rangle \times \langle \overline{u_1} \rangle \cong C_{2^a} \times C_{2^{b+1}} \times C_2 ,$$

onde $u_1 = ux . t_1^{(2^a-1-1)}$.

(iv) L é da família L_6 .

Neste caso provamos que

$$\frac{L}{L'} = \langle \overline{u} \rangle \times \langle \overline{x} \rangle \times \langle \overline{y} \rangle \cong C_{2^a} \times C_{2^{b+1}} \times C_{2^{c+1}} .$$

(v) L é da família L_7 .

Neste caso provamos que

$$\frac{L}{L'} = \langle \overline{t_1} \rangle \times \langle \overline{x} \rangle \times \langle \overline{y} \rangle \times \langle \overline{u} \rangle \cong C_{2^{a-1}} \times C_{2^{b+1}} \times C_{2^{c+1}} \times C_{2^{d+1}} .$$

□

Em particular, para os R.A. 2-loops indecomponíveis do tipo II vale

Corolário 2.1.4

Seja L um R.A. loop indecomponível de tipo II. Escreva $Z(L) \cong L' \times C_{2^b} \times C_{2^c} \times C_{2^d}$ com $b, c, d \geq 0$. Então $\frac{L}{L'} \cong C_{2^{b+1}} \times C_{2^{c+1}} \times C_{2^{d+1}}$.

2.2 As álgebras dos R.A. loops indecomponíveis cujo centro é de expoente 2

Como $Z(L)^2 \triangleleft L$, vamos considerar o quociente $\frac{L}{Z(L)^2}$. Escrevamos $Z(L) = C_{2^{n_1}} \times C_{2^{n_2}} \times \cdots \times C_{2^{n_t}} \times A$, onde A é um grupo abeliano de ordem ímpar e suponhamos que $L' \in C_{2^{n_1}}$.

Se L é um R.A. loop do tipo I, então $n_1 > 1$ e o quociente $\frac{L}{Z(L)^2}$ é um grupo abeliano, pois neste caso $L' \subset Z(L)^2$.

Se L é um R.A. loop do tipo II, então $C_{2^{n_1}} \cong L'$, e neste caso $\frac{L}{Z(L)^2}$ é um R.A. loop. Em particular, se L é um R.A. 2-loop do tipo II, então $Z\left(\frac{L}{Z(L)^2}\right)$ é um grupo abeliano de expoente 2.

Esse tipo de argumento, estudar o quociente $\frac{L}{Z(L)^2}$, será bastante utilizado neste capítulo. Dessa forma é interessante fazer um estudo sobre as álgebras de loops dos R.A. loops indecomponíveis, cujo centro é de expoente 2.

Segundo os resultados da Tabela 1.1.2, existem 7 R.A. loops indecom-

poníveis, cujo centro é de expoente 2. Denotaremos esses loops por $I_1, I_2, \dots, I_7$. Vamos descrever a construção de cada um deles e a decomposição como soma direta de ideais simples das suas álgebras de loops sobre os racionais.

Existem dois grupos indecomponíveis tais que o quociente deles pelo seu centro é isomorfo a $C_2 \times C_2$ e cujo centro é isomorfo a C_2 . Esses grupos, na notação de [24], são o grupo diedral $D_4 = \Gamma_2 a_1 = 8/4$ e o grupo dos quatérnios $Q = \Gamma_2 a_2 = 8/5$ ambos de ordem 8. Se na Tabela 1.1.2 tomamos $D_1 = D_4$, obtemos o R.A. loop indecomponível $I_1 = L(D_4, *, 1)$ de ordem 16, cujo centro é isomorfo a C_2 . Na notação de [3] esse é o loop $M_{16}(Q, 2)$. Denotando $Z(Q) = Q' = \{1, e\}$ e $Z(D_4) = D'_4 = \{1, f\} \cong C_2$, observamos que as construções $L(Q, *, e)$ e $L(D_4, *, f)$ também resultam $M_{16}(Q, 2)$.

Como $Z(I_1) = Z(D_4) \cong C_2$, pelo corolário 2.1.4, temos que $\frac{I_1}{I_1'} \cong C_2 \times C_2 \times C_2$, e pelo teorema 1.3.3, podemos escrever

$$\mathbb{Q} \left[\frac{I_1}{I_1'} \right] \cong \mathbb{Q}[C_2 \times C_2 \times C_2] \cong \underbrace{\mathbb{Q} \oplus \dots \oplus \mathbb{Q}}_{8 \text{ vezes}}.$$

Como

$$Z(\Delta(I_1 : I_1')) \cong \mathbb{Q}[Z(I_1)] \cdot \left(\frac{1-e'}{2} \right) \cong \mathbb{Q}C_2 \cdot \left(\frac{1-e'}{2} \right) \cong \mathbb{Q} ,$$

pelo teorema 1.3.9, temos que $\Delta(I_1 : I_1') \cong \mathcal{A}(Q)$, uma álgebra de Cayley-Dickson sobre Q .

É conhecido que $\Delta(D_4 : D'_4) \cong M_2(Q)$, o anel das matrizes 2×2 sobre Q . Como I_1 contém D_4 segue que $\Delta(D_4 : D'_4) = \mathbb{Q}D_4 \cdot \left(\frac{1-e'}{2} \right) \subset \mathbb{Q}I_1 \cdot \left(\frac{1-e'}{2} \right) \cong \Delta(I_1 : I_1')$, e concluímos que $\Delta(I_1 : I_1') \cong \mathcal{A}(Q)$, uma álgebra de Cayley-Dickson “split”. Como todas as álgebras de Cayley-Dickson “split” sobre Q são isomorfas, podemos tomar $\mathcal{A}(Q) \cong \mathcal{C}(Q, -1, -1, 1) = \mathcal{C}_S(Q)$.

Dessa forma, obtemos

$$\mathbf{QI}_1 \cong \underbrace{\mathbf{Q} \oplus \cdots \oplus \mathbf{Q}}_{8 \text{ vezes}} \oplus \mathcal{C}_S(\mathbf{Q})$$

A título de curiosidade podemos provar de forma explícita o isomorfismo $\Delta(\mathbf{I}_1 : \mathbf{I}_1') \cong \mathcal{C}_S(\mathbf{Q}, -1, -1, 1)$.

O R.A. loop $\mathbf{I}_1 = M_{16}(Q, 2) = D_4 \cup D_4.u = L(D_4, *, 1)$ tem a tábua dada pela Tabela 2.2.1. Observemos que o bloco 8×8 superior á esquerda é a tábua do grupo diedral D_4 com a notação de [24].

Na Tabela 2.2.1, chamando $g_1 = 5.u$, $g_2 = 6.u$, $g_3 = 4$, $g_4 = 8$, $g_5 = 4.u$, $g_6 = u$ e $g_7 = 7$ e lembrando que $L' = \{1, 3\} = \{1, e\}$, podemos escrever os elementos de $\mathbf{I}_1$ na forma

$$\mathbf{I}_1 = \{1, e, g_1, eg_1, \dots, g_7, eg_7\} ,$$

e sua tábua pode ser reescrita na forma da Tabela 2.2.2.

$$\mathbf{I}_1 = M_{16}(Q, 2) = L(D_4, *, 1)$$

	1	2	3	4	5	6	7	8	u	$2.u$	$3.u$	$4.u$	$5.u$	$6.u$	$7.u$	$8.u$
1	1	2	3	4	5	6	7	8	u	$2.u$	$3.u$	$4.u$	$5.u$	$6.u$	$7.u$	$8.u$
2	2	3	4	1	6	7	8	5	$2.u$	$3.u$	$4.u$	u	$8.u$	$5.u$	$6.u$	$7.u$
3	3	4	1	2	7	8	5	6	$3.u$	$4.u$	u	$2.u$	$7.u$	$8.u$	$5.u$	$6.u$
4	4	1	2	3	8	5	6	7	$4.u$	u	$2.u$	$3.u$	$6.u$	$7.u$	$8.u$	$5.u$
5	5	8	7	6	1	4	3	2	$5.u$	$6.u$	$7.u$	$8.u$	u	$2.u$	$3.u$	$4.u$
6	6	5	8	7	2	1	4	3	$6.u$	$7.u$	$8.u$	$5.u$	$4.u$	u	$2.u$	$3.u$
7	7	6	5	8	3	2	1	4	$7.u$	$8.u$	$5.u$	$6.u$	$3.u$	$4.u$	u	$2.u$
8	8	7	6	5	4	3	2	1	$8.u$	$5.u$	$6.u$	$7.u$	$2.u$	$3.u$	$4.u$	u
u	u	$4.u$	$3.u$	$2.u$	$7.u$	$8.u$	$5.u$	$6.u$	1	4	3	2	7	8	5	6
$2.u$	$2.u$	u	$4.u$	$3.u$	$8.u$	$5.u$	$6.u$	$7.u$	2	1	4	3	6	7	8	5
$3.u$	$3.u$	$2.u$	u	$4.u$	$5.u$	$6.u$	$7.u$	$8.u$	3	2	1	4	5	6	7	8
$4.u$	$4.u$	$3.u$	$2.u$	u	$6.u$	$7.u$	$8.u$	$5.u$	4	3	2	1	8	5	6	7
$5.u$	$5.u$	$6.u$	$7.u$	$8.u$	$3.u$	$2.u$	u	$4.u$	5	8	7	6	3	4	1	2
$6.u$	$6.u$	$7.u$	$8.u$	$5.u$	$4.u$	$3.u$	$2.u$	u	6	5	8	7	2	3	4	1
$7.u$	$7.u$	$8.u$	$5.u$	$6.u$	u	$4.u$	$3.u$	$2.u$	7	6	5	8	1	2	3	4
$8.u$	$8.u$	$5.u$	$6.u$	$7.u$	$2.u$	u	$4.u$	$3.u$	8	7	6	5	4	1	2	3

Tabela 2.2.1

$$\mathbf{I}_1 = \mathbf{M}_{16}(\mathbf{Q}, 2)$$

	1	e	g ₁	eg ₁	g ₂	eg ₂	g ₃	eg ₃	g ₄	eg ₄	g ₅	eg ₅	g ₆	eg ₆	g ₇	eg ₇
1	1	e	g ₁	eg ₁	g ₂	eg ₂	g ₃	eg ₃	g ₄	eg ₄	g ₅	eg ₅	g ₆	eg ₆	g ₇	eg ₇
e	e	1	eg ₁	g ₁	eg ₂	g ₂	eg ₃	g ₃	eg ₄	g ₄	eg ₅	g ₅	eg ₆	g ₆	eg ₇	g ₇
g ₁	g ₁	eg ₁	e	1	g ₃	eg ₃	eg ₂	g ₂	g ₅	eg ₅	eg ₄	g ₄	eg ₇	g ₇	g ₆	eg ₆
eg ₁	eg ₁	g ₁	1	e	eg ₃	g ₃	g ₂	eg ₂	eg ₅	g ₅	g ₄	eg ₄	g ₇	eg ₇	eg ₆	g ₆
g ₂	g ₂	eg ₂	eg ₃	g ₃	e	1	g ₁	eg ₁	g ₆	eg ₆	g ₇	eg ₇	eg ₄	g ₄	eg ₅	g ₅
eg ₂	eg ₂	g ₂	g ₃	eg ₃	1	e	eg ₁	g ₁	eg ₆	g ₆	eg ₇	g ₇	g ₄	eg ₄	g ₅	eg ₅
g ₃	g ₃	eg ₃	g ₂	eg ₂	eg ₁	g ₁	e	1	g ₇	eg ₇	eg ₆	g ₆	g ₅	eg ₅	eg ₄	g ₄
eg ₃	eg ₃	g ₃	eg ₂	g ₂	g ₁	eg ₁	1	e	eg ₇	g ₇	g ₆	eg ₆	eg ₅	g ₅	g ₄	eg ₄
g ₄	g ₄	eg ₄	eg ₅	g ₅	eg ₆	g ₆	eg ₇	g ₇	1	e	eg ₁	g ₁	eg ₂	g ₂	eg ₃	g ₃
eg ₄	eg ₄	g ₄	g ₅	eg ₅	g ₆	eg ₆	g ₇	eg ₇	e	1	g ₁	eg ₁	g ₂	eg ₂	g ₃	eg ₃
g ₅	g ₅	eg ₅	g ₄	eg ₄	eg ₇	g ₇	g ₆	eg ₆	g ₁	eg ₁	1	e	g ₃	eg ₃	eg ₂	g ₂
eg ₅	eg ₅	g ₅	eg ₄	g ₄	g ₇	eg ₇	eg ₆	g ₆	eg ₁	g ₁	e	1	g ₃	eg ₃	eg ₂	g ₂
g ₆	g ₆	eg ₆	g ₇	eg ₇	g ₄	eg ₄	eg ₅	g ₅	g ₂	eg ₂	eg ₃	g ₃	1	e	g ₁	eg ₁
eg ₆	eg ₆	g ₆	eg ₇	g ₇	eg ₄	g ₄	g ₅	eg ₅	eg ₂	g ₂	g ₃	eg ₃	e	1	eg ₁	g ₁
g ₇	g ₇	eg ₇	eg ₆	g ₆	g ₅	eg ₅	g ₄	eg ₄	g ₃	eg ₃	g ₂	eg ₂	eg ₁	g ₁	1	e
eg ₇	eg ₇	g ₇	g ₆	eg ₆	eg ₅	g ₅	eg ₄	g ₄	eg ₃	g ₃	eg ₂	g ₂	g ₁	eg ₁	e	1

Tabela 2.2.2

Consideremos os elementos $f_o = \frac{1-e}{2} = 1 - \hat{L}'$, $f_1 = f_o \cdot g_1, \dots, f_7 = f_o \cdot g_7$. É fácil ver que o conjunto $\{f_o, f_1, \dots, f_7\}$ é linearmente independente sobre $\mathbf{Q}$ e como $\dim \left(\mathbf{QI}_1 \cdot \left(\frac{1-e}{2} \right) \right) = 8$, temos que esse conjunto é uma base de $\mathbf{QI}_1 \cdot \left(\frac{1-e}{2} \right) \cong \Delta(\mathbf{I}_1 : \mathbf{I}_1')$ sobre $\mathbf{Q}$. A tábua de multiplicação dessa base é dada pela Tabela 2.2.3.

	f_o	f_1	f_2	f_3	f_4	f_5	f_6	f_7
f_o	f_o	f_1	f_2	f_3	f_4	f_5	f_6	f_7
f_1	f_1	$-f_o$	f_3	$-f_2$	f_5	$-f_4$	$-f_7$	f_6
f_2	f_2	$-f_3$	$-f_o$	f_1	f_6	f_7	$-f_4$	$-f_5$
f_3	f_3	f_2	$-f_1$	$-f_o$	f_7	$-f_6$	f_5	$-f_4$
f_4	f_4	$-f_5$	$-f_6$	$-f_7$	f_o	$-f_1$	$-f_2$	$-f_3$
f_5	f_5	f_4	$-f_7$	f_6	f_1	f_o	f_3	$-f_2$
f_6	f_6	f_7	f_4	$-f_5$	f_2	$-f_3$	f_o	f_1
f_7	f_7	$-f_6$	f_5	f_4	f_3	f_2	$-f_1$	f_o

Tabela 2.2.3

Comparando com a Tabela 1.2.3, vemos que essa base é multiplicativamente isomorfa à base canônica de $\mathcal{C}(\mathbb{Q}, -1, -1, 1)$, e segue o resultado.

Passemos agora ao próximo R.A. loop indecomponível.

Tomando $\mathbf{D}_2 = Q$ na Tabela 1.1.2, obtemos o outro R.A. loop indecomponível de ordem 16, cujo centro é isomorfo a C_2 , que é $\mathbf{I}_2 = L(Q, *, e)$. Na notação de [3], trata-se do loop $M_{16}(Q)$, o chamado loop de Cayley.

O R.A. loop $\mathbf{I}_2 = M_{16}(Q) = Q \cup Qu = L(Q, *, e)$ tem a sua tábua dada pela Tabela 2.2.4. Observemos que o bloco 8×8 superior à esquerda é a tábua do grupo Q dos quatérnios na notação de [24].

$$I_2 = M_{16}(Q) = L(Q, *, e)$$

	1	2	3	4	5	6	7	8	u	$2.u$	$3.u$	$4.u$	$5.u$	$6.u$	$7.u$	$8.u$
1	1	2	3	4	5	6	7	8	u	$2.u$	$3.u$	$4.u$	$5.u$	$6.u$	$7.u$	$8.u$
2	2	3	4	1	6	7	8	5	$2.u$	$3.u$	$4.u$	u	$8.u$	$5.u$	$6.u$	$7.u$
3	3	4	1	2	7	8	5	6	$3.u$	$4.u$	u	$2.u$	$7.u$	$8.u$	$5.u$	$6.u$
4	4	1	2	3	8	5	6	7	$4.u$	u	$2.u$	$3.u$	$6.u$	$7.u$	$8.u$	$5.u$
5	5	8	7	6	3	2	1	4	$5.u$	$6.u$	$7.u$	$8.u$	$3.u$	$4.u$	u	$2.u$
6	6	5	8	7	4	3	2	1	$6.u$	$7.u$	$8.u$	$5.u$	$2.u$	$3.u$	$4.u$	u
7	7	6	5	8	1	4	3	2	$7.u$	$8.u$	$5.u$	$6.u$	u	$2.u$	$3.u$	$4.u$
8	8	7	6	5	2	1	4	3	$8.u$	$5.u$	$6.u$	$7.u$	$4.u$	u	$2.u$	$3.u$
u	u	$4.u$	$3.u$	$2.u$	$7.u$	$8.u$	$5.u$	$6.u$	3	2	1	4	5	6	7	8
$2.u$	$2.u$	u	$4.u$	$3.u$	$8.u$	$5.u$	$6.u$	$7.u$	4	3	2	1	8	5	6	7
$3.u$	$3.u$	$2.u$	u	$4.u$	$5.u$	$6.u$	$7.u$	$8.u$	1	4	3	2	7	8	5	6
$4.u$	$4.u$	$3.u$	$2.u$	u	$6.u$	$7.u$	$8.u$	$5.u$	2	1	4	3	6	7	8	5
$5.u$	$5.u$	$6.u$	$7.u$	$8.u$	u	$4.u$	$3.u$	$2.u$	7	6	5	8	3	4	1	2
$6.u$	$6.u$	$7.u$	$8.u$	$5.u$	$2.u$	u	$4.u$	$3.u$	8	7	6	5	2	3	4	1
$7.u$	$7.u$	$8.u$	u	$6.u$	$3.u$	$2.u$	u	$4.u$	5	8	7	6	1	2	3	4
$8.u$	$8.u$	$5.u$	$6.u$	$7.u$	$4.u$	$3.u$	$2.u$	u	6	5	8	7	4	1	2	3

Tabela 2.2.4

Sabemos que

$$\mathbf{QI}_2 \cong \mathbf{Q} \left[\frac{\mathbf{I}_2}{\mathbf{I}_2'} \right] \oplus \Delta(\mathbf{I}_2 : \mathbf{I}_2').$$

Como $Z(\mathbf{I}_2) = Z(Q) \cong C_2$, pelo corolário 2.1.4, temos que $\frac{\mathbf{I}_2}{\mathbf{I}_2'} \cong C_2 \times C_2 \times C_2$, e pelo teorema 1.3.3, podemos escrever

$$\mathbf{Q} \left[\frac{\mathbf{I}_2}{\mathbf{I}_2'} \right] \cong \mathbf{Q}[C_2 \times C_2 \times C_2] \cong \underbrace{\mathbf{Q} \oplus \cdots \oplus \mathbf{Q}}_{8 \text{ vezes}}.$$

Como $Z(\Delta(\mathbf{I}_2 : \mathbf{I}_2')) \cong \mathbf{Q}[Z(\mathbf{I}_2)] \cdot \left(\frac{1-e}{2}\right) \cong \mathbf{Q}C_2 \cdot \left(\frac{1-e}{2}\right) \cong \mathbf{Q}$, pelo teorema 1.3.9, temos que $\Delta(\mathbf{I}_2 : \mathbf{I}_2') \cong \mathcal{A}(\mathbf{Q})$, uma álgebra de Cayley-Dickson sobre $\mathbf{Q}$. Vamos descrevê-la.

Na Tabela 2.2.4, chamando $g_1 = 2, g_2 = 5, g_3 = 6, g_4 = u, g_5 = 2.u, g_6 = 5.u$ e $g_7 = 6.u$ e lembrando que $L' = \{1, 3\} = \{1, e\}$, podemos escrever os elementos de $\mathbf{I}_2$ na forma

$$\mathbf{I}_2 = M_{16}(Q) = \{1, e, g_1, eg_1, \dots, g_7, eg_7\} \quad ,$$

e sua tabela pode ser reescrita na forma da Tabela 2.2.5.

$$\mathbf{I}_2 = M_{16}(Q)$$

	1	e	g_1	eg_1	g_2	eg_2	g_3	eg_3	g_4	eg_4	g_5	eg_5	g_6	eg_6	g_7	eg_7
1	1	e	g_1	eg_1	g_2	eg_2	g_3	eg_3	g_4	eg_4	g_5	eg_5	g_6	eg_6	g_7	eg_7
e	e	1	eg_1	g_1	eg_2	g_2	eg_3	g_3	eg_4	g_4	eg_5	g_5	eg_6	g_6	eg_7	g_7
g_1	g_1	eg_1	e	1	g_3	eg_3	eg_2	g_2	g_5	eg_5	eg_4	g_4	eg_7	g_7	g_6	eg_6
eg_1	eg_1	g_1	1	e	eg_3	g_3	g_2	eg_2	eg_5	g_5	g_4	eg_4	g_7	eg_7	eg_6	g_6
g_2	g_2	eg_2	eg_3	g_3	e	1	g_1	eg_1	g_6	eg_6	g_7	eg_7	eg_4	g_4	eg_5	g_5
eg_2	eg_2	g_2	g_3	eg_3	1	e	eg_1	g_1	eg_6	g_6	eg_7	g_7	g_4	eg_4	g_5	eg_5
g_3	g_3	eg_3	g_2	eg_2	eg_1	g_1	e	1	g_7	eg_7	eg_6	g_6	g_5	eg_5	eg_4	g_4
eg_3	eg_3	g_3	eg_2	g_2	g_1	eg_1	1	e	eg_7	g_7	g_6	eg_6	eg_5	g_5	g_4	eg_4
g_4	g_4	eg_4	eg_5	g_5	eg_6	g_6	eg_7	g_7	e	1	g_1	eg_1	g_2	eg_2	g_3	eg_3
eg_4	eg_4	g_4	g_5	eg_5	g_6	eg_6	g_7	eg_7	1	e	eg_1	g_1	eg_2	g_2	eg_3	g_3
g_5	g_5	eg_5	g_4	eg_4	eg_7	g_7	g_6	eg_6	eg_1	g_1	e	1	eg_3	g_3	g_2	eg_2
eg_5	eg_5	g_5	eg_4	g_4	g_7	eg_7	eg_6	g_6	g_1	eg_1	1	e	g_3	eg_3	eg_2	g_2
g_6	g_6	eg_6	g_7	eg_7	g_4	eg_4	eg_5	g_5	eg_2	g_2	g_3	eg_3	e	1	eg_1	g_1
eg_6	eg_6	g_6	eg_7	g_7	eg_4	g_4	g_5	eg_5	g_2	eg_2	eg_3	g_3	1	e	g_1	eg_1
g_7	g_7	eg_7	eg_6	g_6	g_5	eg_5	g_4	eg_4	eg_3	g_3	eg_2	g_2	g_1	eg_1	e	1
eg_7	eg_7	g_7	g_6	eg_6	eg_5	g_5	eg_4	g_4	g_3	eg_3	g_2	eg_2	eg_1	g_1	1	e

Tabela 2.2.5

Consideremos os elementos $f_o = \frac{1-e}{2} = 1 - \hat{L}'$, $f_1 = f_o \cdot g_1, \dots, f_7 = f_o \cdot g_7$. Então o conjunto $\{f_o, f_1, \dots, f_7\}$ é uma base de $\mathbf{QI}_2 \cdot \left(\frac{1-e}{2}\right) \cong \Delta(\mathbf{I}_2 : \mathbf{I}_2')$ sobre $\mathbf{Q}$, cuja tábua de multiplicação é dada pela Tabela 2.2.6.

	f_o	f_1	f_2	f_3	f_4	f_5	f_6	f_7
f_o	f_o	f_1	f_2	f_3	f_4	f_5	f_6	f_7
f_1	f_1	$-f_o$	f_3	$-f_2$	f_5	$-f_4$	$-f_7$	f_6
f_2	f_2	$-f_3$	$-f_o$	f_1	f_6	f_7	$-f_4$	$-f_5$
f_3	f_3	f_2	$-f_1$	$-f_o$	f_7	$-f_6$	f_5	$-f_4$
f_4	f_4	$-f_5$	$-f_6$	$-f_7$	$-f_o$	f_1	f_2	f_3
f_5	f_5	f_4	$-f_7$	f_6	$-f_1$	$-f_o$	$-f_3$	f_2
f_6	f_6	f_7	f_4	$-f_5$	$-f_2$	f_3	$-f_o$	$-f_1$
f_7	f_7	$-f_6$	f_5	f_4	$-f_3$	$-f_2$	f_1	$-f_o$

Tabela 2.2.6

Comparando a Tabela 2.2.6 com a Tabela 1.2.1, vemos que essa base é multiplicativamente isomorfa à base canônica de $\mathcal{C}(\mathbf{Q}, -1, -1, -1) = \mathcal{C}(\mathbf{Q})$, que, como sabemos, é uma álgebra de Cayley-Dickson com divisão sobre $\mathbf{Q}$.

Concluimos então que a álgebra $\mathcal{A}(\mathbf{Q})$ é isomorfa a $\mathcal{C}(\mathbf{Q})$ e assim para $\mathbf{I}_2$ obtemos

$$\mathbf{QI}_2 \cong \underbrace{\mathbf{Q} \oplus \dots \oplus \mathbf{Q}}_{8 \text{ vezes}} \oplus \mathcal{C}(\mathbf{Q})$$

Existem dois grupos indecomponíveis G de ordem 16 tais que $\frac{G}{Z(G)} \cong C_2 \times C_2$ e $Z(G) \cong C_2 \times C_2$. Na notação de [24], esses grupos são $S = 16\Gamma_2 C_1 = 16/9$ e $T = 16\Gamma_2 C_2 = 16/10$. Ainda na notação de [24], temos

que

$$S' = \langle 7 \rangle \cong C_2, Z(S) = \langle 7 \rangle \times \langle 3 \rangle = \{1, 3, 5, 7\},$$

$$T' = \langle 3 \rangle = \langle e \rangle \cong C_2 e Z(T) = \langle 3 \rangle \times \langle 9 \rangle = \{1, 3, 9, 11\}.$$

Tomando $\mathbf{D}_3 = S$ na Tabela 1.1.2, obtemos o R.A. loop indecomponível $\mathbf{I}_3 = L(S, *, 1)$ de ordem 32, cujo centro é isomorfo a $C_2 \times C_2$. Esse loop na notação de [3] é o loop $\mathbf{M}_{32}(16\Gamma_2 C_2, 16\Gamma_2 C_2, 16\Gamma_2 C_1, 16\Gamma_2 C_1)$ e ele pode ainda ser obtido pelas construções $L(S, *, 7)$, $L(S, *, 3)$, $L(S, *, 5)$ e $L(T, *, 1)$. Nossos cálculos foram feitos baseados nesta última construção.

De novo, temos

$$\mathbf{QI}_3 \cong \mathbf{Q} \left[\frac{\mathbf{I}_3}{\mathbf{I}_3'} \right] \oplus \Delta(\mathbf{I}_3 : \mathbf{I}_3').$$

Como $Z(\mathbf{I}_3) = Z(T) = \langle 3 \rangle \times \langle 9 \rangle \cong C_2 \times C_2$ temos que $\frac{\mathbf{I}_3}{\mathbf{I}_3'} \cong C_2 \times C_2 \times C_4$ pelo corolário 2.1.4. Aplicando o teorema 1.3.3, obtemos

$$\mathbf{Q} \left[\frac{\mathbf{I}_3}{\mathbf{I}_3'} \right] \cong \mathbf{Q}[C_2 \times C_2 \times C_4] \cong \underbrace{\mathbf{Q} \oplus \cdots \oplus \mathbf{Q}}_{8 \text{ vezes}} \oplus \underbrace{\mathbf{Q}(i) \oplus \cdots \oplus \mathbf{Q}(i)}_{4 \text{ vezes}}.$$

Como

$$Z(\Delta(\mathbf{I}_3 : \mathbf{I}_3')) \cong \mathbf{Q}[Z(\mathbf{I}_3)]. \left(\frac{1-e}{2} \right) \cong \left[\mathbf{Q}C_2. \left(\frac{1-e}{2} \right) \right] C_2 \cong \mathbf{Q}C_2 \cong \mathbf{Q} \oplus \mathbf{Q},$$

pelo teorema 1.3.9, concluímos que $\Delta(\mathbf{I}_3 : \mathbf{I}_3') \cong \mathcal{A}(\mathbf{Q}) \oplus \mathcal{B}(\mathbf{Q})$, onde $\mathcal{A}(\mathbf{Q})$ e $\mathcal{B}(\mathbf{Q})$ são álgebras de Cayley-Dickson sobre $\mathbf{Q}$.

Se considerarmos os subgrupos normais $H_1 = \langle 9 \rangle$ e $H_2 = \langle e.9 \rangle$ de $\mathbf{I}_3$, obtemos $\frac{\mathbf{I}_3}{H_1} \cong \frac{\mathbf{I}_3}{H_2} \cong M_{16}(\mathbf{Q}, 2)$. Escrevendo $\mathbf{QI}_3 \cong \mathbf{Q} \left[\frac{\mathbf{I}_3}{H_i} \right] \oplus \Delta(\mathbf{I}_3 : H_i)$, $i = 1, 2$, concluímos que $\Delta(\mathbf{I}_3 : H_1) \cong \Delta(\mathbf{I}_3 : H_2) \cong \mathcal{C}_S(\mathbf{Q})$.

Como $\widehat{H}_1 \neq \widehat{H}_2$, temos $\mathcal{A}(\mathbf{Q}) \cong \mathcal{C}_S(\mathbf{Q})$ e $\mathcal{B}(\mathbf{Q}) \cong \mathcal{C}_S(\mathbf{Q})$.

Assim finalmente para $\mathbf{I}_3$ obtemos

$$\mathbf{QI}_3 \cong \underbrace{\mathbf{Q} \oplus \cdots \oplus \mathbf{Q}}_{8 \text{ vezes}} \oplus \underbrace{\mathbf{Q}(i) \oplus \cdots \oplus \mathbf{Q}(i)}_{4 \text{ vezes}} \oplus \mathcal{C}_S(\mathbf{Q}) \oplus \mathcal{C}_S(\mathbf{Q})$$

Se tomamos $\mathbf{D}_4 = T$ na Tabela 1.1.2, obtemos o outro R.A. loop indecomponível de ordem 32, cujo centro é isomorfo a $C_2 \times C_2$, que é $\mathbf{I}_4 = L(T, *, e)$. Na notação de [3], esse é o loop $\mathbf{M}_{32}(16\Gamma_2 C_2, 16\Gamma_2 C_2, 16\Gamma_2 C_2^\#, 16\Gamma_2 C_2)$, e ele ainda pode ser obtido pelas construções $L(T, *, 9)$ e $L(T, *, 11)$. Nos nossos cálculos trabalhamos com a construção $L(T, *, e)$.

Como sempre, temos

$$\mathbf{QI}_4 \cong \mathbf{Q} \left[\frac{\mathbf{I}_4}{\mathbf{I}_4'} \right] \oplus \Delta(\mathbf{I}_4 : \mathbf{I}_4').$$

Como $Z(\mathbf{I}_4) = Z(T) = \langle 3 \rangle \times \langle 9 \rangle \cong C_2 \times C_2$, temos que $\frac{\mathbf{I}_4}{\mathbf{I}_4'} \cong C_2 \times C_2 \times C_4$ pelo corolário 2.1.4. Aplicando o teorema 1.3.3, obtemos

$$\mathbf{Q} \left[\frac{\mathbf{I}_4}{\mathbf{I}_4'} \right] \cong \mathbf{Q}[C_2 \times C_2 \times C_4] \cong \underbrace{\mathbf{Q} \oplus \cdots \oplus \mathbf{Q}}_{8 \text{ vezes}} \oplus \underbrace{\mathbf{Q}(i) \oplus \cdots \oplus \mathbf{Q}(i)}_{4 \text{ vezes}}.$$

Como

$$Z(\Delta(\mathbf{I}_4 : \mathbf{I}_4')) \cong \mathbf{Q}[Z(\mathbf{I}_4)]. \left(\frac{1-e}{2} \right) \cong \left[\mathbf{Q}C_2. \left(\frac{1-e}{2} \right) \right] C_2 \cong \mathbf{Q}C_2 \cong \mathbf{Q} \oplus \mathbf{Q} ,$$

pelo teorema 1.3.9, concluímos que $\Delta(\mathbf{I}_4 : \mathbf{I}_4') \cong \mathcal{A}(\mathbf{Q}) \oplus \mathcal{B}(\mathbf{Q})$, onde $\mathcal{A}(\mathbf{Q})$ e $\mathcal{B}(\mathbf{Q})$ são álgebras de Cayley-Dickson sobre $\mathbf{Q}$.

Se considerarmos os subgrupos normais $K_1 = \langle 9 \rangle$ e $K_2 = \langle e.9 \rangle$ de I_4 , obtemos $\frac{I_4}{K_1} \cong M_{16}(Q, 2)$ e $\frac{I_4}{K_2} \cong M_{16}(Q)$. De forma análoga à anterior, concluímos que $\mathcal{A}(Q) \cong \mathcal{C}_S(Q)$ e $\mathcal{B}(Q) \cong \mathcal{C}(Q)$.

Para I_4 então obtemos

$$QI_4 \cong \underbrace{Q \oplus \cdots \oplus Q}_{8 \text{ vezes}} \oplus \underbrace{Q(i) \oplus \cdots \oplus Q(i)}_{4 \text{ vezes}} \oplus \mathcal{C}_S(Q) \oplus \mathcal{C}(Q)$$

Existe apenas um grupo indecomponível G tal que $\frac{G}{Z(G)} \cong C_2 \times C_2$ e $Z(G) \cong C_2 \times C_2 \times C_2$. Na notação de [24] é o grupo $R = \Gamma_2 h = 32/18$.

Ainda na notação de [24], temos $R' = \langle 2 \rangle = \langle e \rangle \cong C_2$ e

$$Z(R) = \langle 2 \rangle \times \langle 6 \rangle \times \langle 22 \rangle = \{1, 2, 5, 6, 17, 18, 21, 22\}.$$

Se tomarmos $D_5 = R$ na Tabela 1.1.2, obtemos o R.A. loop indecomponível $I_5 = L(R, *, 1)$ de ordem 64, cujo centro é isomorfo a $C_2 \times C_2 \times C_2$. Este loop também pode ser obtido através das construções $L(R, *, 6)$, $L(R, *, 18)$ e $L(R, *, 21)$. Nos nossos cálculos trabalhamos com a construção $L(R, *, 1)$.

Como sempre, temos

$$QI_5 \cong Q \left[\frac{I_5}{I_5'} \right] \oplus \Delta(I_5 : I_5').$$

Como $Z(I_5) = Z(R) = \langle 2 \rangle \times \langle 6 \rangle \times \langle 22 \rangle \cong C_2 \times C_2 \times C_2$, temos que $\frac{I_5}{I_5'} \cong C_2 \times C_4 \times C_4$ pelo corolário 2.1.4. Aplicando o teorema 1.3.3, obtemos

$$Q \left[\frac{I_5}{I_5'} \right] \cong Q[C_2 \times C_4 \times C_4] \cong \underbrace{Q \oplus \cdots \oplus Q}_{8 \text{ vezes}} \oplus \underbrace{Q(i) \oplus \cdots \oplus Q(i)}_{12 \text{ vezes}}.$$

$$\text{Como } Z(\Delta(I_5 : I_5')) \cong Q[Z(I_5)] \cdot \left(\frac{1-e}{2} \right) \cong [QC_2 \cdot \frac{1-e}{2}][C_2 \times C_2] \cong$$

$\mathbb{Q}[C_2 \times C_2] \cong \underbrace{\mathbb{Q} \oplus \cdots \oplus \mathbb{Q}}_{4 \text{ vezes}}$, pelo teorema 1.3.9, concluímos que $\Delta(\mathbf{I}_5 : \mathbf{I}_5') \cong \bigoplus_{i=1}^4 \mathcal{A}_i(\mathbb{Q})$, onde cada $\mathcal{A}_i(\mathbb{Q})$ é uma álgebra de Cayley-Dickson sobre $\mathbb{Q}$.

Se considerarmos os subgrupos normais $H_1 = \langle 6 \rangle \times \langle 22 \rangle$, $H_2 = \langle e.6 \rangle \times \langle 22 \rangle$, $H_3 = \langle e.6 \rangle \times \langle e.22 \rangle$ e $H_4 = \langle 6 \rangle \times \langle e.22 \rangle$ de $\mathbf{I}_5$, obtemos $\frac{\mathbf{I}_5}{H_i} \cong M_{16}(\mathbb{Q}, 2)$ para $i = 1, 2, 3, 4$. De forma análoga à anterior, concluímos que $\mathcal{A}_i(\mathbb{Q}) \cong \mathcal{C}_S(\mathbb{Q})$ para $i = 1, 2, 3, 4$.

Para $\mathbf{I}_5$ então obtemos

$$\mathbf{QI}_5 \cong \underbrace{\mathbb{Q} \oplus \cdots \oplus \mathbb{Q}}_{8 \text{ vezes}} \oplus \underbrace{\mathbb{Q}(i) \oplus \cdots \oplus \mathbb{Q}(i)}_{12 \text{ vezes}} \oplus \underbrace{\mathcal{C}_S(\mathbb{Q}) \oplus \cdots \oplus \mathcal{C}_S(\mathbb{Q})}_{4 \text{ vezes}}.$$

O outro R.A. loop indecomponível de ordem 64, cujo centro é isomorfo a $C_2 \times C_2 \times C_2$, é obtido por $\mathbf{I}_6 = L(R, *, e)$. Esse loop também pode ser obtido através das construções $L(R, *, 5)$, $L(R, *, 17)$ e $L(R, *, 22)$. Nos nossos cálculos trabalhamos com a construção $L(R, *, e)$.

Como nas outras vezes, temos

$$\mathbf{QI}_6 \cong \mathbf{Q} \left[\frac{\mathbf{I}_6}{\mathbf{I}_6'} \right] \oplus \Delta(\mathbf{I}_6 : \mathbf{I}_6').$$

Como $Z(\mathbf{I}_6) = Z(R)$ temos, como antes, que $\frac{\mathbf{I}_6}{\mathbf{I}_6'} \cong C_2 \times C_4 \times C_4$ pelo corolário 2.1.4. Aplicando de novo o teorema 1.3.3, obtemos

$$\mathbf{Q} \left[\frac{\mathbf{I}_6}{\mathbf{I}_6'} \right] \cong \mathbf{Q}[C_2 \times C_4 \times C_4] \cong \underbrace{\mathbb{Q} \oplus \cdots \oplus \mathbb{Q}}_{8 \text{ vezes}} \oplus \underbrace{\mathbb{Q}(i) \oplus \cdots \oplus \mathbb{Q}(i)}_{12 \text{ vezes}}.$$

$$\text{Como } Z(\Delta(\mathbf{I}_6 : \mathbf{I}_6')) \cong \mathbf{Q}[Z(\mathbf{I}_6)]. \left(\frac{1-e}{2} \right) \cong \left[\mathbf{Q}C_2. \left(\frac{1-e}{2} \right) \right] [C_2 \times C_2] \cong$$

$\mathbb{Q}[C_2 \times C_2] \cong \underbrace{\mathbb{Q} \oplus \cdots \oplus \mathbb{Q}}_{4 \text{ vezes}}$, pelo teorema 1.3.9, concluímos que $\Delta(\mathbf{I}_6 : \mathbf{I}_6') \cong \bigoplus_{i=1}^4 \mathcal{A}_i(\mathbb{Q})$, onde cada $\mathcal{A}_i(\mathbb{Q})$ é uma álgebra de Cayley-Dickson sobre $\mathbb{Q}$.

Se considerarmos os subgrupos normais $K_1 = \langle 6 \rangle \times \langle 22 \rangle$, $K_2 = \langle e.6 \rangle \times \langle 22 \rangle$, $K_3 = \langle e.6 \rangle \times \langle e.22 \rangle$ e $K_4 = \langle 6 \rangle \times \langle e.22 \rangle$ de $\mathbf{I}_6$, obtemos $\frac{\mathbf{I}_6}{K_i} \cong M_{16}(Q, 2)$ para $i = 1, 2, 3$ e $\frac{\mathbf{I}_6}{K_4} \cong M_{16}(Q)$. De forma análoga às anteriores, concluímos que $\mathcal{A}_i(\mathbb{Q}) \cong \mathcal{C}_S(\mathbb{Q})$ para $i = 1, 2, 3$ e $\mathcal{A}_4 \cong \mathcal{C}(\mathbb{Q})$.

Para $\mathbf{I}_6$ finalmente obtemos

$$\mathbb{Q}\mathbf{I}_6 \cong \underbrace{\mathbb{Q} \oplus \cdots \oplus \mathbb{Q}}_{8 \text{ vezes}} \oplus \underbrace{\mathbb{Q}(i) \oplus \cdots \oplus \mathbb{Q}(i)}_{12 \text{ vezes}} \oplus \mathcal{C}_S(\mathbb{Q}) \oplus \mathcal{C}_S(\mathbb{Q}) \oplus \mathcal{C}_S(\mathbb{Q}) \oplus \mathcal{C}(\mathbb{Q}).$$

O único R.A. loop indecomponível de ordem 128, cujo centro é isomorfo a $C_2 \times C_2 \times C_2 \times C_2$ é obtido, trabalhando-se com o grupo $V = R \times C_2$. Usando-se uma notação análoga à de [24], escrevamos $V' = \langle 2 \rangle = \langle e \rangle$ e

$$Z(V) =$$

$\langle 2 \rangle \times \langle 6 \rangle \times \langle 22 \rangle \times \langle 33 \rangle$. Então o R.A. loop em questão é $\mathbf{I}_7 = L(V, *, 33)$

Como nas outras vezes, temos

$$\mathbb{Q}\mathbf{I}_7 \cong \mathbb{Q} \left[\frac{\mathbf{I}_7}{\mathbf{I}_7'} \right] \oplus \Delta(\mathbf{I}_7 : \mathbf{I}_7').$$

Como $Z(\mathbf{I}_7) = Z(V)$ pelo corolário 2.1.4 temos que $\frac{\mathbf{I}_7}{\mathbf{I}_7'} \cong C_4 \times C_4 \times C_4$ e pelo teorema 1.3.3 segue que

$$\mathbf{QI}_7 \cong \underbrace{\mathbf{Q} \oplus \cdots \oplus \mathbf{Q}}_{8 \text{ vezes}} \oplus \underbrace{\mathbf{Q}(i) \oplus \cdots \oplus \mathbf{Q}(i)}_{28 \text{ vezes}}.$$

Como $Z(\Delta(\mathbf{I}_7 : \mathbf{I}_7')) \cong \mathbf{Q}[Z(\mathbf{I}_7)] \cdot \left(\frac{1-e}{2}\right) \cong \left[\mathbf{Q}C_2 \cdot \left(\frac{1-e}{2}\right)\right] [C_2 \times C_2 \times C_2] \cong \mathbf{Q}[C_2 \times C_2 \times C_2] \cong \underbrace{\mathbf{Q} \oplus \cdots \oplus \mathbf{Q}}_{8 \text{ vezes}}$, pelo teorema 1.3.9, concluimos que $\Delta(\mathbf{I}_7 : \mathbf{I}_7') \cong \bigoplus_{i=1}^8 \mathcal{A}_i(\mathbf{Q})$, onde cada $\mathcal{A}_i(\mathbf{Q})$ é uma álgebra de Cayley-Dickson sobre $\mathbf{Q}$.

Consideremos os seguintes subloops normais de $\mathbf{I}_7$:

$$\begin{aligned} H_1 &= \langle 6 \rangle \times \langle 22 \rangle \times \langle 33 \rangle, \quad H_2 = \langle e.6 \rangle \times \langle 22 \rangle \times \langle 33 \rangle, \\ H_3 &= \langle 6 \rangle \times \langle 22 \rangle \times \langle e.33 \rangle, \quad H_4 = \langle e.6 \rangle \times \langle 22 \rangle \times \langle e.33 \rangle, \\ H_5 &= \langle e.6 \rangle \times \langle e.22 \rangle \times \langle 33 \rangle, \quad H_6 = \langle e.6 \rangle \times \langle e.22 \rangle \times \langle e.33 \rangle, \\ H_7 &= \langle 6 \rangle \times \langle e.22 \rangle \times \langle 33 \rangle \quad \text{e} \quad H_8 = \langle 6 \rangle \times \langle e.22 \rangle \times \langle e.33 \rangle. \end{aligned}$$

Temos que $\frac{\mathbf{I}_7}{H_i} \cong M_{16}(Q, 2)$ para $i = 1, 2, \dots, 7$ e $\frac{\mathbf{I}_7}{H_8} \cong M_{16}(Q)$. De forma análoga às anteriores, concluimos que $\mathcal{A}_i(\mathbf{Q}) \cong \mathcal{C}_S(\mathbf{Q})$ para $i = 1, 2, \dots, 7$ e $\mathcal{A}_8 \cong \mathcal{C}(\mathbf{Q})$.

Para $\mathbf{I}_7$ finalmente obtemos

$$\mathbf{QI}_7 \cong \underbrace{\mathbf{Q} \oplus \cdots \oplus \mathbf{Q}}_{8 \text{ vezes}} \oplus \underbrace{\mathbf{Q}(i) \oplus \cdots \oplus \mathbf{Q}(i)}_{28 \text{ vezes}} \oplus \underbrace{\mathcal{C}_S(\mathbf{Q}) \oplus \cdots \oplus \mathcal{C}_S(\mathbf{Q})}_{7 \text{ vezes}} \oplus \mathcal{C}(\mathbf{Q}).$$

2.3 O Problema do Isomorfismo para os R.A. loops do tipo II

A nossa grande arma nesta seção será o teorema 2.1.1. Como vimos, o problema do isomorfismo para os R.A. loops do tipo I está resolvido no teorema 2.1.2.

Os resultados da seção 2.2 nos indicam que para os R.A. loops do tipo II a condição dada pelo teorema 2.1.2 não é suficiente. Por exemplo, $Z(\Delta(I_1 : I_1')) \cong Z(\Delta(I_2 : I_2')) \cong Q$, e, no entanto, $\Delta(I_1 : I_1') \not\cong \Delta(I_2 : I_2')$.

Sejam L e M dois R.A. loops indecomponíveis e escrevamos

$$Z(L) = C_{2^a} \times C_{2^b} \times C_{2^c} \times C_{2^d e}$$

$$Z(M) = C_{2^{a'}} \times C_{2^{b'}} \times C_{2^{c'}} \times C_{2^{d'}},$$

com $a, a' \geq 1, b \geq c \geq d \geq 0$ e $b' \geq c' \geq d' \geq 0$.

Notemos que essa escolha é sempre possível, se necessário, trocando os papéis dos geradores x, y e u do R.A. loop (veja Tabela 1.1.2).

Na Tabela 2.3.1 reunimos os resultados da proposição 2.1.3 com os cálculos de $Z(\Delta(L : L'))$, conforme a proposição 1.3.7, para os R.A. loops indecomponíveis do tipo I.

Na Tabela 2.3.2 fizemos o mesmo para os R.A. loops indecomponíveis do tipo II.

R.A. loops indecomponíveis do tipo I ($a > 1$)

L	$Z(L)$	$\frac{L}{L'}$	$Z(\Delta(L : L'))$
L_1	C_{2^a}	$C_{2^{a-1}} \times C_2 \times C_2 \times C_2$	$Q(\xi_{2^a})$
L_2	C_{2^a}	$C_{2^a} \times C_2 \times C_2$	$Q(\xi_{2^a})$
L_3	$C_{2^a} \times C_{2^b}$	$C_{2^{a-1}} \times C_{2^{b+1}} \times C_2 \times C_2$	$Q(\xi_{2^a})[C_{2^b}]$
L_4	$C_{2^a} \times C_{2^b}$	$C_{2^a} \times C_{2^{b+1}} \times C_2$	$Q(\xi_{2^a})[C_{2^b}]$
L_5	$C_{2^a} \times C_{2^b} \times C_{2^c}$	$C_{2^{a-1}} \times C_{2^{b+1}} \times C_{2^{c+1}} \times C_2$	$Q(\xi_{2^a})[C_{2^b} \times C_{2^c}]$
L_6	$C_{2^a} \times C_{2^b} \times C_{2^c}$	$C_{2^a} \times C_{2^{b+1}} \times C_{2^{c+1}}$	$Q(\xi_{2^a})[C_{2^b} \times C_{2^c}]$
L_7	$C_{2^a} \times C_{2^b} \times C_{2^c} \times C_{2^d}$	$C_{2^{a-1}} \times C_{2^{b+1}} \times C_{2^{c+1}} \times C_{2^{d+1}}$	$Q(\xi_{2^a})[C_{2^b} \times C_{2^c} \times C_{2^d}]$

Tabela 2.3.1

R.A. loops indecomponíveis do tipo II ($a = 1$)

L	$Z(L)$	$\frac{L}{L'}$	$Z(\Delta(L : L'))$
L_1	C_2	$C_2 \times C_2 \times C_2$	Q
L_2	C_2	$C_2 \times C_2 \times C_2$	Q
L_3	$C_2 \times C_{2^b}$	$C_{2^{b+1}} \times C_2 \times C_2$	$Q[C_{2^b}]$
L_4	$C_2 \times C_{2^b}$	$C_{2^{b+1}} \times C_2 \times C_2$	$Q[C_{2^b}]$
L_5	$C_2 \times C_{2^b} \times C_{2^c}$	$C_{2^{b+1}} \times C_{2^{c+1}} \times C_2$	$Q[C_{2^b} \times C_{2^c}]$
L_6	$C_2 \times C_{2^b} \times C_{2^c}$	$C_{2^{b+1}} \times C_{2^{c+1}} \times C_2$	$Q[C_{2^b} \times C_{2^c}]$
L_7	$C_2 \times C_{2^b} \times C_{2^c} \times C_{2^d}$	$C_{2^{b+1}} \times C_{2^{c+1}} \times C_{2^{d+1}}$	$Q[C_{2^b} \times C_{2^c} \times C_{2^d}]$

Tabela 2.3.2

De acordo com ([14], Teorema 6.4), se L é da família L_2, L_4, L_6 ou L_7 , então L contém um subloop normal K tal que $\frac{L}{K} \cong M_{16}(Q)$, enquanto que se L é

da família $\mathbf{L}_1, \mathbf{L}_3$ ou $\mathbf{L}_5$, L não contém subloop normal K com aquela propriedade. Isso significa que se $L \in \{\mathbf{L}_1, \mathbf{L}_3, \mathbf{L}_5\}$ e $M \in \{\mathbf{L}_2, \mathbf{L}_4, \mathbf{L}_6, \mathbf{L}_7\}$ então $\mathbf{Q}L \not\cong \mathbf{Q}M$, porque $\mathbf{Q}L$ admite $\mathcal{C}(\mathbf{Q})$ como somando direto e $\mathbf{Q}M$ não.

Se L e M são R.A. loops indecomponíveis do tipo I, vamos explorar os resultados do teorema 2.1.2 e da proposição 2.1.3.

Supondo $\mathbf{Q}L \cong \mathbf{Q}M$, temos que estudar o sistema

$$\begin{cases} \frac{L}{L'} \cong \frac{M}{M'} \\ Z(\Delta((L : L'))) \cong Z(\Delta(M : M')) \end{cases} .$$

isto é,

$$\begin{cases} C_{2^{a-1}} \times C_{2^{b+1}} \times C_{2^{c+1}} \times C_{2^{d+1}} \cong C_{2^{a'-1}} \times C_{2^{b'+1}} \times C_{2^{c'+1}} \times C_{2^{d'+1}} \\ \mathbf{Q}(\xi_{2^a})[C_{2^b} \times C_{2^c} \times C_{2^d}] \cong \mathbf{Q}(\xi_{2^{a'}})[C_{2^{b'}} \times C_{2^{c'}} \times C_{2^{d'}}] \end{cases}$$

ou

$$\begin{cases} C_{2^a} \times C_{2^{b+1}} \times C_{2^{c+1}} \times C_{2^d} \cong C_{2^{a'}} \times C_{2^{b'+1}} \times C_{2^{c'+1}} \times C_{2^{d'}} \\ \mathbf{Q}(\xi_{2^a})[C_{2^b} \times C_{2^c} \times C_{2^d}] \cong \mathbf{Q}(\xi_{2^{a'}})[C_{2^{b'}} \times C_{2^{c'}} \times C_{2^{d'}}] \end{cases}$$

dependendo se L e M são da forma $\mathbf{L}_i$, $i = 1, 3, 5$ ou da forma $\mathbf{L}_i$, $i = 2, 4, 6, 7$.

Nos dois sistemas a segunda equação implica que $a = a'$, e a primeira, como os inteiros b, c e d e b', c' e d' estão ordenados, que $b = b', c = c'$ e $d = d'$.

Portanto $L \cong M$, e, dessa forma, $\mathbf{Q}$ determina os R.A. loops indecomponíveis do tipo I.

No entanto, essa implicação não é verdadeira para R.A. loops do tipo I arbitrários.

Podemos ver isso facilmente através do seguinte exemplo: tomemos $L = \mathbf{L}_3$ com $Z(\mathbf{L}_3) \cong C_{2^2} \times C_2$ e $M = \mathbf{L}_2 \times C_2$ com $Z(\mathbf{L}_2) \cong C_{2^2}$, onde $\mathbf{L}_2$ e $\mathbf{L}_3$ são R.A.

loops indecomponíveis não isomorfos como na Tabela 2.2.1. Efetuando os cálculos, obtemos

$$\frac{L}{L'} \cong \frac{M}{M'} \cong C_2 \times C_2 \times C_2 \times C_4 \quad e$$

$$Z(\Delta(L : L')) \cong Z(\Delta(M : M')) \cong \mathbb{Q} \oplus \mathbb{Q} \oplus \mathbb{Q}(i) \quad .$$

Obviamente $L \not\cong M$, mas, pelo teorema 2.1.2, $\mathbb{Q}L \cong \mathbb{Q}M$.

Se L e M são R.A. loops indecomponíveis do tipo II, usamos os resultados do teorema 2.1.1 e do corolário 2.1.4.

Supondo $\mathbb{Q}L \cong \mathbb{Q}M$, então $\frac{L}{L'} \cong \frac{M}{M'}$ e $\Delta(L : L') \cong \Delta(M : M')$. Note que $\frac{L}{L'} \cong \frac{M}{M'}$ implica que $C_{2^{b+1}} \times C_{2^{c+1}} \times C_{2^{d+1}} \cong C_{2^{b'+1}} \times C_{2^{c'+1}} \times C_{2^{d'+1}}$, cuja única solução é $b = b'$, $c = c'$ e $d = d'$.

Logo $L \cong M$, e, portanto, $\mathbb{Q}$ determina os R.A. loops indecomponíveis do tipo II.

Resta esclarecer o que acontece com os R.A. loops do tipo II em geral. É isso que pretendemos estudar nesta seção.

Começemos com alguns fatos gerais.

Pelos resultados de ([14], Teorema 2.2), sabemos que todo R.A. loop L pode ser escrito na forma $L = L_1 \times E \times A$, onde L_1 é um R.A. loop indecomponível, o qual é um 2-loop, E é um 2-grupo abeliano e A é um grupo abeliano de ordem ímpar. Escrevendo $L_2 = L_1 \times E$, nós temos que $L = L_2 \times A$, onde L_2 é um R.A. 2-loop e A é um grupo abeliano de ordem ímpar.

O próximo resultado, que vale em geral, reduz o estudo do problema do isomorfismo aos R.A. 2-loops.

Proposição 2.3.1 *Sejam os R.A.loops $L = L_2 \times A$ e $M = M_2 \times B$, onde L_2 e M_2 são R.A. 2-loops e A e B são grupos abelianos de ordem ímpar. Então $\mathbb{Q}L \cong \mathbb{Q}M$ se e somente se $A \cong B$ e $\mathbb{Q}L_2 \cong \mathbb{Q}M_2$.*

Demonstração: Suponhamos $\mathbb{Q}L \cong \mathbb{Q}M$.

Pelo teorema 2.1.1, nós temos que $\frac{L}{L'} \cong \frac{M}{M'}$ e $\Delta(L : L') \cong \Delta(M : M')$.

Como $\frac{L}{L'} \cong \frac{L_2}{L'_2} \times A$ e $\frac{M}{M'} \cong \frac{M_2}{M'_2} \times B$, segue que $\frac{L_2}{L'_2} \cong \frac{M_2}{M'_2}$ e $A \cong B$.

Pelo teorema 1.3.3, podemos escrever

$$\mathbb{Q}A \cong \mathbb{Q}B \cong \bigoplus_{d \mid |A|} v_d \mathbb{Q}(\xi_d) \cong \mathbb{Q} \oplus T, \quad ,$$

onde $T = \bigoplus_{\substack{d \mid |A| \\ d \neq 1}} v_d \mathbb{Q}(\xi_d)$.

Escrevamos $\mathbb{Q}L \cong \mathbb{Q}L_2 \otimes_{\mathbb{Q}} \mathbb{Q}A \cong (\mathbb{Q} \left[\frac{L_2}{L'_2} \right] \oplus \Delta(L_2 : L'_2)) \otimes_{\mathbb{Q}} \mathbb{Q}A$ e comparemos com $\mathbb{Q}L \cong \mathbb{Q} \left[\frac{L}{L'} \right] \oplus \Delta(L : L')$.

Fazendo a soma de todas as componentes simples não abelianas em ambos os membros, obtemos $\Delta(L : L') \cong \Delta(L_2 : L'_2) \otimes_{\mathbb{Q}} \mathbb{Q}A$.

Logo $\Delta(L : L') \cong \Delta(L_2 : L'_2) \otimes_{\mathbb{Q}} \mathbb{Q}A \cong \Delta(L_2 : L'_2) \oplus (\Delta(L_2 : L'_2) \otimes_{\mathbb{Q}} T)$ e, de forma análoga,

$$\Delta(M : M') \cong \Delta(M_2 : M'_2) \otimes_{\mathbb{Q}} \mathbb{Q}B \cong \Delta(M_2 : M'_2) \oplus (\Delta(M_2 : M'_2) \otimes_{\mathbb{Q}} T).$$

Pelos resultados da seção 1.3, sabemos que $\Delta(L_2 : L'_2)$ (e também que $\Delta(M_2 : M'_2)$) é uma soma direta de álgebras de Cayley-Dickson sobre corpos da forma $\mathbb{Q}(\xi_{2^i})$, enquanto que $\Delta(L_2 : L'_2) \otimes_{\mathbb{Q}} T$ (e $\Delta(M_2 : M'_2) \otimes_{\mathbb{Q}} T$) não contêm tais somandos. Do isomorfismo $\Delta(L : L') \cong \Delta(M : M')$, concluímos que $\Delta(L_2 : L'_2) \cong \Delta(M_2 : M'_2)$ e, novamente pelo teorema 2.1.1, que $\mathbb{Q}L_2 \cong \mathbb{Q}M_2$.

Reciprocamente, temos que

$$\mathbb{Q}L \cong \mathbb{Q}L_2 \otimes_{\mathbb{Q}} \mathbb{Q}A \cong \mathbb{Q}M_2 \otimes_{\mathbb{Q}} \mathbb{Q}B \cong \mathbb{Q}M. \quad \square$$

Em vista da proposição 2.3.1, estudaremos com mais detalhes o problema do isomorfismo para os R.A. 2-loops. A partir de agora fixaremos nossa atenção nos R.A. 2-loops do tipo **II**.

O seguinte teorema nos dá condições necessárias e suficientes para se ter o isomorfismo de álgebras de R.A. 2-loops do tipo **II**.

Teorema 2.3.2 *Sejam L e M dois R.A. 2-loops do tipo **II**. Denotemos por N e P , respectivamente, os loops quocientes $\frac{L}{Z(L)^2}$ e $\frac{M}{Z(M)^2}$. Então $\mathbb{Q}L \cong \mathbb{Q}M$ se e somente se $\frac{L}{L'} \cong \frac{M}{M'}$, $Z(L) \cong Z(M)$ e $\Delta(N : N') \cong \Delta(P : P')$.*

Demonstração: Suponhamos que L e M são R.A. 2-loops do tipo **II** tais que $\mathbb{Q}L \cong \mathbb{Q}M$.

Pelo teorema 2.1.1, temos que $\frac{L}{L'} \cong \frac{M}{M'}$ e $\Delta(L : L') \cong \Delta(M : M')$. Este último isomorfismo implica que $Z(\Delta(L : L')) \cong Z(\Delta(M : M'))$.

Escrevendo $Z(L) = L' \times E$ e $Z(M) = M' \times F$, onde E e F são 2-grupos

abelianos, temos que

$$Z(\Delta(L : L')) \cong \mathbb{Q}[Z(L)].(1 - \hat{L}') \cong [\mathbb{Q}L'.(1 - \hat{L}')]E \cong \mathbb{Q}E \quad e$$

$$Z(\Delta(M : M')) \cong \mathbb{Q}[Z(M)].(1 - \hat{M}') \cong [\mathbb{Q}M'.(1 - \hat{M}')]F \cong \mathbb{Q}F.$$

Portanto $\mathbb{Q}E \cong \mathbb{Q}F$, o que implica $E \cong F$. Desta implicação concluímos que $Z(L) \cong Z(M)$.

Agora, escrevendo $E \cong F \cong C_{2^{n_2}} \times \cdots \times C_{2^{n_t}}$, temos

$$Z(\Delta(L : L')) \cong Z(\Delta(M : M')) \cong \underbrace{\mathbb{Q} \oplus \cdots \oplus \mathbb{Q}}_{2^{t-1} \text{ vezes}} \oplus \mathcal{S},$$

onde $\mathcal{S}$ é uma soma direta de corpos da forma $\mathbb{Q}(\xi_{2^i})$, $i \geq 2$.

Assim, pelo teorema 1.3.9, $\Delta(L : L') \cong \Delta(M : M') \cong \bigoplus_{i=1}^{2^{t-1}} \mathcal{A}_i(\mathbb{Q}) \oplus \mathcal{A}$, onde cada $\mathcal{A}_i(\mathbb{Q})$ é uma álgebra de Cayley-Dickson sobre $\mathbb{Q}$ e $\mathcal{A}$ é uma soma direta de álgebras de Cayley-Dickson sobre $\mathbb{Q}(\xi_{2^i})$, $i \geq 2$. Conforme ([14], Lema 6.2), $\mathcal{A}$ é uma soma direta de álgebras “split”, porque cada uma delas contém $\mathbb{Q}(\xi_{2^i})$, $i \geq 2$ em seu centro.

Escrevendo

$$Z(L) \cong Z(M) \cong C_2 \times C_{2^{n_2}} \times \cdots \times C_{2^{n_t}}$$

e analisando $N = \frac{L}{Z(L)^2}$ e $P = \frac{M}{Z(M)^2}$, vemos que $Z(N) \cong Z(P) \cong \underbrace{C_2 \times \cdots \times C_2}_{t \text{ vezes}}$.

Dessa forma N and P são R.A. loops de ordem 2^{t+3} , e

$$Z(\Delta(N : N')) \cong \underbrace{\mathbb{Q} \oplus \cdots \oplus \mathbb{Q}}_{2^{t-1} \text{ vezes}} \cong Z(\Delta(P : P')).$$

Logo, pelo teorema 1.3.9, $\Delta(N : N') \cong \bigoplus_{i=1}^{2^{t-1}} C_i(\mathbb{Q})$ e $\Delta(P : P') \cong \bigoplus_{i=1}^{2^{t-1}} D_i(\mathbb{Q})$, onde $C_i(\mathbb{Q})$ e $D_i(\mathbb{Q})$ são álgebras de Cayley-Dickson sobre $\mathbb{Q}$.

Assim temos

$$\mathbf{Q}L \cong \mathbf{Q}N \oplus \Delta(L : Z(L)^2) \cong \mathbf{Q} \left[\frac{N}{N'} \right] \oplus \Delta(N : N') \oplus \Delta(L : Z(L)^2) \text{ e}$$

$$\mathbf{Q}M \cong \mathbf{Q}P \oplus \Delta(M : Z(M)^2) \cong \mathbf{Q} \left[\frac{P}{P'} \right] \oplus \Delta(P : P') \oplus \Delta(M : Z(M)^2).$$

Em $\mathbf{Q}L$ existem exatamente 2^{t-1} componentes simples que são álgebras de Cayley-Dickson com centro $\mathbf{Q}$, o mesmo acontecendo com $\mathbf{Q}M$, $\Delta(N : N')$, $\Delta(P : P')$.

Reordenando se necessário, e comparando, podemos concluir que

$$C_i(\mathbf{Q}) \cong \mathcal{A}_i(\mathbf{Q}) \cong D_i(\mathbf{Q}), \quad i = 1, \dots, 2^{t-1}. \text{ Portanto } \Delta(N : N') \cong \Delta(P : P').$$

Reciprocamente, $\frac{L}{L'} \cong \frac{M}{M'}$ implica que $\mathbf{Q} \left[\frac{L}{L'} \right] \cong \mathbf{Q} \left[\frac{M}{M'} \right]$, e, escrevendo,

$$Z(L) \cong Z(M) \cong C_2 \times C_{2^{n_2}} \times \dots \times C_{2^{n_t}},$$

nós temos que

$$Z(\Delta(L : L')) \cong Z(\Delta(M : M')) \cong \underbrace{\mathbf{Q} \oplus \dots \oplus \mathbf{Q}}_{2^{t-1} \text{ vezes}} \oplus \mathcal{S},$$

com $\mathcal{S} \cong \bigoplus_{j=1}^m K_j$, onde cada K_i é um corpo da forma $K_j = \mathbf{Q}(\xi_{2^i})$, $i \geq 2$.

Então, pelo teorema 1.3.9,

$$\Delta(L : L') \cong \bigoplus_{i=1}^{2^{t-1}} \mathcal{A}_i(\mathbf{Q}) \oplus \bigoplus_{j=1}^m \mathcal{A}_j(K_j) \oplus \Delta(M : M') \cong \bigoplus_{i=1}^{2^{t-1}} B_i(\mathbf{Q}) \oplus B_j(K_j),$$

onde $\mathcal{A}_i(\mathbf{Q})$ e $B_i(\mathbf{Q})$, $i = 1, \dots, 2^{t-1}$ são álgebras de Cayley-Dickson sobre $\mathbf{Q}$ e $\mathcal{A}_j(K_j)$ e $B_j(K_j)$, $j = 1, \dots, m$, são álgebras de Cayley-Dickson sobre K_j .

Como cada corpo K_j contém uma raiz 2^i -ésima da unidade com $i \geq 2$, As álgebras $\mathcal{A}_j(K_j)$ e $B_j(K_j)$, $j = 1, \dots, m$, são “split”. Portanto, conforme [25], temos que $\mathcal{A}_j(K_j) \cong B_j(K_j)$, $j = 1, \dots, m$.

A condição $\Delta(N : N') \cong \Delta(P : P')$ implica que $\mathcal{A}_i(\mathbf{Q}) \cong B_i(\mathbf{Q})$, $i = 1, 2, \dots, 2^{t-1}$, e, portanto, $\Delta(L : L') \cong \Delta(M : M')$. Pelo teorema 2.1.1, concluímos que $\mathbf{Q}L \cong \mathbf{Q}M$. $\square$

Vamos fixar mais algumas notações, que valerão ao longo desta seção. Sejam L e M são R.A. 2-loops do tipo II, e escrevamos $L = L_1 \times E$, $M = M_1 \times F$, onde L_1 e M_1 são R.A. loops indecomponíveis e E e F são 2-grupos abelianos (eventualmente triviais). Como no teorema 2.3.2, denotemos $N = \frac{L}{Z(L)^2}$ e $P = \frac{M}{Z(M)^2}$. Denotemos agora $N_1 = \frac{L_1}{Z(L_1)^2}$ e $P_1 = \frac{M_1}{Z(M_1)^2}$. Dessa forma temos que $N \cong N_1 \times \frac{E}{E^2}$ e $P \cong P_1 \times \frac{F}{F^2}$, onde $\frac{E}{E^2}$ e $\frac{F}{F^2}$ são 2-grupos abelianos elementares. Observemos que $\text{posto}(\frac{E}{E^2}) = \text{posto}(E)$ e $\text{posto}(\frac{F}{F^2}) = \text{posto}(F)$.

Observemos também que N_1 e P_1 são R.A. loops indecomponíveis com centros de expoente 2, os quais foram estudados na seção 2.2, e que $\text{posto}(Z(N_1)) = \text{posto}(Z(L_1))$ e $\text{posto}(Z(P_1)) = \text{posto}(Z(M_1))$.

Vamos explorar mais esses fatos.

Proposição 2.3.3 *Sejam L e M dois R.A. 2-loops do tipo II tais que $\mathbf{Q}L \cong \mathbf{Q}M$. Então $\text{posto}(E) = \text{posto}(F)$ e $N_1 \cong P_1$.*

Demonstração: Assumindo $\mathbf{Q}L \cong \mathbf{Q}M$, então pelo teorema 2.3.2, temos que $\frac{L}{L'} \cong \frac{M}{M'}$, $Z(L) \cong Z(M)$ e $\Delta(N : N') \cong \Delta(P : P')$.

Chamando $\alpha = \text{posto}(E)$ e $\beta = \text{posto}(F)$, assim como na demonstração do teorema 2.3.2, nós temos que

$$\Delta(N : N') \cong \Delta(N_1 : N'_1) \otimes_{\mathbf{Q}} \mathbf{Q} \left[\frac{E}{E^2} \right] \text{ e } \Delta(P : P') \cong \Delta(N_1 : N'_1) \otimes_{\mathbf{Q}} \mathbf{Q} \left[\frac{F}{F^2} \right].$$

$$\text{Como } \mathbb{Q} \left[\frac{E}{E^2} \right] \cong \mathbb{Q}[\underbrace{C_2 \times C_2 \times \cdots \times C_2}_{\alpha \text{ vezes}}] \cong \underbrace{\mathbb{Q} \oplus \mathbb{Q} \oplus \cdots \oplus \mathbb{Q}}_{2^\alpha \text{ vezes}} \quad \text{e}$$

$$\mathbb{Q} \left[\frac{F}{F^2} \right] \cong \mathbb{Q}[\underbrace{C_2 \times C_2 \times \cdots \times C_2}_{\beta \text{ vezes}}] \cong \underbrace{\mathbb{Q} \oplus \mathbb{Q} \oplus \cdots \oplus \mathbb{Q}}_{2^\beta \text{ vezes}} \quad ,$$

concluimos que

$$\Delta(N : N') \cong 2^\alpha \cdot \Delta(N_1 : N'_1) \quad \text{e} \quad \Delta(P : P') \cong 2^\beta \cdot \Delta(P_1 : P'_1).$$

Do isomorfismo $\Delta(N : N') \cong \Delta(P : P')$ segue que

$$2^\alpha \cdot \Delta(N_1 : N'_1) \cong 2^\beta \cdot \Delta(P_1 : P'_1).$$

Sabemos que N_1 e P_1 são R.A. loops indecomponíveis com centro de expoente 2, e, dependendo se $\mathcal{C}(\mathbb{Q})$ aparece ou não como somando direto de $\mathbb{Q}L$ e de $\mathbb{Q}M$, concluimos que N_1 e P_1 estão simultaneamente em $\mathcal{A} = \{\mathbf{I}_2, \mathbf{I}_4, \mathbf{I}_6, \mathbf{I}_7\}$ ou em $\mathcal{B} = \{\mathbf{I}_1, \mathbf{I}_3, \mathbf{I}_5\}$, onde $\mathbf{I}_1, \mathbf{I}_2, \dots, \mathbf{I}_7$ denotam os sete R.A. loops indecomponíveis descritos na seção 2.2.

Se N_1 e P_1 estão em $\mathcal{A}$, concluimos que $\alpha = \beta$ pois $\mathcal{C}(\mathbb{Q})$ aparece uma única vez como somando direto na decomposição de $\mathbb{Q}\mathbf{I}_2, \mathbb{Q}\mathbf{I}_4, \mathbb{Q}\mathbf{I}_6$ and $\mathbb{Q}\mathbf{I}_7$.

Vamos considerar agora o caso em que ambos, N_1 e P_1 , estão em $\mathcal{B} = \{\mathbf{I}_1, \mathbf{I}_3, \mathbf{I}_5\}$. É nossa intenção mostrar que a desigualdade $\alpha \neq \beta$ leva a uma contradição. Temos 3 possibilidades a considerar:

(a) $N_1 \cong \mathbf{I}_1$ e $P_1 \cong \mathbf{I}_3$,

(b) $N_1 \cong \mathbf{I}_1$ e $P_1 \cong \mathbf{I}_5$ e

(c) $N_1 \cong \mathbf{I}_3$ e $P_1 \cong \mathbf{I}_5$.

Vamos analisá-las.

(a) Se $N_1 \cong \mathbf{I}_1$ e $P_1 \cong \mathbf{I}_3$ então $\text{posto}(Z(L_1)) = \text{posto}(Z(N_1)) = 1$ e $\text{posto}(Z(M_1)) = \text{posto}(Z(P_1)) = 2$. Escrevendo $Z(M_1) \cong C_2 \times C_{2^{b'}}$, com $b' > 0$; como $Z(L_1) \cong C_2$, $Z(L) \cong Z(L_1) \times E$, $Z(M) \cong Z(M_1) \times F$ e $Z(L) \cong Z(M)$, nós temos que $C_2 \times E \cong C_2 \times C_{2^{b'}} \times F$, o que implica $E \cong C_{2^{b'}} \times F$. Então $L \cong L_1 \times C_{2^{b'}} \times F$ e $\frac{L}{L'} \cong \frac{L_1}{L'_1} \times C_{2^{b'}} \times F$. Pelo corolário 2.1.4, temos que $\frac{L_1}{L'_1} \cong C_2 \times C_2 \times C_2$ e $\frac{M_1}{M'_1} \cong C_2 \times C_2 \times C_{2^{b'+1}}$. Como $\frac{L}{L'} \cong \frac{M}{M'} \cong \frac{M_1}{M'_1} \times F$, segue que $C_2 \times C_2 \times C_2 \times C_{2^{b'}} \times F \cong C_2 \times C_2 \times C_{2^{b'+1}} \times F$, o que implica que $b' = 0$, uma contradição.

(b) Se $N_1 \cong \mathbf{I}_1$ e $P_1 \cong \mathbf{I}_5$, nós temos que $\text{posto}(Z(L_1)) = 1$ e $\text{posto}(Z(M_1)) = 3$. Escrevendo $Z(M_1) \cong C_2 \times C_{2^{b'}} \times C_{2^{c'}}$ com $b' \geq c' > 0$, como $Z(L_1) \cong C_2$, $Z(L) \cong Z(L_1) \times E$, $Z(M) \cong Z(M_1) \times F$ e $Z(L) \cong Z(M)$, temos que $C_2 \times E \cong C_2 \times C_{2^{b'}} \times C_{2^{c'}} \times F$, o que implica $E \cong C_{2^{b'}} \times C_{2^{c'}} \times F$. Então $L \cong L_1 \times C_{2^{b'}} \times C_{2^{c'}} \times F$ e $\frac{L}{L'} \cong \frac{L_1}{L'_1} \times C_{2^{b'}} \times C_{2^{c'}} \times F$. Pela corolário 2.1.4, temos que $\frac{L_1}{L'_1} \cong C_2 \times C_2 \times C_2$ e $\frac{M_1}{M'_1} \cong C_2 \times C_{2^{b'+1}} \times C_{2^{c'+1}}$. Como $\frac{L}{L'} \cong \frac{M}{M'}$, segue que $C_2 \times C_2 \times C_2 \times C_{2^{b'}} \times C_{2^{c'}} \times F \cong C_2 \times C_{2^{b'+1}} \times C_{2^{c'+1}} \times F$, o que implica $b' = c' = 0$, uma contradição.

(c) Suponhamos, finalmente, que $N_1 \cong \mathbf{I}_3$ e $P_1 \cong \mathbf{I}_5$. Então $\text{posto}(Z(L_1)) = 2$ e $\text{posto}(Z(M_1)) = 3$. Escrevamos $Z(L_1) \cong C_2 \times C_{2^b}$ e $Z(M_1) \cong C_2 \times C_{2^{b'}} \times C_{2^{c'}}$, com $b > 0$ e $b' \geq c' > 0$. Com antes, temos $C_2 \times C_{2^b} \times E \cong C_2 \times C_{2^{b'}} \times C_{2^{c'}} \times F$. Se $b = b'$, temos $E \cong C_{2^{c'}} \times F$. Então $L \cong L_1 \times C_{2^{c'}} \times F$, e, assim, $\frac{L}{L'} \cong C_2 \times C_2 \times C_{2^{b+1}} \times C_{2^{c'}} \times F$ e $\frac{M}{M'} \cong C_2 \times C_{2^{b+1}} \times C_{2^{c'+1}} \times F$. Como $\frac{L}{L'} \cong \frac{M}{M'}$, concluímos que $c' = 0$, uma contradição.

O caso $b = c'$ é semelhante, logo, suponhamos $b \neq b', c'$. Como $C_2 \times E \cong C_{2^{b'}} \times C_{2^c} \times F$, existem subgrupos H_1 e K_1 de E e F , respectivamente, tais que

$E \cong C_{2^{b'}} \times C_{2^{c'}} \times H_1$, $F \cong C_{2^b} \times K_1$ e $H_1 \cong K_1$. Então $L \cong L_1 \times C_{2^{b'}} \times C_{2^{c'}} \times H_1$ e $M \cong M_1 \times C_{2^b} \times H_1$. Assim $\frac{L}{L'} \cong C_2 \times C_2 \times C_{2^{b+1}} \times C_{2^{b'}} \times C_{2^{c'}} \times H_1$ e $\frac{M}{M'} \cong C_2 \times C_{2^{b'+1}} \times C_{2^{c'+1}} \times C_{2^b} \times H_1$. Como $\frac{L}{L'}$, temos $b = b' = c' = 0$, uma contradição.

Portanto $\alpha = \beta$, o que implica que $\Delta(N_1 : N'_1) \cong \Delta(P_1 : P'_1)$. Como N_1 e P_1 são R.A. loops indecomponíveis com centro de expoente 2, segue que $N_1 \cong P_1$. $\square$

Proposição 2.3.4 *Sejam L e M dois R.A. 2-loops do tipo II tais que $QL \cong QM$. Consideremos L_1 , M_1 , E e F como antes. Nessas condições, se $E \cong F$ então $L_1 \cong M_1$.*

Demonstração: Como $Z(L) \cong Z(L_1) \times E$, $Z(M) \cong Z(M_1) \times F$ e $Z(L) \cong Z(M)$; se $E \cong F$, então $Z(L_1) \cong Z(M_1)$. Assim, considerando as álgebras de loop $QN_1 \cong QP_1$, observamos que ou ambas admitem $\mathcal{C}(\mathbb{Q})$ como somando direto ou ambas não admitem. O mesmo é verdade para QL_1 e QM_1 . Então L_1 e M_1 estão na mesma família L_j descrita na Tabela 2.1.2. Como $Z(L_1) \cong Z(M_1)$, nós temos $L_1 \cong M_1$. $\square$

Finalmente estamos em condição de provar o principal resultado deste capítulo.

Teorema 2.3.5 *Sejam L e M dois R.A. loops do tipo II. Então $QL \cong QM$ se e somente se $L \cong M$, isto é, $\mathbb{Q}$ determina os R.A. loops do tipo II.*

Demonstração: Pela proposição 2.3.1, podemos assumir que L e M são

R.A. 2-loops do tipo II. Sejam $L_1, M_1, E, F, N, P, N_1$ e P_1 como antes.

Como $\mathbf{Q}L \cong \mathbf{Q}M$, nós temos que $\frac{L}{L'} \cong \frac{M}{M'}$, $Z(L) \cong Z(M)$ e $\Delta(N : N') \cong \Delta(P : P')$, e, também que $N_1 \cong P_1$. Pela proposição 2.3.4, só precisamos mostrar que $E \cong F$. Vamos analisar todas as possibilidades para N_1 e P_1 .

(a) Se $N_1 \cong P_1 \cong \mathbf{I}_1$ ou $\mathbf{I}_2$ então $Z(L_1) \cong C_2 \cong Z(M_1)$. Como $Z(L) \cong Z(M)$, temos que $E \cong F$.

(b) Se $N_1 \cong P_1 \cong \mathbf{I}_3$ ou $\mathbf{I}_4$ então $\text{posto}(Z(L_1)) = \text{posto}(Z(M_1)) = 2$. Escrevamos $Z(L_1) \cong C_2 \times C_{2^b}$ e $Z(M_1) \cong C_2 \times C_{2^{b'}}$. Como $Z(L) \cong Z(M)$, obtemos $C_{2^b} \times E \cong C_{2^{b'}} \times F$.

Se $b \neq b'$, podemos determinar subgrupos H_1 e K_1 de E e F , respectivamente, tais que

$$E \cong C_{2^{b'}} \times H_1, F \cong C_{2^b} \times K_1 \text{ e } H_1 \cong K_1.$$

$$\text{Então } L \cong L_1 \times C_{2^{b'}} \times H_1, M \cong M_1 \times C_{2^b} \times H_1.$$

Pelo corolário 2.1.4, temos

$$\frac{L_1}{L'_1} \cong C_2 \times C_2 \times C_{2^{b+1}}$$

e

$$\frac{M_1}{M'_1} \cong C_2 \times C_2 \times C_{2^{b'+1}}.$$

Como $\frac{L}{L'} \cong \frac{L_1}{L'_1} \times E$ e $\frac{M}{M'} \cong \frac{M_1}{M'_1} \times F$, temos que

$$\frac{L}{L'} \cong C_2 \times C_2 \times C_{2^{b+1}} \times C_{2^{b'}} \times H_1 \text{ e } \frac{M}{M'} \cong C_2 \times C_2 \times C_{2^{b'+1}} \times C_{2^b} \times H_1,$$

o que implica $\frac{L}{L'} \not\cong \frac{M}{M'}$, uma contradição. Logo $E \cong F$.

(c) Se $N_1 \cong P_1 \cong \mathbf{I}_5$ ou $\mathbf{I}_6$, então $\text{posto}(Z(L_1)) = \text{posto}(Z(M_1)) = 3$. Escrevamos $Z(L_1) \cong C_2 \times C_{2^b} \times C_{2^c}$ e $Z(M_1) \cong C_2 \times C_{2^{b'}} \times C_{2^{c'}}$. Então,

$$\frac{L_1}{L'_1} \cong C_2 \times C_{2^{b+1}} \times C_{2^{c+1}} \text{ e } \frac{M_1}{M'_1} \cong C_2 \times C_{2^{b'+1}} \times C_{2^{c'+1}}.$$

Do isomorfismo $Z(L) \cong Z(M)$ concluimos que $C_{2^b} \times C_{2^c} \times E \cong C_{2^{b'}} \times C_{2^{c'}} \times F$.

Se $(b, c) \neq (b', c')$, argumentos simples de contagem levam a contradições em todos possíveis casos. Portanto $E \cong F$.

(d) Se $N_1 \cong P_1 \cong \mathbf{I}_7$, escrevamos $Z(L_1) \cong C_2 \times C_{2^b} \times C_{2^c} \times C_{2^d}$ e

$Z(M_1) \cong C_2 \times C_{2^{b'}} \times C_{2^{c'}} \times C_{2^{d'}}$. Então,

$$\frac{L_1}{L'_1} \cong C_{2^{b+1}} \times C_{2^{c+1}} \times C_{2^{d+1}} \text{ e}$$

$$\frac{M_1}{M'_1} \cong C_{2^{b'+1}} \times C_{2^{c'+1}} \times C_{2^{d'+1}}.$$

Como $Z(L) \cong Z(M)$, obtemos

$$C_{2^b} \times C_{2^c} \times C_{2^d} \times E \cong C_{2^{b'}} \times C_{2^{c'}} \times C_{2^d} \times F.$$

Se $(b, c, d) \neq (b', c', d')$, mais uma vez nós vemos que, em todos possíveis casos tem-se $\frac{L}{L'} \not\cong \frac{M}{M'}$. Logo $E \cong F$. $\square$

Observamos que o teorema 2.3.2, o teorema 2.3.5 e a proposição 2.3.4 nos dão uma caracterização dos R.A. 2-loops do tipo II, que se estende facilmente para R.A. loops arbitrários do tipo II.

Corolário 2.3.6 *Sejam L e M dois R.A. loops do tipo II. Então*

$$L \cong M \text{ se e somente se } \begin{cases} \frac{L}{L'} \cong \frac{M}{M'} \\ Z(L) \cong Z(M) \\ \frac{L}{Z(L)^2} \cong \frac{M}{Z(M)^2} \end{cases}$$

$\square$

Capítulo 3

Corpos Equivalentes sobre Classes de R.A. Loops

3.1 Introdução

Vimos no capítulo anterior que $\mathbf{Q}$ determina os R.A. loops do tipo **II**. Pretendemos agora caracterizar os corpos que tem essa mesma propriedade em relação aos R.A. loops do tipo **II**.

Tratamento semelhante foi dado aos grupos abelianos. Era conhecido desde 1950 o resultado de S. Perlis e G. L. Walker [17] de que $\mathbf{Q}$ determina os grupos abelianos. Em 1974, E. Spiegel [21] conseguiu caracterizar os corpos que determinam os grupos abelianos no caso semisimples. Em trabalho subsequente, E. Spiegel e A. Trojan [22] conseguiram resultados parecidos para p -grupos quaisquer com $p \neq 2$ e, em seguida [23], para os 2-grupos, sempre no caso semisimples.

As seguintes definições são devidas a eles.

Os corpos $\mathbf{F}$ e $\mathbf{K}$ dizem-se *equivalentes* numa classe $\mathcal{G}$ de grupos se para todos G e H em $\mathcal{G}$ tem-se que $\mathbf{F}G \cong \mathbf{F}H$ se e somente se $\mathbf{K}G \cong \mathbf{K}H$.

Denotando por ξ_{2^n} uma raiz 2^n -ésima primitiva da unidade, definimos $\gamma_{\mathbf{K}}(n) = [\mathbf{K}(\xi_{2^{n+2}}) : \mathbf{K}(\xi_{2^{n+1}})]$ e chamamos $\{\gamma_{\mathbf{K}}(n)\}_{n=1,2,\dots}$ a *2-sequência* de $\mathbf{K}$.

Essa sequência tem uma das seguintes formas:

$$1, 1, 1, 1, \dots$$

$$1, 1, 1, 1, \dots, 1, 2, 2, \dots$$

$$2, 2, 2, 2, \dots$$

Definimos ainda:

$$\text{ind}_2(\mathbf{K}) = \begin{cases} 1 & \text{se } \gamma_{\mathbf{K}}(1) = 2 \\ n & \text{se } \gamma_{\mathbf{K}}(n) = 2 \text{ e } \gamma_{\mathbf{K}}(n-1) = 1 \text{ para } n \geq 2 \\ \infty & \text{se } \gamma_{\mathbf{K}}(n) = 1 \text{ para } n = 1, 2, 3, \dots \end{cases}$$

$$O(\mathbf{K}) = \begin{cases} 1 & \text{se } X^2 + 1 = 0 \text{ é solúvel em } \mathbf{K} \\ 0 & \text{se } X^2 + 1 = 0 \text{ não é solúvel em } \mathbf{K} \end{cases}$$

$$t(\mathbf{K}) = \begin{cases} 1 & \text{se } X^2 + Y^2 = -1 \text{ é solúvel em } \mathbf{K} \\ 0 & \text{se } X^2 + Y^2 = -1 \text{ não é solúvel em } \mathbf{K} \end{cases}$$

Eles chamaram $\text{ind}_2(\mathbf{K})$, $O(\mathbf{K})$ e $t(\mathbf{K})$ os *2-invariantes* de $\mathbf{K}$.

Destacamos aqui os seguintes resultados obtidos por eles e que serão de interesse:

Proposição 3.1.1 ([21]) *Os corpos $\mathbf{K}$ e $\mathbf{F}$ são equivalentes na classe dos 2-grupos abelianos finitos se e somente se $O(\mathbf{K}) = O(\mathbf{F})$ e $\text{ind}_2(\mathbf{K}) = \text{ind}_2(\mathbf{F})$.*

Corolário 3.1.2 ([21]) *O corpo K determina a classe dos 2-grupos abelianos finitos se e somente se $O(K) = 0$ e $ind_2(K) = 1$.*

Proposição 3.1.3 ([21]) *Seja K um corpo tal $O(K) = 0$. Então as seguintes condições são equivalentes:*

- (i) K determina a classe de todos 2-grupos abelianos finitos.
- (ii) K determina a família de 2-grupos $\Omega = \{C_8 \times C_2, C_4 \times C_4, C_4 \times C_2 \times C_2\}$.
- (iii) $K \cap \{\sqrt{2}, \sqrt{-2}, \sqrt{-1}\} = \emptyset$.

Proposição 3.1.4 ([23]) *Os corpos K e F são equivalentes na classe de todos os 2-grupos finitos se e somente se $t(K) = t(F)$, $O(K) = O(F)$ e $ind_2(K) = ind_2(F)$.*

É nossa intenção provar resultados semelhantes para os R.A. 2-loops.

Da mesma forma, diremos que dois corpos F e K são *equivalentes* numa classe $\mathcal{L}$ de loops se para todos L e M em $\mathcal{L}$ tem-se que $FL \cong FM$ se e somente se $KL \cong KM$.

Para abordar o problema para os R.A. loops introduzimos um novo 2-invariante:

$$c(K) = \begin{cases} 1 & \text{se } X^2 + Y^2 + Z^2 + W^2 = -1 \text{ é solúvel em } K \\ 0 & \text{se } X^2 + Y^2 + Z^2 + W^2 = -1 \text{ não é solúvel em } K \end{cases}$$

Os resultados da seção 1.2 mostram que esse invariante está relacionado com álgebras de Cayley-Dickson. A parte ii) do corolário 1.2.2 pode ser reescrita na forma do seguinte corolário:

Corolário 3.1.5

A álgebra de Cayley-Dickson $\mathcal{C}(\mathbf{K}, -1, -1, -1)$ é uma álgebra com divisão se e somente se $c(\mathbf{K}) = 0$.

Como $c(\mathbf{Q}) = 0$, temos mais uma vez que a álgebra de Cayley-Dickson $\mathcal{C}(\mathbf{Q}, -1, -1, -1)$ é uma álgebra com divisão.

O corolário 1.2.4 pode ser reinterpretado assim

Corolário 3.1.6

Se $\mathbf{K}$ é um corpo finito, então $c(\mathbf{K}) = 1$. Dessa forma a álgebra de Cayley-Dickson $\mathcal{C}(\mathbf{K}, -1, -1, -1)$ é uma álgebra “split”, quando o corpo $\mathbf{K}$ é finito.

3.2 Álgebras de R.A. 2-Loops Semisimples

Na seção 1.3, estabelecemos o teorema 1.3.9, que trata da estrutura das álgebras de loops semisimples. Em vista dos resultados obtidos no Capítulo 2, podemos explicitar a decomposição da álgebra de loop como soma de ideais bilaterais simples no caso em que o R.A. loop é um 2-loop e a característica do corpo não é 2.

Primeiro vamos analisar a estrutura de $Z(\Delta_{\mathbf{K}}(L : L'))$. Para uso futuro, particularizamos o enunciado da proposição 1.3.8. para R.A. 2-loops.

Proposição 3.2.1 *Sejam $\mathbf{K}$ um corpo com $\text{car}\mathbf{K} \neq 2$ e L um R.A. 2-loop. Escrevamos $Z(L) \cong C_{2^{n_1}} \times C_{2^{n_2}} \times \dots \times C_{2^{n_t}}$, onde $n_1 \geq 1$, $n_i \geq 0$ para $i = 2, 3, \dots, t$*

e $L' \subset C_{2^{n_1}}$. Então

$$Z(\Delta_K(L : L')) \cong \frac{2^{n_1-1}}{[K(\xi_{2^{n_1}}) : K]} \cdot K(\xi_{2^{n_1}})[C_{2^{n_2}} \times \dots \times C_{2^{n_t}}] \quad .$$

Demonstração: Da proposição 1.3.7 temos que

$$\begin{aligned} Z(\Delta_K(L : L')) &\cong K[Z(L)] \cdot \left(\frac{1-e}{2}\right), \text{ isto é,} \\ Z(\Delta_K(L : L')) &\cong K[C_{2^{n_1}} \times C_{2^{n_2}} \times \dots \times C_{2^{n_t}}] \cdot \left(\frac{1-e}{2}\right) \cong \\ &\cong \left[(KC_{2^{n_1}}) \cdot \left(\frac{1-e}{2}\right) \right] (C_{2^{n_2}} \times \dots \times C_{2^{n_t}}) . \end{aligned}$$

Como na demonstração da proposição 1.3.8, escrevamos

$$\begin{aligned} KC_{2^{n_1}} &= KC_{2^{n_1}} \cdot \left(\frac{1+e}{2}\right) \oplus KC_{2^{n_1}} \cdot \left(\frac{1-e}{2}\right). \text{ Observemos que} \\ KC_{2^{n_1}} \cdot \left(\frac{1+e}{2}\right) &\cong K\left(\frac{C_{2^{n_1}}}{\langle e \rangle}\right), \text{ onde } \frac{C_{2^{n_1}}}{\langle e \rangle} \text{ é um grupo cíclico de ordem } 2^{n_1-1}. \end{aligned}$$

$$\text{Do teorema 1.3.3 sabemos que } KC_{2^{n_1}} \cong \bigoplus_{n_i \leq n_1} \frac{n_{2^{n_i}}}{[K(\xi_{2^{n_i}}) : K]} K(\xi_{2^{n_i}}).$$

Aplicando o mesmo teorema para $KC_{2^{n_i-1}}$ é fácil ver que

$$KC_{2^{n_1}} \cong KC_{2^{n_1}} \cdot \left(\frac{1+e}{2}\right) \oplus \frac{n_{2^{n_1}}}{[K(\xi_{2^{n_1}}) : K]} \cdot K(\xi_{2^{n_1}})$$

e segue o resultado. $\square$

Usando a mesma demonstração e a mesma notação da seção 2.2., podemos mostrar que

$$\begin{aligned} KI_1 &\cong \underbrace{K \oplus \dots \oplus K}_{8 \text{ vezes}} \oplus \mathcal{C}(K, -1, -1, 1) \quad e \\ KI_2 &\cong \underbrace{K \oplus \dots \oplus K}_{8 \text{ vezes}} \oplus \mathcal{C}(K, -1, -1, -1) \end{aligned}$$

Observamos, então, que se $c(K) = 1$, temos um exemplo de dois R.A. loops não isomorfos com álgebras de loops isomorfas. Lembremos que $I_1 = M_{16}(Q, 2)$ e $I_2 = M_{16}(Q)$ são os dois R.A. loops não isomorfos de ordem 16.

Para facilitar a notação, escreveremos $\mathcal{C}_S(\mathbf{K})$ no lugar de $\mathcal{C}(\mathbf{K}, -1, -1, 1)$ e $\mathcal{C}(\mathbf{K})$ no lugar de $\mathcal{C}(\mathbf{K}, -1, -1, -1)$.

Assim, igualmente obtemos

$$\mathbf{KI}_3 \cong \underbrace{\mathbf{K} \oplus \cdots \oplus \mathbf{K}}_{8 \text{ vezes}} \oplus \underbrace{\mathbf{K}(i) \oplus \cdots \oplus \mathbf{K}(i)}_{\substack{8 \\ [K(\xi_4):K] \text{ vezes}}} \oplus \mathcal{C}_S(\mathbf{K}) \oplus \mathcal{C}_S(\mathbf{K})$$

$$\mathbf{KI}_4 \cong \underbrace{\mathbf{K} \oplus \cdots \oplus \mathbf{K}}_{8 \text{ vezes}} \oplus \underbrace{\mathbf{K}(i) \oplus \cdots \oplus \mathbf{K}(i)}_{\substack{8 \\ [K(\xi_4):K] \text{ vezes}}} \oplus \mathcal{C}_S(\mathbf{K}) \oplus \mathcal{C}(\mathbf{K})$$

$$\mathbf{KI}_5 \cong \underbrace{\mathbf{K} \oplus \cdots \oplus \mathbf{K}}_{8 \text{ vezes}} \oplus \underbrace{\mathbf{K}(i) \oplus \cdots \oplus \mathbf{K}(i)}_{\substack{24 \\ [K(\xi_4):K] \text{ vezes}}} \oplus \underbrace{\mathcal{C}_S(\mathbf{K}) \oplus \cdots \oplus \mathcal{C}_S(\mathbf{K})}_{4 \text{ vezes}}$$

$$\mathbf{KI}_6 \cong \underbrace{\mathbf{K} \oplus \cdots \oplus \mathbf{K}}_{8 \text{ vezes}} \oplus \underbrace{\mathbf{K}(i) \oplus \cdots \oplus \mathbf{K}(i)}_{\substack{24 \\ [K(\xi_4):K] \text{ vezes}}} \oplus \mathcal{C}_S(\mathbf{K}) \oplus \mathcal{C}_S(\mathbf{K}) \oplus \mathcal{C}_S(\mathbf{K}) \oplus \mathcal{C}(\mathbf{K})$$

$$\mathbf{KI}_7 \cong \underbrace{\mathbf{K} \oplus \cdots \oplus \mathbf{K}}_{8 \text{ vezes}} \oplus \underbrace{\mathbf{K}(i) \oplus \cdots \oplus \mathbf{K}(i)}_{\substack{56 \\ [K(\xi_4):K] \text{ vezes}}} \oplus \underbrace{\mathcal{C}_S(\mathbf{K}) \oplus \cdots \oplus \mathcal{C}_S(\mathbf{K})}_{7 \text{ vezes}} \oplus \mathcal{C}(\mathbf{K})$$

E assim estabelecemos:

Teorema 3.2.2 *Sejam L um R.A. 2-loop e $\mathbf{K}$ um corpo com $\text{car}\mathbf{K} \neq 2$. Então os somandos simples de $\mathbf{KL}$ são extensões de $\mathbf{K}$ por raízes 2^{d_i} -ésimas da unidade*

com $d_i \geq 1$ ou são álgebras de Cayley-Dickson da forma $\mathcal{C}(\mathbf{K})$ ou $\mathcal{C}_S(\mathbf{K}(\xi_{2^{d_i}}))$ com $d_i \geq 1$.

Demonstração: Pela proposição 1.3.4 temos que

$$\mathbf{K}L \cong \mathbf{K} \left[\frac{L}{L'} \right] \oplus \Delta_{\mathbf{K}}(L : L') .$$

Como $\frac{L}{L'}$ é um 2-grupo abeliano, pelo teorema 1.3.3, sabemos que $\mathbf{K} \left[\frac{L}{L'} \right]$ é isomorfo a uma soma direta de extensões de $\mathbf{K}$ por raízes 2^{d_i} -ésimas da unidade.

Escrevamos $Z(L) \cong C_{2^{n_1}} \times C_{2^{n_2}} \times \dots \times C_{2^{n_t}}$, onde $n_1 \geq 1$, $n_i \geq 0$ para $i = 2, 3, \dots, t$ e $L' \subset C_{2^{n_1}}$. Então pela proposição 3.2.1, podemos escrever

$$Z(\Delta_{\mathbf{K}}(L : L')) \cong \frac{2^{n_1-1}}{[\mathbf{K}(\xi_{2^{n_1}}) : \mathbf{K}]} \cdot \mathbf{K}(\xi_{2^{n_1}})[C_{2^{n_2}} \times \dots \times C_{2^{n_t}}] \cong \bigoplus_i \mathbf{K}(\xi_{2^{d_i}}) .$$

Dessa forma $\Delta_{\mathbf{K}}(L : L') \cong \bigoplus_i \mathcal{A}_i(\mathbf{K}_i)$, onde $\mathbf{K}_i = \mathbf{K}(\xi_{2^{d_i}})$.

Se L é do tipo **I** então $n_1 > 1$ e todos os corpos $\mathbf{K}_i$ contém uma raiz 2^{d_i} -ésima da unidade com $d_i \geq 2$. Sabemos por [14] que as álgebras $\mathcal{A}_i(\mathbf{K}_i)$ são álgebras “split”, e, portanto, conforme [25], isomorfas a $\mathcal{C}_S(\mathbf{K}_i)$.

Se L é do tipo **II**, então $n_1 = 1$ e $\Delta_{\mathbf{K}}(L : L')$ tem pelo menos 2^{t-1} somandos diretos simples, cujo centro é $\mathbf{K}$.

Se $\mathbf{K}(\xi_{2^2}) = \mathbf{K}$ então $\mathbf{K}$ contém uma raiz 2^2 -ésima da unidade, o que implica que as álgebras $\mathcal{A}_i(\mathbf{K})$ são “split”. Dessa forma todas as álgebras $\mathcal{A}_i(\mathbf{K}_i)$ são “split”, e, portanto, isomorfas respectivamente a $\mathcal{C}_S(\mathbf{K}_i)$.

Se $\mathbf{K}(\xi_{2^2}) \neq \mathbf{K}$ então $\Delta_{\mathbf{K}}(L : L')$ tem exatamente 2^{t-1} somandos simples que são álgebras de Cayley-Dickson com centro isomorfo a $\mathbf{K}$. Consideremos o R.A. loop $N = \frac{L}{Z(L)^2}$. Então $\Delta_{\mathbf{K}}(L : L')$ tem 2^{t-1} somandos simples, todos com centro $\mathbf{K}$.

Sabemos que

$$\mathbf{K}L \cong \mathbf{K}N \oplus \Delta_{\mathbf{K}}(L : Z(L)^2) \cong \mathbf{K} \left[\frac{N}{N'} \right] \oplus \Delta_{\mathbf{K}}(N : N') \oplus \Delta_{\mathbf{K}}(L : Z(L)^2).$$

Como $Z(N)$ é de expoente 2, escrevamos $N = N_1 \times H$, onde $N_1 \in \{\mathbf{I}_1, \mathbf{I}_2, \dots, \mathbf{I}_7\}$ e H é um 2-grupo abeliano elementar. Em vista das observações que precederam este teorema, é fácil ver que os únicos possíveis somandos simples de $\Delta(N : N')$ são da forma $\mathcal{C}_S(\mathbf{K})$ ou $\mathcal{C}(\mathbf{K})$.

Os outros somandos simples de $\Delta_{\mathbf{K}}(L : L')$, que admitem $\mathbf{K}(\xi_{2^{d_i}})$, $i \geq 2$, como centro, são álgebras “split”, e, portanto, isomorfas a $\mathcal{C}_S(\mathbf{K}(\xi_{2^{d_i}}))$. $\square$

3.3 O Problema da Equivalência

Agora estamos em condições de estudar o problema da equivalência de corpos sobre certas classes de R.A. 2-loops.

Como vimos na seção anterior, os R.A. 2-loops do tipo I e do tipo II têm decomposições diferentes no que concerne a existência de álgebras com divisão como somandos diretos de suas álgebras de loops. Vamos estudá-los separadamente.

Para os R.A. 2-loops do tipo II estabelecemos o seguinte:

Teorema 3.3.1 *Sejam os corpos $\mathbf{F}$ e $\mathbf{K}$ corpos de característica diferente de 2. Seja $\mathcal{L}_2$ a classe dos R.A. 2-loops finitos do tipo II. Então $\mathbf{F}$ é equivalente a $\mathbf{K}$ em $\mathcal{L}_2$ se e somente se as seguintes condições se verificam:*

- (a) $O(\mathbf{F}) = O(\mathbf{K})$
- (b) $ind_2(\mathbf{F}) = ind_2(\mathbf{K})$
- (c) $c(\mathbf{F}) = c(\mathbf{K})$

Demonstração: Suponhamos que $\mathbf{F}$ e $\mathbf{K}$ são equivalentes em $\mathcal{L}_2$. Primeiro vamos provar que $\mathbf{F}$ e $\mathbf{K}$ são equivalentes na classe dos 2-grupos abelianos finitos.

Suponhamos que A e B são 2-grupos abelianos finitos tais que $\mathbf{F}A \cong \mathbf{F}B$. Seja $I = M_{16}(Q)$, o loop de Cayley, do qual sabemos que $\frac{I}{I'} \cong C_2 \times C_2 \times C_2$.

Consideremos os R.A. loops $L = I \times A$ e $M = I \times B$ de $\mathcal{L}_2$. Então $\mathbf{F}L \cong \mathbf{F}M$. Como $\mathbf{F}$ é equivalente a $\mathbf{K}$ em $\mathcal{L}_2$, segue que $\mathbf{K}L \cong \mathbf{K}M$. Deste isomorfismo tiramos que $\mathbf{K} \left[\frac{L}{L'} \right] \cong \mathbf{K} \left[\frac{M}{M'} \right]$, isto é, $\mathbf{K}[C_2 \times C_2 \times C_2 \times A] \cong \mathbf{K}[C_2 \times C_2 \times C_2 \times B]$. Deste último isomorfismo concluímos que $\mathbf{K}A \cong \mathbf{K}B$.

Portanto $\mathbf{F}$ e $\mathbf{K}$ são equivalentes na classe dos 2-grupos abelianos. Pela proposição 3.1.1, temos então que $O(\mathbf{F}) = O(\mathbf{K})$ e $ind_2(\mathbf{F}) = ind_2(\mathbf{K})$.

Se tivéssemos $c(\mathbf{F}) \neq c(\mathbf{K})$, suponhamos que fosse $c(\mathbf{F}) = 1$ e $c(\mathbf{K}) = 0$. Então para $L = M_{16}(Q)$ e $M = M_{16}(Q, 2)$, nós teríamos que $\mathbf{F}L \cong \mathbf{F}M$ e $\mathbf{K}L \not\cong \mathbf{K}M$. Portanto $\mathbf{F}$ e $\mathbf{K}$ não seriam equivalentes em $\mathcal{L}_2$. Logo $c(\mathbf{F}) = c(\mathbf{K})$.

Reciprocamente, suponhamos que valem as condições (a), (b) e (c).

Para L e M em $\mathcal{L}_2$ assumamos que $\mathbf{F}L \cong \mathbf{F}M$. Então pelo teorema 1.3.6,

$$\mathbf{F} \left[\frac{L}{L'} \right] \cong \mathbf{F} \left[\frac{M}{M'} \right] \quad \text{e} \quad \Delta_{\mathbf{F}}(L : L') \cong \Delta_{\mathbf{F}}(M : M').$$

As condições (a) e (b) implicam, pela proposição 3.1.1, que $\mathbf{K} \left[\frac{L}{L'} \right] \cong \mathbf{K} \left[\frac{M}{M'} \right]$. Vamos provar que $\Delta_{\mathbf{K}}(L : L') \cong \Delta_{\mathbf{K}}(M : M')$.

Escrevamos $Z(L) = C_2 \times C_{2^{n_2}} \times \cdots \times C_{2^{n_t}}$ e $Z(M) = C_2 \times C_{2^{m_2}} \times \cdots \times C_{2^{m_r}}$, com $n_i \geq 0$ para $i = 2, \dots, t$ e $m_j \geq 0$ para $j = 2, \dots, r$. Notamos que

$$\begin{aligned} Z(\Delta_{\mathbf{F}}(L : L')) &\cong \mathbf{F}[Z(L)] \cdot (1 - \hat{L}') \cong (\mathbf{F}C_2(1 - \hat{L}'))[C_{2^{n_2}} \times \cdots \times C_{2^{n_t}}] \\ &\cong \mathbf{F}[C_{2^{n_2}} \times \cdots \times C_{2^{n_t}}] \end{aligned}$$

e, analogamente, que

$$Z(\Delta_{\mathbf{F}}(M : M')) \cong \mathbf{F}[C_{2^{m_2}} \times \cdots \times C_{2^{m_r}}] .$$

Como

$$Z(\Delta_{\mathbf{F}}(L : L')) \cong Z(\Delta_{\mathbf{F}}(M : M')) ,$$

nós temos pela proposição 3.2.1,

$$\mathbf{F}[C_{2^{n_2}} \times \cdots \times C_{2^{n_t}}] \cong \mathbf{F}[C_{2^{m_2}} \times \cdots \times C_{2^{m_r}}] \cong \bigoplus_{i=1}^m \mathbf{F}_i ,$$

onde $\mathbf{F}_i = \mathbf{F}(\xi_{2^{b_i}})$ com $b_i \geq 1$ para $i = 1, \dots, m$.

Escrevamos $\Delta_{\mathbf{F}}(L : L') \cong \bigoplus_{i=1}^m \mathcal{A}_i(\mathbf{F}_i)$ e $\Delta_{\mathbf{F}}(M : M') \cong \bigoplus_{i=1}^m \mathcal{B}_i(\mathbf{F}_i)$, onde $\mathcal{A}_i(\mathbf{F}_i)$ e $\mathcal{B}_i(\mathbf{F}_i)$ são álgebras de Cayley-Dickson sobre $\mathbf{F}_i$. Como $\Delta_{\mathbf{F}}(L : L') \cong \Delta_{\mathbf{F}}(M : M')$, nós temos que $\mathcal{A}_i(\mathbf{F}_i) \cong \mathcal{B}_i(\mathbf{F}_i)$ para $i = 1, \dots, m$, reordenando se necessário.

Por outro lado, do mesmo modo, temos que

$$Z(\Delta_{\mathbf{K}}(L : L')) \cong \mathbf{K}[C_{2^{n_2}} \times \cdots \times C_{2^{n_t}}] \quad \text{e}$$

$$Z(\Delta_K(M : M')) \cong K[C_{2^{m_2}} \times \cdots \times C_{2^{m_r}}] \quad .$$

As condições (a) e (b) implicam, pela proposição 3.2.1, que $K[C_{2^{n_2}} \times \cdots \times C_{2^{n_t}}] \cong K[C_{2^{m_2}} \times \cdots \times C_{2^{m_r}}]$.

Logo $Z(\Delta_K(L : L')) \cong Z(\Delta_K(M : M')) \cong \bigoplus_{i=1}^s K_i$, onde $K_i = K(\xi_{2^{a_i}})$ com $a_i \geq 1$ para $i = 1, \dots, s$.

Escrevamos $\Delta_K(L : L') \cong \bigoplus_{i=1}^s \mathcal{C}_i(K_i)$ e $\Delta_K(M : M') \cong \bigoplus_{i=1}^s \mathcal{D}_i(K_i)$, onde $\mathcal{C}_i(K_i)$ e $\mathcal{D}_i(K_i)$ são álgebras de Cayley-Dickson com centro K_i .

Para $K_i = K(\xi_{2^{a_i}})$ com $a_i \geq 2$, temos $\mathcal{C}_i(K_i) \cong \mathcal{D}_i(K_i)$, porque elas são álgebras de Cayley-Dickson “split” sobre o mesmo corpo K_i . Resta analisar o caso em que $K_i = K$.

Se $c(K) = c(F) = 1$ todas as álgebras $\mathcal{C}_i(K)$ e $\mathcal{D}_i(K)$ são “split”, e, portanto, isomorfas.

Se $c(K) = c(F) = 0$, então algumas das álgebras $\mathcal{C}_i(K)$ e $\mathcal{D}_i(K)$ podem ser álgebras com divisão. Nesse caso, pelo teorema 3.2.2, elas são isomorfas à álgebra $\mathcal{C}(K)$. Só precisamos mostrar que o número de tais álgebras em $\Delta_K(L : L')$ e em $\Delta_K(M : M')$ é o mesmo. Pelo corolário 3.1.6 temos $\text{car} F = \text{car} K = 0$. Assim, podemos supor que $\mathbb{Q} \subset F$ e $\mathbb{Q} \subset K$. Da condição $c(F) = c(K) = 0$, também concluímos que $O(F) = O(K) = 0$.

Chamemos $m_K(L)$ o número de somandos diretos de KL , que são álgebras de Cayley-Dickson com divisão. De

$$KL \cong K \otimes_{\mathbb{Q}} QL, \quad KM \cong K \otimes_{\mathbb{Q}} QM, \quad FL \cong F \otimes_{\mathbb{Q}} QL \text{ e } FM \cong F \otimes_{\mathbb{Q}} QM,$$

obtemos

$$m_K(L) = m_{\mathbb{Q}}(L) = m_F(L) \quad \text{e} \quad m_K(M) = m_{\mathbb{Q}}(M) = m_F(M) .$$

Como $\mathbf{F}L \cong \mathbf{F}M$, concluímos que $m_{\mathbf{F}}(L) = m_{\mathbf{F}}(M)$. Portanto $m_{\mathbf{K}}(L) = m_{\mathbf{K}}(M)$, o que nos permite concluir que $\Delta_{\mathbf{K}}(L : L') \cong \Delta_{\mathbf{K}}(M : M')$.

Assim $\mathbf{K}L \cong \mathbf{K}M$ e, portanto, $\mathbf{F}$ e $\mathbf{K}$ são equivalentes em $\mathcal{L}_2$. $\square$

No capítulo 2, mostramos que $\mathbf{Q}$ determina a classe dos R.A. loops finitos do tipo II, em particular, a classe $\mathcal{L}_2$ dos R.A. 2-loops finitos do tipo II. Em presença do teorema 3.3.1, podemos enunciar o seguinte

Corolário 3.3.2

Um corpo $\mathbf{K}$ determina a classe dos R.A. 2-loops finitos do tipo II se e somente se

$$O(\mathbf{K}) = 0, \text{ ind}_2(\mathbf{K}) = 1 \text{ e } c(\mathbf{K}) = 0.$$

Demonstração: Basta observar $O(\mathbf{Q}) = 0, \text{ ind}_2(\mathbf{Q}) = 1$ e $c(\mathbf{Q}) = 0$. $\square$

Se $c(\mathbf{K}) = 0$ então $\text{car}\mathbf{K} = 0$. Nesse caso podemos supor $\mathbf{Q} \subset \mathbf{K}$ e a proposição 3.1.3 de E. Spiegel pode ser ampliada para

Proposição 3.3.3 *Seja $\mathbf{K}$ um corpo com $c(\mathbf{K}) = 0$. As seguintes condições são equivalentes:*

- (i) $\mathbf{K}$ determina a classe dos R.A. 2-loops finitos do tipo II.
- (ii) $\mathbf{K}$ determina a classe dos 2-grupos abelianos finitos.
- (iii) $\mathbf{K}$ determina a família de 2-grupos $\Omega = \{C_8 \times C_2, C_4 \times C_4, C_4 \times C_2 \times C_2\}$.
- (iv) $\mathbf{K} \cap \{\sqrt{2}, \sqrt{-2}, \sqrt{-1}\} = \emptyset$.

Para obtermos um resultado geral, vamos primeiramente estudar os R.A. loops do tipo I.

Começamos com o seguinte

Lema 3.3.4 *Sejam F e K corpos de característica diferente de 2 tais que $\text{ind}_2(F) = \text{ind}_2(K)$ e $O(F) = O(K)$. Então $\text{ind}_2(F(\xi_{2^a})) = \text{ind}_2(K(\xi_{2^a}))$ e $O(F(\xi_{2^a})) = O(K(\xi_{2^a}))$ para todo inteiro $a \geq 1$.*

Demonstração: Se $a = 1$ nada há para se provar. Suponhamos $a > 1$ e que $\text{ind}_2(F) = \text{ind}_2(K) = n$.

De $\text{ind}_2(F) = n$, concluímos que $F(\xi_{2^{n+2}}) \neq F(\xi_{2^{n+1}}) = F(\xi_{2^n})$, o que equivale a dizer que $\xi_{2^{n+1}} \in F(\xi_{2^{n+1}})$ mas $\xi_{2^{n+2}} \notin F(\xi_{2^{n+1}})$.

Suponhamos que $a \leq n + 1$. Claramente $\text{ind}_2(F(\xi_{2^a})) = \text{ind}_2(F)$ e, da mesma forma, $\text{ind}_2(K(\xi_{2^a})) = \text{ind}_2(K)$.

Se $a > n+1$, temos que $\xi_{2^a} \in F(\xi_{2^a})$ mas $\xi_{2^{a+1}} \notin F(\xi_{2^a})$. Logo $\text{ind}_2(F(\xi_{2^a})) = a - 1$. Da mesma forma $\text{ind}_2(K(\xi_{2^a})) = a - 1$.

Em ambos os casos, concluímos que $\text{ind}_2(F(\xi_{2^a})) = \text{ind}_2(K(\xi_{2^a}))$.

A outra igualdade segue do fato de que, como $a > 1$, tem-se $O(F(\xi_{2^a})) = O(K(\xi_{2^a})) = 1$. $\square$

Podemos então enunciar

Teorema 3.3.5 *Sejam os corpos F e K de característica diferente de 2. Seja $\mathcal{L}_1$ a classe dos R.A. 2-loops finitos do tipo I. Então F é equivalente a K em $\mathcal{L}_1$ se e*

somente se valem as seguintes condições:

$$(a) O(\mathbf{F}) = O(\mathbf{K})$$

$$(b) \text{ind}_2(\mathbf{F}) = \text{ind}_2(\mathbf{K}).$$

Demonstração: Suponhamos que $\mathbf{F}$ e $\mathbf{K}$ são equivalentes em $\mathcal{L}_1$. Vamos provar que $\mathbf{F}$ e $\mathbf{K}$ são equivalentes na classe dos 2-grupos abelianos finitos.

Sejam A e B 2-grupos abelianos finitos e suponhamos que $\mathbf{F}A \cong \mathbf{F}B$. Seja I um R.A. loop indecomponível tal que $Z(I) \cong C_4$ e $\frac{I}{I'} \cong C_2 \times C_2 \times C_2 \times C_2$ conforme a Tabela 2.3.1, e consideremos os R.A. loops $L = I \times A$ e $M = I \times B$. Então $\mathbf{F}L \cong \mathbf{F}M$, o que implica $\mathbf{K}L \cong \mathbf{K}M$, e como no teorema 3.3.1 concluímos que $\mathbf{K}A \cong \mathbf{K}B$.

Portanto, $\mathbf{F}$ e $\mathbf{K}$ são equivalentes na classe dos 2-grupos abelianos finitos, e, pela proposição 3.1.1, valem (a) e (b).

Reciprocamente, suponhamos que valem as condições (a) e (b).

Sejam L e M loops em $\mathcal{L}_1$. Escrevamos

$$Z(L) \cong C_{2^{n_1}} \times C_{2^{n_2}} \times \dots \times C_{2^{n_t}}, \text{ onde } n_1 > 1, \ n_i \geq 0 \text{ para } i = 2, 3, \dots, t \text{ e}$$

$$Z(M) \cong C_{2^{m_1}} \times C_{2^{m_2}} \times \dots \times C_{2^{m_r}}, \text{ onde } m_1 > 1, \ m_i \geq 0 \text{ para } i = 2, 3, \dots, r$$

e assumamos que $L' \subset C_{2^{n_1}}$ e $M' \subset C_{2^{m_1}}$.

Suponhamos que $\mathbf{F}L \cong \mathbf{F}M$. Então

$$\mathbf{F} \left[\frac{L}{L'} \right] \cong \mathbf{F} \left[\frac{M}{M'} \right] \text{ e } \Delta_{\mathbf{F}}(L : L') \cong \Delta_{\mathbf{F}}(M : M') .$$

Pela proposição 3.1.1, as condições (a) e (b) implicam que

$K \left[\frac{L}{L'} \right] \cong K \left[\frac{M}{M'} \right]$. Só precisamos provar que $\Delta_K(L : L') \cong \Delta_K(M : M')$.

Pela proposição 3.2.1, sabemos que

$$Z(\Delta_K(L : L')) \cong \frac{2^{n_1-1}}{[K(\xi_{2^{n_1}}) : K]} \cdot K(\xi_{2^{n_1}})[C_{2^{n_2}} \times \dots \times C_{2^{n_t}}] \quad e$$

$$Z(\Delta_K(M : M')) \cong \frac{2^{m_1-1}}{[K(\xi_{2^{m_1}}) : K]} \cdot K(\xi_{2^{m_1}})[C_{2^{m_2}} \times \dots \times C_{2^{m_r}}] \quad .$$

Do mesmo modo, sabemos que

$$Z(\Delta_F(L : L')) \cong \frac{2^{n_1-1}}{[F(\xi_{2^{n_1}}) : F]} \cdot F(\xi_{2^{n_1}})[C_{2^{n_2}} \times \dots \times C_{2^{n_t}}] \quad e$$

$$Z(\Delta_F(M : M')) \cong \frac{2^{m_1-1}}{[F(\xi_{2^{m_1}}) : F]} \cdot F(\xi_{2^{m_1}})[C_{2^{m_2}} \times \dots \times C_{2^{m_r}}] \quad .$$

Chamando $\frac{2^{n_1-1}}{[F(\xi_{2^{n_1}}) : F]} = 2^a$ e $\frac{2^{m_1-1}}{[F(\xi_{2^{m_1}}) : F]} = 2^b$, temos

$$Z(\Delta_F(L : L')) \cong 2^a \cdot F(\xi_{2^{n_1}})[C_{2^{n_2}} \times \dots \times C_{2^{n_t}}] \cong F(\xi_{2^{n_1}})[\underbrace{C_2 \times \dots \times C_2}_{a \text{ vezes}} \times C_{2^{n_2}} \times C_{2^{n_t}}],$$

e, também

$$Z(\Delta_F(M : M')) \cong 2^b \cdot F(\xi_{2^{m_1}})[C_{2^{m_2}} \times \dots \times C_{2^{m_r}}] \cong F(\xi_{2^{m_1}})[\underbrace{C_2 \times \dots \times C_2}_{b \text{ vezes}} \times C_{2^{m_2}} \times C_{2^{m_t}}] \quad .$$

Como $Z(\Delta_F(L : L')) \cong Z(\Delta_F(M : M'))$, comparando ambos os lados obtemos $F(\xi_{2^{n_1}}) \cong F(\xi_{2^{m_1}})$. Portanto

$$F(\xi_{2^{n_1}})[\underbrace{C_2 \times \dots \times C_2}_{a \text{ vezes}} \times C_{2^{n_2}} \times C_{2^{n_t}}] \cong F(\xi_{2^{n_1}})[\underbrace{C_2 \times \dots \times C_2}_{b \text{ vezes}} \times C_{2^{m_2}} \times C_{2^{m_t}}] \quad .$$

Pelo lema 3.3.4, sabemos que $O(F(\xi_{2^{n_1}})) = O(K(\xi_{2^{n_1}}))$ e $\text{ind}_2(F(\xi_{2^{n_1}})) = \text{ind}_2(K(\xi_{2^{n_1}}))$. Então $F(\xi_{2^{n_1}})$ e $K(\xi_{2^{n_1}})$ são equivalentes na classe dos 2-grupos abelianos. Assim, pela proposição 3.1.1, temos que

$$K(\xi_{2^{n_1}})[\underbrace{C_2 \times \dots \times C_2}_{a \text{ vezes}} \times C_{2^{n_2}} \times C_{2^{n_t}}] \cong K(\xi_{2^{n_1}})[\underbrace{C_2 \times \dots \times C_2}_{b \text{ vezes}} \times C_{2^{m_2}} \times C_{2^{m_t}}] \quad .$$

De $O(F) = O(K)$, $\text{ind}_2(F) = \text{ind}_2(K)$ e $F(\xi_{2^{n_1}}) = F(\xi_{2^{m_1}})$, concluímos que também $K(\xi_{2^{n_1}}) = K(\xi_{2^{m_1}})$ e $[F(\xi_{2^{n_1}}) : F] = [K(\xi_{2^{n_1}}) : K]$.

Portanto vale

$$K(\xi_{2^{n_1}})[\underbrace{C_2 \times \dots \times C_2}_{a \text{ vezes}} \times C_{2^{n_2}} \times C_{2^{n_t}}] \cong K(\xi_{2^{m_1}})[\underbrace{C_2 \times \dots \times C_2}_{b \text{ vezes}} \times C_{2^{m_2}} \times C_{2^{m_t}}] \quad ,$$

isto é,

$$2^a \cdot K(\xi_{2^{n_1}})[C_{2^{n_2}} \times \dots \times C_{2^{n_t}}] \cong 2^b \cdot K(\xi_{2^{m_1}})[C_{2^{m_2}} \times \dots \times C_{2^{m_r}}],$$

ou

$$\frac{2^{n_1-1}}{[K(\xi_{2^{n_1}}) : K]} \cdot K(\xi_{2^{n_1}})[C_{2^{n_2}} \times \dots \times C_{2^{n_t}}] \cong \frac{2^{m_1-1}}{[K(\xi_{2^{m_1}}) : K]} \cdot K(\xi_{2^{m_1}})[C_{2^{m_2}} \times \dots \times C_{2^{m_r}}].$$

Assim $Z(\Delta_K(L : L')) \cong Z_K(\Delta(M : M')) \cong \bigoplus_{i=1}^q K_i$, onde $K_i \cong K(\xi_{2^{d_i}})$ para algum $d_i \geq 0$.

$$\text{Escrevamos } \Delta_K(L : L') \cong \bigoplus_{i=1}^q \mathcal{C}_i(K_i) \text{ e } \Delta_K(M : M') \cong \bigoplus_{i=1}^q \mathcal{D}_i(K_i).$$

Como $n_1 > 1$ e $m_1 > 1$, todas as álgebras $\mathcal{C}_i(K_i)$ e $\mathcal{D}_i(K_i)$ são “split”, e, concluímos que $\mathcal{C}_i(K_i) \cong \mathcal{D}_i(K_i)$. Logo $\Delta_K(L : L') \cong \Delta_K(M : M')$.

Portanto $KL \cong KM$, isto é, K é equivalente a F em $\mathcal{L}_1$. $\square$

Dessa forma, o teorema 2.1.2, de G. Leal e C. Polcino Milies pode ser generalizado para:

Teorema 3.3.6

Seja $\mathbf{K}$ um corpo tal que $O(\mathbf{K}) = 0$ e $\text{ind}_2(\mathbf{K}) = 1$. Seja L um R.A. 2-loop e suponhamos que exista um elemento central α tal $\alpha^2 = e \in L'$. Seja M outro R.A. loop. Então

$$\mathbf{KL} \cong \mathbf{KM} \quad \text{se e somente se} \quad \begin{cases} \frac{L}{L'} \cong \frac{M}{M'} \\ Z(\mathbf{KL}) \cong Z(\mathbf{KM}) \end{cases}.$$

Demonstração: Basta verificar que o corpo $\mathbf{K}$ é equivalente a $\mathbf{Q}$ na classe dos R.A. 2-loops finitos do tipo I. $\square$

No caso geral para os R.A. 2-loops finitos, obtemos então o seguinte resultado

Teorema 3.3.7 *Sejam os corpos $\mathbf{F}$ e $\mathbf{K}$ corpos de característica diferente de 2. Seja $\mathcal{L}$ a classe dos R.A. 2-loops finitos. Então $\mathbf{F}$ é equivalente a $\mathbf{K}$ em $\mathcal{L}$ se e somente se as seguintes condições se verificam:*

- (a) $O(\mathbf{F}) = O(\mathbf{K})$
- (b) $\text{ind}_2(\mathbf{F}) = \text{ind}_2(\mathbf{K})$
- (c) $c(\mathbf{F}) = c(\mathbf{K})$

Demonstração: Se $\mathbf{F}$ é equivalente a $\mathbf{K}$ em $\mathcal{L}$, como no teorema 3.3.1, se demonstra que valem (a), (b) e (c).

Reciprocamente, suponhamos que valem (a), (b) e (c). Sejam L e M dois R.A. loops em $\mathcal{L}$, suponhamos que $\mathbf{FL} \cong \mathbf{FM}$ e vamos provar que $\mathbf{KL} \cong \mathbf{KM}$.

Escrevamos

$$Z(L) \cong C_{2^{n_1}} \times C_{2^{n_2}} \times \dots \times C_{2^{n_t}}, \quad \text{onde } n_1 \geq 1, \quad n_i \geq 0 \text{ para } i = 2, 3, \dots, t \text{ e}$$

$Z(M) \cong C_{2^{m_1}} \times C_{2^{m_2}} \times \dots \times C_{2^{m_r}}$, onde $m_1 \geq 1$, $m_i \geq 0$ para $i = 2, 3, \dots, r$ e assumamos que $L' \subset C_{2^{n_1}}$ e $M' \subset C_{2^{m_1}}$.

Do isomorfismo $\mathbf{F}L \cong \mathbf{F}M$ e das condições (a), (b) e (c), exatamente como no teorema 3.3.5, concluimos que

- i) $\mathbf{K} \left[\frac{L}{L'} \right] \cong \mathbf{K} \left[\frac{M}{M'} \right]$
- ii) $\mathbf{K}(\xi_{2^{n_1}}) = \mathbf{K}(\xi_{2^{m_1}})$
- iii) $Z(\Delta_{\mathbf{K}}(L : L')) \cong Z_{\mathbf{K}}(\Delta(M : M')) \cong \bigoplus_{i=1}^q \mathbf{K}_i$, onde $\mathbf{K}_i \cong \mathbf{K}(\xi_{2^{d_i}})$ para algum $d_i \geq 0$.

Falta mostrar que $\Delta_{\mathbf{K}}(L : L') \cong \Delta_{\mathbf{K}}(M : M')$.

Escrevamos $\Delta_{\mathbf{K}}(L : L') \cong \bigoplus_{i=1}^q \mathcal{C}_i(\mathbf{K}_i)$ e $\Delta_{\mathbf{K}}(M : M') \cong \bigoplus_{i=1}^q \mathcal{D}_i(\mathbf{K}_i)$.

Se $n_1 = m_1 = 1$, usando a condição (c), a demonstração é idêntica à demonstração do teorema 3.3.1.

Se $n_1 > 1$ e $m_1 > 1$, a demonstração é idêntica à demonstração do teorema 3.3.5.

Se $n_1 = 1$ e $m_1 > 1$ (ou vice-versa), então $\mathbf{K} = \mathbf{K}(\xi_{2^{n_1}}) = \mathbf{K}(\xi_{2^{m_1}})$ e, assim, $\mathbf{K}$ é um corpo que contém raízes da unidade. Logo todas as álgebras $\mathcal{C}_i(\mathbf{K}_i)$ e $\mathcal{D}_i(\mathbf{K}_i)$ são “split”. Dessa forma podemos concluir que $\mathcal{C}_i(\mathbf{K}_i) \cong \mathcal{D}_i(\mathbf{K}_i)$, $i = 1, \dots, q$, o que implica $\Delta_{\mathbf{K}}(L : L') \cong \Delta_{\mathbf{K}}(M : M')$.

Assim, $\mathbf{K}L \cong \mathbf{K}M$, e $\mathbf{K}$ e $\mathbf{F}$ são equivalentes em $\mathcal{L}$. □

Bibliografia

- [1] R. H. Bruck, *A Survey of Binary Systems*, *Ergeb. der Math. u. ihrer Grenz.*, **30**, Springer-Verlag (Berlin) (1958).
- [2] R. H. Bruck, *What is a Loop?*, *Studies In Modern Algebra* vol. 2, The Math. Assoc. of America, (1963) 59-99.
- [3] O. Chein, *Moufang Loops of Small Order, I*, *Trans. Amer. Math. Soc.* **188**, (1974) 31-51.
- [4] O. Chein, *Moufang Loops of Small Order, II*, *Memoirs Amer. Math. Soc.* **197 (13)**, (1978).
- [5] O. Chein and Edgar G. Goodaire, *Loops whose Loop Rings are Alternative*, *Comm. in Algebra*, **14**, (1986) 293-310.
- [6] D. B. Coleman, *Finite Groups with Isomorphic Group Algebras*, *Trans. Amer. Math. Soc.*, **105**, (1962) 1-8.
- [7] W. E. Deskins, *Finite Abelian Groups with Isomorphic Group Algebras*, *Duke Math. J.* **23**, (1956) 35-40.
- [8] B. Felzenszwald, *Álgebras de Dimensão Finitas*, IMPA (1979).
- [9] E.G. Goodaire, *Alternative Loop Rings*, *Publ. Math. Debrecen*, **30**, (1983) 31-38.

- [10] E. G. Goodaire, *R.A. Loops*, Notas de aula, (1986).
- [11] E.G. Goodaire and M.M. Parmenter, *Semi-simplicity of Alternative Loop Rings*, *Acta Math. Hung.*, 50(3-4), (1987) 241-247.
- [12] E.G. Goodaire and C. Polcino Milies, *Isomorphisms of Integral Alternative Loop Rings*, *Rend. Circolo Mat. Palermo,II*, 37, (1988) 126-135.
- [13] G. Higman, *The Units of Group Rings*, *Proc. London Math. Soc.* 46, (1940), 231-248.
- [14] E. Jespers, G. Leal and C. Polcino Milies, *Indecomposable R.A. loops*, preprint.
- [15] G. Leal and C. Polcino Milies, *Isomorphic Group (and Loop) Algebras*, *J. Algebra* (to appear).
- [16] R. Moufang, *Zur Struktur von Alternativkorper*, *Math. Ann.*, 110, (1935) 416 - 430.
- [17] S. Perlis and G. L. Walker, *Abelian Group Algebras of Finite Order*, *Trans. Amer. Math. Soc.*, 68, (1950) 420-426.
- [18] R. Sandling, *The Isomorphism Problem for Group Rings: a Survey*, *Lectures Notes in Mathematics vol. 1142 Orders and their Applications*, Springer-Verlag, Berlin, (1985)
- [19] R. D. Schafer, *Introduction to non-associative Algebras*, Wiley, Interscience, New York.
- [20] K. C. Smith, *A Characterization of Quaternion Division Algebras*, *Rocky Mountain J. Math.*, 9 (2), (1979) 371-375.
- [21] E. Spiegel, *On Isomorphisms of Abelian Group Algebras*, *Canadian J. Math.*, 27, (1975) 155-161.

- [22] E. Spiegel and A. Trojan, *On Semi-Simple Group Algebras I*, **Pacific J. Math.**, **59**,(1975) 549-555.
- [23] E. Spiegel and A. Trojan, *On Semi-simple Group Algebras II*, **Pacific J. Math.**, **66**(2), (1976) 553-559.
- [24] A.D. Thomas and G.V. Wood, *Group Tables*, Shiva Publ., (1980).
- [25] K.A. Zhevlakov, A.M. Slinko, I.P. Shestakov, A.I. Shirshov, *Rings that are nearly Associative*, Ac. Press, New York (1982).