ALTERNATIVE ALGEBRAS AND RA LOOPS

YONGXIN ZHOU

INFORMATION TO USERS

This manuscript has been reproduced from the microfilm master. UMI films the text directly from the original or copy submitted. Thus, some thesis and dissertation copies are in typewriter face, while others may be from any type of computer printer.

The quality of this reproduction is dependent upon the quality of the copy submitted. Broken or indistinct print, colored or poor quality illustrations and photographs, print bleedthrough, substandard margins, and improper alignment can adversely affect reproduction.

In the unlikely event that the author did not send UMI a complete manuscript and there are missing pages, these will be noted. Also, if unauthorized copyright material had to be removed, a note will indicate the deletion.

Oversize materials (e.g., maps, drawings, charts) are reproduced by sectioning the original, beginning at the upper left-hand corner and continuing from left to right in equal sections with small overlaps.

Photographs included in the original manuscript have been reproduced xerographically in this copy. Higher quality 6" x 9" black and white photographic prints are available for any photographs or illustrations appearing in this copy for an additional charge. Contact UMI directly to order.

Bell & Howell Information and Learning
300 North Zeeb Road, Ann Arbor, MI 48106-1346 USA

UMI®
800-521-0600

Alternative Algebras and RA Loops

by

©Yongxin Zhou

A thesis submitted to the
School of Graduate Studies
in partial fulfillment of the
requirements for the degree of
Doctor of Philosophy

Department of Mathematics and Statistics
Memorial University of Newfoundland

September 1998

St. John's Newfoundland Canada

Abstract

In the first part of this thesis, we study the relationships between three algebra structures: Cayley-Dickson algebras, RA loops and alternative loop algebras.

Let R be a commutative associative ring with 1 and let A be an R-algebra with unity of characteristic different from 2. For any α, β and $\gamma \in A$, let $A(\alpha, \beta, \gamma)$ be the Cayley-Dickson algebra. We construct an RA loop L from each Cayley-Dickson algebra $A(\alpha, \beta, \gamma)$, called the induced RA loop. We show that any RA loop is a homomorphic image of some induced RA loop. After introducing the category of Cayley-Dickson algebras and the category of RA loops, we show that the two categories are equivalent.

Using the induced RA loops, we show that any Cayley-Dickson algebra is a homomorphic image of an alternative loop algebra. Thus we give a new way of representing a Cayley-Dickson algebra. Furthermore, the homomorphism commutes with the norm and trace operations of the alternative loop algebra and the Cayley-Dickson algebra. The kernel of this homomorphism is completely determined. The prime radical and Jacobson radical of some Cayley-Dickson algebras are determined. A result of de Barros is generalized. The more general form of the homomorphism is studied.

Necessary and sufficient conditions for an RA loop to be the Moufang circle loop of a quasiregular alternative algebra are given. The algebra structure of a finite alternative nilpotent ring with the Moufang circle loop being an RA loop is completely determined.

In the second part of this thesis, the alternative rings of order p^4 and p^5 are completely determined, where p is a prime. This generalizes a result of A. T. Gainov. The two smallest alternative rings have order 2^4. For each prime number, there are fifteen alternative rings of order p^n, $n \leq 5$. The relationships between these

fifteen rings are described. From these alternative algebras, a class of group-graded alternative algebras is derived.

Acknowledgments

I am deeply indebted to my supervisor, Dr. Edgar G. Goodaire, without whose encouragement, advice, assistance and financial support this thesis could not have been completed. He has been very generous with his ideas and time. His *RA* loop and alternative loop ring theory provides resourceful knowledge for the present thesis. I also thank him for his very kind concern about my life in these three years.

I am grateful to Drs C. Lee and R. Charron, the other members of my supervisory committee.

I would like to acknowledge the Department of Mathematics and Statistics in general and Drs. B. Watson and H. Gaskill, the past and present Department Heads, in particular for providing me with a friendly atmosphere and the necessary facilities to complete my programme.

I would like to thank Drs. M. M. Parmenter and E. Jespers for their instructions in the algebra seminar and concerning the thesis. I am grateful to Dr. E. Jespers for his financial support.

I sincerely thank my first algebra teacher Professor Yuansen Zhu.

Thanks are also due to Drs Yiqiang Zhou, Yuanlin Li and Mr. Qiang Wang for their suggestions and comments.

I am grateful to the School of Graduate Studies and the Department of Mathematics and Statistics for financial support in the form of Graduate Fellowships and Teaching Assistantships.

Finally, I would like to sincerely thank my wife, Xianghong and my daughter, Lily, for their understanding and support.

Contents

Abstract iii

Acknowledgments v

List of Figures ix

Introduction 1

Chapter I. Cayley-Dickson algebras and RA loops 9
1. Introduction 9
2. Generalized Cayley-Dickson algebras 9
3. Cayley-Dickson algebras and their induced RA loops 12
4. Induced RA loops and other RA loops 17
5. Moufang circle loops and RA loops 20
6. The categories of RA loops and Cayley-Dickson algebras 22

Chapter II. Cayley-Dickson algebras and alternative loop algebras 29
1. Induced alternative loop algebras 29
2. A further description of $\ker(f)$ 36
3. Cayley-Dickson algebras, loop algebras and their radicals 39
4. Quaternion algebras and RA groups 42

Chapter III. Moufang circle loops and loop algebras 45
1. Moufang circle loops and loop algebras 45
2. The augmentation ideal of the loop algebra of an RA loop 48
3. Moufang circle loops and RA circle loops 50

Chapter IV. RA circle loops 57

1. Introduction and some definitions 57
2. Necessary conditions for an RA loop to be a circle loop 58
3. A restriction on the RA circle loop 70

Chapter V. Alternative rings and Peirce decomposition 73
1. Alternative rings and their matrix representations 73
2. More about Peirce decomposition 77
3. Peirce decomposition and group graded rings 79

Chapter VI. Alternative rings of small order 83
1. Introduction 83
2. Alternative rings of order p^n, $n \leq 4$ 83
3. Alternative rings of order p^5 90
4. Alternative rings of order p^5 with unity 91
5. Alternative rings of order p^5 possessing an idempotent $e \neq 1$ 96
6. The 12 rings of order p^5 111
7. The 12 rings of order 32 are distinct alternative rings 116
8. Right alternative rings which are not left alternative 117

Bibliography 119

List of Figures

I.1	Circle operation connects Cayley-Dickson algebras and RA loops	16
II.1	Cayley-Dickson algebras, RA loops and alternative loop algebras	36
IV.1	The structure of finite RA circle loops	65
VI.1	The fifteen alternative rings of order p^n, $n \leq 5$.	109
VI.2	The anti-isomorphism structure of the fifteen alternative rings of order p^n, $n \leq 5$.	110

Introduction

Let R be a commutative associative ring with unity. An R-algebra is an R-module with a multiplication satisfying the right and left distributive laws. An alternative R-algebra is an R-algebra A satisfying the following right and left alternative laws:

$$(yx)x = yx^2 \text{ and } x(xy) = x^2y,$$

for all $x, y \in A$. For general alternative algebra theory, we refer the reader to [**Sch66, ZSSS82**]. Any associative algebra is alternative. In addition to this, there are three well-known classes of alternative rings which are not associative, the Cayley-Dickson algebras, Zorn's vector matrix algebra and alternative loop algebras.

The first example of an alternative ring which is not associative is the Cayley numbers [**Cay45**]. In [**Dic19**], Dickson gave a construction of the Cayley numbers in a way analogous to the construction of the complex numbers from the reals. A. A. Albert [**Alb42**] called these Cayley-Dickson algebras. The construction of Cayley-Dickson algebras and the definition of Zorn's vector matrix algebras are described in [**GJM96**], a book which is primarily devoted to the algebra structure of loop algebras, our third class of alternative algebras.

A loop is a pair $(L, \circ)$ where L is a nonempty set and $(a, b) \mapsto a \circ b$ is a closed binary operation on L with the properties that the equation $a \circ b = c$ determines a unique element $b \in L$ for given $a, c \in L$ and a unique element $a \in L$ for given $b, c \in L$ and the binary operation has a two-sided identity element. A Moufang loop is a loop which satisfies one of the following equivalent identities:

$$((xy)x)z = x(y(xz)),\ ((xy)z)y = x(y(zy)).$$

From the definition, we see that a group is a Moufang loop. But in this thesis, a Moufang loop is a loop which is not associative. For the theory of loops, we recommend [**Bru58, Pfl90, CPe90**], and for the theory and structure of Moufang loops, [**Che74, Che78, GKM**].

For a loop L, one can define the loop algebra RL in exactly the way that the group algebra is defined: addition component-wise and multiplication the extension of multiplication in L via the distributive laws. Alternative loop algebras in characteristic different from two were discovered in the 1980s by Goodaire [**Goo83**]. Since then, this research area has grown rapidly and many research papers have been published [**CG85, CG86, GP86, GP87, CG88, CG90, LM93, GR95, GJM96, GM96**]. The most important reference is the comprehensive book by Goodaire, Jespers and Milies [**GJM96**], which is the main reference for the present thesis. For the theory of group algebras, we refer the reader to [**Pas77, Seh78, Seh93, Kar83**] and the nice paper [**Con63**].

In the theory of alternative loop algebras, the RA loop plays an important role and it is one of the main topics of this thesis. So we recall the definition here. Let G be any group which is an extension of its center $\mathcal{Z}$ by $C_2 \times C_2$. It is easy to see that the commutator subgroup G' of such a group is cyclic of order 2; write $G' = \{1, s\}$. For $g \in G$, define

$$g^* = \begin{cases} g & \text{if } g \in \mathcal{Z} \\ sg & \text{otherwise} \end{cases}$$

Let u be an indeterminate, g_0 an element of $\mathcal{Z}$ and $L = G \cup Gu$. Define multiplication in L by

$$g(hu) = (hg)u$$
$$(gu)h = (gh^*)u$$
$$(gu)(hu) = g_0 h^* g$$

where $g, h \in G$. Then L is a Moufang loop and, over any ring R of characteristic different from 2, the loop algebra RL is alternative, but not associative. We call this loop L an *RA loop*, meaning *ring alternative loop*. For convenience, we call the group G an *RA group* due to its role in constructing the RA loop. E. G. Goodaire [**Goo83**, Theorem 4] showed if L is a loop, and the loop algebra RL is an alternative but not

associative algebra, then the loop L is an RA loop. So it is of the above form, denoted by $M(G, *, g_0)$. By [**Goo83**, Theorem 4], we can rewrite the RA loop $L = M(G, *, g_0)$ in the form

$$L = (\mathcal{Z}\langle a\rangle\langle b\rangle)\langle u\rangle,$$

where a, b and u are three elements of L which do not associate. This form will be used in this thesis.

The smallest RA loops are of order 16 and there are two such loops. One of them is the Cayley loop $M(Q_8, -1, -1)$ defined by the basis elements $\{\pm 1, \pm i, \pm j, \pm ij, \pm k, \pm ik, \pm jk, \pm ij \cdot k\}$ of the Cayley numbers whose products are specified in the following table:

$\cdot$	1	i	j	ij	k	ik	jk	$ij \cdot k$
1	1	i	j	j	k	ik	jk	$ij \cdot k$
i	i	-1	ij	$-j$	ik	$-k$	$-ij \cdot k$	jk
j	j	$-ij$	-1	i	jk	$ij \cdot k$	$-k$	$-ik$
ij	ij	j	$-i$	-1	$ij \cdot k$	$-jk$	ik	$-k$
k	k	$-ik$	$-jk$	$-ij \cdot k$	-1	i	j	k
ik	ik	k	$-ij \cdot k$	jk	$-i$	-1	$-ij$	j
jk	jk	$ij \cdot k$	k	$-ik$	$-j$	ij	-1	$-i$
$ij \cdot k$	$ij \cdot k$	$-jk$	ik	k	$-ij$	$-j$	i	-1

For more information about the structure and properties of the RA loops, see [**GJM96**].

The present thesis consists of two parts. The first part is composed of chapters I, II, III and IV, the second part chapters V and VI.

In the first part of the thesis we study the relationships between any two of the systems: Cayley-Dickson algebras, RA loops and alternative loop algebras. As mentioned above, a loop algebra of characteristic different from 2 is alternative if and only if the loop is an RA loop. So the relationships between Cayley-Dickson algebras and RA loops and alternative loop algebras become very interesting topics, which are the main concern of the first part of this thesis.

In chapter I, we study the relationships between Cayley-Dickson algebras and RA loops. First we generalize the notion of Cayley-Dickson algebras over a field to algebras over a commutative ring of characteristic different from 2. Then we

construct some RA loops from Cayley-Dickson algebras using the circle operation on the algebras.

This class of RA loops induced by the Cayley-Dickson algebras is very special, because we can show that RA loops are their homomorphic images. From this point of view, we can think that they cover all the RA loops.

To deeply investigate the relationships between RA loops and Cayley-Dickson algebras, particularly, the relationships between the loop homomorphisms and the Cayley-Dickson algebra homomorphisms, we study the category of Cayley-Dickson algebras and the category of RA loops, and show that the two categories are equivalent.

In chapter II, we study the relationships between Cayley-Dickson algebras and alternative loop algebras. From chapter I, we know that every Cayley-Dickson algebra induces some RA loop. By using this induced RA loop, we can construct an alternative loop algebra over the base algebra of the given Cayley-Dickson algebra. Then we get an interesting result: any Cayley-Dickson algebra is a quotient algebra of a loop algebra, by constructing a surjective map f from the loop algebra to the Cayley-Dickson algebra. Moreover, we show that this map sends the norm and the trace of the elements in the alternative loop algebra to those of the Cayley-Dickson algebra. From this point of view, alternative loop algebra theory is the representation theory of the Cayley-Dickson algebras, as well as the representation theory of RA loops.

To investigate Cayley-Dickson algebras from the well-developed alternative loop algebra theory, the structure of $\ker(f)$ is an important issue for us to study. In section 2 of the chapter, we give a description of the structure of the kernel. Then we study the structure of some Cayley-Dickson algebras and generalize a result of Luiz G. X. de Barros [**dB93b**]. In section 4, we state the corresponding results for quaternion algebras, without giving proofs.

We will see that the circle operation on the algebra plays an important role for us to bridge the three different algebra structures. Recall the definition of the circle operation on an algebra A:

$$x \circ y = xy + x + y,$$

for any two elements x and y in A. The most famous example of using the circle operation is the proof of the equivalence of the Boolean algebras (lattices) and Boolean rings (rings in which every element is an idempotent) [**Jac74**, Theorem 8.7]. The circle operation is also used in many papers, such as [**San74**], from which we borrow some ideas in constructing the map f used in chapter II.

In view of the interesting properties of the circle operation, it is worth investigating it in a more general way. This is the main topic of our next chapter, chapter III.

In 1987, E. G. Goodaire [**Goo87**] showed that the set of all quasi-regular elements of an alternative algebra A is a Moufang loop under the circle operation and called this loop the Moufang circle loop of A. From chapter I, we know that an RA loop can be the Moufang circle loop of an alternative algebra and the Moufang circle loop of any Cayley-Dickson algebra contains an RA subloop. So it is interesting to investigate the relationships between the alternative algebra, its Moufang circle loop and the loop algebra of the circle loop. Note that, generally speaking, this loop algebra is no longer alternative. This idea is also a generalization of R. Sandling's idea in [**San74**], which dealt with the circle group and its integral group ring. Then we apply the general result to alternative algebras whose Moufang circle loop contains an RA subloop. Note that Cayley-Dickson algebras are algebras of this type.

In chapter IV, we investigate a special Moufang circle loop and its alternative algebra: the alternative algebra is quasiregular and its Moufang circle loop is exactly an RA loop. This problem is triggered by the following observation.

From the structure theorem of RA loops [**GJM96**, Theorem IV.3.1] we know that an RA loop is a kind of loop extension of an RA group, which is a kind of nilpotent group of class 2. There is a nice result that all nilpotent groups of class 2 are circle groups of some nilpotent rings of nilpotent index 3 [**AW73, Kum94**]. Groups which are circle groups of some nilpotent rings have some nice properties and have been much investigated, for example, see [**TH83, Roh82, Roh90, Bov96**].

Since all our RA loops are nilpotent loops of class 2, it is natural to ask whether these RA loops are the Moufang circle loops of nilpotent (or quasi-regular) alternative rings. Note that all nilpotent rings of nilpotency index 3 are associative rings, so the old way of constructing a nilpotent ring from a nilpotent group used in [**AW73, Kum94**] does not apply to the RA loop case. Making the problem more complicated,

a result of E. G. Goodaire [**Goo**] shows that there are no nilpotent alternative rings of order less than or equal to 64 that have circle RA loops as their Moufang circle loops and the proof heavily depends on the order. Therefore, to determine whether there is an RA circle loop or not appears to be quite difficult and this question is still open.

In chapter IV, we study the problem by investigating the conditions for an RA loop to be a Moufang circle loop of an alternative Jacobson radical algebra. We find necessary and sufficient conditions for an RA loop to be an RA circle loop. Finally we describe the structure that finite RA circle loops and their nilpotent alternative algebras must have. We still hope that an RA loop with some large order will turn out to be an RA circle loop.

The second part of this thesis is composed of chapter V and chapter VI. The main topic of this part is to find all alternative algebras of small order which are not associative. This problem is triggered by the problem of finding an RA circle loop, which is the main topic of chapter IV. To do this, we find that we must know some examples of alternative rings of small order. For other algebra systems, such as groups [**TW80**], Moufang loops [**CP71, Che74, Che78, GKM**], commutative Moufang loops [**KP81**], RA loops [**JLM95, GJM96**], Bol loops [**GM**], associative rings [**KP69, McD74**] and Lie algebras [**Mor58**], the results are well known. For alternative rings, there are few general results. M. I. Badalov [**Bad84**] described all nilpotent alternative algebras of dimension 6 over a field and showed that all the nilpotent alternative algebras of dimension ≤ 5 are associative. E. G. Goodaire[**Goo87, GZa**] showed that all the alternative nilpotent rings of orders p^4 and p^5 are associative. In this work, we find all alternative rings of order p^n, $n \leq 5$, and all alternative algebras of dimension at most 5 over a field. This generalizes the work of A. T. Gainov[**Gai63**].

In chapter V, we do some preparation for the next chapter, but this is also interesting for its own sake. In the first section of this chapter, we give a matrix representation of the finite alternative algebras. In this way, we can easily check whether a ring is alternative or not. Then we recall the Peirce decomposition of an alternative ring and develop an interesting lemma which is used widely in the next chapter to remove cases that yield only associative algebras. In the last section, we show that the Peirce decomposition can induce some group-graded algebras which are alternative, but the

interesting thing is that the base algebras are associative. Many of the alternative algebras we find in the next chapter have this property. Note that lots of research has been done on group-graded and semigroup-graded algebras after the two fundamental papers [**Dad80**] and [**CM84**], but rarely has something been done about alternative algebras which are graded by a group.

In chapter VI, we use the results of chapter V to determine alternative algebras of small order. None of the alternative algebras we found belongs to the known classes of alternative algebras: alternative loop algebras and Cayley-Dickson algebras. Combining with M. I. Badalov and E. G. Goodaire's results we determine all the finite alternative algebras of order p^4 and p^5. Moreover, from the multiplication tables of these alternative algebras, we can construct all the alternative algebras of dimensions 4 and 5 over any field. Furthermore, the relationships between all these algebras are described. An interesting observation about these relationships is that, for each prime p, all the alternative algebras of order p^4 and p^5 are derived from one smallest alternative algebra of order p^4, either by anti-isomorphism, adding a unity, or some other kind of algebra extension.

CHAPTER I

Cayley-Dickson algebras and RA loops

1. Introduction

In the first section of this chapter, we generalize the notion of the Cayley-Dickson algebra from an algebra over a field to an algebra over a commutative ring. After constructing RA loops from Cayley-Dickson algebras by using the circle operation, we prove that RA loops are homomorphic images of some induced RA loops. Then, examples of a Cayley-Dickson algebra whose Moufang circle loop is an RA loop are given. In the last section, we introduce two concepts: the category of Cayley-Dickson algebras and the category of RA loops by using the induced RA loops, and show that the two categories are equivalent[**GZb**].

2. Generalized Cayley-Dickson algebras

The term "generalized Cayley-Dickson algebra" has been used by many authors, but with two different meanings. One is to follow the Cayley-Dickson process to generate some alternative algebras by choosing different α, β and γ [**GJM96**]. The other is to follow the Cayley-Dickson process's three steps to go further to get some general algebras which are not alternative [**Bro67**]. For more information about Cayley numbers and Cayley-Dickson algebras, we refer the reader to [**Cur63, Kle63**].

The following theorem describes a general version of the standard Cayley-Dickson process [**Sch66**][**GJM96**, Proposition 3.1].

THEOREM I.1. *Let A be a ring with 1 and with an involution $a \mapsto \overline{a}$, for any $a \in A$, such that $a + \overline{a} \in \mathcal{Z}(A)$, the center of A, and $a\overline{a} = \overline{a}a \in \mathcal{Z}(A)$ for all $a \in A$. For any $\alpha \in \mathcal{Z}(A)$, we can define a new ring $B = A(\alpha)$ by defining addition component-wise and multiplication*

$$(a + b\ell)(c + d\ell) = (ac + \alpha\overline{d}b) + (da + b\overline{c})\ell.$$

Here ℓ is an indeterminate. Then B is an alternative ring if and only if A is associative.

If A is associative, then B has an involution defined by

$$\overline{a+b\ell} = \overline{a} - b\ell.$$

For any $x \in B$, $x+\overline{x} \in \mathcal{Z}(A)$ and $x\overline{x} = \overline{x}x \in \mathcal{Z}(A)$.

PROOF. This can be checked in the standard way. We give a brief proof here for the sake of completeness.

It is easy to see that B is a ring. For any two elements $x = a + b\ell$ and $y = c + d\ell$, we have

$$x^2y = a^2c + \alpha\overline{b}b \cdot c + \alpha\overline{d} \cdot ba + \alpha\overline{d} \cdot b\overline{a} + (da^2 + \alpha d \cdot \overline{b}b + ba \cdot \overline{c} + b\overline{a} \cdot \overline{c})\ell,$$

and

$$x(xy) = a \cdot ac + \alpha a \cdot \overline{d}b + \alpha\overline{a}\overline{d} \cdot b + \alpha c\overline{b} \cdot b + (da \cdot a + b\overline{c} \cdot a + b \cdot \overline{c}\overline{a} + \alpha b \cdot \overline{b}d)\ell.$$

Then

$$\begin{aligned}
[x,x,y] &= x^2y - x(xy) \\
&= (a^2c - a \cdot ac) + (\alpha\overline{b}b \cdot c - \alpha c\overline{b} \cdot b) + (\alpha\overline{d} \cdot ba + \alpha\overline{d} \cdot b\overline{a} - \alpha a \cdot \overline{d}b - \alpha\overline{a}\overline{d} \cdot b) \\
&+ (da^2 - da \cdot a)\ell + (\alpha d \cdot \overline{b}b - \alpha b \cdot \overline{b}d)\ell + (ba \cdot \overline{c} + b\overline{a} \cdot \overline{c} - b\overline{c} \cdot a - b \cdot \overline{c}\,\overline{a})\ell \\
&= ([a,a,c] + \alpha[c,b,b] - \alpha[a,d,b]) + ([d,a,a] + [b,c,a] - \alpha[b,b,d])\ell.
\end{aligned}$$

To obtain this, we use repeatedly that $a + \overline{a} \in \mathcal{Z}(A)$ and $a\overline{a} = \overline{a}a \in \mathcal{Z}(A)$, so that, for example

$$\begin{aligned}
\overline{d} \cdot ba + \overline{d} \cdot b\overline{a} - a \cdot \overline{d}b - \overline{a}\overline{d} \cdot b &= \overline{d} \cdot b(a + \overline{a}) - a \cdot \overline{d}b - \overline{a}\overline{d} \cdot b \\
&= (a + \overline{a}) \cdot \overline{d}b - a \cdot \overline{d}b - \overline{a}\overline{d} \cdot b \\
&= a \cdot \overline{d}b - a \cdot \overline{d}b + \overline{a} \cdot \overline{d}b - \overline{a}\overline{d} \cdot b \\
&= -[\overline{a}, \overline{d}, b] \\
&= -[(a + \overline{a}) - a, (d + \overline{d}) - d, b] \\
&= -[-a, -d, b] \\
&= -[a, d, b].
\end{aligned}$$

Now suppose that B is an alternative ring. Then so is A and

$$0 = [x, x, y] = -\alpha[a, d, b] + [b, c, a]\ell$$

for all a, b, c, $d \in A$. It follows that B is associative. On the other hand, associativity of A clearly implies that $[x, x, y] = 0$.

So B is left alternative if and only if A is associative. Similarly, B is right alternative if and only if A is associative. The statements hold. As for the involution, it is not hard to check. □

THEOREM I.2. *(The Generalized Cayley-Dickson Algebra) Let A be a commutative associative ring with 1 and $2 \neq 0$ in A. Let α, β and γ be in $U(A)$, the unit group A. Then the free A-module with basis 1, i, j, ij, k, ij, ik, jk, $ij \cdot k$ is a Cayley-Dickson algebra $A(\alpha, \beta, \gamma)$ with multiplication defined by*

$\cdot$	1	i	j	ij	k	ik	jk	$ij \cdot k$
1	1	i	j	j	k	ik	jk	$ij \cdot k$
i	i	α	ij	αj	ik	αk	$-ij \cdot k$	$-\alpha jk$
j	j	$-ij$	β	$-\beta i$	jk	$ij \cdot k$	βk	βik
ij	ij	$-\alpha j$	βi	$-\alpha\beta$	$ij \cdot k$	αjk	$-\beta ik$	$-\alpha\beta k$
k	k	$-ik$	$-jk$	$-ij \cdot k$	γ	$-\gamma i$	$-\gamma j$	$-\gamma k$
ik	ik	$-\alpha k$	$-ij \cdot k$	$-\alpha jk$	γi	$-\alpha\gamma$	γij	$\alpha\gamma j$
jk	jk	$ij \cdot k$	$-\beta k$	βik	γj	$-\gamma ij$	$-\beta\gamma$	$-\beta\gamma i$
$ij \cdot k$	$ij \cdot k$	αjk	$-\beta ik$	$\alpha\beta k$	γij	$-\alpha\gamma j$	$\beta\gamma i$	$\alpha\beta\gamma$

Thus $A(\alpha, \beta, \gamma)$ is an alternative ring which is not associative.

PROOF. The map $a \mapsto a$, $a \in A$ is certainly an involution on A. Apply Theorem I.1 to get ring $A(\alpha)$. This is a commutative associative ring. Then we can construct $A(\alpha, \beta)$, which is a non-commutative algebra. We can verify that $A(\alpha, \beta)$ is associative, too. By Theorem I.1, algebra $A(\alpha, \beta, \gamma)$ is an alternative algebra. Note that $(ij)k \neq i(jk)$ because $i(jk) = -(ij)k$ and $2 \neq 0$ in A. So this algebra is not associative. □

REMARK I.3. From the proof of the above theorem, we know that $2 \neq 0$ is the necessary and sufficient condition for the Cayley-Dickson algebra to be an alternative algebra which is not associative.

3. Cayley-Dickson algebras and their induced *RA* loops

In this section, we use the circle operation to construct *RA* loops from Cayley-Dickson algebras introduced in the previous section. The following identity, which is not hard to check, will be used widely in this thesis. For any x and y in an algebra A with unity 1,

$$(x-1)\circ(y-1) = xy - 1.$$

In particular, $(-2)\circ(y-1) = (-1-1)\circ(y-1) = -y-1$.

Recall that an element $x \in A$ is quasi-regular if there exists an element y in A such that $x \circ y = y \circ x = 0$. Let $Quasi(A)$ be the set of all quasi-regular elements of the algebra A. If A is an associative algebra with 1, then $(Quasi(A), \circ) \cong (U(A), \cdot)$, the unit group of A. If A is alternative, then $(Quasi(A), \circ)$ is a Moufang loop by [**Goo87**, Theorem 1], called the Moufang circle loop of A.

We know that the unity of the circle loop is the 0 of the algebra. In this thesis, to avoid confusion, we use θ instead of 0 when we refer to the unity of the circle loop of an algebra.

Note that if A has 1, then -2 is always in $Quasi(A)$ with $-2 \circ -2 = \theta$, of order 2. We have seen that $2 \neq 0$ is important for us to construct the Cayley-Dickson algebra, see Remark I.3, and we will see that this -2 is important for the *RA* loops induced from Cayley-Dickson algebras.

THEOREM I.4. *Let A be a commutative associative ring with unity 1 and $2 \neq 0$. Let $\alpha - 1$, $\beta - 1$ and $\gamma - 1$ be elements in $Quasi(A)$. Let*

$$A(\alpha,\beta,\gamma) = A + Ai + Aj + Aij + Ak + Aik + Ajk + Aij \cdot k$$

be the Cayley-Dickson algebra in which $i^2 = \alpha$, $j^2 = \beta$ and $k^2 = \gamma$.

1. *Let $Quasi(A(\alpha,\beta,\gamma))$ be the Moufang circle loop of $A(\alpha, \beta, \gamma)$. Let $a = i - 1$, $b = j - 1$ and $u = k - 1$. Then a, b, $u \in Quasi(A(\alpha,\beta,\gamma))$. Let L_0 be the*

subgroup of $Quasi(A)$ *generated by* $\{\theta, -2, \alpha-1, \beta-1, \gamma-1\}$. *Then*

$$G = L_0 \circ \langle a \rangle \circ \langle b \rangle$$

is an RA group, $L_0 = \mathcal{Z}(G)$ *and*

$$L = G \cup G \circ u$$

is an RA loop, in which -2 *is the unique nonzero commutator-associator.*

2. *In* L, $l^* = \bar{l}$, *for any* $l \in L$, *where* $l \mapsto l^*$ *is the involution of the RA loop and* $l \mapsto \bar{l}$ *is the involution of the Cayley-Dickson algebra.*
3. $$H = Quasi(A) \circ \langle a \rangle \circ \langle b \rangle$$

   is an RA group, and

   $$P = H \cup H \circ u$$

   is an RA loop in which -2 *is the unique nonzero commutator-associator.*
4. *The RA loop* P *contains* L, *and* L *is the smallest RA subloop that contains the elements* a, b *and* u. *The loop* L *is completely determined by* α, β *and* γ.

PROOF. Note that $\alpha, \beta, \gamma \in U(A)$. By Theorem I.2, $A(\alpha, \beta, \gamma)$ is a generalized Cayley-Dickson algebra and

$$A(\alpha, \beta, \gamma) = A + Ai + Aj + Aij + Ak + Aik + Ajk + Aij \cdot k.$$

Because $a \circ a = (i-1) \circ (i-1) = i^2 - 1 = \alpha - 1$, which is in $Quasi(A)$, there exists $(\alpha-1)^{-1} \in Quasi(A) \subseteq Quasi(A(\alpha, \beta, \gamma))$, such that

$$(i-1) \circ ((i-1) \circ (\alpha-1)^{-1}) = \theta.$$

So a is a quasi-regular element with $a^{-1} = (i-1) \circ (\alpha-1)^{-1} \in G$. So is b by the same argument. Note that $a \circ a = \alpha - 1 \in L_0$, $b \circ b = \beta - 1 \in L_0$, and

$$b \circ a = ji - 1 = -ij - 1 = (-1-1) \circ (i-1) \circ (j-1) = (-2) \circ a \circ b,$$

and $-2 \in L_0$, $a \circ b \neq b \circ a$, so $G/L_0 \cong C_2 \times C_2$. Note that G is an RA group if and only if $G/\mathcal{Z}(G) \cong C_2 \times C_2$ by [**GJM96**, Proposition 3.6]. Therefore, to show that G is an RA group, it remains only to show that $\mathcal{Z}(G) = L_0$.

For any $z = l_0 \circ a^p \circ b^q \in \mathcal{Z}(G)$, where $p, q = 0, 1$ and $l_0 \in L_0$, we show that $p = q = 0$. In fact, if $p = 1$, $z \circ b = b \circ z$ implies $l_0 \circ a \circ b^q \circ b = b \circ l_0 \circ a \circ b^q =$

$(-2) \circ l_0 \circ a \circ b \circ b^q$, and then $-2 = 0$, a contradiction. Hence $p = 0$. Similarly, q must be 0. So $z \in L_0$. Since $L_0 \subseteq A$, whose elements commute with any elements of $A(\alpha, \beta, \gamma)$, $L_0 \subseteq \mathcal{Z}(G)$. Thus $\mathcal{Z}(G) = L_0$.

Note that -2 is the unique commutator-associator, so the involution of the *RA* group G is

$$g^* = \begin{cases} g & \text{if } g \in \mathcal{Z}(G) \\ (-2) \circ g & \text{otherwise} \end{cases}$$

for any $g \in G$. To show that $L = G \cup G \circ u$ is an *RA* loop, we will use its definition. Note that for any $g = l_0 \circ a \circ b \in G$, where $l_0 \in L_0$, $g \circ u = ((l_0 + 1) - 1) \circ ((i - 1) \circ (j - 1)) \circ (k - 1) = (l_0 + 1)ij \cdot k - 1$. Since -1 is quasi-regular if and only if $1 + (-1) = 0$ is a unit of the algebra, which is not true, $-1 \notin L_0$. Therefore, for any $l_0 \in L_0$, $l_0 + 1 \neq 0$. Thus $g \circ u = (l_0 + 1)ij \cdot k - 1 \notin G$ because each element in G is of the form

$$l_0 \circ a^{m_1} \circ b^{m_2} = (l_0 + 1)i^{m_1} j^{m_2} - 1,$$

where $m_1, m_2 = 0, 1$. Therefore, $G \cap G \circ u = \emptyset$.

Now we claim that for any $g, h \in G$, the three identities

$$g \circ (h \circ u) = (h \circ g) \circ u,$$

$$(g \circ u) \circ h = (g \circ h^*) \circ u,$$

$$(g \circ u) \circ (h \circ u) = g_0 \circ h^* \circ g$$

hold, where $g_0 = \gamma - 1$. By using the multiplication table of the Cayley-Dickson algebra and the formula $(x - 1) \circ (y - 1) = xy - 1$, we can check these identities for any $g, h \in G$. This is a long process and we just check two cases here.

Suppose that $g = l_0 \circ a$, $h = l_1 \circ a \circ b$, where $l_0, l_1 \in L_0$. Let us check that $g \circ (h \circ u) = (h \circ g) \circ u$. Note that

$$\begin{aligned} g \circ (h \circ u) &= l_0 \circ a \circ ((l_1 \circ a \circ b) \circ u) \\ &= (l_0 \circ l_1) \circ (a \circ ((a \circ b) \circ u)) \\ &= (l_0 \circ l_1) \circ (a \circ (ij \cdot k - 1) \\ &= (l_0 \circ l_1) \circ (i(ij \cdot k) - 1) \end{aligned}$$

$$= (l_0 \circ l_1) \circ (-\alpha jk - 1)$$

and

$$\begin{aligned}(h \circ g) \circ u &= ((l_1 \circ a \circ b) \circ (l_0 \circ a)) \circ u \\ &= (l_1 \circ l_0) \circ (((a \circ b) \circ a) \circ u) \\ &= (l_1 \circ l_0) \circ (((ij \cdot i)k - 1)) \\ &= (l_1 \circ l_0) \circ (-\alpha jk - 1).\end{aligned}$$

So $g \circ (h \circ u) = (h \circ g) \circ u$. Also, if $g = l_0 \circ b$ and $h = l_1 \circ a \circ b$, $(g \circ u) \circ (h \circ u) = g_0 \circ h^* \circ g$. Note that $g^* = -2 \circ g$ if $g \notin Z(G)$, so

$$\begin{aligned}(g \circ u) \circ (h \circ u) &= (l_0 \circ b \circ u) \circ (l_1 \circ (a \circ b) \circ u) \\ &= (l_0 \circ l_1) \circ ((b \circ u) \circ ((a \circ b) \circ u)) \\ &= (l_0 \circ l_1) \circ ((jk)((ij)k) - 1) \\ &= (l_0 \circ l_1) \circ (-\beta\gamma i - 1)\end{aligned}$$

and, since $h^* = -2 \circ h$,

$$\begin{aligned}g_0 \circ h^* \circ g &= (\gamma - 1) \circ ((l_1 \circ a \circ b \circ (-2)) \circ (l_0 \circ b)) \\ &= (\gamma - 1) \circ l_1 \circ (-2) \circ l_0 \circ ((ij)j - 1) \\ &= (-\gamma - 1) \circ l_1 \circ l_0 \circ (\beta i - 1) \\ &= (l_0 \circ l_1) \circ (-\beta\gamma i - 1),\end{aligned}$$

so the identity holds.

Next let us show that for any l in L, $l^* = \bar{l}$. This follows since

$$\bar{a} = \overline{i-1} = -i - 1 = (-2) \circ (i - 1) = (i - 1)^* = a^*$$

$$\bar{b} = \overline{j-1} = -j - 1 = (-2) \circ (j - 1) = (j - 1)^* = b^*$$

$$\bar{u} = \overline{k-1} = -k - 1 = (-2) \circ (k - 1) = (k - 1)^* = u^*$$

and $\overline{l_0} = l_0 = l_0^*$ for any $l_0 \in L_0 = \mathcal{Z}(G)$.

Finally, since L is a subloop of P, only the centers are different, it is easy to check that P is an RA loop. Note that any RA subloop of P which contains a, b and u must contain L_0 because

$$a \circ a = \alpha - 1, \; b \circ b = \beta - 1, \text{ and } u \circ u = \gamma - 1$$

and $-2 = a \circ b \circ a^{-1} \circ b^{-1}$. Therefore, L is the smallest RA subloop of P which contains a, b and u. □

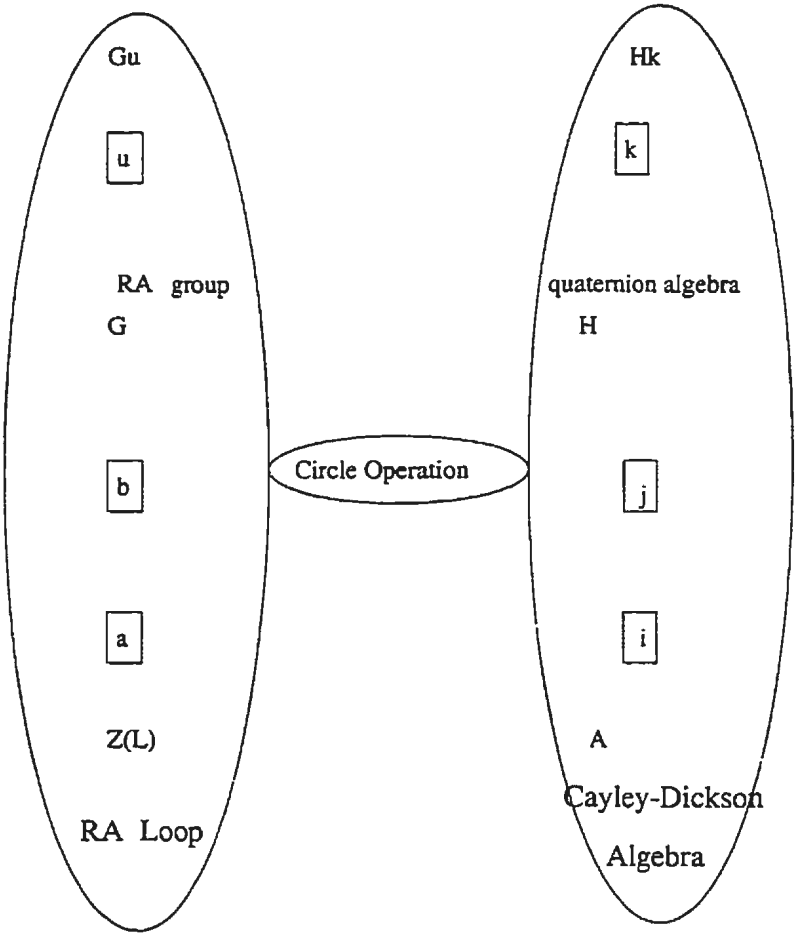

FIGURE I.1. Circle operation connects Cayley-Dickson algebras and *RA* loops

We give the following definition:

DEFINITION I.5. *The RA loop L in the above theorem is called the RA loop induced by the Cayley-Dickson algebra $A(\alpha, \beta, \gamma)$. The RA loop P is called the major RA loop induced by $A(\alpha, \beta, \gamma)$.*

REMARK I.6. The Cayley-Dickson process can be recursively used n times to get the so called generalized Cayley-Dickson algebras which are not alternative if $n > 3$, as shown in [**Bro67**] [**ES90**]. As in [**dBJ96**, Section 3], we can define generalized RA loops. Constructing RA loops as in Theorem I.4, we can get generalized RA loops from generalized Cayley-Dickson algebras.

4. Induced RA loops and other RA loops

The following lemma will be needed in Theorem I.8 and in Section 6.

LEMMA I.7. *Let $P = (\mathcal{Z}(P)\langle a\rangle\langle b\rangle)\langle u\rangle$ and $L = (\mathcal{Z}(L)\langle c\rangle\langle d\rangle)\langle v\rangle$ be two RA loops. Let f be a group homomorphism from $\mathcal{Z}(P)$ to $\mathcal{Z}(L)$ such that*

$$f(a^2) = c^2,\ f(b^2) = d^2,\ f(u^2) = v^2,\ f((a,b)) = (c,d),$$

where (a,b) and (c,d) are the unique nonidentity commutators of the loops P and L, respectively. Then f can be extended to a loop homomorphism from P to L by setting

$$f(za^{m_1}b^{m_2} \cdot u^{m_3}) = f(z)c^{m_1}d^{m_2} \cdot v^{m_3},$$

for any $z \in \mathcal{Z}(P)$. Moreover, if $f\colon \mathcal{Z}(P) \mapsto \mathcal{Z}(L)$ is an isomorphism, so is its extension.

PROOF. Because any element in P can be uniquely expressed in the form

$$za^{m_1}b^{m_2} \cdot u^{m_3}$$

for some $z \in \mathcal{Z}(P)$, and the same property holds for L, map f is well-defined. Note that for any elements $x = z_1a^{m_1}b^{m_2}$ and $y = z_2a^{n_1}b^{n_2}$, where $m_i,\ n_i = 0,\ 1,\ i = 1,\ 2$, we have

$$xy = z_1z_2(a,b)^{m_2n_1}a^{m_1+n_1}b^{m_2+n_2}.$$

Thus

$$f(xy) \quad = \quad f(z_1)f(z_2)(c,d)^{m_2n_1}c^{m_1+n_1}d^{m_2+n_2}$$

$$\begin{aligned} &= f(z_1)c^{m_1}d^{m_2} \cdot f(z_2)c^{n_1}d^{m_2} \\ &= f(x)f(y). \end{aligned}$$

Therefore f is a group homomorphism from the *RA* group $\mathcal{Z}(P)\langle a\rangle\langle b\rangle$ to the *RA* group $\mathcal{Z}(L)\langle c\rangle\langle d\rangle$. Suppose $g \in \mathcal{Z}(P)\langle a\rangle\langle b\rangle$. If $g \in \mathcal{Z}(P)$, then $f(g^*) = f(g) = f(g)^*$ since $f(g)$ is in the center of L; if $g \notin \mathcal{Z}(P)$, then $f(g^*) = f((a, b)g) = (c, d)f(g) = f(g)^*$ since $f(g)$ is not in the center of L. Therefore $f(g^*) = f(g)^*$ for any $g \in \mathcal{Z}(P)\langle a\rangle\langle b\rangle$.

We extend the map f to a map from P to L in the following way. For any $gu \in P$, let $f(gu) = f(g)v$, where $g \in \mathcal{Z}(P)\langle a\rangle\langle b\rangle$. Then it is true that f is a map from P to L because

$$P = \mathcal{Z}(P)\langle a\rangle\langle b\rangle \cup \mathcal{Z}(P)\langle a\rangle\langle b\rangle u, \text{ and } \mathcal{Z}(P)\langle a\rangle\langle b\rangle \cap \mathcal{Z}(P)\langle a\rangle\langle b\rangle u = \emptyset.$$

For any g, h in the *RA* group of P we have

$$\begin{aligned} f(g(hu)) &= f((hg)u) = f(hg)f(u) = (f(h)f(g))f(u) \\ &= (f(h)f(g))v = f(g)(f(h)v) = f(g)f(hu), \\ f((gu)h) &= f(gh^*)u = (f(g)f(h^*))f(u) = (f(g)f(h)^*)v \\ &= (f(g)v)f(h) = f(gu)f(h), \\ f((gu)(hu)) &= f(u^2h^*g) = f(u^2)f(h^*)f(g) = v^2f(h)^*f(g) \\ &= (f(g)v)(f(h)v) = f(gu)f(hu). \end{aligned}$$

Thus f is a loop homomorphism from P to L. Note that if f is an isomorphism from $\mathcal{Z}(P)$ to $\mathcal{Z}(L)$ then so is the extension. □

THEOREM I.8. *Any RA loop is a homomorphic image of the major RA loop P induced by some Cayley-Dickson algebra* $A(\alpha, \beta, \gamma)$.

PROOF. Let W be any given *RA* loop. By the structure theorem of *RA* loops, we can assume that $W = (\mathcal{Z}(W)\langle a\rangle\langle b\rangle)\langle u\rangle$. Since $\mathcal{Z}(W)$ is an abelian group, we can find a ring V such that the multiplication is trivial and $(V, +) \cong (\mathcal{Z}(W), \cdot)$. Then the circle group $(Quasi(V), \circ)$ of V, which is identical to $(V, +)$, is isomorphic to $\mathcal{Z}(W)$. Assume that under this isomorphism f_0, $f_0(\alpha) = a^2$, $f_0(\beta) = b^2$, and $f_0(\gamma) = u^2$, where α, β and $\gamma \in V$. We can make these assumptions because a^2, b^2 and u^2 are in $\mathcal{Z}(W)$.

Let $A = \mathrm{Z} \oplus V$, where Z is the integer ring. Define addition and multiplication on A by

$$(m,v) + (m_1,v_1) = (m+m_1, v+v_1)$$

$$(m,v)(m_1,v_1) = (mm_1, mv_1 + m_1v).$$

Note that A is an associative commutative ring with 1. We claim that

$$(Quasi(A), \circ) = \{(t,v) \mid t \in \{0,-2\}, v \in V = Quasi(V)\}.$$

For any $(m, v) \in Quasi(A)$, there is a (m_1, v_1) such that $(m, v) \circ (m_1, v_1) = (0, 0)$. Hence

$$(mm_1 + m + m_1, m_1v + mv_1 + v + v_1) = (0,0).$$

This implies that $m = m_1 = 0$ or $m = m_1 = -2$. Therefore,

$$(m,v) \in \{(t,v) \mid t \in \{0,-2\}, v \in V = Quasi(V)\}.$$

On the other hand, for any $v \in V$, $(0,v) \circ (0,-v) = (0,0)$ and $(-2,v) \circ (-2,-v) = (4-2-2, -2v+2v+v-v) = (0,0)$, so the two sets are equal.

Note that $(-2, v) = (-2, 0) \circ (0, -v)$, and $(-2,0)$ is of order 2 in the group. Thus

$$(Quasi(A), \circ) = \{(0,0), (-2,0)\} \times (0, Quasi(V)),$$

is the direct product of two subgroups. Note that $(1,\alpha)(1,-\alpha) = (1,0)$, the identity of A, so $(1,\alpha) \in U(A)$. Similarly, $(1,\beta)$ and $(1,\gamma)$ are in $U(A)$ and $2 \neq 0$. Thus $(1,\alpha) - (1,0)$, $(1,\beta) - (1,0)$ and $(1,\gamma) - (1,0)$ are in $Quasi(A)$, and the conditions of Theorem I.4 are satisfied. By Theorem I.4,

$$\begin{aligned} P &= (Quasi(A) \circ \langle i-1\rangle \circ \langle j-1\rangle) \circ \langle k-1\rangle \\ &= (\{(0,0),(-2,0)\} \times (0, Quasi(V)) \circ \langle i-1\rangle \circ \langle j-1\rangle) \circ \langle k-1\rangle \end{aligned}$$

is an RA loop with $(i-1)\circ(i-1) = (0,\alpha)$, $(j-1)\circ(j-1) = (0,\beta)$ and $(k-1)\circ(k-1) = (0,\gamma)$.

Define f_1 from $Quasi(A)$ to $\mathcal{Z}(W)$ by

$$f_1(0,v) = f_0(v), f_1((-2,0)) = s,$$

where s is the unique nonidentity commutator-associator of W. Thus

$$f_1((-2,0)^m \circ (0,v)) = s^m f_0(v),$$

where $m = 0, 1$. For any elements $(-2,0)^m \circ (0,v)$, $(-2,0)^n \circ (0,w) \in Quasi(A)$, where $m, n = 0, 1$, we have

$$\begin{aligned} f_1((-2,0)^m \circ (0,v) \circ (-2,0)^n \circ (0,w)) &= f_1((-2,0)^{m+n} \circ (0, v \circ w)) \\ &= s^{m+n} f_0(v \circ w) \\ &= s^{m+n} f_0(v) f_0(w) \\ &= s^m f_0(v) s^n f_0(w) \\ &= f_1((-2,0)^m \circ (0,v)) f_1((-2,0)^n \circ (0,w)). \end{aligned}$$

Therefore, f_1 is a group homomorphism, with $f_1((-2,0)) = s$, and

$$f_1((i-1)\circ(i-1)) = f_1((0,\alpha)) = f_0(\alpha) = a^2,\ f_1((j-1)\circ(j-1)) = f_1((0,\beta)) = f_0(\beta) = b^2,$$

$$f_1((k-1) \circ (k-1)) = f_1((0,\gamma)) = u^2.$$

By Lemma I.7, f_1 can be extended to a loop homomorphism f from P to W. Because the map f_1 is surjective, it is easy to see that the map f is also surjective. So W is a homomorphic image of P. □

Luiz G. X. de Barros [**dB93a**] classified *RA* loops into two types: type *I* and *II*. Let us recall the definition [**GJM96**, Definition 2.1]. An *RA* loop L is of type *I* if the unique non-identity commutator-associator s of L is a square in $\mathcal{Z}(L)$; that is, if there exists $t \in \mathcal{Z}(L)$ such that $t^2 = s$. If there is no such element, the loop is said to be of type *II*.

In the above theorem, the nonidentity commutator-associator of the *RA* loop P is $(-2,0)$, and the center of the loop P is $(Quasi(A), \circ) = (0, Quasi(V)) \cup (-2, Quasi(V))$. So it is easy to see that P is of type *II*. From the above theorem, we have the following

COROLLARY I.9. *Any RA loop is the homomorphic image of an RA loop of type II.*

5. Moufang circle loops and *RA* loops

From [**Goo87**, Theorem 1], we know that the set of all quasi-regular elements of an alternative ring forms a Moufang loop under the circle operation called a Moufang

circle loop. In section 3 we have shown that the Moufang circle loop of a Cayley-Dickson algebra always contains an *RA* circle loop as a subloop. It is natural to ask when an *RA* loop happens to be the Moufang circle loop of an alternative ring.

The smallest *RA* loops are of order 16, the Cayley loop $M_{16}(Q_8)$ and $M(Q_8,\ 2)$, or $M(Q_8, *, t_1)$ and $M(D_4, *, 1)$ [**GJM96**, Table 4, p.145]. In this section, we show that these two loops are Moufang circle loops of alternative algebras.

PROPOSITION I.10. *Let* Z *be the integers. Let* $\alpha = \pm 1$, $\beta = \pm 1$, $\gamma = \pm 1$ *and let A be the Cayley-Dickson algebra* $\mathrm{Z}(\alpha,\ \beta,\ \gamma)$. *Then the major RA loops, which are two RA loops of order* 16, *induced from the these Cayley-Dickson algebras, are Moufang circle loops. In particular, the major loop induced by* $\mathrm{Z}(-1,-1,-1)$ *is the Cayley loop* $M_{16}(Q_8)$ *and the major loop induced by* $\mathrm{Z}(1,1,1)$ *is* $M(Q_8,\ 2)$.

PROOF. Let x be an invertible element of the Cayley-Dickson algebra $\mathrm{Z}(\alpha,\ \beta,\ \gamma)$. Then there exists $y \in \mathrm{Z}(\alpha,\ \beta,\ \gamma)$ such that $xy = 1$. Let n be the norm on $\mathrm{Z}(\alpha,\ \beta,\ \gamma)$. Since $1 = n(xy) = n(x)n(y)$, $n(x) = \pm 1$. Since x is of the form

$$x = x_0 + x_1 i + x_2 j + x_3 ij + x_4 k + x_5 ik + x_6 jk + x_7 ij \cdot k,$$

$$x = \pm 1,\ \pm i,\ \pm j,\ \pm ij,\ \pm k,\ \pm ik,\ \pm jk,\ \pm ij \cdot k.$$

Since x is invertible if and only if $x - 1$ is quasi-regular, the circle Moufang loop of $\mathrm{Z}(\alpha,\ \beta,\ \gamma)$ is

$$\{\theta,\ -2,\ \pm i - 1,\ \pm j - 1,\ \pm ij - 1,\ \pm k - 1,\ \pm ik - 1,\ \pm jk - 1,\ \pm ij \cdot k - 1, \},$$

which is the major *RA* loop

$$P = \{\theta,\ -2\} \circ (\langle i - 1\rangle \circ \langle j - 1\rangle) \circ \langle k - 1\rangle$$

induced from the Cayley-Dickson algebra $\mathrm{Z}(\alpha,\ \beta,\ \gamma)$.

Let $\alpha = -1$, $\beta = -1$ and $\gamma = -1$. Then $(i-1) \circ (i-1) = i^2 - 1 = \alpha - 1 = -2$ and $(j-1) \circ (j-1) = j^2 - 1 = \beta - 1 = -2$. Similarly, $(k-1) \circ (k-1) = k^2 - 1 = -2$. In this case P is the Cayley loop $M_{16}(Q_8)$ by [**GJM96**, table 4, p.145] because -2 is the commutator-associator.

Let $\alpha = 1$, $\beta = 1$ and $\gamma = 1$. Then $(i-1) \circ (i-1) = i^2 - 1 = \alpha - 1 = \theta$, $(j-1) \circ (j-1) = \theta$ and $(k-1) \circ (k-1) = \theta$. In this case P is $M(D_4, *, 1)$ by

[**GJM96**, Table 4, p.145] because θ is the unity of the circle loop P. Note that $M(D_4, *, 1)$ is $M(Q_8, 2)$.

Since there are only two nonisomorphic RA loops of order 16 [**JLM95**] [**GJM96**, Table 4, p.145], the other RA loops are isomorphic to one of the above two loops. □

6. The categories of RA loops and Cayley-Dickson algebras

In this section, we define the categories of RA loops and Cayley-Dickson algebras and show that they are equivalent. For basic concepts of category theory, we refer the reader to [**Jac80**].

First we define some notation. In this section, we always assume that R is a fixed commutative associative ring with 1, R-algebras have unities and $2 \neq 0$. For a given Cayley-Dickson algebra $A(\alpha, \beta, \gamma)$, we let $T_{A(\alpha,\beta,\gamma)}$ be the submonoid generated by $\{i, j, k\}$ in the multiplication monoid of this Cayley-Dickson algebra. Let $Alg_{A(\alpha,\beta,\gamma)}$ denote the R-subalgebra of $A(\alpha, \beta, \gamma)$ generated by $\{i, j, k\}$.

Now we define the category of Cayley-Dickson algebras Γ. The objects in Γ are all the Cayley-Dickson algebras $A(\alpha, \beta, \gamma)$, where A is a commutative associative R-algebra.

For any two objects $A(\alpha, \beta, \gamma)$ and $A_1(\alpha_1, \beta_1, \gamma_1)$ in Γ we define

$$hom_\Gamma(A(\alpha, \beta, \gamma), A_1(\alpha_1, \beta_1, \gamma_1))$$

to be the set of all R-algebra homomorphisms f from the R-subalgebra $Alg_{A(\alpha,\beta,\gamma)}$ to the R-subalgebra $Alg_{A_1(\alpha_1,\beta_1,\gamma_1)}$ with i, j, and $k \in \langle f(T_{A(\alpha,\beta,\gamma)}), -1\rangle$, the submonoid of $(A_1(\alpha_1, \beta_1, \gamma_1), \cdot)$ generated by $f(T_{A(\alpha,\beta,\gamma)})$ and -1.

For each ordered triple of objects $(A_1(\alpha_1, \beta_1, \gamma_1), A_2(\alpha_2, \beta_2, \gamma_2), A_3(\alpha_3, \beta_3, \gamma_3))$, a map from

$$hom_\Gamma(A_1(\alpha_1, \beta_1, \gamma_1), A_2(\alpha_2, \beta_2, \gamma_2)) \times hom_\Gamma(A_2(\alpha_2, \beta_2, \gamma_2), A_3(\alpha_3, \beta_3, \gamma_3))$$

to $hom_\Gamma((A_1(\alpha_1, \beta_1, \gamma_1), A_3(\alpha_3, \beta_3, \gamma_3))$ can be defined to be the composition of the morphisms. In fact, let $f \in hom_\Gamma(A_1(\alpha_1, \beta_1, \gamma_1), A_2(\alpha_2, \beta_2, \gamma_2))$ and

$g \in hom(A_2(\alpha_2, \beta_2, \gamma_2), A_3(\alpha_3, \beta_3, \gamma_3))$. Since i, j, and $k \in \langle f(T_{A(\alpha,\beta,\gamma)}), -1\rangle$, the submonoid generated by i, j, and k is in $\langle f(T_{A(\alpha,\beta,\gamma)}), -1\rangle$, i.e.,

$$\langle T_{A_2(\alpha_2,\beta_2,\gamma_2)}, -1\rangle \subseteq f(\langle T_{A_1(\alpha_1,\beta_1,\gamma_1)}, -1\rangle).$$

Therefore,

$$g(\langle T_{A_2(\alpha_2,\beta_2,\gamma_2)}, -1\rangle) \subseteq \langle gf(T_{A(\alpha,\beta,\gamma)}), -1\rangle.$$

But i, j, and $k \in g(T_{A_2(\alpha_2,\beta_2,\gamma_2)})$, so i, j, and $k \in gf(\langle T_{A(\alpha,\beta,\gamma)}, -1\rangle)$. Therefore, the composition of the morphisms satisfies the restriction and

$$gf \in hom_\Gamma((A_1(\alpha_1,\beta_1,\gamma_1), A_3(\alpha_3,\beta_3,\gamma_3)).$$

Naturally, the morphisms are disjoint for different pairs of objects. Since all the morphisms in hom are R-algebra homomorphisms, the associative law holds for the composition of the morphisms. For each object $A(\alpha,\beta,\gamma)$, the identity map is the unity of $hom(A(\alpha,\beta,\gamma),A(\alpha,\beta,\gamma))$. By definition, Γ is a category.

Now we define the category of RA loops Θ. The objects in Θ are all RA loops L induced by a Cayley-Dickson algebra, as described in Theorem I.4. So any object in Θ can be expressed as $L = (\mathcal{Z}(L)\langle a_L\rangle\langle b_L\rangle)\langle u_L\rangle$ with $s = -2$, and $a = i - 1$, $b = j - 1$ and $u = k - 1$, where $\mathcal{Z}(L)$ is the center of the loop and s is the unique commutator-associator. We will use this expression to refer to this object.

For each pair of objects in Θ, L and P, we define $hom_\Theta(L,P)$ to be the set of all loop homomorphisms f from L onto P such that $(f(a), f(b), f(u)) \neq 0$.

Now we show that under this definition, Θ is a category. For each ordered triple of objects (L, P, Q), a map from

$$hom(L,P) \times hom(P,Q) \text{ to } hom(L,Q)$$

can be defined to be the composition of the morphisms. In fact, let $f \in hom(L,P)$ and $g \in hom(P,Q)$, then gf is an onto map from L to Q since f and g are onto maps. By definition, $(f(a_L), f(b_L), f(u_L)) \neq 0 \in P$, so $(f(a_L), f(b_L), f(u_L)) = (a_P, b_P, u_P)$ because the associator is unique in the RA loop P. Since $(g(a_P), g(b_P), g(u_P)) \neq 0 \in Q$,

$$(gf(a_L), gf(b_L), gf(u_L)) = g((f(a_L), f(b_L), f(u_L))) = g((a_P, b_P, u_P)) \neq 0.$$

Thus $gf \in hom(L,Q)$. Naturally, the morphisms are disjoint for different pair of objects. Since all the morphisms in hom are loop homomorphisms, the associative law holds for the composition of the maps. For each object L, the identity map is the unity of the $hom(L,L)$. By definition, Θ is a category.

To show that the two categories are equivalent, we need the following lemmas.

LEMMA I.11. *For each object $A(\alpha,\beta,\gamma)$ in Γ, let $F(A(\alpha,\beta,\gamma))$ be the RA loop induced by $A(\alpha,\beta,\gamma)$. For any pair of objects $A(\alpha,\beta,\gamma)$ and $A_1(\alpha_1,\beta_1,\gamma_1)$ and any homomorphism $f \in hom(A(\alpha,\beta,\gamma), A_1(\alpha_1,\beta_1,\gamma_1))$, define $F(f)$ to be the loop homomorphism induced by f. Then F is a functor from Γ to Θ.*

PROOF. For each object $A(\alpha,\beta,\gamma)$ in Γ, following Theorem I.4,

$$L = (L_0 \circ \langle i-1\rangle \circ \langle j-1\rangle) \circ \langle u-1\rangle$$

is an RA loop with

$$L_0 = \langle s=-2, (i-1)\circ(i-1) = \alpha-1, (j-1)\circ(j-1) = \beta-1, (k-1)\circ(k-1) = \gamma-1\rangle.$$

By definition, $L = F(A(\alpha,\beta,\gamma)) \in \Theta$.

For any pair of objects $A(\alpha,\beta,\gamma)$ and $A_1(\alpha_1,\beta_1,\gamma_1)$, let the corresponding RA loops be L and L_1. For any $f \in hom(A(\alpha,\beta,\gamma), A_1(\alpha_1,\beta_1,\gamma_1))$, by definition, f is an R-algebra homomorphism from the R-subalgebra $Alg_{A(\alpha,\beta,\gamma)}$ to the R-subalgebra $Alg_{A_1(\alpha_1,\beta_1,\gamma_1)}$. And $i, j, k \in f(T_{A(\alpha,\beta,\gamma)})$. We want to show that $F(f) \in hom(L, L_1)$.

Since f is an algebra homomorphism, it induces a loop homomorphism from L to L_1. This map is $F(f)$.

Since i, j and k are in $\langle f(T_{A(\alpha,\beta,\gamma)}), -1\rangle$, we can assume that

$$i = (-1)^{n_0}(f(i)^{n_1} f(j)^{n_2}) \cdot f(k)^{n_3}.$$

Following the formula $xy - 1 = (x-1)\circ(y-1)$, we have

$$\begin{aligned} i-1 &= (-2)^{n_0} \circ (f(i)-1)^{n_1} \circ (f(j)-1)^{n_2}) \circ (f(k)-1)^{n_3} \\ &= (-2)^{n_0} \circ (f(i-1)^{n_1} \circ f(j-1)^{n_2}) \circ f(k-1)^{n_3}. \end{aligned}$$

Thus $i-1$ is in $F(f)(L)$. So are $j-1$ and $k-1$ by the same argument. Therefore, $F(f)$ is an onto map. Let θ be the unity of the loop. If the loop associator of $f(i-1)$, $f(j-1)$ and $f(k-1)$ were θ, by [**GJM96**, Theorem 5.4], the three elements would generate a group. So the associator of $i-1$, $j-1$ and $k-1$ would be θ, a contradiction. Thus $F(f)$ is in $hom(L, L_1)$.

For $1_{A(\alpha,\beta,\gamma)}$, we know $F(1_{A(\alpha,\beta,\gamma)}) = 1$. Let $f \in hom(A(\alpha,\beta,\gamma), A_1(\alpha_1,\beta_1,\gamma_1))$ and let $g \in hom(A_1(\alpha_1,\beta_1,\gamma_1), A_2(\alpha_2,\beta_2,\gamma_2))$. Then $F(gf) = F(g)F(f)$ because $F(f)$ and $F(g)$ are the restrictions of f and g on the loops. Thus F is a functor from Cayley-Dickson algebra category Γ to the loop category Θ.

□

LEMMA I.12. *The functor F defined above from Γ to Θ is faithful.*

PROOF. Recall that a functor from Γ to Θ is faithful if for any pair of objects $A(\alpha,\beta,\gamma)$ and $A_1(\alpha_1,\beta_1,\gamma_1)$ in Γ the map $f \longrightarrow F(f)$ of $hom(A(\alpha,\beta,\gamma), A_1(\alpha_1,\beta_1,\gamma_1))$ to $hom(F(A(\alpha,\beta,\gamma)), F(A_1(\alpha_1,\beta_1,\gamma_1)))$ is injective.

Since $F(f)$ is defined by the restriction of f on the induced loop L, which is generated by $\{i-1,\ j-1,\ k-1\}$, we can show that the map is injective. In fact, if $g \in hom(A(\alpha,\beta,\gamma), A_1(\alpha_1,\beta_1,\gamma_1))$ and $F(g) = F(f)$, then $g(x) = F(g)(x) = F(f)(x) = f(x)$, for any $x = i-1,\ j-1,\ k-1$. Since f and g are R-algebra homomorphisms, $f(i) = g(i)$, $f(j) = g(j)$ and $f(k) = g(k)$ and the two morphisms are identical.

□

LEMMA I.13. *The functor defined above from Γ to Θ is full.*

PROOF. Recall that a functor is full from Γ to Θ if for any pair of objects $A(\alpha,\beta,\gamma)$ and $A_1(\alpha_1,\beta_1,\gamma_1)$ in Γ the map $f \longrightarrow F(f)$ of $hom(A(\alpha,\beta,\gamma), A_1(\alpha_1,\beta_1,\gamma_1))$ to $hom(F(A(\alpha,\beta,\gamma)), F(A_1(\alpha_1,\beta_1,\gamma_1)))$ is surjective.

Suppose that $F(A(\alpha,\beta,\gamma)) = L$ and $F(A_1(\alpha_1,\beta_1,\gamma_1)) = L_1$. For any $g \in hom(L, L_1)$, by definition, the associator $(g(i-1),\ g(j-1),\ g(k-1)) \neq \theta$. Assume that

$$g(i-1) = (-2)^{m_0} \circ ((i-1)^{m_1} \circ (j-1)^{m_2})) \circ (k-1)^{m_3}$$
$$g(j-1) = (-2)^{n_0} \circ ((i-1)^{n_1} \circ (j-1)^{n_2})) \circ (k-1)^{n_3}$$
$$g(k-1) = (-2)^{p_0} \circ ((k-1)^{p_1} \circ (j-1)^{p_2})) \circ (k-1)^{p_3}.$$

We want to define a map from $Alg_{A(\alpha,\beta,\gamma)}$, the R-subalgebra of $A(\alpha,\beta,\gamma)$ generated by $\{i,j,k\}$ to $Alg_{A_1(\alpha_1,\beta_1,\gamma_1)}$, the R-subalgebra of $A_1(\alpha_1,\beta_1,\gamma_1)$ generated by $\{i,\ j,\ k\}$ such that $i,\ j,\ k \in \langle f(T_{A(\alpha,\beta,\gamma)}),\ -1\rangle$.

Define

$$f(i) = (-1)^{m_0}(i^{m_1} j^{m_2}) k^{m_3}$$
$$f(j) = (-1)^{n_0}(i^{n_1} j^{n_2}) k^{n_3}$$
$$f(k) = (-1)^{p_0}(i^{p_1} j^{p_2}) k^{p_3}.$$

Then f can be extended to an R-algebra homomorphism from the R-subalgebra $Alg_{A(\alpha,\beta,\gamma)}$ to the R-subalgebra $Alg_{A_1(\alpha_1,\beta_1,\gamma_1)}$. Now we show that $i, j, k \in \langle f(T_{A(\alpha,\beta,\gamma)}), -1\rangle$.

Since g is an onto map, $i-1$, $j-1$ and $k-1$ are in the image of g. Furthermore, $i-1$ can be expressed as some circle multiplication of -2, $g(i-1)$, $g(j-1)$ and $g(k-1)$. Suppose that

$$\begin{aligned} i-1 &= (-2)^{q_0} \circ (g(i-1)^{q_1} \circ g(j-1)^{q_2}) \circ g(k-1)^{q_3} \\ &= (-2)^{q_0} \circ [((i^{m_1}j^{m_2})k^{m_3}-1)^{q_1} \circ ((i^{n_1}j^{n_2})k^{n_3}-1)^{q_2}] \circ ((i^{p_1}j^{p_2})k^{p_3}-1)^{q_3} \\ &= (-2)^{p} \circ [((f(i)-1)^{q_1} \circ ((f(j)-1)^{q_2}] \circ ((f(k)-1)^{q_3} \\ &= (-1)^{p}((f(i))^{q_1}f(j)^{q_2})f(k)^{q_3}-1. \end{aligned}$$

Thus $i \in \langle f(T_{A(\alpha,\beta,\gamma)}), -1\rangle$. So are j and k by the same argument. Therefore, $f \in hom(A(\alpha,\beta,\gamma), A_1(\alpha_1,\beta_1,\gamma_1))$.

The last step of this proof is to show that $F(f) = g$. This is not hard because the definition of f tells us that

$$f(i-1) = (-2)^{m_0} \circ ((i-1)^{m_1} \circ (j-1)^{m_2})) \circ (k-1)^{m_3} = g(i-1),$$

$$f(j-1) = (-2)^{n_0} \circ ((i-1)^{n_1} \circ (j-1)^{n_2})) \circ (k-1)^{n_3} = g(j-1),$$

$$f(k-1) = (-2)^{q_0} \circ ((i-1)^{p_1} \circ (j-1)^{p_2})) \circ (k-1)^{p_3} = g(k-1).$$

Since $F(f)$ is defined by the restriction of the algebra homomorphism, $F(f) = g$.

□

THEOREM I.14. *Γ and Θ are equivalent categories.*

PROOF. By the above lemmas, we have shown that the functor F is faithful and full. By the definition of Θ, for every object P in Θ, there is an object $A(\alpha,\beta,\gamma)$ in Γ such that $F(A(\alpha,\beta,\gamma))$ is equal to P. By [**Jac80**, Proposition 1.3], Γ and Θ are equivalent categories.

□

We have seen that an *RA* loop is a homomorphic image of a loop induced by a Cayley-Dickson algebra. Now we show that certain *RA* loops contains subloops which are *RA* loops induced by Cayley-Dickson algebras.

PROPOSITION I.15. *For any RA loop* $P = (\mathcal{Z}(P)\langle a\rangle\langle b\rangle)\langle u\rangle$ *with* $s \notin \langle a^2, b^2, u^2\rangle$, *there is an object* $A(\alpha,\beta,\gamma)$ *in* Γ *such that the induced RA loop of* $A(\alpha,\beta,\gamma)$ *is isomorphic to the subloop of* P *generated by* a, b *and* u.

PROOF. Assume that $P = (\mathcal{Z}(P)\langle a\rangle\langle b\rangle)\langle u\rangle$ is an RA loop with $s \notin \langle a^2, b^2, u^2\rangle$, where $\mathcal{Z}(P)$ is the center of P. We know that a^2, b^2, u^2 are in $\mathcal{Z}(P)$. Set

$$P_0 = \{1, s\} \times \langle a^2, b^2, u^2\rangle$$

in P. Since s is of order 2 and it is not in the subgroup $\langle a^2, b^2, u^2\rangle$ by assumption, P_0 is the direct product of $\{1, s\}$ and $\langle a^2, b^2, u^2\rangle$.

Consider the Cayley-Dickson algebra $R\mathcal{Z}(P)(a^2, b^2, u^2)$, where $R\mathcal{Z}(P)$ is the commutative group algebra of $\mathcal{Z}(P)$ over R. By Theorem I.4, the induced RA loop L has the properties that $(i-1)\circ(i-1) = a^2 - 1$, $(j-1)\circ(j-1) = b^2 - 1$ and $(k-1)\circ(k-1) = u^2 - 1$. Set

$$L_0 = \{\theta, -2\} \times \langle a^2 - 1, b^2 - 1, u^2 - 1\rangle$$

Since -2 is of order 2 and it is not in $(\mathcal{Z}(P) - 1, \circ)$, L_0 is a direct product of the two subgroups.

Note that the subgroup of $\mathcal{Z}(P)$ generated by $\{a^2, b^2, u^2\}$ is isomorphic through map f_0 to the circle subgroup of L generated by $\{a^2 - 1, b^2 - 1, u^2 - 1\}$, where $f_0(x) = x - 1$, for any $x = a^2, b^2, u^2$ and their products. Extend this map f_0 to a map f from the subloop of P generated by a, b and u to L by setting $f(s) = -2$. Then it is a group isomorphism.

Note that under this isomorphism, $f(s) = -2$, $f(a^2) = (i-1)\circ(i-1)$, $f(b^2) = (j-1)\circ(j-1)$, and $f(u^2) = (k-1)\circ(k-1)$. Thus this map induces a loop homomorphism from the subloop of P generated by a, b and u to L by Lemma I.7, sending s, a, b, u, a^2, b^2 and u^2 to -2, $i-1$, $j-1$, $k-1$, a^2-1, b^2-1 and u^2-1, respectively. It is easy to see that this f is a loop isomorphism. □

CHAPTER II

Cayley-Dickson algebras and alternative loop algebras

In the previous chapter, we have shown that any Cayley-Dickson algebra can induce an RA loop. Certainly, this induced RA loop must be tightly related to this Cayley-Dickson algebra. In this chapter we will show an interesting relationship between them: any Cayley-Dickson algebra is a quotient algebra of the alternative loop algebra of the induced RA loop. Then we determine the kernel of the map and the properties preserved. After this a known result is generalized [**Zho**].

1. Induced alternative loop algebras

LEMMA II.1. *Every element in the Cayley-Dickson algebra $A(\alpha, \beta, \gamma)$ can be uniquely expressed in the form*

$$r_0 + r_1 a + r_2 b + r_3 a \circ b + r_4 u + r_5 a \circ u + r_6 b \circ u + r_7 (a \circ b) \circ u,$$

where $a = i - 1$, $b = j - 1$, $u = k - 1$ and $r_i \in A$, $i = 0, 1, \ldots, 7$.

PROOF. We show uniqueness first. Assume that

$$r_0 + r_1 a + r_2 b + r_3 a \circ b + r_4 u + r_5 a \circ u + r_6 b \circ u + r_7 (a \circ b) \circ u = 0.$$

Then

$$r_0 + r_1(i-1) + r_2(j-1) + r_3(i-1) \circ (j-1) + r_4(k-1) + r_5(i-1) \circ (k-1)$$

$$+ r_6(j-1) \circ (k-1) + r_7((i-1) \circ (j-1)) \circ (k-1) = 0.$$

Recall the formula $(x-1) \circ (y-1) = xy - 1$. Thus

$$r_0 - \sum_{i=1}^{7} r_i + r_1 i + r_2 j + r_3 ij + r_4 k + r_5 ik + r_6 jk + r_7 ij \cdot k = 0.$$

Therefore, $r_i = 0$, $i = 1, 2, \ldots, 7$, and then $r_0 = 0$.

Since $i = a + 1$, $j = b + 1$, $k = u + 1$, $ij = a \circ b + 1$, $ik = a \circ u + 1$, $jk = b \circ u + 1$, $ij \cdot k = (a \circ b) \circ u + 1$, any element

$$t_0 + t_1 i + t_2 j + t_3 ij + t_4 k + t_5 ik + t_6 jk + t_7 ij \cdot k$$

in $A(\alpha, \beta, \gamma)$ can be expressed in the form

$$r_0 + r_1 a + r_2 b + r_3 a \circ b + r_4 u + r_5 a \circ u + r_6 b \circ u + r_7 (a \circ b) \circ u.$$

This completes the proof. □

Let us recall the definitions of the involution of an alternative loop algebra and its norm and trace. Let AL be the loop algebra of RA loop L over algebra A. Let $l \mapsto l^*$ be the involution of the RA loop L. Then the involution on L extends linearly to an algebra involution of the loop algebra AL which we also denote $*$:

$$(\sum_{l \in L} r_l l)^* = \sum_{l \in L} r_l l^*.$$

The norm $n(x)$ and trace $t(x)$ of $x \in AL$ are defined by $n(x) = xx^*$ and $t(x) = x + x^*$, respectively. For more information, we refer the reader to the book by Goodaire, Jespers and Polcino Milies [**GJM96**, pp. 100-105].

THEOREM II.2. *Suppose A is a commutative associative ring with unity 1 and $2 \neq 0$. Let $\alpha - 1$, $\beta - 1$ and $\gamma - 1$ be elements in $Quasi(A)$. Let AL be the alternative loop algebra of the RA loop L over A, where L is either the RA loop or the major RA loop induced by the Cayley-Dickson algebra $A(\alpha, \beta, \gamma)$.*

1. *$AL = A\theta \oplus \omega(AL)$, direct sum as A-modules, where $\omega(AL)$ is the augmentation ideal of AL and θ is the unity of the loop L. Let f be the map from AL to $A(\alpha, \beta, \gamma)$ defined as follows. For any $x = r\theta + \sum_{l \in L} r_l l \in AL$, where $r \in A$ and $\sum_{l \in L} r_l l \in \omega(AL)$,*

$$f(r\theta + \sum_{l \in L} r_l l) = r + \sum_{l \in L} r_l \cdot l.$$

The operator "$\cdot$" in the expression $\sum_{l \in L} r_l \cdot l$ denotes multiplication in the algebra $A(\alpha, \beta, \gamma)$. Then f is an A-algebra homomorphism from AL onto $A(\alpha, \beta, \gamma)$, and

$$AL / \ker(f) \cong A(\alpha, \beta, \gamma)$$

as A-algebras. Thus every generalized Cayley-Dickson algebra is a quotient algebra of an RA loop algebra.

2. *The kernel of f is*

$$\{\sum_{l\in L} r_l l \mid \sum_{l\in L_0} r_{low}\cdot l = -\sum_{l\in L_0} r_{low},\ \forall r_{low}\in A, \forall l\in L_0, \forall w = \theta, a, b, a\circ b, u, a\circ u, b\circ u, (a\circ b)\circ u\},$$

where L_0 is the center of the loop L.

3. *The map f commutes with the involutions of the alternative loop algebra and Cayley-Dickson algebra. That is, for any $x\in AL$,*

$$f(x^*) = \overline{f(x)}.$$

4. *For the norm n and trace tr of the alternative loop algebra AL and the Cayley-Dickson algebra $A(\alpha,\beta,\gamma)$, we have $fn = nf$ and $ftr = trf$, that is, for any $x\in AL$,*

$$f(n(x)) = n(f(x)),$$
$$f(tr(x)) = tr(f(x)).$$

PROOF. We first show that f is an A-algebra homomorphism from the loop algebra AL to the Cayley-Dickson algebra $A(\alpha,\beta,\gamma)$.

For any element $x = r\theta + \sum_{l\in L} r_l l \in AL$, where $r\in A$ and $\sum_{l\in L} r_l l\in\omega(AL)$, we have

$$f(x) = r + \sum_{l\in L} r_l\cdot l \in A(\alpha,\beta,\gamma)$$

because

$$A(\alpha,\beta,\gamma) = A + Aa + Ab + Aa\circ b + Au + Aa\circ u + Ab\circ u + A(a\circ b)\circ u$$

contains the loop L, which is constructed from $A(\alpha,\beta,\gamma)$. Since AL is the direct sum of A and $\omega(AL)$, the map f is well defined.

For any two elements $x = r\theta + \sum_{l\in L} r_l l$, $y = r'\theta + \sum_{l\in L} r'_l l \in AL$, it is easy to check that

$$f(x+y) = r + r' + \sum_{l\in L}(r_l + r'_l)\cdot l = f(x) + f(y)$$

and $f(tx) = tf(x)$ for any $t\in A$. Thus f is an A-module homomorphism.

Let $v \in A(\alpha, \beta, \gamma)$. By Lemma II.1, we can write

$$v = r_0 + r_1 a + r_2 b + r_3 a \circ b + r_4 u + r_5 a \circ u + r_6 b \circ u + r_7 (a \circ b) \circ u.$$

Let

$$x = (r_0 - \sum_{i=1}^{7} r_i)\theta + r_1 a + r_2 b + r_3 a \circ b + r_4 u + r_5 a \circ u + r_6 b \circ u + r_7 (a \circ b) \circ u.$$

Then x can be written as

$$\begin{aligned} x &= r_0\theta + \{r_1(a-\theta) + r_2(b-\theta) + r_3(a \circ b - \theta) + r_4(u-\theta) + r_5(a \circ u - \theta) \\ &\quad + r_6(b \circ u - \theta) + r_7((a \circ b) \circ u - \theta)\} \in A\theta + \omega(AL). \end{aligned}$$

Thus

$$f(x) = r_0 + r_1 a + r_2 b + r_3 a \circ b + r_4 u + r_5 a \circ u + r_6 b \circ u + r_7 (a \circ b) \circ u = v,$$

since θ is 0 in the algebra. Therefore, f is onto.

The interesting part of the proof is to show that f is a ring homomorphism. For any two elements x and y in AL, let $x = r\theta + \sum_{l \in L} r_l l$ and $y = t\theta + \sum_{h \in L} t_h h$, where $\sum_{l \in L} r_l l$ and $\sum_{h \in L} t_h h$ are in $\omega(AL)$. Then

$$xy = rt\theta + \{t \sum_{l \in L} r_l l + r \sum_{h \in L} t_h h + \sum_{l \in L, h \in L} r_l t_h l \circ h\},$$

and the second part in the expression of xy is in $\omega(AL)$. So

$$\begin{aligned} f(xy) &= rt + \{t \sum_{l \in L} r_l \cdot l + r \sum_{h \in L} t_h \cdot h + \sum_{l \in L, h \in L} r_l t_h \cdot l \circ h\} \\ &= rt + t \sum_{l \in L} r_l \cdot l + r \sum_{h \in L} t_h \cdot h + \sum_{l \in L, h \in L} r_l t_h \cdot (l \cdot h + l + h) \\ &= rt + t \sum_{l \in L} r_l \cdot l + r \sum_{h \in L} t_h \cdot h + \sum_{l \in L, h \in L} r_l t_h \cdot l \cdot h \\ &\quad + \sum_{l \in L, h \in L} r_l t_h \cdot l + \sum_{l \in L, h \in L} r_l t_h \cdot h \\ &= rt + t \sum_{l \in L} r_l \cdot l + r \sum_{h \in L} t_h \cdot h + \sum_{l \in L, h \in L} r_l t_h \cdot l \cdot h \\ &\quad + (\sum_{l \in L} r_l \cdot l) \sum_{h \in L} t_h + (\sum_{l \in L} r_l) \cdot \sum_{h \in L} t_h \cdot h \end{aligned}$$

$$\begin{aligned} &= rt + t\sum_{l\in L} r_l \cdot l + r\sum_{h\in L} t_h \cdot h + \sum_{l\in L, h\in L} r_l t_h \cdot l \cdot h \\ &= (r + \sum_{l\in L} r_l \cdot l)(t + \sum_{h\in L} t_h \cdot h) \\ &= f(x)f(y). \end{aligned}$$

Therefore, f is an A-algebra homomorphism from the loop algebra onto the Cayley-Dickson algebra. Now we investigate the kernel. Since L is an RA loop, by the structure theorem of RA loops [**GJM96**, Theorem 3.1, p.123], L can be expressed as

$$\begin{aligned} L &= L_0 \cup L_0 \circ a \cup L_0 \circ b \cup L_0 \circ a \circ b \cup L_0 \circ u \\ &\quad \cup L_0 \circ a \circ u \cup L_0 \circ b \circ u \cup L_0 \circ (a \circ b) \circ u, \end{aligned} \tag{II.1}$$

which is a pairwise disjoint union. Therefore, for any $x = \sum_{l\in L} r_l l \in AL$,

$$x = (\sum_{l\in L} r_l)\theta + \sum_{l\in L} r_l(l - \theta),$$

we have

$$\begin{aligned} x &= (\sum_{l\in L} r_l)\theta + \sum_{l\in L_0} r_l(l-\theta) + \sum_{l\in L_0} r_{loa}(l\circ a - \theta) + \sum_{l\in L_0} r_{lob}(l\circ b - \theta) \\ &\quad + \sum_{l\in L_0} r_{lo(aob)}(l\circ(a\circ b) - \theta) + \sum_{l\in L_0} r_{lou}(l\circ u - \theta) \\ &\quad + \sum_{l\in L_0} r_{lo(aou)}(l\circ(a\circ u) - \theta) + \sum_{l\in L_0} r_{lo(bou)}(l\circ(b\circ u) - \theta) \\ &\quad + \sum_{l\in L_0} r_{lo((aob)ou)}(l\circ(a\circ b)\circ u) - \theta). \end{aligned}$$

By definition,

$$\begin{aligned} f(x) &= \sum_{l\in L} r_l + \sum_{l\in L_0} r_l \cdot l + \sum_{l\in L_0} r_{loa} \cdot l\circ a + \sum_{l\in L_0} r_{lob} \cdot l \circ b \\ &\quad + \sum_{l\in L_0} r_{lo(aob)} \cdot l\circ(a\circ b) + \sum_{l\in L_0} r_{lou} \cdot l\circ u \\ &\quad + \sum_{l\in L_0} r_{lo(aou)} \cdot l\circ(a\circ u) + \sum_{l\in L_0} r_{lo(bou)} \cdot l\circ(b\circ u) \end{aligned}$$

$$
\begin{aligned}
&+\sum_{l\in L_0} r_{lo((a\circ b)\circ u)}\cdot l\circ(a\circ b)\circ u)\\
=\;&\sum_{l\in L} r_l+\sum_{l\in L_0} r_l\cdot l+\sum_{l\in L_0} r_{loa}\cdot(l\cdot a+l+a)+\sum_{l\in L_0} r_{lob}\cdot(l\cdot b+l+b)\\
&+\sum_{l\in L_0} r_{lo(a\circ b)}\cdot(l\cdot(a\circ b)+l+(a\circ b))+\sum_{l\in L_0} r_{lou}\cdot(l\cdot u+l+u)\\
&+\sum_{l\in L_0} r_{lo(a\circ u)}\cdot(l\cdot(a\circ u)+l+a\circ u)+\sum_{l\in L_0} r_{lo(b\circ u)}\cdot(l\cdot(b\circ u)+l+b\circ u)\\
&+\sum_{l\in L_0} r_{lo((a\circ b)\circ u)}\cdot(l\cdot(a\circ b)\circ u)+l+(a\circ b)\circ u))\\
=\;&\sum_{l\in L} r_l+\sum_{l\in L_0}(r_l+r_{loa}+r_{lob}+r_{lo(a\circ b)}+r_{lou}+r_{lo(a\circ u)}+r_{lo(b\circ u)}+r_{lo((a\circ b)\circ u)})\cdot l\\
&+\sum_{l\in L_0} r_{loa}(l+1)a+\sum_{l\in L_0} r_{lob}(l+1)b\\
&+\sum_{l\in L_0} r_{lo(a\circ b)}(l+1)\cdot(a\circ b)+\sum_{l\in L_0} r_{lou}(l+1)u\\
&+\sum_{l\in L_0} r_{lo(a\circ u)}(l+1)\cdot(a\circ u)+\sum_{l\in L_0} r_{lo(b\circ u)}(l+1)\cdot(b\circ u)\\
&+\sum_{l\in L_0} r_{lo((a\circ b)\circ u)}(l+1)\cdot(a\circ b)\circ u.
\end{aligned}
$$

Suppose $f(x)=0$. By Lemma II.1, the coefficients of 1, a, b, $a\circ b$, u, $a\circ u$, $b\circ u$ and $(a\circ b)\circ u$ are zero. So,

$$
\begin{aligned}
&\sum_{l\in L} r_l+\sum_{l\in L_0}(r_l+r_{loa}+r_{lob}+r_{lo(a\circ b)}+\\
&+r_{lou}+r_{lo(a\circ u)}+r_{lo(b\circ u)}+r_{lo((a\circ b)\circ u)})\cdot l=0 \qquad \text{(II.2)}\\
&\sum_{l\in L_0} r_{loa}\cdot l=-\sum_{l\in L_0} r_{loa} \qquad \text{(II.3)}\\
&\sum_{l\in L_0} r_{lob}\cdot l=-\sum_{l\in L_0} r_{lob} \qquad \text{(II.4)}\\
&\sum_{l\in L_0} r_{lo(a\circ b)\cdot l}=-\sum_{l\in L_0} r_{lo(a\circ b)} \qquad \text{(II.5)}\\
&\sum_{l\in L_0} r_{lou}\cdot l=-\sum_{l\in L_0} r_{lou} \qquad \text{(II.6)}
\end{aligned}
$$

$$\sum_{l\in L_0} r_{lo(aou)}\cdot l = -\sum_{l\in L_0} r_{lo(aou)} \tag{II.7}$$

$$\sum_{l\in L_0} r_{lo(bou)}\cdot l = -\sum_{l\in L_0} r_{lo(bou)} \tag{II.8}$$

$$\sum_{l\in L_0} r_{lo((aob)ou)}\cdot l = -\sum_{l\in L_0} r_{lo((aob)ou)} \tag{II.9}$$

in A. Since

$$\sum_{l\in L} r_l = \sum_{l\in L_0}(r_l + r_{loa} + r_{lob} + r_{lo(aob)} + r_{lou} + r_{lo(aou)} + r_{lo(bou)} + r_{lo((aob)ou)}),$$

by substituting the equations II.3 to II.9 into equation II.2, we get

$$\sum_{l\in L_0} r_l\cdot l = -\sum_{l\in L_0} r_l. \tag{II.10}$$

Thus $x\in \ker(f)$ if and only if the coefficients of x satisfy equations II.3 to II.10. For any $x=\sum_{l\in L} r_l l \in AL$,

$$\begin{aligned} x &= (\sum_{l\in L} r_l)\theta + \sum_{l\in L} r_l(l-\theta) \\ &= (\sum_{l\in L} r_l)\theta + \sum_{l\in L_0} r_l(l-\theta) + \sum_{l\in L\setminus L_0} r_l(l-\theta). \end{aligned}$$

Therefore,

$$x^* = (\sum_{l\in L} r_l)\theta + \sum_{l\in L_0} r_l(l-\theta) + \sum_{l\in L\setminus L_0} r_l(-2)\circ(l-\theta).$$

Now

$$f(x) = \sum_{l\in L} r_l + \sum_{l\in L_0} r_l\cdot l + \sum_{l\in L\setminus L_0} r_l\cdot l,$$

$$f(x^*) = \sum_{l\in L} r_l + \sum_{l\in L_0} r_l\cdot l + \sum_{l\in L\setminus L_0} r_l\cdot(-2)\circ l,$$

and

$$\overline{f(x)} = \sum_{l\in L} r_l + \sum_{l\in L_0} r_l\cdot l + \sum_{l\in L\setminus L_0} r_l\cdot \bar{l}.$$

Since $\bar{l} = l^* = -2\circ l$, for $l\in L\setminus L_0$,

$$f(x^*) = \overline{f(x)}.$$

For any $x \in AL$, $tr(x) = x + x^*$ and $n(x) = xx^*$. So

$$f(tr(x)) = f(x + x^*) = f(x) + f(x^*) = f(x) + \overline{f(x)} = tr(f(x)),$$

$$f(n(x)) = f(xx^*) = f(x)f(x^*) = f(x)\overline{f(x)} = n(f(x)).$$

□

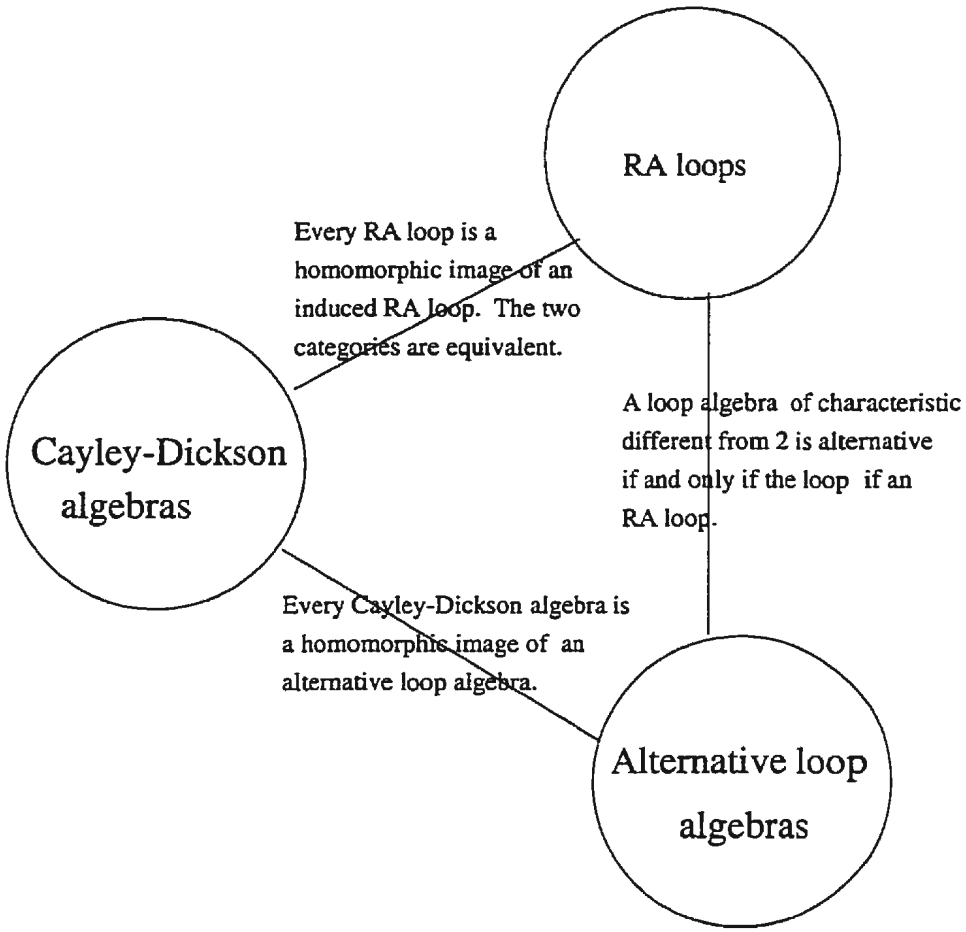

FIGURE II.1. Cayley-Dickson algebras, *RA* loops and alternative loop algebras

2. A further description of $\ker(f)$

Since every Cayley-Dickson algebra is a homomorphic image of an alternative loop algebra by Theorem II.2, the kernel of the map f is very important for connecting

the loop algebra to the Cayley-Dickson algebra. In this section we give a description of the elements in ker(f) in more detail.

THEOREM II.3. *Suppose A is a commutative associative ring with unity 1 and $2 \neq 0$. Let α, β and γ be elements in $U(A)$. Let AL be the alternative loop algebra of the induced RA loop L. Let L_0 be the center of L. Let I be the group generated by -1, α, β and γ in A. Then*

1. *The map $h\colon L_0 \mapsto I$ defined by*

$$h(x) = x + 1 \text{ for any } x \in L_0,$$

is a group isomorphism.

2.

$$\ker(f) = \{ \sum_{w \in T, l \in L_0} r_l^w l \circ w \in AL \mid \text{for any } w \in T, \sum_{l \in L_0} r_l^w \cdot h(l) = 0 \text{ in } A\}$$

where $T = \{\theta,\ a,\ b,\ a \circ b,\ u,\ a \circ u,\ b \circ u,\ (a \circ b) \circ u\}$.

3. *Let*

$$\Omega(AL_0) = \{\sum_{l \in L_0} r_l l \in AL_0 \mid \sum_{l \in L_0} r_l \cdot h(l) = 0 \text{ in } A\}.$$

Then $\Omega(AL_0)$ is an ideal of AL_0.

4. $\ker(f) = AL\Omega(AL_0) = \Omega(AL_0)AL$.

5. *If $L_0 = \{\theta,\ -2\}$ and $-2 \in U(A)$, then*

$$AL\Omega(AL_0) = ALe,$$

where $e = (1/2)(\theta + (-2))$.

PROOF. Since L is the induced RA loop, L_0 is the circle group generated by $\{\theta, -2, \alpha - 1, \beta - 1, \gamma - 1\}$ by Theorem I.4. By the formula $(x-1) \circ (y-1) = xy - 1$, we know that each element in L_0 is of the form θ, -2, $\alpha^{n_0}\beta^{n_1}\gamma^{n_2} - 1$, for some integers $n_i \in \mathbf{Z}$, $i = 0, 1, 2$. It is easy to check that the map from L_0 to I defined by

$$h(x) = x + 1, \text{ for } x \in L_0$$

is a group isomorphism from the circle group $(L_0, \circ)$ to the group $(I\ , \cdot)$. Because of equation II.1, each $x = \sum_{l \in L} r_l l$ can be expressed as

$$x = \sum_{w \in T} \sum_{l \in L_0} r_l^w l \circ w.$$

By Theorem II.2, we know that

$$\begin{aligned} x \in \ker(f) \quad &\iff \sum_{l \in L_0} r_l^w \cdot l = -\sum_{l \in L_0} r_l^w, \text{ for each } w \in T, \\ &\iff \sum_{l \in L_0} r_l^w \cdot (l+1) = \sum_{l \in L_0} r_l^w \cdot h(l) = 0, \text{ for each } w \in T. \end{aligned}$$

So statement 2 is true. Now we show that $\Omega(AL_0)$ is an ideal of AL_0. Let $\sum_{l \in L_0} r_l l \in \Omega(AL_0)$. Then $\sum_{l \in L_0} r_l \cdot h(l) = 0$ in A. We just need to show that $A\Omega(AL_0) \subseteq \Omega(AL_0)$ and $L_0\Omega(AL_0) \subseteq \Omega(AL_0)$.

For any $x \in A$, $x \sum_{l \in L_0} r_l l = \sum_{l \in L_0} x r_l l$ in AL_0, so

$$\sum_{l \in L_0} (x r_l) \cdot h(l) = x \sum_{l \in L_0} r_l \cdot h(l) = 0$$

in A, and so $x \sum_{l \in L_0} r_l l \in \Omega(AL_0)$. For any $x \in L_0$,

$$x \sum_{l \in L_0} r_l l = \sum_{l \in L_0} r_l (x \circ l),$$

and

$$\sum_{l \in L_0} r_l \cdot h(x \circ l) = \sum_{l \in L_0} r_l \cdot (h(x) \cdot h(l)) = h(x)(\sum_{l \in L_0} r_l \cdot h(l)) = 0,$$

so we have $L_0(\Omega(AL_0)) \subseteq \Omega(AL_0)$. Thus $\Omega(AL_0)$ is an ideal of AL_0.

Since $AL = \sum_{w \in T} AL_0 w$ and $AL_0 w = wAL_0$, for any $w \in T$, the above description of $\ker(f)$ gives us that $\ker(f) = AL\Omega(AL_0) = \Omega(AL_0)AL$. If $L_0 = \{\theta, \ -2\}$, then for any $r_\theta \theta + r_{-2}(-2) \in \Omega(AL_0)$, $r_\theta h(\theta) + r_{-2} h(-2) = r_\theta + r_{-2}(-1) = 0$ implies that $r_\theta = r_{-2}$, so $\Omega(AL_0) = A(\theta + (-2)) = Ae$, where $e = (1/2)(\theta + (-2))$.

□

3. Cayley-Dickson algebras, loop algebras and their radicals

In this section, we investigate properties of Cayley-Dickson algebras over group algebras by using the description of $\ker(f)$ in the previous section, and generalize some known results. As for the radicals of associative rings and alternative rings, we refer the reader to [**Div65, Sza81, ZSSS82**], for the radicals of group algebras and loop algebras, [**Kar87, JKW85, GJM96, Zho95**].

LEMMA II.4. *Let D be a commutative associative ring with $2 \in U(D)$, the unit group of D. Then*

$$D(\underbrace{C_2 \times \cdots \times C_2}_{n \text{ factors}}) \cong \underbrace{D \oplus \cdots \oplus D}_{2^n \text{ times}},$$

where C_2 is the group of two elements.

PROOF. Let $e = (1/2)(1 + c)$, where $1 \neq c \in C_2$. Then $e^2 = e \in DC_2$, and

$$DC_2 \cong De \oplus D(1 - e) \cong D \oplus D.$$

Since $D(\underbrace{C_2 \times \cdots \times C_2}_{n \text{ factors}}) = (D(\underbrace{C_2 \times \cdots \times C_2}_{n-1 \text{ factors}}))C_2$, and $D(\underbrace{C_2 \times \cdots \times C_2}_{n-1 \text{ factors}})$ is a commutative ring R with $2 \in U(R)$, the statement holds by induction on n. □

LEMMA II.5. *Let L be the RA loop induced by a Cayley-Dickson algebra $A(\alpha,\ \beta,\ \gamma)$ and AL be the induced loop algebra with $-2 \in U(A)$. Then*

1. *$e = (\theta + s)/2$ is a central element of the loop algebra AL.*
2. $(AL)e \cong \underbrace{A \oplus \cdots \oplus A}_{8 \text{ times}}$.
3. $$(AL)e \subseteq \ker(f) \text{ and } f(AL(\theta - e)) = A(\alpha,\ \beta,\ \gamma),$$
   where f is the map from AL to $A(\alpha, \beta, \gamma)$ defined in Theorem II.2.
4. *If $\ker(f) = (AL)e$ and L is a 2-loop, then the prime radical $P(A(\alpha, \beta, \gamma))$ of the Cayley-Dickson algebra is*

$$P(A) + P(A)i + P(A)j + P(A)ij + P(A)k + P(A)ik + P(A)jk + P(A)ij \cdot k,$$

and the Jacobson radical $J(A(\alpha, \beta, \gamma))$ of the Cayley-Dickson algebra $A(\alpha,\ \beta,\ \gamma)$ is

$$J(A) + J(A)i + J(A)j + J(A)ij + J(A)k + J(A)ik + J(A)jk + J(A)ij \cdot k.$$

PROOF. Since $s = -2 \in L_0$, $e = (\theta + s)/2$ is a central element in the loop algebra AL so

$$AL = (AL)e \oplus AL(\theta - e).$$

Recall that $L' = \{\theta,\ s\}$, the commutator subloop of the loop L with

$$L/L' \cong C_2 \times C_2 \times C_2.$$

Then we have

$$(AL)e \cong A(L/L') \cong A(C_2 \times C_2 \times C_2) \cong 8A$$

by Lemma II.4. Furthermore,

$$f(AL) = f(ALe) \oplus f(AL(\theta - e)) = A(\alpha, \beta, \gamma)f(e) \oplus A(\alpha, \beta, \gamma)f(\theta - e).$$

Since

$$f(e) = (1/2)f(\theta + s) = (1/2)f(2\theta + (s - \theta)) = (1/2)(2 + s) = (1/2)(2 - 2) = 0,$$

we have $f(\theta - e) = 1$. Therefore

$$(AL)e \subseteq \ker(f) \text{ and } f(AL(\theta - e)) = A(\alpha, \beta, \gamma).$$

As for the radicals, by [**GJM96**, Theorem 3.4, p.161], we know that if L is a torsion loop, then

$$J(AL) = J(A)L + \sum_{p \in P} J(A)_p \omega(L, L_p),$$

where P is the set of prime numbers.

Recall that for any ideal I of an algebra A and a positive integer n, I_n is the set of all elements $r \in R$ with $nr \in I$ [**GJM96**, p.157] and

$$J(A)_p = \{r \in J(A) \mid pr \in J(A)\}.$$

Since L is a 2-loop, $L_p = \theta$ if $p \neq 2$. But $2 \in U(A)$, so $J(A)_2 = J(A)$. Therefore,

$$J(AL) = J(A)L.$$

Let $B = AL(\theta - e)$. Then

$$AL = (AL)e \oplus AL(\theta - e) = \ker(f) \oplus B,$$

by the assumption that $\ker(f) = (AL)e$. Because the Jacobson radical is hereditary [**ZSSS82**],

$$J(B) = J(AL) \cap B = (J(A)L) \cap B.$$

Because $\ker(f) \cap B = 0$, f is an isomorphism from B to $A(\alpha, \beta, \gamma)$. Thus

$$J(A(\alpha, \beta, \gamma)) = f((J(A)L) \cap B) = f((J(A)L) \cap AL(\theta - e)).$$

Note that

$$J(A)L = (J(A)L)e \oplus (J(A)L)(\theta - e),$$

so $J(A)L \cap AL(\theta - e) = J(A)L(\theta - e)$. In fact, it is easy to see the right hand side is contained in the left hand side. For any $x \in J(A)L \cap AL(\theta - e)$, $x = x_1 e + x_2(\theta - e)$, where $x_1, x_2 \in J(A)L$. Since $x \in AL(\theta - e)$, $x_1 = 0$, so $x \in J(A)L(\theta - e)$. Therefore,

$$\begin{aligned}
J(A(\alpha, \beta, \gamma)) &= f((J(A)L) \cap B) \\
&= f(J(A)L(\theta - e)) \\
&= f(J(A)L(\theta - s)/2) \\
&= f(J(A)L) \quad (\text{since } f((\theta - s)/2) = 1)) \\
&= f(J(A)(L - \theta + \theta)) \\
&= f(J(A)(L - \theta) + J(A)) \\
&= f(J(A)(L - \theta)) + J(A) \text{ (by the definition of } f) \\
&= J(A) + J(A)a + J(A)b + J(A)a \circ b + J(A)u \\
&\quad + J(A)a \circ u + J(A)b \circ u + J(A)(a \circ b) \circ u \\
&= J(A) + J(A)i + J(A)j + J(A)ij + J(A)k + J(A)ik \\
&\quad + J(A)jk + J(A)ij \cdot k, \text{ (by Lemma II.1).}
\end{aligned}$$

In the same way, we can obtain the analogous property of the prime radical of the Cayley-Dickson algebra. □

REMARK II.6. In the above lemma, we see that $AL(\theta - e) \subset \omega(AL)$, so the part of the Cayley-Dickson algebra which is not associative is in the image of the augmentation ideal of the loop algebra AL.

The following is a generalization of [**dB93b**, Proposition 3.9] (see also [**GJM96**, p. 186]).

THEOREM II.7. *Suppose A is a commutative associative ring with unity 1 and $2 \in U(A)$, the unit group of A. Let $\alpha = \pm 1$, $\beta = \pm 1$ and $\gamma = \pm 1$. Let L be the RA loop induced by the Cayley-Dickson algebra $A(\alpha, \beta, \gamma)$. Then*

1. *L is an RA loop of order 16 and*

$$AL = \ker(f) \oplus B,$$

where $\ker(f) \cong 8A$, $B \cong A(\alpha, \beta, \gamma)$, and f is the map defined in Theorem II.2.

2. *The Jacobson radical of the Cayley-Dickson algebra $A(\alpha, \beta, \gamma)$ is*

$$J(A) + J(A)i + J(A)j + J(A)ij + J(A)k + J(A)ik + J(A)jk + J(A)ij \cdot k.$$

3. *The prime radical of the Cayley-Dickson algebra $A(\alpha, \beta, \gamma)$ is*

$$P(A) + P(A)i + P(A)j + P(A)ij + P(A)k + P(A)ik + P(A)jk + P(A)ij \cdot k.$$

PROOF. Since $\alpha = \pm 1$, $\beta = \pm 1$, $\gamma = \pm 1$, and L_0 is generated by θ, -2, $\alpha - 1$, $\beta - 1$ and $\gamma - 1$, we have $L_0 = \{\theta, -2\}$. Thus L has 16 elements and it is a 2-loop. Let $e = (\theta + (-2))/2$. By Theorem II.3 (3), (4) and (5), $(AL)e = \ker(f)$. Since $AL = (AL)e \oplus (AL)(\theta - e)$, the remaining statements follow from Lemma II.5. □

4. Quaternion algebras and *RA* groups

If we remove k and u in the results of the previous chapter and this chapter, we have corresponding results about quaternion algebras and RA groups, which is a generalization of the quaternion group. We just mention the results here.

THEOREM II.8. *(Generalized Quaternion Algebras) Let R be a commutative associative ring with unity 1 and $2 \neq 0$ in R. Let A be a commutative associative R-algebra. Let α and β be in A. Then we have a generalized quaternion algebra*

$$B = A + Ai + Aj + Aij$$

where $i^2 = \alpha$, $j^2 = \beta$ and the multiplication table of the i, j is the same as the old one. The associative algebra B is called the generalized quaternion algebra and denoted by $A(\alpha, \beta)$.

Some ring properties of generalized quaternion rings were investigated by A. A. Tuganbaev in [**Tug92, Tug93**].

THEOREM II.9. *Let A be a commutative associative R-algebra with unity 1 and $2 \neq 0$. Let $\alpha - 1$ and $\beta - 1$ be elements in $Quasi(A)$. Let*

$$A(\alpha, \beta) = A + Ai + Aj + Aij$$

be the quaternion algebra in which $i^2 = \alpha$ and $j^2 = \beta$.

1. *Let $Quasi(A(\alpha, \beta))$ be the circle group of $A(\alpha, \beta)$. Let $a = i - 1$ and $b = j - 1$. Then $a, b \in Quasi(A(\alpha, \beta))$. Let G_0 be the subgroup of $Quasi(A)$ which is generated by $\{\theta, -2, \alpha - 1, \beta - 1\}$. Then*

   $$G = G_0 \circ \langle a \rangle \circ \langle b \rangle$$

   is an RA group.
2. *$H = Quasi(A) \circ \langle a \rangle \circ \langle b \rangle$ is an RA group, in which -2 is the unique nonzero commutator-associator.*
3. *The RA group H contains G and G is the smallest RA subgroup of H that contains the elements a and b.*

THEOREM II.10. *Let AG be the group algebra of G over A, where G is the circle RA group induced by the quaternion algebra $A(\alpha, \beta)$. Then $AG = A\theta \oplus \omega(AG)$, the direct sum of A-modules, where $\omega(AG)$ is the augmentation ideal of AG and θ is the unity of the group G. Let f the map from AG to $A(\alpha, \beta)$ defined by*

$$f(r\theta + \sum_{l \in G} r_l l) = r + \sum_{l \in G} r_l \cdot l,$$

where $r \in A$ and $\sum_{l \in G} r_l l \in \omega(AG)$. Then f is an A-algebra homomorphism from AG onto $A(\alpha, \beta, \gamma)$, and

$$AG / \ker(f) \cong A(\alpha, \beta)$$

as A-algebras. Thus, every generalized quaternion algebra is a quotient algebra of an RA group algebra. The kernel of f is

$$\{\sum_{l \in G} r_l l \mid \sum_{l \in G_0} r_{low} \cdot l = -\sum_{l \in G_0} r_{low}, \forall r_{low} \in A, \forall l \in G_0, \forall w = \theta, a, b, a \circ b\}.$$

CHAPTER III

Moufang circle loops and loop algebras

From [**Goo87**] Theorem 1 we know that the set of all the quasi-regular elements of an alternative algebra A is a Moufang loop under the circle operation. We call it the Moufang circle loop $Quasi(A)$ of the alternative algebra A. From the previous chapters we know that an RA loop can be the Moufang circle loop of an alternative algebra and the Moufang circle loop of any Cayley-Dickson algebra contains an RA subloop. In this chapter, we investigate the relationships between the alternative algebra, its Moufang circle loop and the loop algebra of the circle loop.

1. Moufang circle loops and loop algebras

Let L be the circle loop of an alternative R-algebra A, where R is a commutative associative ring with unity. Recall that the circle operation on A is defined by

$$a \circ b = ab + a + b,$$

where $a,\ b \in A$. The 0 of the algebra A is the identity element of the circle loop $Quasi(A)$. We use θ instead of 0 to denote the identity of $Quasi(A)$. In this section we investigate the relationship between the algebras and their circle loops.

THEOREM III.1. *Let $L = Quasi(A)$ be the Moufang circle loop of an alternative R-algebra A and let RL be the loop algebra of the loop L over the commutative associative ring R. We define a map ρ from RL to A by*

$$\rho\colon \sum_{l\in L} r_l l \mapsto \sum_{l\in L} r_l \cdot l$$

where $r_l \in R$, and $l \in L$. Then

1. *ρ is an R-module homomorphism from RL to A.*
2. *$\rho\,|_{\omega(RL)}$ is an R-algebra homomorphism from the algebra $\omega(RL)$ to the algebra A.*

3. *Let $K = \omega(RL) \cap \ker(\rho)$. Then K is an ideal of the loop algebra RL, and $\omega(RL)/K$ is isomorphic to a subalgebra of A. If A is a Jacobson radical algebra, that is, every element of A is quasiregular, then*

$$\omega(RL)/K \cong A$$

as R-algebras.

PROOF. By the definition of the loop algebra and the definition of ρ, the first statement is not hard to check.

For the second statement, we should be careful. The augmentation ideal $\omega(RL)$ is a free R-module with basis

$$\{l - \theta \mid l \in L\},$$

where θ is the identity element of the loop L. For any $\alpha = \sum_{l\in L} r_l(l-\theta) \in \omega(RL)$, $\beta = \sum_{h\in L} t_h h(h-\theta) \in \omega(RL)$, we have

$$\begin{aligned}
\alpha\beta &= (\sum_{l\in L} r_l(l-\theta)) \cdot (\sum_{h\in L} t_h(h-\theta)) \\
&= \sum_{l\in L, h\in L} r_l t_h (l-\theta)\cdot(h-\theta) \\
&= \sum_{l\in L, h\in L} r_l t_h (l\circ h - l\circ\theta - h\circ\theta + \theta\circ\theta) \\
&= \sum_{l\in L, h\in L} r_l t_h (l\circ h - l - h + \theta).
\end{aligned}$$

Therefore

$$\begin{aligned}
\rho(\alpha\beta) &= \sum_{l\in L, h\in L} (r_l t_h)\cdot(l\circ h - l - h + 0) \\
&= \sum_{l\in L, h\in L} (r_l t_h)\cdot(lh + l + h - l - h) \\
&= \sum_{l\in L, h\in L} (r_l t_h)\cdot(lh) \\
&= (\sum_{l\in L} r_l l)(\sum_{h\in L} t_h h) \\
&= \rho((\sum_{l\in L} r_l(l-\theta))(\sum_{h\in L} t_h(h-\theta)))
\end{aligned}$$

Therefore, the map ρ is an R-algebra homomorphism from $\omega(RL)$ to A. Next we show that K is an ideal of the loop algebra RL.

It is easy to verify that the augmentation ideal $\omega(RL)$ is an ideal of the loop algebra RL. To show that K is an ideal we just show that the product of any element from the loop algebra and an element in K is in the kernel of the map ρ. Assume that

$$\sum_{l\in L} r_l l \in K = \omega(RL) \cap \ker(\rho).$$

Then for any h in L, we have

$$\begin{aligned}(\sum_{l\in L} r_l l)h &= \sum_{l\in L} r_l l \circ h \\ &= \sum_{l\in L} r_l l(h-\theta) + \sum_{l\in L} r_l l \circ \theta \\ &= \sum_{l\in L} r_l l(h-\theta) + \sum_{l\in L} r_l l\end{aligned}$$

Because ρ is an R-algebra homomorphism from $\omega(RL)$ to A, we have

$$\begin{aligned}\rho((\sum_{l\in L} r_l l)h) &= \rho(\sum_{l\in L} r_l l(h-\theta)) + \rho(\sum_{l\in L} r_l l) \\ &= \rho(\sum_{l\in L} r_l l)\rho(h-\theta) + 0 \\ &= 0 \cdot \rho((h-\theta) + 0 \\ &= 0.\end{aligned}$$

Therefore, $(\sum_{l\in L} r_l l)h \in K$. So, for any $\sum_{h\in L} t_h h \in RL$, we have that

$$(\sum_{l\in L} r_l l)(\sum_{h\in L} t_h h) = \sum_{l\in L, h\in L} r_l t_h l \circ h = \sum_{h\in L}(\sum_{l\in L} t_h r_l l)h \in K.$$

So K is a right ideal of RL. In the same way, we can obtain that K is a left ideal.

For the case when A is a Jacobson radical algebra, we must show that ρ is surjective from $\omega(RL)$ to A for then the map ρ induces an isomorphism from $\omega(RL)/K$ to A. In fact, ρ is surjective because for any $a \in A$ we have $a - \theta \in \omega(RL)$ and $\rho(a-\theta) = a - 0 = a$.

□

2. The augmentation ideal of the loop algebra of an RA loop

In this section we will investigate the augmentation ideals of the loop algebra of an RA loop and an RA circle loop. For the definition and properties of the RA loop, cf [**GJM96**]. Here we just recall that the unique commutator-associator s defines an anti-automorphism on the loop L and can be extended to an anti-automorphism of the loop ring RL denoted by $*$.

PROPOSITION III.2. *Let R be a commutative associative ring with unity and let L be an RA loop and assume that*

$$L = M(G, *, g_0) = G \cup Gu.$$

Then the loop ring

$$RL = RG + RGu$$

is a direct sum of RG-modules. For any ideal I of the group algebra RG,

$$(I + Iu) \text{ is an ideal of } RL \iff I^* \subseteq I \iff I^* = I.$$

PROOF. The claim that $RL = RG + RGu$ is a direct sum of RG-modules follows from the structure of the RA loop. We just show the second claim. Assume that I is an ideal of the group algebra RG such that $I^* = I$. It is easy to check that $(I+Iu, +)$ is an abelian group. For any $x + yu \in RL$, where x and y are two elements in the group algebra RG, and for any $a, b \in I$, we have

$$(a + bu)(x + yu) = (ax + g_0 y^* b) + (ya + bx^*)u.$$

Since a and b are in I, an ideal of RG, then ax, $g_0 y^* b$, ya and bx^* are in I. Hence

$$(a + bu)(x + yu) \in I + Iu.$$

For right multiplication, we have

$$(x + yu)(a + bu) = (xa + g_0 b^* y) + (bx + ya^*)u.$$

Since $I^* = I$, $b^* \in I$ and $a^* \in I$. Thus xa, $g_0 b^* y$, bx and ya^* are all in I. So $(x + yu)(a + bu) \in I + Iu$. Thus $I + Iu$ is an ideal of the loop algebra RL.

Now assume that I is an ideal of the group algebra RG, and $I+Iu$ is an ideal of the loop algebra RL. We show that I is fixed under the map $*$. For any $a = \sum_{g\in G} r_g g \in I$, ua is in the ideal $I + Iu$. While $ua = \sum_{g\in G} r_g ug = (\sum_{g\in G} r_g g^*)u$, so

$$(ua)u = ((\sum_{g\in G} r_g g^*)u)u = (\sum_{g\in G} r_g g^*)u^2 = (\sum_{g\in G} r_g g^*)g_0 \in I.$$

Therefore

$$(\sum_{g\in G} r_g g^*)g_0 g_0^{-1} = \sum_{g\in G} r_g g^* = (\sum_{g\in G} r_g g)^* \in I.$$

Thus $I^* \subseteq I$. Since the map $*$ is an involution of the loop algebra, we have

$$I = (I^*)^* \subseteq I^*,$$

thus $I = I^*$, and I is fixed under the map $*$. □

COROLLARY III.3. *Let L be an RA loop with $L = M(G, *, g_0)$ and let R be a commutative associative ring with* 1. *Then*

$$\omega(RG) + \omega(RG)u \text{ is an ideal of } RL \text{ and } \omega(RG) + \omega(RG)u \subseteq \omega(RL).$$

PROOF. Since $(\omega(RG))^* = \omega(RG)$, the result follows. □

An interesting result about the augmentation ideal of the loop algebra of an *RA* loop is the following, which describes the augmentation ideal of the loop algebra by its group algebra.

PROPOSITION III.4. *([**GJM96**] Lemma 1.1, p.150) Let L be an RA loop with $L = M(G, *, g_0)$ and let R be a commutative associative ring with unity. Then*

$$\omega(RL) = \omega(RG) + RG(1 - u).$$

PROOF. It is obvious that $\omega(RG) + RG(1 - u) \subseteq \omega(RL)$. On the other hand, if $\sum_{l\in L} r_l l \in \omega(RL)$, then $\sum_{l\in L} r_l = 0$ by the definition of the augmentation ideal. Since

$$RL = RG + RGu,$$

we can assume that

$$\sum_{l\in L} r_l l = \sum_{g\in G} r_g g + \sum_{h\in G} t_h hu,$$

where $\sum_{g\in G} r_g g, \sum_{h\in G} t_h h \in RG$. Since $\sum_{l\in L} r_l = 0$, we have

$$\sum_{g\in G} r_g + \sum_{h\in G} t_h = 0.$$

Then

$$\begin{aligned}
\sum_{l\in L} r_l l &= \sum_{g\in G} r_g g + \sum_{h\in G} t_h hu \\
&= \sum_{g\in G} r_g g + \sum_{h\in G} t_h h + \sum_{h\in G} t_h hu - \sum_{h\in G} t_h h \\
&= (\sum_{g\in G} r_g g + \sum_{h\in G} t_h h) + \sum_{h\in G} t_h h(u-1) \\
&\subseteq \omega(RG) + RG(u-1) \\
&= \omega(RG) + RG(1-u)
\end{aligned}$$

□

Since $RG = R + \omega(RG)$, $RG(1-u) = R(1-u) + \omega(RG)(u-1)$. Then we have another version of the proposition:

$$\begin{aligned}
\omega(RL) &= \omega(RG) + RG(1-u) \\
&= \omega(RG) + R(1-u) + \omega(RG)(1-u) \\
&= \omega(RG) + \omega(RG)u + R(1-u).
\end{aligned}$$

Therefore, we have the following:

COROLLARY III.5. *Let L be an RA loop with $L = M(G, *, g_0)$. Let R be a commutative ring with unity. Then*

$$\omega(RG) + \omega(RG)u = \omega(RG) + \omega(RG)(1-u)$$

$$\omega(RL) = \omega(RG) + RG(1-u) = \omega(RG) + \omega(RG)u + R(1-u).$$

3. Moufang circle loops and RA circle loops

In this section we investigate some basic properties of the Moufang circle loop and then investigate some basic properties of RA loops by using the results of the previous sections.

PROPOSITION III.6. *Let L be a Moufang loop and let $\omega(RL)$ be the augmentation ideal of the loop algebra RL, where R is a commutative ring with* 1. *Then L is a subloop of the circle loop of the algebra $\omega(RL)$.*

PROOF. Define the map $f: L \to \omega(RL)$ by

$$f(l) = l - 1,$$

for any $l \in L$. Then this is an injective map from L to $(\omega(RL), \circ)$. □

PROPOSITION III.7. *All finite RA 2-loops are subloops of the Moufang circle loops of nilpotent alternative rings of characteristic* 2.

PROOF. By [**Goo95**], for the finite RA 2-loops L, the augmentation ideal of the loop algebra F_2L is nilpotent, where F_2 is a field of characteristic 2. Since F_2L is an alternative algebra, [**Goo87**] Theorem 1 tells us that $(\omega(F_2L), \circ)$ is a Moufang loop. Then the result follows the Proposition III.6. □

Now we discuss alternative algebras with an RA loop as a subloop of its Moufang circle loop. From the first chapter we know that all Cayley-Dickson algebras are of this sort.

Let A be an alternative R-algebra with $Quasi(A)$ having an RA subloop L. Then the loop ring RL is an R-algebra and it is an alternative algebra because L is an RA loop. Recall the definition of ρ (cf Theorem III.1) from RL to A:

$$\rho(\sum_{l \in L} r_l \cdot l) = \sum_{l \in L} r_l l,$$

for any $\sum_{l \in L} r_l \cdot l \in RL$.

Since L is an RA loop, we can assume $L = M(G, *, g_0)$ by the structure theorem of RA loops. In determining if an RA loop is the circle loop of a Jacobson radical algebra, the RA group G plays an important role since L is a kind of extension of the group G.

From section 1 we know that the properties of the augmentation ideal $\omega(RL)$ and the map ρ are essential for the loop to be a circle loop, while from section 2 we know that

$$\omega(RL) = \omega(RG) + \omega(RG)u + R(1 - u).$$

Thus we should investigate the relationships between the two augmentation ideals and the map ρ, and its restrictions on some subrings. We need the following lemma:

LEMMA III.8. 1. $(\omega(RG)u) \cap \ker(\rho) = (\omega(RG) \cap \ker(\rho))u$;
2. *If* $x + yu \in \ker(\rho)$, *where* $x, y \in \omega(RG)$, *then*

$$x \in \ker(\rho) \Longleftrightarrow y \in \ker(\rho);$$

$$x^* \in \ker(\rho) \Longleftrightarrow y^* \in \ker(\rho).$$

PROOF. Let us show the first statement. To prove that the right hand side is included in the left hand side, first note that

$$(\omega(RG) \cap \ker(\rho))u \subseteq \omega(RG)u,$$

and second, for any $x \in \omega(RG) \cap \ker(\rho)$, because ρ is an algebra homomorphism from $\omega(RL)$ to A by Theorem III.1,

$$\rho(xu) = \rho(x(u-1)+x) = \rho(x)\rho(u-1) + \rho(x) = 0 \text{ since } \rho(x) = 0,$$

therefore $\rho(xu) = 0$, and

$$(\omega(RG) \cap \ker(\rho))u \subseteq \ker(\rho).$$

Now let us show that the left hand side is in the right hand side. If $x \in \omega(RG)$, and $xu \in \ker(\rho)$, then $xu = x(u-1) + x$ and then

$$0 = \rho(xu) = \rho(x)\rho(u-1) + \rho(x) = \rho(x)u + \rho(x).$$

Therefore,

$$\rho(x)u + \rho(x) + u = u$$

so that

$$\rho(x) \circ u = u.$$

Since $\rho(x)$ and u are in the alternative algebra A diassociativity of the algebra implies the two elements generate an associative algebra. Since $u \in Quasi(A)$, $\rho(x) \circ u = u$ implies that $\rho(x) = 0$ in the ring. Then $x \in \ker(\rho)$. Thus

$$xu \in (\omega(RG) \cap \ker(\rho))u.$$

For the second statement, we just check it by the definition of the map ρ. For any elements x and y in $\omega(RG)$ with $x+yu \in \ker(\rho)$, since $x+yu = x+y+y(u-1)$, and ρ is an algebra homomorphism from $\omega(RL)$ to A, we have:

$$0 = \rho(x+yu) = \rho(x+y+y(u-1)) = \rho(x)+\rho(y)+\rho(y)u.$$

Therefore,

$$\rho(y)u+\rho(x)+\rho(y)+u = u$$

and

$$\rho(y)\circ u+\rho(x) = u.$$

Thus

$$x \in \ker(\rho) \Longleftrightarrow \rho(x) = 0 \Longleftrightarrow \rho(y)\circ u = u \Longleftrightarrow \rho(y) = 0 \Longleftrightarrow y \in \ker(\rho).$$

Now we show $x^* \in \ker(\rho) \Longleftrightarrow y^* \in \ker(\rho)$. By Theorem III.1, $\ker(\rho) \cap \omega(RL)$ is an ideal of the loop ring RL. If $x+yu \in \ker(\rho)$, where $x, y \in \omega(RG)$, then $x+yu \in \ker(\rho) \cap \omega(RL)$, and so

$$(x+yu)u \in \ker(\rho) \cap \omega(RL) \subseteq \ker(\rho).$$

Thus $(x+yu)u = y^*g_0 + x^*u \in \ker(\rho)$. Note that $x^*, y^* \in \omega(RG)$. So by the above argument, we know that

$$x^* \in \ker(\rho) \Longleftrightarrow y^*g_0 \in \ker(\rho).$$

Since $y^*g_0 = y^*(g_0-1)+y^*$, then

$$\begin{aligned} y^*g_0 \in \ker(\rho) &\Longleftrightarrow \rho(y^*)\rho(g_0-1)+\rho(y^*) = 0 \\ &\Longleftrightarrow \rho(y^*)g_0+\rho(y^*)+g_0 = g_0 \\ &\Longleftrightarrow \rho(y^*)\circ g_0 = g_0 \\ &\Longleftrightarrow \rho(y^*) = 0. \end{aligned}$$

Therefore

$$x^* \in \ker(\rho) \Longleftrightarrow y^* \in \ker(\rho).$$

□

Now we can show our main result:

THEOREM III.9. *Let R be a commutative associative ring with 1. Let A be an alternative R-algebra with Quasi(A) having an RA subloop L. Let G be an RA group of L with $L = G \cup G \circ u$. Let RL be the loop ring of L over R. Define*

$$\rho\colon RL \to (A, +, \cdot)$$

by

$$\sum_{l\in L} r_l l \longrightarrow \sum_{l\in L} r_l \cdot l,$$

for any element $\sum_{l\in L} r_l l$ in the loop algebra RL. Then

1. $\ker(\rho) \cap \omega(RG) + (\ker(\rho) \cap \omega(RG))u$ *is an ideal of the loop algebra RL.*
2. $(\ker(\rho) \cap \omega(RG))^* = \ker(\rho) \cap \omega(RG)$.

PROOF. By Theorem III.1, the restriction of ρ to the subring $\omega(RL)$ is an algebra homomorphism from $\omega(RL)$ to A. Now consider the restriction of ρ to $\omega(RG)$. It is an algebra homomorphism from $\omega(RG)$ to A and the kernel is $\ker(\rho)\cap\omega(RG)$. Therefore $\ker(\rho) \cap \omega(RG)$ is an ideal of $\omega(RG)$. Since $RG = \omega(RG) + R$, $\ker(\rho) \cap \omega(RG)$ is an ideal of RG.

Next we show that

$$\ker(\rho) \cap \omega(RG) + (\ker(\rho) \cap \omega(RG))u$$

is an ideal of the loop ring RL. Again, since $RL = \omega(RL) + R$, it is sufficient to show that $\ker(\rho)\cap\omega(RG) + (\ker(\rho)\cap\omega(RG))u$ is an ideal of $\omega(RL)$. Working in the subring $\omega(RL)$ we can take advantage of the fact that ρ is an algebra homomorphism instead of a module homomorphism.

For any $x_0 \in \ker(\rho) \cap \omega(RG)$ and for any $x + yu \in \omega(RL)$, we have

$$\rho(x_0(x + yu)) = \rho(x_0)\rho(x + yu) = 0.$$

So

$$x_0x + (yx_0)u \in \ker(\rho).$$

Also $\rho(x_0x) = 0$ because x_0x is in the ideal $\ker(\rho) \cap \omega(RG)$. So

$$\rho(yx_0) = 0$$

by Lemma III.8. Thus,

$$x_0(x + yu) = x_0x + (yx_0)u \in \ker(\rho) \cap \omega(RG) + (\ker(\rho) \cap \omega(RG))u.$$

Now

$$(x+yu)x_0 = xx_0 + yx_0^*u.$$

Since $\rho(xx_0) = 0$, $\rho(yx_0^*) = 0$ by Lemma III.8. Therefore,

$$(x+yu)x_0 \in \ker(\rho) \cap \omega(RG) + (\ker(\rho) \cap \omega(RG))u.$$

As for $(x+yu)x_0u$, we have

$$(x+yu)x_0u = (x_0x)u + x_0^*yg_0.$$

Again, by Lemma III.8, $x_0x \in \ker(\rho)$ implies that $x_0^*yg_0 \in \ker(\rho)$. Hence

$$(x+yu)x_0u \in \ker(\rho) \cap \omega(RG) + (\ker(\rho) \cap \omega(RG))u.$$

Similarly, we have

$$x_0u(x+yu) = x_0x^*u + y^*x_0g_0.$$

Therefore

$$x_0u(x+yu) \in \ker(\rho) \cap \omega(RG) + (\ker(\rho) \cap \omega(RG))u.$$

Thus

$$\ker(\rho) \cap \omega(RG) + (\ker(\rho) \cap \omega(RG))u$$

is an ideal of RL. Since it is an ideal of the loop ring RL and $\ker(\rho) \cap \omega(RG)$ is an ideal of RG, Proposition III.2 tells us that the ideal $\ker(\rho) \cap \omega(RG)$ is fixed under the map $*$. So the second statement is true. □

COROLLARY III.10. *Suppose that* $x+yu \in \ker(\rho)$, *where* x *and* $y \in \omega(RG)$. *Then*

$$x \in \ker(\rho) \iff y \in \ker(\rho) \iff x^* \in \ker(\rho) \iff y^* \in \ker(\rho).$$

For any $\sum_{g\in G} r_g g \in RG$,

$$\sum_{g\in G} r_g g = 0 \iff \sum_{g\in G} r_g g^* = 0.$$

where the multiplication is in the ring A.

PROOF. It follows from Lemma III.8 and Theorem III.9 because

$$x \in \ker(\rho) \iff x^* \in \ker(\rho).$$

The second statement of the corollary follows. □

CHAPTER IV

RA circle loops

1. Introduction and some definitions

As mentioned in the introduction of this thesis, we will investigate the necessary and sufficient conditions for an RA loop to be a Moufang circle loop of an alternative quasiregular algebra, i.e., an alternative Jacobson radical ring. Furthermore, we give the algebraic structure of finite nilpotent alternative algebras whose Moufang circle loops are RA loops. In this chapter, an RA circle loop means the Moufang circle loop, which is an RA loop, of a quasiregular alternative algebra.

Since Artin's Theorem will be used later in this thesis, we record it here [**Sch66**, Theorem 3.1]:

THEOREM IV.1. *(Artin) The subalgebra generated by any two elements of an alternative algebra is associative.*

We cite some nice results about nilpotent groups here. As for the group and nilpotent group theory, we refer the reader to [**Hal59, Rob82, Rot95, Khu93**].

PROPOSITION IV.2. [**AW73, Kum94**] *Let G be a finite nilpotent group of class 2. Then G is the circle group of a nilpotent ring of nilpotency index 3.*

Recall that if G is a group with $G/\mathcal{Z}(G) \cong C_2 \times C_2$, G is called an RA group, where $\mathcal{Z}(G)$ is the center of group G and C_2 is the cyclic group of order 2. Since an RA group is a nilpotent group of class 2, from the above result we have:

COROLLARY IV.3. *A finite RA group is the circle group of an associative nilpotent ring of index 3.*

PROOF. This proof is a modification of that given in [**Kum94**]. By the definition $G/\mathcal{Z}(G) \cong C_2 \times C_2$, we can assume that

$$G = \mathcal{Z}(G) \cup \mathcal{Z}(G)a \cup \mathcal{Z}(G)b \cup \mathcal{Z}(G)ab$$

with $a^2 \in \mathcal{Z}(G)$ and $b^2 \in \mathcal{Z}(G)$. Therefore, for any $g \in G$, $g \in \mathcal{Z}(G)a^i b^j$, where $i, j = 0, 1$.

Now for any $g, h \in G$, we can define the following binary relation m on G by

$$m(g,h) = (a,b)^{i_g \cdot j_h}$$

and

$$g + h = hgm(g,h)$$

$$g \times h = m(g,h)$$

where (a,b) is the group commutator of the two elements a and b in the group G. Then it is not very hard to check that $(G, +, \times)$ is an associative ring with nilpotency index 3, and most importantly, $(G, \circ) = (G, \cdot)$. □

2. Necessary conditions for an *RA* loop to be a circle loop

In this section, the basic algebraic properties of *RA* circle loops are studied. The main results are Theorem IV.6 and Theorem IV.8. To prove these we need some lemmas.

LEMMA IV.4. *Let $(L, \circ)$ be the Moufang circle loop of an alternative quasi-regular ring $(A, +, \cdot)$. Note that as sets, $L = A$. Let S be a subset of L and K be a subring of $(A, +, \cdot)$ with the properties that*

$$(K, K, S) = (S, K, K) = (K, S, K) = 1$$

in the loop $(L, \circ)$. Then the set

$$C_K(S) = \{k \in K \mid k \circ s = s \circ k, \forall s \in S\} = \{k \in K \mid ks = sk, \forall s \in S\}$$

is a subring of $(A, +, \cdot)$.

PROOF. Since K is a subring of $(A, +, \cdot)$, $0 = \theta \in K$, the unity of the loop $(L, \circ)$. This also implies that $C_K(S) \neq \emptyset$. For any two elements k_1 and $k_2 \in C_K(S)$, we show that (1) $k_1 \pm k_2 \in C_K(S)$ and (2) $k_1 \cdot k_2 \in C_K(S)$, so that $C_K(S)$ is a subring of A. We have $k_1 \pm k_2$ and $k_1 \cdot k_2$ in K because K is a subring. In what follows, we use extensively the identity:

$$x \circ y - y \circ x = xy - yx$$

for any x, $y \in A$.

(1). For any $s \in S$, we have

$$\begin{aligned}(k_1 \pm k_2) \circ s - s \circ (k_1 \pm k_2) &= (k_1 \pm k_2) \cdot s - s \cdot (k_1 \pm k_2) \\ &= (k_1 \cdot s - s \cdot k_1) \pm (k_2 \cdot s - s \cdot k_2) \\ &= (k_1 \circ s - s \circ k_1) \pm (k_2 \circ s - s \circ k_2) \\ &= 0\end{aligned}$$

The last step follows from the definition of $C_K(S)$.

(2). By the assumption of the lemma, we have

$$\begin{aligned}(k_1 \circ k_2) \circ s &= k_1 \circ (k_2 \circ s)(\text{ since } (K, K, S) = 1) \\ &= k_1 \circ (s \circ k_2)(\text{ since } k_2 \in C_K(S)) \\ &= (k_1 \circ s) \circ k_2(\text{ since } (K, S, K) = 1) \\ &= (s \circ k_1) \circ k_2(\text{ since } k_1 \in C_K(S)) \\ &= s \circ (k_1 \circ k_2)(\text{ since } (S, K, K) = 1)\end{aligned}$$

Thus $(k_1 \circ k_2) \circ s = s \circ (k_1 \circ k_2)$. Because

$$x \circ y = y \circ x \Longleftrightarrow xy = yx,$$

then

$$(k_1 \circ k_2) \cdot s = s \cdot (k_1 \circ k_2) \Longleftrightarrow (k_1 \circ k_2) \circ s = s \circ (k_1 \circ k_2).$$

We have

$$(k_1 \circ k_2) \cdot s = (k_1 k_2 + k_1 + k_2) \cdot s = k_1 k_2 \cdot s + k_1 s + k_2 s,$$

and

$$s \cdot (k_1 \circ k_2) = s \cdot (k_1 k_2 + k_1 + k_2) = s \cdot k_1 k_2 + s k_1 + s k_2.$$

By comparing the above two equalities using the fact that

$$k_i s = s k_i, \text{ i=0, 1,}$$

for any $s \in S$, we have

$$k_1 k_2 \cdot s = s \cdot k_1 k_2.$$

Hence $k_1 k_2 \in C_K(S)$. □

LEMMA IV.5. *Let G be an RA group with $G = \mathcal{Z}(G) \circ \langle a \rangle \circ \langle b \rangle$. Then*

$$C_G(a) = \mathcal{Z}(G) \circ \langle a \rangle, \text{ and } C_G(b) = \mathcal{Z}(G) \circ \langle b \rangle.$$

PROOF. By the definition of $C_G(a)$, we have that

$$C_G(a) \supseteq \mathcal{Z}(G) \circ \langle a \rangle.$$

Because a and b do not commute in the group,

$$G \supset C_G(a).$$

Therefore, $[G : C_G(a)] > 1$. On the other hand, for the subgroup $\mathcal{Z}(G) \circ \langle a \rangle$, G has two cosets, $\mathcal{Z}(G) \circ \langle a \rangle$ and $\mathcal{Z}(G) \circ \langle a \rangle \circ b$ since $b^2 \in \mathcal{Z}(G)$. Hence

$$2 = [G\colon \mathcal{Z}(G) \circ \langle a \rangle] = [G : C_G(a)][C_G(a)\colon \mathcal{Z}(G) \circ \langle a \rangle].$$

We must have

$$[C_G(a)\colon \mathcal{Z}(G) \circ (a)] = 1.$$

Then the result follows. Following the same argument, $C_G(b) = \mathcal{Z}(G) \circ \langle b \rangle$. □

THEOREM IV.6. *Let $(L, \circ)$ be an RA circle loop of an alternative quasi-regular ring $(A, +, \cdot)$. Let a, b and u be any three elements in the loop $(L, \cdot)$ which do not associate. Then*

1. *$(\mathcal{Z}(L), +, \cdot)$ is an associative commutative quasi-regular subring of the ring $(A, +, \cdot)$ with circle subgroup $(\mathcal{Z}(L), \circ)$.*
2. *$(\mathcal{Z}(L) \circ \langle a \rangle, +, \cdot)$, $(\mathcal{Z}(L) \circ \langle b \rangle, +, \cdot)$ and $(\mathcal{Z}(L) \circ \langle u \rangle, +, \cdot)$ are associative commutative quasi-regular subrings of $(A, +, \cdot)$ with circle subgroups $(\mathcal{Z}(L) \circ \langle a \rangle, \circ)$, $(\mathcal{Z}(L) \circ \langle b \rangle, \circ)$ and $(\mathcal{Z}(L) \circ \langle u \rangle, \circ)$, respectively.*
3. *Let G be the RA group $\mathcal{Z}(L) \circ \langle a \rangle \circ \langle b \rangle$. Then $(G, +, \cdot)$ is an associative quasi-regular subring of $(A, +, \cdot)$ with circle subgroup $(G, \circ)$.*
4. *We have the following subring chains*

$$(\mathcal{Z}(L), +, \cdot) \subset (\mathcal{Z}(L) \circ \langle a \rangle, +, \cdot) \subset (G, +, \cdot) \subset (A, +, \cdot)$$

$$(\mathcal{Z}(L), +, \cdot) \subset (\mathcal{Z}(L) \circ \langle b \rangle, +, \cdot) \subset (G, +, \cdot) \subset (A, +, \cdot)$$

and subloop chains

$$(\mathcal{Z}(L), \circ) \subset (\mathcal{Z}(L) \circ \langle a \rangle, \circ) \subset (G, \circ) = \mathcal{Z}(G) \circ \langle a \rangle \circ \langle b \rangle \subset (L, \circ) = (\mathcal{Z}(G) \circ \langle a \rangle \circ \langle b \rangle) \circ \langle u \rangle.$$

$$(\mathcal{Z}(L),\circ) \subset (\mathcal{Z}(L)\circ\langle b\rangle,\circ) \subset (G,\circ) = \mathcal{Z}(G)\circ\langle a\rangle\circ\langle b\rangle \subset (L,\circ) = (\mathcal{Z}(G)\circ\langle a\rangle\circ\langle b\rangle)\circ\langle u\rangle.$$

with the relations

$$a^2 + 2a + g_1 = 0$$
$$b^2 + 2b + g_2 = 0$$
$$u^2 + 2u + g_3 = 0$$

where g_1, g_2 and g_3 are three elements in $\mathcal{Z}(L)$.

PROOF. By properties of *RA* loops, $G = \mathcal{Z}(G) \circ \langle a\rangle \circ \langle b\rangle$ is an *RA* group and $\mathcal{Z}(L) = \mathcal{Z}(G)$. Next we show that $(G,+,\cdot)$ is a subring of the ring A. Let H be the subring of A generated by $\mathcal{Z}(G)$, a and b. Since

$$\mathcal{Z}(G) = N(L) = N(A,+,\cdot),$$

and because of Theorem IV.1, i.e., Artin's theorem, H is an associative subring of A. Therefore H is a proper subring of A because A is not associative. Moreover,

$$H \supseteq G$$

by the definition of G. Since L is an *RA* loop, by the properties of the loop, we have

$$L = G \cup G \circ u = A \supset H \supseteq G.$$

If $G = H$, we are done. Now assume $H \supset G$ and $H \neq G$. Then there exists an element $x \in H \subset L, x \notin G$. Thus $x \in G \circ u$. This implies that there is an element $g \in G \subset H$ such that $x = g \circ u$. So

$$\begin{aligned} g^{-1} \circ (g \circ u) &= g^{-1} + g \circ u + g^{-1} \cdot (g \circ u) \\ &= g^{-1} + x + g^{-1} \cdot x \end{aligned}$$

is in subring H because g^{-1}, g and x are in H. On the other hand, in the loop L, g^{-1}, g and u associate,

$$g^{-1} \circ (g \circ u) = (g^{-1} \circ g) \circ u = 0 \circ u = u;$$

thus u $\in H$. Therefore,

$$g \circ u = g \cdot u + g + u \in H$$

for any $g \in G$. Hence $H = A$, a contradiction. Therefore, $H = G$, and G is a subring of A. Since G is a group, for any element $g \in G$, there exists an element $h \in G$ such

that $g \circ h = 0$; that is, $g \cdot h + g + h = 0$. Therefore ring $(G, +, \cdot)$ is a quasi-regular subring of A. Now we can use our Lemma IV.4 to show the result. Let G be the K and let G be the S in Lemma IV.4. The conditions in the lemma are satisfied because G is a subring and

$$(G, G, G) = 1.$$

By Lemma IV.4, we get that

$$C_K(S) = C_G(G) = \mathcal{Z}(G) = \mathcal{Z}(L)$$

is a subring of the ring A. Since $(\mathcal{Z}(G), \circ)$ is a subgroup of the loop L, the quasi-inverses of the elements in the subring $(\mathcal{Z}(G), +, \cdot)$ are contained in the subring. Therefore, $(\mathcal{Z}(G), +, \cdot)$ is a quasi-regular ring with circle subgroup $(\mathcal{Z}(L), \circ)$.

Let G be the K and let $\{a\}$ be the S in Lemma IV.4. The conditions of the lemma are satisfied because

$$(G, G, a) = (G, a, G) = (G, a, a) = 1$$

and then

$$C_K(S) = C_G(a) = \mathcal{Z}(G) \circ \langle a \rangle$$

is a subring of A by Lemma IV.5. Therefore, $\mathcal{Z}(G) \circ \langle a \rangle$ is a quasi-regular subring with circle subgroup $(\mathcal{Z}(L) \circ \langle a \rangle, \circ)$.

By the same argument, we know that $G \circ \langle b \rangle$ is a quasi-regular subring with circle subgroup $(\mathcal{Z}(L) \circ \langle b \rangle, \circ)$. Since the three elements a, b and u do not associate in the loop L, by the properties of the RA loop and the above argument, we know that $\mathcal{Z}(G) \circ \langle u \rangle$ is a quasi-regular subring with circle subgroup $(\mathcal{Z}(L) \circ (u), \circ)$. The remaining results in the theorem follow the above argument. □

Next, we will discuss a structure theorem of finite RA circle loops. We need some lemmas for our main result.

LEMMA IV.7. *Let L be a finite RA circle loop of a finite quasi-regular alternative ring $(A, +, \cdot)$. Then for any $a \notin \mathcal{Z}(L)$,*

$$2a,\ a^2 \in \mathcal{Z}(L),$$

$$a \cdot \mathcal{Z}(L),\ \mathcal{Z}(L) \cdot a \subseteq \mathcal{Z}(L).$$

Moreover, $\mathcal{Z}(L) \circ a = \mathcal{Z}(L) + a$ and $\mathcal{Z}(L) \circ \langle a \rangle = \mathcal{Z}(L) \cup (\mathcal{Z}(L) + a)$.

PROOF. Consider the subgroup $\mathcal{Z}(L) \circ \langle a \rangle$. Since $a \notin \mathcal{Z}(L)$ and L is an RA loop, there exist two elements b and u in L, such that a, b and u do not associate. By Theorem IV.8, $\mathcal{Z}(L)$ and $\mathcal{Z}(L) \circ \langle a \rangle$ are quasi-regular subrings of the ring A. By the properties of finite RA loops,

$$|\mathcal{Z}(L) \circ \langle a \rangle| = 2|\mathcal{Z}(L)|.$$

Since $\mathcal{Z}(L)$ and $\mathcal{Z}(L) + a$ are two disjoint subsets of the subring $\mathcal{Z}(L) \circ \langle a \rangle$ and each with order $|\mathcal{Z}(L)|$,we get

$$\mathcal{Z}(L) \circ \langle a \rangle = \mathcal{Z}(L) \cup (\mathcal{Z}(L) + a),$$

and $\mathcal{Z}(L) \circ a = \mathcal{Z}(L) + a$. In the subring $(\mathcal{Z}(L) \circ \langle a \rangle, +, \cdot)$, $2a = a + a$ is in $\mathcal{Z}(L)$ or $\mathcal{Z}(L) + a$. If it were in $\mathcal{Z}(L) + a$, then $a \in \mathcal{Z}(L)$, a contradiction. So $2a \in \mathcal{Z}(L)$. Since $a \circ a = 2a + a^2$, then $a^2 \in \mathcal{Z}(L)$.

Now let us show that $a \cdot \mathcal{Z}(L) \subseteq \mathcal{Z}(L)$. For any $g \in \mathcal{Z}(L)$, $a \cdot g \in \mathcal{Z}(L) \circ \langle a \rangle = \mathcal{Z}(L) \cup (\mathcal{Z}(L) + a)$. If $a \cdot g \in \mathcal{Z}(L)$, we are done. Now suppose that $ag \in \mathcal{Z}(L) + a$, then there exists an element $z \in \mathcal{Z}(L)$, such that $ag = z + a$. Then

$$\begin{aligned} a \circ g &= a \cdot g + a + g \\ &= z + a + a + g \\ &= (z + g) + 2a \in \mathcal{Z}(L) \text{ since } \mathcal{Z}(L) \text{ is a subring} \end{aligned}$$

a contradiction. Therefore $a \cdot \mathcal{Z}(L) \subseteq \mathcal{Z}(L)$. Since the center of the loop is the same as the center of the ring, we have $\mathcal{Z}(L) \cdot a \subseteq \mathcal{Z}(L)$. □

THEOREM IV.8. *(The structure of finite RA circle loops)*

Let $(L, \circ)$ be a finite RA circle loop of an alternative quasi-regular ring $(A, +, \cdot)$. Then

1. *$\mathcal{Z}(L)$ and $\mathcal{Z}(L) \circ \langle a \rangle$ and $\mathcal{Z}(L) \circ \langle a \rangle \circ \langle b \rangle$ are ideals of the ring $(A, +, \cdot)$, where a and b are any two non-commutating elements in the ring(loop). Moreover, $a \cdot b, 2a, a^2 \in \mathcal{Z}(L)$.*
2. *we have the following normal extensions:*
   (a) *Loop extension:*

$$\{1\} \subset (\mathcal{Z}(L), \circ) \subset (\mathcal{Z}(L) \circ \langle a \rangle, \circ) \subset (\mathcal{Z}(L) \circ \langle a \rangle \circ \langle b \rangle, \circ) \subset (L, \circ).$$

Every term in the chain is a normal subloop of L.

(b) *Ring extension:*

$$\{0\} \subset (\mathcal{Z}(L), +, \cdot) \subset (\mathcal{Z}(L) \circ \langle a \rangle, +, \cdot) \subset (\mathcal{Z}(L) \circ \langle a \rangle \circ \langle b \rangle, +, \cdot) \subset (A, +, \cdot).$$

Every term in the chain is an ideal of the ring A.

(c) *The two extensions have the following properties:*

(i) $((L, +, \cdot)/(\mathcal{Z}(L), +, \cdot), \circ) \cong (L, \circ)/(\mathcal{Z}(L), \circ) \cong C_2 \times C_2 \times C_2$.

(ii) $((L, +, \cdot)/(\mathcal{Z}(L) \circ \langle a \rangle, +, \cdot), \circ) \cong (L, \circ)/(\mathcal{Z}(L) \circ \langle a \rangle, \circ) \cong C_2 \times C_2$.

(iii) $((L, +, \cdot)/(\mathcal{Z}(L) \circ \langle a \rangle \circ \langle b \rangle, +, \cdot), \circ) \cong (L, \circ)/(\mathcal{Z}(L) \circ (a) \circ \langle b \rangle, \circ) \cong C_2$.

(iv) $((\mathcal{Z}(L) \circ \langle a \rangle \circ \langle b \rangle, +, \cdot)/(\mathcal{Z}(L), +, \cdot), \circ) \cong ((\mathcal{Z}(L) \circ \langle a \rangle, \circ)/(\mathcal{Z}(L) \circ \langle a \rangle, \circ) \cong C_2$.

3. *For any three elements a, b and u which do not associate in the loop $(L, \circ)$, we have*

$$\mathcal{Z}(L) \circ \langle a \rangle = \mathcal{Z}(L) \cup (\mathcal{Z}(L) + a)$$

$$\mathcal{Z}(L) \circ \langle a \rangle \circ \langle b \rangle = \mathcal{Z}(L) \circ \langle a \rangle \cup (\mathcal{Z}(L) \circ \langle a \rangle + b)$$

$$= \mathcal{Z}(L) \cup (\mathcal{Z}(L) + a) \cup (\mathcal{Z}(L) + b) \cup (\mathcal{Z}(L) + a + b).$$

The loop L is a pairwise disjoint union of the subsets:

$$\begin{aligned} L &= G \cup G \circ u \\ &= \mathcal{Z}(L) \circ \langle a \rangle \circ \langle b \rangle \cup (\mathcal{Z}(L) \circ \langle a \rangle \circ \langle b \rangle + u) \\ &= \mathcal{Z}(L) \cup (\mathcal{Z}(L) + a) \cup (\mathcal{Z}(L) + b) \cup (\mathcal{Z}(L) + u) \\ &\quad \cup (\mathcal{Z}(L) + a + b) \cup (\mathcal{Z}(L) + a + u) \cup (\mathcal{Z}(L) + b + u) \\ &\quad \cup (\mathcal{Z}(L) + a + b + u). \end{aligned}$$

4. *For any three elements a, b and u which do not associate, we have the following identities of ring subsets and loop subsets :*

$$\mathcal{Z}(L) \circ a = \mathcal{Z}(L) + a$$

$$(\mathcal{Z}(L) + a) \circ b = \mathcal{Z}(L) + a + b$$

$$(\mathcal{Z}(L) + a + b) \circ u = \mathcal{Z}(L) + a + b + u$$

$$(L, \circ) = G \cup G \circ u = G \cup (G + u).$$

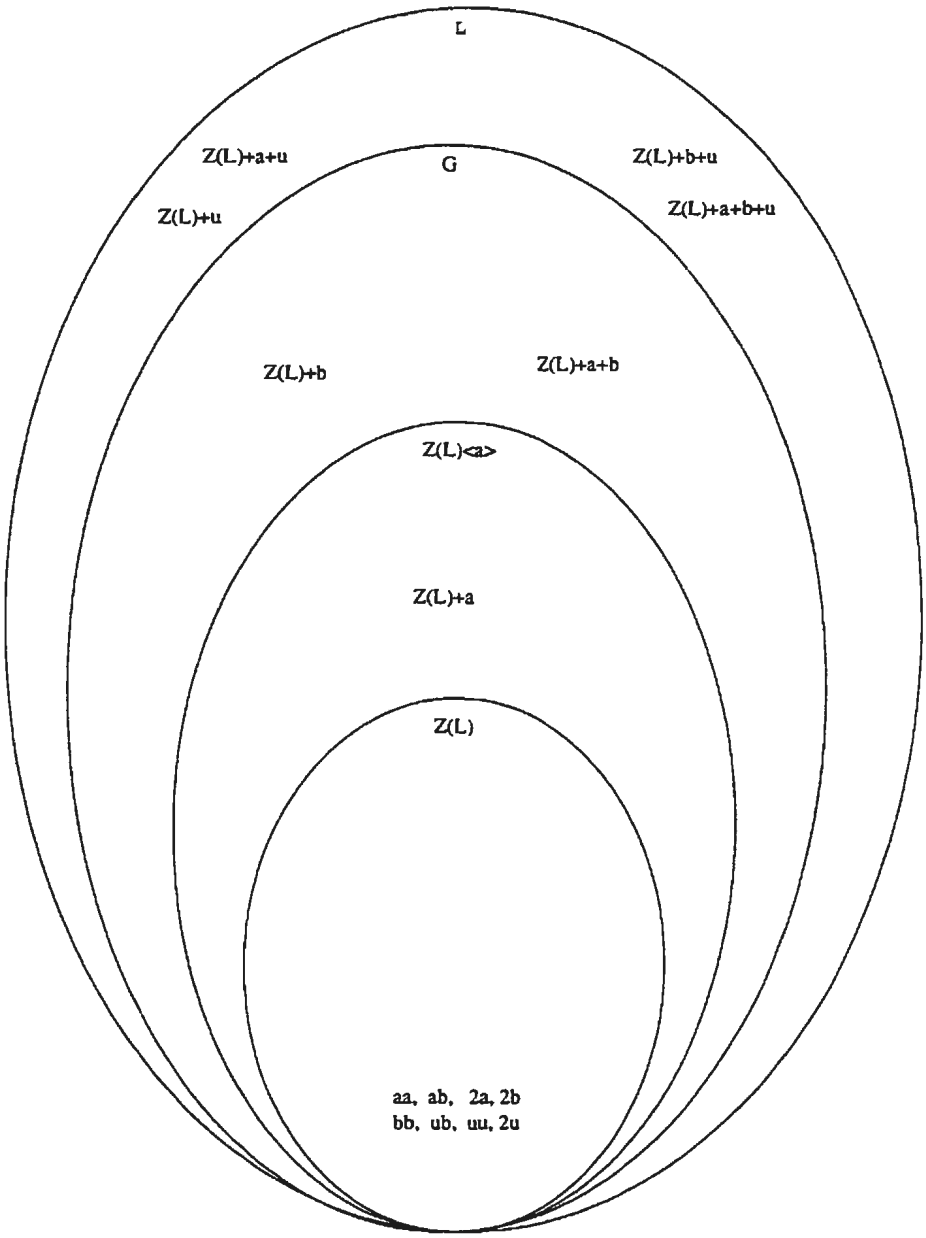

FIGURE IV.1. The structure of finite *RA* circle loops

PROOF. By Theorem IV.6 and Lemma IV.7, $\mathcal{Z}(L)$ is an ideal of the ring A. We will show that $\mathcal{Z}(L) \circ \langle a \rangle$ is an ideal, too. Note that Theorem IV.6 has told us that it is a subring of the ring A.

Let u be an element in loop L such that a, b and u do not associate in L. Because L is an RA loop we can find this element u in loop L. Then it follows that

$$L = (\mathcal{Z}(L) \circ \langle a \rangle \circ \langle b \rangle) \circ \langle u \rangle.$$

Therefore, every element y in L that is not in $\mathcal{Z}(L) \circ \langle a \rangle$ is of the form $x \circ b, x \circ u$ or $x \circ (b \circ u)$ for some $x \in \mathcal{Z}(L) \circ \langle a \rangle$. We are going to show that

$$\mathcal{Z}(L) \circ \langle a \rangle \cdot y \subseteq \mathcal{Z}(L) \circ \langle a \rangle.$$

Because $a \circ y \neq y \circ a$,

$$(\mathcal{Z}(L) \circ \langle a \rangle \circ \langle y \rangle, \circ)$$

is an RA group by the properties of the RA loop. Then $(\mathcal{Z}(L) \circ \langle a \rangle \circ \langle y \rangle, +, \cdot)$ is a subring of the ring A with order $4|\mathcal{Z}(L)| = 2|\mathcal{Z}(L) \circ \langle a \rangle|$ because

$$\mathcal{Z}(L) \circ \langle a \rangle \circ \langle y \rangle / \mathcal{Z}(L) \cong C_2 \times C_2.$$

Since

$$|(\mathcal{Z}(L) \circ \langle a \rangle) \cup ((\mathcal{Z}(L) \circ \langle a \rangle) + y)|$$

is of order $2|\mathcal{Z}(L) \circ \langle a \rangle|$ and the two subsets are disjoint subsets in the subring $(\mathcal{Z}(L) \circ \langle a \rangle \circ (y), +, \cdot)$, we have

$$(\mathcal{Z}(L) \circ \langle a \rangle \circ (y), +, \cdot) = \mathcal{Z}(L) \circ \langle a \rangle \cup (\mathcal{Z}(L) \circ \langle a \rangle + y).$$

Then $ya \in \mathcal{Z}(L) \circ \langle a \rangle$ or $\mathcal{Z}(L) \circ \langle a \rangle + y$. If the latter case occurs, $ya = g + y$ for some $g \in \mathcal{Z}(L) \circ \langle a \rangle$, and so

$$y \circ a = ya + y + a = g + y + y + a = g + a + 2y \in \mathcal{Z}(L) \circ \langle a \rangle$$

because $2y \in \mathcal{Z}(L) \circ \langle a \rangle$ by Lemma IV.7, a contradiction.

Therefore $y \cdot a \in \mathcal{Z}(L) \circ \langle a \rangle$. Similarly, $a \cdot y \in \mathcal{Z}(L) \circ \langle a \rangle$. Thus $(\mathcal{Z}(L) \circ \langle a \rangle, +, \cdot)$ is an ideal of ring A.

Next we show that $G = (\mathcal{Z}(L) \circ \langle a \rangle \circ \langle b \rangle, +, \cdot)$ is an ideal of $(L, +, \cdot)$. We already know that it is a subring by Theorem IV.6. As before, we assume that element u is in

L such that a, b and u do not associate. Then it follows that $L = G \cup G \circ u$. Suppose $x \in G$, then $x \circ u \notin G$. We will show that

$$(x \circ u) \cdot G \subseteq G, \; G \cdot (x \circ u) \subseteq G.$$

For any $g \in G$, consider the element $g \cdot (x \circ u)$. Following the same argument as above, we know that

$$L = G \cup (G + x \circ u).$$

Therefore, $g \cdot (x \circ u) \in G$ or $g \cdot (x \circ u) \in G + x \circ u$. If $g \cdot (x \circ u) \in G$, we are done. Now assume that $g \cdot (x \circ u) \in G + x \circ u$. Then there exists an element h in G such that $g \cdot (x \circ u) = h + (x \circ u)$. Then

$$\begin{aligned} g \circ (x \circ u) &= g + x \circ u + g \cdot x \circ u \\ &= g + x \circ u + h + x \circ u \\ &= g + h + 2(x \circ u) \end{aligned}$$

is in G because $2(x \circ u)$ is in $\mathcal{Z}(G) \subset G$ by Lemma IV.7, a contradiction. Therefore $g \cdot (x \circ u) \in G$. Following the same argument, we can show that $(x \circ u) \cdot g \in G$. Thus G is an ideal. It is not hard to show the chains of loop extensions and ring extensions. By Lemma IV.7, $\mathcal{Z}(L) \circ \langle a \rangle = \mathcal{Z}(L) \cup (\mathcal{Z}(L) + a)$ and $\mathcal{Z}(L) \circ a = \mathcal{Z}(L) + a$. From the above argument it follows that

$$\mathcal{Z}(L) \circ \langle a \rangle \circ \langle b \rangle = \mathcal{Z}(L) \circ \langle a \rangle \cup (\mathcal{Z}(L) \circ \langle a \rangle + b),$$

and

$$\mathcal{Z}(L) \circ \langle a \rangle \circ b = \mathcal{Z}(L) \circ \langle a \rangle + b = (\mathcal{Z}(L) \cup (\mathcal{Z}(L) + a)) + b = (\mathcal{Z}(L) + b) \cup (\mathcal{Z}(L) + a + b).$$

On the other hand,

$$\mathcal{Z}(L) \circ \langle a \rangle \circ b = (\mathcal{Z}(L) \cup (\mathcal{Z}(L) + a)) \circ b = (\mathcal{Z}(L) \circ b) \cup ((\mathcal{Z}(L) + a) \circ b).$$

So

$$(\mathcal{Z}(L) + b) \cup (\mathcal{Z}(L) + a + b) = (\mathcal{Z}(L) \circ b) \cup ((\mathcal{Z}(L) + a) \circ b).$$

Because $\mathcal{Z}(L) \circ b = \mathcal{Z}(L) + b$, and the above unions are disjoint, we have $(\mathcal{Z}(L) + a) \circ b = \mathcal{Z}(L) + a + b$.

Taking $0 \in \mathcal{Z}(L)$, we get $(0+a) \circ b = a \circ b = a \cdot b + a + b \in \mathcal{Z}(L) + a + b$. This implies that $a \cdot b \in \mathcal{Z}(L)$. Therefore,

$$\begin{aligned} L &= G \cup (G \circ u) \\ &= G \cup (G + u) \\ &= \mathcal{Z}(L) \circ \langle a \rangle \circ \langle b \rangle \cup (\mathcal{Z}(L) \circ \langle a \rangle \circ \langle b \rangle + u) \\ &= \mathcal{Z}(L) \circ \langle a \rangle \cup (\mathcal{Z}(L) \circ a + b) \cup (\mathcal{Z}(L) \circ \langle a \rangle + u) \cup ((\mathcal{Z}(L) \circ \langle a \rangle + b) + u) \\ &= \mathcal{Z}(L) \circ \langle a \rangle \cup (\mathcal{Z}(L) \circ a + b) \cup (\mathcal{Z}(L) \circ \langle a \rangle + u) \cup (\mathcal{Z}(L) \circ \langle a \rangle + b + u) \\ &= \mathcal{Z}(L) \cup (\mathcal{Z}(L) + a) \cup (\mathcal{Z}(L) + b) \cup (\mathcal{Z}(L) + a + b) \cup (\mathcal{Z}(L) + u) \\ &\cup (\mathcal{Z}(L) + a + u) \cup (\mathcal{Z}(L) + b + u) \cup (\mathcal{Z}(L) + a + b + u). \end{aligned}$$

Certainly, the subsets here are pairwise disjoint. By the same argument, we can get the other identities of sets. □

COROLLARY IV.9. *If a finite nilpotent alternative ring $(A, +, \cdot)$ has an RA circle loop $(A, \circ)$, then every subring containing the center $\mathcal{Z}(A)$ is an ideal of the ring.*

PROOF. Assume that S is a subring which contains the center $\mathcal{Z}(A)$. For any $x \in S$, if $x \in \mathcal{Z}(A)$, then $Ax \subseteq \mathcal{Z}(A) \subseteq S$ and $xA \subseteq \mathcal{Z}(A) \subseteq S$ because $\mathcal{Z}(A)$ is an ideal; if $x \notin \mathcal{Z}(A)$, then $\mathcal{Z}(A) \circ \langle x \rangle$ is an ideal. So $xA \subseteq \mathcal{Z}(A) \circ \langle x \rangle \subseteq S$. Therefore, S is an ideal. □

THEOREM IV.10. *(Necessary and sufficient conditions for a finite nilpotent alternative ring to have an RA circle loop)*

Let $(A, +, \cdot)$ be an alternative finite nilpotent ring. Then $(A, \circ)$ is an RA loop if and only if

1. *there exists an ideal $(G, +, \cdot)$ of A such that $(A, +, \cdot)$ is generated by G and another element u in A,*
2. *$(G, \circ)$ is an RA group with a unique group commutator s.*
3. *for any $g, h \in G$ the following identities are satisfied by the elements in the ring A:*
   (a) $g \cdot hu + gh = hg \cdot u + hg$,
   (b) $gu \cdot h + gh + uh + h = gh^* \cdot u + h^*u + gh^* + h^*$

(c) $gu \cdot hu + gu \cdot h + gu \cdot u + g \cdot hu + gu + gh + u \cdot hu + uh + hu = g_0h^*g + g_0g + h^*g + g_0h^* + h^* - gh - g - h - g_0 - (u^2 + 2u)$;

(d) $A = G \cup G \circ u$ *and* $G \cap G \circ u = \emptyset$, *where* g_0 *is a fixed element in the center* $\mathcal{Z}(A)$, *and* $g^* = g$ *if* $g \in \mathcal{Z}(A)$, $g^* = gs + g + s$ *if* $g \notin \mathcal{Z}(A)$. *If the conditions are satisfied, then the ring and the group have the following properties:*

(i) $gu + g + u \notin G$,

(ii) *if* $x \in A$ *and* $x \notin G$, *then there exists* $g \in G$ *and* $u \in A$, *such that* $x = gu + g + u$;

PROOF. We prove the sufficiency first. Since $(A, +, \cdot)$ is a nil alternative ring, then $(A, \circ)$ is a Moufang loop by [**Goo87**]. To show that $(A, \circ)$ is an RA loop, we just need to check that $(A, \circ) = M(G, *, g_0)$. Since $(G, \circ)$ is an RA group by (2), we have

$$(A, \circ) = G \cup (G \circ u), G \cap (G \circ u) = \emptyset$$

by the structure theorem of RA loops. Now we can check the three identities. For any g, h in G,

- $g \circ (h \circ u) - (h \circ g) \circ u = g \cdot h \circ u + h \circ u + g - (hg + h + g)u - hg - h - g - u$
  $= g \cdot hu + gh + gu + hu + h + u + g - hg \cdot u - hu - gu - hg - h - g - u$
  $= g \cdot hu + gh - hg \cdot u - hg = 0$ by (3).
- $(g \circ u) \circ h - (g \circ h^*) \circ u = (gu + g + u)h + gu + g + u + h - gh^* \cdot u - gu - h^*u - gh^* - g - h^* - u = gu \cdot h + gh + uh + h - gh^* \cdot u - h^*u - gh^* - h^* = 0$ by (3).
- $(g \circ u) \circ (h \circ u) - g_0 \circ h^* \circ g = (gu + g + u) \circ (hu + h + u) - (g_0h^* + g_0 + h^*) \circ g$
  $= gu \cdot hu + gu \cdot h + gu \cdot u + g \cdot hu + gh + gu + u \cdot hu + uh + u^2 + gu + g + u + hu + h + u$
  $- g_0h^*g - g_0g - h^*g - g_0h^* - g_0 - h^* - g = 0$ by the assumption.

Therefore, $A = G \cup G \circ u$ and $G \cap G \circ u = \emptyset$, and for any two elements g and $h \in G$, we have

$$g \circ (h \circ u) = (h \circ g) \circ u$$

$$(g \circ u) \circ h = (g \circ h^*) \circ u$$

$$(g \circ u) \circ (h \circ u) = g_0 \circ h^* \circ g.$$

By the structure theorem, $(A, \circ)$ is an RA loop.

For the necessary part, note that if the circle loop of the ring A is an RA loop, then it must satisfy the above conditions. So the above equations hold. □

3. A restriction on the *RA* circle loop

In this section we give another condition that an RA circle loop must satisfy. The result follows from the definition of RA loop and the definition of the circle loop.

THEOREM IV.11. *If RA loop $(L, \circ)$ is the circle loop of a nil alternative ring A, then the abelian subgroup of A which is generated by the ring commutators of the ring A, denoted by $\langle [A, A], + \rangle$, is an abelian 2-group.*

COROLLARY IV.12. *The circle loop of any 2-torsion free nil alternative ring is not an RA loop.*

PROOF. For any element $l \in L$, $l \circ l$ is in the center of the loop by the properties of the RA loop. Since an RA loop is a Moufang loop, the loop is left alternative, and then we have the following:

$$(x \circ x) \circ y = y \circ (x \circ x) = x \circ (x \circ y).$$

Let us calculate the three expressions according to the circle operation. First

$$(x \circ x) \circ y = (x^2 + 2x) \circ y = x^2y + 2xy + x^2 + 2x + y;$$

$$y \circ (x \circ x) = y \circ (x^2 + 2x) = yx^2 + 2yx + x^2 + 2x + y;$$

$$x \circ (x \circ y) = x \circ (xy + x + y) = x \cdot xy + x^2 + 2xy + 2x + y.$$

From the first and the second ones, we have that:

$$x^2y + 2xy = yx^2 + 2yx.$$

Then $x^2y - yx^2 = 2(yx - xy)$, and

$$[x^2, y] = 2[y, x].$$

Then $[y, x^2] = 2[x, y]$. Therefore, for any x and y, we have

$$[x^2, y] = 2[y, x].$$

This implies that

$$[x^{2^2}, y] = 2[y, x^2] = 2^2[x, y],$$

and

$$[x^{2^3}, y] = 2[y, x^{2^2}] = 2^2[x^2, y] = 2^3[y, x].$$

In general we have the following formula:

$$[x^{2^n}, y] = \begin{cases} 2^n[x, y] & \text{if n is even} \\ 2^n[y, x] & \text{if n is odd} \end{cases}$$

Since $(A, +, \cdot)$ is a nil ring, for any $x \in A$, there exist an n such that $x^{2^n} = 0$. Then for any $y \in A$,

$$0 = [x^{2^n}, y] = 2^n[x, y]$$

or

$$0 = 2^n[y, x].$$

In either case, we always have

$$2^n[x, y] = 0$$

since $[x, y] = -[y, x]$. Therefore the subgroup generated by the subset $[A, A]$ is a 2-group. Since the loop L is not commutative, the ring A is not commutative. Thus $[A, A] \neq 0$. So the subgroup is a nonzero 2-group. □

CHAPTER V

Alternative rings and Peirce decomposition

In the last two chapters of this thesis we will study alternative rings of small order. In this chapter, we first recall some basic techniques to construct alternative rings on an abelian group, then give a lemma which will be used extensively in the next chapter, and finally, introduce a class of alternative group graded rings.

1. Alternative rings and their matrix representations

To check whether a given ring is alternative or not, using the matrix representation is more efficient than directly using its elements. For more information, we refer the reader to [**KP69**, Chapter II] and [**Tos63**].

Let A_+ be a finite abelian group which is a direct sum of finite cyclic groups and let u_0, u_1, ..., u_n be the generators of these cyclic subgroups with orders t_0, t_1, t_2, ..., t_n, respectively; that is

$$A_+ = \mathbb{Z}u_0 \oplus \mathbb{Z}u_1 \oplus \cdots \oplus \mathbb{Z}u_n,$$

where $u_i = 1 + (t_i) \in \mathbb{Z}/(t_i)$, $i = 0, \ldots, n$. If we use the following Cayley table to define the multiplication of the generators of the abelian group A_+

$*$	u_0	u_1	$\cdots$	u_j	$\cdots$	u_n
u_0	$\sum_k T_{[0][0][k]}u_k$	$\sum_k T_{[0][1][k]}u_k$	$\cdots$	$\sum_k T_{[0][j][k]}u_k$	$\cdots$	$\sum_k T_{[0][n][k]}u_k$
u_1	$\sum_k T_{[1][0][k]}u_k$	$\sum_k T_{[1][1][k]}u_k$	$\cdots$	$\sum_k T_{[1][j][k]}u_k$	$\cdots$	$\sum_k T_{[1][n][k]}u_k$
$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$
u_i	$\sum_k T_{[i][0][k]}u_k$	$\sum_k T_{[i][1][k]}u_k$	$\cdots$	$\sum_k T_{[i][j][k]}u_k$	$\cdots$	$\sum_k T_{[i][n][k]}u_k$
$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$
u_n	$\sum_k T_{[n][0][k]}u_k$	$\sum_k T_{[0][1][k]}u_k$	$\cdots$	$\sum_k T_{[n][j][k]}u_k$	$\cdots$	$\sum_k T_{[n][n][k]}u_k$

where T is a three dimensional array of size $(n+1) \times (n+1) \times (n+1)$, by [**Bea48**], the multiplication is well defined by using the table and distributive laws if and only

if

$$t_i(\sum_k T_{[i][j][k]}u_k) = t_j(\sum_k T_{[i][j][k]}u_k) = 0,$$

where $i, j, k = 0, 1, \ldots, n$. That is, the additive order of the product of any two elements in the basis is a divisor of the orders of the two elements.

Let $X = X_{[0]}u_0 + X_{[1]}u_1 + \cdots + X_{[n]}u_n$ be an element of the algebra. If we define the left transformation $L(X)$ of X on the algebra A by

$$L(X)(Y) = XY,$$

for any $Y = Y_{[0]}u_0 + Y_{[1]}u_1 + \cdots + Y_{[n]}u_n \in A$, then $L(X)$ is a linear transformation. So, $L(X)$ is fully determined by $L(X)(u_0), L(X)(u_1), \ldots, L(X)(u_n)$. If we define a matrix $M_l(X) = [a_{ij}]$ by the following:

$$\begin{bmatrix} L(X)(u_0) \\ L(X)(u_1) \\ \vdots \\ L(X)(u_n) \end{bmatrix} = \begin{bmatrix} Xu_0 \\ Xu_1 \\ \vdots \\ Xu_n \end{bmatrix} = \begin{bmatrix} a_{00} & a_{01} & \cdots & a_{0n} \\ a_{10} & a_{11} & \cdots & a_{1n} \\ \vdots & \vdots & \vdots & \vdots \\ a_{n0} & a_{n1} & \cdots & a_{nn} \end{bmatrix} \begin{bmatrix} u_0 \\ u_1 \\ \vdots \\ u_n \end{bmatrix},$$

where a_{ij} are elements in Z_{t_j} and

$$L(X)(u_i) = Xu_i = \sum_k a_{ik}u_k,$$

for $i = 0, 1, \ldots, n$, we have that

$$\begin{aligned} XY &= L(X)(Y) = Y_{[0]}Xu_0 + Y_{[1]}Xu_1 + \cdots + Y_{[n]}Xu_n \\ &= \begin{bmatrix} Y_{[0]} & Y_{[1]} & \cdots & Y_{[n]} \end{bmatrix} M_l(X) \begin{bmatrix} u_0 \\ u_1 \\ \vdots \\ u_n \end{bmatrix}. \end{aligned}$$

Now let us find out the relationship between the a_{ij}s and the parameters in the Cayley table. Note that

$$Xu_i = (\sum_j X_{[j]}u_j)u_i$$

$$\begin{aligned} &= \sum_j X_{[j]}(u_j u_i) \\ &= \sum_j X_{[j]} \sum_k T_{[j][i][k]} u_k \\ &= \sum_k (\sum_j X_{[j]} T_{[j][i][k]}) u_k. \end{aligned}$$

Therefore,

$$a_{ik} = \sum_j X_{[j]} T_{[j][i][k]}.$$

We know that A is associative if and only if $(XY)Z = X(YZ)$, for any X, Y and $Z \in A$. Expressed in another way, A is associative if and only if

$$L(XY)(Z) = (L(X)L(Y))(Z),$$

for any X, Y and $Z \in A$.

Assume $Z = Z_{[0]}u_0 + Z_{[1]}u_1 + \cdots + Z_{[n]}u_n$. Then

$$(XY)Z = L(XY)(Z) = \begin{bmatrix} Z_{[0]} & Z_{[1]} & \cdots & Z_{[n]} \end{bmatrix} M_l(XY) \begin{bmatrix} u_0 \\ u_1 \\ \vdots \\ u_n \end{bmatrix}.$$

On the other hand,

$$\begin{aligned} X(YZ) = \ & (L(X)L(Y))(Z) = L(X)(L(Y)(Z)) \\ & = \begin{bmatrix} Z_{[0]} & Z_{[1]} & \cdots & Z_{[n]} \end{bmatrix} M_l(Y)M_l(X) \begin{bmatrix} u_0 \\ u_1 \\ \vdots \\ u_n \end{bmatrix}. \end{aligned}$$

Therefore, the algebra A is associative if and only if for any two elements X and Y in A,

$$M_l(XY) = M_l(Y)M_l(X).$$

In particular, an algebra A is left alternative if and only if $M_l(XX) = M_l(X)M_l(X)$ for any $X \in A$.

Since we can easily determine the matrix from the algebra A, checking the equations of matrices is more efficient than checking the elements from A.

As for the right alternative law, we can develop the matrix equation as above, and then check the right alternative law. We just record the results here.

Let $X = X_{[0]}u_0 + X_{[1]}u_1 + \cdots + X_{[n]}u_n$ be an element of the algebra. Then we can define a matrix $M_r(X) = [b_{ij}]$ by the following form:

$$\begin{bmatrix} u_0X \\ u_1X \\ \vdots \\ u_nX \end{bmatrix} = \begin{bmatrix} b_{00} & b_{01} & \cdots & b_{0n} \\ b_{10} & b_{11} & \cdots & b_{1n} \\ \vdots & \vdots & \vdots & \vdots \\ b_{n0} & b_{n1} & \cdots & b_{nn} \end{bmatrix} \begin{bmatrix} u_0 \\ u_1 \\ \vdots \\ u_n \end{bmatrix},$$

where b_{ij} are elements in Z_{t_j} and

$$u_iX = \sum_k b_{ik}u_k,$$

for $i = 0, 1, \ldots, n$.

As for the relationship between the b_{ij}s and the parameters in the Cayley table, we have

$$\begin{aligned} u_iX &= u_i(\sum_j X_{[j]}u_j) \\ &= \sum_j X_{[j]}(u_iu_j) \\ &= \sum_j X_{[j]}(\sum_k T_{[i][j][k]}u_k) \\ &= \sum_k(\sum_j X_{[j]}T_{[i][j][k]})u_k. \end{aligned}$$

Therefore, $b_{ik} = \sum_j X_{[j]}T_{[i][j][k]}$, $i, k = 0, 1, \ldots, n$. Then A is a right alternative ring if and only if $M_r(XX) = M_r(X)M_r(X)$, for any $X \in A$.

From the above discussion, we get the following algorithm to construct an alternative ring which is not associative:

1. define a Cayley table by fixing the three dimensional array T;

2. write a subroutine to take an $X \in A$ as input and output the matrices $M_l(X)$ and $M_r(X)$;
3. compute the product of any two elements in the algebra A by using the matrix $M_l(X)$;
4. check the left and right alternative laws by using the matrices $M_l(X)$ and $M_r(X)$;
5. use matrix multiplication to check whether or not the ring is associative;
6. output the table T' if the table T determines an alternative ring which is not associative.

2. More about Peirce decomposition

By [**Sch66**, Proposition III 3.3], if a finite alternative ring R, or a finite dimensional algebra R over a field, is not nilpotent, then it has a nonzero idempotent, e. For any $x \in R$, we can write

$$x = exe + (ex - exe) + (xe - exe) + (x - ex - xe + exe);$$

thus, as an additive group,

$$R = R_{11} \oplus R_{10} \oplus R_{01} \oplus R_{00} \tag{V.1}$$

where $R_{ij} = \{x \in R \mid ex = ix, xe = jx\}$, $i, j = 0, 1$. The decomposition in (V.1) is called the *Peirce decomposition* of R and the additive subgroups R_{ij} the Peirce *components* of R. It is easy to check that $x_{ij}^2 = 0$ for $x_{ij} \in R_{ij}$ and $i \neq j$ and also to verify other multiplicative properties of the components which are recorded in the table below. (See [**Sch66**, III.2] for details.) For instance, the table shows that $R_{01}R_{10} \subseteq R_{00}$ and that R_{11} and R_{00} are subrings of R.

	R_{11}	R_{10}	R_{01}	R_{00}
R_{11}	R_{11}	R_{10}	0	0
R_{10}	0	R_{01}	R_{11}	R_{10}
R_{01}	R_{01}	R_{00}	R_{10}	0
R_{00}	0	0	R_{01}	R_{00}

If A, B and C are subsets of a ring, we denote by $[A, B, C]$ the set of all associators of the form $[a, b, c]$, $a \in A$, $b \in B$, $c \in C$, and write $[A, B, C] = 0$ if all associators of the form $[a, b, c]$ are 0. In the next chapter, we will frequently be concerned with the possible associativity of an alternative ring with idempotent. Since the associator is linear in each argument, such a ring will be associative provided $[A, B, C] = 0$ for each choice of $A, B, C \in \{R_{11}, R_{10}, R_{01}, R_{00}\}$. Moreover, since the associator is an alternating function of its arguments, whenever $[A, B, C] = 0$, each of the six associators obtained by permuting A, B and C is also 0.

We list below the 20 possible associators of Peirce components (ignoring order of arguments), noting those associators which are always zero just by virtue of the way Peirce components multiply. First, we list the four associators involving three identical components, then the four involving distinct components, and finally the $4 \times 3 = 12$ involving precisely two identical components.

$$\begin{array}{cccc} [R_{11}, R_{11}, R_{11}] & [R_{10}, R_{10}, R_{10}] & [R_{01}, R_{01}, R_{01}] & [R_{00}, R_{00}, R_{00}] \\ [R_{11}, R_{10}, R_{01}] = 0 & [R_{11}, R_{10}, R_{00}] = 0 & [R_{11}, R_{01}, R_{00}] = 0 & [R_{10}, R_{01}, R_{00}] = 0 \end{array}$$

$$\begin{array}{ccc} [R_{11}, R_{11}, R_{10}] = 0 & [R_{11}, R_{11}, R_{01}] = 0 & [R_{11}, R_{11}, R_{00}] = 0 \\ [R_{10}, R_{10}, R_{11}] & [R_{10}, R_{10}, R_{01}] & [R_{10}, R_{10}, R_{00}] \\ [R_{01}, R_{01}, R_{11}] & [R_{01}, R_{01}, R_{10}] & [R_{01}, R_{01}, R_{00}] \\ [R_{00}, R_{00}, R_{11}] = 0 & [R_{00}, R_{00}, R_{10}] = 0 & [R_{00}, R_{00}, R_{01}] = 0. \end{array}$$

Note that it is sometimes necessary to rearrange the order of the arguments to see why some of the above associators are zero. For instance, $[R_{11}, R_{10}, R_{01}] = -[R_{11}, R_{01}, R_{10}] \subseteq -0 \cdot R_{10} + R_{11} \cdot R_{00} = 0$.

The following lemma will be used extensively in the next chapter.

LEMMA V.1. *Let R be an alternative ring with a nonzero idempotent e and let $R = R_{11} \oplus R_{10} \oplus R_{01} \oplus R_{00}$ be the corresponding Peirce decomposition. If any of the following conditions is satisfied, then R is associative.*

(a) *R_{11} and R_{00} are associative and one of R_{10}, R_{01} is zero.*

(b) *R_{11} and R_{00} are associative and both R_{10} and R_{01} are cyclic groups.*

PROOF. As the remarks preceding the lemma indicate, it is sufficient to show that any associator of one of the following ten types is zero.

$$[R_{11}, R_{11}, R_{11}] \qquad [R_{10}, R_{10}, R_{10}] \qquad [R_{01}, R_{01}, R_{01}] \qquad [R_{00}, R_{00}, R_{00}]$$

$$\begin{array}{lll} [R_{10}, R_{10}, R_{11}] & [R_{10}, R_{10}, R_{01}] & [R_{10}, R_{10}, R_{00}] \\ [R_{01}, R_{01}, R_{11}] & [R_{01}, R_{01}, R_{10}] & [R_{01}, R_{01}, R_{00}] \end{array}$$

In case (a) with $R_{10} = 0$, associativity follows from the following observations.

- $[R_{11}, R_{11}, R_{11}] = [R_{00}, R_{00}, R_{00}] = 0$ since R_{11} and R_{00} are associative;
- $[R_{01}, R_{01}, R_{01}] = 0$ because $R_{01}^2 \subseteq R_{10} = 0$;
- $[R_{01}, R_{01}, R_{11}] \subseteq 0 \cdot R_{11} - R_{01} \cdot R_{01} \subseteq R_{10} = 0$;
- $[R_{01}, R_{01}, R_{00}] \subseteq 0 \cdot R_{00} - R_{01} \cdot 0 = 0$.

We know that any ring $(R, +, \cdot)$ is anti-isomorphic to its opposite ring $(R^{\mathrm{op}}, +, \star)$, where $(R^{\mathrm{op}}, +) = (R, +)$ and $a \star b = ba$. If R has an idempotent, then this element is also idempotent in R^{op}, R_{11} and R_{00} are the same in R and in R^{op}, and R_{10} and R_{01} are interchanged. It follows that any ring with the structure of the second part of case (a)—$R_{01} = 0$—is anti-isomorphic to a ring with the structure of the first part—$R_{10} = 0$. Thus such a ring is associative too.

To establish associativity of the rings described by case (b), we note that

$$[R_{11}, R_{11}, R_{11}] = [R_{00}, R_{00}, R_{00}] = 0$$

because R_{11} and R_{00} are associative and all other required associators are 0 because of Artin's Theorem and the fact that each of the additive groups R_{10} and R_{01} is generated by a single element. □

3. Peirce decomposition and group graded rings

Before starting an investigation of alternative rings, we exhibit a class of alternative group graded rings derived from the Peirce decomposition. Later on we can see that most of the alternative rings we find in the following chapter are group graded rings, with the base rings associative, but the group graded rings are alternative but not associative.

For the associative group-graded ring theory, we refer the reader to three basic papers [**Dad80, CR83, CM84**].

DEFINITION V.2. *Let R be a ring (not necessarily associative nor with unity) and let G be a group. We say that the ring R is group graded by a group G if R is a direct sum of $\mathbb{Z}$–modules R_g, i.e,*

$$R = \oplus_{g \in G} R_g$$

such that

$$R_g \cdot R_h \subseteq R_{gh}$$

for any $g, h \in G$. Moreover, if we have

$$R_g \cdot R_h = R_{gh}$$

for any $g, h \in G$, then we call ring R strongly group graded.

Now we have the following result.

PROPOSITION V.3. *Let R be an alternative ring with an idempotent $\neq 0, 1$. If the Peirce decomposition of R for this idempotent is*

$$R = R_{11} \oplus R_{10} \oplus R_{01} \oplus R_{00}$$

and $R_{00} = \{0\}$, then R is a non-trivial group graded ring. The group is a cyclic group of order 3:

$$R = R_1 \oplus R_g \oplus R_{g^2}$$

and the $\mathbb{Z}$–modules are

$$R_1 = R_{11},\ R_g = R_{10},\ R_{g^2} = R_{01},$$

or

$$R_1 = R_{11},\ R_g = R_{01},\ R_{g^2} = R_{10}.$$

Moreover, this group graded ring is not strongly group graded.

PROOF. Following the Peirce decomposition of the ring and the assumption, we have

$$R = R_{11} \oplus R_{10} \oplus R_{01}.$$

Now set

$$R_1 = R_{11},\ R_g = R_{10},\ R_{g^2} = R_{01}.$$

We have

$$R = R_1 \oplus R_g \oplus R_{g^2}.$$

Now let us check the definition of the group graded ring by using the properties of the Peirce decomposition.

- $R_1 \cdot R_1 = R_{11} \cdot R_{11} \subseteq R_{11} = R_1$
- $R_1 \cdot R_g = R_{11} \cdot R_{10} \subseteq R_{10} = R_g = R_{1 \cdot g}$
- $R_1 \cdot R_{g^2} = R_{11} \cdot R_{01} \subseteq R_{00} = \{0\} \subseteq R_{1 \cdot g^2}$
- $R_g \cdot R_1 = R_{10} \cdot R_{11} \subseteq R_{00} = \{0\} \subseteq R_g$
- $R_g \cdot R_g = R_{10} \cdot R_{10} \subseteq R_{01} = R_{g^2} = R_{g \cdot g}$
- $R_g \cdot R_{g^2} = R_{10} \cdot R_{01} \subseteq R_{11} = R_1 = R_{g \cdot g^2}$
- $R_{g^2} \cdot R_g = R_{01} \cdot R_{10} \subseteq R_{00} = \{0\} \subseteq R_1 = R_{g^2 \cdot g}$
- $R_{g^2} \cdot R_{g^2} = R_{01} \cdot R_{01} \subseteq R_{10} = R_g = R_{g^2 \cdot g^2}$

Therefore the ring is a group graded ring , and it is nontrivial because the idempotent is nontrivial.

Since

$$R_1 \cdot R_{g^2} \subseteq R_{00} = \{0\} \subset R_{1 \cdot g^2}$$

and

$$R_g \cdot R_1 = R_{10} \cdot R_{11} \subseteq R_{00} = \{0\} \subset R_g$$

and either R_{10} or R_{01} or both are nonzero, the ring is not a strongly group graded ring. □

CHAPTER VI

Alternative rings of small order

1. Introduction

In this chapter we determine all the alternative rings having order p^n, $n \leq 5$, and alternative algebras that have dimension n over a field with $n \leq 5$, cf [**GZa**]. None of these rings is a Cayley-Dickson algebra or alternative loop algebra.

It is well known that the smallest Moufang loop which is not associative has order 12 [**CP71**], and the smallest RA loop has order 16 [**CG86**]. In this chapter we show that the smallest alternative rings which are not associative have order 16.

The Wedderburn principal theorem will be used in this chapter and we cite it here

THEOREM VI.1. [**Sch66**, Theorem 3.18] *Let A be a finite-dimensional alternative algebra over field F with radical $Rad(A)$. If $A/Rad(A)$ is separable, then*

$$A = B + Rad(A)$$

as direct sum of vector spaces over F, where B is an algebra isomorphic to $A/Rad(A)$.

2. Alternative rings of order p^n, $n \leq 4$

For a given ring R we let R_+ denote the abelian group $(R, +)$. The following lemma tells us that only rings of prime power order need to be investigated.

LEMMA VI.2. *Let R be a finite ring. Then there is a ring decomposition*

$$R = R_{p_1} \oplus R_{p_2} \oplus \cdots \oplus R_{p_n}$$

where

$$R_{p_i} = \{r \in R \mid \exists n, \textit{such that } p_i^n r = 0\}.$$

Let us cite a result of [**GZa**], which will be used later.

PROPOSITION VI.3. *Let p be a prime. Any alternative nil ring of order p^n, $n \leq 5$, is associative.*

Throughout this section, p denotes a prime. Consideration of additive structure and Artin's Theorem imply that the only alternative rings of order p or p^2 are associative. If an alternative ring has order p^3 and it is nil, then it is associative by Proposition VI.3; otherwise, it has a nonzero idempotent and at least one nonzero Peirce component. Using Lemma V.1, it is easy to see that such a ring must also be associative unless $R_{11} = Z_p \oplus Z_p \oplus Z_p$ in which case R has 1 and Artin's theorem implies the associativity of the ring.

Let R be an alternative ring of order p^4 which is not nil. By [**Sch66**, Proposition III 3.3], we may assume that R has a nonzero idempotent, e. In view of Artin's Theorem, if R is not associative, then it must have additive structure $Z_{p^2} \oplus Z_p \oplus Z_p$ or $Z_p \oplus Z_p \oplus Z_p \oplus Z_p$.

Suppose $R_+ \cong Z_{p^2} \oplus Z_p \oplus Z_p$. If R has a unity, then this element generates that component of R_+ which is isomorphic to Z_{p^2} and associativity easily follows from Artin's Theorem. If R does not have a unity, then $e \neq 1$, so R_{11} is the direct sum of at most two cyclic groups; hence R_{11} is associative. Similarly, R_{00} is associative, so R is associative by Lemma V.1.

It remains only to consider the case

$$R = R_{11} \oplus R_{10} \oplus R_{01} \oplus R_{00} \cong Z_p \oplus Z_p \oplus Z_p \oplus Z_p$$

which we handle according to the four possibilities for R_{11}; namely, $R_{11} \cong Z_p \oplus Z_p \oplus Z_p \oplus Z_p$, $Z_p \oplus Z_p \oplus Z_p$, $Z_p \oplus Z_p$ or Z_p.

Case 1. If $R_{11} \cong Z_p \oplus Z_p \oplus Z_p \oplus Z_p$, then $R = R_{11}$ is an algebra with unity over the field F_p of p elements. Any semisimple finite dimensional alternative algebra which is not associative contains a Cayley-Dickson algebra which is 8-dimensional over its center [**Sch66**, Theorems 3.12 and 3.17]. Clearly in our case then, the nil radical, $\mathrm{Rad}(R)$, of R is not 0; neither is it R. Thus $\dim \mathrm{Rad}(R)$ is 1, 2 or 3. Also, since we are working over finite and hence perfect fields, the Wedderburn Principal Theorem tells us that $R = S + \mathrm{Rad}(R)$.

Suppose $\dim \mathrm{Rad}(R) = 1$. Let $\mathrm{Rad}(R) = \langle c \rangle$ and let $a, b \in R$. Since $\mathrm{Rad}(R)$ is an ideal of R, we have $ca = \alpha c$ and $bc = \beta c$ for some $\alpha, \beta \in F_p$. Then $[b, c, a] = (bc)a - b(ca) = \beta ca - b(\alpha c) = \beta \alpha c - \alpha \beta c = 0$. It follows that R is associative.

If $\dim \mathrm{Rad}(R) = 2$, then R is the vector space direct sum of a two-dimensional semisimple algebra S and a nilpotent ring of order p^2. The latter either has trivial multiplication or it is generated by a single element [**KP69**, Theorem 2.3.3]. Selecting a basis for R of the form $\{1, s, a, b\}$, $s \in S$, $a, b \in \mathrm{Rad}(R)$, and remembering Artin's theorem, it follows immediately that the associator of any three of these basis elements is 0, so R is associative.

If $\dim \mathrm{Rad}(R) = 3$, then R is associative because it is generated by 1 and an associative ring.

Case 2. If $R_{11} \cong \mathsf{Z}_p \oplus \mathsf{Z}_p \oplus \mathsf{Z}_p$, then both R_{11} and $R_{00} = 0$ are associative and at least one of R_{10} or R_{01} is 0, so R is associative by Lemma V.1.

Case 3. If $R_{11} \cong \mathsf{Z}_p \oplus \mathsf{Z}_p$, then again both R_{11} and R_{00} are associative. Also $R_{10} \oplus R_{01}$ is the direct sum of at most two cyclic groups. Again Lemma V.1 assures us of associativity.

Case 4. We treat the case $R_{11} \cong \mathsf{Z}_p$ by considering the various possibilities for R_{00}. If $R_{00} \cong \mathsf{Z}_p \oplus \mathsf{Z}_p \oplus \mathsf{Z}_p$ or $\mathsf{Z}_p \oplus \mathsf{Z}_p$ or Z_p, then R_{00} is associative, $R_{10} \oplus R_{01}$ is the direct sum of at most two copies of Z_p and Lemma V.1 tells us that R is associative.

Suppose $R_{00} = 0$. If either R_{10} or R_{01} is 0, then R is associative by Lemma V.1. Thus there are just two situations which require further study:

Case 4a: $R_{11} \cong \mathsf{Z}_p$, $R_{00} = 0$, $R_{10} \cong \mathsf{Z}_p$, $R_{01} \cong \mathsf{Z}_p \oplus \mathsf{Z}_p$ and

Case 4b: $R_{11} \cong \mathsf{Z}_p$, $R_{00} = 0$, $R_{10} \cong \mathsf{Z}_p \oplus \mathsf{Z}_p$, $R_{01} \cong \mathsf{Z}_p$.

In case 4a, let $R_{11} = \langle e \rangle$, $R_{10} = \langle a \rangle$ and $R_{01} = \langle b \rangle \oplus \langle c \rangle$. The possible products amongst the elements e, a, b, c are shown below,

	e	a	b	c
e	e	a	0	0
a	0	0	ie	je
b	b	0	0	ka
c	c	0	ma	0

where i, j, k, m are integers. Since $[e, a, b] = [e, a, c] = [a, b, c] = 0$, in order to avoid associativity, we must have $[e, b, c] = -ka \neq 0$. Therefore $k \neq 0$. Since $-ma = [e, c, b] = -[e, b, c]$, $m = -k$ and since $(ab)a = a(ba)$ and $(ac)a = a(ca)$, necessarily $i = j = 0$. It is now straightforward to check that these conditions define an alternative ring which is not associative. Replacing b by $k^{-1}b$, we may assume $k = 1$.

Case 4b leads to rings anti-isomorphic to those of Case 4a since under the opposite operation, R_{01} and R_{10} are interchanged while R_{11} and R_{00} are unchanged.

THEOREM VI.4. *For any prime p, there are precisely two alternative rings of order p^4 which are not associative. They are anti-isomorphic. Neither has a unity, but both have a nonzero idempotent e. Each ring is a four-dimensional vector space over F_p with nil radical of dimension 3. With respect to a basis $\{e, a, b, c\}$, their multiplication tables are defined as follows:*

4/1:

	e	a	b	c
e	e	a	0	0
a	0	0	0	0
b	b	0	0	a
c	c	0	$-a$	0

4/2:

	e	a	b	c
e	e	0	b	c
a	a	0	0	0
b	0	0	0	a
c	0	0	$-a$	0

Moreover, the two rings are group-graded rings. For 4/1,

$$R = R_1 \oplus R_g \oplus R_{g^2},$$

where $R_1 = R_{11} = \mathbb{Z}_p e$, $R_g = R_{10} = \mathbb{Z}_p a$ and $R_{g^2} = R_{01} = \mathbb{Z}_p b \oplus \mathbb{Z}_p c$, and $g^3 = 1$. A similar result holds for 4/2.

REMARK VI.5. The above is a generalization of A. T. Gainov[**Gai63**] in which a more complicated way was used to obtain the result under the condition $p \neq 2$ and $p \neq 3$.

PROOF. First we show the tables determine two nonassociative alternative rings and then show that they are not isomorphic.

We use the matrix representation to show that the ring 4/1 satisfies the left and right alternative laws.

For the left alternative law, let

$$X = x_0 e + x_1 a + x_2 b + x_3 c$$

be an arbitrary element in the ring. From the table we have

$$X^2 = x_0^2 e + x_0 x_1 a + x_0 x_2 b + x_0 x_3 c.$$

Then the left matrix can be determined by the left transformation:

$$\begin{bmatrix} Xe \\ Xa \\ Xb \\ Xc \end{bmatrix} = \begin{bmatrix} x_0 & 0 & x_2 & x_3 \\ 0 & x_0 & 0 & 0 \\ 0 & -x_3 & 0 & 0 \\ 0 & x_2 & 0 & 0 \end{bmatrix} \cdot \begin{bmatrix} e \\ a \\ b \\ c \end{bmatrix}$$

Therefore

$$M_l(X) = \begin{bmatrix} x_0 & 0 & x_2 & x_3 \\ 0 & x_0 & 0 & 0 \\ 0 & -x_3 & 0 & 0 \\ 0 & x_2 & 0 & 0 \end{bmatrix}$$

Similarly, for the element X^2, we have

$$\begin{bmatrix} X^2e \\ X^2a \\ X^2b \\ X^2c \end{bmatrix} = \begin{bmatrix} x_0^2 & 0 & x_0x_2 & x_0x_3 \\ 0 & x_0^2 & 0 & 0 \\ 0 & -x_0x_3 & 0 & 0 \\ 0 & x_0x_2 & 0 & 0 \end{bmatrix} \cdot \begin{bmatrix} e \\ a \\ b \\ c \end{bmatrix}$$

Therefore

$$M_l(X^2) = \begin{bmatrix} x_0^2 & 0 & x_0x_2 & x_0x_3 \\ 0 & x_0^2 & 0 & 0 \\ 0 & -x_0x_3 & 0 & 0 \\ 0 & x_0x_2 & 0 & 0 \end{bmatrix}$$

It is easy to check that

$$M_l(X)M_l(X) = \begin{bmatrix} x_0^2 & x_2x_3 - x_3x_2 & x_0x_2 & x_0x_3 \\ 0 & x_0^2 & 0 & 0 \\ 0 & -x_0x_3 & 0 & 0 \\ 0 & x_0x_2 & 0 & 0 \end{bmatrix}$$

which is $M_l(X^2)$. Thus $M_l(X)M_l(X) = M_l(X^2)$, and the ring is left alternative. To check it is a right alternative ring, we have

$$\begin{bmatrix} eX \\ aX \\ bX \\ cX \end{bmatrix} = \begin{bmatrix} x_0 & x_1 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & x_3 & x_0 & 0 \\ 0 & -x_2 & 0 & x_0 \end{bmatrix} \cdot \begin{bmatrix} e \\ a \\ b \\ c \end{bmatrix}$$

Therefore

$$M_r(X) = \begin{bmatrix} x_0 & x_1 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & x_3 & x_0 & 0 \\ 0 & -x_2 & 0 & x_0 \end{bmatrix}$$

Similarly, for the element X^2, we have

$$\begin{bmatrix} eX^2 \\ aX^2 \\ bX^2 \\ cX^2 \end{bmatrix} = \begin{bmatrix} x_0^2 & x_0x_1 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & x_0x_3 & x_0^2 & 0 \\ 0 & -x_0x_2 & 0 & x_0^2 \end{bmatrix} \cdot \begin{bmatrix} e \\ a \\ b \\ c \end{bmatrix}$$

and

$$M_r(X^2) = \begin{bmatrix} x_0^2 & x_0x_1 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & x_0x_3 & x_0^2 & 0 \\ 0 & -x_0x_2 & 0 & x_0^2 \end{bmatrix}$$

It is easy to check that

$$M_r(X)M_r(X) = \begin{bmatrix} x_0^2 & x_0x_1 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & x_0x_3 & x_0^2 & 0 \\ 0 & -x_0x_2 & 0 & x_0^2 \end{bmatrix}$$

Therefore, $M_r(X)M_r(X) = M_r(X^2)$ and the ring is right alternative. From the construction of the ring, we know it is not associative. In fact, we have $e(bc) \neq (eb)c$. So this ring is an alternative ring which is not associative.

Since 4/2 is anti-isomorphic to 4/1, the second ring is a nonassociative alternative ring. It remains only to remark that the two rings identified here are not isomorphic because a is a (nonzero) left annihilator in 4/1 while 4/2 has no such element. In fact, in the second ring, assuming $X = x_0e + x_1a + x_2b + x_3c$ is a left annihilator, then for any $Y = y_0e + y_1a + y_2b + y_3c$,

$$XY = x_0y_0e + (x_1y_0 + x_3y_2 - x_2y_3)a + x_0y_2b + x_0y_3c = 0.$$

Taking $y_0 = 0, y_2 = 0$ and $y_3 = 1$, we have $XY = x_0c - x_2a = 0$, so $x_0 = 0$ and $x_2 = 0$. If we let $y_0 = 0, y_2 = 1$, then $x_3 = 0$. We can get $x_1 = 0$ by taking $y_0 = 1$. Thus $X = 0$. Therefore, there is no nonzero left annihilator in the second ring.

The claim about the group-graded rings follows from Proposition V.3. □

REMARK VI.6. The tables given in this theorem (and elsewhere in this chapter) define alternative rings of many different orders and dimensions. The above tables, for instance, define alternative algebras of dimension four over any field (finite or infinite). They also define alternative rings with additive structure $\mathbb{Z}_{p^n} \oplus \mathbb{Z}_{p^m} \oplus \mathbb{Z}_{p^r} \oplus \mathbb{Z}_{p^s}$ provided, for each $x, y \in \{e, a, b, c\}$, the additive order of xy divides the additive orders of x and y. More generally, we have

COROLLARY VI.7. *Let R be a ring with*

$$R_+ = \mathbb{Z}_{n_0}e \oplus \mathbb{Z}_{n_1}a \oplus \mathbb{Z}_{n_2}b \oplus \mathbb{Z}_{n_3}c,$$

where n_0, n_1, n_2, n_3 are any integers with the property that

$$n_1|n_0, n_1|n_2, n_1|n_3, n_2|n_0, n_3|n_0$$

then the following Cayley table gives us a nonassociative alternative ring:

$*$	e	a	b	c
e	e	0	b	c
a	a	0	0	0
b	0	0	0	$-a$
c	0	0	a	0

Since the first example of an alternative ring is the Cayley numbers which is an algebra of dimension 8 the following corollary is interesting.

COROLLARY VI.8. *The smallest alternative algebras over the field of real numbers are the two algebras with the above Cayley tables* 4/1 *and* 4/2.

PROOF. Because there are no nilpotent alternative algebras of dimension 4 [**Bad84**, Corollary 1], the alternative algebras have non-zero idempotents. Therefore the above algebras are of the smallest dimension. □

3. Alternative rings of order p^5

Throughout this section, p denotes a prime and R is an alternative ring of order p^5 which is not associative. Since there are no nil rings of this order which are not associative by Proposition VI.3, we also assume that R has a nonzero idempotent.

Again we denote the additive group of R by R_+. By Artin's Theorem, there are four possibilities for the structure of R_+.

$R_+ \cong Z_p \oplus Z_p \oplus Z_p \oplus Z_p \oplus Z_p$;

$R_+ \cong Z_{p^2} \oplus Z_p \oplus Z_p \oplus Z_p$;

$R_+ \cong Z_{p^2} \oplus Z_{p^2} \oplus Z_p$;

$R_+ \cong Z_{p^3} \oplus Z_p \oplus Z_p$.

Suppose $R_+ \cong Z_{p^2} \oplus Z_{p^2} \oplus Z_p$ or $R_+ \cong Z_{p^3} \oplus Z_p \oplus Z_p$.

If R has a unity, we may assume this is the generator of a cyclic component of highest order. Associativity then follows immediately from Artin's Theorem. If R has an idempotent e which is not a unity, then $R_{11} \neq 0$ and so at least one of R_{00}, R_{10}, R_{01} must be 0 since there are only three summands in the decomposition of R_+ but four components in the Peirce decomposition.

If $R_{00} = 0$, then $R = R_{11} \oplus R_{10} \oplus R_{01}$. By the uniqueness of the decomposition of a finite abelian group, each Peirce component of R_+ is the sum of one or more of the three cyclic subgroups in the decomposition of R_+. Now R_{11} is the sum of at most two of these subgroups since e is the unity of R_{11} and R has no unity. Therefore, R_{11} is always associative. If R_{11} is the sum of two cyclic subgroups, then one of R_{10}, R_{01} is 0 and R is an associative ring by part (a) of Lemma V.1. If R_{11} is cyclic and one of R_{10}, R_{01} is the sum of two cyclic subgroups, then the other must be 0 and again R is associative. There remains the case in which each Peirce component is a cyclic group, but now part (b) of Lemma V.1 shows that R is associative.

If $R_{00} \neq 0$, one of R_{10}, R_{01} must be 0 and R_{00} is associative because it is the direct sum of at most two cyclic groups. By Lemma V.1, R is associative.

It remains to consider the possibilities that $R_+ \cong \mathsf{Z}_p \oplus \mathsf{Z}_p \oplus \mathsf{Z}_p \oplus \mathsf{Z}_p \oplus \mathsf{Z}_p$ or $R_+ \cong \mathsf{Z}_{p^2} \oplus \mathsf{Z}_p \oplus \mathsf{Z}_p \oplus \mathsf{Z}_p$ and we do so according as R has a unity or an idempotent $e \neq 1$.

4. Alternative rings of order p^5 with unity

Suppose $R_+ \cong \mathsf{Z}_{p^2} \oplus \mathsf{Z}_p \oplus \mathsf{Z}_p \oplus \mathsf{Z}_p$. Without loss of generality Z_{p^2} is generated by 1. Assume the generators of the other cyclic components are a, b, c respectively. The set $R_0 = \{x \in R \mid px = 0\}$ is a subring of R containing $p1$, a, b and c, so it has order at least p^4 and hence exactly p^4 since $R \neq R_0$. Noting that $p1$ is a two-sided annihilator for R_0 and that neither of the two alternative rings of order p^4 described in Theorem VI.4 has such an element, R_0 must be associative. Since every $x \in R$ can be written in the form $x = \alpha 1 + x_0$, $x_0 \in R_0$, it follows readily that R is associative too.

In the remaining case, $R_+ \cong \mathsf{Z}_p \oplus \mathsf{Z}_p \oplus \mathsf{Z}_p \oplus \mathsf{Z}_p \oplus \mathsf{Z}_p$ is an algebra of dimension 5 over F_p, the field of p elements. Because every finite semisimple alternative ring which is not associative must contain an 8-dimensional Cayley-Dickson algebra, R must have a nonzero nil radical $\mathrm{Rad}(R)$, of dimension at most four. Thus the semisimple ring $R/\mathrm{Rad}(R)$ also has dimension at most four; in particular, it is associative. Again the Wedderburn Principal Theorem tells us that $R = S + \mathrm{Rad}(R)$ with $S \cong R/\mathrm{Rad}(R)$ and hence semisimple associative.

Suppose first that S is a field. In this situation, we employ an argument of E. G. Goodaire. If $S = F_p$, $R = \mathrm{Rad}(R) + S$ must be associative since R is generated by 1 and the associative algebra $\mathrm{Rad}(R)$. If $S = F_p(t)$ is 4-dimensional, then $\mathrm{Rad}(R)$ is 1-dimensional and R is associative by Artin's Theorem since it is generated by two elements and 1. If $S = F_p(t)$ is 3-dimensional, then $\mathrm{Rad}(R)$ is a nilpotent associative ring of order p^2. Any such ring either has trivial multiplication or it is generated by one element [**KP69**, 3.3.1], so again R is associative. If $S = F_p(t)$ is 2-dimensional, then $\mathrm{Rad}(R)$ is nilpotent, associative of order p^3. Such rings have also been classified by Kruse and Price [**KP69**, 3.3.2]. As before, if $\mathrm{Rad}(R)$ has trivial multiplication or is generated by one element, then R is associative. This leaves three possibilities

for Rad(R) which require further investigation. In each case, we assume Rad(R) has basis $\{a, b, c\}$ with c a two-sided annihilator; products not specified are 0.

Case 1: $a^2 = b^2 = 0$, $ab = -ba = c$;

Case 2: $a^2 = c$, $b^2 = \gamma c$, $ab = ba = 0$, $\gamma \in F_p$;

Case 3: $a^2 = ab = c$, $ba = 0$, $b^2 = \varphi c$, $\varphi \in F_p$.

In case 1, we use the fact that $(bt)a + (ba)t = b(ta) + b(at)$ which is a consequence of $b(t+a)^2 = [b(t+a)](t+a)]$. Remembering too that Rad(R) is an ideal, we have

$$(bt)a + (ba)t = (\alpha_1 a + \alpha_2 b + \alpha_3 c)a - ct = -\alpha_2 c - ct$$

whereas

$$b(ta) + b(at) = b(\beta_1 a + \beta_2 b + \beta_3 c) + b(\beta_4 a + \beta_5 b + \beta_6 c) = -\beta_1 c - \beta_4 c$$

(all $\alpha_i, \beta_i \in F_p$) and conclude that $ct = \tau c$ for some $\tau \in F_p$. Thus

$$(ct)t = \tau ct = \tau^2 c \text{ while } ct^2 = c(k_0 + k_1 t) = ck_0 + k_1 \tau c$$

($\gamma_i, k_i \in F_p$) and hence τ is a root of the polynomial $x^2 - k_1 x - k_0$, contradicting its irreducibility: recall that $t^2 = k_0 + k_1 t$ and $t \notin F_p$.

In case 2, we have

$$a^2 t = ct = \alpha_1 a + \alpha_2 b + \alpha_3 c$$

whereas

$$a(at) = a(\beta_1 a + \beta_2 b + \beta_3 c) = \beta_1 c$$

so $\alpha_1 = \alpha_2 = 0$; that is $ct = \alpha_3 c$. Then $(ct)t = \alpha_3^2 c$ while $ct^2 = c(k_0 + k_1 t) = k_0 c + k_1 \alpha_3 c$ so α_3 is a root of $x^2 - k_1 x - k_0$, a contradiction as before.

Case 3 is virtually identical to case 2. Since

$$a^2 t = ct = \alpha_1 a + \alpha_2 b + \alpha_3 c$$

whereas

$$a(at) = a(\beta_1 a + \beta_2 b + \beta_3 c) = \beta_1 c + \beta_2 c$$

we again have $\alpha_1 = \alpha_2 = 0$; that is $ct = \alpha_3 c$. Then $(ct)t = \alpha_3^2 c$ and $ct^2 = c(k_0 + k_1 t) = k_0 c + k_1 \alpha_3 c$ so α_3 is a root of $x^2 - k_1 x - k_0$, a contradiction.

If S is not a field, then it contains an idempotent e which is neither 0 nor 1. We use this idempotent to analyze the structure of R. Thus we have the Peirce decomposition $R_+ = R_{11} \oplus R_{01} \oplus R_{10} \oplus R_{00}$.

Since $e \neq 1$, $1 - e \in R_{00} \neq 0$. If $R_{00} \cong \mathbb{Z}_p \oplus \mathbb{Z}_p$, $R_{00} \cong \mathbb{Z}_p \oplus \mathbb{Z}_p \oplus \mathbb{Z}_p$, or $R_{00} \cong 4\mathbb{Z}_p$, then $R_{10} \oplus R_{01}$ is the direct sum of at most two copies of $\mathbb{Z}_p$, so Lemma V.1 tells us that R is associative.

Suppose $R_{00} = \mathbb{Z}_p$. If either R_{10} or R_{01} is 0, Lemma V.1 says R is associative. If $R_{10} = \langle a \rangle \cong \mathbb{Z}_p$ and $R_{01} = \langle b \rangle \oplus \langle c \rangle \cong \mathbb{Z}_p \oplus \mathbb{Z}_p$, the products of pairs of $1, e, a, b, c$ are as recorded below

	1	e	a	b	c
1	1	e	a	b	c
e	e	e	a	0	0
a	a	0	0	$x_0 1 + x_1 e$	$y_0 1 + y_1 e$
b	b	b	0	0	ka
c	c	c	0	ja	0

where $x_i, y_i, j, k \in F_p$. Since R is not associative, at least one of the associators $[e, a, b]$, $[e, a, c]$, $[e, b, c]$ and $[a, b, c]$ must be nonzero. Since $[e, b, a] = 0$, so also $0 = [e, a, b] = ab - e(x_0 1 + x_1 e) = x_0 1 + x_1 e - x_0 e - x_1 e = x_0 1 - x_0 e$; thus $x_0 = 0$. Similarly, $[e, c, a] = 0$, so $0 = [e, a, c] = ac - e(y_0 1 + y_1 e) = y_0 1 + y_1 e - y_0 e - y_1 e = y_0 1 - y_0 e$ and $y_0 = 0$. It is easy to check that $[a, b, c] = 0$, so $[e, b, c] = -ka \neq 0$. Since $-ja = [e, c, b] = -[e, b, c]$, $j = -k$. Finally, $x_1 a = (ab)a = a(ba) = 0$ and $0 = (ca)c = c(ac) = y_1 c$ implies $x_1 = y_1 = 0$ and the multiplication table for a basis of R becomes

	1	e	a	b	c
1	1	e	a	b	c
e	e	e	a	0	0
a	a	0	0	0	0
b	b	b	0	0	ka
c	c	c	0	$-ka$	0

where $0 \neq k \in F_p$. It is straightforward to verify that such a ring is indeed alternative (and not associative). Replacing b by $k^{-1}b$, we may assume $k = 1$. This gives the following table.

	1	e	a	b	c
1	1	e	a	b	c
e	e	e	a	0	0
a	a	0	0	0	0
b	b	b	0	0	a
c	c	c	0	$-a$	0

If $R_{10} \cong \mathbb{Z}_p \oplus \mathbb{Z}_p$ and $R_{01} \cong \mathbb{Z}_p$, the rings we obtain are anti-isomorphic to the rings just investigated. Thus we obtain one alternative (not associative) ring, with multiplication table

	1	e	a	b	c
1	1	e	a	b	c
e	e	e	0	b	c
a	a	0	0	0	0
b	b	0	0	0	a
c	c	0	0	$-a$	0

Changing to the basis $\{1, 1-e, a, b, c\}$, it is clear that this ring is identical to the previous.

THEOREM VI.9. *Up to isomorphism, there is just one alternative ring of order p^5 which has a unity and is not associative. This is an algebra of dimension 5 over F_p with basis $\{1, e, a, b, c\}$, nil radical of dimension 3 and multiplication defined by the following table.*

5/0:

	1	e	a	b	c
1	1	e	a	b	c
e	e	e	a	0	0
a	a	0	0	0	0
b	b	b	0	0	a
c	c	c	0	$-a$	0

This ring contains both 4/1 and 4/2 as anti-isomorphic ideals, with bases $\{e, a, b, c\}$ *and* $\{1 - e, a, b, c\}$ *respectively, and is the standard ring extension of* 4/1 *or* 4/2 *to a ring with a unity. Moreover, this ring is a group-graded ring as shown in Proposition V.3.*

PROOF. It remains only to show that the ring is the standard extension of 4/1.

Let us recall the standard way to adjoin 1 to a ring that does not have 1 [**Sch66**, p11].

Let R be an alternative algebra over a field F. A new ring on the set $F \times R$ is defined by addition and multiplication as follows:

$$(m, r) + (n, s) = (m + n, r + s);$$

$$(m, r)(n, s) = (mn, ms + nr + rs),$$

where r, $s \in R$, m, $n \in F$.

Then the ring $F \times R$ is alternative with unity $(1, 0)$ in which R is an ideal.

We have shown that there are two alternative rings of order 16 and none has a unity.

Now we follow the above process on the ring 4/1 to get the new alternative ring $Z_p \times 4/1$.

It is easy to check that the following identity map of the basis elements implies the isomorphism of the two rings:

$$1 \mapsto 1, e \mapsto e, a \mapsto a, b \mapsto b, c \mapsto c.$$

Since 4/1 is a group-graded ring, using that grading by adding 1 to R_1, it is easy to check this grading results in the group-graded ring 5/0.

□

5. Alternative rings of order p^5 possessing an idempotent $e \neq 1$

Let us consider alternative rings of order p^5 possessing an idempotent e which is not a unity.

In this section, we will establish 12 tables. Any such table defines an alternative, but not associative ring. We leave the proof to Section 6.

Recall that there are two cases to consider—$R_+ \cong Z_p \oplus Z_p \oplus Z_p \oplus Z_p \oplus Z_p$ and $R_+ \cong Z_{p^2} \oplus Z_p \oplus Z_p \oplus Z_p$. Let $e \neq 0, 1$ be an idempotent and $R = R_{11} \oplus R_{10} \oplus R_{01} \oplus R_{00}$ the corresponding Peirce decomposition of R.

Case 1: $R_+ \cong Z_p \oplus Z_p \oplus Z_p \oplus Z_p \oplus Z_p$. We analyze this case in terms of the possibilities for R_{11}, which is the direct sum of at most four copies of Z_p since $e \neq 1$. Since e is a unity for R_{11} and alternative rings with unity and order at most p^4 are associative, we know that R_{11} is associative.

If R_{11} is the direct sum of four copies of Z_p, then R_{00} is 0 or Z_p; in either case R is associative by Lemma V.1. If R_{11} is the direct sum of three copies of Z_p, then R_{11} is associative and R_{00} is 0, Z_p or $Z_p \oplus Z_p$. If $R_{00} = 0$, then $R_{10} \oplus R_{01} \cong Z_p \oplus Z_p$, so one of R_{01}, R_{10} is 0 or both are cyclic groups. In either case, R is associative by Lemma V.1. If R_{00} is isomorphic to Z_p or $Z_p \oplus Z_p$, similar arguments again imply associativity. The complicated cases are those where R_{11} is the direct sum of one or two copies of Z_p.

Case 1a: $R_{11} = \langle e \rangle \oplus \langle a \rangle \cong Z_p \oplus Z_p$ is the direct sum of two copies of Z_p. Here, R_{00} will be the direct sum of at most three copies of Z_p. If R_{00} is not 0, Lemma V.1 readily gives that R is an associative ring. The remaining case requires more thought.

Suppose $R_{00} = 0$. Then $R_{10} \oplus R_{01} \cong Z_p \oplus Z_p \oplus Z_p$ and, by Lemma V.1, we may assume that neither R_{10} nor R_{01} is 0.

If $R_{10} = \langle c \rangle \oplus \langle d \rangle \cong Z_p \oplus Z_p$ and $R_{01} = \langle b \rangle \cong Z_p$, the products amongst e, a, b, c, d are as shown in Table 1 with i, j, k and all x_i, y_i, z_i, r_i, s_i in F_p.

Since $[e, c, d] = cd - e(jb) = jb - 0 = jb$ and $[e, c, d] = -[e, d, c] = -dc + e(kb) = -kb$, we must have $k = -j$. Since the only associators amongst $\{e, a, b, c, d\}$ which are not automatically 0 are $[e, c, d] = jb$ and $[a, c, d] = -[d, c, a] = (dc)a - d(ca) =$

TABLE 1.

	e	a	b	c	d
e	e	a	0	c	d
a	a	$x_0e + x_1a$	0	$y_0c + y_1d$	$s_0c + s_1d$
b	b	ib	0	0	0
c	0	0	$z_0e + z_1a$	0	jb
d	0	0	$r_0e + r_1a$	kb	0

$kba - 0 = kib = -jib$, we must have $j \neq 0$. Replacing c by $j^{-1}c$, we may assume $j = 1$ (and $k = -1$).

If $i \neq 0$, we can replace b by $i^{-1}b$ and assume $i = 1$. With respect to the basis $\{e, a - e, b, c, d\}$, the multiplication table takes the form shown below for suitable $x_i', y_i', z_i', r_i', s_i'$.

	e	$a - e$	b	c	d
e	e	$a - e$	0	c	d
$a - e$	$a - e$	$x_0'e + x_1'(a - e)$	0	$y_0'c + y_1'd$	$s_0'c + s_1'd$
b	b	0	0	0	0
c	0	0	$z_0'e + z_1'a$	0	b
d	0	0	$r_0'e + r_1'(a - e)$	$-b$	0

It follows that we may assume $i = 0$ in Table 1. In this case, all parameters except x_1 are fixed as the following calculations show.

- $ba^2 = (ba)a = 0 \implies b(x_0e + x_1a) = x_0b = 0$, so $x_0 = 0$;
- $0 = c^2d = c(cd) = cb = z_0e + z_1a \implies z_0 = z_1 = 0$.
- $0 = d^2c = d(dc) = -db = -(r_0e + r_1a) \implies r_0 = r_1 = 0$;
- $d(a + c)^2 = d(a^2 + ac + ca + c^2) = d(x_0e + x_1a) + d(y_0c + y_1d) = -y_0b$ and $(d(a + c))(a + c) = -b(a + c) = 0 \implies y_0 = 0$;
- $c(a + c)^2 = c(a^2 + ac + ca + c^2) = c(x_0e + x_1a) + c(y_0c + y_1d) = y_1b$ and $(c(a + c))(a + c) = 0 \implies y_1 = 0$;

- $d(a+d)^2 = d(a^2+ad+da+d^2) = d(x_0e+x_1a)+d(s_0c+s_1d) = -s_0b$ and $(d(a+d))(a+d) = 0 \implies s_0 = 0$;
- $c(a+d)^2 = c(a^2+ad+da+d^2) = c(x_0e+x_1a)+c(s_0c+s_1d) = s_1b$ and $(c(a+d))(a+d) = b(a+d) = 0 \implies s_1 = 0$.

At this point, our table is

	e	a	b	c	d
e	e	a	0	c	d
a	a	x_1a	0	0	0
b	b	0	0	0	0
c	0	0	0	0	b
d	0	0	0	$-b$	0

Any such table defines an alternative ring. In any ring with $x_1 \neq 0$, we may assume $x_1 = 1$ by replacing a by $x_1^{-1}a$. Then, with respect to the basis $\{e-a, a, b, c, d\}$, we get the table

	$e-a$	a	b	c	d
$e-a$	$e-a$	0	0	c	d
a	0	a	0	0	0
b	b	0	0	0	0
c	0	0	0	0	b
d	0	0	0	$-b$	0

in which $e-a$ and a are orthogonal idempotents. Not possessing orthogonal idempotents, the ring with $x_1 = 0$ is not isomorphic to the ring with $x_1 = 1$.

We have obtained two new rings which are alternative but not associative (cf Section 6) , defined by the following tables.

5/1:

	e	a	b	c	d
e	e	a	0	c	d
a	a	0	0	0	0
b	b	0	0	0	0
c	0	0	0	0	b
d	0	0	0	$-b$	0

5/2:

	e	a	b	c	d
e	e	0	0	c	d
a	0	a	0	0	0
b	b	0	0	0	0
c	0	0	0	0	b
d	0	0	0	$-b$	0

If $R_{01} \cong \mathbb{Z}_p \oplus \mathbb{Z}_p$ and $R_{10} \cong \mathbb{Z}_p$, the rings obtained are anti-isomorphic to the ones just described because under the opposite operation, R_{01} and R_{10} are interchanged. Thus we get two more rings.

5/3:

	e	a	b	c	d
e	e	a	b	0	0
a	a	0	0	0	0
b	0	0	0	0	0
c	c	0	0	0	b
d	d	0	0	$-b$	0

5/4:

	e	a	b	c	d
e	e	0	b	0	0
a	0	a	0	0	0
b	0	0	0	0	0
c	c	0	0	0	b
d	d	0	0	$-b$	0

Note that 5/2 (respectively 5/4) is the ring direct sum of 4/2 (respectively 4/1) and the one-dimensional algebra over F_p with basis a and $a^2 = a$.

Case 1b: $R_{11} = \langle e \rangle \cong \mathbb{Z}_p$. Here R_{00} is the direct sum of at most four copies of $\mathbb{Z}_p$.

If $R_{00} = 0$, then $R_{01} \oplus R_{10} \cong \mathbb{Z}_p \oplus \mathbb{Z}_p \oplus \mathbb{Z}_p \oplus \mathbb{Z}_p$. Moreover, we may assume $R_{01} \neq 0$ and $R_{10} \neq 0$ by Lemma V.1.

If $R_{01} = \langle a \rangle \cong \mathbb{Z}_p$ and $R_{10} = \langle b \rangle \oplus \langle c \rangle \oplus \langle d \rangle \cong \mathbb{Z}_p \oplus \mathbb{Z}_p \oplus \mathbb{Z}_p$, we have a multiplication table of the form

	e	a	b	c	d
e	e	0	b	c	d
a	a	$y_0 b + y_1 c + y_2 d$	0	0	0
b	0	$x_0 e$	0	$z_0 a$	$z_1 a$
c	0	$x_1 e$	$z_2 a$	0	$z_3 a$
d	0	$x_2 e$	$z_4 a$	$z_5 a$	0

where the x_i, y_i and z_i are elements of F_p. The following arguments fix some of the parameters:

- $(ba)b = (x_0e)b = x_0b$ and $b(ab) = 0 \implies x_0 = 0$;
- $(ca)c = (x_1e)c = x_1c$ and $c(ac) = 0 \implies x_1 = 0$;
- $(da)d = (x_2e)d = x_2d$ and $d(ad) = 0 \implies x_2 = 0$;
- $ea^2 = e(y_0b+y_1c+y_2d) = y_0b+y_1c+y_2d$ and $(ea)a = 0 \implies y_0 = y_1 = y_2 = 0$;
- $[e,b,c] = bc-e(z_0a) = bc = z_0a$ and $[e,b,c] = -[e,c,b] = -cb+e(z_2a) = -cb = -z_2a \implies z_2 = -z_0$;
- $[e,b,d] = bd-e(bd) = bd-e(z_1a) = z_1a$ and $[e,b,d] = -[e,d,b] = -db+e(z_4a) = -z_4a \implies z_4 = -z_1$;
- $[e,c,d] = cd-e(z_3a) = z_3a$ and $[e,c,d] = -[e,d,c] = -dc+e(z_5a) = -z_5a \implies z_5 = -z_3$.

The table is now

	e	a	b	c	d
e	e	0	b	c	d
a	a	0	0	0	0
b	0	0	0	z_0a	z_1a
c	0	0	$-z_0a$	0	z_3a
d	0	0	$-z_1a$	$-z_3a$	0

and, since $[e,a,b] = [e,a,c] = [e,a,d] = [a,b,c] = [a,b,d] = [b,c,d] = [a,c,d] = 0$, to avoid associativity, one of z_0, z_1, z_3 must be nonzero. Since $\{b,c,d\}$ is a basis for R_{10}, there is no loss of generality in assuming $z_0 \neq 0$. Replacing b by $z_0^{-1}b$, we may assume that $bc = a$ and $cb = -a$. Finally, replacing $\{b,c,d\}$ by $\{b+z_1c, c, d+z_3b-z_1c\}$ as basis for R_{10}, we obtain

	e	a	$b+z_1c$	c	$d+z_3b-z_1c$
e	e	0	$b+z_1c$	c	$d+z_3b-z_1c$
a	a	0	0	0	0
$b+z_1c$	0	0	0	a	0
c	0	0	$-a$	0	0
$d+z_3b-z_1c$	0	0	0	0	0

which can be checked as follows:

Since $ea = 0, eb = b$, $ec = c$ and $ed = d$, we have the first row. The second row follows from the fact that a is a left annihilator. For the third row, we have:

- $(b + z_1c)e = 0; (b + z_1c)a = 0; (b + z_1c)^2 = b^2 + z_1(bc + cb) + (z_1c)^2 = 0;$
- $(b+z_1c)c = a; (b+z_1c)(d+z_3b-z_1c) = z_1a - z_1a + z_1z_3a + z_1z_3(-a) = 0.$ The fourth row is obvious. For the fifth row, we have
- $(d + z_3b - z_1c)e = (d + z_3b - z_1c)a = 0;$
- $(d + z_3b - z_1c)(b + z_1c) = -z_1a + z_1(-z_3a) + z_3z_1a - z_1(-a) = 0,$
- $(d + z_3b - z_1c)c = -z_3a + z_3a = 0,$
- $(d + z_3b - z_1c)^2 = d^2 + z_1z_3(bc + cb) + z_3(bd + db) - z_1(dc + cd) + z_1^2c^c = 0.$

After the obvious change of basis, it defines a new ring which is alternative, but not associative (cf Section 6).

5/5:

	e	a	b	c	d
e	e	0	b	c	d
a	a	0	0	0	0
b	0	0	0	a	0
c	0	0	$-a$	0	0
d	0	0	0	0	0

If $R_{01} = \langle a \rangle \oplus \langle b \rangle \cong \mathbb{Z}_p \oplus \mathbb{Z}_p$ and $R_{10} = \langle c \rangle \oplus \langle d \rangle \cong \mathbb{Z}_p \oplus \mathbb{Z}_p$, we have the table

	e	a	b	c	d
e	e	0	0	c	d
a	a	0	$x_0c + x_1d$	0	0
b	b	$x_2c + x_3d$	0	0	0
c	0	x_4e	x_5e	0	$y_0a + y_1b$
d	0	x_6e	x_7e	$z_0a + z_1b$	0

with all x_i, y_i, z_i in F_p. Observe

- $(ca)c = x_4ec = x_4c$ and $c(ac) = 0 \implies x_4 = 0;$
- $(cb)c = x_5ec = x_5c$ and $c(bc) = 0 \implies x_5 = 0;$
- $(da)d = x_6ed = x_6d$ and $d(ad) = 0 \implies x_6 = 0;$

- $(db)d = x_7ed = x_7d$ and $d(bd) = 0 \implies x_7 = 0$;
- $[e,a,b] = -e(ab) = -e(x_0c + x_1d) = -x_0c - x_1d$ and $[e,a,b] = -[e,b,a] = e(ba) = e(x_2c + x_3d) = x_2c + x_3d \implies x_2 = -x_0$ and $x_3 = -x_1$;
- $[e,c,d] = cd - e(y_0a + y_1b) = cd = y_0a + y_1b$ and $[e,c,d] = -[e,d,c] = -dc + e(z_0a + z_1b) = -dc = -z_0a - z_1b \implies y_0 = -z_0$ and $y_1 = -z_1$.

This gives the table

	e	a	b	c	d
e	e	0	0	c	d
a	a	0	$x_0c + x_1d$	0	0
b	b	$-x_0c - x_1d$	0	0	0
c	0	0	0	0	$y_0a + y_1b$
d	0	0	0	$-y_0a - y_1b$	0

Since

- $[e,a,b] = -x_0c - x_1d$;
- $[e,c,d] = y_0a + y_1b$;
- $[e,a,c] = [e,a,d] = [e,b,c] = [e,b,d] = 0$;
- $[a,b,c] = (x_0c + x_1d)c = -x_1(y_0a + y_1b)$;
- $[a,b,d] = (x_0c + x_1d)d = x_0(y_0a + y_1b)$;
- $[b,c,d] = -b(y_0a + y_1b) = y_0(x_0c + x_1d)$;
- $[a,c,d] = -a(y_0a + y_1b) = -y_1(x_0c + x_1d)$;

in order to avoid associativity, either $x_0c + x_1d$ or $y_0a + y_1b$ must be nonzero.

Suppose $x_0c + x_1d \neq 0$. Since $(a+b+c)^2d = (a^2+b^2+c^2+ab+ba+ac+ca+bc+cb)d = 0$ while $(a+b+c)[(a+b+c)d] = (a+b+c)(y_0a+y_1b) = (y_1-y_0)(x_0c+x_1d)$ we must have $y_0 = y_1$. On the other hand, since $(a+d)^2c = 0$ and $(a+d)[(a+d)c] = (a+d)(-y_0a - y_1b) = -y_1(x_0c+x_1d)$ we know that $y_1 = 0$. Now, replacing $\{c,d\}$ by $\{x_0c+x_1d, d\}$ as basis for R_{10}, we obtain the multiplication table for a new alternative ring which is not associative (cf Section 6).

5/6:

	e	a	b	c	d
e	e	0	0	c	d
a	a	0	c	0	0
b	b	$-c$	0	0	0
c	0	0	0	0	0
d	0	0	0	0	0

Similarly, if $y_0a + y_1b \neq 0$, we obtain the ring defined by the following table.

5/7:

	e	a	b	c	d
e	e	0	0	c	d
a	a	0	0	0	0
b	b	0	0	0	0
c	0	0	0	0	a
d	0	0	0	$-a$	0

If $R_{01} \cong Z_p \oplus Z_p \oplus Z_p$ and $R_{10} \cong Z_p$, the rings are anti-isomorphic to those considered previously. We find one new ring (anti-isomorphic to 5/5).

5/8:

	e	a	b	c	d
e	e	a	0	0	0
a	0	0	0	0	0
b	b	0	0	a	0
c	c	0	$-a$	0	0
d	d	0	0	0	0

If $R_{00} \cong Z_p$, then $R_{10} \oplus R_{01} \cong Z_p \oplus Z_p \oplus Z_p$. Any alternative ring with $R_{01} = 0$ and $R_{10} \cong Z_p \oplus Z_p \oplus Z_p$ or with $R_{01} \cong Z_p \oplus Z_p \oplus Z_p$ and $R_{10} = 0$ is associative by part (a) of Lemma V.1. This leaves two cases.

If $R_{01} = \langle b \rangle \cong Z_p$ and $R_{10} = \langle c \rangle \oplus \langle d \rangle \cong Z_p \oplus Z_p$, we have a multiplication table of the following sort

	e	a	b	c	d
e	e	0	0	c	d
a	0	x_0a	x_1b	0	0
b	b	0	0	x_2a	x_3a
c	0	x_4c+x_5d	x_6e	0	ib
d	0	x_7c+x_8d	x_9e	jb	0

where i, j and all x_i are in F_p.

Of the ten possible associators of basis elements (order irrelevant), the only ones which are not automatically zero are $[e,c,d] = cd - e(ib) = cd = ib$ and $[a,c,d] = 0 - a(ib) = -ix_1b$. In order to avoid associativity, we must have $i \neq 0$. Moreover, since $ib = [e,c,d] = -[e,d,c] = -dc + e(jb) = -jb$, we have also $j = -i$. Replacing c by $i^{-1}c$, we may assume $i = 1$, $j = -1$.

Observe

- $(dc)d = (jb)d = -x_3a$ and $d(cd) = d(ib) = x_9e \implies x_3 = x_9 = 0$;
- $(cd)c = (ib)c = x_2a$ and $c(dc) = c(jb) = -x_6e \implies x_2 = x_6 = 0$;
- $(ca)c = (x_4c + x_5d)c = x_5(jb) = -x_5b$ and $c(ac) = 0 \implies x_5 = 0$;
- $(da)d = (x_7c + x_8d)d = x_7(ib) = x_7b$ and $d(ad) = 0 \implies x_7 = 0$;
- $(a+c)^2d = (x_0a+x_4c+x_5d)d = x_4(ib) = x_4b$ and $(a+c)[(a+c)d] = (a+c)(ib) = x_1b + x_6e = x_1b \implies x_1 = x_4$;.
- $(a+d)^2c = (x_0a + x_7c + x_8d)c = x_8(jb) = -x_8b$ and $(a+d)[(a+d)c] = (a+d)(jb) = -(x_1b + x_9e) = -x_1b \implies x_1 = x_8$.

Set $x_1 = x_4 = x_8 = k$. Then

$$(a+c)^2a = (x_0a + x_4c + x_5d)a = (x_0a + kc)a = x_0^2a + k^2c$$

and

$$(a+c)((a+c)a) = (a+c)(x_0a + kc) = x_0^2a + x_0(x_4c + x_5d) = x_0^2a + x_0kc$$

implies $k^2 = x_0k$. If $k = x_0 = 0$, we obtain

5/9:

	e	a	b	c	d
e	e	0	0	c	d
a	0	0	0	0	0
b	b	0	0	0	0
c	0	0	0	0	b
d	0	0	0	$-b$	0

which is the ring direct sum of 4/2 and the one-dimensional trivial algebra with basis a. If $k = 0$ and $x_0 \neq 0$ (without loss of generality, $x_0 = 1$), the ring is the direct sum of 4/2 and the one-dimensional algebra over F_p with basis a and $a^2 = a$. This is the ring 5/2 already determined. If $k \neq 0$, then $k = x_0$ and we get the following table:

	e	a	b	c	d
e	e	0	0	c	d
a	0	ka	kb	0	0
b	b	0	0	0	0
c	0	kc	0	0	b
d	0	kd	0	$-b$	0

For any element Y in this ring, it is easy to check that $(ke + a)Y = kY$ and $Y(ke + a) = kY$, thus the element $(1/k)(ke + a)$ is a unity and our ring is the unique ring identified in Theorem VI.9.

If $R_{01} \cong Z_p \oplus Z_p$ and $R_{10} \cong Z_p$, the rings obtained are anti-isomorphic to those just considered. We find one new alternative ring,

5/10:

	e	a	b	c	d
e	e	0	b	0	0
a	0	0	0	0	0
b	0	0	0	0	0
c	c	0	0	0	b
d	d	0	0	$-b$	0

which is the ring direct sum of 4/1 and the one-dimensional algebra over F_p with basis a and trivial multiplication.

If $R_{00} \cong Z_p \oplus Z_p$, then $R_{10} \oplus R_{01} \cong Z_p \oplus Z_p$ and there are no alternative rings which are not associative, by Lemma V.1.

If $R_{00} \cong Z_p \oplus Z_p \oplus Z_p$, then R_{10} and R_{01} are either 0 or cyclic groups, so the ring is associative by Lemma V.1.

If $R_{00} \cong Z_p \oplus Z_p \oplus Z_p \oplus Z_p$, then the ring $R = R_{00} \oplus R_{11}$ is a direct sum of a ring of order p and another of order p^4, and these cases have already been included in our enumeration.

Examining all the rings determined in this section to this point, we see that they all contain one of the rings 4/1 or 4/2. In fact, assuming that the basis elements of 4/1 or 4/2 are e, a, b, c with multiplication tables as defined in Theorem VI.4, they are all extensions of one of these rings by a one-dimensional ideal generated over F_p by d. Specifically, they have the following structure ($\oplus$ here indicating ring direct sum).

5/1: $4/2 + Z_p d$, $d^2 = 0$, $ed = de = d$, $ad = da = bd = db = cd = dc = 0$;
5/2: $4/2 \oplus Z_p d$, $d^2 = d$;
5/3: $4/1 + Z_p d$, $d^2 = 0$, $ed = de = d$, $ad = da = bd = db = cd = dc = 0$;
5/4: $4/1 \oplus Z_p d$, $d^2 = d$;
5/5: $4/2 + Z_p d$, $d^2 = 0$, $ed = d$, $de = 0 = ad = da = bd = db = cd = dc = 0$;
5/6: $4/1 + Z_p d$, $d^2 = 0$, $ed = d$, $de = 0 = ad = da = bd = db = cd = dc = 0$;
5/7: $4/2 + Z_p d$, $d^2 = 0$, $de = d$, $ed = ad = da = bd = db = cd = dc = 0$;
5/8: $4/1 + Z_p d$, $d^2 = 0$, $de = d$, $ed = ad = da = bd = db = cd = dc = 0$;
5/9: $4/2 \oplus Z_p d$, $d^2 = 0$;
5/10: $4/1 \oplus Z_p d$, $d^2 = 0$.

Case 2: $R_+ \cong Z_{p^2} \oplus Z_p \oplus Z_p \oplus Z_p$. Since R has no unity, $R_{11} \neq R$. If $R_{11} \cong Z_{p^2} \oplus Z_p \oplus Z_p$, then R_{11} is an alternative ring of order p^4 which is not an algebra over F_p, so it is associative by Theorem VI.4. If $R_{11} \cong Z_p \oplus Z_p \oplus Z_p$ or $R_{11} \cong Z_{p^2} \oplus Z_p$ or $R_{11} \cong Z_p \oplus Z_p$, it is also associative. In each of these cases, R_{00} is associative too and, if neither R_{10} nor R_{01} is zero, they are both cyclic groups. By Lemma V.1, R is associative. There remain the cases $R_{11} \cong Z_{p^2}$ and $R_{11} \cong Z_p$.

Case 2a: $R_{11} = \langle e \rangle \cong Z_{p^2}$. If $R_{00} \cong Z_p \oplus Z_p$ or $Z_p \oplus Z_p \oplus Z_p$, then R is associative by Lemma V.1. If $R_{00} \cong Z_p$, then $R_{10} \oplus R_{01} \cong Z_p \oplus Z_p$ and again

Lemma V.1 says that R is associative. If $R_{00} = 0$, then $R_{10} \oplus R_{01} \cong Z_p \oplus Z_p \oplus Z_p$, and, using Lemma V.1, there are just two situations in which there could exist a ring which is not associative.

If $R_{01} = \langle a \rangle \cong Z_p$, $R_{10} = \langle b \rangle \oplus \langle c \rangle \cong Z_p \oplus Z_p$ the multiplication table for the basis of R looks like

	e	a	b	c
e	e	0	b	c
a	a	0	0	0
b	0	ie	0	ja
c	0	ke	ma	0

where i, j, k and m are elements of F_p. Since $[e,a,b] = [e,a,c] = [a,b,c] = 0$ while $[e,b,c] = ja$, to avoid associativity, we must have $j \neq 0$. Since $ma = [c,b,e] = -[e,b,c]$, we have $m = -j$. Since $(a+b)^2a = (a^2 + ab + ba + b^2)b = (ie)b = ib$ and $(a+b)[(a+b)b] = 0$, we have $i = 0$. Since $kc = (a+c)^2c = (a+c)[(a+c)c] = 0$, also $k = 0$. We now have the table

	e	a	b	c
e	e	0	b	c
a	a	0	0	0
b	0	0	0	ja
c	0	0	$-ja$	0

and, without loss of generality, we may assume $j = 1$. We obtain another alternative ring which is not associative, with the following multiplication table for a basis.

5/11:

	e	a	b	c
e	e	0	b	c
a	a	0	0	0
b	0	0	0	a
c	0	0	$-a$	0

If $R_{01} \cong Z_p \oplus Z_p$ and $R_{10} \cong Z_p$, the rings determined are anti-isomorphic to those just discussed. We obtain one more ring, with multiplication specified as shown.

5/12:

	e	a	b	c
e	e	a	0	0
a	0	0	0	0
b	b	0	0	a
c	c	0	$-a$	0

Case 2b: $R_{11} = \langle e \rangle \cong \mathbf{Z_p}$. In this case, if $x \in R_{10}$, then $px = p(ex) = (pe)x = 0$; similarly, $px = 0$ for any $x \in R_{01}$. Thus R_{00} contains a subgroup isomorphic to Z_{p^2}. If $R_{00} \cong Z_{p^2} \oplus Z_p$ or $R_{00} \cong Z_{p^2} \oplus Z_p \oplus Z_p$, then the ring is associative by Lemma V.1. If $R_{00} \cong Z_{p^2}$, then $R_{10} \oplus R_{01} \cong Z_p \oplus Z_p$ and, by Lemma V.1, any such ring is associative.

THEOREM VI.10. *Let p be a prime. There are twelve alternative rings of order p^5 which are not associative and do not have a unity. Of these, ten are 5-dimensional algebras over F_p with 4-dimensional nil radicals and two have additive structure $Z_{p^2} \oplus Z_p \oplus Z_p \oplus Z_p$ with nil radicals which are 3-dimensional algebras over F_p. Moreover all the rings are group-graded rings with the grading as in Proposition V.3.*

PROOF. By the arguments above and the proofs in Section 6 and Section 7. □

Bearing in mind that any finite ring is the direct product of ideals each of which has prime power order, Theorems VI.10 and VI.4 make clear that we have found in this chapter all alternative rings of order less than 64.

COROLLARY VI.11. *There are fifteen alternative rings of order less than 64 which are not associative. Two have order 16; thirteen have order 32. None is nilpotent. Only one, of order 32, has a unity.*

COROLLARY VI.12. *None of the alternative rings of order p^n, $n \leq 5$, is a Cayley-Dickson algebra or an alternative loop algebra.*

PROOF. Note that both kinds of alternative rings mentioned have unities. From Theorem VI.4 and Theorem VI.9, only one ring of order p^5 has a unity. By Theorem VI.9, this ring is a Z_p algebra, so it is not a Cayley-Dickson algebra because a finite Cayley-Dickson algebra over Z_p has order p^8 and it is not a loop algebra since the smallest RA loop has order 16 and then the loop algebra has order at least 2^{16}. □

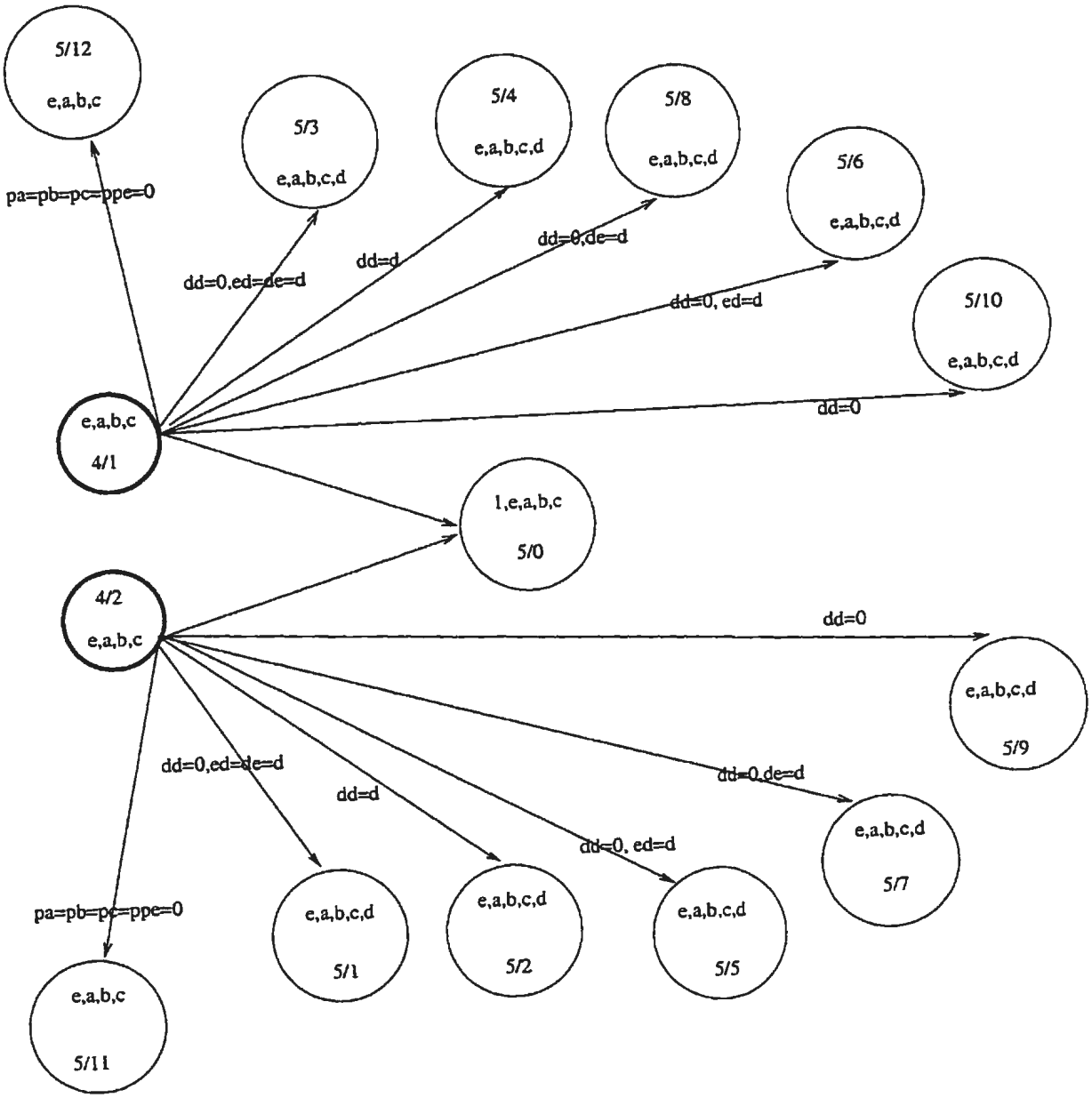

FIGURE VI.1. The fifteen alternative rings of order p^n, $n \leq 5$.

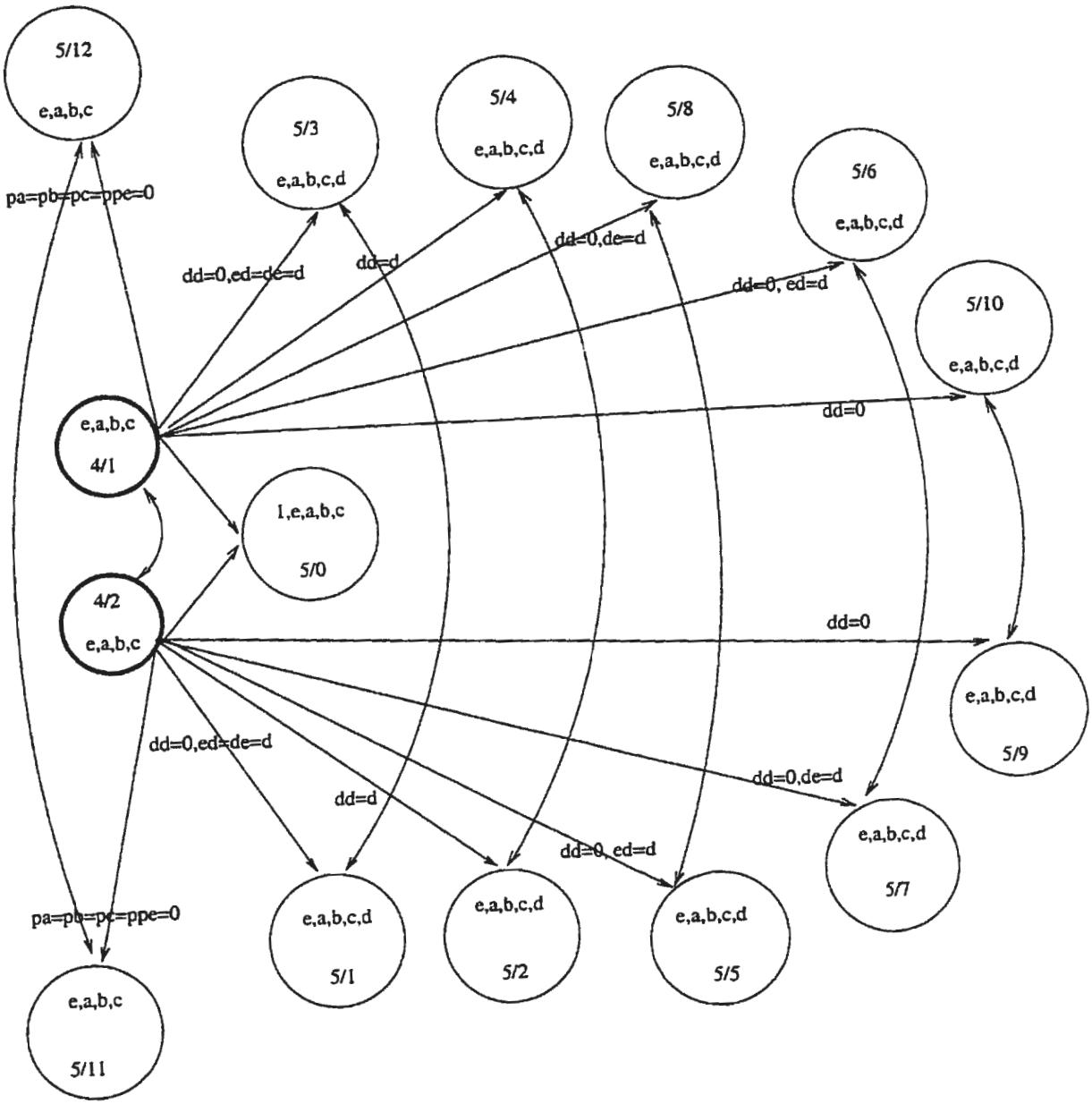

FIGURE VI.2. The anti-isomorphism structure of the fifteen alternative rings of order p^n, $n \leq 5$.

6. The 12 rings of order p^5

Now let us check that the above 12 rings are really alternative rings, and moreover, they are not isomorphic to each other.

Since 5/11 and 5/12 have the same tables as those of 4/2 and 4/1, respectively, and $p^2a = p^2b = p^2c = 0$, these rings are alternative.

Let us show that the remaining ten rings are alternative. From the figure, we just need to check 5/1, 5/2, 5/5, 5/7 and 5/9. Since 5/2 and 5/9 are ring direct sums of 4/2 and an associative ring, it remains only to show that 5/1, 5/5 and 5/7 are alternative rings.

6.1. 5/1 is an alternative ring: Let

$$X = x_0e + x_1a + x_2b + x_3c + x_4d$$

be an arbitrary element in the ring. We check the left alternative law first.

From the table we have

$$X^2 = x_0^2e + 2x_0x_1a + x_0x_2b + x_0x_3c + x_0x_4d.$$

Then the left matrix can be determined by the left transformation:

$$\begin{bmatrix} Xe \\ Xa \\ Xb \\ Xc \\ Xd \end{bmatrix} = \begin{bmatrix} x_0 & x_1 & x_2 & 0 & 0 \\ 0 & x_0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & -x_4 & x_0 & 0 \\ 0 & 0 & x_3 & 0 & x_0 \end{bmatrix} \cdot \begin{bmatrix} e \\ a \\ b \\ c \\ d \end{bmatrix}$$

Therefore

$$M_l(X) = \begin{bmatrix} x_0 & x_1 & x_2 & 0 & 0 \\ 0 & x_0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & -x_4 & x_0 & 0 \\ 0 & 0 & x_3 & 0 & x_0 \end{bmatrix}$$

Similarly, for the element X^2, we have

$$\begin{bmatrix} X^2e \\ X^2a \\ X^2b \\ X^2c \\ X^2d \end{bmatrix} = \begin{bmatrix} x_0^2 & 2x_0x_1 & x_0x_2 & 0 & 0 \\ 0 & x_0^2 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & -x_0x_4 & x_0^2 & 0 \\ 0 & 0 & x_0x_3 & 0 & x_0^2 \end{bmatrix} \cdot \begin{bmatrix} e \\ a \\ b \\ c \\ d \end{bmatrix}$$

Therefore

$$M_l(X^2) = \begin{bmatrix} x_0^2 & 2x_0x_1 & x_0x_2 & 0 & 0 \\ 0 & x_0^2 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & -x_0x_4 & x_0^2 & 0 \\ 0 & 0 & x_0x_3 & x_0^2 & 0 \end{bmatrix}$$

It is easy to check that

$$M_l(X)M_l(X) = M_l(X^2).$$

Thus the ring is left alternative. To check it is a right alternative ring, we have

$$\begin{bmatrix} eX \\ aX \\ bX \\ cX \\ dX \end{bmatrix} = \begin{bmatrix} x_0 & x_1 & 0 & x_3 & x_4 \\ 0 & x_0 & 0 & 0 & 0 \\ 0 & 0 & x_0 & 0 & 0 \\ 0 & 0 & x_4 & 0 & 0 \\ 0 & 0 & -x_3 & 0 & 0 \end{bmatrix} \cdot \begin{bmatrix} e \\ a \\ b \\ c \\ d \end{bmatrix}$$

Therefore

$$M_r(X) = \begin{bmatrix} x_0 & x_1 & 0 & x_3 & x_4 \\ 0 & x_0 & 0 & 0 & 0 \\ 0 & 0 & x_0 & 0 & 0 \\ 0 & 0 & x_4 & 0 & 0 \\ 0 & 0 & -x_3 & 0 & 0 \end{bmatrix}$$

Similarly, for the element X^2, we have

$$\begin{bmatrix} eX^2 \\ aX^2 \\ bX^2 \\ cX^2 \\ dX^2 \end{bmatrix} = \begin{bmatrix} x_0^2 & 2x_0x_1 & 0 & x_0x_3 & x_0x_4 \\ 0 & x_0^2 & 0 & 0 & 0 \\ 0 & 0 & x_0^2 & 0 & 0 \\ 0 & 0 & x_0x_4 & 0 & 0 \\ 0 & 0 & -x_0x_3 & 0 & 0 \end{bmatrix} \cdot \begin{bmatrix} e \\ a \\ b \\ c \\ d \end{bmatrix}$$

and

$$M_r(X^2) = \begin{bmatrix} x_0^2 & 2x_0x_1 & 0 & x_0x_3 & x_0x_4 \\ 0 & x_0^2 & 0 & 0 & 0 \\ 0 & 0 & x_0^2 & 0 & 0 \\ 0 & 0 & x_0x_4 & 0 & 0 \\ 0 & 0 & -x_0x_3 & 0 & 0 \end{bmatrix}$$

It is easy to check that $M_r(X)M_r(X) = M_r(X^2)$ and then, the ring is right alternative. From the construction of the ring, we know it is not associative. So this ring is an alternative ring which is not associative.

6.2. 5/5 is an alternative ring: Let

$$X = x_0e + x_1a + x_2b + x_3c + x_4d$$

be an arbitrary element in the ring. We check the left alternative law first.

From the table we have

$$X^2 = x_0^2e + x_0x_1a + x_0x_2b + x_0x_3c + x_0x_4d.$$

Then the left matrix can be determined by the left transformation:

$$\begin{bmatrix} Xe \\ Xa \\ Xb \\ Xc \\ Xd \end{bmatrix} = \begin{bmatrix} x_0 & x_1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & -x_3 & x_0 & 0 & 0 \\ 0 & x_2 & 0 & x_0 & 0 \\ 0 & 0 & 0 & 0 & x_0 \end{bmatrix} \cdot \begin{bmatrix} e \\ a \\ b \\ c \\ d \end{bmatrix} = M_l(X) \begin{bmatrix} e \\ a \\ b \\ c \\ d \end{bmatrix}.$$

Similarly, for the element X^2, we have

$$\begin{bmatrix} X^2e \\ X^2a \\ X^2b \\ X^2c \\ X^2d \end{bmatrix} = \begin{bmatrix} x_0^2 & x_0x_1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & -x_0x_3 & x_0^2 & 0 & 0 \\ 0 & x_0x_2 & 0 & x_0^2 & 0 \\ 0 & 0 & 0 & 0 & x_0^2 \end{bmatrix} \cdot \begin{bmatrix} e \\ a \\ b \\ c \\ d \end{bmatrix} = M_l(X^2) \begin{bmatrix} e \\ a \\ b \\ c \\ d \end{bmatrix}.$$

It is easy to check that

$$M_l(X)M_l(X) = M_l(X^2).$$

Thus the ring is left alternative. To check it is a right alternative ring, we have

$$\begin{bmatrix} eX \\ aX \\ bX \\ cX \\ dX \end{bmatrix} = \begin{bmatrix} x_0 & 0 & x_2 & x_3 & x_4 \\ 0 & x_0 & 0 & 0 & 0 \\ 0 & x_3 & 0 & 0 & 0 \\ 0 & -x_2 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \end{bmatrix} \cdot \begin{bmatrix} e \\ a \\ b \\ c \\ d \end{bmatrix} = M_r(X) \begin{bmatrix} e \\ a \\ b \\ c \\ d \end{bmatrix}.$$

Similarly, for the element X^2, we have

$$\begin{bmatrix} eX^2 \\ aX^2 \\ bX^2 \\ cX^2 \\ dX^2 \end{bmatrix} = \begin{bmatrix} x_0^2 & 0 & x_0x_2 & x_0x_3 & x_0x_4 \\ 0 & x_0^2 & 0 & 0 & 0 \\ 0 & x_0x_3 & 0 & 0 & 0 \\ 0 & -x_0x_2 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \end{bmatrix} \cdot \begin{bmatrix} e \\ a \\ b \\ c \\ d \end{bmatrix} = M_r(X^2) \begin{bmatrix} e \\ a \\ b \\ c \\ d \end{bmatrix}.$$

It is easy to check that $M_r(X)M_r(X) = M_r(X^2)$ and then, the ring is right alternative. From the construction of the ring, we know it is not associative. So this ring is an alternative ring which is not associative.

6.3. 5/7 is an alternative ring: Let

$$X = x_0e + x_1a + x_2b + x_3c + x_4d$$

be an arbitrary element in the ring. We check the left alternative law first.

From the table we have

$$X^2 = x_0^2 e + x_0 x_1 a + x_0 x_2 b + x_0 x_3 c + x_0 x_4 d.$$

Then the left matrix can be determined by the left transformation:

$$\begin{bmatrix} Xe \\ Xa \\ Xb \\ Xc \\ Xd \end{bmatrix} = \begin{bmatrix} x_0 & x_1 & x_2 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & -x_4 & 0 & x_0 & 0 \\ 0 & x_3 & 0 & 0 & x_0 \end{bmatrix} \cdot \begin{bmatrix} e \\ a \\ b \\ c \\ d \end{bmatrix} = M_l(X) \begin{bmatrix} e \\ a \\ b \\ c \\ d \end{bmatrix}.$$

Similarly, for the element X^2, we have

$$\begin{bmatrix} X^2e \\ X^2a \\ X^2b \\ X^2c \\ X^2d \end{bmatrix} = \begin{bmatrix} x_0^2 & x_0x_1 & x_0x_2 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & -x_0x_4 & 0 & x_0^2 & 0 \\ 0 & x_0x_3 & 0 & 0 & x_0^2 \end{bmatrix} \cdot \begin{bmatrix} e \\ a \\ b \\ c \\ d \end{bmatrix} = M_l(X^2) \begin{bmatrix} e \\ a \\ b \\ c \\ d \end{bmatrix}.$$

It is easy to check that

$$M_l(X)M_l(X) = M_l(X^2).$$

Thus the ring is left alternative.

To check it is a right alternative ring, we have

$$\begin{bmatrix} eX \\ aX \\ bX \\ cX \\ dX \end{bmatrix} = \begin{bmatrix} x_0 & 0 & 0 & x_3 & x_4 \\ 0 & x_0 & 0 & 0 & 0 \\ 0 & 0 & x_0 & 0 & 0 \\ 0 & x_4 & 0 & 0 & 0 \\ 0 & -x_3 & 0 & 0 & 0 \end{bmatrix} \cdot \begin{bmatrix} e \\ a \\ b \\ c \\ d \end{bmatrix} = M_r(X) \begin{bmatrix} e \\ a \\ b \\ c \\ d \end{bmatrix}.$$

Similarly, for the element X^2, we have

$$\begin{bmatrix} eX^2 \\ aX^2 \\ bX^2 \\ cX^2 \\ dX^2 \end{bmatrix} = \begin{bmatrix} x_0^2 & 0 & 0 & x_0x_3 & x_0x_4 \\ 0 & x_0^2 & 0 & 0 & 0 \\ 0 & 0 & x_0^2 & 0 & 0 \\ 0 & x_0x_4 & 0 & 0 & 0 \\ 0 & -x_0x_3 & 0 & 0 & 0 \end{bmatrix} \cdot \begin{bmatrix} e \\ a \\ b \\ c \\ d \end{bmatrix} = M_r(X^2) \begin{bmatrix} e \\ a \\ b \\ c \\ d \end{bmatrix}.$$

It is easy to check that $M_r(X)M_r(X) = M_r(X^2)$ and then, the ring is right alternative. From the construction of the ring, we know it is not associative. So this ring is an alternative ring which is not associative.

7. The 12 rings of order 32 are distinct alternative rings

For $p = 2$, we use machine computation to get the number of elements of square 0, the number of idempotents, the number of left unities, the number of left annihilators, the number of right unities, the number of right annihilators, and the number of elements that commute with all elements in the ring. From 5/1 to 5/10 the vectors of the above special elements are:

1. [9, 9, 0, 1, 0, 2, 2]
2. [18, 18, 0, 1, 0, 2, 2]
3. [9, 9, 0, 2, 0, 1, 2]
4. [8, 18, 0, 2, 0, 1, 2]
5. [17, 17, 0, 2, 0, 2, 1]
6. [17, 17, 0, 4, 0, 1, 1]
7. [17, 17, 0, 1, 0, 4, 1]
8. [17, 17, 0, 2, 0, 2, 1]
9. [9, 9, 0, 2, 0, 4, 2]
10. [9, 9, 0, 4, 0, 2, 2].

Note that only 5/5 and 5/8 have the same vectors so we have only to show that these two rings are not isomorphic. From 5/5 and the vector we know that the ring has only one nonzero left annihilator d, and Z_2d is an ideal of the ring with quotient ring 4/2. While from 5/8 and the vector we know that the only nonzero left annihilator is a and Z_2a is an ideal of the ring. But the quotient ring is

	e	b	c	d
e	e	0	0	0
b	b	0	0	0
c	c	0	0	0
d	d	0	0	0

which is an associative ring. So 5/5 and 5/8 are not isomorphic.

Therefore the ten rings are not isomorphic. Because 5/11 and 5/12 are not Z_2 algebras, and the two are distinct, the 12 rings are not isomorphic to each other.

8. Right alternative rings which are not left alternative

In this section, we exhibit a class of right alternative rings which are not left alternative. These rings have order p^4 or are of dimension 4 over a field.

THEOREM VI.13. *The following table gives us a right alternative but not left alternative algebra over any field (note that the table differs from* 4/1 *only in that* $ea = a$*):*

	e	a	b	c
e	e	0	0	0
a	0	0	0	0
b	b	0	0	a
c	c	0	$-a$	0

PROOF. Since $(e+c)^2 b = -a$ and $(e+c)((e+c)b) = 0$, the algebra is not a left alternative algebra. We use the matrix representation to show that it is right alternative.

For any element $X = x_0 e + x_1 a + x_2 b + x_3 c$ in the ring, we have

$$\begin{bmatrix} eX \\ aX \\ bX \\ cX \end{bmatrix} = \begin{bmatrix} x_0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & x_3 & x_0 & 0 \\ 0 & -x_2 & 0 & x_0 \end{bmatrix} \cdot \begin{bmatrix} e \\ a \\ b \\ c \end{bmatrix}$$

Therefore

$$M_r(X) = \begin{bmatrix} x_0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & x_3 & x_0 & 0 \\ 0 & -x_2 & 0 & x_0 \end{bmatrix}$$

Similarly, for element $X^2 = x_0^2 e + x_0 x_2 b + x_0 x_3 c$, we have

$$\begin{bmatrix} eX^2 \\ aX^2 \\ bX^2 \\ cX^2 \end{bmatrix} = \begin{bmatrix} x_0^2 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & x_0 x_3 & x_0^2 & 0 \\ 0 & -x_0 x_2 & 0 & x_0^2 \end{bmatrix} \cdot \begin{bmatrix} e \\ a \\ b \\ c \end{bmatrix}$$

and

$$M_r(X^2) = \begin{bmatrix} x_0^2 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & x_0 x_3 & x_0^2 & 0 \\ 0 & -x_0 x_2 & 0 & x_0^2 \end{bmatrix}$$

It is easy to check that $M_r(X)M_r(X) = M_r(X^2)$. So the ring is right alternative. □

REMARK VI.14. The opposite rings of rings in the above theorem are left alternative but not right alternative.

Bibliography

[Alb42] A. A. Albert. Quadratic forms permitting composition. *Anal. Math.*, 43:161–177, 1942.

[AW73] J. C. Ault and J. F. Watters. Circle groups of nilpotent rings. *Amer. Math. Monthly*, 80:48–52, 1973.

[Bad84] M. I. Badalov. Nilpotent alternative algebras. *Algebra and Logic*, 23:167–181, 1984.

[Bea48] R. A. Beaumont. Rings with additive group which is the direct sum of cyclic groups. *Duke Math. J.*, 15:367–369, 1948.

[Bov96] A. A. Bovdi. On circle groups of nilpotent rings of characteristic 2. *Period. Math. Hungar.*, 32:31–34, 1996.

[Bro67] R. Brown. On generalized Cayley-Dickson algebras. *Pacific J. Math.*, 20:415–422, 1967.

[Bru58] R. H. Bruck. *A survey of binary systems*, volume 20 of *Ergeb. Math. Grenzgeb.* Springer-Verlag, 1958.

[Cay45] A. Cayley. On Jacobi's elliptic functions, in reply to Rev. Brice Brownin and on quaternions. *Philos. Mag. and Jour. of Science*, 3:210–213, 1845.

[CG85] Orin Chein and Edgar G. Goodaire. Isomorphism of loops which have an alternative loop rings. *Comm. Algebra*, 13(1):1–20, 1985.

[CG86] Orin Chein and Edgar G. Goodaire. Loops whose loop rings are alternative. *Comm. Algebra*, 14(2):293–310, 1986.

[CG88] Orin Chein and Edgar G. Goodaire. Is a right alternative loop ring alternative? *Algebras Groups Geom.*, 5:297–304, 1988.

[CG90] Orin Chein and Edgar G. Goodaire. Loops whose loop rings in characteristic 2 are alternative. *Comm. Algebra*, 18(3):659–688, 1990.

[Che74] Orin Chein. Moufang loops of small order I. *Trans. Amer. Math. Soc.*, 188:31–51, 1974.

[Che78] Orin Chein. Moufang loops of small order. *Mem. Amer. Math. Soc.*, 13(197), 1978.

[CM84] M. Cohen and S. Montgomery. Group-graded rings, smash products, and group actions. *Trans. Amer. Math. Soc.*, 282(237–258), 1984.

[Con63] I. G. Connell. On the group ring. *Canad. J. Math.*, 15:650–685, 1963.

[CP71] O. Chein and H. O. Pflugfelder. The smallest Moufang loop. *Arch. Math. (Basel)*, 22:573–576, 1971.

[CPe90] O. Chein, H. O. Pflugfelder, and J. D. H. Smith (editors). *Quasigroups and loops: theory and applications*. Heldermann Verlag, Berlin, 1990.

[CR83] M. Cohen and L. Rowen. Group graded rings. *Comm. Algebra*, 11(1253–1270), 1983.

[Cur63] Charles W. Curtis. The four and eight square problem and division algebras. In A. A. Albert, editor, *Studies in modern algebra*, volume 2 of *Studies in Mathematics*, pages 100–125. Math. Assoc. of America, 1963.

[Dad80] E. C. Dade. Group-graded rings and modules. *Math. Z.*, 174:241–262, 1980.

[dB93a] Luiz. G. X. de Barros. Isomorphisms of rational loop algebras. *Comm. Algebra*, 21:3977–3993, 1993.

[dB93b] Luiz. G. X. de Barros. On semisimple alternative loop algebras. *Comm. Algebra*, 21:3995–4011, 1993.

[dBJ96] Luiz. G. X. de Barros and Stanley O. Juriaans. Units in integral loop rings. *J. Algebra*, 183:637–648, 1996.

[Dic19] L. E. Dickson. On quaternions and their generalization and the history of the eight square theorem. *Anal. Math.*, 20:151–171, 1919.

[Div65] N. J. Divinsky. *Rings and radicals*. Number 14 in Mathematical Expositions. University of Toronto Press, Toronto, 1965.

[ES90] P. Eakin and A. Sathaye. On automorphisms and derivations of Cayley-Dickson algebras. *J. Algebra*, 129(2):263–278, 1990.

[Gai63] A. T. Gainov. Alternative algebras of rank 3 and 4. *Algebra i Logika Sem*, 2:41–46, 1963.

[GJM96] E. G. Goodaire, E. Jespers, and C. Polcino Milies. *Alternative Loop Rings*. Elsevier, North-Holland, Amsterdam, 1996.

[GKM] Edgar G. Goodaire, Maitreyi Kothandaraman, and Sean May. The Moufang loops of order less than 64. unpublished monograph.

[GM] Edgar G. Goodaire and Sean May. Bol loops of order less than 32. unpublished monograph.

[GM96] Edgar G. Goodaire and C. Polcino Milies. Finite subloops of units in an alternative loop ring. *Proc. Amer. Math. Soc.*, 124(4):995–1002, 1996.

[Goo] Edgar G. Goodaire. No RA-circle loops of order 32 and 64. unpublished.

[Goo83] Edgar G. Goodaire. Alternative loop rings. *Publ. Math. Debrecen*, 30:31–38, 1983.

[Goo87] Edgar G. Goodaire. Circle loops of radical alternative rings. *Algebras Groups Geom.*, 4:461–474, 1987.

[Goo95] Edgar G. Goodaire. The radical of a modular alternative loop algebra. *Proc. Amer. Math. Soc.*, 123(11):4289–3299, 1995.

[GP86] Edgar G. Goodaire and M. M. Parmenter. Units in alternative loop rings. *Israel J. Math.*, 53(2):209–216, 1986.

[GP87] Edgar G. Goodaire and M. M. Parmenter. Semi-simplicity of alternative loop rings. *Acta Math. Hungar.*, 50(3–4):241–247, 1987.

[GR95] Edgar G. Goodaire and D. A. Robinson. A class of loops whose loop rings are strongly right alternative. *Comm. Algebra*, 22(14):5623–5634, 1995.

[GZa] Edgar G. Goodaire and Yongxin Zhou. Alternative rings of small order. submitted for publication.

[GZb] Edgar G. Goodaire and Yongxin Zhou. Cayley-Dickson algebras and RA-loops. submitted for publication.

[Hal59] M. Hall, Jr. *The theory of groups*. MacMillan, New York, 1959.

[Jac74] Nathan Jacobson. *Basic Algebra I*. W. H. Freeman and Company, San Francisco, 1974.

[Jac80] Nathan Jacobson. *Basic Algebra II*. W. H. Freeman and Company, San Francisco, 1980.

[JKW85] E. Jespers, J. Krempa, and P. Wauters. The Brown-McCoy radicals of semigroup rings of commutative cancellative semigroups. *Glasgow Math. J.*, 26:107–113, 1985.

[JLM95] E. Jespers, G. Leal, and C. Polcino Milies. Classifying indecomposable RA loops. *J. Algebra*, 176:5057–5076, 1995.

[Kar83] G. Karpilovsky. *Commutative group algebras*. Marcel Dekker, New York, 1983.

[Kar87] G. Karpilovsky. *The Jacobson radicals of group algebras*. Elsevier, North-Holland, Amsterdam, 1987.

[Khu93] E. I. Khukhro. *Nilpotent groups and their automorphisms*. W. de Gruyte, Berlin, 1993.

[Kle63] E. Kleinfeld. A characterization of the Cayley numbers. In A. A. Albert, editor, *Studies in modern algebra*, volume 2 of *Studies in Mathematics*, pages 126–143. Math. Assoc. of America, 1963.

[KP69] R. L. Kruse and D. T. Price. *Nilpotent Rings*. Gordon and Greach Science Publishers, New York, 1969.

[KP81] T. Kepka and P. N. Praha. Commutative moufang loops and distributive groupoids of small orders. *Czechoslovak Math. J.*, 31:633–669, 1981.

[Kum94] Yogesh Kumar. On a theorem of Ault and Watters. *Mathematics Today*, XII:51–52, 1994.

[LM93] G. Leal and C. Polcino Milies. Isomorphic group (and loop) algebras. *J. Algebra*, 155:195–210, 1993.

[McD74] B. R. McDonald. *Finite rings with identity*. Marcel Dekker, New York, 1974.

[Mor58] V. V. Morozov. The classification of nilpotent Lie algebras of order six. *Izv. Vyssh. Uchebn. Zaved., Mat.*, 4:161–171, 1958.

[Pas77] D. S. Passman. *The algebraic structure of group rings*. Wiley-Interscience, New York, 1977.

[Pfl90] H. O. Pflugfelder. *Quasigroups and loops: Introduction*. Heldermann Verlag, Berlin, 1990.

[Rob82] D. J. S. Robinson. *A course in the theory of groups*. Springer-Verlag, New York, 1982.

[Roh82] Frank Rohl. On the isomorphism problem for integral group rings of circle groups. *Math. Z.*, 180:419–422, 1982.

[Roh90] Frank Rohl. On automorphisms of complete algebras and the isomorphism problem for modular group rings. *Canad. J. Math.*, XLII:383–394, 1990.

[Rot95] Joseph J. Rotman. *An introduction to the theory of groups*, volume 148 of *Graduate texts in mathematics*. Springer-Verlag, New York, fourth edition, 1995.

[San74] R. Sandling. Group rings of circle and unit groups. *Math. Z.*, 140:195–202, 1974.

[Sch66] R. D. Schafer. *An introduction to nonassociative algebras*. Academic Press, New York, 1966.

[Seh78] S. K. Sehgal. *Topics in group rings*. Marcel Dekker, New York, 1978.

[Seh93] S. K. Sehgal. *Units in integral group rings*. Longman Scientific & Technical Press, Harlow, 1993.

[Sza81] F. Szasz. *Radicals of rings*. J. Wiley, London, 1981.

[TH83] Ken-Ichi Tahara and Akinori Hosomi. *On the circle group of finite nipotent rings*, volume 1098 of *Lecture Notes in Mathematics*. Springer-Verlag, 1983.

[Tos63] B. R. Toskey. Rings on a direct sum of cyclic groups. *Publ. Math. Debrecen*, 10:93–95, 1963.

[Tug92] A. A. Tuganbaev. Quaternion algebras over local rings. *Uspekhi Mat. Nauk*, 47:179–180, 1992. Translation in Russian Math. Surveys 47 (1992), no. 3, 194–195.

[Tug93] A. A. Tuganbaev. Generalized quaternion algebras. *Mat. Zametki*, 53:120–128, 1993. Translated in Math. Notes 53 (1993), no. 5-6, 534–538.

[TW80] A. D. Thomas and G. V. Wood. *Group Tables*. Shiva Publishing, Orpington, 1980.

[Zho] Yongxin Zhou. Cayley-Dickson algebras and alternative loop algebras. submitted for publication.

[Zho95] Yongxin Zhou. The Jacobson and Brown-McCoy radicals of certain group rings. *Chinese Quarterly J. Math.*, 10:91–96, 1995.

[ZSSS82] K. A. Zhevlakov, A. M. Slin'ko, I. P. Shestakov, and A. I. Shirshov. *Rings that are nearly associative*. Academic Press, New York, 1982. translated by Harry F. Smith.