Aspects of the circle composition operation in rings

Helen L. Chick, B.Sc.(Hons), Dip.Ed.

Submitted in fulfilment of
the requirements for the degree of
Doctor of Philosophy

Department of Mathematics
University of Tasmania

December 1996

I declare that this thesis contains no material which has been accepted for the award of a degree or diploma by the University or any other institution, and that, to the best of my knowledge and belief, it contains no material previously published or written by another person except when due reference is made in the text of the thesis.

Helen L. Chick

Abstract

In this thesis we will investigate some of the properties of the circle composition (or adjoint) operation in rings, where the operation $\circ$ is defined by $a \circ b = a + b + ab$. In arbitrary rings, R, the properties of addition and multiplication imply that $(R, \circ)$ is a semigroup; in certain classes of rings this semigroup has additional properties and we shall examine a few of these.

Our main concern will be commutative quasiregular (Jacobson radical) rings. In such rings $(R, \circ)$ is an abelian group, giving R a second such structure besides $(R, +)$. It seems a natural question to ask if these group structures can ever be isomorphic. The zero rings, in which multiplication is trivial, obviously have this property since the additive and circle composition groups coincide; thus the class, $\mathcal{K}$, of rings having isomorphic additive and circle composition groups is non-empty. There are also non-trivial examples and we illustrate the construction of some, including the so-called quasifields which are constructed on partially ordered sets, and examples which use finite groups for addition. It might be suspected that for these less trivial examples the isomorphism between addition and circle composition will still force multiplication to behave in a nearly trivial way, so that perhaps such rings are nil or nilpotent. This need not be the case as there is a ring in $\mathcal{K}$ which has no zero divisors. In fact, we show that there exist rings in $\mathcal{K}$ which are nilpotent but not zero rings, nil but not nilpotent, and quasiregular without being nil.

We will also consider the algebraic properties of the class $\mathcal{K}$, including the question of its inheritance under ring theoretic constructions. In particular, we show that $\mathcal{K}$ is not a radical class, that it is closed under direct products, but that it is not hereditary and that it is not closed under homomorphisms nor taking quasiregular subrings. There are, however, certain subclasses of $\mathcal{K}$ which are better behaved, including, for example, rings which are algebras over $\mathbf{Z}_p$ or

$\mathbf{Q}$ and the rings constructed on certain finite groups.

For commutative nilpotent rings we prove the existence of a polynomial homomorphism between the additive and circle composition groups, which in certain circumstances will be an isomorphism. We show, too, that all finitely generated nilpotent $\mathbf{Q}$-algebras and $\mathbf{Z}$-algebras are in $\mathcal{K}$. The former result allows us to demonstrate that all commutative nil $\mathbf{Q}$-algebras are in $\mathcal{K}$.

We conclude by considering a family of ring examples in which the circle composition semigroup is regular. Our construction is developed from the idea behind the quasifield construction and also generalised power series rings. We investigate the existence of nilpotence in such rings, and show that, like $\mathcal{K}$, the class of rings in which $(R, \circ)$ is a regular semigroup is not a radical class. This result also holds for the stronger property that $(R, \circ)$ is a union of groups.

Acknowledgements

It's embarrassing to mention
When I first had the intention
Of embarking on a pure maths PhD;
Now it's drawn to a conclusion
And I'm under no delusion
That the end result is solely down to me.

For I know I have grown wiser
So I thank my supervisor
Dr Barry Gardner. Now let it be known:
In his field he is outstanding,
Partial orders notwithstanding,
And his expertise runs rings around my own.

At our quasiregular meetings —
Where my semisimple bleatings
Met with patience quantified by aleph-nought —
He gave ideal supervision,
Errors met decomposition;
He made torsion-free my convoluted thought.

From the time that I first started
(Though they later both departed)
I've had help — and fun and games — from Nick and Tim;
While in matters of computing
There is surely no refuting
I appreciated Michael, Spoon and Kym.

It should also be reported
That Jane Watson has supported
My endeavours through this nearly endless time
(And we even gained some glory ...
But that's another story,
Which is told in yet another lengthy rhyme).

Things took longer, since employment
Interfered but gave enjoyment;
The Department has been good to be around.
I am grateful, too, for Betty
(Minder of the cash that's petty)
Who encouraged me when things went up and down.

And a very thankful daughter
Is determined that she ought to
Give her parents heartfelt thanks for all they've done.
They have helped me through the ages
I've required to fill these pages ...
I'll forgive them if they only read page one!

A mathematician is a machine for turning coffee into theorems.

— Paul Erdős

A Mormon mathematician is at a disadvantage. I hope that orange juice is a reasonable substitute; however, I would also like to acknowledge the coffee consumed by my supervisor.

— H. L. C.

Contents

Chapter 1

Introduction

1.1 Introduction

In the study of rings it is of interest to investigate the group of units and the Jacobson radical. The Jacobson radical is the largest ideal in which the circle composition operation defined by $a \circ b = a + b + ab$ — which is a semigroup in arbitrary rings — gives rise to a group. In rings with identity, if x is in the Jacobson radical then $1 + x$ is in the group of units of the ring. Quasiregular rings, in which the whole ring is Jacobson radical, include the nil (and hence also nilpotent) rings. Such rings have two group structures, addition and circle composition, and it is a natural question to ask how the group properties of the two are related. Certain aspects of this issue have been investigated by Amberg and Dickenschied [1] who showed, for example, that if one of the groups in a nil ring is a p-group (or is torsion-free) then so is the other.

If a ring's multiplication is commutative the circle composition commutes; the ring then has two *abelian* group structures associated with it. The main purpose of this thesis is to investigate whether or not the two groups can be

isomorphic and, if so, what implications this has for the ring. That there *are* such rings having isomorphic additive and circle composition groups is obvious: zero rings (where multiplication is trivial) clearly have the desired property, since the additive and circle composition groups coincide. We will also consider conditions on the ring which force an isomorphism between the groups.

Throughout this thesis $\mathcal{K}$ will denote the class of all rings in which $(R, \circ)$ is isomorphic to $(R, +)$.

We begin in Chapter 2 by illustrating the construction of some non-trivial examples of rings in $\mathcal{K}$, initially based on the work of Kesava Menon [22] and Haukkanen [18]. These rings comprise a set of functions defined on a certain type of partially ordered set and which take their value in some underlying ring with identity. Circle composition is defined *via* a convolution-type operation. The properties of the poset and the underlying ring ensure that the resulting ring — which we call a *quasifield* in the case that multiplication is commutative — is quasiregular. In certain circumstances we demonstrate the existence of an isomorphism between the additive and circle composition groups, either by giving an explicit isomorphism function or by considering the ranks of the two groups.

In the third chapter we will investigate what, if any, implications there are for a ring if it *has* isomorphic additive and circle composition groups. Given the relationship between $+$ and $\circ$ it might be expected that for a ring in $\mathcal{K}$ the multiplication is trivial or close to it. Consequently, we will consider examples which show the extent to which nilness and nilpotence can be expected. In particular we shall present instances of rings in $\mathcal{K}$ which are nilpotent, nil but not nilpotent, and quasiregular without being nil, including one with no zero-divisors.

The ring properties of $\mathcal{K}$-rings are further investigated in Chapter 4, where we show that this class is not a radical class by showing that it is not closed under

extensions. We also investigate the inheritance or otherwise of $\mathcal{K}$ under various ring-theoretic actions, such as direct products and sums and the taking of ideals and homomorphic images. For the former pair of structures we will show that $\mathcal{K}$ *is* closed under their construction, while for the latter we will obtain partial results initially, before showing later in the thesis that homomorphic images and ideals of rings in $\mathcal{K}$ need not be in $\mathcal{K}$.

We return to constructing rings in Chapter 5, this time taking finite abelian groups and determining whether or not they can form the additive group of a non-trivial ring in $\mathcal{K}$. If p is a prime we can show that there is only the trivial $\mathcal{K}$-ring with $\mathbf{Z}_p$ as the additive group; we also show that $\mathbf{Z}_4$ and $\mathbf{Z}_2 \oplus \mathbf{Z}_2$ do not support non-trivial rings in $\mathcal{K}$. Of the remaining finite groups, for those of the form $\mathbf{Z}_{p^n}$ we show exactly how to obtain non-trivial examples of rings in $\mathcal{K}$ and indicate the number of non-isomorphic classes that arise for a given group; while for other finite abelian groups we indicate how to obtain at least one non-trivial example of a $\mathcal{K}$-ring using direct sums. In the final section we look at two examples of rings constructed on infinite abelian groups. The first shows that any non-divisible infinite abelian p-group will support a non-trivial ring in $\mathcal{K}$, and we can use it to show that $\mathcal{K}$ is not hereditary. The second gives an example of a mixed group on which there is a non-trivial $\mathcal{K}$-ring.

Chapter 6 concentrates on nilpotent rings; here we are able to obtain an explicit polynomial homomorphism between the additive and circle composition groups. If the ring has no p-torsion for values of p less than the index of nilpotence then the homomorphism is injective and with extra conditions it is an isomorphism. Free commutative nilpotent $\mathbf{Q}$-algebras and, as a consequence, finitely generated nilpotent $\mathbf{Q}$-algebras are shown to be in $\mathcal{K}$ using this homomorphism, while for free commutative nilpotent $\mathbf{Z}$-algebras we determine the ranks of the two groups to achieve the same result. From this result we can demonstrate that $\mathcal{K}$ is not homomorphically closed.

Rational algebras continue to receive attention in Chapter 7. We investigate the torsion and divisibility properties of the circle group, leading to a proof that all commutative nil $\mathbf{Q}$-algebras are in $\mathcal{K}$. We also obtain a similar result for commutative $\mathbf{Q}$-algebras which are complete in their ring-adic metrics. By considering a particular subring of the Jacobson radical of the p-adic integers we can show that $\mathcal{K}$ is not closed under taking quasiregular subrings. We conclude the chapter with an example of a ring which is a torsion ring with respect to addition, but its circle composition group is torsion-free.

The final chapter is, in part, Section 2.2 revisited. We begin by constructing some more quasiregular rings, but using a particular class of monoids instead of a poset. This serves as an introduction to the second section, where by using a slightly different class of monoids we can construct examples of rings in which the circle composition semigroup is regular rather than a group. It is well-known that the class of rings for which $(R, \circ)$ is a group is a radical class (the Jacobson radical class), and we conclude the thesis by showing that when this constraint on the semigroup $(R, \circ)$ is relaxed we do not necessarily obtain a radical class. In particular, we show that the class of rings for which the circle composition semigroup is a union of groups (or an inverse semigroup or a regular semigroup) is not a radical class.

As will be seen, more complete results have been obtained for rings in $\mathcal{K}$ which have the additional property that they are algebras over $\mathbf{Z}_p$ for some prime p, or are algebras over a field of characteristic zero. The behaviour of the former class of rings is characterized by Theorem 3.1.1, and the latter by results in Chapters 6 and 7.

We note that many of the results of Section 2.2 and Chapters 3 and 4 have appeared in [4], [5] and [6].

Some of the more important results and their locations are highlighted below.

- $\mathcal{K}$ is closed under direct sums and products and filtered products — Section 4.3;
- $\mathcal{K}$ is not closed under extensions — Example 4.1.1;
- $\mathcal{K}$ is not hereditary — Corollary 5.3.2;
- $\mathcal{K}$ is not homomorphically closed — Theorem 6.3.3;
- $\mathcal{K}$ is not closed under taking quasiregular subrings — Theorem 7.1.10;
- The class of rings for which $(R, \circ)$ is a union of groups (or is an inverse or a regular semigroup) is not a radical class — Section 8.3.

1.2 Preliminaries

Most of this section may be skipped with impunity by those with a strong background in algebra; it is included mainly for reference. However, the section on the circle composition operation will be used extensively throughout the thesis.

Additional information on group theory can be found in Rotman [34] and Fuchs [16]; ring theory in Hungerford [20]; radical theory (including nil, nilpotent and quasiregular rings) in Divinsky [11] and Wiegandt [41]; semigroup theory in [30]; and filters in Chang and Keisler [3].

GROUP THEORY

In what follows the groups are abelian and, hence, written additively.

An element $x \neq 0$ of a group has *n-torsion*, where $n \in \mathbf{N}$, if $nx = 0$. A group is *torsion* if each element has n-torsion for some $n \in \mathbf{N}$. A p-group is a torsion group, the orders of whose elements are powers of a fixed prime p. A group is *torsion-free* if no element has n-torsion for any $n \in \mathbf{N}$, i.e. $nx = 0$ implies $x = 0$.

A *mixed group* contains both elements of finite order (i.e. torsion elements) and elements of infinite order. A group, G, is *divisible* if for every $x \in G$, $n \in \mathbf{N}$ there exists $y \in G$ such that $ny = x$ (i.e. we can "divide" elements by any n). A group is *reduced* if it has only the trivial divisible subgroup.

The following results concerning such groups are important for our work; for proofs see, for example, [34] and [16].

Theorem 1.2.1 *Every torsion-free divisible group is the direct sum of copies of* $\mathbf{Q}$. □

Theorem 1.2.2 *Every group is the direct sum of a divisible group and a reduced group, where the divisible group is uniquely determined and the reduced group is unique up to isomorphism.* □

The group $\mathbf{Z}(p^\infty)$ for a prime p is the set, under multiplication, of all p^nth complex roots of unity where n runs over all non-negative integers. Alternatively, we can write it additively as the set generated by the elements $\{y_0, y_1, y_2, \ldots\}$ satisfying $py_0 = 0$, $py_1 = y_0$ and, in general, $py_n = y_{n-1}$. It is a p-group.

THE CIRCLE COMPOSITION OPERATION

On any associative ring, R, the operation of circle composition (also known as the adjoint operation) is defined *via*

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

for all $a, b \in R$. This operation is associative, so that $(R, \circ)$ is a semigroup, and commutative in the case that multiplication in R is commutative.

We define $a^{\circ n}$ inductively via $a^{\circ 2} = a \circ a = a + a + a^2 = 2a + a^2$, and $a^{\circ(n+1)} = (a^{\circ n}) \circ a$. It is straightforward to use induction (see, for example, [42]) to show that

$$a^{\circ n} = (1 + a)^n - 1 = \sum_{r=1}^{n} \binom{n}{r} a^r$$

where, if necessary, we have adjoined a formal 1. These results will be used frequently.

In a quasiregular ring it is well-known that $(R, \circ)$ is a group (in fact, the two conditions are equivalent). In this case we shall use $a^{\circ(-1)}$ to denote the $\circ$-inverse or quasi-inverse of a with respect to circle composition; more generally we use $a^{\circ(-n)}$ to denote the quasi-inverse of $a^{\circ n}$ for $n \in \mathbf{N}$. Finally, the identity for the circle composition group is 0, which we may also write as $a^{\circ 0}$.

RING THEORY

All rings considered herein are associative but need not have an identity unless specifically stated; frequently we will focus on commutative rings. A ring in which the multiplication is trivial (i.e. all products vanish) is called a *zero ring*.

The primary decomposition theorem, which deals with rings whose additive groups are torsion, will be used in Chapter 5 and is stated below. A discussion of it is found in Kruse and Price [26]. A p-ring is a ring in which every element has order a power of p; it is the ring analogue of a p-group.

Theorem 1.2.3 *If R is a ring with a torsion additive group, then R is uniquely expressible as a direct sum of p-rings R_p for different primes p.* □

An element r of a ring R is *nilpotent* if there exists $n \in \mathbf{N}$ such that $r^n = 0$, and the ring R is said to be *nil* if every element is nilpotent (where the index of nilpotence of an element depends on the element). A ring R is *nilpotent* if there exists $n \in \mathbf{N}$ such that $R^n = \{\sum r_1 r_2 \cdots r_n\} = 0$. We call n the *index of nilpotence* of the ring R. A ring is said to be *left [resp. right] T-nilpotent* if for every sequence $r_1, r_2, r_3, \ldots$ there exists an n such that $r_1 r_2 \cdots r_n = 0$ [resp. $r_n r_{n-1} \cdots r_1 = 0$]. A ring is *quasiregular* if for every $r \in R$ there exists $a \in R$ such that $r + a + ra = 0$. (See also additional comments in the previous section on the circle composition operation.)

We have the following hierarchy of classes of rings:

$$\text{Nilpotent} \subset T\text{-nilpotent} \subset \text{Nil} \subset \text{Quasiregular}.$$

There are a number of equivalent ways of characterizing a radical class; the following best suits our purposes. Note that if a ring R is a member of a class of rings, $\mathcal{R}$, we sometimes say that R is an $\mathcal{R}$-ring. A *radical class* is a class, $\mathcal{R}$, of rings which satisfy (a) and (b) and either (c) or (d):

(a). Every homomorphic image of an $\mathcal{R}$-ring is an $\mathcal{R}$-ring (i.e. $\mathcal{R}$ is *homomorphically closed*).

(b). In every ring R there is an $\mathcal{R}$-ideal $\mathcal{R}(R)$ which contains every other $\mathcal{R}$-ideal of R.

(c). $\mathcal{R}(R/\mathcal{R}(R)) = 0$

(d). If I is an ideal of R and both $I, R/I \in \mathcal{R}$, then $R \in \mathcal{R}$ (i.e. $\mathcal{R}$ is *closed under extensions*).

A class $\mathcal{R}$ is said to be *hereditary* if, for $R \in \mathcal{R}$ and $I \lhd R$ we have $I \in \mathcal{R}$. The classes of nil and quasiregular rings are (hereditary) radical classes; the class of quasiregular rings is also called the *Jacobson radical class*, denoted by $\mathcal{J}$.

A ring R is a *subdirect product* of the rings $\{R_\lambda \mid \lambda \in \Lambda\}$ if for each λ there is an ideal I_λ of R with $R/I_\lambda \cong R_\lambda$ and $\cap_{\lambda\in\Lambda} I_\lambda = 0$. A commutative ring R is said to be *artinian* if it has the descending chain condition on ideals, i.e. for every chain of ideals $R \rhd I_1 \rhd I_2 \rhd \ldots$ there exists $m \in \mathbf{N}$ such that $I_m = I_{m+1}$.

SEMIGROUPS AND SEMIGROUP RINGS

A *semigroup* is a set with an associative binary operation, usually called multiplication (although in Chapter 8 we will also use addition at times). A *monoid*

is a semigroup with identity, while a *semilattice* is a commutative semigroup, S, in which every element is *idempotent*, i.e. $s^2 = s$ for all $s \in S$.

Of particular interest in Chapter 8 are the following classes. An element s of a semigroup, S, is *regular* if there exists $a \in S$ such that $s = sas$. A semigroup is *regular* if every element is regular. We say a is an *inverse* of $s \in S$ if $s = sas$ and $a = asa$. Every regular element has an inverse and conversely. An *inverse semigroup* is a regular semigroup in which every element has a *unique* inverse. A *group* is a semigroup with identity, e, such that for each $s \in S$ there exists s^{-1} such that $ss^{-1} = s^{-1}s = e$. A semigroup S may be a *union of groups*, in which case each idempotent will be the identity of one of the groups.

We have the following hierarchy of classes of semigroups:

Groups $\subset$ Union of groups $\subset$ Inverse semigroups $\subset$ Regular semigroups.

Let R be a ring and S a semigroup. Then the *semigroup ring* $R[S]$ consists of all formal sums $\sum_{s\in S} r_s s$ such that $r_s \in R$ and $r_s = 0$ for all but finitely many $s \in S$. Addition is defined component-wise, that is,

$$\sum_{s\in S} r_s s + \sum_{s\in S} a_s s = \sum_{s\in S} (r_s + a_s)s$$

and multiplication *via*

$$(\sum_{s\in S} r_s s)(\sum_{s\in S} a_s s) = \sum_{s\in S} (\sum_{s_i s_j = s} r_{s_i} a_{s_j})s.$$

NUMBER THEORY

The following number-theoretic lemma is used on various occasions in Chapters 5 and 7.1.

Lemma 1.2.4 *(i) The binomial coefficient* $\binom{p^n}{k}$ *is divisible by* p^n *if and only if* p *is not a factor of* k*. If* p *divides* k *with* $k \neq p^n$ *then* $\binom{p^n}{k}$ *has at least one factor of* p*.*

(ii) If p^s *does not divide* k *then* $\binom{p^s r}{k}$ *has at least one factor of* p*.*

Proof: First observe that if m is a natural number then we can write

$$\binom{mp}{k} = \frac{mp(mp-1)(mp-2)\dots(mp-(k-1))}{k \times 1 \times 2 \dots \times (k-1)}.$$

If we ignore the first term in the numerator and the denominator, so that we are considering $(mp-1)(mp-2)\dots(mp-(k-1))$ and $1\times 2\dots\times(k-1)$ respectively, we find that the positions of the occurrences of the factor p coincide. For example, there are factors of p in the terms $(mp-p)$, $(mp-2p)$, $(mp-3p)$ and so on in the numerator, and in the terms p, $2p$, $3p$ and so on in the denominator. So, every pth term of both expressions has a factor of p; the rest of the proof will concern itself with determining where and how many extra factors of p arise.

(i) If, in fact, we have $m = p^{n-1}$, so that we are considering the binomial coefficient $\binom{p^n}{k}$ we see that not only do the factors of p occur in the same positions but with the same multiplicity. For example, the pth terms are $(p^n - p)$ and p, which both have a single factor of p, as do the $2p$th terms $(p^n - 2p)$ and $2p$, and so on; the p^2 terms are $(p^n - p^2)$ and p^2 which both have factors of p^2, and so on. Thus there are exactly the same number of factors of p in both $(p^n-1)(p^n-2)\dots(p^n-(k-1))$ and $1\times 2\dots\times(k-1)$ and hence the number of factors of p in $\binom{p^n}{k}$ is solely determined by p^n/k. If p does not divide k then $\binom{p^n}{k}$ has a factor of p^n. On the other hand, even if p *does* divide k, the requirement that $k \neq p^n$ ensures that $\binom{p^n}{k}$ will still have at least one factor of p.

(ii) If we now consider $\binom{p^s r}{k}$ and look at each of the terms $1 \times 2 \dots \times (k-1)$ and $(p^s r - 1)(p^s r - 2)\dots(p^s r - (k-1))$ from the denominator and numerator respectively we note that every pth term — starting with p in the case of the denominator and $p^s r - p$ in the numerator — has a factor of p. We will show that there cannot be more factors of p in the denominator than there are in the numerator. We assert that the product $1 \times 2 \dots \times (k-1)$ has the minimal number of factors of p of any product of $k-1$ consecutive numbers. This is because the first factor of p does not appear until the pth term, the first

single p^2 factor (as opposed to a product of two factors of p arising in different locations) will not appear until p^2 itself, and so on. This is the sparsest possible distribution of factors of the prime p among $k-1$ consecutive numbers; other sets of consecutive numbers could have their first factor of p or p^2 or even p^6 much earlier in the list. If we consider the expression from the numerator, we note that although it will not have its first factor of p until the pth term (which is $(p^s r - p)$), it is conceivable that p^2 or p^3 factors could arise earlier than the p^2th or p^3th terms. To give a specific example, suppose that $r = p + 1$ and that $s = 1$. Then the pth term of the numerator, namely $(p^s r - p)$, is equal to $p(p+1) - p = p^2$, and so it actually has two factors of p and not just the guaranteed one. It follows that there are at least as many factors of p present in $(p^s r - 1)(p^s r - 2)\ldots(p^s r - (k-1))$ as there are in $1 \times 2 \ldots \times (k-1)$. If k has no factor of p^s then there are also additional factors of p in the numerator from the $p^s r$ term which we have not included until now. It follows that p is a factor of $\binom{p^s r}{k}$ provided p^s does not divide k. $\square$

Chapter 2

Some quasiregular ring constructions

2.1 Introduction

In this chapter we will illustrate the construction of various quasiregular rings. In some cases the example will just illustrate the fact that a quasiregular ring has been constructed; in other cases we will be able to show that, in addition, the ring actually has isomorphic circle composition and additive groups, i.e. is in $\mathcal{K}$. These examples provide us not only with a demonstration that such rings exist, but are also useful for results concerning the ring properties of such rings as we shall see in Chapters 3 and 4.

We begin by defining quasi-division rings, adapting a definition given by Kesava Menon in [22].

Definition 2.1.1 *A quasi-division ring is a set Q, together with operations $+$ and $\circ$ such that*

(i) $(Q, +)$ is an abelian group;

(ii) $(Q, \circ)$ *is a group; and*

(iii) the left and right quasi-distributive laws hold, viz.:

$a \circ (b + c) + a = (a \circ b) + (a \circ c)$ *and*

$(b + c) \circ a + a = (b \circ a) + (c \circ a)$ *for all* a, b *and* $c \in Q$.

Structures like quasifields have arisen in other contexts independently of the 1963 work of Kesava Menon [22]. In 1961 Climescu, in [8] (and later [9]), investigated *weak rings* $(Q, +, \circ)$ where $(Q, +)$ is an abelian group, $(Q, \circ)$ is a semigroup and there is a weakened form of distributivity of $\circ$ over addition. It was pointed out that any ring $(R, +, \cdot)$ could be turned into a weak ring $(R, +, \circ)$ by defining the circle operation in the expected way, viz.: $a \circ b = a + b + ab$. He also considered more general quasi-distributive laws. Čupona ([10] in 1969) considered *quasirings* where addition need not be abelian and quasi-distributivity is as above, and Ştefănescu's 1979 paper [37] synthesized and further developed these concepts in a study of *infra-near rings* in which addition can be non-commutative and the more general quasi-distributive laws of [8] hold, namely:

(i) $x \circ (y + z) + x \circ 0 = x \circ y + x \circ z$

(ii) $(x + y) \circ z + 0 \circ z = x \circ z + y \circ z$.

Left and right infra-near rings are considered by taking only one or other of the above so-called infra-distributive laws. In the case of the eastern Europeans, the possibility of having $(Q, \circ)$ as a group was not considered; however, as early as 1948, Andrunakievich [2] was aware of the direct relationship between the operation $\circ$ in a quasi-division ring and the property of quasiregularity in rings, where circle composition and multiplication are related via $a \cdot b = a \circ b - (a + b)$.

Lemma 2.1.2 *(See [2].)* $(Q, +, \circ)$ *is a quasi-division ring if and only if* $(Q, +, \cdot)$ *is a quasiregular ring.*

Proof: Note that $(Q, \circ)$ is a group if and only if elements of $(Q, +, \cdot)$ have quasi-inverses with respect to circle composition $a \circ b = a \cdot b + a + b$, i.e. if and only if $(Q, +, \cdot)$ is quasiregular. It is easily shown that the quasi-distributivity of circle composition over addition implies the distributivity of multiplication over addition and vice versa. In $(Q, +, \circ)$ the element 0 is the identity for both addition and circle composition. □

If we insist that $(Q, \circ)$ forms an abelian group (leaving us with one quasi-distributive law), then we have a *quasifield* $(Q, +, \circ)$, which is a commutative quasiregular ring when considered as $(Q, +, \cdot)$.

In the paper [22] where Kesava Menon introduced quasifields *per se* the connection with quasiregularity is not made explicit. The main thrust of his work was to produce an example of a quasifield whose additive and circle composition groups were isomorphic; further examples of such quasifields have also been constructed by Haukkanen [18] who also misses the link with quasiregularity. In many of these examples the quasifield consisted of particular functions defined on some partially ordered set, with circle composition being an appropriate convolution operation.

In the next section we will generalise the results of Kesava Menon and Haukkanen, which will enable us to obtain further examples of quasiregular rings. *As we now know that quasi-division rings and quasifields exactly coincide with quasiregular and commutative quasiregular rings respectively we shall reserve the former terms specifically for those rings constructed using the approach of Section 2.2.* Some of the examples which we consider will, in fact, be quasifields with isomorphic additive and circle composition groups. Later in the thesis we will adapt this construction to certain types of monoids rather than the posets used here. This will enable us to obtain additional examples in Chapter 8.

In addition to the papers of Kesava Menon and Haukkanen, some of the results presented were developed from a number of sources. Incidence algebras, with their convolution, gave rise to one of the examples presented herein and actually provided the inspiration for the main generalisation presented in Section 2.2. McCarthy [28] presents some proofs concerning incidence algebras (such as showing the existence of an inverse with respect to convolution) and these results have been generalised.

In this chapter our interest will focus on the method of construction of the ring and the circle composition operation itself, and so at first our primary emphasis will be on the structures as quasi-division rings. In Chapters 3 and 4 our attention will shift to multiplication, and we will examine some of the properties of the quasi-division rings as quasiregular rings.

2.2 Quasifields and quasi-division rings

To construct our quasi-division rings we need a particular type of partially ordered set. Some of the conditions imposed on this set may initially seem strange or restrictive, but, as can be seen from the examples presented later in this section, there are many quite natural posets satisfying the necessary requirements.

Let $(P, \leq)$ be a locally finite partially ordered set such that for any $x \in P$ there exists exactly one minimal element $e \in P$ satisfying $e \leq x$, and let $\#(x)$ denote the number of elements of P less than or equal to x. (By *locally finite* we mean that between any two comparable members of P there are only finitely many elements of P.) Let $\mathrm{Min}(P)$ denote the set of minimal elements in P and, for each $x \in P$, let e_x denote the element of P such that $e_x \in \mathrm{Min}(P)$ and $e_x \leq x$. We observe that such a poset is equivalent to a number of disjoint posets, each of whose least elements is one of the above minimal elements.

In addition, suppose that there exists a function $w(x, y)$ — in some sense "what's left over when you 'take' y from x" — defined for all $x, y \in P$, $y \leq x$, satisfying

$(w1)$: $w(x, y) \in P$;

$(w2)$: $w(x, y) = x$ if and only if $y \in \text{Min}(P)$ (i.e. if and only if $y = e_x$);

$(w3)$: $w(x, y) \in \text{Min}(P)$ if and only if $y = x$; and

$(w4)$: $\#(w(x, y)) \leq \#(x)$, with equality only when $y \in \text{Min}(P)$.

[We note that our function w generalises the idea of a *factor function*, introduced by Wiegandt in [40]. A factor function satisfies

(i) $w(x, y) \leq x$;

(ii) $w(x, y) < w(z, y)$ when $y \leq x < z$;

(iii) $w(x, w(x, y)) = y$

(iv) $w(w(x, y), w(z, y)) = w(x, z)$ when $y \leq z \leq x$.]

Furthermore, let S be the subset of $P \times P$ with $(y, z) \in S$ if and only if there exists $x \in P$ such that $y \leq x$ and $z \leq w(x, y)$. Then, suppose there exists a function $c : S \to P$ which satisfies the following for any given x :

$(c1)$: $c(y, z) = x$ if and only if $y \leq x$ and $z = w(x, y)$; and

$(c2)$: if c is regarded as a partial binary operation on P then it is associative; that is, y, u, v satisfy $c(y, c(u, v)) = x$ if and only if y, u, v satisfy $c(c(y, u), v) = x$.

We have already defined $\#(x)$ as the number of elements less than or equal to x in the poset P; later it will be useful to consider the *height* of an element and, where appropriate, a poset. We define the "height", $h(x)$, of a poset element x by

$$h(x) = \text{maximum length of the chains between} e_x \text{and } x.$$

If the set of all $h(x)$ values ($x \in P$) has a maximum, n, then we define this to be the height of the poset and denote it by $h(P)$. We observe that it is possible for infinite posets to have finite height.

We will now show how to construct a quasi-division ring on this partially ordered set. Let K be a ring with identity 1 — we shall call this the *underlying ring* — and let $f : P \to K$ be a function satisfying $f(x) = 1$ for $x \in \mathrm{Min}(P)$. Let F denote the set of all such functions; if necessary we could use $F((P, \leq), K)$ to more completely characterize F by being specific about the poset and underlying ring involved. However, we will not usually do this. We may now define $f + g$ and $f \circ g$ for $f, g \in F$ as follows:

$$(f+g)(x) = \begin{cases} 1, & \text{if } x \in \mathrm{Min}(P); \\ f(x) + g(x), & \text{otherwise.} \end{cases}$$

$$(f \circ g)(x) = \begin{cases} 1, & \text{if } x \in \mathrm{Min}(P); \\ \sum_{y \leq x} f(y)g(w(x,y)), & \text{otherwise.} \end{cases}$$

Property $(c1)$ means that we can rewrite the circle composition operation as $(f \circ g)(x) = \sum_{c(y,z)=x} f(y)g(z)$, where $x \notin \mathrm{Min}(P)$.

[It is possible to recast this definition using the more natural value of 0 on the minimal elements. In order to do this and still obtain a quasiregular ring the convolution operation must be used for *multiplication* rather than circle composition. We have left the notation as above because of the historical development of this material — this was the approach used in [22] and [18] — and also because it is more tractable when we are focussing on the circle operation. See page 137 for additional discussion about this issue.]

We now show that $(F, +, \circ)$ is a quasi-division ring. In what follows we denote by δ the function in F satisfying

$$\delta(x) = \begin{cases} 1, & \text{if } x \in \mathrm{Min}(P); \\ 0, & \text{otherwise.} \end{cases}$$

Lemma 2.2.1 *$(F, +)$ is an abelian group.*

Proof: Addition is obviously associative and commutative. $(f+\delta)(e) = 1 = f(e)$ when $e \in \mathrm{Min}(P)$, and for $x \notin \mathrm{Min}(P)$ we have $(f+\delta)(x) = f(x)+\delta(x) = f(x)$, so that δ is the additive identity. Furthermore, f has an additive inverse denoted by $(-f)$ and defined by

$$(-f)(x) = \begin{cases} 1, & \text{if } x \in \mathrm{Min}(P); \\ -(f(x)), & \text{otherwise.} \end{cases} \quad \square$$

Lemma 2.2.2 *$(F, \circ)$ is a group.*

Proof: If $x \in \mathrm{Min}(P)$ then $(f \circ (g \circ h))(x) = 1 = ((f \circ g) \circ h)(x)$. If $x \notin \mathrm{Min}(P)$ then we have

$$\begin{aligned}
(f \circ (g \circ h))(x) &= \sum_{y \le x} f(y)(g \circ h)(w(x,y)) \\
&= \sum_{c(y,z)=x} f(y)(g \circ h)(z) \\
&= \sum_{c(y,z)=x} f(y) \left(\sum_{c(u,v)=z} g(u)h(v) \right) \\
&= \sum_{c(y,c(u,v))=x} f(y)g(u)h(v) \\
&= \sum_{c(c(y,u),v)=x} f(y)g(u)h(v) \\
&= \sum_{c(t,v)=x} \left(\sum_{c(y,u)=t} f(y)g(u) \right) h(v) \\
&= \sum_{c(t,v)=x} (f \circ g)(t)h(v) \\
&= ((f \circ g) \circ h)(x),
\end{aligned}$$

by applying first $(c1)$ and then $(c2)$, where the sums are over the appropriate variables from P. Hence circle composition is associative.

The element δ acts as an identity for $\circ$, since when $x \notin \mathrm{Min}(P)$ (the $x \in \mathrm{Min}(P)$ case being trivial) we have $(f \circ \delta)(x) = \sum_{y \le x} f(y)\delta(w(x,y))$, however $\delta(w(x,y)) = 0$ except when $w(x,y) \in \mathrm{Min}(P)$. This only occurs when $y = x$ by $(w3)$, so that $(f \circ \delta)(x) = f(x)$. Similarly, we have $(\delta \circ f)(x) = f(x)$, since $\delta(y) = 1$ only when $y \in \mathrm{Min}(P)$, and $w(x,y) = x$ in this case, by $(w2)$.

We now establish that each f has a $\circ$-inverse, $f^{\circ(-1)}$. If $x \in \mathrm{Min}(P)$ define $f^{-1}(x) = 1$; then for $x \notin \mathrm{Min}(P)$ we define $f^{\circ(-1)}(x)$ by induction on $\#(x)$, the number of elements of P less than or equal to x. Suppose $f^{\circ(-1)}(y)$ is defined for all y such that $\#(y) < \#(x)$. Since $x \notin \mathrm{Min}(P)$ we require

$$\begin{aligned} 0 = \delta(x) &= (f \circ f^{\circ(-1)})(x) = \sum_{y \leq x} f(y) f^{\circ(-1)}(w(x,y)) \\ &= \sum_{y \leq x, y \neq e_x} f(y) f^{\circ(-1)}(w(x,y)) + f(e_x) f^{\circ(-1)}(w(x,e_x)) \\ &= \sum_{y \leq x, y \neq e_x} f(y) f^{\circ(-1)}(w(x,y)) + f^{\circ(-1)}(x), \end{aligned}$$

by $(w2)$ and the properties of f . Thus we have

$f^{\circ(-1)}(x) = -\sum_{y \leq x, y \neq e_x} f(y) f^{\circ(-1)}(w(x,y))$,

where the values of $f^{\circ(-1)}$ on the right-hand side exist by $(w4)$ and the inductive hypothesis. It is straightforward to verify that the $f^{\circ(-1)}$ so obtained *is* the $\circ$-inverse for f. We observe that Theorem 4 of [40] proves that $(F, \circ)$ is also abelian if and only if w is a factor function. □

Lemma 2.2.3 *Circle composition is left and right quasi-distributive over addition.*

Proof: The case $x \in \mathrm{Min}(P)$ is trivial, so consider $x \notin \mathrm{Min}(P)$.

$$\begin{aligned} &(f \circ (g+h) + f)(x) \\ &\quad = (f \circ (g+h))(x) + f(x) \\ &\quad = \sum_{y \leq x} f(y)(g+h)(w(x,y)) + f(x) \\ &\quad = \sum_{y < x} f(y)(g+h)(w(x,y)) + f(x)(g+h)(w(x,x)) + f(x) \\ &\quad = \sum_{y < x} f(y) g(w(x,y)) + \sum_{y < x} f(y) h(w(x,y)) + f(x) + f(x) \\ &\quad = \sum_{y < x} f(y) g(w(x,y)) + f(x) g(w(x,x)) + \\ &\qquad \sum_{y < x} f(y) h(w(x,y)) + f(x) h(w(x,x)) \end{aligned}$$

$$
\begin{aligned}
&= \sum_{y \leq x} f(y)(g)(w(x,y)) + \sum_{y \leq x} f(y)(h)(w(x,y)) \\
&= (f \circ g)(x) + (f \circ h)(x) \\
&= ((f \circ g) + (f \circ h))(x)
\end{aligned}
$$

as required, by applying $(w3)$ and the fact that $f(e) = 1$ for $e \in \mathrm{Min}(P)$. The proof of right quasi-distributivity is similar, but instead of separating x and $y < x$ and applying $(w3)$, we separate $e_x \in \mathrm{Min}(P)$ and $y \neq e_x$ and then apply $(w2)$. □

Theorem 2.2.4 *F is a quasi-division ring.*

Proof: This follows immediately from Lemmas 2.2.1 to 2.2.3. This means that $(F, +, \cdot)$ (where multiplication is defined by $f \cdot g = f \circ g - (f + g)$) is a quasiregular ring, and is, furthermore, commutative if F is a quasifield (i.e. if $\circ$ is commutative). □

If we have a collection of partially ordered sets each having a least element (rather than a number of minimal elements), then we can form a quasi-division ring on each of them, and take the direct sum to form a quasi-division ring. Let $P = \bigcup_{i \in \Lambda} P_i$ be the union of a collection of disjoint locally finite posets, each having a least element $e_i (i \in \Lambda)$ and possessing the required structure for the formation of a quasi-division ring, F_i. Then, the direct sum $F = \bigoplus_{i \in \Lambda} F_i$ comprises elements of the form $f = (f_i)_\Lambda$, made up of components $f_i \in F_i$, $i \in \Lambda$. For any $i \in \Lambda$, $x_i \in P_i$ (so that $x_i \in P$) we define $f(x_i) = f_i(x_i)$, and addition and circle composition are defined via $(f + g)(x_i) = (f_i + g_i)(x_i)$ and $(f \circ g)(x_i) = (f_i \circ g_i)(x_i)$ respectively, while the identity, δ, is determined by $\delta(x_i) = \delta_i(x_i)$. It is trivial to show that F forms a quasi-division ring under these operations.

If we have a locally finite partially ordered set with a number of minimal elements, but still satisfying the requirement that a given element is comparable

with only one of these minimal elements, then it can be broken up into a number of disjoint posets having a least element. However, we note that it may be possible to form a quasi-division ring on the poset as a whole which is *not* the direct sum of the disjoint posets. This is seen in Example 2.2.13.

In the case that $\circ$ commutes we can consider whether or not the additive and circle composition groups of the quasi-division ring are isomorphic. Recall, first, that for $f \in F$, f maps P to the ring K. Now suppose there exists a function λ defined on P such that either λ maps P to $\mathbf{N} \cup \{0\}$ and K is an algebra over the rationals, or λ maps P to K where K is a field. Furthermore, suppose that for any $y \leq x$ in P, the function λ satisfies $\lambda(y) + \lambda(w(x,y)) = \lambda(x)[= \lambda(c(y, w(x,y)))]$ and also that $\lambda(x) \neq 0$ when $x \notin \mathrm{Min}(P)$. The former property implies that $\lambda(e_x) = 0$ and that λ can be thought of as a logarithm-like function. If such a λ exists then we can show that $(F, +)$ is isomorphic to $(F, \circ)$. The following proofs are similar to those of [18] and [31].

Define the operator L on F as follows:

$$(Lf)(x) = \begin{cases} 1, & \text{if } x \in \mathrm{Min}(P); \\ \sum_{y \leq x} f(y) f^{\circ(-1)}(w(x,y))\lambda(y) & \text{otherwise,} \end{cases}$$

so that $Lf \in F$. Denote $f(y)\lambda(y)$ by $f'(y)$, so that $(\mathrm{L}f\,)(x) = (f' \circ f^{\circ(-1)})(x)$. We note that f' need not be in F since $f'(e) = f(e)\lambda(e)$ may not equal 1 when $e \in \mathrm{Min}(P)$. In what follows we will use a slightly more natural addition for functions in F, defined by $(f \hat{+} g)(x) = f(x) + g(x)$, for all $x \in P$.

Now for all $x \in P$,

$$(f \circ g)'(x) = (f \circ g)(x)\lambda(x) = \sum_{y \leq x} f(y) g(w(x,y))\lambda(x).$$

Further,

$$\begin{aligned} &((f' \circ g) \hat{+} (f \circ g'))(x) \\ &\quad = (f' \circ g)(x) + (f \circ g')(x) \end{aligned}$$

$$
\begin{aligned}
&= \sum_{y\le x} f'(y)g(w(x,y)) + \sum_{y\le x} f(y)g'(w(x,y)) \\
&= \sum_{y\le x} f(y)\lambda(y)g(w(x,y)) + \sum_{y\le x} f(y)g(w(x,y))\lambda(w(x,y)) \\
&= \sum_{y\le x} f(y)g(w(x,y))[\lambda(y) \ + \ \lambda(w(x,y))] \\
&= \sum_{y\le x} f(y)g(w(x,y))\lambda(x),
\end{aligned}
$$

by the conditions on λ. Hence $(f \circ g)' = (f' \circ g)\hat{+}(f \circ g')$.

Finally, note that $\circ$ is distributive (as opposed to quasi-distributive) over $\hat{+}$:

$$
\begin{aligned}
((f\hat{+}g) \circ h)(x) &= \sum_{y\le x}(f\hat{+}g)(y)h(w(x,y)) \\
&= \sum_{y\le x}(f(y)+g(y))h(w(x,y)) \\
&= \sum_{y\le x} f(y)h(w(x,y)) + \sum_{y\le x} g(y)h(w(x,y)) \\
&= (f \circ h)(x)\hat{+}(g \circ h)(x).
\end{aligned}
$$

Lemma 2.2.5 *If $\circ$ is commutative then L is a logarithm operator between $(F, \circ)$ and $(F, +)$.*

Proof: $[L(f \circ g)](e) = 1 = [(Lf) + (Lg)](e)$ for $e \in \mathrm{Min}(P)$. If $x \notin \mathrm{Min}(P)$ then

$$
\begin{aligned}
&[L(f \circ g)](x) \\
&= [(f \circ g)' \circ (f \circ g)^{\circ(-1)}](x) \\
&= [\{(f' \circ g)\hat{+}(f \circ g')\} \circ (f \circ g)^{\circ(-1)}](x) \\
&= [\{(f' \circ g)\hat{+}(f \circ g')\} \circ g^{\circ(-1)} \circ f^{\circ(-1)}](x) \\
&= [\{(f' \circ g) \circ g^{\circ(-1)} \circ f^{\circ(-1)}\}\hat{+}\{(f \circ g') \circ g^{\circ(-1)} \circ f^{\circ(-1)}\}](x) \\
&= [(f' \circ f^{\circ(-1)})\hat{+}(g' \circ g^{\circ(-1)})](x) \\
&= (Lf)(x) + (Lg)(x) = (Lf + Lg)(x),
\end{aligned}
$$

noting that many of the above operations took place outside F where $\circ$ distributes over $\hat{+}$. Consequently $L(f \circ g) = Lf + Lg$ so we conclude that L is a group homomorphism. $\square$

Theorem 2.2.6 *When $\circ$ is commutative and a suitable function λ exists, $(F, \circ)$ is isomorphic to $(F, +)$.*

Proof: We need only show that L is a bijection. Given $g \in F$, we obtain $f \in F$ such that $Lf = g$ by induction on $\#(x)$. Define $f(e) = 1$ for $e \in \mathrm{Min}(P)$, and suppose that $f(u)$ and $f^{\circ(-1)}(u)$ are defined for all u such that $\#(u) < \#(x)$. Now

$$\begin{aligned} g(x) &= (Lf)(x) = \sum_{y \leq x} f'(y) f^{\circ(-1)}(w(x,y)) \\ &= \sum_{y<x} f'(y) f^{\circ(-1)}(w(x,y)) + f'(x) f^{\circ(-1)}(w(x,x)) \\ &= \sum_{y<x} f'(y) f^{\circ(-1)}(w(x,y)) + f'(x)\lambda(x) \\ &= \sum_{y<x} f(y) f^{\circ(-1)}(w(x,y))\lambda(y) + f(x)\lambda(x), \end{aligned}$$

as $w(x,x) \in \mathrm{Min}(P)$ (by $(w3)$) and so $f^{\circ(-1)}(w(x,x)) = 1$. Therefore

$$f(x) = [\lambda(x)]^{-1} \left\{ g(x) - \sum_{y<x} f(y) f^{\circ(-1)}(w(x,y))\lambda(y) \right\},$$

where the right-hand side exists by the inductive hypothesis, $(w4)$ and the fact that $\lambda(e_x) = 0$. Note that $[\lambda(x)]^{-1} \left\{ g(x) - \sum_{y<x} f(y) f^{\circ(-1)}(w(x,y))\lambda(y) \right\}$ exists since $\lambda(x) \neq 0$ when $x \notin \mathrm{Min}(P)$, and because either $\lambda(x) \in \mathbf{N}$ and K is an algebra over the rationals, or $\lambda(x) \in K$ and K is a field. It is routine to verify that f satisfies $Lf = g$ as required. Thus L is surjective; it is also injective since this value of $f(x)$ is uniquely determined. Hence L is an isomorphism and so $(F, \circ) \cong (F, +)$. □

We will now present some examples which show how this construction can be applied to specific posets. Some of these examples subsume or supplement the results of [22] and [18], while others are new. In the case of Examples 2.2.7 to 2.2.11 we can demonstrate that in certain circumstances such rings will be in $\mathcal{K}$. The later examples, on the other hand, are not commutative with respect to

the circle operation, so the question of the existence of an isomorphism between the additive and circle groups does not arise.

Example 2.2.7 *Uniquely Complemented Locally Finite Lattices*

Let P be a lattice such that for any $x \in P$ there exists a unique minimal element e_x such that $e_x \leq x$ and which satisfies the condition that the set $[e_x, x] = \{y \in P \mid e_x \leq y \leq x\}$ is a uniquely complemented locally finite lattice. (By *uniquely complemented lattice* we mean a lattice which has greatest and least elements 1 and 0 respectively, such that for any element y in the lattice there exists a unique lattice element y' — called the *complement* of y — satisfying $y \wedge y' = 0$ and $y \vee y' = 1$; this contrasts with *complemented lattices* in which an element may have a number of complements.) Then we can form a quasifield on P, as we can show that it satisfies the required conditions. Given x and $y \leq x$, let y'_x denote the (unique) complement of y with respect to x, so that within the lattice $[e_x, x]$ we have $y \vee y'_x = x$ and $y \wedge y'_x = e_x$. (Note that for $y \leq x$ we have $y \vee x = x$ and $y \wedge x = y$.)

$(w1)$: For $y \leq x$ define $w(x, y) = y'_x \in P$, and so w is a function.

$(w2)$: $w(x, y) = y'_x = x \Leftrightarrow y \vee y'_x = y \vee x = x$ and $y \wedge y'_x = y \wedge x = e_x \Leftrightarrow y = e_x$.

$(w3)$: $w(x, y) = y'_x = e_x \Leftrightarrow y \vee y'_x = y \vee e_x = x$ and $y \wedge y'_x = y \wedge e_x = e_x \Leftrightarrow y = x$.

$(w4)$: $\#(x)$ is finite $(= |[e_x, x]|)$, and as $y'_x \leq x$ then $\#(w(x, y)) \leq \#(x)$.

Now S is the subset of $P \times P$ such that $(y, z) \in S$ if and only if there exists $x \in P$ such that $y \leq x$ and $z \leq w(x, y) = y'_x$. For such $(y, z) \in S$ define $c(y, z) = y \vee z$. This is defined, since $y \leq x$ and $z \leq y'_x \leq x$ (i.e. $y, z \in [e_x, x]$ for some x; $[e_x, x]$ is a lattice and so the join exists). Now consider a given $x \in P$.

$(c1)$: Given $(y, z) \in S$ there exists $k \in P$ such that $y \leq k$ and $z \leq w(k, y) = y'_k$. Now suppose $c(y, z) = y \vee z = x$. Then $y \leq x$ and $z \leq x$; whence $y \wedge z \leq y \wedge y'_k = e_x$ (since $z \leq y'_k$). Thus $y \wedge z = e_x$ and $y \vee z = x$, so

that $z = y'_x$ as required. Conversely, if $y \leq x$ and $z = w(x, y) = y'_x$ then $c(y, z) = y \vee z = y \vee y'_x = x$ as required.

$(c2)$: For a given x we have that y, u, v satisfies the condition $c(y, c(u, v)) = x \Leftrightarrow y \vee (u \vee v) = x$ if and only if y, u, v satisfies $(y \vee u) \vee v = x \Leftrightarrow c(c(y, u), v) = x$.

Consequently we have a quasi-division ring on P; if K is commutative then the commutativity of $\circ$ follows since circle composition involves each element of $[e_x, x]$ and its complement. However, the complements are also elements of $[e_x, x]$, and the complement of the complement of a given element must be the original element (since we have a uniquely complemented lattice). Therefore, $(f \circ g)(x)$ will involve terms of the form $f(y)g(y'_x)$ and also $f(y'_x)g(y)$, as will $(g \circ f)(x)$. □

We will now give a specific instance of such a lattice.

Example 2.2.8 *Sets (see also [22])*

The classic example of a partially ordered set satisfying the above requirements is the set, $\mathcal{S}$, of finite subsets of some set S, ordered by inclusion, which has the empty set as its least element. Given a particular finite subset $A \in \mathcal{S}$ and $B \subseteq A$ then the complement of B within the lattice of subsets of A is just the usual set complement $C = A \backslash B$. This satisfies $B \cap C = \emptyset$ and $B \cup C = A$, and is clearly unique. Consequently a quasi-division ring can be formed on $\mathcal{S}$, by Example 2.2.7.

In the case that K is commutative we have a quasifield, and it can then be shown (provided K is further required to be an algebra over the rationals) that the additive and circle composition groups are isomorphic. For $B \subseteq A$ define $\lambda(B) = |B|$. Then for $C \subseteq B \subseteq A$ we have $\lambda(C) + \lambda(w(B, C)) = \lambda(C) + \lambda(B \backslash C) = |C| + |B \backslash C| = |B| = \lambda(B)$ as required, and the result follows by Theorem 2.2.6. K is required to be a commutative algebra over the rationals because λ maps to $\mathbf{N} \cup \{0\}$. Furthermore, this isomorphism differs from that

constructed in [22]. There, the underlying ring with identity need have no additional constraints, and the logarithm function $L : (F, \circ) \to (F, +)$ is given by $(L(f))(0) = 1$ and $(L(f))(A) = \sum_{r=1}^{|A|} \frac{(-1)^{r-1}}{r} f^r(A)$. □

Example 2.2.9 *Cauchy Convolution (see also H-convolution in [18])*

Let P be the set of whole numbers with the usual ordering; this set has least element 0.

($w1$): If $m \leq n$ then we define $w(n, m) = n - m$ and this is clearly in P.

($w2$): $w(n, m) = n - m = n \Leftrightarrow m = 0$.

($w3$): $w(n, m) = n - m = 0 \Leftrightarrow m = n$.

($w4$): $\#(w(n, m)) = n - m + 1 \leq n + 1 = \#(n)$, and equality only occurs when $m = 0$.

Consider $n_1, n_2 \in P$. Then $n = n_1 + n_2$ is such that $n_1 \leq n$ and $n_2 \leq w(n, n_1)$ (in fact, $n_2 = w(n, n_1)$), so $S = P \times P$. Define $c(n_1, n_2) = n_1 + n_2$; this is in P.

($c1$): $c(n_1, n_2) = n_1 + n_2 = n \Leftrightarrow n_1 \leq n$ and $n_2 = n - n_1 = w(n, n_1)$.

($c2$): This is guaranteed by the associativity of addition.

Again the Cauchy convolution, $\circ$, is commutative when K is, and Haukkanen [18] shows that the additive and convolution groups are isomorphic via $\lambda(n) = n$, a function which satisfies the desired conditions for the application of Theorem 2.2.6. We note that since $\lambda(n) \in \mathbf{N} \cup \{0\}$ we also require K to be an algebra over the rationals.

[Note the equivalence of the Cauchy Convolution as presented here and the power series ring $XK[[X]]$ consisting of those power series having zero constant term.] □

Example 2.2.10 *Divisibility: The Dirichlet Convolution (see also [18])*

The familiar Dirichlet convolution from the theory of arithmetical functions gives rise to another example of a quasifield with isomorphic groups. Let $P = \mathbf{N}$

be the set of natural numbers ordered by divisibility, with the least element being 1, and for d, $n \in P$ where $d|n$ we define $w(n,d) = \frac{n}{d}$, which is clearly in $\mathbf{N}$, i.e. $(w1)$ holds.

$(w2)$: $w(n,d) = \frac{n}{d} = n \Leftrightarrow d = 1$.

$(w3)$: $w(n,d) = \frac{n}{d} = 1 \Leftrightarrow d = n$.

$(w4)$: $\#(w(n,d)) = \#(\frac{n}{d})$ = the number of divisors of $\frac{n}{d}$. Any divisor of $\frac{n}{d}$ divides n so that $\#(\frac{n}{d}) \leq \#(n)$. Equality only occurs when $d = 1$.

Consider $n_1, n_2 \in \mathbf{N}$. Then $n = n_1 n_2$ is such that $n_1|n$ and $n_2|w(n,n_1)$ (again, $n_2 = w(n,n_1)$). Thus $S = \mathbf{N} \times \mathbf{N}$ so we can define c for all elements of $\mathbf{N} \times \mathbf{N}$. In particular, define $c(n_1,n_2) = n_1 n_2$; this is clearly in $\mathbf{N}$.

$(c1)$: $c(n_1,n_2) = n \Leftrightarrow n_1 n_2 = n \Leftrightarrow n_1|n$ and $n_2 = \frac{n}{n_1} = w(n,n_1)$.

$(c2)$: Given $n \in \mathbf{N}$, suppose r, s, t satisfy $c(r, c(s,t)) = n$. Then $r(st) = n$, and, by associativity, $(rs)t = n$ so that $c(c(r,s),t) = n$ as required; the converse is similar.

Provided K is commutative, the commutativity of $\circ$ follows from the fact that as d runs through all the divisors of n then so does $\frac{n}{d}$. Haukkanen [18] shows that the isomorphism of the additive and circle composition groups follows via the logarithm function $\lambda(n) = \log(n)$, by restricting K to $\mathbf{R}$. If K is a commutative algebra over the rationals we can still obtain an isomorphism. Suppose that $n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}$ (p_i prime, $\alpha_i \in \mathbf{N}$) is n's complete prime factorization. Define $\lambda(1) = 0$ and $\lambda(n) = \alpha_1 + \alpha_2 + \cdots + \alpha_k$. Then, if $d|n$, d will have some of these prime factors while $\frac{n}{d}$ will have those that remain, so that $\lambda(d) + \lambda(\frac{n}{d}) = \lambda(n)$ as required. Hence, by Theorem 2.2.6, $(F,+) \cong (F,\circ)$. $\square$

Example 2.2.11 *Polynomials Over the Integers*

Let P be the set of all polynomials having integer coefficients and ordered by divisibility. The least element of this set is the polynomial 1.

$(w1)$: If $q(x)|p(x)$ then we define $w(p(x),q(x)) = p(x)/q(x)$ which is in P.

($w2$): $w(p(x), q(x)) = p(x)/q(x) = p(x) \Leftrightarrow q(x) = 1$.

($w3$): $w(p(x), q(x)) = p(x)/q(x) = 1 \Leftrightarrow q(x) = p(x)$.

($w4$): $\#(w(p(x), q(x))) = \#(p(x)/q(x))$ and this is the number of divisors of $p(x)/q(x)$. Any polynomial divisor of $p(x)/q(x)$ will divide $p(x)$ so that $\#(p(x)/q(x)) \leq \#(p(x))$, with equality occurring if and only if $q(x) = 1$.

Consider $p_1(x), p_2(x) \in P$. Then $p(x) = p_1(x)p_2(x)$ is such that $p_1(x)|p(x)$ and $p_2(x)|w(p(x), p_1(x))$ (with $p_2(x) = w(p(x), p_1(x))$, in fact), so $S = P \times P$. For $p_1(x), p_2(x) \in P$ we define $c(p_1(x), p_2(x)) = p_1(x)p_2(x)$; this is in P.

($c1$): $c(p_1(x), p_2(x)) = p_1(x)p_2(x) = p(x)$ if and only if $p_1(x)|p(x)$ and $p_2(x) = p(x)/p_1(x)$.

($c2$): This follows from the associativity of polynomial multiplication.

Circle composition is commutative when the underlying ring is (for the same reasons as for the Dirichlet convolution), so now we can consider the existence or otherwise of an isomorphism between $(F, +)$ and $(F, \circ)$. In the following discussion we shall denote the greatest (positive) integer factor of a polynomial $p(x)$ by "gif($p(x)$)" and the degree of the polynomial by the usual "deg($p(x)$)". Let $K = \mathbf{R}$ and define λ via

$$\lambda(p(x)) = \deg(p(x)) + \log(\text{gif}(p(x))).$$

If $q(x)|p(x)$ we have

$$\begin{aligned} &\lambda(q(x)) + \lambda(p(x)/q(x)) \\ &\quad = \deg(q(x)) + \log(\text{gif}(q(x))) + \deg(p(x)/q(x)) + \log(\text{gif}(p(x)/q(x))) \\ &\quad = \deg(p(x)) + \log(\text{gif}(p(x))), \end{aligned}$$

by the properties of degrees of polynomials and since

$$\begin{aligned} &\log(\text{gif}(q(x))) + \log(\text{gif}(p(x)/q(x))) \\ &\quad = \log(\text{gif}(q(x)) \cdot \text{gif}(p(x)/q(x))) = \log(\text{gif}(p(x))). \end{aligned}$$

Now $\lambda(p(x)) = 0$ if and only if $\deg(p(x)) = 0$ and $\log(\text{gif}(p(x))) = 0$, whence we have first that $p(x)$ is a constant polynomial, and then that $\text{gif}(p(x)) = 1$. Therefore $p(x) = 1$; so that λ satisfies the requirements for the existence of an isomorphism between $(F, +)$ and $(F, \circ)$, provided $K = \mathbf{R}$. □

Our final examples are included in order to show the generality of the construction. They are not, however, commutative, and so they are of limited interest because they will not have an isomorphism between the additive and circle composition groups.

Example 2.2.12 *Words*

Let P be the set of words formed by an alphabet A and ordered by left inclusion (for example, if $A = \{a, b, c\}$ then $caba \in P$ and $c, ca, cab, caba \leq caba$, while a, b, aba, $cba \not\leq caba$). The empty word is the least element of P.

$(w1)$: If α, β are words and $\beta \leq \alpha$ then define $w(\alpha, \beta)$ to be the word remaining when β is removed from the beginning of α. This is clearly in P.

$(w2)$: If $\beta \leq \alpha$ then $w(\alpha, \beta) = \alpha \Leftrightarrow \beta$ is the empty word.

$(w3)$: If $\beta \leq \alpha$ then $w(\alpha, \beta)$ is the empty word $\Leftrightarrow \alpha = \beta$.

$(w4)$: Since, for $\beta \leq \alpha$, $w(\alpha, \beta)$ is a shorter word than α (or possibly equal) then $\#(w(\alpha, \beta)) \leq \#(\alpha)$, with equality occurring if and only if β is the empty word.

Consider $\alpha, \beta \in P$. Then $\gamma = \alpha\beta$ (where, by $\alpha\beta$ we mean α and β concatenated) is such that $\alpha \leq \gamma$ and $\beta \leq w(\gamma, \alpha)$; in fact, equality is clear, so that $S = P \times P$. For any $\alpha, \beta \in P$ define $c(\alpha, \beta)$ to be the concatenation of α and β as $\alpha\beta$. This is obviously in P.

$(c1)$: $c(\alpha, \beta) = \gamma \Leftrightarrow \alpha\beta = \gamma \Leftrightarrow \alpha \leq \gamma$ and $\beta = w(\alpha, \gamma)$ as required.

$(c2)$: Given $\theta \in P$, suppose α, β, γ satisfy $c(\alpha, c(\beta, \gamma)) = \theta$. Then $\theta = c(\alpha, \beta\gamma) = \alpha(\beta\gamma) = (\alpha\beta)\gamma = c(c(\alpha, \beta), \gamma)$ as required.

Consequently there is a quasi-division ring defined on this poset of words. We note that $\circ$ is not commutative because of the left-biassed ordering. $\square$

Example 2.2.13 *Intervals/Incidence Algebras*

In this example the underlying poset may have numerous minimal elements. However, although it may thus be the union of a corresponding number of disjoint posets each having a least element, the quasi-division ring we construct is *not* a direct sum of quasi-division rings formed on the disjoint posets (see under ($w1$) below for the reason).

Let P be the poset formed by considering a locally finite poset $(\mathcal{P}, \preceq)$, with $[x, y] \in P$ if $x, y \in \mathcal{P}$ and $x \preceq y$. The ordering, $\leq$, on P is given by $[x, y] \leq [z, w]$ if and only if $x = z$ and $y \preceq w$ (i.e. $[x, y] \leq [x, z]$ when $y \preceq z$). $\text{Min}(P) = \{[x, x] | x \in \mathcal{P}\}$, so that every $x \in \mathcal{P}$ gives rise to a minimal element in P, and thus we can think of P as the union of a collection of disjoint locally finite posets P_x, where P_x consists of elements of the form $[x, y]$, $x \preceq y$, and has least element $[x, x]$.

($w1$): For $[x, y] \leq [x, z]$ define $w([x, z], [x, y]) = [y, z]$ which is in P as required, since $y \preceq z$. (We note, however, that while $[x, y]$ and $[x, z]$ are in P_x, $[y, z]$ is in P_y, so although w is defined on $P_x \times P_x$ its images don't necessarily lie in P_x. Thus, we are not forming a quasi-division ring on P_x alone and so we do not have the quasi-division ring arising as a direct sum.)

($w2$): If $[x, y] \leq [x, z]$ then $w([x, z], [x, y]) = [y, z] = [x, z] \Leftrightarrow y = x$, i.e. $[x, y] = [x, x] \in \text{Min}(P)$ as required.

($w3$): If $[x, y] \leq [x, z]$ then $w([x, z], [x, y]) = [y, z] \in \text{Min}(P) \Leftrightarrow y = z$, i.e. $[x, y] = [x, z]$ as required.

($w4$): $\#([x, y]) =$ the number of elements of $\mathcal{P}$ between x and y inclusive. For $[x, y] \leq [x, z]$ we have $\#(w([x, z], [x, y])) = \#([y, z]) =$ the number of elements of $\mathcal{P}$ between y and z inclusive. However, $x \preceq y$ so that $\#([y, z]) \leq \#([x, z])$,

as required. Equality occurs when $y = x$, i.e. when $[x, y] = [x, x] \in \mathrm{Min}(P)$.

To determine $S \subseteq P \times P$ we note that $([x, y], [v, z]) \in S$ if and only if there exists $[a, b] \in P$ such that $[x, y] \leq [a, b]$ and $[v, z] \leq w([a, b], [x, y])$. This means that $x = a$ and $y \preceq b$, from which we have $w([a, b], [x, y]) = w([x, b], [x, y]) = [y, b]$, and so for $[v, z] \leq [y, b]$ we have $v = y$ and $z \preceq b$, whence S comprises elements of the form $([x, y], [y, z])$ with $x \preceq y \preceq z$. We define c on S via $c([x, y], [y, z]) = [x, z] \in P$.

$(c1)$: $c([x, y], [y, z]) = [x, z] \Leftrightarrow [x, y] \leq [x, z]$ and $[y, z] = w([x, z], [x, y])$.

$(c2)$: Suppose $[x, z] \in P$ and that $[a, b]$, $[d, e]$ and $[e, f]$ are elements in P satisfy $c([a, b], c([d, e], [e, f])) = [x, z]$. Then we must have $c([a, b], [d, f]) = [x, z]$, whence $b = d$ and $a = x$, $f = z$. Then

$$c(c([a, b], [d, e]), [e, f]) = c(c([x, b], [b, e]), [e, z]) = c([x, e], [e, z]) = [x, z]$$

The converse is similar.

Thus we can construct a quasi-division ring on the poset of intervals P. Note that in this case $\circ$ is not commutative, because the intervals are ordered by keeping the "lower" end fixed and comparing the "upper" ends of the intervals, using $\mathcal{P}$'s ordering $\preceq$. □

Before concluding this section, we observe that if we have a poset which is suitable for the construction of a quasi-division ring then it may be possible to consider some restriction of the poset and still be able to construct a (different) quasi-division ring. For example, we can consider a restricted version of the Cauchy convolution quasifield of Example 2.2.9 by taking, for example, all the whole numbers less than or equal to some n; or with the Dirichlet convolution quasifield of Example 2.2.10 by taking either the same restriction as for the restricted Cauchy convolution or by taking some $n \in \mathbf{N}$ together with all its factors. Consequently there exist quasifields which are constructed on posets of finite height. Results concerning such structures will be considered in the next

section as well as Chapter 3 and Section 4.5. Whether or not such rings are in $\mathcal{K}$ depends on the underlying ring.

[Note: Haukkanen [18] and Wyss [42] show that for some posets — in particular, those leading to the Cauchy and Dirichlet convolution quasifields — an extra term can be incorporated in the definition of circle composition. Haukkanen defines circle composition for non-minimal $x \in P$ as $(f \circ g)(x) = \sum_{y \leq x} f(y)g(w(x,y))H(x,y)$, where H is a function from a subset of $P \times P$ to K which satisfies

(i) $H(x,x) = H(x,e_x) = 1$ for all $x \in P$;

(ii) $H(x,y)H(y,z) = H(x,z)H(w(x,z),w(y,z))$ for all $z \leq y \leq x$; and

(iii) $H(x,y) = H(x,w(x,y))$ for all $y \leq x$.

These conditions ensure the existence of an identity, and associativity and commutativity respectively. Wyss's example of a quasiregular ring is the Cauchy convolution with $H(n,i) = \binom{n}{i}$ which meets Haukkanen's requirements. Haukkanen is able to obtain an isomorphism in these cases. We have not attempted to generalise this part of Haukkanen's results.]

2.3 Finite quasifields over Z

In the previous section we constructed quasifields using a poset and an underlying ring with identity. However, in order to obtain examples which had isomorphic additive and circle composition groups we had to place additional constraints on the underlying ring, such as being a field or an algebra over the rationals. The integers are neither, and yet it is possible to obtain quasifields which are in $\mathcal{K}$ when the underlying ring is $\mathbf{Z}$. We do this by showing that the groups $(F,+)$ and $(F,\circ)$ have the same rank and are free, but in order to achieve this we need to place constraints on the poset.

In what follows P is a *finite* poset which, in addition, satisfies the conditions

for the construction of a quasifield (see Section 2.2; examples include the finite restrictions of the partially ordered sets discussed later on page 76). Let $P' = P \backslash \mathrm{Min}(P)$ and then for each $x \in P'$ let ε_x denote the element of the quasifield F which satisfies the following conditions:

$$\begin{aligned} &\varepsilon_x(x) = 1 \\ &\varepsilon_x(y) = 1 \text{ for } y \in \mathrm{Min}(P), \text{ and} \\ &\varepsilon_x(y) = 0 \text{ for all } y \in P', y \neq x. \end{aligned}$$

We will eventually prove that the set $B = \{\varepsilon_x \,|\, x \in P'\}$ is a basis for $(F, \circ)$ (and, more obviously, for $(F, +)$). There will be obvious similarities between these proofs and those of Section 2.4.

Our first lemma is merely a useful observation about our partially ordered sets.

Lemma 2.3.1 *If $x, y, t \in P$ with $t \leq y$ and where y and x are incomparable, then either (i) t and x are incomparable, or (ii) $t < x$.*

Proof: The third alternative, namely $t \geq x$ is not possible because then we would have $x \leq t \leq y$ contradicting the incomparability of x and y. □

Our next lemma examines the behaviour of elements of B under repeated circle composition. As usual we shall denote "powers" of an element $f \in F$ by $f^{\circ k}$. It will be important to recall that the functions in F are taking their values in $\mathbf{Z}$ in this case.

Lemma 2.3.2 *If $n \in \mathbf{Z}$ then $\varepsilon_x^{\circ n}(x) = n$, while $\varepsilon_x^{\circ n}(y) = 0$ when y satisfies $e_x < y < x$ or when y is not related to x.*

Proof: [Note that in this proof we are not concerning ourselves with the values of $\varepsilon_x^{\circ n}(y)$ when $y > x$, because it will turn out that these values — which are computationally non-trivial — have no bearing on whether or not B forms a basis.]

First, let us observe that by the definition of ε_x the result holds for $n = 1$. Second, suppose that the result holds for $n = k - 1$. Then for any $y \in P$ we have, by the definition of the circle composition operation in F, that $\varepsilon_x^{\circ k}(y) = (\varepsilon_x \circ \varepsilon_x^{\circ(k-1)})(y) = \sum_{t \leq y} \varepsilon_x(t)\varepsilon_x^{\circ(k-1)}(w(y,t))$. There are three cases to consider: $y < x$, y is not comparable with x, and $y = x$. We will consider the first two situations together.

We are concerned with what happens to the values of $\varepsilon_x(t)$ for $t \leq y$. In the case that $y < x$ we have $t < x$, while in the case that y is not related to x then by Lemma 2.3.1 either $t < x$ or t is not related to x. From this and the definition of ε_x it follows that $\varepsilon_x(t) = 0$ for all non-minimal $t \leq y$. Thus $\varepsilon_x^{\circ k}(y) = \varepsilon_x(e_y)\varepsilon_x^{\circ(k-1)}(w(y,e_y)) = \varepsilon_x^{\circ(k-1)}(y) = 0$ by the inductive hypothesis and since we always have $f(z) = 1$ for $z \in \mathrm{Min}(P)$ and $w(y,e_y) = y$ by property $(w2)$ of Section 2.2. Note that, as in that section, e_y is the unique minimal element less than or equal to y.

On the other hand, when $y = x$ we have

$$\begin{aligned}
\varepsilon_x^{\circ k}(x) &= (\varepsilon_x \circ \varepsilon_x^{\circ(k-1)})(x) \\
&= \sum_{t \leq x} \varepsilon_x(t)\varepsilon_x^{\circ(k-1)}(w(x,t)) \\
&= \varepsilon_x(e_x)\varepsilon_x^{\circ(k-1)}(w(x,e_x)) + \varepsilon_x(x)\varepsilon_x^{\circ(k-1)}(w(x,x)) \\
&= \varepsilon_x^{\circ(k-1)}(x) + \varepsilon_x(x)
\end{aligned}$$

because, in addition to the properties used at the end of the previous paragraph, we also have $\varepsilon_x(t) = 0$ for all $e_x < t < x$ and $w(x,x) \in \mathrm{Min}(P)$ by property $(w3)$ of Section 2.2. Using the inductive hypothesis and the definition of ε_x we thus have $\varepsilon_x^{\circ k}(x) = (k-1) + 1 = k$, as required.

This gives the required result for all positive integers n; if in addition we define $f^{\circ 0}(z) = 0$ for all $f \in F, z \notin \mathrm{Min}(P)$, all that remains is to look at the negative integers, which we shall do by considering the circle composition inverse of $\varepsilon_x^{\circ n}$. We have $\varepsilon_x^{\circ n} \circ \varepsilon_x^{\circ(-n)} = \delta$ and hence $0 = (\varepsilon_x^{\circ n} \circ \varepsilon_x^{\circ(-n)})(y) =$

$\sum_{t\leq y} \varepsilon_x^{\circ n}(t)\varepsilon_x^{\circ(-n)}(w(y,t))$ for all $y \notin \mathrm{Min}(P), y \neq x$.

Now for all y not related to x and all $y < x$ if $t \leq y$ then we know that either $t < x$ or t is not related to x and so, by the earlier part of this proof, $\varepsilon_x^{\circ n}(t) = 0$, except for $t = e_y$. Thus, in this situation, $0 = \varepsilon_x^{\circ n}(e_y)\varepsilon_x^{\circ(-n)}(w(y,e_y)) = \varepsilon_x^{\circ(-n)}(y)$ as required.

Finally, if $y = x$ we have

$$\begin{aligned} 0 &= (\varepsilon_x^{\circ n} \circ \varepsilon_x^{\circ(-n)})(x) \\ &= \sum_{t\leq x} \varepsilon_x^{\circ n}(t)\varepsilon_x^{\circ(-n)}(w(x,t)) \\ &= \varepsilon_x^{\circ n}(e_x)\varepsilon_x^{\circ(-n)}(w(x,e_x)) + \varepsilon_x^{\circ n}(x)\varepsilon_x^{\circ(-n)}(w(x,x)) \end{aligned}$$

since we have proved that $\varepsilon_x^{\circ n}(t) = 0$ for all $t < x, e_x \neq t$. Thus

$$0 = \varepsilon_x^{\circ(-n)}(x) + \varepsilon_x^{\circ n}(x) = \varepsilon_x^{\circ(-n)}(x) + n$$

from which it follows that $\varepsilon_x^{\circ(-n)}(x) = -n$, completing the proof. □

We next examine how a basis element interacts with an arbitrary element of F under circle composition.

Lemma 2.3.3 *If $\varepsilon_x \in B$ and f is an arbitrary element of F then the following relationships hold:*

(i) $(\varepsilon_x^{\circ n} \circ f)(x) = f(x) + n$

(ii) $(\varepsilon_x^{\circ n} \circ f)(y) = f(y)$ *for all* $y < x$ *and for all* y *not related to* x.

Proof: (i) From Lemma 2.3.2 we know that $\varepsilon_x^{\circ n}(t) = 0$ for $e_x \neq t < x$. It follows that $(\varepsilon_x^{\circ n} \circ f)(x) = \sum_{t\leq x} \varepsilon_x^{\circ n}(t)f(w(x,t)) = \varepsilon_x^{\circ n}(e_x)f(x) + \varepsilon_x^{\circ n}(x)f(w(x,x)) = f(x) + n$ by Lemma 2.3.2 since $w(x,x) \in \mathrm{Min}(P)$.

(ii) If $y < x$ then any $t < y$ is also less than x. On the other hand if y is not related to x then Lemma 2.3.1 tells us that either t is not related to x or $t < x$. Thus for y and x satisfying the conditions stated for the second part of

the current Lemma we know, by Lemma 2.3.2, that $\varepsilon_x^{\circ n}(t) = 0$ for $e_y \neq t \leq y$. Consequently $(\varepsilon_x^{\circ n} \circ f)(y) = \sum_{t \leq y} \varepsilon_x^{\circ n}(t) f(w(y,t)) = \varepsilon_x^{\circ n}(e_y) f(y) = f(y)$ as required.

Again, as intimated in the proof of the previous lemma, the interaction of the basis element ε_x with an arbitrary element of F on poset elements *larger* than x, while non-trivial, has no bearing on our results. □

In what follows — and later in the thesis — we shall use the symbol $\coprod$ for circle composition in the same way as $\sum$ and Π are used for addition and multiplication respectively. Recall (see page 16) the definition of the height function defined on posets.

Theorem 2.3.4 *If F is a quasifield constructed on a poset of finite height with* $\mathbf{Z}$ *as underlying ring then $(F, +) \cong (F, \circ)$*

Proof: We shall prove this result by showing that the set $B = \{\varepsilon_x \,|\, x \in P'\}$ is a basis for $(F, \circ)$, where $P' = P \backslash \mathrm{Min}(P)$. It is obvious that B is a basis for $(F, +)$ since $(F, +)$ is a direct sum of $|P \backslash \mathrm{Min}(P)|$ copies of $\mathbf{Z}$.

First of all we shall show that B generates $(F, \circ)$. Given $f \in F$, consider the circle composition product $\coprod_{x \in P'} \varepsilon_x^{\circ n_x}$, where the values of n_x are defined inductively via $n_x = f(x)$ for $x \in P'$ such that $h(x) = 1$ and $n_x = f(x) - (\coprod_{0 < h(y) < k} \varepsilon_y^{\circ n_y})(x)$ where $h(x) = k$. We will use induction to show that, in fact, $\coprod_{x \in P'} \varepsilon_x^{\circ n_x} = f$.

Suppose that $y \in P'$ is an element of height 1. Then we have

$$\begin{aligned}
(\coprod_{x \in P'} \varepsilon_x^{\circ n_x})(y) &= (\varepsilon_y^{\circ n_y} \circ \coprod_{x \in P' \backslash y} \varepsilon_x^{\circ n_x})(y) \\
&= \varepsilon_y^{\circ n_y}(y) + (\coprod_{x \in P' \backslash y} \varepsilon_x^{\circ n_x})(y) \\
&\quad \text{(as } (f \circ g)(y) = f(y) + g(y) \text{ for elements } y \text{ of height 1)} \\
&= \varepsilon_y^{\circ n_y}(y)
\end{aligned}$$

(since y, being of height 1, is either smaller than or incomparable with any of the remaining $x \in P'$)

$= n_y$ (by Lemma 2.3.2)

$= f(y)$ (by definition).

Suppose that $(\coprod_{x\in P'} \varepsilon_x^{\circ n_x})(y) = f(y)$ for all $y \in P'$ such that $h(y) < k$ and now consider $y \in P'$ having height k. Then

$$\begin{aligned}(\coprod_{x\in P'} \varepsilon_x^{\circ n_x})(y) &= (\coprod_{h(x)>k} \varepsilon_x^{\circ n_x} \circ \coprod_{0<h(x)\leq k} \varepsilon_x^{\circ n_x})(y) \\ &= \sum_{t\leq y}(\coprod_{h(x)>k} \varepsilon_x^{\circ n_x})(t)(0 < \coprod_{h(x)\leq k} \varepsilon_x^{\circ n_x})(w(y,t)).\end{aligned}$$

Consider $(\coprod_{h(x)>k} \varepsilon_x^{\circ n_x})(t)$. The expansion of this will involve sums of products of terms, each product comprising at least one term of the form $\varepsilon_x^{\circ n_x}(s)$ for some x and where $s \leq t$. If $e_y \neq s \leq t \leq y$ then $h(s) \leq k$ and as $h(x) > k$ we cannot have $s \geq x$. Thus we must have $s < x$ or s not related to x. In either case, by Lemma 2.3.2, we have $\varepsilon_x^{\circ n_x}(s) = 0$ and hence $(\coprod_{h(x)>k} \varepsilon_x^{\circ n_x})(t) = 0$ for all t, except for $t = e_y$, in which case it equals 1.

Returning to our expansion we have

$$\begin{aligned}(\coprod_{x\in P'} \varepsilon_x^{\circ n_x})(y) &= (\coprod_{0<h(x)\leq k} \varepsilon_x^{\circ n_x})(y) \\ &= (\varepsilon_y^{\circ n_y} \circ \coprod_{x\neq y, 0<h(x)\leq k} \varepsilon_x^{\circ n_x})(y) \\ &= n_y + (\coprod_{x\neq y, 0<h(x)\leq k} \varepsilon_x^{\circ n_x})(y) \qquad \text{(using Lemma 2.3.3)} \\ &= f(y) - (\coprod_{0<h(x)<k} \varepsilon_x^{\circ n_x})(y) + (\coprod_{x\neq y, 0<h(x)\leq k} \varepsilon_x^{\circ n_x})(y)\end{aligned}$$

by the definition of n_y.

By the inductive hypothesis the values of n_x are known for $h(x) < k$ so the only terms causing difficulties in $\coprod_{x\neq y, 0<h(x)\leq k} \varepsilon_x^{\circ n_x}$ are those having values of x for which $h(x) = k$. However, in this case such an element x will be

incomparable with y since y also has height k. It follows that if z is one of the elements of height k then

$$(\coprod_{x\neq y, 0<h(x)\leq k} \varepsilon_x^{\circ n_x})(y) = (\varepsilon_z^{\circ n_z} \circ \coprod_{x\neq y,z;\, 0<h(x)\leq k} \varepsilon_x^{\circ n_x})(y) = \coprod_{x\neq y,z;\, 0<h(x)\leq k} \varepsilon_x^{\circ n_x}(y)$$

by Lemma 2.3.3. Repeating this process of extracting the functions ε_x when x is an element of height k and applying Lemma 2.3.3 yields $(\coprod_{x\neq y;\, 0<h(x)\leq k} \varepsilon_x^{\circ n_x})(y) = (\coprod_{0<h(x)<k} \varepsilon_x^{\circ n_x})(y)$. Consequently, on returning to the previous calculations, we have

$$(\coprod_{x\in P'} \varepsilon_x^{\circ n_x})(y) = f(y) - (\coprod_{0<h(x)<k} \varepsilon_x^{\circ n_x})(y) + (\coprod_{0<h(x)<k} \varepsilon_x^{\circ n_x})(y) = f(y)$$

as required.

Thus we see that the set B of proposed basis elements generates F.

We can now turn our attention to proving that B is a linearly independent set. The inductive approach and the calculations will be similar to those used in proving that B is a generating set and so we will omit those fine details which are essentially the same. Suppose that $\coprod_{x\in P'} \varepsilon_x^{\circ n_x} = \delta$ (recalling that δ is the zero element for F). Then for any $y \in P'$ such that $h(y) = 1$ we must have $(\coprod_{x\in P'} \varepsilon_x^{\circ n_x})(y) = \delta(y) = 0$. As before, $(\coprod_{x\in P'} \varepsilon_x^{\circ n_x})(y) = n_y$ for elements y of height 1, whence $n_y = 0$.

Now assume that $n_y = 0$ for all elements $y \in P'$ such that $h(y) < k$, and then consider $y \in P'$ such that $h(y) = k$. Using our previous calculations we have

$$0 = \delta(y) = (\coprod_{x\in P'} \varepsilon_x^{\circ n_x})(y) = n_y + (\coprod_{x\in P';h(x)<k} \varepsilon_x^{\circ n_x})(y) = n_y$$

by the inductive hypothesis. Thus $n_y = 0$ as required for all elements y of height k. Consequently B is a linearly independent set and hence a basis for $(F, \circ)$. Thus $\text{rank}((F, +)) = \text{rank}((F, \circ))$, whence $(F, +) \cong (F, \circ)$. □

This result, and a later result concerning quasifields whose underlying ring is $\mathbf{Z}_p$ (Corollary 3.2.5), imply that some quasifield constructions result in $\mathcal{K}$-rings even though the sufficient condition on the underlying ring is not fulfilled, i.e. we do not always have to have K being an algebra over the rationals.

Further results concerning nilpotent (and, hence, quasiregular) $\mathbf{Z}$-algebras are discussed in Section 6.3.

2.4 The Zassenhaus algebra

The construction of this example is similar to Cauchy convolution example of Section 2.2, but here the poset used is not locally finite. The approach taken here could be generalised by identifying the key features of the real interval which we use as the poset; however, this specific example suffices to exhibit this kind of ring. Although presented here slightly differently, this ring is the Zassenhaus algebra of Divinsky ([11], Example 3, page 19). Divinsky shows that the ring is nil (and hence quasiregular) but not nilpotent; however, we shall present the same results here and in Section 3.4 using notation and terminology which highlights the similarities between this example and the quasifield construction and which will enable us to prove that in certain circumstances a ring so constructed is in $\mathcal{K}$, a result which is *not* included in [11]. In the two cases where we prove that some of the Zassenhaus algebras can have isomorphic groups — Lemma 2.4.2 to Theorem 2.4.5, and Theorem 2.4.6 — our approaches are similar to those of Section 2.3 in using a basis and those of Theorem 2.2.6 and Example 2.2.9 in the use of a logarithm operator, respectively.

For a positive real number c let P denote the real interval $[0, c]$ with the usual ordering $\leq$, and let K be a ring with identity. Consider the set of functions

$$F = \{f : P \to K \mid \mathrm{supp}(f) \text{ is finite and } f(0) = 1\}$$

where, as is almost usual, $\text{supp}(f) = \{x \,|\, x > 0, f(x) \neq 0\}$. For $f, g \in F$ and $x \in P$ define addition and circle composition in F as follows:

$$(f + g)(x) = f(x) + g(x)$$

$$(f \circ g)(x) = \sum_{0 \leq y \leq x} f(y)g(x - y) = \sum_{y+z=x} f(y)g(z)$$

when $x \neq 0$ and $(f + g)(0) = 1 = (f \circ g)(0)$. We note that since f and g have finite support then the set

$$X = \{x \,|\, y + z = x, y \in \text{supp}(f) \cup \{0\} \text{ and } z \in \text{supp}(g) \cup \{0\}\}$$

is finite, so that F is closed under circle composition. Finite support is also maintained under addition as required.

By analogy with Section 2.2, we use δ to denote the function $\delta(x) = 0$ for all non-zero $x \in P$ and $\delta(0) = 1$.

Theorem 2.4.1 *The Zassenhaus algebra $(F, +, \circ)$ over a ring with identity, K, is a quasidivision ring (or, equivalently, $(F, +, \cdot)$ is a quasiregular ring).*

Proof: $(F, +)$ is clearly an abelian group. Circle composition (and, hence, multiplication) is associative and it is also easy to see that δ is the identity for $\circ$ and the zero for multiplication. We now show that each $f \in F$ has a $\circ$-inverse $f^{\circ(-1)}(x) \in F$, noting that after setting $f^{\circ(-1)}(0) = 1$ we require the following to hold for non-zero x:

$$0 = \delta(x) = (f \circ f^{\circ(-1)})(x) = f(x) + f^{\circ(-1)}(x) + \sum_{0<y<x} f(y)f^{\circ(-1)}(x - y).$$

For each $f \in F$ define

$$S_f = \{\sum \pm a_i \,|\, a_i \neq 0, a_i \in \text{supp}(f), 0 < \sum \pm a_i \leq c\},$$

where $[0, c]$ is the interval on which the functions in F are defined. This is the set of all sums of elements of $\text{supp}(f)$ with elements allowed to be repeated

in the summations; furthermore, $\mathrm{supp}(f) \subseteq S_f$. As $\mathrm{supp}(f)$ is finite and $[0, c]$ is a finite interval then S_f must be finite, and so we can list its elements in increasing order, viz.:

$$S_f = \{x_1, x_2, \ldots, x_m \,|\, 0 < x_1 < x_2 < \ldots < x_m\}.$$

We note that it may be possible for an element $x_i \in S_f$ to arise from two or more different summations (for example, on the interval $[0, 1]$ if $\mathrm{supp}(f) = \{0.25, 0.5\}$ then $0.5 \in S_f$ arises from $0.25 + 0.25$ as well as 0.5 itself). We also point out that S_f is closed under addition, provided, of course, that the sum stays within $P = [0, c]$.

Given $f \in F$ define $f^{\circ(-1)}$ as follows:

$$f^{\circ(-1)}(x) = \begin{cases} 1 & \text{if } x = 0 \\ 0 & \text{if } x \notin S_f \\ -f(x) - \sum_{0<y<x} f(y) f^{\circ(-1)}(x-y) & \text{if } x \in S_f \end{cases}$$

where we note that the inductive definition for $x \in S_f$ can be determined. We show that $f^{\circ(-1)}$ is entitled to the notation, i.e. that it *is* the quasi-inverse for f. For $x \notin S_f$ we have

$$\begin{aligned} (f \circ f^{\circ(-1)})(x) &= \sum_{0 \le y \le x} f(y) f^{\circ(-1)}(x-y) \\ &= f^{\circ(-1)}(x) + \sum_{0<y\le x, y \in S_f} f(y) f^{\circ(-1)}(x-y) \\ &= 0 + 0 = 0 \end{aligned}$$

because if $y \in S_f$ and $x \notin S_f$ then if $z = x - y \in S_f$ we would have $x = z + y \in S_f$ which is a contradiction, and so $f^{\circ(-1)}(x-y) = 0$. Finally, for $x \in S_f$ we have

$$\begin{aligned} &(f \circ f^{\circ(-1)})(x) \\ &= \sum_{0 \le y \le x} f(y) f^{\circ(-1)}(x-y) \\ &= f(x) + f^{\circ(-1)}(x) + \sum_{0<y<x} f(y) f^{\circ(-1)}(x-y) \end{aligned}$$

$$
\begin{aligned}
&= f(x) - f(x) - \sum_{0<y<x} f(y) f^{\circ(-1)}(x-y) + \sum_{0<y<x} f(y) f^{\circ(-1)}(x-y) \\
&= 0
\end{aligned}
$$

as required. Thus $f^{\circ(-1)}$ can be determined and its support is finite since S_f is finite, whence $f^{\circ(-1)} \in F$ exists as required.

Finally, we observe that if K is commutative then so is F. □

By choosing the underlying ring K to be the set, $\mathbf{Z}$, of integers we show that F can have isomorphic additive and circle composition groups. To do this we shall show that the groups are free. For each real number r in the interval $(0, c]$ let ε_r be that element of F which satisfies the following conditions:

$$
\begin{aligned}
&\varepsilon_r(r) = 1 \\
&\varepsilon_r(0) = 1 \\
&\varepsilon_r(x) = 0 \text{ for all } x \neq r.
\end{aligned}
$$

We will show that the set of all such functions forms a basis for the circle composition group, it being obvious that it does for the additive group. The next three lemmas investigate the way that these basis elements interact with other elements of F and operate on elements of $[0, c]$. We will omit the details concerning the $f(0) = 1$ case.

Lemma 2.4.2 *For $n \in \mathbf{Z}$ we have $\varepsilon_r^{\circ n}(r) = n$ and $\varepsilon_r^{\circ n}(x) = 0$ if x is not an integer multiple of r. Finally, $\varepsilon_r^{\circ n}(kr)$ may be non-zero for $k \in \mathbf{Z}^+$.*

Proof: Note that $\varepsilon_r^{\circ 0}(x) = 0$ for all $x \in (0, c]$ as required. Now let us consider $n > 0$; we shall use induction to prove that $\varepsilon_r^{\circ n}(kr) = \binom{n}{k}$ for $n \geq k$, and $\varepsilon_r^{\circ n}(x) = 0$ for x not a positive integer multiple of r. Setting $n = 2$ we find

$$
\varepsilon_r^{\circ 2}(x) = (\varepsilon_r \circ \varepsilon_r)(x) = \sum_{y+z=x} \varepsilon_r(y)\varepsilon_r(z) = 0
$$

unless $x = r$ or $y = z = r$. In the first case we have $\varepsilon_r^{\circ 2}(r) = \varepsilon_r(r)\varepsilon_r(0) + \varepsilon_r(0)\varepsilon_r(r) = 2 = \binom{2}{1}$; while in the second we have $\varepsilon_r^{\circ 2}(2r) = \varepsilon_r(r)\varepsilon_r(r) = 1 = \binom{2}{2}$.

Assume that the results hold for the $n-1$ case and suppose x is not an integer multiple of r. Then

$$\begin{aligned}
\varepsilon_r^{\circ n}(x) &= (\varepsilon_r \circ \varepsilon_r^{\circ(n-1)})(x) \\
&= \sum_{y+z=x} \varepsilon_r(y)\varepsilon_r^{\circ(n-1)}(z) \\
&= \begin{cases} \varepsilon_r^{\circ(n-1)}(x) & \text{if } x < r \\ \varepsilon_r^{\circ(n-1)}(x) + \varepsilon_r(r)\varepsilon_r^{\circ(n-1)}(x-r) & \text{if } x \geq r \end{cases} \\
&= 0
\end{aligned}$$

by the inductive hypothesis. On the other hand, if $x = kr$ for some $k \in \mathbf{Z}^+$ we find

$$\begin{aligned}
\varepsilon_r^{\circ n}(kr) &= \sum_{y+z=kr} \varepsilon_r(y)\varepsilon_r^{\circ(n-1)}(z) \\
&= \varepsilon_r^{\circ(n-1)}(kr) + \varepsilon_r(r)\varepsilon_r^{\circ(n-1)}((k-1)r) \\
&= \begin{cases} \varepsilon_r^{\circ(n-1)}((k-1)r) & \text{if } k > n-1 \\ \binom{n-1}{k} + 1 \cdot \binom{n-1}{k-1} & \text{if } k \leq n-1 \end{cases} \\
&= \begin{cases} 0 & \text{if } k-1 > n-1 \\ \binom{n-1}{n-1} = \binom{n}{n} & \text{if } k-1 = n-1 \\ \binom{n}{k} & \text{if } k \leq n-1 \end{cases}
\end{aligned}$$

using the inductive hypothesis on several occasions and also the properties of binomial coefficients. We have proved our assertions for positive values of n.

We will not be quite so specific for $-n$ if $n > 0$. From the fact that $0 = \delta(x) = (\varepsilon_r^{\circ n} \circ \varepsilon_r^{\circ(-n)})(x)$ we deduce that for $x = r$ we have $0 = (\varepsilon_r^{\circ n} \circ \varepsilon_r^{\circ(-n)})(r) = \varepsilon_r^{\circ n}(r) + \varepsilon_r^{\circ(-n)}(r) = \binom{n}{1} + \varepsilon_r^{\circ(-n)}(r)$; therefore $\varepsilon_r^{\circ(-n)}(r) = -\binom{n}{1} = -n$. Finally, we know that for $n > 0$ the non-zero values of $\varepsilon_r^{\circ n}$ arise on the integer multiples of r. By the proof of the previous theorem, the inverse, $\varepsilon_r^{\circ(-n)}$, will take its non-zero values on those as well. □

Lemma 2.4.3 *In evaluating $f \circ \varepsilon_r^{\circ n}$ the function $\varepsilon_r^{\circ n}$ only influences those values of $x \in (0, c]$ satisfying $x \geq r$.*

Proof: (i) $(\varepsilon_r^{\circ n} \circ f)(r) = \sum_{y+z=r} \varepsilon_r^{\circ n}(y) f(z) = \varepsilon_r^{\circ n}(r) + f(r) = n + f(r)$ as all other terms vanish by Lemma 2.4.2.

(ii) If $x < r$ then $(\varepsilon_r^{\circ n} \circ f)(x) = \sum_{y+z=x} \varepsilon_r^{\circ n}(y) f(z) = f(x)$, again by the previous lemma.

(iii) If $x > r$ then

$$(\varepsilon_r^{\circ n} \circ f)(x) = \sum_{y \le x} \varepsilon_r^{\circ n}(y) f(x-y) = f(x) + \sum_{i=1}^{k} \varepsilon_r^{\circ n}(ir) f(x-ir)$$

where k is such that $kr \le x$ and $(k+1)r > x$. Observe that if $(x - ir) \notin \mathrm{supp}(f)$ for all $i \in \{0, 1, \ldots, k\}$ then $(\varepsilon_r^{\circ n} \circ f)(x) = 0$. □

Consider a set $\{\varepsilon_{r_1}, \varepsilon_{r_2}, \ldots, \varepsilon_{r_m}\}$ of basis elements. In analogous fashion to the definition of S_f, define $S_{\{r_1, r_2, \ldots, r_m\}}$ to be the set of all possible sums of the $\pm r_i$ with repetitions allowed; that is,

$$S_{\{r_1, r_2, \ldots, r_m\}} = \{\sum \pm r_i \,|\, 0 < \sum \pm r_i \le c, r_i \in \{r_1, \ldots, r_m\}\}.$$

As on page 36 we shall use the symbol $\coprod$ for repeated circle composition.

Lemma 2.4.4 *If $x \notin S_{\{r_1, \ldots, r_m\}}$ then for any $\{n_1, \ldots, n_m\} \subset \mathbf{N}$ we have*

$$(\coprod_{r_i \in \{r_1, \ldots, r_m\}} \varepsilon_{r_i}^{\circ n_i})(x) = 0.$$

Proof: We proceed by induction on the size of $\{r_1, \ldots, r_m\}$.

For $\{r_1\}$ we note that $S_{\{r_1\}} = \{r_1, 2r_1, 3r_1, \ldots\}$ and so Lemma 2.4.2 implies $\varepsilon_{r_1}^{\circ n_1}(x) = 0$.

Suppose now that the result holds for sets of size $(m-1)$. Then

$$\begin{aligned}
(\coprod_{r_i \in \{r_1, \ldots, r_m\}} \varepsilon_{r_i}^{\circ n_i})(x) &= (\varepsilon_{r_1}^{\circ n_1} \circ \coprod_{r_i \in \{r_2, \ldots, r_m\}} \varepsilon_{r_i}^{\circ n_i})(x) \\
&= \sum_{y \le x} \varepsilon_{r_1}^{\circ n_1}(y) (\coprod_{r_i \in \{r_2, \ldots, r_m\}} \varepsilon_{r_i}^{\circ n_i})(x-y) \\
&= \sum_{i=0}^{k} \varepsilon_{r_1}^{\circ n_1}(ir_1) (\coprod_{r_i \in \{r_2, \ldots, r_m\}} \varepsilon_{r_i}^{\circ n_i})(x - ir_1)
\end{aligned}$$

where k is such that $kr < x$ and $(k+1)r > x$. Now $(x - ir_1)$ cannot be in $S_{\{r_2,\ldots,r_m\}}$ since if there was such a $y = x - ir_1 \in S_{\{r_2,\ldots,r_m\}}$ then $x = y + ir_1$ would be an element of $S_{\{r_1,r_2,\ldots,r_m\}}$ which is a contradiction. By the inductive hypothesis $(\coprod_{r_i \in \{r_2,\ldots,r_m\}} \varepsilon_{r_i}^{\circ n_i})(x - ir_1) = 0$ and so $\left(\coprod_{r_i \in \{r_1,\ldots,r_m\}} \varepsilon_{r_i}^{\circ n_i}\right)(x) = 0$ as required. □

Theorem 2.4.5 *The ring, F, constructed as described above with underlying ring $K = \mathbf{Z}$ is in $\mathcal{K}$.*

Proof: We will prove that the set $B = \{\varepsilon_r \,|\, r \in \mathbf{R}\}$ is a basis for $(F, \circ)$; it is clearly a basis for $(F, +)$. Given $f \in F$ recall the definition of

$$\begin{aligned} S_f &= \{\textstyle\sum \pm a_i \,|\, a_i \in \mathrm{supp}(f), 0 < \sum \pm a_i \leq c\} \\ &= \{0 < x_1, \ldots, x_m | x_1 < x_2 < \ldots < x_m\}. \end{aligned}$$

We wish to show that we can determine a finite set of basis elements and a linear combination (with respect to $\circ$) which produce f.

First, we observe that such a set cannot contain ε_x for $x \notin S_f$, since $f(x) = 0$ for such an x, while

$$\left(\varepsilon_x^{\circ n_x} \circ \coprod_{x_i \in S_f} \varepsilon_{x_i}^{\circ n_i}\right)(x) = n_x + \left(\coprod_{x_i \in S_f} \varepsilon_{x_i}^{\circ n_i}\right)(x) = n_x$$

where we have used Lemmas 2.4.2 and 2.4.4 together with the fact that $S_f = S_{\{x_1,\ldots,x_m\}}$. Consequently, if f *is* produced by a set of elements from B then the set is finite and the elements are determined by the elements of S_f.

Secondly, and following on from this, Lemma 2.4.4 above implies that we have $\left(\coprod \varepsilon_{x_i}^{\circ n_i}\right)(x) = 0$ for all values of $x \notin S_{\{x_1,\ldots,x_m\}}$ which means that f and $\left(\coprod \varepsilon_{x_i}^{\circ n_i}\right)$ coincide on those elements x which are not in S_f.

Thirdly, we will show that the values of n_i can be calculated by considering what happens for the elements $x_i \in S_f$, so that $f = \left(\coprod \varepsilon_{x_i}^{\circ n_i}\right)$. We shall proceed

by induction on the subscripts of the x_i. Consider $x_1 = \min(S_f)$. If we choose $n_1 = f(x_1)$ we will have

$$\begin{aligned}
&\left(\coprod_{x_i \in S_f} \varepsilon_{x_i}^{\circ n_i}\right)(x) \\
&= \left(\varepsilon_{x_1}^{\circ f(x_1)} \circ \coprod_{x_i \in S_f \setminus \{x_1\}} \varepsilon_{x_i}^{\circ n_i}\right)(x) \\
&= \begin{cases}
f(x_1) + \left(\coprod_{x_i \in S_f \setminus \{x_1\}} \varepsilon_{x_i}^{\circ n_i}\right)(x_1) & \text{if } x = x_1, \text{ by Lemma 2.4.2 above} \\
\left(\coprod_{x_i \in S_f \setminus \{x_1\}} \varepsilon_{x_i}^{\circ n_i}\right)(x) & \text{if } x < x_1 \\
\left(\coprod_{x_i \in S_f \setminus \{x_1\}} \varepsilon_{x_i}^{\circ n_i}\right)(x) + \sum_{i=1}^{j} \varepsilon_{x_1}^{\circ (f_{x_1})}(ix_1)\left(\coprod_{x_i \in S_f \setminus \{x_1\}} \varepsilon_{x_i}^{\circ n_i}\right)(x - ix_i) & \\
\qquad \text{for } x > x_1
\end{cases} \\
&= \begin{cases}
f(x_1) & \text{if } x = x_1, \text{ by Lemma 2.4.4} \\
0 & \text{if } x < x_1, \text{ by Lemma 2.4.3} \\
\left(\coprod_{x_i \in S_f \setminus \{x_1\}} \varepsilon_{x_i}^{\circ n_i}\right)(x) + \sum_{i=1}^{j} \varepsilon_{x_1}^{\circ (f_{x_1})}(ix_1)\left(\coprod_{x_i \in S_f \setminus \{x_1\}} \varepsilon_{x_i}^{\circ n_i}\right)(x - ix_i) & \\
\qquad \text{for } x > x_1
\end{cases}
\end{aligned}$$

where the third option will be non-zero only when $x \in S_f$.

Suppose that the values of n_i are known for all $i < k$. Lemma 2.4.2 implies that for $x < x_k$ we have

$$\left(\varepsilon_{x_k}^{\circ f(x_k)} \circ \coprod_{x_i \in S_f \setminus \{x_k\}} \varepsilon_{x_i}^{\circ n_i}\right)(x) = \left(\coprod_{x_i \in S_f \setminus \{x_k\}} \varepsilon_{x_i}^{\circ n_i}\right)(x),$$

which is to say that ε_{x_k} has no influence on the function values of elements of $(0, c]$ smaller than x_k. By the same lemma

$$\begin{aligned}
&\left(\varepsilon_{x_k}^{\circ f(x_k)} \circ \coprod_{x_i \in S_f \setminus \{x_k\}} \varepsilon_{x_i}^{\circ n_i}\right)(x_k) \\
&= n_k + \left(\coprod_{x_i \in S_f \setminus \{x_k\}} \varepsilon_{x_i}^{\circ n_i}\right)(x_k) \\
&= n_k + \left(\coprod_{x_i \in \{x_1, \ldots, x_{k-1}\}} \varepsilon_{x_i}^{\circ n_i} \circ \coprod_{x_i \in \{x_{k+1}, \ldots, x_m\}} \varepsilon_{x_i}^{\circ n_i}\right)(x_k) \\
&= n_k + \left(\coprod_{x_i \in \{x_1, \ldots, x_{k-1}\}} \varepsilon_{x_i}^{\circ n_i}\right)(x_k)
\end{aligned}$$

by repeated applications of Lemma 2.4.3, since $x_k < x_{k+1} < \ldots < x_m$. The value of $\left(\coprod_{x_i \in \{x_1,\ldots,x_{k-1}\}} \varepsilon_{x_i}^{\circ n_i}\right)(x_k)$ can be determined by the inductive hypothesis, from which we can deduce that by setting $n_k = f(x_k) - \left(\coprod_{x_i \in \{x_1,\ldots,x_{k-1}\}} \varepsilon_{x_i}^{\circ n_i}\right)(x_k)$ we will have $f(x_k) = (\coprod_{x_i \in S_f} \varepsilon_{x_i}^{\circ n_i})(x_k)$ and the desired result follows. It is clear that the values of n_i are uniquely determined.

Finally, it is also obvious that the basis elements form a linearly independent set, because if we take any non-trivial finite linear combination $\coprod_{\{r_1,\ldots,r_m\}} \varepsilon_{r_i}^{\circ n_i}$ with $r_1 < r_2 < \ldots < r_k$ then $(\coprod \varepsilon_{r_i}^{\circ n_i})(r_1) = n_1 + (\coprod_{\{r_2,\ldots,r_m\}} \varepsilon_{r_i}^{\circ n_i})(r_1)$, by Lemma 2.4.3, which lemma also implies that the last term vanishes, leaving us with $(\coprod \varepsilon_{r_i}^{\circ n_i})(r_1) = n_1 \neq 0$. It is with no small sigh of relief that we place a box at the end of this proof. □

We now consider what happens in the case where the underlying ring is $\mathbf{R}$.

Theorem 2.4.6 *If F is the ring constructed as described in this section with $K = \mathbf{R}$ then $(F, +) \cong (F, \circ)$.*

Proof: Define $L : (F, \circ) \to (F, +)$ so that for $f \in F$ we have $(Lf)(0) = 1$ and $(Lf)(x) = \sum_{0 \leq y \leq x} f(y) f^{\circ(-1)}(x - y)y$, for $x \neq 0$. Note that Lf has finite support and so is in F. This function is similar to that applied around page 22, with $\lambda(x) = x$ and $w(x, y) = x - y$ for $y \leq x$. This function λ satisfies $\lambda(y) + \lambda(w(x, y)) = y + (x - y) = x = \lambda(x)$ as required on those pages. Furthermore, the arguments put forward about L being a logarithm operator apply in this case as well (with 0 being the sole minimal element). All that remains is to prove the analogue of Theorem 2.2.6.

Suppose we have $g \in F$; we wish to find $f \in F$ such that $Lf = g$. Recall the ordered listing of elements of S_g as $S_g = \{x_1 < \ldots < x_m\}$. As usual, define $f(0) = 1$. We must have $f(x) = 0$ for all $x \notin S_g$. To see this, suppose that it is *not* the case. Then, as $\mathrm{supp}(f)$ is finite, there exists a minimal $x' \notin S_g$ such that $f(x') \neq 0$. Then $(Lf)(x') = \sum_{0 < y \leq x'} f(y) f^{\circ(-1)}(x' - y)y = f(x')x' +$

$\sum_{0<y<x'} f(y)f^{\circ(-1)}(x'-y)y = f(x')x' + \sum_{0<y<x',y\in S_g} f(y)f^{\circ(-1)}(x'-y)y$ since $f(y) = 0$ for all $y < x'$ whenever $y \notin S_g$. Suppose that there exists $y' \in S_g$ such that $x'-y'$ is minimal among all the values of $x'-y$ satisfying $f^{\circ(-1)}(x'-y) \neq 0$, and note that such an $x'-y'$ is not in S_g. Then we must have

$$\begin{aligned} 0 &= \delta(x'-y') = (f \circ f^{\circ(-1)})(x'-y') \\ &= \sum_{0\leq k\leq x'-y'} f(k)f^{\circ(-1)}(x'-y'-k) \\ &= \sum_{0\leq k\leq x'-y', k\in S_g} f(k)f^{\circ(-1)}(x'-y'-k) \\ &= f^{\circ(-1)}(x'-y') + f(x'-y') \\ &\qquad + \sum_{0<k<x'-y', k\in S_g} f(k)f^{\circ(-1)}(x'-y'-k) \end{aligned}$$

but, with y' and k both in S_g and x' not, it follows that $x'-y'-k \notin S_g$ and $x'-y'-k < x'-y'$, whence $f^{\circ(-1)}(x'-y'-k) = 0$ by the minimality assumption on $x'-y'$. Thus $\sum_{0<k<x'-y',k\in S_g} f(k)f^{\circ(-1)}(x'-y'-k) = 0$, and therefore $0 = f^{\circ(-1)}(x'-y') + f(x'-y') = f^{\circ(-1)}(x'-y')$ by the minimality assumption on x' (as $y' \in S_g$ implies $x'-y'$ is not in S_g). From this contradiction we see that $(Lf)(x') = f(x')x'$ but then we can never have $Lf = g$ since $g(x') = 0$ (as $x' \notin S_g$). We conclude that we require f to satisfy $f(x) = 0$ for all $x \notin S_g$. Note that, as a result, $S_f \subseteq S_g$.

Let $x_1 = \min\{x \,|\, x \in S_g\}$. Then $(Lf)(x_1) = \sum_{0<y\leq x_1} f(y)f^{\circ(-1)}(x_1-y)y = f(x_1)x_1$ since $f^{\circ(-1)}(x_1-y) = 0$ for all $y < x_1$ because $y \notin S_g \supseteq S_f \supseteq S_{f^{\circ(-1)}}$. Thus we have $(Lf)(x_1) = g(x_1)$ if and only if $f(x_1) = \frac{1}{x_1}g(x_1)$.

Suppose the values of $(Lf)(x_i)$ are known for all $x_i \in \{x_1 < \ldots < x_{k-1}\} \subseteq S_g$ and consider $x_k \in S_g$. Then

$$\begin{aligned} (Lf)(x_k) &= \sum_{0<y\leq x_k} f(y)f^{\circ(-1)}(x_k-y)y \\ &= f(x_k)x_k + \sum_{0<y<x_k} f(y)f^{\circ(-1)}(x_k-y)y \\ &= g(x_k) \end{aligned}$$

when $f(x_k) = \frac{1}{x_k}[g(x_k) - \sum_{0<y<x_k} f(y)f^{\circ(-1)}(x_k - y)y]$ where the terms on the right hand side are known by the inductive hypothesis (noting that once we have values for $f(y)$ for all $y \leq x$ we can determine $f^{\circ(-1)}(x)$; see Theorem 2.4.1).

We now confirm that this function f satisfies $Lf = g$. If $x \notin S_g$ then $(Lf)(x) = \sum_{0<y\leq x} f(y)f^{\circ(-1)}(x-y)y = \sum_{0<y<x, y\in S_g} f(y)f^{\circ(-1)}(x-y)y$. Now $x - y \notin S_g$ (otherwise $x \in S_g$) and so, since $S_{f^{\circ(-1)}} \subseteq S_f \subseteq S_g$, $f^{\circ(-1)}(x-y) = 0$. Therefore $(Lf)(x) = 0 = g(x)$ as required. Furthermore,

$$\begin{aligned}
&(Lf)(x_k) \\
&= \sum_{0<y\leq x_k} f(y)f^{\circ(-1)}(x_k - y)y \\
&= f(x_k)x_k + \sum_{0<y<x_k} f(y)f^{\circ(-1)}(x_k - y)y \\
&= \{\frac{1}{x_k}[g(x_k) - \sum_{0<y<x_k} f(y)f^{\circ(-1)}(x_k - y)y]\}x_k \\
&\qquad + \sum_{0<y<x_k} f(y)f^{\circ(-1)}(x_k - y)y \\
&= [g(x_k) - \sum_{0<y<x_k} f(y)f^{\circ(-1)}(x_k - y)y] + \sum_{0<y<x_k} f(y)f^{\circ(-1)}(x_k - y)y \\
&= g(x_k).
\end{aligned}$$

Thus L is a bijection, and so $F \in \mathcal{K}$. □

Later in the thesis Theorem 7.1.8 will show that all commutative nil algebras are in $\mathcal{K}$, which will subsume the above result: the Zassenhaus algebra is commutative and we will show that it is nil in Section 3.4. However, here we have been able to obtain an *explicit* isomorphism between the additive and circle composition groups.

The ring properties of the Zassenhaus algebra are discussed further in Section 3.4.

Chapter 3

Nil and nilpotent rings in $\mathcal{K}$

As has been mentioned earlier in this thesis, zero rings are trivially in $\mathcal{K}$ because their additive and isomorphic groups correspond. The nature of the relationship between the three operations of addition, circle composition and multiplication — namely, $a \circ b = a + b + ab$ — would seem to suggest that should a ring have isomorphic additive and circle composition groups then the multiplication on the ring is, perhaps, not far removed from being trivial, so that perhaps the ring is nilpotent or nil at worst. This need not be the case. The purpose of this chapter is to consider examples of rings which are in $\mathcal{K}$ to show that they can be nilpotent (without merely being a zero ring), nil but not nilpotent, or quasiregular but not nil (including an example which has no zero divisors whatsoever). Thus, having isomorphic additive and circle composition groups does not necessarily give any additional information about the ring besides quasiregularity. Some of our examples arise from the quasifield constructions of [22], [18] and Section 2.2.

Before we look at these examples, we establish an important result concerning rings which are algebras over $\mathbf{Z}_p$, and then consider the behaviour of multiplication in quasi-division rings.

3.1 Algebras over $\mathbf{Z}_p$

The result of this section gives a characterization of those algebras over $\mathbf{Z}_p$ (p prime) which are in $\mathcal{K}$. This will be used extensively in this chapter. Later, in Chapter 7, we will obtain results about algebras over the *rationals* and circumstances in which they are in $\mathcal{K}$.

Theorem 3.1.1 *If R is a commutative ring which is an algebra over $\mathbf{Z}_p$ where p is prime then $(R,+) \cong (R,\circ)$ if and only if $r^p = 0$ for all r in $(R,+,\cdot)$.*

Proof: "Only if": Suppose $(R,+) \cong (R,\circ)$. Then there exists an isomorphism L such that $L(r \circ s) = L(r) + L(s)$ for $r,s \in R$. In particular, we have $L(r^{\circ p}) = pL(r)$. Now since R is a $\mathbf{Z}_p$-algebra then $pL(r) = 0$, so that $r^{\circ p} = 0$. But $r^{\circ p} = \sum_{i=1}^{p} \binom{p}{i} r^i = \sum_{i=1}^{p-1} \binom{p}{i} r^i + r^p$, and therefore $0 = \sum_{i=1}^{p-1} \binom{p}{i} r^i + r^p$. But $p|\binom{p}{i}$ for all $i \neq 0, p$ since p is a prime, so that $\sum_{i=1}^{p-1} \binom{p}{i} r^i = 0$ (again since the underlying ring has characteristic p). Consequently $r^p = 0$.

"If": Conversely, suppose that $(R,+,\cdot)$ is commutative and satisfies $r^p = 0$ for all $r \in R$. Then R is nil and hence quasiregular, so $(R,\circ)$ is an abelian group. Furthermore, as R is an algebra over $\mathbf{Z}_p$, $r^{\circ p} = \sum_{i=1}^{p-1} \binom{p}{i} r^i + r^p = r^p = 0$, so that either r has order p or $r^{\circ k} = 0$ for some $k|p$. However, the only value of k satisfying this is $k = 1$ and $r^{\circ 1} = 0$ if and only if $r = 0$, whence $r \neq 0$ has order p in the group $(R,\circ)$. Then $(R,\circ)$ is a $\mathbf{Z}_p$-vector space, and is thus the direct sum of n copies of $\mathbf{Z}_p$, where n is the dimension of the vector space. Further, $(R,+)$ is also a $\mathbf{Z}_p$-vector space, and, as $|(R,\circ)| = |(R,+)|$, it must have the same dimension. Hence there exists an isomorphism (a vector space isomorphism) between $(R,\circ)$ and $(R,+)$. □

3.2 Products in quasifields

In order to develop some of the results in the later sections of this chapter we need to consider what happens under repeated multiplication of elements in a quasi-division ring. In what follows F denotes a quasi-division ring defined on a poset P with underlying ring K, constructed as described in Section 2.2. Since multiplication can be obtained from the operations $+$ and $\circ$ on a quasi-division ring via $f \cdot g = f \circ g - (f + g)$ then for the particular class of quasi-division rings already discussed, the multiplication is given by $(f \cdot g)(e) = 1$ for $e \in \text{Min}(P)$ and $(f \cdot g)(x) = (f \circ g)(x) - f(x) - g(x) = \sum_{y \leq x} f(y)g(w(x,y)) - f(x) - g(x) = \sum_{e_x < y < x} f(y)g(w(x,y))$ otherwise.

Lemma 3.2.1 *If $f_1, f_2, \ldots, f_{n+1} \in F$ for F a quasi-division ring then*

$$(f_1 f_2 \cdots f_{n+1})(x) = 0$$

for all $x \in P$ such that $0 < h(x) \leq n$.

Proof: We will prove this result by induction on n. First, suppose that $n = 1$ so that $x \in P$ must satisfy $h(x) = 1$ (which means x covers e_x; i.e. x is an atom). Then

$$\begin{aligned}
(f_1 f_2)(x) &= (f_1 \circ f_2)(x) - f_1(x) - f_2(x) \\
&= \sum_{y \leq x} f_1(y) f_2(w(x,y)) - f_1(x) - f_2(x) \\
&= f_1(e_x) f_2(w(x,e_x)) + f_1(x) f_2(w(x,x)) - f_1(x) - f_2(x) \\
&= f_2(x) + f_1(x) - f_1(x) - f_2(x) = 0.
\end{aligned}$$

Now suppose the result is true for $n \leq k$, that x is such that $h(x) \leq k+1$, with $f_1, f_2, \ldots f_{k+2} \in F$. We have

$$\begin{aligned}
(f_1 f_2 \cdots f_{k+1} f_{k+2})(x) &= ((f_1 f_2 \cdots f_{k+1}) f_{k+2})(x) \\
&= \sum_{e_x < y < x} (f_1 f_2 \cdots f_{k+1})(y) f_{k+2}(w(x,y)).
\end{aligned}$$

Now since $y < x$ we have $h(y) < h(x) \leq k+1$, so that by the inductive hypothesis $(f_1 f_2 \cdots f_{k+1})(y) = 0$, and hence $(f_1 f_2 \cdots f_{k+1} f_{k+2})(x) = 0$ as required. □

Corollary 3.2.2 *If F is a quasi-division ring and $f \in F$ then $f^n(x) = 0$ for all x satisfying $h(x) < n$.* □

Corollary 3.2.3 *If x covers e_x then $(fg)(x) = 0$ for all $f, g \in F$.* □

Theorem 3.2.4 *If P is a poset with $h(P) = n$ then the ring associated with the quasi-division ring on P is nilpotent of index $n+1$.*

Proof: If $h(P) = n$ then by Lemma 3.2.1 we have $(f_1 \cdots f_{n+1})(x) = 0$ for any $x \in P\,(x \notin \mathrm{Min}(P))$ and any $f_1, \ldots, f_{n+1} \in F$. Furthermore, $(f_1 \cdots f_{n+1})(e) = 1$ for any $e \in \mathrm{Min}(P)$, so that $f_1 \cdots f_{n+1} = \delta$ for any $f_1, \ldots, f_{n+1} \in F$. Thus $F^{n+1} = \{\delta\}$, whence F is nilpotent. □

Corollary 3.2.5 *If p is a prime and F is a quasifield over $\mathbf{Z}_p$ with $h(P) < p$ then $(F, +) \cong (F, \circ)$.*

Proof: As $h(P) < p$ then by the above Theorem $F^p = \{\delta\}$ and the result follows by Theorem 3.1.1. □

We will now consider various examples of rings to determine what, if anything, being in $\mathcal{K}$ can tell us about the multiplication of a ring. Recall that we denote the height of the poset by $h(P)$ in the case that it is finite.

3.3 Non-trivial nilpotent rings in $\mathcal{K}$

We begin our selection of examples by repeating the observation that zero rings — which satisfy $R^2 = \{0\}$ and have identical additive and circle composition

groups — are nilpotent and in $\mathcal{K}$. Less trivial nilpotent examples come by considering suitable quasifields, F, constructed on posets having finite height in such a way that they are in $\mathcal{K}$. If the height of the poset is n then Theorem 3.2.4 states that $F^{n+1} = \{0\}$. Such examples exist: for instance, choose the underlying ring to be an algebra over $\mathbf{Z}_p$ and take a suitable poset, P, whose height is less than p. The resulting quasifield is nilpotent because of the aforementioned theorem and hence satisfies $a^p = 0$ for all $a \in F$. It is thus a ring in $\mathcal{K}$ by Theorem 3.1.1.

Moreover, we can have rings in $\mathcal{K}$ which are algebras over $\mathbf{Z}_p$ and thus have $a^p = 0$ for all a, but which have an arbitrarily large index of nilpotence. To see this, consider the quasifield constructed on the set of subsets of a finite set with underlying ring $\mathbf{Z}_p$. As we shall see in Theorem 3.4.3 this ring is in $\mathcal{K}$ because we have $f^p = 0$; however the arguments in the proof of Theorem 3.4.4 guarantee that if the poset is of height n then we will need $k = n + 1$ in order to obtain $F^k = \{0\}$.

We also have the family of rings described in Section 2.3, which are constructed on finite posets (whose finite height implies they are nilpotent by Theorem 3.2.4) but whose underlying ring is the integers, $\mathbf{Z}$. That these rings have isomorphic additive and circle composition groups was shown in Theorem 2.3.4. Here the index of nilpotence for a given element will vary up to the value of the height of the poset. To see this, consider an appropriate variation of Lemma 3.5.2.

3.4 Examples of rings in $\mathcal{K}$ which are nil but not nilpotent

Theorem 3.4.1 *There exist rings of prime characteristic in $\mathcal{K}$ which are nil*

but not nilpotent.

Proof: Let R be a ring satisfying $x^2 = 0$ and $2x = 0$. It is a well-known exercise to show that R is commutative; while $x^2 = 0$ implies R is nil and hence quasiregular. Such a ring is an algebra over $\mathbf{Z}_2$, and so, by Theorem 3.1.1 we have $R \in \mathcal{K}$. Now R is nil, but Duncan and Macdonald in [12] have constructed examples of such rings in which each element is factorable: that is, given $x \in R$ there exist $y, z \in R$ such that $x = yz$ so that any element of R can be written as a product of arbitrary length. Thus R is not nilpotent. □

To obtain another representative of a class of examples we will construct a quasifield on the set, $\mathcal{S}$, of finite subsets of an infinite set, S, using $\mathbf{Z}_p$ as the underlying ring. For results 3.4.2 to 3.4.4 below let F denote the quasifield constructed in such a manner. For a given set A, by *partition* we mean a *set* of disjoint subsets whose union is A. We need the following result, which is Theorem 3.3 of [22].

Lemma 3.4.2 *If $f \in F$ then $f^n(A) = n! \sum f(S_1)f(S_2)\dots f(S_n)$, where the sum is over all partitions of A into n non-empty disjoint subsets, $S_1, \dots, S_n$.* □

Theorem 3.4.3 *If F is the quasifield constructed on the poset of subsets of a set S, with underlying ring $\mathbf{Z}_p$, then F is in $\mathcal{K}$ (and hence nil).*

Proof: From Lemma 3.4.2 we have $f^p(A) = p! \sum f(S_1)f(S_2)\dots f(S_p)$ and since the underlying ring is $\mathbf{Z}_p$ we must have $f^p(A) = 0$ for all non-empty A in the poset. Thus $f^p = \delta$. By Theorem 3.1.1 we have $F \in \mathcal{K}$. □

In fact the above theorem applies to the poset of subsets of *any* set, not just an infinite one. In the following result, however, we need an *infinite* set, since using a finite set causes the resulting poset to have finite height, forcing the constructed quasifield to be nilpotent by Theorem 3.2.4.

Theorem 3.4.4 *There exist quasifields in $\mathcal{K}$ which are nil but not nilpotent.*

Proof: As seen in Theorem 3.4.3, the quasifield F on the poset of subsets with underlying ring $\mathbf{Z}_p$ is nil and in $\mathcal{K}$. We now show that F is not nilpotent. To do this we will use induction to show that for any $n \in \mathbf{N}$ we can find $f_1, f_2, \ldots, f_n$ such that $f_1 f_2 \ldots f_n \neq \delta$. In particular, our approach will be to show that we can always ensure that $(f_1 f_2 \ldots f_n)(A) \neq 0$ for some $A \in \mathcal{S}$ such that $|A| = n$.

Since $F \neq \{\delta\}$ we must have the existence of $f \neq \delta$ so that the $n = 1$ case is true. Suppose there exists $A \in \mathcal{S}$ with $|A| = k$ such that $(f_1 f_2 \ldots f_k)(A) \neq 0$. Write $A = \{a_1, a_2, \ldots, a_k\}$. Now consider $A' = \{a_1, a_2, \ldots, a_k, a_{k+1}\}$. We wish to prove that we can find $f_{k+1} \in F$ such that $(f_1 f_2 \ldots f_k f_{k+1})(A') \neq 0$. Recalling that for the poset of subsets we have $h(A) = |A| = k$ and, by Lemma 3.2.1, that $(f_1 f_2 \ldots f_k)(B) = 0$ for all $\emptyset \neq B \subset A$. Consequently

$$\begin{aligned}
&(f_1 f_2 \ldots f_k f_{k+1})(A') \\
&= \sum_{\emptyset \neq B \subset A} (f_1 f_2 \ldots f_k)(B) f_{k+1}(A' \backslash B) \\
&= \sum_{i=1}^{k+1} (f_1 f_2 \ldots f_k)(A' \backslash \{a_i\}) f_{k+1}(\{a_i\}) \\
&= (f_1 f_2 \ldots f_k)(A) f_{k+1}(\{a_{k+1}\}) + \sum_{i=1}^{k} (f_1 f_2 \ldots f_k)(A' \backslash \{a_i\}) f_{k+1}(\{a_i\}).
\end{aligned}$$

Since, by the inductive hypothesis, we have $(f_1 f_2 \ldots f_k)(A) \neq 0$ we can choose f_{k+1} from functions in F having, say, $f_{k+1}(\{a_{k+1}\}) = 1$ and $f_{k+1}(\{a_i\}) = 0$ for all $i \neq k+1$. Clearly such a function exists and it will ensure that $(f_1 f_2 \ldots f_k f_{k+1})(A') \neq 0$ whence $f_1 f_2 \ldots f_k f_{k+1} \neq \delta$. The non-nilpotence of F follows. In fact, we can see that F is not even T-nilpotent since for the sequence $\langle f_1, f_2, \ldots, f_n, \ldots \rangle$ just constructed there is no k such that $f_1 f_2 \ldots f_k = \delta$. $\square$

In the above example the elements have index of nilpotence p. We conclude this section by considering two examples of rings which are nil but not nilpotent,

where the elements have *unbounded* index of nilpotence. One of the examples is T-nilpotent and the other is not.

Recall the ring — the Zassenhaus algebra over K — constructed in Section 2.4, in which, for a positive real number c, P denotes the real interval $[0, c]$ with the usual ordering $\leq$, K is a ring with identity and and our ring is the set of functions

$$F = \{f : P \to K \,|\, \text{supp}(f) \text{ is finite and } f(0) = 1\}$$

where addition is defined point-wise and circle composition is defined by the usual convolution. For each $f \in F$ define

$$\begin{aligned} S_f &= \{\textstyle\sum \pm a_i \,|\, a_i \neq 0, a_i \in \text{supp}(f), \sum \pm a_i \leq c\} \\ &= \{x_1, x_2, \ldots, x_m \,|\, 0 < x_1 < x_2 < \ldots < x_m\}. \end{aligned}$$

For $f, g \in F$ observe that for non-zero $x \in [0, c]$ we have

$$(fg)(x) = (f \circ g - f - g)(x) = \sum_{0<y<x} f(y)g(x-y).$$

Note that Divinsky ([11], Example 3, page 19) has proved the result we require — that the ring is nil but not nilpotent — but we present the proofs for completeness and use the notation which shows the connection with quasifields.

Lemma 3.4.5 *If $x \notin S_f \cup \{0\}$ then $f^n(x) = 0$ for all $n \in \mathbf{N}$.*

Proof: Once again induction comes to the fore, the $n = 1$ case being trivial. Suppose the result holds for $k = n - 1$; then

$$f^n(x) = (ff^{n-1})(x) = \sum_{0<y<x} f(y)f^{n-1}(x-y) = \sum_{0<y<x, y\in\text{supp}(f)} f(y)f^{n-1}(x-y)$$

since all other values of $f(y)$ are zero. Now $x - y \notin S_f$ since y is and x isn't, and the inductive hypothesis then implies $f^{n-1}(x - y) = 0$ whence $f^n(x) = 0$ as required. □

Lemma 3.4.6 *If $k \in \mathbf{N}$ then $f^k(x_i) = 0$ for all $i < k, x_i \in S_f$.*

Proof: We shall proceed by induction on k. With $k = 2$ we have $f^2(x_1) = \sum_{0<y<x_1} f(y)f(x_1 - y) = 0$ since there are no values of $y \in \text{supp}(f)$ satisfying $y < x_1$. Now suppose that $f^{k-1}(x_i) = 0$ for all $i < k - 1$ and consider f^k. For $i < k$ we have $f^k(x_i) = \sum_{0<y<x_i} f(y)f^{k-1}(x_i - y)$ where, as in the previous lemma, we can assume that $y \in \text{supp}(x)$. This in turn implies that $x_i - y \in S_f$ and, moreover, if $x_i - y = x_j$ then $x_j < x_i$ so $j < i < k$ and thus $j < k - 1$. We can apply the inductive hypothesis to conclude that $f^{k-1}(x_i - y) = 0$ for all $i < k$, and the result follows. □

Corollary 3.4.7 *The Zassenhaus algebra, F, over a ring with identity is nil.*

Proof: If $S_f = \{x_1, \ldots, x_m\}$ then by the previous lemmas $f^{m+1}(x) = 0$ for all $x \in (0, c]$, so $f^{m+1} = \delta$. □

Theorem 3.4.8 *The Zassenhaus algebra, F, over a ring with identity is nil but not nilpotent. Furthermore, elements have unbounded index of nilpotence and the ring is not T-nilpotent.*

Proof: We show that for any $n \in \mathbf{N}$ we can find $f \in F$ such that $f^n \neq \delta$. Remembering that the interval on which our functions are defined is $[0, c]$, and using notation similar to that employed in Section 2.3 consider the function $f = \varepsilon_{\frac{c}{n}} \in F$ satisfying

$$\varepsilon_{\frac{c}{n}}(x) = \begin{cases} 1 & \text{for } x = 0 \\ 1 & \text{for } x = \frac{c}{n} \\ 0 & \text{otherwise.} \end{cases}$$

We will show that $\varepsilon^n_{\frac{c}{n}}(c) = 1$ and hence $\varepsilon^n_{\frac{c}{n}} \neq \delta$, by showing that $\varepsilon^k_{\frac{c}{n}}(\frac{kc}{n}) = 1$ for all $k \in \mathbf{N}$. Not surprisingly we use induction, with the $k = 1$ case being trivial. Now $\varepsilon^k_{\frac{c}{n}}(\frac{kc}{n}) = \sum_{0<y<\frac{kc}{n}} \varepsilon_{\frac{c}{n}}(y)\varepsilon^{k-1}_{\frac{c}{n}}(\frac{kc}{n} - y) = \varepsilon_{\frac{c}{n}}(\frac{c}{n})\varepsilon^{k-1}_{\frac{c}{n}}(\frac{(k-1)c}{n}) = 1 \times 1 = 1$ if we assume that the $k - 1$ case holds. The desired result follows, and we conclude

that there exists no $n \in \mathbf{N}$ such that $F^n = \{0\}$ even though, by the previous corollary, F is nil. Moreover, F is not T-nilpotent (consider, for example, the sequence $\langle \varepsilon_{\frac{1}{2}}, \varepsilon_{\frac{1}{4}}, \ldots, \varepsilon_{\frac{1}{2^n}}, \ldots \rangle$). □

If we take the underlying ring to be $K = \mathbf{Z}$ or $\mathbf{R}$ (using the results of Section 2.4) then we know that $F \in \mathcal{K}$ and so we have another example of a ring in $\mathcal{K}$ which is nil but not nilpotent. In this case, however, the elements of F have unbounded index of nilpotence. This contrasts with the example of Theorem 3.4.4 in which all the elements are nilpotent of index p. Using the results of Theorem 7.1.8 we can also allow K to be an algebra over the rationals.

For our final example in this section we need a couple of results which will not be proved until later in the thesis.

Example 3.4.9 *There is a nil ring in $\mathcal{K}$ whose elements have unbounded index of nilpotence, and which is T-nilpotent.*

Proof: For each prime p let R_p denote a finite ring in $\mathcal{K}$ which is an algebra over $\mathbf{Z}_p$. There exists a non-trivial example of such a ring for each p as a consequence of our results in Section 5.2. Recall that if $R_p \in \mathcal{K}$ then Theorem 3.1.1 implies that $x^p = 0$ for $x \in R_p$. In addition, each ring is nilpotent because it is finite and quasiregular.

Suppose $x \in \bigoplus_{p \text{ prime}} R_p$ and that $q = \max\{p \,|\, p \in \text{supp}(x)\}$. Then $x^q = 0$ since $(x)_p^p = 0$ for each component, $(x)_p$, of x by Theorem 3.1.1. Since $\mathcal{K}$ is closed under direct sums (which will be proved in Theorem 4.3.1) we know that $\bigoplus_{p \text{ prime}} R_p \in \mathcal{K}$; however this ring is clearly not nilpotent because the value of q required in order to obtain $x^q = 0$ can be arbitrarily large. This gives us another example of a ring which is nil but not nilpotent, with the elements having unbounded index of nilpotence.

To prove that the ring is T-nilpotent, consider a sequence of elements of $\bigoplus_{p \text{ prime}} R_p$; say, $\langle x_1, x_2, x_3, \ldots \rangle$. Now since $\text{supp}(x_i)$ is finite for all x_i it follows

that $\bigcap_{i\in\mathbf{N}} \mathrm{supp}(x_i)$ is finite. If $\bigcap_{i\in\mathbf{N}} \mathrm{supp}(x_i) = \emptyset$ then choose the minimum value of k such that $\bigcap_{i\leq k} \mathrm{supp}(x_i) = \emptyset$; it is then obvious that $x_1x_2\cdots x_k = 0$ since no p-component is everywhere non-zero on $\{x_1, x_2, \ldots, x_k\}$. On the other hand, if $\bigcap_{i\in\mathbf{N}} \mathrm{supp}(x_i) \neq \emptyset$ then let

$$N = \max_{p\in\bigcap_{i\in\mathbf{N}} \mathrm{supp}(x_i)} \{n_p \mid R_p^{n_p} = 0\}$$

so that N is the largest index of nilpotence for rings contributing to the support of the sequence. Then $x_1x_2\cdots x_N = 0$. □

3.5 Examples of rings in $\mathcal{K}$ which are not nil

In this section we will present two examples of quasifields which demonstrate that rings in $\mathcal{K}$ may not be nil, and may, in fact, have no zero divisors.

In what follows let F denote the quasifield constructed as a Cauchy convolution on the set of whole numbers ordered by $\leq$ (we shall call this the *complete* Cauchy convolution; it is possible to obtain variants by restricting the poset). For the Cauchy convolution if $y \leq x$ then $w(x, y) = x - y$. We first prove the following lemma and corollary; the corollary will be important here, while the lemma will be required in a later section to prove Theorem 7.1.12.

Lemma 3.5.1 *In the complete Cauchy convolution quasifield, F, given $f \in F$ let k be the smallest natural number such that $f(k) \neq 0$. Then for $k, r \in \mathbf{N}$ we have $f^n(nk) = (f(k))^n$, and $f^n(r) = 0$ for $0 < r < nk$.*

Proof: We shall prove this by induction on n, with the $n = 1$ case being trivial. Assume that $f^n(nk) = (f(k))^n$ and that $f^n(r) = 0$ for $0 < r < nk$; then $f^{n+1}((n+1)k) = (ff^n)((n+1)k) = \sum_{1\leq m<(n+1)k} f(m)f^n((n+1)k - m) = \sum_{1\leq m\leq k} f(m)f^n((n+1)k - m)$ because if $m > k$ then $(n+1)k - m < nk$ and

so, by the inductive hypothesis $f^n((n+1)k-m)=0$. Thus

$$\begin{aligned} f^{n+1}((n+1)k) &= f(k)f^n((n+1)k-k)+\sum_{1\le m<k} f(m)f^n((n+1)k-m) \\ &= f(k)f^n(nk)=(f(k))^{n+1} \end{aligned}$$

since $f(m)=0$ for $m<k$ and from the inductive assumption. Furthermore, if $s<(n+1)k$ we have

$$\begin{aligned} f^{n+1}(s) &= (ff^n)(s)=\sum_{1\le m<s} f(m)f^n(s-m) \\ &= \sum_{k\le m<s} f(m)f^n(s-m)=0 \end{aligned}$$

since $f(m)=0$ for $m<k$ and when $m\ge k$ we have $s-m<(n+1)k-m<nk$ and so the inductive assumption can be applied. □

Corollary 3.5.2 *If $f\in F$ and $f(1)\neq 0$ then $f^n(n)=(f(1))^n$.* □

Theorem 3.5.3 *If F is the complete Cauchy convolution quasifield then F is not nil.*

Proof: Choose $f\in F$ such that $f(1)=1$ (since our construction requires that the underlying ring has an identity). Then, by Corollary 3.5.2 we have $f^n(n)=(f(1))^n=1$ whence $f^n\neq\delta$. The result follows. □

For suitable choices of the underlying ring (for example, an algebra over the rationals; see Section 2.2) it can be shown that there exist complete Cauchy convolution rings which are in $\mathcal{K}$, giving our first example of a ring in $\mathcal{K}$ which is not nil. In fact, this ring has no zero divisors.

Example 3.5.4 *The quasifield formed using the Cauchy convolution on the set of whole numbers has no zero divisors when the underlying ring is an integral domain.*

Proof: Suppose $fg = \delta$ and that, without loss of generality, $g \neq \delta$. We prove $f = \delta$ inductively, by proving $f(n) = 0$ for all $n \in \mathbf{N}$. Since $g \neq \delta$, let $N = \min\{n \in \mathbf{N} | g(n) \neq 0\}$. Then, since $fg = \delta$ we have

$$\begin{aligned} 0 &= (fg)(N+1) \\ &= f(1)g(N) + f(2)g(N-1) + ... + f(N-1)g(2) + f(N)g(1) \\ &= f(1)g(N), \end{aligned}$$

as $g(i) = 0$ for all $i < N$, and thus $f(1) = 0$ (since $g(N) \neq 0$, and the underlying ring has no zero divisors). Now suppose $f(n) = 0$ for all $n \leq k$, and consider

$$\begin{aligned} 0 &= (fg)(N+k+1) \\ &= f(1)g(N+k) + ... + f(k)g(N+1) + f(k+1)g(N) + \\ &\qquad f(k+2)g(N-1) + ... + f(N+k)g(1) \\ &= f(k+1)g(N) \end{aligned}$$

by the inductive hypothesis and the nature of g. Therefore $f(k+1) = 0$, and hence $f = \delta$ by induction. □

The Cauchy convolution quasifield is not the only example of a ring in $\mathcal{K}$ which is not nil. Let F now denote the quasifield formed using the Dirichlet convolution: here the poset P is the set of natural numbers ordered by divisibility. Bearing in mind that we will sometimes restrict this poset for further investigation we shall call this F the *complete* Dirichlet convolution. If $x \in P$ with $x = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_k^{\alpha_k}$ being the prime factorization of x, then the height of x is given by $h(x) = \alpha_1 + \alpha_2 + \dots + \alpha_k$. Further, if $y|x$ then $w(x, y) = x/y$.

First we give a result concerning powers of $f \in F$.

Lemma 3.5.5 *Suppose F is a Dirichlet convolution quasifield over a commutative ring with identity. If the prime factorization of x is given by $x =$*

$p_1^{\alpha_1}p_2^{\alpha_2}\ldots p_k^{\alpha_k}$ *and we write* $n = h(x) = \alpha_1 + \alpha_2 + \ldots + \alpha_k$ *then*

$$f^n(x) = \frac{n!}{\alpha_1!\alpha_2!\ldots\alpha_k!}(f(p_1))^{\alpha_1}(f(p_2))^{\alpha_2}\ldots(f(p_k))^{\alpha_k}.$$

Proof: We prove this by induction on n, the height of elements of P. If $n = 1$ then x must be a prime, so that $x = p$ for some p, and the result holds. Suppose the result holds for all $x \in P$ such that $h(x) = n$ and consider x such that $h(x) = n + 1$. Such an x has an extra prime factor compared with those elements of height n. Now suppose $y|x$ with $y = p_1^{\alpha_1}p_2^{\alpha_2}\ldots p_k^{\alpha_k}$ so that $h(y) = n$. Then there are two possibilities for this extra factor: either it is a repeat of a factor which already appears, so that, without loss of generality, $x = p_1^{\alpha_1+1}p_2^{\alpha_2}\ldots p_k^{\alpha_k}$; or it is different from those already present, giving $x = p_1^{\alpha_1}p_2^{\alpha_2}\ldots p_k^{\alpha_k}p_{k+1}$. In what follows, by $y|^*x$ we mean that y is a proper divisor of x.

Case 1: If $x = p_1^{\alpha_1+1}p_2^{\alpha_2}\ldots p_k^{\alpha_k}$ we have

$$\begin{aligned}
f^{n+1}(x) &= f^{n+1}(p_1^{\alpha_1+1}p_2^{\alpha_2}\ldots p_k^{\alpha_k}) \\
&= (ff^n)(p_1^{\alpha_1+1}p_2^{\alpha_2}\ldots p_k^{\alpha_k}) = \sum_{y|^*x} f(y)f^n(x/y) \\
&= f(p_1)f^n(p_1^{\alpha_1}p_2^{\alpha_2}\ldots p_k^{\alpha_k}) + f(p_2)f^n(p_1^{\alpha_1+1}p_2^{\alpha_2-1}\ldots p_k^{\alpha_k}) \\
&\quad + \ldots + f(p_k)f^n(p_1^{\alpha_1+1}p_2^{\alpha_2}\ldots p_k^{\alpha_k-1})
\end{aligned}$$

since all the other f^n terms will vanish because the height of the elements on which they act are less than n. Then, by the inductive hypothesis we have

$$\begin{aligned}
&f^{n+1}(x) \\
&= f(p_1)(\frac{n!}{\alpha_1!\alpha_2!\ldots\alpha_k!}(f(p_1))^{\alpha_1}(f(p_2))^{\alpha_2}\ldots(f(p_k))^{\alpha_k}) \\
&\quad + f(p_2)(\frac{n!}{(\alpha_1+1)!(\alpha_2-1)!\ldots\alpha_k!}(f(p_1))^{\alpha_1+1}(f(p_2))^{\alpha_2-1}\ldots(f(p_k))^{\alpha_k}) \\
&\quad + \ldots \\
&\quad + f(p_k)(\frac{n!}{(\alpha_1+1)!\alpha_2!\ldots(\alpha_k-1)!}(f(p_1))^{\alpha_1+1}(f(p_2))^{\alpha_2}\ldots(f(p_k))^{\alpha_k-1})
\end{aligned}$$

$$
\begin{aligned}
&= (f(p_1))^{\alpha_1+1}(f(p_2))^{\alpha_2}\ldots(f(p_k))^{\alpha_k} \\
&\quad \times\Big(\frac{n!}{\alpha_1!\alpha_2!\ldots\alpha_k!}+\frac{n!}{(\alpha_1+1)!(\alpha_2-1)!\ldots\alpha_k!} \\
&\quad\quad +\ldots+\frac{n!}{(\alpha_1+1)!\alpha_2!\ldots(\alpha_k-1)!}\Big) \\
&= (f(p_1))^{\alpha_1+1}(f(p_2))^{\alpha_2}\ldots(f(p_k))^{\alpha_k}\frac{n!}{\alpha_1!(\alpha_2-1)!\ldots(\alpha_k-1)!} \\
&\quad \times\Big(\frac{1}{\alpha_2\alpha_3\ldots\alpha_k}+\frac{1}{(\alpha_1+1)\alpha_3\ldots\alpha_k}+\ldots+\frac{1}{(\alpha_1+1)\alpha_2\ldots\alpha_{k-1}}\Big) \\
&= (f(p_1))^{\alpha_1+1}(f(p_2))^{\alpha_2}\ldots(f(p_k))^{\alpha_k}\frac{n!}{\alpha_1!(\alpha_2-1)!\ldots(\alpha_k-1)!} \\
&\quad \times\frac{(\alpha_1+1)+\alpha_2+\ldots+\alpha_k}{(\alpha_1+1)\alpha_2\ldots\alpha_k} \\
&= (f(p_1))^{\alpha_1+1}(f(p_2))^{\alpha_2}\ldots(f(p_k))^{\alpha_k}\frac{(n+1)!}{(\alpha_1+1)!\alpha_2!\ldots\alpha_k!}
\end{aligned}
$$

as required, since $(\alpha_1+1)+\alpha_2+\ldots+\alpha_k = n+1$.

Case 2: If $x = p_1^{\alpha_1}p_2^{\alpha_2}\ldots p_k^{\alpha_k}p_{k+1}$ then using arguments similar to those applied in Case 1 we have

$$
\begin{aligned}
&f^{n+1}(x) \\
&= f(p_1)f^n(p_1^{\alpha_1-1}p_2^{\alpha_2}\ldots p_k^{\alpha_k}p_{k+1})+f(p_2)f^n(p_1^{\alpha_1}p_2^{\alpha_2-1}\ldots p_k^{\alpha_k}p_{k+1}) \\
&\quad +\ldots+f(p_k)f^n(p_1^{\alpha_1}p_2^{\alpha_2}\ldots p_k^{\alpha_k-1}p_{k+1})+f(p_{k+1})f^n(p_1^{\alpha_1}p_2^{\alpha_2}\ldots p_k^{\alpha_k}) \\
&= (f(p_1))^{\alpha_1}(f(p_2))^{\alpha_2}\ldots(f(p_k))^{\alpha_k}f(p_{k+1}) \\
&\quad \times\Big(\frac{n!}{(\alpha_1-1)!\alpha_2!\ldots\alpha_k!}+\frac{n!}{\alpha_1!(\alpha_2-1)!\ldots\alpha_k!}+\ldots \\
&\quad\quad +\frac{n!}{\alpha_1!\alpha_2!\ldots(\alpha_k-1)!}+\frac{n!}{\alpha_1!\alpha_2!\ldots\alpha_k!}\Big) \\
&= (f(p_1))^{\alpha_1}(f(p_2))^{\alpha_2}\ldots(f(p_k))^{\alpha_k}f(p_{k+1})\frac{n!}{(\alpha_1-1)!(\alpha_2-1)!\ldots(\alpha_k-1)!} \\
&\quad \times\Big(\frac{1}{\alpha_2\alpha_3\ldots\alpha_k}+\frac{1}{\alpha_1\alpha_3\ldots\alpha_k}+\ldots+\frac{1}{\alpha_1\alpha_2\ldots\alpha_{k-1}}+\frac{1}{\alpha_1\alpha_2\ldots\alpha_k}\Big) \\
&= (f(p_1))^{\alpha_1}(f(p_2))^{\alpha_2}\ldots(f(p_k))^{\alpha_k}f(p_{k+1})\frac{n!}{(\alpha_1-1)!(\alpha_2-1)!\ldots(\alpha_k-1)!} \\
&\quad \times\frac{\alpha_1+\alpha_2+\ldots+\alpha_k+1}{\alpha_1\alpha_2\ldots\alpha_k}
\end{aligned}
$$

$$= \quad (f(p_1))^{\alpha_1}(f(p_2))^{\alpha_2}\ldots(f(p_k))^{\alpha_k}f(p_{k+1})\frac{(n+1)!}{\alpha_1!\alpha_2!\ldots\alpha_k!1!}$$

since $\alpha_1+\alpha_2+\ldots+\alpha_k+1=n+1$. This gives the desired result. □

Theorem 3.5.6 *If F is the complete Dirichlet convolution quasifield over a commutative ring with identity then F is not nil.*

Proof: Choose $f \in F$ such that $f(p)=1$ for some prime p. Then, by the above lemma, we have $f^n(p^n)=n!/n!(f(p))^n=1$ and so $f^n \neq \delta$. □

Again, as for the Cauchy convolution presented earlier in this section, a suitable choice of underlying ring will yield a complete Dirichlet convolution quasifield which is in $\mathcal{K}$.

Note that as a consequence of Theorem 3.1.1 it follows that there are no complete Cauchy convolution or Dirichlet convolution quasifields over $\mathbf{Z}_p$ which are in $\mathcal{K}$. In fact, in Theorem 7.1.12, we will show that the Cauchy convolution ring over $\mathbf{Z}_p$ is additively torsion (obviously) while its circle group is torsion-free.

3.6 Further results on nilness and nilpotence

In the final section of this chapter we show that if a ring is in $\mathcal{K}$ and its additive group is a p-group then the ring is nil.

Theorem 3.6.1 *If $R \in \mathcal{K}$ and $(R,+)$ is a p-group then R is nil.*

Proof: Since $(R,+)$ is a p-group and $(R,+) \cong (R,\circ)$ then $(R,\circ)$ is also a p-group. Suppose that $a \in R$ has additive order p^m and $\circ$-order p^n so that $a^{\circ p^n}=0$. But $a^{\circ p^n}=\sum_{k=1}^{p^n}\binom{p^n}{k}a^k = a^{p^n}+\sum_{k=1}^{p^n-1}\binom{p^n}{k}a^k$. From the proof of Lemma 1.2.4 we know p is a factor of $\binom{p^n}{k}$, from which it follows that we can write $a^{p^n}=-\sum_{k=1}^{p^n-1}\binom{p^n}{k}a^k=-p\sum_{k=1}^{p^n-1}r_k a^k$ for suitable values of r_k. By raising both sides to the power of m the nilpotence of a is apparent because R is an

additive p-group. $\square$

There is no converse to this theorem. Rings in $\mathcal{K}$ can be nil without the additive group being a p-group, as is seen by the Zassenhaus algebra over $\mathbf{Z}$ discussed in Sections 2.4 and 3.4. On the other hand, if F is the Zassenhaus algebra over $\mathbf{Z}_p$, then F is nil and its additive group is a p-group. However since, for example, $\varepsilon_{\frac{c}{p}}^{p} \neq \delta$ (see the proof of Theorem 3.4.8) F is not in $\mathcal{K}$ by Theorem 3.1.1.

Chapter 4

Ring properties of $\mathcal{K}$-rings

This chapter contains results about the ring properties of rings with isomorphic additive and circle composition groups. In particular we look at closure properties such as whether or not $\mathcal{K}$ is hereditary, closed under homomorphisms and closed under direct sums. Some of the questions will be answered only partially at this stage, for certain special cases.

4.1 $\mathcal{K}$ is not a radical class

As the following example shows, $\mathcal{K}$ is not closed under extensions and, as a result, cannot be a radical class.

Example 4.1.1 *$\mathcal{K}$ is not closed under extensions.*

Proof: Our example arises from the Cauchy convolution quasifield constructed on the set $\{0, 1, 2\}$ with underlying ring $\mathbf{Z}_2$. It comprises four elements, the functions δ, a, b, c where δ is the additive and circle composition identity. We

shall call this quasifield F. The binary operation tables are given below:

Circle composition

	δ	a	b	c
δ	δ	a	b	c
a	a	b	c	δ
b	b	c	δ	a
c	c	δ	a	b

Addition

	δ	a	b	c
δ	δ	a	b	c
a	a	δ	c	b
b	b	c	δ	a
c	c	b	a	δ

Multiplication

	δ	a	b	c
δ	δ	δ	δ	δ
a	δ	b	δ	b
b	δ	δ	δ	δ
c	δ	b	δ	b

Now, inspection of the tables shows that this ring is a quasifield with $I = \{\delta, b\}$ as an ideal; moreover, this ideal is a zero ring and hence in $\mathcal{K}$. The factor ring F/I has the following tables and is also a zero ring.

Circle composition

	I	$a+I$
I	I	$a+I$
$a+I$	$a+I$	I

Addition

	I	$a+I$
I	I	$a+I$
$a+I$	$a+I$	I

Multiplication

	I	$a+I$
I	I	I
$a+I$	I	I

Thus $I, F/I \in \mathcal{K}$, but, since $(F, \circ)$ has an element of order 4 while $(F, +)$ does not, we have $F \notin \mathcal{K}$. In fact, $(F, \circ) \cong \mathbf{Z}_4$ while $(F, +) \cong \mathbf{Z}_2 \oplus \mathbf{Z}_2$. Thus $\mathcal{K}$ is not closed under extensions and so is not a radical class. □

4.2 Ideals and homomorphic images

This section contains a collection of partial results concerning whether $\mathcal{K}$ is hereditary and closed under homomorphisms. For certain classes of rings in $\mathcal{K}$ both properties hold (including a class which we will not consider until Chapter 5; we shall prove the relevant results there, in Theorem 5.1.10). However, neither holds in general as we shall see later in the thesis: Corollary 5.3.2 shows that $\mathcal{K}$ is not hereditary, while Theorem 6.3.3 shows that $\mathcal{K}$ is not closed under homomorphisms. In Theorem 7.1.10 we also show that a quasiregular subring (not necessarily an ideal) of a ring in $\mathcal{K}$ need not be in $\mathcal{K}$. For the moment, however, we prove *some* results for a couple of cases which are tractable with the tools currently at our disposal.

Proposition 4.2.1 *If $R \in \mathcal{K}$ is an algebra over $\mathbf{Z}_p$ (p prime) and I is an ideal of R then both I and R/I are in $\mathcal{K}$. Subrings of R are also in $\mathcal{K}$.*

Proof: By Theorem 3.1.1 we have $r^p = 0$ for all $r \in R$ and thus, in particular, for all $r \in I$ or in any subring of R. For $g + I \in R/I$ this also means that $(g + I)^p = g^p + I = I$. In both cases the result follows from the converse of Theorem 3.1.1. □

Suppose $R \in \mathcal{K}$ with isomorphism f and I is an ideal of R with $f(I) = I$. It is thus true, trivially, that $I \in \mathcal{K}$. We mention this because many of the ideals which will be identified and studied in Section 4.5 satisfy this property. As the next result shows, if I is invariant under the isomorphism then the factor ring R/I is in $\mathcal{K}$, too.

Theorem 4.2.2 *Suppose $R \in \mathcal{K}$, I is an ideal of R and f is an isomorphism $f : (R, \circ) \to (R, +)$ such that $f(I) = I$. Then $R/I \in \mathcal{K}$.*

Proof: Define $f^* : (R/I, \circ) \to (R/I, +)$ *via* $f^*(a \circ I) = f(a) + I$. Now f^* is well-defined since if $a \circ I = b \circ I$ then $a = b \circ i$ for some $i \in I$. Since f is an isomorphism from $(R, \circ)$ to $(R, +)$ then $f(a) = f(b \circ i) = f(b) + f(i)$. Since we know $f(i)$ is in I it follows that $f(a) + I = f(b) + I$ as required. Now $f^*((a \circ I) \circ (b \circ I)) = f^*((a \circ b) \circ I) = f(a \circ b) + I = (f(a) + f(b)) + I = (f(a)+I)+(f(b)+I) = f^*(a \circ I)+f^*(b \circ I)$, so that f^* is a group homomorphism. Hence $(R/I, +) = Im(f^*) \cong (R, \circ)/Ker(f^*) = (R, \circ)/\{a \circ I | f^*(a \circ I) = I\} = (R, \circ)/\{a \circ I | f(a) + I = I\} = (R, \circ)/(I, \circ) \cong (R/I, \circ)$ and thus $R/I \in \mathcal{K}$. □

Theorem 4.2.3 *If $R \in \mathcal{K}$ and p is a prime then $R/pR \in \mathcal{K}$ if and only if $f(pR) \subseteq pR$, where f is the group isomorphism from $(R, +)$ to $(R, \circ)$.*

Proof: First we observe that R/pR is an algebra over $\mathbf{Z}_p$. Secondly, given that $f : (R, +) \to (R, \circ)$ is an isomorphism, then for all $r \in R$ we have

$$f(pr) = (f(r))^{\circ p} = \sum_{k=1}^{p} \binom{p}{k} (f(r))^k = (f(r))^p + \sum_{k=1}^{p-1} \binom{p}{k} (f(r))^k$$

where $\sum_{k=1}^{p-1}\binom{p}{k}(f(r))^k \in pR$. The following statements are then equivalent, the equivalence of (iii) and (iv) hinging on f being a bijection and the equivalence of (v) and (vi) on Theorem 3.1.1.

(i) $f(pR) \subseteq pR$.

(ii) $f(pr) \in pR$ for all $r \in R$.

(iii) $(f(r))^p \in pR$ for all $r \in R$.

(iv) $x^p \in pR$ for all $x \in R$.

(v) $(x + pR)^p = 0$ for all $x \in R$.

(vi) $R/pR \in \mathcal{K}$. □

We conclude this section by examining the connection between ideals of quasiregular rings and normal subgroups of the corresponding circle composition group. The following result is well-known (see, for example, [26] page 12).

Proposition 4.2.4 *If I is an ideal of a quasiregular ring R then $(I, \circ)$ is a normal subgroup of the group $(R, \circ)$.* □

The converse does not hold in general, nor for rings in $\mathcal{K}$. Consider the operation tables of the following ring in $\mathcal{K}$.

Circle composition table:

	0	a	b	c	d	e	f	g	h
0	0	a	b	c	d	e	f	g	h
a	a	g	d	e	f	h	b	0	c
b	b	d	e	g	h	0	c	f	a
c	c	e	g	d	0	f	a	h	b
d	d	f	h	0	c	a	e	b	g
e	e	h	0	f	a	b	g	c	d
f	f	b	c	a	e	g	h	d	0
g	g	0	f	h	b	c	d	a	e
h	h	c	a	b	g	d	0	e	f

Addition table:

	0	a	b	c	d	e	f	g	h
0	0	a	b	c	d	e	f	g	h
a	a	b	0	e	f	g	h	c	d
b	b	0	a	g	h	c	d	e	f
c	c	e	g	d	0	f	a	h	b
d	d	f	h	0	c	a	e	b	g
e	e	g	c	f	a	h	b	d	0
f	f	h	d	a	e	b	g	0	c
g	g	c	e	h	b	d	0	f	a
h	h	d	f	b	g	0	c	a	e

Multiplication table:

	0	a	b	c	d	e	f	g	h
0	0	0	0	0	0	0	0	0	0
a	0	c	d	0	0	c	c	d	d
b	0	d	c	0	0	d	d	c	c
c	0	0	0	0	0	0	0	0	0
d	0	0	0	0	0	0	0	0	0
e	0	c	d	0	0	c	c	d	d
f	0	c	d	0	0	c	c	d	d
g	0	d	c	0	0	d	d	c	c
h	0	d	c	0	0	d	d	c	c

This is a ring in $\mathcal{K}$: it is an algebra over $\mathbf{Z}_3$ in which $x^3 = 0$ for all x from which Theorem 3.1.1 implies that the additive and circle composition groups are isomorphic. The only proper non-trivial ideal is $\{0, c, d\}$, while the non-trivial proper subgroups with respect to circle composition are $\{0, a, g\}, \{0, b, e\}, \{0, c, d\}$ and $\{0, f, h\}$.

4.3 Direct products, subdirect products and filtered products

Theorem 4.3.1 *$\mathcal{K}$ is closed under direct products and direct sums.*

Proof: If $\{A_\lambda | \lambda \in \Lambda\} \subseteq \mathcal{K}$ then for each $\lambda \in \Lambda$ let f_λ denote an isomorphism $f_\lambda : (A_\lambda, \circ) \to (A_\lambda, +)$. Define the function $f : (\prod_{\lambda\in\Lambda} A_\lambda, \circ) \to (\prod_{\lambda\in\Lambda} A_\lambda, +)$ so

that for $a \in \prod_{\lambda\in\Lambda} A_\lambda$ we have $(f(a))(\lambda) = f_\lambda(a(\lambda))$. It is routine to show that f is an isomorphism. The proof for direct sums is similar, and again hinges on the component isomorphisms, f_λ. □

For our next result we need the concept of a *filter* and a filtered product. Let I be a non-empty set. A set D of subsets of I is a filter over I if

(i) $\emptyset \notin D$, $I \in D$;

(ii) If $A \in D$ and $A \subseteq B$ then $B \in D$ (D is closed under supersets); and

(iii) If $A, B \in D$ then $A \cap B \in D$ (D is closed under intersections).

Suppose that $\mathcal{D}$ is a filter on the index set Λ. Let

$$M_{\mathcal{D}} = \{a \in \prod A_\lambda \,|\, D_a = \{\lambda \,|\, a(\lambda) = 0\} \in \mathcal{D}\};$$

it is straightforward to show that $M_{\mathcal{D}}$ is an ideal of $\prod A_\lambda$. The *filtered product* (also called the *reduced product*) is $\prod A_\lambda / M_{\mathcal{D}}$.

Theorem 4.3.2 *The class $\mathcal{K}$ is closed under filtered products.*

Proof: Suppose $\mathcal{D}$ is a filter on Λ and $\{A_\lambda | \lambda \in \Lambda\} \subseteq \mathcal{K}$. By Theorem 4.3.1 we have $\prod_{\lambda\in\Lambda} A_\lambda \in \mathcal{K}$; let f be the isomorphism defined in that proof. If $a \in M_{\mathcal{D}}$ we have $(f(a))(\lambda) = 0$ if and only if $f_\lambda(a(\lambda)) = 0$ if and only if $a(\lambda) = 0$ as each f_λ is an isomorphism. We thus have $D_{f(a)} = D_a \in \mathcal{D}$ and hence $f(M_{\mathcal{D}}) = \{f(a) \,|\, D_a \in \mathcal{D}\} = \{f(a) \,|\, D_{f(a)} \in \mathcal{D}\} = M_{\mathcal{D}}$. Theorem 4.2.2 implies $\prod_{\lambda\in\Lambda} A_\lambda / M_{\mathcal{D}} \in \mathcal{K}$ as required. □

Corollary 4.3.3 *If $\{A_\lambda | \lambda \in \Lambda\} \subseteq \mathcal{K}$ then $\prod_{\lambda\in\Lambda} A_\lambda / \bigoplus_{\lambda\in\Lambda} A_\lambda \in \mathcal{K}$.*

Proof: Let $\mathcal{D}$ be the set of subsets of Λ with finite complements. This is a filter, and $M_{\mathcal{D}} = \bigoplus_{\lambda\in\Lambda} A_\lambda$. □

Proposition 4.3.4 *Suppose $\{R_\lambda | \lambda \in \Lambda\}$ is a family of rings with $R_\lambda \in \mathcal{K}$ and R_λ is an algebra over $\mathbf{Z}_p$ for all $\lambda \in \Lambda$, where p is a fixed prime. Then any subdirect product of the R_λ is in $\mathcal{K}$.*

Proof: If R_λ is in $\mathcal{K}$ and is an algebra over $\mathbf{Z}_p$ then by Theorem 3.1.1 $f^p = 0$ for all $f \in R_\lambda$. Thus $x^p = 0$ for all x in any subdirect product of the R_λ. Furthermore, any such subdirect product will also be an algebra over $\mathbf{Z}_p$ and so by the converse of Theorem 3.1.1 it follows that it must be in $\mathcal{K}$. □

The question of the closure of $\mathcal{K}$ under finite subdirect products is still open.

4.4 Semigroup rings

Theorem 4.4.1 *If S is a commutative semigroup and R is an algebra over $\mathbf{Z}_p$ with $R \in \mathcal{K}$ then $R[S] \in \mathcal{K}$.*

Proof: We note that since S and R are commutative then $R[S]$ is commutative. Furthermore, since R is both in $\mathcal{K}$ and an algebra over $\mathbf{Z}_p$ we have $r^p = 0$ for all $r \in R$ by Theorem 3.1.1. In typical semigroup ring fashion we define the *support* of an element $a = \sum_{\alpha \in S} r_\alpha \alpha \in R[S]$ by $\text{supp}(a) = \{\alpha \mid \alpha \in S, r_\alpha \neq 0\}$. We wish to show that $a^p = 0$ for all $a \in R[S]$. We shall proceed by induction on $|\text{supp}(a)|$. If $|\text{supp}(a)| = 1$ then there exists some non-zero r_α such that $a = r_\alpha \alpha$. Then $a^p = r_\alpha^p \alpha^p = 0\alpha^p = 0$ as required.

Now suppose that $a^p = 0$ for all $a \in R[S]$ such that $|\text{supp}(a)| = n$. Consider $a \in R[S]$ with $|\text{supp}(a)| = n + 1$. Writing $A = \text{supp}(a)$ we have

$$\begin{aligned} a^p &= (\sum_{\alpha \in A} r_\alpha \alpha)^p = (r_{\alpha'}\alpha' + \sum_{\alpha \in A \setminus \{\alpha'\}} r_\alpha \alpha)^p \\ &= (r_{\alpha'}\alpha')^p + \sum_{k=1}^{p-1} \binom{p}{k} (r_{\alpha'}\alpha')^{p-k} (\sum_{\alpha \in A \setminus \{\alpha'\}} r_\alpha \alpha)^k + (\sum_{\alpha \in A \setminus \{\alpha'\}} r_\alpha \alpha)^p \end{aligned}$$

where $\alpha' \in A$. Now $\binom{p}{k}$ is divisible by p for all $1 \leq k \leq p-1$ and so the double summation term in the final expression vanishes. Furthermore, $(r_{\alpha'}\alpha')^p$ vanishes because $(r_{\alpha'})^p$ does, and, finally, $(\sum_{\alpha \in A \setminus \{\alpha'\}} r_\alpha \alpha)^p$ vanishes by the inductive hypothesis. Thus $a^p = 0$ for all $a \in R[S]$, and since $R[S]$ is also an algebra over $\mathbf{Z}_p$ we have $R[S] \in \mathcal{K}$ by Theorem 3.1.1. □

4.5 Some ideals of quasifields

In what follows, unless stated otherwise, F represents a quasi-division ring (sometimes a quasifield) formed on a poset P using the construction described in Section 2.2, where K is the underlying ring.

There are a number of ideals of quasi-division rings which are easily identified and whose properties can be determined to varying degrees. Here we will consider three classes of ideals, while observing that not all the ideals of a quasifield are included in these classes (for example, the quasifield over $\mathbf{Z}_3$ determined by subsets of the set $\{1, 2\}$ (as in Example 2.2.8) has a number of ideals in addition to those discussed in this section; however, the nature of all its ideals is determined by Proposition 4.2.1). In some cases these ideals will be zero rings.

In order to obtain our first class of ideals we require that P satisfies

$(w5)$: $h(x) \geq h(y) + h(w(x, y))$ for $x \in P$, $y \leq x$.

This condition is satisfied by all the examples considered in Section 2.2. If this condition is not satisfied by a poset but the poset is still suitable for the construction of a quasi-division ring then the sets defined below will be right ideals.

Given $n \in \mathbf{N}$, let

$$I_n = \{f \in F \mid f(x) = 0 \text{for all } x \notin \text{Min}(P) \text{such that } h(x) \ \leq \ n\}.$$

Then, for $f \in I_n$, $g \in F$ and $x \notin \text{Min}(P)$ such that $h(x) \leq n$, we have

$$(fg)(x) = \sum_{e_x < y < x} f(y)g(w(x, y)),$$

and since $y < x$ we have $h(y) < h(x) \leq n$ so that $f(y) = 0$, whence $(fg)(x) = 0$. Similarly, since $h(w(x, y)) \leq h(x) \leq n$ by $(w5)$, we have

$$(gf)(x) = \sum_{e_x < y < x} g(y)f(w(x, y)) = 0.$$

Thus fg, $gf \in I_n$; and clearly $f_1 - f_2 \in I_n$ for f_1, $f_2 \in I_n$, so that I_n is an ideal of F.

[We note that, in fact, a similar proof yields $f \in I_n$, $g \in F$ implies fg, $gf \in I_{n+1}$. This gives us a descending chain of ideals $I_1 \triangleright I_2 \triangleright I_3 \triangleright \ldots$, where the chain terminates at $I_m = \{\delta\}$ in the case of posets of finite height m. This series of ideals is, in fact, an annihilator series since FI_n, $I_nF \subseteq I_{n+1}$, so that I_n/I_{n+1} annihilates F/I_{n+1} (see [26], $p.4$). By Theorem 3.2.4 and Theorem 1.3.1 of [26] we expect F to have an annihilator series as it is nilpotent; indeed, the inductive products in Theorem 3.2.4 work their way through these ideals.]

Corollary 3.2.3 then yields the following result.

Proposition 4.5.1 *F/I_1 is a zero ring.*

Proof: Consider $f + I_1$ and $g + I_1$ in F/I_1. Then $(f + I_1)(g + I_1) = fg + I_1$ and the result follows since, by Corollary 3.2.3, $fg \in I_1$ for any $f, g \in F$. □

In what follows, let P satisfy the following additional condition:

($w6$): If $h(P) = n$ then for $x \in P$, $y \leq x$ we have $h(y) \leq \left\lceil \frac{n}{2} \right\rceil$ or $h(w(x, y)) \leq \left\lceil \frac{n}{2} \right\rceil$ or both.

Note that ($w5$) implies ($w6$).

Proposition 4.5.2 *If P satisfies ($w6$) with $h(P) = n$ and $k \geq \left\lceil \frac{n}{2} \right\rceil$ then I_k is a zero ring.*

Proof: Take $f, g \in I_k$ and consider any $x \in P$, $x \notin \mathrm{Min}(P)$ (the $x \in \mathrm{Min}(P)$ case being trivial). As $h(x) \leq k$ implies $(f\ g)(x) = 0$, suppose that $h(x) \geq k$ and consider $(fg)(x) = \sum_{e_x < y < x} f(y)g(w(x, y))$. Then, by ($w6$), $h(w(x, y)) \leq \left\lceil \frac{n}{2} \right\rceil \leq k$ and so $g(w(x, y)) = 0$ (because $g \in I_k$), or $h(y) \leq \left\lceil \frac{n}{2} \right\rceil \leq k$ so $f(y) = 0$ (as $f \in I_k$). In either case $f(y)g(w(x, y)) = 0$ for all $e_x < y < x$ where $h(x) \geq k$, so that $fg = \delta$. □

As we will show, many of the partially ordered sets considered in Section 3 or their finite restrictions satisfy condition ($w6$).

Sets (See Example 2.2.8): If P is the set of subsets of a *finite* set S where $|S| = n$ then we have $h(P) = n$. We note that $A \in P$ (i.e. $A \subseteq S$) satisfies $h(A) = |A|$, and if $B \subseteq A$ we have $w(A, B) = A \backslash B$. Since for such sets $|B| + |A \backslash B| = |A|$ (which is to say $h(B) + h(w(A, B)) = h(A)$), and as $|A| \leq n$, then $|B| \leq \left\lfloor \frac{n}{2} \right\rfloor$ or $|A \backslash B| \leq \left\lfloor \frac{n}{2} \right\rfloor$ or both, so that ($w6$) is satisfied.

Cauchy Convolution (See Example 2.2.9): Restrict P to the set of whole numbers less than or equal to some $n \in \mathbf{N}$ so that $h(P) = n$; furthermore, for $x \in P$ we have $h(x) = x$ as P is a chain anchored by 0. For $x \in P$, $y \leq x$ we have $w(x, y) = x - y$ so that $x = y + w(x, y)$. This is equivalent to $h(y) + h(w(x, y)) = h(x)$, so clearly ($w6$) is satisfied.

Divisibility/Dirichlet Convolution (See Example 2.2.10): In this case let P be the set of natural numbers less than or equal to some m (we can restrict the Dirichlet convolution to this finite poset instead of the usual $\mathbf{N}$ and still obtain a quasifield). If $x = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}$ is the prime factorization of $x \in P$ then $h(x) = \alpha_1 + \alpha_2 + ... + \alpha_k$. Suppose $h(P) = n$, noting that the height of P is determined by those elements of P having the greatest multiplicity of factors. For $x \in P$, if $y|x$ it is clear that $h(y) + h(w(x, y)) = h(x)$ (see the argument for $\lambda(x)$ in Example 2.2.10), and, as $h(x) \leq n$, ($w6$) must be satisfied.

Words (See Example 2.2.12): Restrict P to the set of words of length less than or equal to n (observing that the alphabet — and hence the poset — may still be infinite). Then $h(P) = n$, and the height of a word is given by its length. If $\alpha \in P$ and $\beta \leq \alpha$ then, since $w(\alpha, \beta)$ is the word remaining when β is removed from the beginning of α, we have $h(\alpha) = h(\beta) + h(w(\alpha, \beta))$, so that ($w6$) is satisfied.

Intervals (See Example 2.2.13): In the previous examples the posets actually satisfied $h(x) = h(y) + h(w(x, y))$, whenever $y \leq x \in P$. This is not necessarily

true in the case of intervals. Let $(\mathcal{P}, \preceq)$ be a locally finite poset having height n. Then the height of P, the corresponding poset of intervals, will also be n, and, moreover, the height of an interval $[x, y] \in P$ is determined by the maximum length of all chains in $\mathcal{P}$ between the element determining the "bottom" of the interval, x, and that determining the "top", y. Now, for $[x, u] \leq [x, y]$ in P (which is to say $u \preceq y$ in $\mathcal{P}$) we have $w([x, y], [x, u]) = [u, y]$. Then $h([x, y]) \geq h([x, u]) + h([u, y])$, as the height of an interval is given by the *maximum* chain length between its end-points, and the chains between x and u and between u and y give rise to at least one chain between x and y (although not necessarily the maximal one). Since $h([x, y]) \leq n$ then it is obvious that $h([x, u]) \leq \left\lceil \frac{n}{2} \right\rceil$ or $h([u, y]) \leq \left\lceil \frac{n}{2} \right\rceil$ or both, as required by $(w6)$.

Thus far we have examined those ideals determined by *all* the elements of a poset having a given height. We will now look at ideals determined by a given element. We can do this when the poset satisfies the condition

$(w7)$: If $y \leq x$ then $w(x, y) \leq x$;

a condition which is fulfilled by all the partially ordered sets of Section 2.2 except the poset of words and the poset of intervals. For a given $x \in P$ let

$$I_x = \{f \in F | f(y) = 0 \text{for all } y \leq x, y \notin \text{Min}(P)\}.$$

[We note that in some cases the elements of P may be natural numbers, but the context should eliminate possible confusion between the ideals I_x and the previously discussed I_n.] The fact that I_x is an ideal of F for a given x follows in similar fashion to the proof that I_n is an ideal, provided $(w7)$ is satisfied — if $(w7)$ is not satisfied then we have right ideals. If $y \leq x$ then $I_y \triangleleft I_x$ so that we have a partially ordered set of these ideals which is the dual of P.

In the case of P having finite height the situation can arise whereby none of the I_x are zero rings. For example, consideration of the multiplication operation from the quasi-division ring determined by the poset of intervals arising from

one of the five element posets (the one having least and greatest elements and with two chains, of length four and three, joining them) leads to the conclusion that none of the I_x are necessarily zero rings. However, in at least one class of quasi-division rings zero rings *are* obtained from some members of this class of ideals, as the following result reveals.

Proposition 4.5.3 *Let F be the quasi-division ring formed on the set of subsets of a finite set S, where $|S| = n$. Then I_A is a zero ring for any $A \subseteq S$ such that $|A| = n - 1$.*

Proof: Let $A \subseteq S$ satisfy the conditions of the proposition, and consider $f, g \in I_A$. If $X \subseteq A \subseteq S$ we have $(fg)(X) = \sum_{\emptyset \neq Y \subset X} f(Y)g(X \backslash Y) = 0$ since $f(Y) = 0$ for $Y \subset X \subseteq A$. Now suppose X is not a subset of A. Then, as $|A| = n - 1$ and $|S| = n$, there must be one element $x \in S$ such that $x \notin A$. Denote by Y' those subsets of X that contain x; thus $(fg)(X) = \sum_{\emptyset \neq Y \subset X} f(Y)g(X \backslash Y) = \sum_{Y' \subset X} f(Y')g(X \backslash Y')$, since those subsets, Y, which do not contain x will be subsets of A (as A contains all the elements of S except x), and $f(Y) = 0$ for such Y. However $X \backslash Y'$ will not contain x so that $X \backslash Y' \subseteq A$ and thus $g(X \backslash Y') = 0$, whence $(fg)(X) = 0$. Thus, $(fg)(X) = 0$ for all $X \subset S$ $(X \neq \emptyset)$ and so $fg = \delta$. □

We note that none of the other I_A need be zero rings.

Another ideal is given by

$$I_K = \{f \in F \mid \exists\ k \in K \text{ such that } f(x) = k \text{ for all atoms } x \in P\}.$$

This is clearly closed under subtraction, and Corollary 3.2.3 takes care of multiplication.

Now, zero rings trivially have isomorphic additive and circle composition groups as the two correspond. The question then arises as to whether or not

any of the above classes of ideals — in particular, those ideals of rings/quasi-division rings having the isomorphism property — also have isomorphic groups even when not guaranteed to be zero rings.

Theorem 4.5.4 *If F is a quasifield with isomorphic additive and circle composition groups (with isomorphism as given by L in Section 2.2) then the ideals determined by I_n and I_x have the same isomorphic property, as do F/I_n and F/I_x.*

Proof: Suppose $f \in I_n$ and that $h(x) \leq n$, with $x \notin \mathrm{Min}(P)$. Then, from Section 2.2, we have

$$\begin{aligned}(Lf)(x) &= \sum_{y \leq x} f(y) f^{\circ(-1)}(w(x,y))\lambda(y) \\ &= \sum_{e_x \neq y \leq x} f(y) f^{\circ(-1)}(w(x,y))\lambda(y) + f(e_x) f^{\circ(-1)}(w(x,e_x))\lambda(e_x) \\ &= 0,\end{aligned}$$

as $f^{\circ(-1)}(w(x,e_x)) = f^{\circ(-1)}(x) = \sum_{e_x \neq y \leq x} f(y) f^{\circ(-1)}(w(x,y))$ from Lemma 2.2.2 (determination of the $\circ$-inverse) and $f(y) = 0$ for all $y \leq x$ (since $f \in I_n$ and $h(y) \leq h(x) \leq n$). Thus (Lf) $\in I_n$, and so $L(I_n) \subseteq I_n$. Using the arguments of Theorem 2.2.6 (in proving that L is surjective) we see that L^{-1} can be defined inductively on f by $(L^{-1}(f))(x) = 1$ for $x \in \mathrm{Min}(P)$ and

$$(L^{-1}(f))(x) = \frac{1}{\lambda(x)} \left\{ f(x) - \sum_{y<x} (L^{-1}(f))(y) (L^{-1}(f))^{\circ(-1)}(w(x,y))\lambda(y) \right\}.$$

We can then use induction to show that if f is in I_n then so is $L^{-1}(f)$. If $f(x) = 0$ for all x such that $h(x) \leq n$, then for atomic x we have $(L^{-1}(f))(x) = \frac{1}{\lambda(x)}\{f(x) - (L^{-1}(f))(e_x)(L^{-1}(f))^{\circ(-1)}(w(x,e_x))\lambda(e_x)\} = 0$ since $\lambda(e_x) = 0$ (see page 21) and $f(x) = 0$. Assuming $(L^{-1}(f))(y) = 0$ for all y such that $h(y) < k$ then for x satisfying $h(x) = k \leq n$ we deduce that

$$(L^{-1}(f))(x) = \frac{1}{\lambda(x)}\{f(x) - \sum_{y<x} (L^{-1}(f))(y) (L^{-1}(f))^{\circ(-1)}(w(x,y))\lambda(y)\} = 0$$

by the inductive hypothesis and the fact that $f \in I_n$. Thus $L^{-1}(I_n) \subseteq I_n$ and hence $L(I_n) = I_n$. It follows that $I_n \in \mathcal{K}$ and, by Theorem 4.2.2, that $F/I_n \in \mathcal{K}$ too. Similar arguments yield the same result for the ideals of the form I_x. □

The situation is not quite so straightforward for the ideal I_K. The extra condition in the statement of the following proposition — that $\lambda(x)$ is constant for all atomic $x \in P$ — is satisfied by all the quasifields of Section 2.2 having isomorphic additive and circle composition groups, with the exception of the quasifield formed on the set of polynomials. In this case $\lambda(p(x)) = \deg(p(x)) + \log(\text{gif}(p(x)))$, while the atomic polynomials are the primes and the irreducibles. Clearly $\lambda(p(x))$ can vary for different atomic polynomials.

Proposition 4.5.5 *If F is a quasifield in $\mathcal{K}$ and the logarithm function λ satisfies the condition that $\lambda(x)$ is a constant for all atomic $x \in P$, then I_K and F/I_K also have isomorphic additive and circle composition groups.*

Proof: If $f \in I_K$ and x is an atom of P, then

$$\begin{aligned}(Lf)(x) &= \sum_{y \leq x} f(y) f^{\circ(-1)}(w(x,y))\lambda(y) \\ &= f(e_x) f^{\circ(-1)}(w(x,e_x))\lambda(e_x) + f(x) f^{\circ(-1)}(w(x,x))\lambda(x) \\ &= f^{\circ(-1)}(x)\lambda(e_x) + f(x)\lambda(x) = f(x)\lambda(x).\end{aligned}$$

as $\lambda(e_x) = 0$ (see page 21). This will be a constant by the requirements of the Proposition and because $f(x)$ is a constant for all atomic x since $f \in I_K$. Furthermore, applying the arguments used in the previous theorem about L^{-1}, we see that $(L^{-1}(f)) = \frac{1}{\lambda(x)}\{f(x) - (L^{-1}(f))(e_x)(L^{-1}(f))^{\circ(-1)}(w(x,e_x))\lambda(e_x) = \frac{f(x)}{\lambda(x)}$ and this is constant for all atomic x as both $f(x)$ and $\lambda(x)$ are. Thus $L(I_K) = I_K$, whence the restriction of L to I_K is as required, and, once again, Theorem 4.2.2 implies that $F/I_K \in \mathcal{K}$. □

Chapter 5

Rings constructed on torsion groups

Our aim in this chapter is to determine some of the circumstances in which a torsion group can be the additive group of a ring in $\mathcal{K}$. We shall be interested only in non-trivial examples; obviously we can construct a zero ring on any (additive) group. We will talk about rings which are *supported* by an abelian group, so that if $(R, +, \cdot)$ is a ring then $(R, +)$ is the group which supports the ring, and observe that a group may support of number of different rings.

Haimo [17] has considered which groups are the additive groups of Jacobson radical rings and these results will form, to some extent, a prelude to our endeavours of further determining which such rings are also in $\mathcal{K}$. Fischer and Eldridge, in [15], obtained some partial results for finite cyclic groups, which we will clarify and extend. We will also consider all other finite abelian groups, as well as an infinite p-group and a mixed group.

5.1 Finite rings on $\mathbf{Z}_{p^n}$

In this section we study finite rings, including those in which the additive group is isomorphic to the finite group $\mathbf{Z}_n$. Finite rings are, of course, torsion rings and the primary decomposition theorem (see Theorem 1.2.3) states that every torsion ring can be expressed uniquely as a direct sum of p-rings. Here a p-ring is one in which, for each element a, there exists $k \in \mathbf{N}$ such that $p^k a = 0$. In the case of a ring, R, whose additive group is isomorphic to $\mathbf{Z}_n$, where $n = p_1^{i_1} p_2^{i_2} \dots p_k^{i_k}$, then $R \cong \bigoplus_{1 \le j \le k} R_{p_j}$ where R_{p_j} is a ring whose additive group is isomorphic to $\mathbf{Z}_{p_j^{i_j}}$. Furthermore, it is known that when $R = \bigoplus_\Lambda R_\lambda$ then R is quasiregular if and only if each R_λ is quasiregular, and so we can establish quasiregularity in a ring by establishing it in the components of the direct sum.

For the most part we will consider rings whose additive group is isomorphic to $\mathbf{Z}_{p^n}$ and ascertain when the ring is quasiregular and then whether or not the additive group is isomorphic to the circle composition group, or, in other words, if the ring is in $\mathcal{K}$. We will be particularly interested in rings which are not zero rings, since rings which have the trivial multiplication are obviously in $\mathcal{K}$ as the additive and circle composition groups coincide. By *non-trivial ring* we will mean a ring which is not a zero ring.

Lemma 5.1.1 *Let $(A, +, \cdot)$ be a ring with $(A, +) \cong \mathbf{Z}_{p^n}$ where p is prime. We will write $A = \{\overline{0}, \overline{1}, \overline{2}, \overline{3}, \dots, \overline{p^n - 1}\}$. If $\overline{1} \cdot \overline{1} = \overline{a} \in A$ then $\overline{k} \cdot \overline{m} = \overline{kma} = km\overline{a}$ for all $\overline{k}, \overline{m} \in A$.*

Proof: This result follows from distributivity and the fact that additively we are in $\mathbf{Z}_{p^n}$. □

It is also clear that $\overline{k} \cdot \overline{m} = \overline{m} \cdot \overline{k}$ for all $\overline{k}, \overline{m} \in A$.

Now circle composition is defined from addition and multiplication via $a \circ b =$

$a+b+a\cdot b$ and so for $\overline{k},\overline{m}\in A$ we must have $\overline{k}\circ\overline{m}=\overline{k}+\overline{m}+km\overline{a}$. In order to verify that $(A,\circ)$ is an abelian group we need only check that for all $x\in A$ there exists $x'\in A$ such that $x\circ x'=0$, since it is already clear that $\circ$ is well-defined, associative, commutative and has 0 as its identity. In the case that A is finite this is equivalent to showing that $x\circ y=x\circ z$ implies that $y=z$. We will often think of the action of the circle composition operation in terms of a Cayley table, showing the action of $\circ$ on pairs of elements. So, showing that $(A,\circ)$ is a group is equivalent to showing that there is no repetition of elements in any row or column of the circle composition Cayley table.

If $(A,\circ)$ has been established to be a group, then the question of whether or not it is isomorphic to $\mathbf{Z}_{p^n}$ can be answered by determining if $(A,\circ)$ is cyclic of order p^n. Alternatively, in showing that the groups are not isomorphic, we can consider the values of $x\circ x$. In the Cayley table of $\mathbf{Z}_{p^n}$ the diagonal, where values of $x+x$ appear, has 2^{n-1} different entries each appearing twice if $p=2$, and p^n entries, all different, if p is odd. Consequently, if we consider the diagonals of the Cayley table of $(A,\circ)$ and find that too many different values of x give rise to the same result $x\circ x$ then we know that we cannot have a group which is isomorphic to $\mathbf{Z}_{p^n}$.

We will consider rings $(A,+,\cdot)$ and first determine whether or not they are quasiregular. As in our previous Lemma we write $A=\{\overline{0},\overline{1},\overline{2},\overline{3},\ldots,\overline{p^n-1}\}$ and we use the notation $\overline{a}=\overline{1}\cdot\overline{1}$. We frequently will use equality instead of the full congruence mod p^n notation.

The following result was first proved by Haimo in [17]; we give a slightly more elementary proof.

Theorem 5.1.2 *If $(A,+,\cdot)$ is the ring constructed on $\mathbf{Z}_{p^n}$ by setting $\overline{1}\cdot\overline{1}=\overline{a}$ then A is quasiregular if and only if a is a multiple of p.*

Proof: Since A is finite it is artinian, and the radical of an artinian ring

is known to be nilpotent. However, A is quasiregular so its radical is itself and therefore A is quasiregular if and only if it is nilpotent (if and only if it is nil). Lemma 5.1.1 implies that for $\overline{x}, \overline{y} \in A$ we have $\overline{x} \cdot \overline{y} = xy\overline{a}$, and hence, in general, $\overline{x_1} \cdot \overline{x_2} \cdots \overline{x_k} = x_1 x_2 \cdots x_k \overline{a}^{k-1}$. If p is a factor of a then it is clear that $A^{n+1} = 0$ as we are working in $\mathbf{Z}_{p^n}$. On the other hand, if p is not a factor of a, then $\overline{1}^m = \overline{a}^{m-1} \neq 0$ for all m, as a^m has no factor of p. Thus A is not nil and hence not quasiregular. □

Corollary 5.1.3 *There is no non-trivial quasiregular ring with* $(A, +) \cong \mathbf{Z}_p$.□

Haimo asserts that the p^{n-1} quasiregular rings which can be constructed on the additive group $\mathbf{Z}_{p^n}$, fall into n isomorphic classes, one of which is the zero ring. (See [17], Theorem 8). He omits the proof and so we give one here.

Lemma 5.1.4 *If A is a quasiregular ring whose additive group is isomorphic to $\mathbf{Z}_{p^n}$ then A lies in one of n classes of isomorphic rings.*

Proof: Since $(A, +)$ is isomorphic to $\mathbf{Z}_{p^n}$ it follows from Theorem 5.1.2 that a has a factor of p in order for A to be quasiregular, where $\overline{a} = \overline{1} \cdot \overline{1}$.

Let $(A_1, +, \cdot)$ and $(A_2, +, *)$ be two rings defined on $\mathbf{Z}_{p^n}$ by $\overline{1} \cdot \overline{1} = \overline{r_1 p^{k_1}}$ and $\overline{1} * \overline{1} = \overline{r_2 p^{k_2}}$ respectively, where p does not divide r_1 nor r_2 and $k_1 \neq k_2$. Now in the multiplication table of one of our quasiregular rings on $\mathbf{Z}_{p^n}$ the row associated with the element 1 will be one of those with the most non-zero entries, since the product of $\overline{m}$ and $\overline{k}$ is given by $mk\overline{a}$ and 1 is relatively prime to p^n. Then in A_1 we have $\overline{1} \cdot \overline{s_1 p^{n-k_1}} = 1 \times s_1 p^{n-k_1} \overline{r_1 p^{k_1}} = s_1 r_1 \overline{p^n} = 0$, while in A_2 we have $\overline{1} * \overline{s_2 p^{n-k_2}} = 1 \times s_2 p^{n-k_2} \overline{r_2 p^{k_2}} = s_2 r_2 \overline{p^n} = 0$. Since there are p^{k_1} multiples of $\overline{p^{n-k_1}}$ in $\mathbf{Z}_{p^n}$ then there are p^{k_1} occurrences of 0 in row 1, compared with p^{k_2} occurrences in row 1 of A_2. It follows that A_1 is not isomorphic to A_2.

Now suppose that we have rings $(A_1, +, \cdot)$ and $(A_2, +, *)$ with multiplication given by $\overline{1} \cdot \overline{1} = \overline{p^k}$ and $\overline{1} * \overline{1} = \overline{rp^k}$ respectively, where p does not divide r. We

will prove that $A_1 \cong A_2$. Since p and r are relatively prime we have that the order of $\overline{r}$ is p^n so that, additively, A_2 is generated by $\overline{r}$; that is, $A_2 = \langle \overline{r} \rangle$. Define $f : A_2 \to A_1$ via $f(m\overline{r}) = \overline{m}$. Clearly f is a bijection; furthermore addition is preserved. Finally $f(\overline{m} * \overline{j}) = f(mj\overline{rp^k}) = f(mjp^k\overline{r}) = \overline{mjp^k} = mj\overline{p^k} = \overline{m} \cdot \overline{j}$. Thus $A_1 \cong A_2$ and hence the isomorphic classes are determined by the number of factors of p in the square of 1. □

We shall use $\mathbf{Z}_{p^n}^{p^k}$ to denote the quasiregular ring $\mathbf{Z}_{p^n}$ by setting $\overline{1} \cdot \overline{1} = rp^k$ where p does not divide r. The proof of Theorem 5.1.2 implies that the index of nilpotence of such a ring is m, where m is the smallest integer greater than or equal to $\frac{n+k}{k}$, i.e. $m = \lceil \frac{n+k}{k} \rceil$. This is because in order to have $\overline{x_1} \cdot \overline{x_2} \cdots \overline{x_m} = x_1 x_2 \cdots x_m \overline{a}^{m-1} = 0$ when $a = rp^k$ we must have $(p^k)^{m-1} \geq p^n$ and hence $mk - k \geq n$.

Recalling that torsion rings can be written as a direct sum of p-rings, we have the following result concerning the inheritance of $\mathcal{K}$ between a certain type of torsion ring and its direct sum components.

Theorem 5.1.5 *Let A be a torsion nil ring. Then $A \in \mathcal{K}$ if and only if $A_p \in \mathcal{K}$ for all primes p where $A = \bigoplus_p A_p$.*

Proof: Since A is a torsion ring then by the primary decomposition theorem we can write $A = \bigoplus_p A_p$ where each A_p is a p-ring for all primes p. Then by Theorem 4.3.1 we know that $\mathcal{K}$ is closed under direct sums and so we have half of the proof.

Now suppose that A is in $\mathcal{K}$, implying A is quasiregular. Let f denote an isomorphism $f : (A, +) \to (A, \circ)$. Since A is nil so is each p-ring A_p; Lemma 2.4 of [1] then implies that $(A_p, \circ)$ is also a p-group. If we express $a \in A$ in terms of its direct sum components as $a = a_1 + a_2 + \ldots + a_n$ where $a_i \in A_{p_i}$, then $a_1 \circ a_2 \circ \ldots \circ a_n = a_1 + a_2 + \ldots + a_n = a$ as all product terms involving $a_i a_j, i \neq j$ vanish because a_i and a_j are from different components of the direct

sum (i.e. $A_{p_i} \lhd A$ for all i, and $A_{p_i} \cap A_{p_j} = \{0\}$ for $i \neq j$). It follows that $(A, \circ) = \sum(A_p, \circ) = \bigoplus(A_p, \circ)$ because each $(A_p, \circ)$ is a p-group. Returning to the isomorphism f, we now view it as $f : \bigoplus(A_p, +) \to \bigoplus(A_p, \circ)$ and, again because we are dealing with p-groups, we must have $f(A_p, +) = (A_p, \circ)$ for all p. Thus f induces an isomorphism on each A_p, whence $A_p \in \mathcal{K}$. □

We know that a ring whose additive group is isomorphic to $\mathbf{Z}_n$ can be expressed as a direct sum of rings whose additive groups are isomorphic to $\mathbf{Z}_{p^n}$ for various primes p. The above theorem implies that in order to ascertain if such a ring has its circle composition group isomorphic to $\mathbf{Z}_n$ (and hence whether or not the ring is in $\mathcal{K}$) it suffices to examine rings whose additive groups are isomorphic to $\mathbf{Z}_{p^n}$. In order to answer the question of which rings constructed on $\mathbf{Z}_{p^n}$ are in $\mathcal{K}$ we need the following observations.

Observation (i): Since repeated circle composition yields $x^{\circ m} = \sum_{t=1}^{m} \binom{m}{t} x^t$ we have $\overline{1}^{\circ m} = \sum_{t=1}^{m} \binom{m}{t} \overline{a}^{t-1}$ where $\overline{1} \cdot \overline{1} = \overline{a}$.

Observation (ii): Suppose we have constructed a quasiregular ring, A, whose additive group is isomorphic to $\mathbf{Z}_{p^n}$. Then $(A, \circ)$ is an abelian group of order p^n and so the order of any element in A with respect to $\circ$ must be a power of p. In order to determine if $(A, \circ)$ is isomorphic to $\mathbf{Z}_{p^n}$, and hence to $(A, +)$, we shall investigate the values of m for which $\overline{1}^{\circ m} = 0$. We know m will be a power of p; where appropriate we will show that, in fact, m must be greater than or equal to p^n so that $(A, \circ)$ is cyclic. Since any two cyclic groups of order p^n are isomorphic then achieving this proves that $(A, \circ) \cong \mathbf{Z}_{p^n}$ as desired.

Observation (iii): From Lemma 1.2.4 we note that if $m = p^i$, the number of factors of p appearing in $\binom{m}{t}$ exactly depends on the difference between the number of factors of p in m and the number of factors of p in t.

The following lemmas will also be used.

Lemma 5.1.6 *In the ring constructed on* $\mathbf{Z}_{2^n}$ *where* $n \geq 3$ *by setting* $\overline{1} \cdot \overline{1} = \overline{a}$

we have $\overline{x} \circ \overline{x} = \overline{(x + 2^{n-1})} \circ \overline{(x + 2^{n-1})}$.

Proof: Noting that $\overline{x} \circ \overline{x} = 2\overline{x} + \overline{x} \cdot \overline{x} = 2\overline{x} + x^2\overline{a}$ where $\overline{1} \cdot \overline{1} = \overline{a}$ we have $\overline{(x + 2^{n-1})} \circ \overline{(x + 2^{n-1})} = 2\overline{(x + 2^{n-1})} + (x + 2^{n-1})^2\overline{a} = 2\overline{x} + 2^n + x^2\overline{a} + 2^n x\overline{a} + 2^{2n-2}\overline{a} = 2\overline{x} + x^2\overline{a} = \overline{x} \circ \overline{x}$. □

Lemma 5.1.7 *If* $\overline{x} \circ \overline{x} = 0$ *in the ring constructed on* $\mathbf{Z}_{2^n}$ *by setting* $\overline{1} \cdot \overline{1} = \overline{a}$ *then* $\overline{(2^n - x)} \circ \overline{(2^n - x)} = 0$ *in the ring constructed on* $\mathbf{Z}_{2^n}$ *by setting* $\overline{1} * \overline{1} = \overline{2^n - a}$.

Proof: In $(\mathbf{Z}_{2^n}, +, *)$ we have $\overline{(2^n - x)} \circ \overline{(2^n - x)} = 2\overline{(2^n - x)} + (2^n - x)^2\overline{(2^n - a)} = \overline{(2^{n+1} - 2x)} + (2^{2n} - 2^{n+1}x + x^2)\overline{(2^n - a)} = -(2\overline{x} + x^2\overline{a}) = -(\overline{x} \circ \overline{x}) = 0$ as required. Note that at the final step $\overline{x}$ was in $(\mathbf{Z}_{2^n}, +, \cdot)$ □

We will now determine when a quasiregular ring $\mathbf{Z}_{p^n}^{p^k}$ is in $\mathcal{K}$. Part of the following result was known to Fischer and Eldridge in [15]. They observed, while omitting the verification, that the circle group on a quasiregular ring supported by $\mathbf{Z}_{p^n}$ is cyclic for p odd, but they only noted that in the $p = 2$ case the circle group may or may not be cyclic. We clarify the situation here, ascertaining what happens in that case, as well as giving a complete proof of their assertions for odd p.

Theorem 5.1.8 *Consider rings, A, constructed with their additive groups isomorphic to* $\mathbf{Z}_{p^n}$.

(i) If $n = 1$ *then there is no non-trivial* $A \in \mathcal{K}$.

(ii) If p *is odd and* $n \geq 2$ *then there exists at least one non-trivial* $A \in \mathcal{K}$.

(iii) If $p = 2$ *and* $n = 2$ *then there is no non-trivial* $A \in \mathcal{K}$.

(iv) If $p = 2$ *with* $n \geq 3$ *then there exists at least one non-trivial* $A \in \mathcal{K}$.

Proof: By Theorem 5.1.2 we know when we can obtain quasiregular rings based on $\mathbf{Z}_{p^n}$ as the additive group, and so we need only check the diagonals of

$(A, \circ)$ or determine if the order of one its elements is p^n to ascertain whether or not $(A, \circ)$ is isomorphic to $\mathbf{Z}_{p^n}$ and hence if A is in $\mathcal{K}$.

Case (i): We know from Corollary 5.1.3 that the only quasiregular ring on $\mathbf{Z}_p$ is the zero ring.

Case (ii): Suppose that p is odd with $n \geq 2$. From Theorem 5.1.2 we know that choosing $a = rp$ ($r \in \mathbf{N}$) gives the only quasiregular rings; we also know, from Observation (ii), that m must be a power of p in order to have $\overline{1}^{\circ m} = 0$. Choose $m = p^i$ with $i < n$; we will consider whether or not $\overline{1}^{\circ m} = 0$. Now $\overline{1}^{\circ m} = \sum_{t=1}^{m} \binom{m}{t} \overline{a}^{t-1} = m + \binom{m}{2}\overline{a} + \binom{m}{3}\overline{a}^2 + \ldots + \binom{m}{m-1}\overline{a}^{m-2} + \binom{m}{m}\overline{a}^{m-1}$. Now, in considering $\binom{m}{t}\overline{a}^{t-1}$ for $t \geq 2$, suppose that t has $j < i$ factors of p. Then, by Observation (iii), $\binom{m}{t}$ will have j fewer factors of p than does m, so that the number of factors of p in $\binom{m}{t}$ is $i - j \geq 1$. However, a^{t-1} has at least $t - 1$ factors of p because $a = rp$, and, since $t - 1 \geq p^j - 1 > j$ (as p is an odd prime), it follows that $\binom{m}{t}a^{t-1}$ has at least $i + 1$ factors of p (as $(i - j) + (t - 1) > i - j + j = i$). Thus $p^{i+1} | \binom{m}{t}a^{t-1}$. Writing $\alpha_{t-1} = \binom{m}{t}a^{t-1}/p^i$ we have $1^{\circ m} = p^i(1 + \alpha_1 + \alpha_2 + \ldots + \alpha_{m-1})$. Then $\alpha_1 + \alpha_2 + \ldots + \alpha_{m-1}$ has p as a factor but $1 + \alpha_1 + \alpha_2 + \ldots + \alpha_{m-1}$ does not. As a consequence $1^{\circ m}$ lacks this extra factor of p and so p^n does not divide $1^{\circ m}$. Hence $\overline{1}^{\circ m} \neq \overline{0}$ for all $m < p^n$, and as a result $\overline{1}$ has order p^n in $(A, \circ)$. Thus $(A, \circ) \cong \mathbf{Z}_{p^n}$, yielding $A \in \mathcal{K}$.

Case (iii): If $p = 2$ and $n = 2$ then we are working in a ring whose additive group is isomorphic to $\mathbf{Z}_4$. We know that choosing $a = 2$ gives the only non-trivial quasiregular ring. From the identity $\overline{x} \circ \overline{x} = 2\overline{x} + x^2\overline{a}$ in this ring we have $\overline{1} \circ \overline{1} = 2 \times \overline{1} + 1 \times \overline{2} = \overline{2} + \overline{2} = \overline{0}$ and $\overline{3} \circ \overline{3} = 2 \times \overline{3} + 9 \times \overline{2} = \overline{2} + \overline{2} = \overline{0}$ in addition to $\overline{0} \circ \overline{0} = \overline{0}$ and $\overline{2} \circ \overline{2} = \overline{0}$. A group which is isomorphic to $\mathbf{Z}_{2k}$ will have only two zero entries on the diagonal. Here we have four and so this circle composition group is not isomorphic to $\mathbf{Z}_4$ nor, obviously, to the ring's additive group, and so the ring is not in $\mathcal{K}$. Thus the only ring in $\mathcal{K}$ whose additive group is isomorphic to $\mathbf{Z}_4$ is the trivial ring.

Case (iv): If $p = 2$ and $n \geq 3$ we know that choosing $a = 2r$ gives a quasiregular ring.

Suppose that r is odd. We will show that there is no non-trivial ring in $\mathcal{K}$ by using the results of our previous two lemmas to show that there are too many occurrences of 0 on the diagonal of the circle composition table. Note that in any quasiregular ring constructed on $\mathbf{Z}_{2^n}$ we have $\overline{0} \circ \overline{0} = \overline{0}$ and $\overline{2^{n-1}} \circ \overline{2^{n-1}} = 2\overline{2^{n-1}} + (2^{n-1})^2\overline{a} = \overline{0}$; so we shall be seeking other elements $\overline{x}$ such that $\overline{x} \circ \overline{x} = \overline{0}$. If we find such an $\overline{x}$, then the first our little lemmas guarantees the existence of a second such element. We will call such elements "zero $\circ$-square" . We shall proceed by induction on n.

If $n = 3$ then there are quasiregular rings on $\mathbf{Z}_8$ obtained by choosing $a = 2, 4$ or 6; however the choice of 4 does not satisfy the requirement that r be odd. If $a = 2$ then we have $\overline{3} \circ \overline{3} = 2 \times \overline{3} + 9 \times \overline{2} = \overline{6} + \overline{2} = \overline{0}$ and so $\overline{0}, \overline{3}, \overline{4}$ and $\overline{7}$ (by Lemma 5.1.6) are zero $\circ$-square. Similarly, if $a = 6$ then $\overline{1} \circ \overline{1} = 2 \times \overline{1} + 1 \times \overline{6} = \overline{2} + \overline{6} = \overline{0}$, whence $\overline{0}, \overline{1}, \overline{4}$ and $\overline{5}$ are zero $\circ$-square. Thus these values of a do not give rise to non-trivial rings in $\mathcal{K}$.

For the inductive hypothesis, suppose that the choice of $a = 2r$, where r is odd, always gives rise to two extra zero $\circ$-square elements in the quasiregular ring constructed on $\mathbf{Z}_{2^n}$. Consider, now, quasiregular rings constructed on $\mathbf{Z}_{2^{n+1}}$. To begin with, take $r < 2^{n+1}/4$ so that a is less than 2^n. This value of a is one which generates extra zero $\circ$-square elements in the quasiregular ring constructed on $\mathbf{Z}_{2^n}$. By the inductive hypothesis and Lemma 5.1.6 suppose that these two elements are $\overline{x}$ and $\overline{x + 2^{n-1}}$. These are zero $\circ$-square in $\mathbf{Z}_{2^n}$ which means that when $\circ$-squared they have a factor of 2^n; let us consider what happens to these elements in the ring on $\mathbf{Z}_{2^{n+1}}$ constructed with the same choice of a. Now $\overline{x} \circ \overline{x} = 2\overline{x} + x^2\overline{a}$ while $\overline{(x + 2^{n-1})} \circ \overline{(x + 2^{n-1})} = 2\overline{(x + 2^{n-1})} + (x + 2^{n-1})^2\overline{a} = 2\overline{x} + \overline{2^n} + x^2\overline{a} + 2^n x\overline{a} + 2^{2n-2}\overline{a} = 2\overline{x} + \overline{2^n} + x^2\overline{a} + 2^{n+1}x\overline{r} + 2^{(n+1)+(n-3)}\overline{a} = 2\overline{x} + \overline{2^n} + x^2\overline{a} = \overline{x} \circ \overline{x} + \overline{2^n}$. Now we know that $\overline{x} \circ \overline{x}$ has a factor of 2^n; if it does

not have an extra factor of 2 then it must be the case that $\overline{x} \circ \overline{x} + \overline{2^n}$ does, or *vice versa*. Thus either $\overline{x} \circ \overline{x}$ or $\overline{(x + 2^{n-1})} \circ \overline{(x + 2^{n-1})}$ has a factor of 2^{n+1} and so there is a zero $\circ$-square element in the ring on $\mathbf{Z}_{2^{n+1}}$ which is not $\overline{0}$ or $\overline{2^n}$. Hence the ring is not in $\mathcal{K}$. For values of a such that $2^n < a < 2^{n+1}$ we can apply the second of our lemmas. We have just proved that, since $2^{n+1} - a < 2^n$, we can find an additional zero $\circ$-square element, $\overline{x}$, in the ring with $\overline{1} \cdot \overline{1} = \overline{(2^{n+1} - a)}$; Lemma 5.1.7 implies that $\overline{(2^{n+1} - x)}$ is an additional zero $\circ$-square element in the ring with $\overline{1} \cdot \overline{1} = \overline{a}$. This gives the required result: if $a = 2r$ is chosen with r odd then the resulting ring is not in $\mathcal{K}$.

On the other hand, suppose that we construct a ring on $\mathbf{Z}_{2^n}$ by choosing $a = 4r$. We know this is quasiregular; we will show that it is also in $\mathcal{K}$.

Setting $m = 2^i$ with $i < n$, consider

$$\overline{1}^{\circ m} = \sum_{t=1}^{m} \binom{m}{t} \overline{a}^{t-1} = m + \binom{m}{2}\overline{a} + \binom{m}{3}\overline{a}^2 + \ldots + \binom{m}{m-1}\overline{a}^{m-2} + \binom{m}{m}\overline{a}^{m-1}.$$

Since a has a factor of 4 then for $t \geq 2$ we have that a^{t-1} has $2t - 2$ factors of 2, and if t has $j < i$ factors of 2 — so that we can write $t = 2^j s$ for some $i > j \geq 0, s \geq 1$ — then Observation (iii) implies that $\binom{m}{t}$ has $i - j$ factors of 2. Thus the total number of factors of 2 in $\binom{m}{t}a^{t-1}$ is $i - j + 2t - 2$. Now $i - j + 2t - 2 \geq i + 1$ provided $2t - j = 2^{j+1}s - j \geq 3$. For $j \geq 1$ this is obviously true since then $2^{j+1} - j \geq 3$ and s is greater than or equal to 1. If $j = 0$ then the result still holds because $t \geq 2$. Hence every term $\binom{m}{t}a^{t-1}$ for $t \geq 2$ has a factor of 2^{i+1}. Writing $\alpha_{t-1} = \binom{m}{t}a^{t-1}/2^i$ we have $1^{\circ m} = 2^i(1 + \alpha_1 + \alpha_2 + \ldots + \alpha_{n-1})$. Now $\alpha_1 + \alpha_2 + \ldots + \alpha_{n-1}$ has an additional factor of 2 but $1 + \alpha_1 + \alpha_2 + \ldots + \alpha_{z-1}$ does not. As a consequence $1^{\circ m}$ lacks this extra factor of 2 and so 2^n does not divide $1^{\circ m}$. It follows that $\overline{1}^{\circ m} \neq 0$ for all $m < 2^n$, and as a result $\overline{1}$ has order 2^n in $(A, \circ)$. Thus $(A, \circ) \cong \mathbf{Z}_{2^n}$, yielding $A \in \mathcal{K}$. □

These results are summarized in the following table.

Values of p and n for rings on $\mathbf{Z}_{p^n}$	Does a non-trivial quasiregular ring exist?	Does a non-trivial ring in $\mathcal{K}$ exist?
p prime, $n = 1$	No	No
$p = 2, n = 2$	Yes ($a = 2$), $\mathbf{Z}_4^2$	No
p odd prime, $n \geq 2$	Yes ($a = rp$), $\mathbf{Z}_{p^n}^{rp}$	Yes ($a = rp$), $\mathbf{Z}_{p^n}^{rp}$
$p = 2, n \geq 3$	Yes ($a = 2r$), $\mathbf{Z}_{2^n}^{2r}$	Yes ($a = 4r$), $\mathbf{Z}_{2^n}^{4r}$

where r is a natural number chosen to ensure that $a < p^n$.

We can use this classification to highlight the fact that the quasifield construction is not the only way to obtain rings in $\mathcal{K}$. This will be illustrated further by other examples later in the thesis, but for now we have

Proposition 5.1.9 *There exist rings in $\mathcal{K}$ which do not arise from the poset quasifield construction method of Section 2.2.*

Proof: By Theorem 5.1.8 we know that there is a non-trivial ring in $\mathcal{K}$ whose additive group is $\mathbf{Z}_8$. Now if there is a poset construction which produces this ring then the poset must have at least three elements: it must have at least one minimal element and it must have at least one element of height two since if all the elements are of height one we have a zero ring (this will be proved in Corollary 3.2.3). Observe that the size of a poset constructed quasifield is given by $|K|^m$ where K is the underlying ring on which the functions/elements in the quasifield take their values, and $m = |P \backslash \mathrm{Min}(P)|$. Now in our case we have $m \geq 2$ so that the only solution for $|K|^m = 8$ is $m = 3$ and $|K| = 2$. However, since addition is defined pointwise and K has only two elements then the elements of the resulting poset constructed quasifield must have order 2. However, the ring in $\mathcal{K}$ on $\mathbf{Z}_8$ has four elements of order 8 and thus cannot be constructed from a poset. □

In fact, similar arguments show that none of the rings in $\mathcal{K}$ which we have considered here — namely those whose additive and circle composition groups are isomorphic to $\mathbf{Z}_{p^n}$ but which are not zero rings — arise from a poset construction.

We conclude this section by considering the status of ideals and homomorphic images of rings like $\mathbf{Z}_{p^n}^{p^k}$ which are in $\mathcal{K}$.

Theorem 5.1.10 *Suppose $\mathbf{Z}_{p^n}^{p^k}$ is a ring in $\mathcal{K}$ as constructed in Section 5.1. If I is an ideal of $\mathbf{Z}_{p^n}^{p^k}$ then $I \in \mathcal{K}$ and $\mathbf{Z}_{p^n}^{p^k}/I \in \mathcal{K}$.*

Proof: [Note: for $p = 2$ we must have $n \geq 3$ and $k \geq 2$ in order for $\mathbf{Z}_{p^n}^{p^k}$ to be in $\mathcal{K}$ non-trivially, by Theorem 5.1.8.] Suppose that $I \lhd \mathbf{Z}_{p^n}^{p^k}$ and that there exists $\overline{b} \in I$ such that $\gcd(b, p) = 1$. Then b has additive order p^n in $\mathbf{Z}_{p^n}$ and so $I = \mathbf{Z}_{p^n}^{p^k}$. If I is not all of $\mathbf{Z}_{p^n}^{p^k}$ then there exists a minimal value of $m < n$ such that $p^m | b$ for all $\overline{b} \in I$. Then, as I is an ideal, we must have $I \supseteq \{\overline{sp^m} \mid 0 \leq s < p^{n-m}\}$, so that I contains all multiples of p^m and, hence, all multiples of $p^{m+1}, \ldots, p^{n-1}$. But then, in fact, we must have $I = (p^m)$, the principal ideal generated by p^m, and all ideals of $\mathbf{Z}_{p^n}^{p^k}$ have this form.

Let $I_m = (p^m)$. Now if $2m + k \geq n$ we can show that I_m is a zero ring, since if $\overline{sp^m}, \overline{rp^m} \in I_m$ it follows that $\overline{sp^m} \cdot \overline{rp^m} = \overline{sp^m rp^m p^k} = \overline{srp^{2m+k}} = \overline{0}$.

On the other hand, if $2m + k < n$ we have $n - m > m + k$ and in this case we can show that I_m is isomorphic to $\mathbf{Z}_{p^{n-m}}^{p^{k+m}}$. Define $f : I_m \to \mathbf{Z}_{p^{n-m}}^{p^{k+m}}$ by $f(\overline{sp^m}) = \overline{s}$; clearly f is a bijection. In addition, we have $f(\overline{s_1 p^m} + \overline{s_2 p^m}) = f(\overline{(s_1 + s_2)p^m}) = \overline{s_1 + s_2} = \overline{s_1} + \overline{s_2} = f(\overline{s_1 p^m}) + f(\overline{s_2 p^m})$ and $f(\overline{s_1 p^m} \cdot \overline{s_2 p^m}) = f(\overline{(s_1 p^m s_2 p^m p^k}) = f(\overline{s_1 s_2 p^{m+k} p^m}) = \overline{s_1 s_2 p^{m+k}} = \overline{s_1} \cdot \overline{s_2} = f(\overline{s_1 p^m}) \cdot f(\overline{s_2 p^m})$, so that f is an isomorphism. We conclude that $I_m \in \mathcal{K}$.

We will now consider the homomorphic images of $\mathbf{Z}_{p^n}^{p^k}$. If $m \leq k$ then $\mathbf{Z}_{p^n}^{p^k}/I_m$ is a zero ring as $(\overline{a} + I_m)(\overline{b} + I_m) = \overline{abp^k} + I_m = I_m$. In this case $\mathbf{Z}_{p^n}^{p^k}/I_m \in \mathcal{K}$ as required. Finally we shall show that $\mathbf{Z}_{p^n}^{p^k}/I_m \cong \mathbf{Z}_{p^m}^{p^k}$ when $m > k$. Define

$f : \mathbf{Z}_{p^n}^{p^k}/I_m \to \mathbf{Z}_{p^m}^{p^k}$ via $f(\overline{a} + I_m) = \overline{a}$. It is obvious that this is a bijection which preserves addition; all that remains is to consider multiplication. From $f((\overline{a} + I_m) \cdot (\overline{a} + I_m)) = f(\overline{a} \cdot \overline{b} + I_m) = f(\overline{abp^k} + I_m) = \overline{abp^k} = \overline{a} \cdot \overline{b} = f(\overline{a} + I_m) \cdot f(\overline{b} + I_m)$ we deduce that f is an isomorphism and that all factor rings of $\mathbf{Z}_{p^n}^{p^k}$ are thus in $\mathcal{K}$. □

5.2 Rings on other finite abelian groups

Having determined which of the finite cyclic groups support non-trivial rings in $\mathcal{K}$ and how, we now turn our attention to more general finite abelian groups. By the end of this section we will have completely categorized all such groups according to whether they can or cannot support a non-trivial $\mathcal{K}$-ring.

From Theorem 5.1.8 we have seen that there are no non-trivial rings in $\mathcal{K}$ constructed on the groups $\mathbf{Z}_p$ for p prime, nor on $\mathbf{Z}_4$.

Furthermore, there is no non-trivial ring in $\mathcal{K}$ with $\mathbf{Z}_2 \oplus \mathbf{Z}_2$ as its additive group. To see this, consider $(1,0)$ and $(0,1)$ as basis elements for the additive group then define a multiplication by defining the products $(1,0)(1,0)$, $(0,1)(0,1)$ and $(1,0)(0,1) = (0,1)(1,0)$ and extending to the rest of the ring via distributivity. Now if the ring is to be in $\mathcal{K}$ it must have its squares equal to zero, since it is an algebra over $\mathbf{Z}_2$ (Theorem 3.1.1), from which we conclude that $(1,0)(1,0) = (0,0) = (0,1)(0,1)$. By associativity we must have $[(0,1)(0,1)](1,0) = (0,1)[(0,1)(1,0)]$ so if $(1,0)(0,1) = (a,b)$ we have

$$\begin{aligned}(0,1)[(0,1)(1,0)] &= (0,1)(a,b) = (0,1)[a(1,0) + b(0,1)] \\ &= a(0,1)(1,0) + b(0,1)(0,1) = a(a,b) = (a^2, ab),\end{aligned}$$

while $[(0,1)(0,1)](1,0) = (0,0)(1,0) = (0,0)$. Similarly

$$\begin{aligned}(0,0) &= [(1,0)(1,0)](0,1) = (1,0)[(1,0)(0,1)] = (1,0)(a,b) \\ &= (1,0)[a(1,0) + b(0,1)] = b(1,0)(0,1) = b(a,b) = (ba, b^2).\end{aligned}$$

We conclude that $a = b = 0$ and so the $\mathcal{K}$-ring on $\mathbf{Z}_2 \oplus \mathbf{Z}_2$ is trivial.

For primes bigger than 2, we *can* construct non-trivial rings on $\mathbf{Z}_p \oplus \mathbf{Z}_p$ which are in $\mathcal{K}$. To do this, consider, for example, the Cauchy Convolution quasifield (see Example 2.2.9) constructed on the poset $(\{0, 1, 2\}, \leq)$ with underlying ring $\mathbf{Z}_p$. We will use F_p to denote such a ring. Additively, this is just $\mathbf{Z}_p \oplus \mathbf{Z}_p$ because addition is defined pointwise on the non-minimal elements. The poset is of height 2, and since $p > 2$ we can invoke Corollary 3.2.5 to conclude that F_p is in $\mathcal{K}$. However, multiplication is non-trivial since, for example, if $f \in F_p$ is such that $f(1) \neq 0$, then $f^2(2) = (f(1))^2 \neq 0$ since the underlying ring is $\mathbf{Z}_p$. Thus F_p is not a zero ring.

There exists a non-trivial ring in $\mathcal{K}$ having $\mathbf{Z}_2 \oplus \mathbf{Z}_2 \oplus \mathbf{Z}_2$ as its additive group. This is the subsets quasifield (see Example 2.2.8) constructed on the poset of subsets of $\{1, 2\}$ ordered with respect to $\subseteq$, having $\mathbf{Z}_2$ as its underlying ring. It is known (Corollary 3.2.3) that $f^2(\{1\}) = f^2(\{2\}) = 0$, and we can see that $f^2(\{1, 2\}) = 2f(\{1\})f(\{2\}) = 0$ since the ring is of characteristic 2. Thus we have $f^2 = 0\,(= \delta)$ and so Theorem 3.1.1 implies that the ring is in $\mathcal{K}$. However, it is non-trivial because $(fg)(\{1, 2\}) = f(\{1\})g(\{2\}) + f(\{2\})g(\{1\})$ need not be zero.

Finally, we also have a non-trivial ring in $\mathcal{K}$ having $\mathbf{Z}_2 \oplus \mathbf{Z}_4$ as the additive group, and a 16 element non-trivial $\mathcal{K}$-ring on $\mathbf{Z}_4 \oplus \mathbf{Z}_4$. The tables for these are shown below; the first set shows the ring constructed on $\mathbf{Z}_2 \oplus \mathbf{Z}_4$.

Addition table:

	0	1	2	3	4	5	6	7
0	0	1	2	3	4	5	6	7
1	1	2	3	0	5	6	7	4
2	2	3	0	1	6	7	4	5
3	3	0	1	2	7	4	5	6
4	4	5	6	7	0	1	2	3
5	5	6	7	4	1	2	3	0
6	6	7	4	5	2	3	0	1
7	7	4	5	6	3	0	1	2

Circle composition table:

	0	1	2	3	4	5	6	7
0	0	1	2	3	4	5	6	7
1	1	6	3	4	5	2	7	0
2	2	3	0	1	6	7	4	5
3	3	4	1	6	7	0	5	2
4	4	5	6	7	0	1	2	3
5	5	2	7	0	1	6	3	4
6	6	7	4	5	2	3	0	1
7	7	0	5	2	3	4	1	6

Multiplication table:

	0	1	2	3	4	5	6	7
0	0	0	0	0	0	0	0	0
1	0	4	0	4	0	4	0	4
2	0	0	0	0	0	0	0	0
3	0	4	0	4	0	4	0	4
4	0	0	0	0	0	0	0	0
5	0	4	0	4	0	4	0	4
6	0	0	0	0	0	0	0	0
7	0	4	0	4	0	4	0	4

Ring constructed on $\mathbf{Z}_4 \oplus \mathbf{Z}_4$.

Addition table:

	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
0	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
1	1	2	3	0	5	6	7	4	9	10	11	8	13	14	15	12
2	2	3	0	1	6	7	4	5	10	11	8	9	14	15	12	13
3	3	0	1	2	7	4	5	6	11	8	9	10	15	12	13	14
4	4	5	6	7	8	9	10	11	12	13	14	15	0	1	2	3
5	5	6	7	4	9	10	11	8	13	14	15	12	1	2	3	0
6	6	7	4	5	10	11	8	9	14	15	12	13	2	3	0	1
7	7	4	5	6	11	8	9	10	15	12	13	14	3	0	1	2
8	8	9	10	11	12	13	14	15	0	1	2	3	4	5	6	7
9	9	10	11	8	13	14	15	12	1	2	3	0	5	6	7	4
10	10	11	8	9	14	15	12	13	2	3	0	1	6	7	4	5
11	11	8	9	10	15	12	13	14	3	0	1	2	7	4	5	6
12	12	13	14	15	0	1	2	3	4	5	6	7	8	9	10	11
13	13	14	15	12	1	2	3	0	5	6	7	4	9	10	11	8
14	14	15	12	13	2	3	0	1	6	7	4	5	10	11	8	9
15	15	12	13	14	3	0	1	2	7	4	5	6	11	8	9	10

Circle composition table:

	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
0	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
1	1	8	3	10	5	12	7	14	9	0	11	2	13	4	15	6
2	2	3	0	1	6	7	4	5	10	11	8	9	14	15	12	13
3	3	10	1	8	7	14	5	12	11	2	9	0	15	6	13	4
4	4	5	6	7	10	11	8	9	12	13	14	15	2	3	0	1
5	5	12	7	14	11	2	9	0	13	4	15	6	3	10	1	8
6	6	7	4	5	8	9	10	11	14	15	12	13	0	1	2	3
7	7	14	5	12	9	0	11	2	15	6	13	4	1	8	3	10
8	8	9	10	11	12	13	14	15	0	1	2	3	4	5	6	7
9	9	0	11	2	13	4	15	6	1	8	3	10	5	12	7	14
10	10	11	8	9	14	15	12	13	2	3	0	1	6	7	4	5
11	11	2	9	0	15	6	13	4	3	10	1	8	7	14	5	12
12	12	13	14	15	2	3	0	1	4	5	6	7	10	11	8	9
13	13	4	15	6	3	10	1	8	5	12	7	14	11	2	9	0
14	14	15	12	13	0	1	2	3	6	7	4	5	8	9	10	11
15	15	6	13	4	1	8	3	10	7	14	5	12	9	0	11	2

Multiplication table:

	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
1	0	10	0	10	0	10	0	10	0	10	0	10	0	10	0	10
2	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
3	0	10	0	10	0	10	0	10	0	10	0	10	0	10	0	10
4	0	0	0	0	2	2	2	2	0	0	0	0	2	2	2	2
5	0	10	0	10	2	8	2	8	0	10	0	10	2	8	2	8
6	0	0	0	0	2	2	2	2	0	0	0	0	2	2	2	2
7	0	10	0	10	2	8	2	8	0	10	0	10	2	8	2	8
8	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
9	0	10	0	10	0	10	0	10	0	10	0	10	0	10	0	10
10	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
11	0	10	0	10	0	10	0	10	0	10	0	10	0	10	0	10
12	0	0	0	0	2	2	2	2	0	0	0	0	2	2	2	2
13	0	10	0	10	2	8	2	8	0	10	0	10	2	8	2	8
14	0	0	0	0	2	2	2	2	0	0	0	0	2	2	2	2
15	0	10	0	10	2	8	2	8	0	10	0	10	2	8	2	8

It should be noted that there are at least two other non-isomorphic examples of rings in $\mathcal{K}$ which have $\mathbf{Z}_4 \oplus \mathbf{Z}_4$ as their additive groups.

We can now conclude that when constructing rings whose additive groups are finite abelian groups, the only ones which do not produce non-trivial rings in

$\mathcal{K}$ are $\mathbf{Z}_p$ for p prime, $\bigoplus_{p_i \in P} \mathbf{Z}_{p_i}$ for a set P of distinct primes, $\mathbf{Z}_4$, and $\mathbf{Z}_2 \oplus \mathbf{Z}_2$. For any other finite abelian group we can either obtain a non-trivial ring in $\mathcal{K}$ directly (such as for $\mathbf{Z}_{p^n}$ by Theorem 5.1.8 and $\mathbf{Z}_p \oplus \mathbf{Z}_p$ by the remarks above) or by taking the ring direct sum of a non-trivial ring in $\mathcal{K}$ and a trivial ring (for instance, we can construct a non-trivial $\mathcal{K}$-ring on $\mathbf{Z}_3 \oplus \mathbf{Z}_3 \oplus \mathbf{Z}_2$ by taking a non-trivial $\mathcal{K}$-ring on $\mathbf{Z}_3 \oplus \mathbf{Z}_3$ as indicated above and combining it as a ring direct sum with the zero-ring on $\mathbf{Z}_2$). We summarize these results in

Theorem 5.2.1 *The only finite abelian groups which do not support a non-trivial ring in $\mathcal{K}$ are $\mathbf{Z}_p$ (p prime), $\mathbf{Z}_4$ and $\mathbf{Z}_2 \oplus \mathbf{Z}_2$.* □

5.3 Rings on other groups

Here we present a couple of interesting examples of infinite groups which support rings in $\mathcal{K}$. The first uses torsion groups, and we will use the result to show that $\mathcal{K}$ is not hereditary.

Theorem 5.3.1 *Every non-divisible infinite abelian p-group is the additive group of a non-trivial ring in $\mathcal{K}$.*

Proof: Let G be a non-divisible infinite abelian p-group. We can write $G = D \oplus H$, where D is a divisible p-group and thus a direct sum of copies of $\mathbf{Z}(p^\infty)$ (see, for example, [34] Theorem 9.14), and H is reduced.

In the case that H is infinite, then because it is a reduced p-group it has a cyclic p-group as a direct summand (see [16], Corollary 27.2), say $\langle x_1 \rangle \neq 0$, and so we have $H = \langle x_1 \rangle \oplus H_1$. However, H_1 has the same properties as H and so $H_1 = \langle x_2 \rangle \oplus H_2$ and, similarly, $H_2 = \langle x_3 \rangle \oplus H_3$, etc. In general we can write $H = \langle x_1 \rangle \oplus \langle x_2 \rangle \oplus \ldots \oplus \langle x_n \rangle \oplus H_n$, where $\langle x_1 \rangle, \langle x_2 \rangle, \ldots, \langle x_n \rangle$ are non-zero p-groups and H_n is reduced and infinite. If p is odd then by Theorems 5.1.8 and 5.2.1 we only require at most two cyclic groups in order to form the additive group of a

non-trivial ring in $\mathcal{K}$ (as we can construct a non-trivial ring on $\mathbf{Z}_p \oplus \mathbf{Z}_p$ or on $\mathbf{Z}_{p^n}$ for $n \geq 2$). On the other hand, for $p = 2$ we need at most three cyclic groups ($\mathbf{Z}_2 \oplus \mathbf{Z}_2 \oplus \mathbf{Z}_2$ at the worst, but we may only need two — for example, $\mathbf{Z}_2 \oplus \mathbf{Z}_4$ — or even just one — as in $\mathbf{Z}_{32}$, for instance) in order to construct a non-trivial ring. In either case there is some n so that $\langle x_1 \rangle \oplus \langle x_2 \rangle \oplus \ldots \oplus \langle x_n \rangle = R^+$ where R is a non-trivial ring in $\mathcal{K}$. Let the remaining summands, $D \oplus H_n$, support a zero ring, denoted by $(D \oplus H_n)^o$. Then, as a *ring* direct sum $R \oplus (D + H_n)^o$ is a non-trivial ring in $\mathcal{K}$, while $G = (R \oplus (D + H_n)^o, +)$.

Now consider the case where H is finite. Then, as $H \neq 0$ (since G is not divisible), H must have a finite abelian group as a direct summand, while D must be infinite (as G is) and hence, as a p-group, contains a copy of $\mathbf{Z}(p^\infty)$ as a direct summand. We conclude that $G = \mathbf{Z}_{p^n} \oplus \mathbf{Z}(p^\infty) \oplus F$ for some F. Let x denote a generator for $\mathbf{Z}_{p^n}$ so that $\langle x \rangle \cong \mathbf{Z}_{p^n}$; and for $\mathbf{Z}(p^\infty)$ we have $\langle y_0, y_1, y_2, \ldots \rangle \cong \mathbf{Z}(p^\infty)$ where $py_0 = 0$ and $py_i = y_{i-1}$ for all $i \in \mathbf{N}$.

Let A denote the ring supported by $\langle x \rangle \oplus \langle y_0, y_1, y_2, \ldots \rangle$ with multiplication defined as follows:

$$(mx + \sum_i k_i y_i)(rx + \sum_j t_j y_j) = mry_{n-1}$$

noting that, as far as order is concerned, we have $o(y_{n-1}) = p^n = o(x)$. Clearly A is a nilpotent ring of index three.

Now it is easy to see that $\langle y_0, y_1, y_2, \ldots \rangle$ is an ideal of A (in fact, the maximal divisible ideal), while multiplication in $\langle y_0, y_1, y_2, \ldots \rangle$ is trivial so that addition and circle composition coincide. Thus $(\langle y_0, y_1, y_2, \ldots \rangle, \circ)$, as a subgroup of $(A, \circ)$, is divisible too.

On the other hand, as a ring, $A/\langle y_0, y_1, y_2, \ldots \rangle$ is isomorphic to the zero ring on $\mathbf{Z}_{p^n}$, so again addition and circle composition coincide. It follows that since $A/\langle y_0, y_1, y_2, \ldots \rangle$ is reduced with respect to addition then it is also reduced with respect to $\circ$. Since for an abelian group, G, it is known that G/H is reduced

if and only if H contains the maximal divisible subgroup (see Theorem 9.12 of [34]) we deduce that $\langle y_0, y_1, y_2, \ldots \rangle$ is the maximal divisible subgroup of $(A, \circ)$. Moreover, for such groups $G \cong H \oplus G/H$ and hence

$$\begin{aligned}(A, \circ) &\cong \langle y_0, y_1, y_2, \ldots \rangle \oplus A/\langle y_0, y_1, y_2, \ldots \rangle \\ &\cong \mathbf{Z}(p^\infty) \oplus \mathbf{Z}_{p^n} \\ &\cong (A, +).\end{aligned}$$

Consequently, $A \in \mathcal{K}$ but A is not a zero ring. If we now let F^o be the zero ring on F, then $G = (A \oplus F^o, +)$ where $A \oplus F^o$ is a non-trivial ring in $\mathcal{K}$. □

Corollary 5.3.2 *The class $\mathcal{K}$ is not hereditary.*

Proof: Using the notation of the second half of the proof of Theorem 5.3.1, where the reduced summand of the group is finite, we constructed a ring on $\mathbf{Z}_{p^n} \oplus \mathbf{Z}(p^\infty) = \langle x \rangle \oplus \langle y_0, y_1, y_2, \ldots \rangle$. Now we can see clearly that the ring on $\langle x \rangle \oplus \langle y_{n-1} \rangle$ is an ideal of the ring $A = \langle x \rangle \oplus \langle y_0, y_1, y_2, \ldots \rangle$. We know from that proof that A is in $\mathcal{K}$, regardless of the values of p or n. Furthermore, the ring on $\langle x \rangle \oplus \langle y_{n-1} \rangle$ is certainly not a zero ring. In the specific case of the group $\mathbf{Z}_2 \oplus \mathbf{Z}(2^\infty)$ we have $p = 2$ and $n = 1$ and so the additive group of the ideal $\langle x \rangle \oplus \langle y_{n-1} \rangle = \langle x \rangle \oplus \langle y_0 \rangle$ is isomorphic to $\mathbf{Z}_2 \oplus \mathbf{Z}_2$. We know, by Theorem 5.2.1, that for this group there is no non-trivial ring in $\mathcal{K}$. Thus the ideal $\langle x \rangle \oplus \langle y_{n-1} \rangle$ is not in $\mathcal{K}$. The result follows. □

We conclude this chapter with an example of a *mixed* group which supports a ring in $\mathcal{K}$. This ring was first studied by Szele in [39].

Given a prime p, consider the group $\mathbf{Q} \oplus \mathbf{Z}(p^\infty)$. This is a mixed group as the rationals are torsion-free while $\mathbf{Z}(p^\infty)$ is a p-group. Observe that any element of $\mathbf{Q}$ can be written in the form αp^{-k}, where $\alpha = \frac{r}{s}$ and p is not a factor of s. The set $\{\frac{r}{s} \,|\, r, s \in \mathbf{Z}, \gcd(p, s) = 1\}$ is sometimes denoted $\mathbf{Z}_{(p)}$. Secondly, as in

Theorem 5.3.1, note that $\mathbf{Z}(p^\infty) \cong \langle y_0, y_1, y_2, \ldots \rangle$ where $py_0 = 0$ and $py_i = y_{i-1}$ for all $i \in \mathbf{N}$. Finally, it is possible to show that $\mathbf{Z}(p^\infty)$ is a $\mathbf{Z}_{(p)}$-module: $\mathbf{Z}(p^\infty)$ is q-torsion-free for all primes $q \neq p$, whence division by q in $\mathbf{Z}(p^\infty)$ is uniquely defined, so that $\mathbf{Z}(p^\infty)$ has a natural $\mathbf{Z}_{(p)}$-module structure. Consequently it makes sense to talk about $\frac{r}{s}a$ for $\frac{r}{s} \in \mathbf{Z}_{(p)}$ and $a \in \mathbf{Z}(p^\infty)$.

Construct a ring on $\mathbf{Q} \oplus \mathbf{Z}(p^\infty)$ by defining multiplication *via*

$$(\alpha p^{-k}, a)(\beta p^{-m}, b) = (0, \alpha\beta y_{1+k+m}).$$

It is routine to confirm that this *is* a ring with a well-defined multiplication. Let $R_{ST,p}$ denote the ring so constructed.

Theorem 5.3.3 *The ring $R_{ST,p}$ is in $\mathcal{K}$.*

Proof: First of all, $R_{ST,p}$ is nilpotent of index 3. If a ring, A, satisfies $A^3 = 0$ then $A^2 \lhd A$, $(A^2)^2 = 0$ and $A/A^2 = 0$. We then have the following series of ideals

$$0 \subseteq A^2 \subseteq A;$$

but this is also a normal series for both $(A, +)$ and $(A, \circ)$ as groups (by Proposition 4.2.4). Consequently $(A, +)$ is an extension of $(A^2, +)$ by $(A/A^2, +)$, and similarly $(A, \circ)$ is an extension of $(A^2, \circ)$ by $(A/A^2, \circ)$. Furthermore $(A^2, +) \cong (A^2, \circ)$ and $(A/A^2, +) \cong (A/A^2, \circ)$ as both A^2 and A/A^2 are zero rings and thus in $\mathcal{K}$. We conclude that both $(A, +)$ and $(A, \circ)$ are both extensions of one group by another, noting that it is well-known that, in general, extensions in such a situation are not necessarily uniquely determined.

If we take the ring, $A = R_{ST,p}$, we note that $R_{ST,p}^2$ is the zero ring on $\mathbf{Z}(p^\infty)$, while $R_{ST,p}/R_{ST,p}^2$ is the zero ring on $\mathbf{Q}$, and so both $(R_{ST,p}, +)$ and $(R_{ST,p}, \circ)$ are extensions of $\mathbf{Z}(p^\infty)$ by $\mathbf{Q}$, and the *only* such extension is $\mathbf{Q} \oplus \mathbf{Z}(p^\infty)$. This is because $\mathbf{Z}(p^\infty)$ is divisible; the splitting extension is the only such extension

in this case. Thus $(R_{ST,p}, +) \cong (R_{ST,p}, \circ)$ and hence $R_{ST,p} \in \mathcal{K}$. $\square$

As mentioned above, $R_{ST,p}$ is nilpotent with index of nilpotence equal to 3; in addition, it has n-torsion only for $n = p$. In the next chapter we will consider nilpotent rings and the role of torsion in determining whether or not they are in $\mathcal{K}$. In particular, the results obtained there will show that $R_{ST,p}$ is in $\mathcal{K}$ for $p > 2$ by giving a specific isomorphism. Nevertheless, Theorem 5.3.3 is still needed in order to take care of the $p = 2$ case.

Chapter 6

More on nilpotent rings in $\mathcal{K}$

We will focus our attention on nilpotent rings in this chapter, showing in the first section that there exists a homomorphism between the additive and circle groups of *any* commutative nilpotent ring. In certain circumstances this homomorphism will be an isomorphism, enabling us to prove that every finitely generated **Q**-algebra is in $\mathcal{K}$. In a similar vein, but by using a different proof technique, we will also prove that every free commutative nilpotent **Z**-algebra of rank n is in $\mathcal{K}$. This leads to an example which shows that $\mathcal{K}$ is not homomorphically closed.

6.1 A homomorphism from $(R,+)$ to $(R,\circ)$

Lemma 6.1.1 *Let R be a commutative ring satisfying $R^{n+1}=0$. Then the function $p:(R,+)\to(R,\circ)$ defined by*

$$p(x)=\frac{(n!)^n}{n!}x^n+\frac{(n!)^{n-1}}{(n-1)!}x^{n-1}+\ldots+\frac{(n!)^3}{3!}x^3+\frac{(n!)^2}{2!}x^2+n!x$$

is a (group) homomorphism.

Proof: In the third step of the following computation we make use of the fact that $R^{n+1} = \{0\}$.

$$
\begin{aligned}
& p(x) \circ p(y) \\
&= \sum_{i=1}^{n} \frac{(n!)^i}{i!} x^i + \sum_{i=1}^{n} \frac{(n!)^i}{i!} y^i + \left(\sum_{i=1}^{n} \frac{(n!)^i}{i!} x^i \right) \left(\sum_{i=1}^{n} \frac{(n!)^i}{i!} y^i \right) \\
&= \sum_{i=1}^{n} \frac{(n!)^i}{i!} x^i + \sum_{i=1}^{n} \frac{(n!)^i}{i!} y^i + \\
&\quad \left[\frac{(n!)^n}{n!} x^n + \frac{(n!)^{n-1}}{(n-1)!} x^{n-1} + \ldots + \frac{(n!)^2}{2!} x^2 + n!x \right] \times \\
&\quad \left[\frac{(n!)^n}{n!} y^n + \frac{(n!)^{n-1}}{(n-1)!} y^{n-1} + \ldots + + \frac{(n!)^2}{2!} y^2 + n!y \right] \\
&= \sum_{i=1}^{n} \frac{(n!)^i}{i!} x^i + \sum_{i=1}^{n} \frac{(n!)^i}{i!} y^i + \frac{(n!)^{n-1}}{(n-1)!} x^{n-1} n!y + \\
&\quad \frac{(n!)^{n-2}}{(n-2)!} x^{n-2} \left[\frac{(n!)^2}{2!} y^2 + n!y \right] + \\
&\quad \frac{(n!)^{n-3}}{(n-3)!} x^{n-3} \left[\frac{(n!)^3}{3!} y^3 + \frac{(n!)^2}{2!} y^2 + n!y \right] + \ldots + \\
&\quad n!x \left[\frac{(n!)^{n-1}}{(n-1)!} y^{n-1} + \frac{(n!)^{n-2}}{(n-2)!} y^{n-2} + \ldots + \frac{(n!)^2}{2!} y^2 + n!y \right] \\
&\qquad \text{(expanding the product)} \\
&= \sum_{i=1}^{n} \frac{(n!)^i}{i!} x^i + \sum_{i=1}^{n} \frac{(n!)^i}{i!} y^i + \left[\frac{(n!)^n}{(n-1)!} x^{n-1} y + \right. \\
&\quad \left. \frac{(n!)^n}{(n-2)!2!} x^{n-2} y^2 + \frac{(n!)^n}{(n-3)!3!} x^{n-3} y^3 + \ldots + \frac{(n!)^n}{(n-1)!} x y^{n-1} \right] + \\
&\quad \left[\frac{(n!)^{(n-1)}}{(n-2)!} x^{n-2} y + \frac{(n!)^{(n-1)}}{(n-3)!2!} x^{n-3} y^2 + \ldots + \frac{(n!)^{(n-1)}}{(n-2)!} x y^{n-2} \right] + \ldots + \\
&\quad \left[\frac{(n!)^3}{2!} x^2 y + \frac{(n!)^3}{2!} x y^2 \right] + (n!)^2 xy \\
&\qquad \text{(after gathering terms of the same total degree} \\
&\qquad\quad \text{from the expanded product)} \\
&= \sum_{i=1}^{n} \frac{(n!)^i}{i!} x^i + \sum_{i=1}^{n} \frac{(n!)^i}{i!} y^i + \\
&\quad \frac{(n!)^n}{n!} \left[\tbinom{n}{1} x^{n-1} y + \tbinom{n}{2} x^{n-2} y^2 + \ldots + \tbinom{n}{n-1} x y^{n-1} \right] +
\end{aligned}
$$

$$
\begin{aligned}
& \frac{(n!)^{(n-1)}}{(n-1)!}\left[\tbinom{n-1}{1}x^{n-2}y+\tbinom{n-1}{2}x^{n-3}y^2+\ldots+\tbinom{n-1}{n-2}xy^{n-2}\right]+\ldots+ \\
& \frac{(n!)^3}{3!}\left[\tbinom{3}{1}x^2y+\tbinom{3}{2}xy^2\right]+\frac{(n!)^2}{2!}\tbinom{2}{1}xy \\
& \qquad \left(\text{since } \tbinom{m}{r}=\frac{m!}{(m-r)!r!}\ \right) \\
= \ & \frac{(n!)^n}{n!}\left[x^n+\tbinom{n}{1}x^{n-1}y+\ldots+\tbinom{n}{n-1}xy^{n-1}+y^n\right]+ \\
& \frac{(n!)^{(n-1)}}{(n-1)!}\left[x^{n-1}+\tbinom{n-1}{1}x^{n-2}y+\ldots+\tbinom{n-1}{n-2}xy^{n-2}+y^{n-1}\right]+\ldots+ \\
& \frac{(n!)^3}{3!}\left[x^3+\tbinom{3}{1}x^2y+\tbinom{3}{2}xy^2+y^3\right]+\frac{(n!)^2}{2!}\left[x^2+\tbinom{2}{1}xy+y^2\right] \\
& \qquad \left(\text{after incorporating the terms from the first two}\right. \\
& \qquad\qquad \left.\text{summation expressions}\right) \\
= \ & \frac{(n!)^n}{n!}(x+y)^n+\ldots+\frac{(n!)^k}{k!}(x+y)^k+\ldots+n!(x+y) \\
= \ & p(x+y)
\end{aligned}
$$

and thus p is a homomorphism. □

Because of the number and nature of the terms involved, and because it will be used extensively in what follows, we shall refer to this particular homomorphism as the *superhomomorphism*. It is essentially the only possible polynomial homomorphism between the additive and circle composition groups of an arbitrary commutative nilpotent ring. To see this, consider the free commutative nilpotent ring of rank 2, R, which satisfies $R^{n+1}=0\neq R^n$. We can write R as $R=\mathbf{Z}[X,Y]^-/I$, where $\mathbf{Z}[X,Y]^-$ is the set of all polynomials in 2 indeterminates X and Y having no term of degree zero, and I is the ideal generated by all products of length $n+1$. Let $x=X+I$ and $y=Y+I$ so that R is free with basis

$$\{x,y,x^2,xy,y^2,x^3,x^2y,xy^2,y^3,\ldots,x^n,\ldots,y^n\}.$$

Consider the polynomial function $p(z) = a_n z^n + a_{n-1} z^{n-1} + \ldots + a_1 z$. Then for $x, y \in R$ we have

$$\begin{aligned} & p(x) \circ p(y) \\ = \; & a_n x^n + a_{n-1} x^{n-1} + \ldots + a_1 x + a_n y^n + a_{n-1} y^{n-1} + \ldots + a_1 y \\ & + (a_n x^n + a_{n-1} x^{n-1} + \ldots + a_1 x) \cdot (a_n y^n + a_{n-1} y^{n-1} + \ldots + a_1 y) \\ = \; & \sum_{i=1}^{n} a_i (x^i + y^i) + \sum_{i=1}^{n} \sum_{j=1}^{n} a_i a_j x^i y^j \end{aligned}$$

while

$$\begin{aligned} & p(x + y) \\ = \; & a_n (x + y)^n + a_{n-1} (x + y)^{n-1} + \ldots + a_1 (x + y) \\ = \; & a_n (x^n + y^n) + a_{n-1} (x^{n-1} + y^{n-1}) + \ldots + a_1 (x + y) \\ & \quad + a_n \sum_{i=1}^{n-1} \tbinom{n}{i} x^i y^{n-i} + a_{n-1} \sum_{i=1}^{n-2} \tbinom{n-1}{i} x^i y^{n-1-i} + \ldots + 2a_2 xy \\ = \; & \sum_{i=1}^{n} a_i (x^i + y^i) + \sum_{k=2}^{n} \sum_{i+j=k} a_{i+j} \tbinom{i+j}{i} x^i y^j \end{aligned}$$

where $i, j > 0$. In the free nilpotent ring equality of expressions is determined by the degrees of the indeterminates and the associated coefficients. By considering the degrees of x and y we see that both expressions have the same terms involving just the one indeterminate x or y. For mixed terms, we find that in the former expression the coefficient of $x^i y^j$ is $a_i a_j$ and in the latter we have $\binom{i+j}{i} a_{i+j}$. Consequently the two expressions $p(x) \circ p(y)$ and $p(x + y)$ can only be equal — and p be a homomorphism — if

$$a_i a_j = \tbinom{i+j}{i} a_{i+j}.$$

An inductive proof then yields $n! a_n = a_1^n$ for all $n \in \mathbf{N}$. For the coefficients a_i to take integer values they must generally be of the form given in the superhomomorphism, give or take a negative sign, though occasionally smaller values for the coefficients than are given may work. For example, for a ring

satisfying $R^5 = 0$, the polynomial $p(x) = 864x^4 + 288x^3 + 72x^2 + 12x$ is an alternative homomorphism in addition to the superhomomorphism $p(x) = 13824x^4 + 2304x^3 + 288x^2 + 24x$; whereas if $R^4 = 0$ the polynomial $p(x) = -36x^3 + 18x^2 - 6x$ is the only other homomorphism in addition to the superhomomorphism $p(x) = 36x^3 + 18x^2 + 6x$.

Lemma 6.1.2 *If R is a commutative ring satisfying $R^{n+1} = \{0\}$ and having no a_1-torsion then any homomorphism $p : (R, +) \to (R, \circ)$ of the form*

$$p(x) = a_n x^n + a_{n-1}x^{n-1} + \ldots + a_2 x^2 + a_1 x, \quad a_i \in \mathbf{Z}$$

is injective.

Proof: If $p(x) = 0$ then $a_2x^2 = -a_nx^n - a_{n-1}x^{n-1} - \ldots - a_3x^3 - a_1x$. Since $R^{n+1} = 0$ we have

$$\begin{aligned} 0 &= x^{n+1} = a_2x^{n+1} = (a_2x^2)x^{n-1} \\ &= (-a_nx^n - a_{n-1}x^{n-1} - \ldots - a_3x^3 - a_1x)x^{n-1} = -a_1x^n. \end{aligned}$$

Consequently $x^n = 0$ because R has no a_1-torsion. Having $x^n = 0$ implies that $p(x) = a_{n-1}x^{n-1} + \ldots + a_2x^2 + a_1x$ and using both these facts and repeating the procedure just applied we will obtain $x^{n-1} = 0$. Continuing in this manner we will eventually obtain $x = 0$. Thus $p(x) = 0$ implies that $x = 0$, whence p is injective. □

In order to relate this result to the superhomomorphism we need to talk about rings which are $n!$-torsion-free. However, a ring is k-torsion-free if and only if it is p-torsion-free for all primes p such that $p|k$, and for $k = n!$ we thus have $p|n!$ if and only if $p \leq n$. We conclude that a ring is $n!$-torsion-free if and only if it is p-torsion-free for all primes $p \leq n$.

The following result is immediate as a consequence of the previous comments and the preceding pair of lemmas.

Corollary 6.1.3 *If R is a commutative ring satisfying $R^{n+1} = \{0\}$ and having no p-torsion for all primes $p \leq n$ then*

$$p(x) = \frac{(n!)^n}{n!}x^n + \frac{(n!)^{n-1}}{(n-1)!}x^{n-1} + \ldots + \frac{(n!)^3}{3!}x^3 + \frac{(n!)^2}{2!}x^2 + n!x$$

is an injective homomorphism from $(R, +)$ to $(R, \circ)$. □

Corollary 6.1.4 *If R is a finite commutative ring satisfying $R^{n+1} = \{0\}$ and having no p-torsion for primes $p \leq n$ then $R \in \mathcal{K}$.*

Proof: An injective homomorphism from $(R, +)$ to $(R, \circ)$ where R is finite is an isomorphism. □

A natural question to ask concerns the status of finite nilpotent rings satisfying $R^{n+1} = 0$ which *do* have p-torsion for $p \leq n$. As the following examples show we cannot tell whether they are in $\mathcal{K}$ or not from these conditions alone.

For instance, if $R = \mathbf{Z}_8^4$ (see page 85 in Section 5.1) then R is a finite commutative ring satisfying $R^3 = \{0\}$ and which is in $\mathcal{K}$ by Theorem 5.1.8. However, it has 2-torsion, and so the conditions of the corollary are sufficient, but not necessary.

On the other hand, consider the Cauchy convolution quasifield, F, constructed on $P = (\{0, 1, 2\}, \leq)$ with $\mathbf{Z}_2$ as the underlying ring. This, too, has 2-torsion and satisfies $F^3 = 0$ by Theorem 3.2.4. However, by Corollary 3.5.2 $f^2(1) = (f(1))^2 \neq 0$ for some $f \in F$, and so Theorem 3.1.1 reveals that $F \notin \mathcal{K}$.

If the ring R is infinite, then the homomorphism may not be surjective. To see this, consider (as a specific instance of a more general situation) the quasifield F, constructed on the poset $P = (\{0, 1, 2\}, \leq)$ with underlying ring $K = \mathbf{Z}$. This is torsion-free and because of the poset's finite height satisfies $F^3 = 0$ by Theorem 3.2.4. However, the polynomial $p(x) = 2x^2 + 2x$, which is the corresponding homomorphism for this index of nilpotence, is not surjective. This is because all functions in F which are images of p will take only even

values in $\mathbf{Z}$. As it turns out, this particular example *is* in $\mathcal{K}$ by the results of Section 2.3.

Before we apply the superhomomorphism to quasifields, let us briefly consider the ring of Szele constructed on $\mathbf{Q} \oplus \mathbf{Z}(p^\infty)$ as discussed in Theorem 5.3.3, which is an example of an infinite ring. Recall that this ring is nilpotent of index 3. For odd primes the ring $R_{ST,p}$ has no 2-torsion and so the superhomomorphism $p(x) = 2x^2 + 2x$ is injective by Corollary 6.1.3. However, it is also surjective since

$$2(\alpha p^{-k}, a)^2 + 2(\alpha p^{-k}, a) = (2\alpha p^{-k}, 2a + 2\alpha^2 y_{1+2k})$$

and given $(\beta p^{-m}, b)$ we can determine α, k and a so that $(2\alpha p^{-k}, 2a+2\alpha^2 y_{1+2k}) = (\beta p^{-m}, b)$. Consequently $R_{ST,p} \in \mathcal{K}$, although we knew this already from Theorem 5.3.3. On the other hand, $R_{ST,2}$ has 2-torsion, and so we cannot use the results of this section. Nevertheless, we also know that this ring is in $\mathcal{K}$ as well.

We conclude this section by examining the role of the superhomomorphism for certain quasifields.

Lemma 6.1.5 *Suppose F is a quasifield constructed on a poset satisfying (w5) in addition to the usual poset conditions and in which the underlying ring is a_1-divisible. Then the function*

$$p(x) = a_n x^n + a_{n-1} x^{n-1} + \ldots + a_2 x^2 + a_1 x, \quad a_i \in \mathbf{Z}$$

is surjective.

Proof: [In this proof recall the notation of Section 2.2: e_y, y and z denote poset elements, f and g denote elements of the quasifield, and h denotes the height function which acts on poset elements; $(w5)$ is defined on page 74.]

Lemma 3.2.1 states that when taking the product of $n+1$ elements of the poset constructed quasifields we obtain $(f_1 f_2 \cdots f_{n+1})(y) = 0$ for all non-minimal y of height less than or equal to n. We wish to prove that for any $g \in F$ there exists $f \in F$ such that $p(f) = a_n f^n + a_{n-1} f^{n-1} + \ldots + a_2 f^2 + a_1 f = g$.

For $g \in F$ we define f inductively: $f(y) = g(y)/a_1$ if y has height one, and if y is of height k then

$$f(y) = \frac{1}{a_1}\left(g(y) - \sum_{i=1}^{k}\left[a_{i+1}\sum_{e_y<z<y} f(z)f^i(w(y,z))\right]\right),$$

where $a_{k+1} = 0$ for all $k \geq n$. Since the poset satisfies $(w5)$ — a property satisfied by all the posets described in the examples of Section 2.2 — we have that $h(w(y,z)) < h(y)$ for $e_y < z < y$. The computation of terms like $f^i(w(y,z))$ will involve the evaluation of $f(t)$ for various values of t which are smaller in height than $w(y,z)$ and hence y, and so the expression on the right hand side is well-defined.

Suppose that $y \in P$ has height one. Then

$$\begin{aligned}(p(f))(y) &= (a_n f^n + a_{n-1}f^{n-1} + \ldots + a_2 f^2 + a_1 f)(y)\\ &= a_n(f^n(y)) + a_{n-1}(f^{n-1}(y)) + \ldots + a_2(f^2(y)) + a_1 f(y)\\ &= a_1 f(y) = g(y)\end{aligned}$$

since $(f^k)(y)$ vanishes for $k > h(y) = 1$ by the aforementioned Lemma 3.2.1.

If $y \in P$ has height k then $f^i(y) = \sum_{e_y<z<y} f(z)f^{i-1}(w(y,z))$, and note that $f^m(y)$ vanishes for $m > h(y) = k+1$. We then have

$$\begin{aligned}(p(f))(y) &= (a_{k+1}f^{k+1} + a_k f^k + \ldots + a_2 f^2 + a_1 f)(y)\\ &= a_{k+1}\sum_{e_y<z<y} f(z)f^k(w(y,z)) + a_k \sum_{e_y<z<y} f(z)f^{k-1}(w(y,z))\\ &\quad + \ldots + a_2 \sum_{e_y<z<y} f(z)f(w(y,z)) +\\ &\quad a_1 \times \frac{1}{a_1}\left(g(y) - \sum_{i=1}^{k}\left[a_{i+1}\sum_{e_y<z<y} f(z)f^i(w(y,z))\right]\right)\\ &= g(y) + \sum_{i=1}^{k}\left[a_{i+1}\sum_{e_y<z<y} f(z)f^i(w(y,z))\right] -\\ &\quad \sum_{i=1}^{k}\left[a_{i+1}\sum_{e_y<z<y} f(z)f^i(w(y,z))\right]\end{aligned}$$

which is $g(y)$ as required. Thus p is surjective. □

Corollary 6.1.6 *If F is a quasifield constructed on a poset of height n which satisfies (w5) and if the underlying ring K is p-divisible and has no p-torsion for all primes $p \leq n$ then $F \in \mathcal{K}$.*

Proof: Since the poset is of height n we have $F^{n+1} = \{0\}$ by Theorem 3.2.4. The fact that the underlying ring has no p-torsion guarantees that F itself has no p-torsion because addition is defined pointwise. Then by the lemmas and corollary of this section we have that

$$p(f) = \frac{(n!)^n}{n!}f^n + \frac{(n!)^{n-1}}{(n-1)!}f^{n-1} + \ldots + \frac{(n!)^3}{3!}f^3 + \frac{(n!)^2}{2!}f^2 + n!f \text{ for } f \in F$$

is an isomorphism from $(F, +)$ to $(F, \circ)$, whence $F \in \mathcal{K}$ as required. □

Note that we already knew this in the case of K being an algebra over the rationals for the quasifields constructed using sets, Dirichlet convolution and Cauchy convolution where the height of the poset is finite. (The results here do not help us for the complete (infinite) posets, but we already know from Section 2.2 that those quasifields are in $\mathcal{K}$.) The only specific gains are for the finite height version of the polynomials over the integers example, where K no longer has to be restricted to $\mathbf{R}$ in order to have an isomorphism, and, in the other examples, we can relax the condition that K be an algebra over the rationals.

6.2 Free nilpotent Q-algebras

The results of this section deal with commutative nilpotent $\mathbf{Q}$-algebras, and, in the next chapter, allow us to take care of all commutative *nil* $\mathbf{Q}$-algebras. We note that Kruse, in [25], has shown that every finitely generated commutative *quasiregular* ring, in fact, is nilpotent.

Theorem 6.2.1 *Every free commutative nilpotent* $\mathbf{Q}$*-algebra of rank n is in $\mathcal{K}$.*

Proof: The free (commutative) $\mathbf{Q}$-algebra of rank n in the variety of nilpotent rings of index $k+1$ — denoted by $\mathrm{VAR}(y_1 y_2 \ldots y_{k+1} = 0)$ — is

$$F_n = \mathbf{Q}[X_1, X_2, \ldots, X_n]^- / I$$

where $\mathbf{Q}[X_1, X_2, \ldots, X_n]^-$ is the set of all polynomials over the rationals in the indeterminates $X_1, X_2, \ldots, X_n$ having no term of degree zero, and

$$I = (\{X_{i_1} X_{i_2} \ldots X_{i_{k+1}} \,|\, 1 \leq i_j \leq n\})$$

is the ideal generated by all products of length $k+1$.

Let $u_i = X_i + I$ for all i. Then F_n is a $\mathbf{Q}$-algebra with basis

$$\{u_{i_1}, u_{i_1} u_{i_2}, \ldots, u_{i_1} u_{i_2} \ldots u_{i_k} \,|\, i_j \in \{1, 2, \ldots, n\} \ \forall j \ \text{ and } i_1 \leq i_2 \leq \ldots \leq i_j\}.$$

An element $x \in F_n$ can be written in the form

$$\begin{aligned} x &= \sum a_{i_1} u_{i_1} + \sum a_{i_1 i_2} u_{i_1} u_{i_2} + \ldots + \sum a_{i_1 i_2 \ldots i_k} u_{i_1} u_{i_2} \ldots u_{i_k} \\ &= A_1 + A_2 + \ldots + A_k \end{aligned}$$

where $A_m = \sum a_{i_1 i_2 \ldots i_m} u_{i_1} u_{i_2} \ldots u_{i_m}$. Note that all terms in A_m have degree m. Now by the multinomial theorem, which is a generalisation of the binomial theorem (see, for example, [36], pp. 16–17), we have

$$x^j = (A_1 + A_2 + \ldots + A_k)^j = \sum \frac{j!}{t_1! \ldots t_k!} A_1^{t_1} A_2^{t_2} \ldots A_k^{t_k}$$

where the sum extends over all non-negative integers t_i such that $\sum t_i = j$. Bearing in mind that all products of length greater than or equal to $k+1$ vanish we have the additional requirement that $\sum i t_i \leq k$, since this ensures that the degree of $A_1^{t_1} A_2^{t_2} \ldots A_k^{t_k}$ is no more than k.

Since F_n is a torsion-free ring which is nilpotent of index $k+1$, by Corollary 6.1.3 the following is an injective homomorphism from $(F_n, +)$ to $(F_n, \circ)$.

$$p(x) = \frac{(k!)^k}{k!} x^k + \frac{(k!)^{k-1}}{(k-1)!} x^{k-1} + \ldots + \frac{(k!)^3}{3!} x^3 + \frac{(k!)^2}{2!} x^2 + k! x$$

$$
\begin{aligned}
= \quad & \frac{(k!)^k}{k!} \sum \frac{k!}{t_1! \ldots t_k!} A_1^{t_1} A_2^{t_2} \ldots A_k^{t_k} && \text{[line } (*k)\text{]} \\
& + \frac{(k!)^{k-1}}{(k-1)!} \sum \frac{(k-1)!}{t_1! \ldots t_k!} A_1^{t_1} A_2^{t_2} \ldots A_k^{t_k} && \text{[line } (*(k-1))\text{]} \\
& + \ldots + \frac{(k!)^2}{2!} \sum \frac{2!}{t_1! \ldots t_k!} A_1^{t_1} A_2^{t_2} \ldots A_k^{t_k} && \text{[line } (*2)\text{]} \\
& + k! \sum \frac{1!}{t_1! \ldots t_k!} A_1^{t_1} A_2^{t_2} \ldots A_k^{t_k} && \text{[line } (*1)\text{]}
\end{aligned}
$$

where for the summand indicated in line $(*j)$ of the above expression we have the following constraints: $\sum t_i = j$ and $\sum i t_i \leq k$. We note that $\sum i t_i$ gives the degree of the basis elements involved in any particular expression.

We will take an arbitrary element, y, of F_n and show that there exists $x \in F_n$ such that $p(x) = y$, thus demonstrating that the function p is an isomorphism. Suppose that

$$
\begin{aligned}
y &= \sum b_{i_1} u_{i_1} + \sum b_{i_1 i_2} u_{i_1} u_{i_2} + \ldots + \sum b_{i_1 i_2 \ldots i_k} u_{i_1} u_{i_2} \ldots u_{i_k} \\
&= B_1 + B_2 + \ldots + B_k
\end{aligned}
$$

where $B_j = \sum b_{i_1 i_2 \ldots i_k} u_{i_1} u_{i_2} \ldots u_{i_k}$, again noting that B_j contains all the terms of degree j.

Define

$$
\begin{aligned}
x &= \sum a_{i_1} u_{i_1} + \sum a_{i_1 i_2} u_{i_1} u_{i_2} + \ldots + \sum a_{i_1 i_2 \ldots i_k} u_{i_1} u_{i_2} \ldots u_{i_k} \\
&= A_1 + A_2 + \ldots + A_k
\end{aligned}
$$

inductively via $a_{i_1} = \frac{1}{k!} b_{i_1}$ for all $i_1 \in \{1, 2, \ldots, n\}$ and

$$
a_{i_1 \ldots i_m} = \frac{1}{k!} \left[b_{i_1 \ldots i_m} - \sum_{j=2}^{m} c_{j, i_1 \ldots i_m} \right]
$$

where $c_{j, i_1 \ldots i_m}$ is the coefficient of $u_{i_1} u_{i_2} \ldots u_{i_m}$ in

$$
\frac{(k!)^j}{j!} \sum \frac{j!}{t_1! t_2! \ldots t_{m-1}!} A_1^{t_1} A_2^{t_2} \ldots A_{m-1}^{t_{m-1}}
$$

and the terms in this summation satisfy $\sum i t_i = m$. Note that all the terms in said summation involve coefficients of the form $a_{i_1 \ldots i_s}$ where $s < m$, so that it *is*

a satisfactory inductive definition. We shall prove that $p(x) = y$ by considering the terms of degree m in both $p(x)$ and y. In y the terms of degree m are in $B_m = \sum b_{i_1 i_2 \ldots i_m} u_{i_1} u_{i_2} \ldots u_{i_m}$, while in $p(x)$ the situation is more complicated! We shall consider which lines of the expansion of $p(x)$ contain such terms.

In line (*1) of the expansion of $p(x)$ above there is only one occurrence of a degree m term, namely when $t_m = 1$ and all other $t_i = 0$. (Note that this choice of values for the t_i yields $\sum i t_i = m t_m = m \leq k$ as required by the second of the constraints.) Thus line (*1) gives us the term $k! \frac{1!}{1!} A_m = k! \sum a_{i_1 i_2 \ldots i_m} u_{i_1} u_{i_2} \ldots u_{i_m}$ and the $a_{i_1 i_2 \ldots i_m}$ terms are given by the inductive definition of x.

In considering now line $(*j)$ we note that we cannot have $j > m$. This is because the constraints require that $\sum t_i = j$, but since the degree of any expression for some choice of the t_i is given by $\sum i t_i$ and we are interested in those terms satisfying $\sum i t_i = m$ we would have a contradiction since $\sum i t_i \geq \sum t_i$ for non-negative t_i. Consequently we turn our attention only to those lines $(*j)$ where $j \leq m$. In these lines terms of degree m can arise in possibly more than one way; all that we require is a choice of values for the t_i such that $\sum t_i = j$ and $\sum i t_i = m$. [So, for example, with $m = 5$ and $j = 3$ we can have $\{t_1 = 1, t_2 = 2,$ and $t_i = 0$ for $i = 3, \ldots, k\}$ and $\{t_1 = 2, t_3 = 1$ and $t_i = 0$ for $i = 2, 4, 5, \ldots, k\}$. This gives rise to two sets of degree five terms on line (*3), namely $\frac{3!}{1!2!} A_1 A_2^2$ and $\frac{3!}{2!1!} A_1^2 A_3$.]

Now, we observe that given various choices of t_i on line $(*j)$ we have terms like $\sum \frac{j!}{t_1! \ldots t_k!} A_1^{t_1} A_2^{t_2} \ldots A_k^{t_k}$; however, we cannot have a factor of A_l for any $l > m$ since otherwise (if $t_l > 0$) we would have $\sum i t_i \geq l t_l \geq l > m$ and so the degree of the term would be larger than the requisite m. Moreover, the factor A_m can only be involved on line (*1). This follows because if $t_m \neq 0$ then to satisfy $\sum i t_i = m$ we must have $t_m = 1$ and all other $t_i = 0$ from which we have $\sum t_i = 1$ and hence we must be on line (*1). Thus on line $(*j)$, where $1 < j \leq m$, terms

of degree m involve expressions like $\frac{j!}{t_1!\ldots t_{m-1}!}A_1^{t_1}A_2^{t_2}\ldots A_{m-1}^{t_{m-1}}$, and each of the A_s will involve the coefficients $a_{i_1}, a_{i_1 i_2}, \ldots, a_{i_1 i_2 \ldots i_{m-1}}$, all of which are given by the definition of x. Consequently *all* the terms of degree m in $p(x)$ are given by

$$k!A_m + \sum_{j=2}^{m}\left(\frac{(k!)^j}{j!}\left[\sum \frac{j!}{t_1!\ldots t_{m-1}!}A_1^{t_1}A_2^{t_2}\ldots A_{m-1}^{t_{m-1}}\right]\right)$$

where the sum is over all choices of t_i such that $\sum it_i = m$. Now

$$\begin{aligned}
&k!A_m + \sum_{j=2}^{m}\left(\frac{(k!)^j}{j!}\left[\sum \frac{j!}{t_1!\ldots t_{m-1}!}A_1^{t_1}A_2^{t_2}\ldots A_{m-1}^{t_{m-1}}\right]\right)\\
&= k!\sum a_{i_1 i_2 \ldots i_m}u_{i_1}u_{i_2}\ldots u_{i_m}\\
&\qquad + \sum_{j=2}^{m}\left(\frac{(k!)^j}{j!}\left[\sum \frac{j!}{t_1!\ldots t_{m-1}!}A_1^{t_1}A_2^{t_2}\ldots A_{m-1}^{t_{m-1}}\right]\right)\\
&= k!\sum \frac{1}{k!}\left[b_{i_1\ldots i_m} - \sum_{j=2}^{m} c_{j,i_1\ldots i_m}\right]u_{i_1}u_{i_2}\ldots u_{i_m}\\
&\qquad + \sum_{j=2}^{m}\left(\frac{(k!)^j}{j!}\left[\sum \frac{j!}{t_1!\ldots t_{m-1}!}A_1^{t_1}A_2^{t_2}\ldots A_{m-1}^{t_{m-1}}\right]\right)\\
&= \sum b_{i_1\ldots i_m}u_{i_1}u_{i_2}\ldots u_{i_m} - \sum\sum_{j=2}^{m} c_{j,i_1\ldots i_m}u_{i_1}u_{i_2}\ldots u_{i_m}\\
&\qquad + \sum_{j=2}^{m}\left(\frac{(k!)^j}{j!}\left[\sum \frac{j!}{t_1!\ldots t_{m-1}!}A_1^{t_1}A_2^{t_2}\ldots A_{m-1}^{t_{m-1}}\right]\right)\\
&= \sum b_{i_1\ldots i_m}u_{i_1}u_{i_2}\ldots u_{i_m}
\end{aligned}$$

because of the definition of $c_{j,i_1\ldots i_m}$ and its relationship to

$$\sum_{j=2}^{m}\left(\frac{(k!)^j}{j!}\left[\sum \frac{j!}{t_1!\ldots t_{m-1}!}A_1^{t_1}A_2^{t_2}\ldots A_{m-1}^{t_{m-1}}\right]\right).$$

We conclude that p is surjective, and therefore the algebra F_n is in $\mathcal{K}$. □

Corollary 6.2.2 *Every finitely generated nilpotent* **Q***-algebra is in* $\mathcal{K}$.

Proof: Every finitely generated **Q**-algebra satisfying $y_1y_2\ldots y_{k+1} = 0$ is a homomorphic image of some F_n (F_n as in Theorem 6.2.1). Suppose A is such a finitely generated **Q**-algebra with $\phi : F_n \to A$ a surjective ring homomorphism

for some appropriate F_n. Now A satisfies the requirements for the superhomomorphism of Corollary 6.1.3 to be injective; all we need to do is show that it is surjective. For $a \in A$ there exists $x \in F_n$ such that $a = \phi(x)$. Also, since the superhomomorphism is known to be surjective in F_n by Theorem 6.2.1 then there exists a $y \in F_n$ such that $x = \frac{(k!)^k}{k!}y^k + \frac{(k!)^{k-1}}{(k-1)!}y^{k-1} + \frac{(k!)^3}{3!}y^3 + \frac{(k!)^2}{2!}y^2 + k!y$. It follows that

$$\begin{aligned}
&\frac{(k!)^k}{k!}(\phi(y))^k + \frac{(k!)^{k-1}}{(k-1)!}(\phi(y))^{k-1} + \frac{(k!)^3}{3!}(\phi(y))^3 + \frac{(k!)^2}{2!}(\phi(y))^2 + k!\phi(y) \\
&= \frac{(k!)^k}{k!}\phi(y^k) + \frac{(k!)^{k-1}}{(k-1)!}\phi(y^{k-1}) + \frac{(k!)^3}{3!}\phi(y^3) + \frac{(k!)^2}{2!}\phi(y^2) + k!\phi(y) \\
&= \phi(\frac{(k!)^k}{k!}y^k + \frac{(k!)^{k-1}}{(k-1)!}y^{k-1} + \frac{(k!)^3}{3!}y^3 + \frac{(k!)^2}{2!}y^2 + k!y) \\
&= \phi(x) = a
\end{aligned}$$

and so the superhomomorphism in A is surjective. Thus there exists an isomorphism from $(A, +)$ to $(A, \circ)$ and hence every finitely generated nilpotent $\mathbf{Q}$-algebra is in $\mathcal{K}$. □

6.3 Free nilpotent Z-algebras

In this section we will obtain the analogue of Theorem 6.2.1 for free nilpotent $\mathbf{Z}$-algebras. However our approach is necessarily different: the superhomomorphism need not be surjective. As an example, consider a free $\mathbf{Z}$-algebra which is nilpotent of index three. The homomorphism $p(x) = 2x^2 + 2x$ is injective by Corollary 6.1.3, but produces only elements with even coefficients and so cannot be surjective.

The other main outcome will be a proof that $\mathcal{K}$ is not homomorphically closed.

We begin with a lemma which indicates what quasi-inverses look like in a nilpotent ring.

Lemma 6.3.1 *If R is a ring satisfying $R^{k+1} = 0$ then*

$$u^{\circ m} = (1+u)^m - 1 = mu + \frac{m(m-1)}{2!}u^2 + \ldots + \frac{m(m-1)\ldots(m-k+1)}{k!}u^k$$

for all $m \in \mathbf{Z}$.

Proof: For $m \in \mathbf{N}$ the result has already been discussed in Section 1.2; for $m = 0$ the result is obvious. For $m \in \mathbf{N}$ observe that in a nilpotent ring

$$u^{\circ(-1)} = -u + u^2 - u^3 + \ldots + (-1)^k u^k$$

and that $u^{\circ(-m)} = (u^{\circ(-1)})^{\circ m}$. Then we have

$$(u^{\circ(-1)})^{\circ m} = \sum_{r=1}^{m} \tbinom{m}{r} (-u + u^2 - u^3 + \ldots + (-1)^k u^k)^r.$$

Let us consider where the coefficients of u^j arise. In expanding the expression $(-u + u^2 - u^3 + \ldots + (-1)^k u^k)^r$ before worrying about gathering terms or multiplying together the powers of u, we will obtain expressions like

$$(-1)^{i_1} u^{i_1} (-1)^{i_2} u^{i_2} \cdots (-1)^{i_r} u^{i_r}.$$

So, to obtain a u^j term we require $i_1 + i_2 + \ldots + i_r = j$. Now the number of ways of partitioning j into r natural numbers $i_1, i_2, \ldots, i_r$ to satisfy this condition is $\binom{j-1}{r-1}$. (To see this, imagine j dots and $r-1$ dividers placed among the $j-1$ spaces between the dots to partition j as required.) Thus the coefficient of u^j arising from $(-u + u^2 - u^3 + \ldots + (-1)^k u^k)^r$ is $(-1)^j \binom{j-1}{r-1}$, and so the coefficient of u^j in the whole expression is

$$(-1)^j \left[m + \tbinom{m}{2}\tbinom{j-1}{1} + \tbinom{m}{3}\tbinom{j-1}{2} + \ldots + \tbinom{m}{j-1}\tbinom{j-1}{j-2} + \tbinom{m}{j}\tbinom{j-1}{j-1} \right] = (-1)^j \sum_{i=1}^{j} \tbinom{j-1}{i-1}\tbinom{m}{i}.$$

By [36] (pages 209 and 15) and using the notation there we have

$$\sum_{i=1}^{j} \tbinom{j-1}{i-1}\tbinom{m}{i} = \left(\!\tbinom{m}{j}\!\right) = \tbinom{m+j-1}{j}.$$

Now

$$\begin{aligned}(-1)^j\binom{m+j-1}{j} &= (-1)^j\frac{(m+j-1)(m+j-2)\dots(m+1)m}{j!}\\ &= \frac{(-m-j+1)(-m-j+2)\dots(-m-1)(-m)}{j!}\\ &= \frac{(-m)(-m-1)\dots(-m-j+2)(-m-j+1)}{j!}\end{aligned}$$

and so, for $m \in \mathbf{N}$ we have

$$u^{\circ(-m)} = -mu + \frac{-m(-m-1)}{2!}u^2 + \ldots + \frac{-m(-m-1)\dots(-m-k+1)}{k!}u^k$$

as required. □

Alternatively, we could have proved this result using the work of Niven [29] on formal power series rings, using techniques similar to those employed in Lemma 7.1.3.

Theorem 6.3.2 *Every free commutative nilpotent* $\mathbf{Z}$*-algebra of rank* n *is in* $\mathcal{K}$.

Proof: We will now consider the free (commutative) $\mathbf{Z}$-algebra of rank n in $\mathrm{VAR}(y_1y_2\dots y_{k+1}=0)$, the variety of nilpotent rings of index $k+1$. In similar fashion to the previous section, we will denote this by

$$F_n = \mathbf{Z}[X_1, X_2, \dots, X_n]^-/I$$

where $\mathbf{Z}[X_1, X_2, \dots, X_n]^-$ is the set of all polynomials in the n indeterminates $X_1, X_2, \dots, X_n$ having no term of degree zero, and

$$I = (\{X_{i_1}X_{i_2}\dots X_{i_{k+1}} \mid 1 \le i_j \le n\})$$

is the ideal generated by all products of length $k+1$.

Let $u_i = X_i + I$ for all i. Then $(F_n, +)$ is free abelian with basis

$$B = \{u_{i_1}, u_{i_1}u_{i_2}, \dots, u_{i_1}u_{i_2}\dots u_{i_k} \mid i_j \in \{1,2,\dots,n\}\ \forall j \text{ and } i_1 \le i_2 \le \ldots \le i_j\}.$$

We will show that this set is also a basis for $(F_n, \circ)$.

We will use Lemma 6.3.1 in what follows; in addition, we need to establish the result of circle composing a number of elements. Recall (see page 36) that we use $\coprod$ for circle composition in the same way that $\sum$ and Π are used for addition and multiplication respectively. It can be shown, using induction, that

$$\coprod_{i=1}^{n} a_i = \sum_{i=1}^{n} a_i + \sum_{i_1<i_2} a_{i_1}a_{i_2} + \sum_{i_1<i_2<i_3} a_{i_1}a_{i_2}a_{i_3} + \ldots + a_1a_2\ldots a_n \qquad (*)$$

where the i_j values are taken from the set $\{1, 2, \ldots, n\}$.

To show that B is a basis for $(F_n, \circ)$ we shall demonstrate that we can find values for $m_{i_1 i_2 \ldots i_j}$ such that

$$\begin{aligned}\coprod_{i_1} u_{i_1}^{\circ m_{i_1}} \circ \coprod_{i_1\le i_2} (u_{i_1}u_{i_2})^{\circ m_{i_1 i_2}} \circ \ldots \circ \coprod_{i_1\le i_2\le\ldots\le i_k} (u_{i_1}u_{i_2}\ldots u_{i_k})^{\circ m_{i_1 i_2\ldots i_k}} \\ = \sum a_{i_1}u_{i_1} + \sum a_{i_1 i_2}u_{i_1}u_{i_2} + \ldots + \sum a_{i_1 i_2\ldots i_k}u_{i_1}u_{i_2}\ldots u_{i_k} \qquad (\dagger)\end{aligned}$$

where, as before, the i_j values are taken from the set $\{1, 2, \ldots, n\}$ and where the expression on the right hand side is an arbitrary element of F_n. We will proceed by induction on the degree of the basis elements, and we shall denote the left and right sides of equation (†) by LHS(†) and RHS(†) respectively.

The degree one terms of RHS(†) come from the $\sum a_{i_1}u_{i_1}$ term, while the only term on LHS(†) contributing such terms when that side is expanded is $\coprod_{i_1} u_{i_1}^{\circ m_{i_1}}$. Now by (*) we have

$$\coprod_{i_1} u_{i_1}^{\circ m_{i_1}} = \sum u_{i_1}^{\circ m_{i_1}} + \sum u_{i_1}^{\circ m_{i_1}} u_{i_2}^{\circ m_{i_2}} + \text{terms of higher degree}$$

and in this the degree one terms come from $\sum u_{i_1}^{\circ m_{i_1}}$ which equals

$$\sum (m_{i_1}u_{i_1} + \frac{m_{i_1}(m_{i_1}-1)}{2!}u_{i_1}^2 + \ldots + \frac{m_{i_1}(m_{i_1}-1)\ldots(m_{i_1}-k+1)}{k!}u_{i_1}^k)$$

from which it can be seen that the degree one terms are simply $\sum m_{i_1}u_{i_1}$. It follows that we must have $m_{i_1} = a_{i_1}$ for all $i_1 \in \{1, 2, \ldots, n\}$.

Now assume that we have all the values $m_{i_1}, m_{i_1 i_2}, \ldots, m_{i_1 i_2 \ldots i_{j-1}}$; we will prove that we can determine $m_{i_1 i_2 \ldots i_j}$ by considering the terms of degree j. In RHS(†) such terms arise from $\sum a_{i_1 i_2 \ldots i_j} u_{i_1} u_{i_2} \ldots u_{i_j}$. To ascertain what happens in LHS(†) we will expand it using (*) while ignoring nilpotence for the moment.

$$
\begin{aligned}
&\text{LHS}(\dagger) \\
&= \ (\sum u_{i_1}^{\circ m_{i_1}} + \sum u_{i_1}^{\circ m_{i_1}} u_{i_2}^{\circ m_{i_2}} + \ldots + u_{i_1}^{\circ m_{i_1}} u_{i_2}^{\circ m_{i_2}} \ldots u_{i_n}^{\circ m_{i_n}}) \qquad (\dagger 1) \\
&\quad \circ (\sum (u_{i_1} u_{i_2})^{\circ m_{i_1 i_2}} + \sum (u_{i_1} u_{i_2})^{\circ m_{i_1 i_2}} (u_{i_3} u_{i_4})^{\circ m_{i_3 i_4}} + \ldots) \qquad (\dagger 2) \\
&\quad \circ (\sum (u_{i_1} u_{i_2} u_{i_3})^{\circ m_{i_1 i_2 i_3}} + \\
&\qquad \sum (u_{i_1} u_{i_2} u_{i_3})^{\circ m_{i_1 i_2 i_3}} (u_{i_4} u_{i_5} u_{i_6})^{\circ m_{i_4 i_5 i_6}} + \ldots) \qquad (\dagger 3) \\
&\quad \circ \ldots \circ (\sum (u_{i_1} \ldots u_{i_j})^{\circ m_{i_1 \ldots i_j}} + \\
&\qquad \sum (u_{i_1} \ldots u_{i_j})^{\circ m_{i_1 \ldots i_j}} (u_{i_{j+1}} \ldots u_{i_{2j}})^{\circ m_{i_{j+1} \ldots i_{2j}}} + \ldots) \qquad (\dagger j) \\
&\quad \circ \ldots \circ (\sum (u_{i_1} \ldots u_{i_k})^{\circ m_{i_1 \ldots i_k}} + \\
&\qquad \sum (u_{i_1} \ldots u_{i_k})^{\circ m_{i_1 \ldots i_k}} (u_{i_{k+1}} \ldots u_{i_{2k}})^{\circ m_{i_{k+1} \cdots i_{2k}}} + \ldots) \qquad (\dagger k)
\end{aligned}
$$

where there are various restrictions on the values of the i_s being used, arising from (*) and the types of basis elements in B. After further expansion, LHS(†) will comprise sums and products of the given terms, and so we can seek out those terms of degree j.

For rows $(\dagger(j+1))$ to $(\dagger k)$ there will be no such terms, as the degrees of all the terms here are greater than j. In row $(\dagger j)$, the only j^{th} degree terms will arise from $\sum (u_{i_1} u_{i_2} \ldots u_{i_j})^{m_{i_1 i_2 \ldots i_j}}$; in particular, after expanding $(u_{i_1} u_{i_2} \ldots u_{i_j})^{m_{i_1 i_2 \ldots i_j}}$ using the binomial result, the only terms will be $\sum m_{i_1 i_2 \ldots i_j} (u_{i_1} u_{i_2} \ldots u_{i_j})$. Note that this expression contains the sought after $m_{i_1 i_2 \ldots i_j}$ coefficients.

The remaining (very large quantity of) j^{th} degree terms will come from sums and products of terms within and between the rows $(\dagger 1)$ to $(\dagger(j-1))$. For example, in row $(\dagger 1)$ the expansion of each $u_{i_1}^{\circ m_{i_1}}$ could have a degree j term (depending on the value of m_{i_1}) as could the expansion of $u_{i_1}^{\circ m_{i_1}} u_{i_2}^{\circ m_{i_2}}$, and so on.

Furthermore, terms from row (†1) will multiply with terms from higher rows too, to give j^{th} degree terms when all the remaining circle composition operations are carried out; and the same applies to other rows as well. However, all these additional terms of degree j involve the coefficients $m_{i_1}, m_{i_1 i_2}, \ldots, m_{i_1 i_2 \ldots i_{j-1}}$ which are assumed to be known by the inductive hypothesis. Thus on equating the j^{th} degree terms on LHS(†) with those from RHS(†) the $m_{i_1 i_2 \ldots i_j}$ coefficients can be determined.

We conclude that B generates $(F_n, \circ)$. Moreover, it is clear from the above arguments that if

$$0 = \coprod_{i_1} u_{i_1}^{\circ m_{i_1}} \circ \coprod_{i_1 \leq i_2} (u_{i_1} u_{i_2})^{\circ m_{i_1 i_2}} \circ \ldots \circ \coprod_{i_1 \leq i_2 \leq \ldots \leq i_k} (u_{i_1} u_{i_2} \ldots u_{i_k})^{\circ m_{i_1 i_2 \ldots i_k}}$$

then all the coefficients $m_{i_1 i_2 \ldots i_j}$ must be zero. Thus B is, in fact, a basis for $(F_n, \circ)$ whence $(F_n, \circ)$ is free abelian with the same rank as $(F_n, +)$. We then have $(F_n, +) \cong (F_n, \circ)$, so that $F_n \in \mathcal{K}$. □

Theorem 6.3.3 *$\mathcal{K}$ is not homomorphically closed.*

Proof: As in the previous theorem, let F_n denote the free commutative $\mathbf{Z}$-algebra of rank n which has index of nilpotence $k+1$. Choose a prime p such that $p \leq k$. Then $F_n/pF_n = \mathbf{Z}_p[v_1, v_2, \ldots, v_n]$ where $v_i = u_i + pF_n$ (where the u_i are as defined in Theorem 6.3.2). Now F_n/pF_n is obviously a $\mathbf{Z}_p$-algebra; however, since $p \leq k$, we do not have $v_i^p = 0$ and so by Theorem 3.1.1 we conclude that $F_n/pF_n \notin \mathcal{K}$ and the result follows. □

Note that the results of Section 2.3 are still required. The quasifields therein are constructed on finite posets with $\mathbf{Z}$ as the underlying ring, and are finitely generated nilpotent $\mathbf{Z}$-algebras. However, even though such a ring is a homomorphic image of one of the free nilpotent $\mathbf{Z}$-algebras of Theorem 6.3.2, Theorem 6.3.3 implies that there is no guarantee that this quasifield is in $\mathcal{K}$. We should

note, too, that while the approaches used in Theorem 6.3.2 and the section considering the quasifields is similar, there may be multiplicative identities relating basis elements in the quasifield case. As a particular example, in the quasifield F over $\mathbf{Z}$ constructed on the poset $P = (\{0, 1, 2\}, \leq)$ and using the notation of Section 2.3, the identity $(\varepsilon_1)^2 = \varepsilon_2$ holds.

Chapter 7

More on rational algebras

7.1 Nil and complete rational algebras

We have already considered numerous examples in which the groups $(R, +)$ and $(R, \circ)$ are essentially the same; in this chapter we will investigate further the question of how similar or different these groups can be for different kinds of quasiregular rings. Torsion properties will be of particular interest.

In discussing the group properties of $(R, \circ)$ we may occasionally use the prefix *quasi*, so that, for example, we shall say that R is quasitorsion-free if $(R, \circ)$ is torsion-free.

We shall be begin by considering an example to see how different the additive and circle composition groups can be in a commutative Jacobson radical ring. The definitive example of a commutative quasiregular ring is

$$R = \{\frac{2m}{2n+1} \mid m, n \in \mathbf{Z}\},$$

colloquially referred to as the ring of evens over odds. It is a quasiregular subring of the rationals. In [1] Amberg and Dickenschied point out that the additive group of this ring has Prüfer rank 1 (which means that every finitely generated

subgroup of $(R, +)$ can be generated by one element), while the circle group has infinite torsion-free rank. In addition, we observe that there is no torsion in the additive group (being a subgroup of the rationals), while the element -2 has 2-torsion in the circle group. We will clarify and prove these claims for a family of quasiregular subrings of $\mathbf{Q}$ which are generalisations of the evens over the odds.

Example 7.1.1 *In generalisations of the ring of evens over odds, the additive and circle composition groups have different ranks.*

Proof: Let p be a prime, and consider

$$H_p = \{\frac{m}{n} \mid m, n \in \mathbf{Z}, m \equiv n \not\equiv 0 (\text{mod } p); \quad \gcd(m, n) = 1\},$$

$$G_p = \{\frac{m}{n} \mid m, n \in \mathbf{Z}, \text{and } p \not| \, n \neq 0 \text{ and } p \mid m\}.$$

It is easy to show that G_p is a quasiregular subring of $\mathbf{Q}$, with G_2 being the familiar "evens over odds" example; while H_p is a subgroup of $(\mathbf{Q}\backslash\{0\}, \cdot)$. If $\frac{m}{n} \in G_p$ then it follows that $1 + \frac{m}{n} \in H_p$, since $1 + \frac{m}{n} = \frac{n+m}{n}$ and because $p \mid m$ implies that $n + m \equiv n (\text{mod } p)$. On the other hand, given $\frac{m}{n} \in H_p$ then $\frac{m}{n} = \frac{n+m-n}{n} = 1 + \frac{m-n}{n}$, where, firstly, p cannot divide n as $n \not\equiv 0 (\text{mod } p)$ and, secondly, having $m \equiv n (\text{mod } p)$ causes p to be a factor of $m - n$. We conclude that $\frac{m-n}{n} \in G_p$ and, hence, $H_p = \{1 + x \mid x \in G_p\}$.

Define the function $f : G_p \to H_p$ by $f(x) = 1+x$. This function is a bijection and, furthermore, $f(x)f(y) = (1+x)(1+y) = 1+x+y+xy = 1+x\circ y = f(x\circ y)$ for all $x, y \in G_p$. Therefore $(G_p, \circ) \cong (H_p, \cdot)$, and so we can study $(G_p, \circ)$ by considering $(H_p, \cdot)$.

To determine the elements of finite order in H_p we find those values of x for which $x^k = 1$, and since we are dealing with rational (and, hence, real) numbers we must have $x = \pm 1$. If $x = 1 + \frac{m}{n} = \pm 1$ then $\frac{m}{n} = 0$ or -2, with the conditions $p|m$ and $p \not| \, n$ implying that $p = 2$ for non-triviality. Thus G_p is torsion-free if

p is odd. For $p = 2$ the torsion subgroup of G_2 is $\langle -2 \rangle = \{-2, 0\}$, which is a direct summand, for example because $\langle -1 \rangle = \langle 1 + (-2) \rangle$ is a direct summand of $(\mathbf{Q}\backslash\{0\}, \cdot)$ and hence of $(H_p, \cdot)$.

Now $(\mathbf{Q}\backslash\{0\}, \cdot)$ is $\langle -1 \rangle \oplus \langle p \mid p \text{ prime} \rangle$ with the primes generating a free group. Since $H_p \cap \langle -1 \rangle = \{1\}$ in the case that p is odd, we have, by one of the group isomorphism theorems,

$$\begin{aligned} H_p &\cong H_p/(H_p \cap \langle -1 \rangle) \cong (H_p + \langle -1 \rangle)/\langle -1 \rangle \\ &\subseteq \langle -1 \rangle \oplus \langle p \mid p \text{ prime} \rangle / \langle -1 \rangle \cong \langle \text{p} \mid \text{p prime} \rangle. \end{aligned}$$

It follows that H_p, and hence $(G_p, \circ)$, is free of rank $\aleph_o$. This contrasts with $(G_p, +)$ which, as a subset of $(\mathbf{Q}, +)$, has rank 1. For $p = 2$, $(G_2, +)$ also has rank 1, while $(G_2, \circ)$ is the direct sum of $\mathbf{Z}_2$ and an abelian group which is free of rank $\aleph_o$. This means that the additive group of G_p is a homomorphic image of the circle composition group but not vice versa. □

In [1] (Theorem B) Amberg and Dickenschied showed that for a Jacobson radical ring, R, if $(R, \circ)$ has finite torsion-free rank (i.e. has finite rank when the torsion subgroup has been factored out) then so does $(R, +)$ and, in fact, R is nil and the ranks are equal. In addition, they have shown ([1], Lemma 2.4) that if R is a nil ring then $(R, +)$ is torsion-free if and only if $(R, \circ)$ is torsion-free, and if p is a prime then $(R, +)$ is a p-group if and only if $(R, \circ)$ is a p-group.

In the case of a quasiregular ring which is a $\mathbf{Q}$-algebra we do not need the assumption of nilness in order for the ring's circle group to inherit the property of being torsion-free as the next result shows.

Theorem 7.1.2 *If R is a quasiregular $\mathbf{Q}$-algebra then $(R, \circ)$ is torsion-free.*

Proof: Suppose $a^{\circ n} = 0$ for some $n \in \mathbf{Z}^+$. Then

$$0 = a^n + na^{n-1} + \tbinom{n}{2}a^{n-2} + \ldots + \tbinom{n}{2}a^2 + na$$

and hence $na = -a^n - na^{n-1} - \binom{n}{2}a^{n-2} - \ldots - \binom{n}{2}a^2$. If we now write $c = \frac{1}{n}(-a^{n-1} - na^{n-2} - \binom{n}{2}a^{n-3} - \ldots - \binom{n}{2}a)$ we have $a = ca = ac$. Since R is quasiregular there exists $d \in R$ such that $0 = (-c) \circ d = -c + d - cd$, and so, on multiplying by a, we obtain $0 = -ac + ad - acd = -a + ad - ad = -a$. Thus $(R, \circ)$ is torsion-free. □

Divisibility plays a critical role in the above proof. If we have only that R is (additively) torsion-free then it *is* possible for the circle group to have torsion as is shown by -2 in the example of the evens over odds.

In order to return to nil rings which are also $\mathbf{Q}$-algebras we need to consider algebras on which a metric can be defined. Suppose that A is a $\mathbf{Q}$-algebra satisfying $\cap_{n \in \mathbf{Z}^+} A^n = 0$. We can define the *$A$-adic metric*, d, on A as follows:

$$d(x,y) = \begin{cases} 2^{-\max\{m \,|\, x-y \in A^m\}}, & \text{if this exists;} \\ 0, & \text{if } x - y \in A^m \text{ for all } m, \text{ i.e. } x = y. \end{cases}$$

Since $\cap_{n \in \mathbf{Z}^+} A^n = 0$, it follows that d *is* a metric; in more general rings and algebras it is a pseudometric.

We note that if a ring R is complete in the R-adic metric then it is, in fact, quasiregular (see Lam [27], Remark 21.30, page 330).

Lemma 7.1.3 *If R is a commutative $\mathbf{Q}$-algebra which is complete in the R-adic metric, then $(R, \circ)$ is divisible.*

Proof: Consider the ring, $\mathbf{Q}[[X]]$, of formal power series over the rationals, and in this ring let $\sigma = 1 + \frac{1}{n}X + \frac{\frac{1}{n}(\frac{1}{n}-1)}{2}X^2 + \frac{\frac{1}{n}(\frac{1}{n}-1)(\frac{1}{n}-2)}{3}X^3 + \ldots$ be a rational series for $n \in \mathbf{Z}^+$. Then, by Theorem 11 of [29], we have $\sigma = (1+X)^{\frac{1}{n}}$ and hence $\sigma^n = 1 + X$. If we set $\tau = \sigma - 1$ then $1 + X = \sigma^n = (\tau + 1)^n$ and so $X = (\tau + 1)^n - 1 = \tau^{\circ n}$ in $\mathbf{Q}[[X]]$ and also $X\mathbf{Q}[[X]]$, the latter being the ring of power series over the rationals having zero constant term.

Note that $X\mathbf{Q}[X]$, the ring of *polynomials* with zero constant term, is a

free algebra on X. It follows that for any $a \in R$ there exists a homomorphism $f : X\mathbf{Q}[X] \to R$ with $f(r_1X + r_2X^2 + \ldots r_tX^t) = r_1a + r_2a^2 + \ldots r_ta^t$.

Let τ_m denote the m^{th} partial sum of τ for all $m \in \mathbf{Z}^+$. Then each τ_m is in $X\mathbf{Q}[X]$, so we can consider $f(\tau_m)$. If $m_1 > m_2$ then $X^{m_2+1}|(\tau_{m_1} - \tau_{m_2})$, so in R we have $a^{m_2+1}|(f(\tau_{m_1}) - f(\tau_{m_2})) = f(\tau_{m_1} - \tau_{m_2})$. It follows that $f(\tau_{m_1}) - f(\tau_{m_2}) \in R^{m_2+1}$ and, hence, for every $l \in \mathbf{Z}^+$ we obtain $f(\tau_{m_1}) - f(\tau_{m_2}) \in R^{m_2+1} \subseteq R^l$ whenever $m_1 > m_2 > l$. Since we now have $d(f(\tau_{m_1}), f(\tau_{m_2})) \leq 2^{-l}$ for all $m_1 > m_2 > l$, we deduce that $\langle f(\tau_m) \rangle$ is a Cauchy sequence in R. Finally, since R is complete, there exists $c \in R$ such that $\lim_{m\to\infty} f(\tau_m) = c$.

Returning to $X\mathbf{Q}[X]$, consider the $X\mathbf{Q}[X]$-adic metric, which we shall denote by d as well (this is also known as the X-adic or (X)-adic metric). For $l \in \mathbf{Z}^+$, if $t \in X\mathbf{Q}[X]$ and $d(t, X) < 2^{-l}$, then $t - X \in (X\mathbf{Q}[X])^{l+1}$. We then have $f(t) - a = f(t) - f(X) = f(t - X) \in R^{l+1}$ and thus $d(f(t), a) \leq 2^{-(l+1)} < 2^{-l}$. Hence f is continuous at X. However, since f is a group homomorphism and d is invariant in both algebras (which is to say that $d(x, y) = d(x + z, y + z)$ for all x, y, z), we see that f is actually uniformly continuous everywhere in $X\mathbf{Q}[X]$.

Since $X\mathbf{Q}[X]$ is dense in $X\mathbf{Q}[[X]]$, and $X\mathbf{Q}[[X]]$ is closed in $\mathbf{Q}[[X]]$, we deduce that $X\mathbf{Q}[[X]]$ is a completion of $X\mathbf{Q}[X]$ for the X-adic metric. Hence there is a homomorphism $\hat{f} : X\mathbf{Q}[[X]] \to R$ which extends f and, furthermore, $\hat{f}$ is continuous. In $X\mathbf{Q}[[X]]$ we have $\lim_{m\to\infty} \tau_m = \tau$ for some τ in $X\mathbf{Q}[[X]]$, and then, by continuity, we have

$$\hat{f}(\tau) = \hat{f}(\lim_{m\to\infty} \tau_m) = \lim_{m\to\infty} \hat{f}(\tau_m) = c.$$

However, upon recalling that $\tau^{\circ n} = X$, we obtain $c^{\circ n} = (\hat{f}(\tau))^{\circ n} = \hat{f}(\tau^{\circ n}) = \hat{f}(X) = f(X) = a$. Thus, for all $a \in R$ and $n \in \mathbf{Z}^+$ there exists $c \in R$ such that $a = c^{\circ n}$, and so $(R, \circ)$ is divisible. □

Corollary 7.1.4 *If R is a nilpotent $\mathbf{Q}$-algebra then $(R, \circ)$ is divisible.*

Proof: Nilpotence implies that the R-adic metric is discrete (as there exists some n such that $R^m = 0$ for all $m \geq n$), and discrete metrics are complete. □

Corollary 7.1.5 *If R is a commutative nil* $\mathbf{Q}$*-algebra then $(R, \circ)$ is divisible.*

Proof: For any $b \in R$ let $\langle b \rangle$ denote the $\mathbf{Q}$-subalgebra generated by b. Then, as R is nil, $\langle b \rangle$ is nilpotent and so $(\langle b \rangle, \circ)$ is divisible by Corollary 7.1.4. Therefore, for all $n \in \mathbf{Z}^+$ there exists a $c \in \langle b \rangle \subseteq R$ such that $b = c^{\circ n}$. □

As a consequence of this result and Theorem 7.1.2 we see that any ring which is a nil $\mathbf{Q}$-algebra has a torsion-free divisible circle composition group. It is well-known that such a group is a $\mathbf{Q}$-vector space and, with the additive group having the same property, the question of whether or not the two groups are isomorphic again arises. The question is settled by considering the size and dimensions of the groups; this will be the outcome of Theorem 7.1.8. The difficult case is when the dimension of the additive group is countably infinite, and so some important lemmas will precede the final conclusion.

Lemma 7.1.6 *Let R be a commutative nilpotent* $\mathbf{Q}$*-algebra of dimension $\aleph_0$. Then R is in $\mathcal{K}$.*

Proof: Since R is a nilpotent $\mathbf{Q}$-algebra it is nil and so, by [1], Lemma 2.4 (or Theorem 7.1.2) and Corollary 7.1.5, $(R, \circ)$ is torsion-free and divisible. Furthermore, R (being torsion-free) satisfies the conditions of Corollary 6.1.3, so there exists an injective homomorphism, f, from $(R, +)$ to $(R, \circ)$ such that $f(x)$ is a polynomial in x for all $x \in R$. It follows that $(R, +) \cong \mathrm{Im}(f) \subseteq (R, \circ)$, and thus $\aleph_0 = \dim(R, +) \leq \dim(R, \circ) \leq \aleph_0$. We cannot have $\dim(R, \circ) > \aleph_0$ because then $|R|$ would be uncountably infinite, which is impossible since it is a $\mathbf{Q}$-algebra with a countably infinite basis (for addition). We conclude that $(R, +) \cong (R, \circ)$, as required. □

Lemma 7.1.7 *Suppose that R is a commutative nil* $\mathbf{Q}$*-algebra of dimension* $\aleph_0$*. Then* $R \in \mathcal{K}$*.*

Proof: Note that once again [1], Lemma 2.4 (or Theorem 7.1.2) and Corollary 7.1.5 reveal that $(R, \circ)$ is torsion-free and divisible, and so, like the additive group, is a $\mathbf{Q}$-vector space. We need to show that the dimension of $(R, \circ)$ is $\aleph_0$, which we do by showing it cannot be finite. (A dimension larger than $\aleph_0$ is impossible for the same reasons as explicated at the end of the previous proof.) If R is nilpotent the result follows from Lemma 7.1.6. Suppose, then, that R is *not* nilpotent and that $\{u_1, u_2, \ldots\}$ is a basis. Since R is nil it is locally nilpotent, and so all finitely generated subrings are nilpotent, whence R cannot be generated as an algebra by $\{u_1, \ldots u_n\}$ for any n. Let R_n denote the algebra generated by $\{u_1, \ldots u_n\}$ for all n. Then we must have $R_1 \subseteq R_2 \subseteq \ldots$ and $R = R_1 \cup R_2 \cup \ldots$. Thus there must exist infinitely many indices $n_1 < n_2 < \ldots$ such that $\dim(R_{n_1}) < \dim(R_{n_2}) < \ldots < \dim(R_{n_i}) < \ldots$. Now R_{n_i} is nilpotent for all i and so by Corollary 6.1.3 there is an injective homomorphism $f_i : (R_{n_i}, +) \to (R_{n_i}, \circ)$ and $(R_{n_i}, \circ) \subseteq (R, \circ)$ for all i. Hence $\dim(R, \circ) \geq \dim(R_{n_i}, \circ) \geq \dim(R_{n_i}, +)$, again for all i, which implies that $\dim(R, \circ)$ is infinite. Thus $(R, +)$ and $(R, \circ)$ are both $\mathbf{Q}$-vector spaces of dimension $\aleph_0$ and so $(R, +) \cong (R, \circ)$. □

Theorem 7.1.8 *All commutative nil* $\mathbf{Q}$*-algebras are in* $\mathcal{K}$*.*

Proof: Let R be a commutative nil $\mathbf{Q}$-algebra. If $\dim(R)$ is finite then R is nilpotent and, because it is finite dimensional, it is in $\mathcal{K}$ by Corollary 6.2.2. If $\dim(R) = \aleph_0$ then Lemma 7.1.7 yields the desired result. Finally, if $\dim(R) > \aleph_0$ then $\dim(R) = |R|$ and so $\dim(R, +) = |(R, +)| = |(R, \circ)| = \dim(R, \circ)$ and we again have $(R, +) \cong (R, \circ)$. □

Let us return to rings which are complete in their ring-adic metrics. By the Baire category theorem (see, for example, [24], if R is complete in the R-adic

metric then either R is uncountable or the R-adic metric is discrete. For, if R is countable then for some $a \in R$ $\{a\}$ has non-empty interior, so is open, whence by continuity of addition, all singletons are open.

Proposition 7.1.9 *If a commutative ring R is a* $\mathbf{Q}$*-algebra which is complete in the R-adic metric then R is in $\mathcal{K}$.*

Proof: By Theorems 7.1.2 and 7.1.3 $(R, \circ)$ is torsion-free and divisible. Now if R is uncountable then, since $\mathbf{Q}$ is countable it follows that $(R, +)$ and $(R, \circ)$ have uncountable dimension and are thus isomorphic. On the other hand, if R is not uncountable then the R-adic metric must be discrete. This implies that the ring is nilpotent. In the case that R has countably infinite dimension as a $\mathbf{Q}$-algebra we can invoke Lemma 7.1.6 to conclude that $R \in \mathcal{K}$. Finally, if R has finite dimension as a $\mathbf{Q}$-algebra, then Corollary 6.2.2 is applicable, and $R \in \mathcal{K}$ in this case, too. □

For the following example — from which we will deduce that quasiregular subrings of rings in $\mathcal{K}$ need not be in $\mathcal{K}$ — we will consider the ring of *p-adic integers* for some prime p. This can be thought of as the set of formal sums of the form $a_0 + a_1 p + a_2 p^2 + a_3 p^3 + \ldots$ where $a_i \in \{0, 1, 2, \ldots, p-1\}$, with addition and multiplication carried out term-wise modulo the appropriate powers of p. We shall denote this ring by $\mathbf{I}_p$. The p-adic integers are a subset of the p-adic numbers; this set is the completion of the rationals with respect to the *p-adic metric* which on $\mathbf{I}_p$ is defined by

$$d(x, y) = \begin{cases} p^{-\max\{m \mid p^m \text{ divides } x-y\}}, & \text{if this exists;} \\ 0, & \text{if } x = y. \end{cases}$$

The p-adic integers, like their rational integer counterparts, are torsion-free. For additional information on p-adic numbers and their topological properties see [35] or [23].

It is straightforward to show that the Jacobson radical of the p-adic integers is $\mathcal{J}(\mathbf{I}_p) = p\mathbf{I}_p$. Denote this by J. We note that $(\mathbf{I}_p, +) \cong (p\mathbf{I}_p, +)$ using $x \mapsto px$ (cf. Example 7.1.1). Then

$$(J, \circ) \cong (\{1 + x \,|\, x \in J\}, \cdot) \subseteq U(\mathbf{I}_p)$$

where $U(\mathbf{I}_p)$ is the group of units of $\mathbf{I}_p$ and the isomorphism is *via* $x \mapsto 1 + x$. Denote by V_p the set $\{1+x \,|\, x \in J\}$ so that, on rewriting, we have $(J, \circ) \cong (V_p, \cdot)$. Since $J = p\mathbf{I}_p$ we see that V_p is the set of units of $\mathbf{I}_p$ which are congruent to $1 \pmod p$. Karpilovsky ([21], pages 473–4) shows that in the case where p is odd, $(V_p, \cdot) \cong (\mathbf{I}_p, +)$ and so

$$(J, +) = (p\mathbf{I}_p, +) \cong (\mathbf{I}_p, +) \cong (V_p, \cdot) \cong (J, \circ).$$

On the other hand, if $p = 2$ then [21] proves $(V_2, \cdot) \cong \mathbf{I}_2 \times \mathbf{Z}_2$ so $(J, \circ) \cong \mathbf{I}_2 \times \mathbf{Z}_2$. Consequently $(J, \circ)$ (or, equivalently, $(V_p, \cdot)$) is torsion-free if and only if $p \neq 2$; furthermore, $J = \mathcal{J}(\mathbf{I}_p) \in \mathcal{K}$ if and only if $p \neq 2$.

We now examine whether or not J is complete in the p-adic topology. First, observe that since $J = p\mathbf{I}_p$ everything in J has the form px for $x \in \mathbf{I}_p$. Then, $J^n = p^{n-1}J = p^n\mathbf{I}_p$ for all $n \in \mathbf{N}$. Thus in J the p-adic and the J-adic (see page 125) topologies coincide. Second, J is a closed set in $\mathbf{I}_p$. To see this we point out that J is an open ball with radius 1 and centre 0 since $d(x, 0) = p^{-\max\{m \,|\, p^m \text{ divides } x-y\}} \leq p^{-1} < 1$ for $x \in J = p\mathbf{I}_p$. However, J is also a subgroup of $\mathbf{I}_p$, and if a subgroup is open then so are its cosets. What is more, any union of open sets is open (this is true in any topological space). Now, $\mathbf{I}_p \backslash J = \cup_{x \notin J}(x+J)$ which is a union of cosets of J. Thus $\mathbf{I}_p \backslash J$ is open, whence J is closed in $\mathbf{I}_p$.

So, since J *is* a closed set in a complete metric space, we see that J itself is complete in the p-adic — and hence the J-adic — metric (see [24], Theorem 1.4-7).

In the case that $p = 2$ we can now see that J is torsion-free, J-adically

complete but *not* in $\mathcal{K}$ since we showed that $(J, \circ) \cong \mathbf{I}_2 \times \mathbf{Z}_2$ which has 2-torsion. This contrasts with Proposition 7.1.9, where we showed that any ring R which is torsion-free, R-adically complete *and* divisible *is* in $\mathcal{K}$.

On the other hand, if p is odd we have a ring J which is complete in the J-adic metric and is also in $\mathcal{K}$ but which has a quasiregular subring which is not in $\mathcal{K}$, as the following result shows.

Theorem 7.1.10 *There exists a ring in $\mathcal{K}$ with a quasiregular subring not in $\mathcal{K}$.*

Proof: In the previous example we showed that if p is an odd prime then $J = \mathcal{J}(I_p) = p\mathbf{I}_p$ is in $\mathcal{K}$. The set $\{\frac{m}{n} \mid p \text{ does not divide } n\}$ is a subring of $\mathbf{I}_p$. This is because it is possible to find values of $a_0, a_1, a_2, a_3, \ldots$ to solve $m = n(a_0 + a_1 p + a_2 p^2 + a_3 p^3 + \ldots)$. The set $\{\frac{pm}{n} \mid p \text{ does not divide } n\}$ is then a quasiregular subring of J. However, this ring is not in $\mathcal{K}$ by the results of Example 7.1.1. □

Let us return to the torsion properties of the additive and circle composition groups of nil rings. Note that the quasifield construction can yield rings which are not nil (see, for example, Theorems 3.5.3 and 3.5.6). However, we have the following.

Proposition 7.1.11 *Suppose F is a quasifield, with underlying ring K. If K is torsion-free [divisible] then F is quasitorsion-free [quasidivisible].*

Proof: In what follows, $f \in F$, $x, y \in P$, where P is the partially ordered set on which the quasifield is constructed, and e_x is the minimal element of P which is less than x. Recall, too, that $\#(x)$ is the number of elements of P less than or equal to x.

We shall deal with the torsion-free property first, proving that if $f^{\circ n} = \delta$ then $f = \delta$, i.e. $f(x) = 0$ for all $x \notin \mathrm{Min}(P)$. Now,

$$f^{\circ n} = f^n + \tbinom{n}{1} f^{n-1} + \tbinom{n}{2} f^{n-2} + \ldots + nf,$$

while Corollary 3.2.2 shows that $f^n(x) = 0$ for all elements x with height less than n. If x is such that $\#(x) = 1$ ($= h(x)$) then from $f^{\circ n} = \delta$ we have $0 = f^{\circ n}(x) = nf(x)$ whence $f(x) = 0$ as K is torsion-free. Now suppose that $f(x) = 0$ for all x such that $\#(x) \leq k - 1$, and consider x with $\#(x) = k$. Since $f^m(x) = \sum_{e_x < y < x} f^{m-1}(y) f(w(x, y))$ (for $m \geq 2$) and the properties of P together with $(w4)$ imply that $\#(y), \#(w(x, y)) < \#(x)$ we conclude that $f^m(x)$ is a function of values of $f(y)$ where $\#(y) < \#(x) = k$. The inductive hypothesis then implies $f^m(x) = 0$ for $m \geq 2$, and so $f^{\circ n}(x) = nf(x)$. This can only equal 0 when $f(x) = 0$; hence we see that $f = \delta$ and so $(F, \circ)$ is torsion-free.

To prove the inheritance of divisibility, we need to show that for any $n \in \mathbf{N}$ and $g \in F$ we can find $f \in F$ such that $f^{\circ n} = g$. It is easy to verify that for height one elements we must have $f(x) = \frac{g(x)}{n}$, with the remaining values defined inductively on $\#(x)$ via $f(x) = \frac{1}{n}(g(x) - f^n(x) - \binom{n}{1} f^{n-1}(x) - \ldots - \binom{n}{2} f^2(x))$. The terms on the right hand side exist since, as before, $f^m(x)$ depends only on values of $f(y)$ where $\#(y) < \#(x)$. □

So for quasifields we see that $(R, +)$ torsion-free and divisible implies that $(R, \circ)$ is torsion-free and divisible.

We will now show that it is possible for a commutative quasiregular ring to have torsion, but to be quasitorsion-free.

Theorem 7.1.12 *The complete Cauchy convolution ring over* $\mathbf{Z}_p$ *(p prime) is a torsion ring which is quasitorsion-free.*

Proof: Given $f \in F$ suppose k is the least natural number such that $f(k) \neq 0$. Now for $m \geq 2$ we have $f^m(k) = \sum_{1 \leq r < k} f(r) f^{m-1}(k-r) = 0$, and so $f^{\circ n}(k) = f^n(k) + \binom{n}{1} f^{n-1}(k) + \ldots + nf(k) = nf(k)$. It follows that in order to have $f^{\circ n} = \delta$ we must have $p|n$. Let $n = p^s r$ where $s \in \mathbf{N}$ and p does not divide r. Then, by Lemma 1.2.4, where we showed that $\binom{p^s r}{j}$ always has at least one factor of p except when p^s divides j, we see that

$$\begin{aligned} & f^{\circ p^s r}(p^s k) \\ &= f^{p^s r}(p^s k) + \tbinom{p^s r}{1} f^{p^s r - 1}(p^s k) + \ldots + \tbinom{p^s r}{2} f^2(p^s k) + p^s r f(p^s k) \\ &= f^{p^s r}(p^s k) + \tbinom{p^s r}{p^s} f^{(r-1)p^s}(p^s k) + \tbinom{p^s r}{2p^s} f^{(r-2)p^s}(p^s k) + \ldots \\ &\qquad + \tbinom{p^s r}{jp^s} f^{(r-j)p^s}(p^s k) + \ldots + \tbinom{p^s r}{p^s(r-1)} f^{p^s}(p^s k) \\ &= \tbinom{p^s r}{p^s(r-1)} f^{p^s}(p^s k) \end{aligned}$$

since, by Lemma 3.5.1, $f^m(t) = 0$ for $t < mk$, and we have $p^s k < (r-i)p^s k$ for $0 \leq i \leq r-2$. Applying the first part of Lemma 3.5.1 to the remaining term yields $f^{\circ p^s r}(p^s k) = \binom{p^s r}{p^s(r-1)} f^{p^s}(p^s k) = \binom{p^s r}{p^s(r-1)} (f(p^s k))^{p^s} \neq 0$, from which we conclude that $(F, \circ)$ is torsion-free. $\square$

Chapter 8

Semigroup properties of $(R, \circ)$

Throughout most of this thesis we have been studying Jacobson radical rings; we reiterate that such a ring, R, is characterized by the fact that its circle composition semigroup $(R, \circ)$ is a group, and, moreover, that group is abelian in the case that the multiplication in the ring is commutative.

In [7], Clark introduced the idea of a *generalised radical* ring in which $(R, \circ)$ is a union of groups. Among other things he showed that rings which are strongly regular (with respect to multiplication) are generalised radical rings. Du Xiankun, in [13], investigated these rings further, and, in [14], considered *adjoint regular* rings in which $(R, \circ)$ is a regular semigroup, showing, for example, that regular rings are adjoint regular.

In this chapter we will use an approach similar to that of Section 2.2 to construct an additional class of examples of quasiregular rings, and also indicate that in certain circumstances it is possible to obtain rings in which $(R, \circ)$ is regular. We will conclude by showing that neither the class of adjoint regular rings nor the class of generalised radical rings is a radical class.

8.1 Collapsing monoids

In Section 2.2 our aim was to construct rings in such a way that the circle composition operation gave rise to a group. The construction relied, in part, on the properties of the underlying partially ordered set. In this Section we will construct some more quasiregular rings by considering rings constructed on a class of commutative monoids — these monoids will play a role analogous to that of the posets in the quasifield construction. The construction is developed from the idea of generalized power series rings as outlined by Ribenboim in, for example, [32] and [33], and is also related to the results of Chapter 2. Following this, in the next section we will adapt these ideas to show the construction of rings in which the circle composition semigroup is regular, i.e. for each $a \in R$ there exists $b \in R$ such that $a = a \circ b \circ a$.

Let S be a commutative monoid which we shall write additively, so the identity is 0. For every $s \in S$ define the set $X_s = \{(t, u) \in S \times S \mid t + u = s\}$. Furthermore let S satisfy the following conditions:

(CM1): $X_0 = \{(0, 0)\}$;

(CM2): X_s is finite for all $s \in S$; and

(CM3): $|X_u| < |X_s|$ whenever $u \neq s$ is such that there exists $t \in S$ with $(t, u) \in X_s$.

(CM4): $(u, s), (s, u) \in X_s$ if and only if $u = 0$.

[Note that (CM1) is equivalent to the assertion that X_0 is the only subgroup of S.]

We shall give the name *collapsing* monoid to any commutative monoid satisfying (CM1) to (CM4). Later we shall show that there are a number of naturally occurring examples of such monoids.

Theorem 8.1.1 *Let S be a collapsing monoid, K a ring. Let F be the set of all functions $f : S \to K$, such that $f(0) = 0$. Then, under the usual*

pointwise addition and with multiplication defined by the convolution operation $(fg)(s) = \sum_{(t,u)\in X_s} f(t)g(u)$, *$F$ is a commutative quasiregular ring.*

Proof: It is trivial to show that under pointwise addition F is an abelian group, where $\delta \in F$ defined by $\delta(s) = 0$ for all $s \in S$ is the additive identity for F. Turning our attention to multiplication, (CM2) guarantees that the sum can be evaluated and so the operation is well-defined. Furthermore, F is closed under multiplication since $(fg)(0) = \sum_{(t,u)\in X_0} f(t)g(u) = f(0)g(0) = 0$ by (CM1). The properties of S and K ensure that multiplication in F is associative and commutative and distributes over addition. We will now show that for each $f \in F$ there exists an element $f^{\circ(-1)}$ such that $f \circ f^{\circ(-1)} = \delta$, where $\delta \in F$ is the function satisfying $\delta(x) = 0$ for all x.

Define $f^{\circ(-1)}$ as follows: $f^{\circ(-1)}(0) = 0$ and, for $s \neq 0$,

$$f^{\circ(-1)}(s) = -f(s) - \sum_{(t,u)\in X_s, u\neq s} f(t)f^{\circ(-1)}(u).$$

This is an inductive definition and the values of $f^{\circ(-1)}$ are known because if $u \neq s$ and $(t,u) \in X_s$ then $|X_u| < |X_s|$ by (CM3).

It is clear that $(f \circ f^{\circ(-1)})(0) = 0$. For non-zero $s \in S$ we have

$$\begin{aligned}
(f \circ f^{\circ(-1)})(s) &= (f + f^{\circ(-1)} + ff^{\circ(-1)})(s) \\
&= f(s) + f^{\circ(-1)}(s) + \sum_{(t,u)\in X_s} f(t)f^{\circ(-1)}(u) \\
&= f(s) - f(s) - \sum_{(t,u)\in X_s, u\neq s} f(t)f^{\circ(-1)}(u) + \sum_{(t,u)\in X_s} f(t)f^{\circ(-1)}(u) \\
&= -\sum_{(t,u)\in X_s, u\neq s} f(t)f^{\circ(-1)}(u) + \sum_{(t,u)\in X_s, u\neq s} f(t)f^{\circ(-1)}(u) \\
&\qquad + \sum_{(t,s)\in X_s} f(t)f^{\circ(-1)}(s)
\end{aligned}$$

and this is 0 since (CM4) implies that if we have $(t,s) \in X_s$ then $t = 0$ and $f(0) = 0$. Thus for each $f \in F$ there exists $f^{\circ(-1)}$ so that $f \circ f^{\circ(-1)} = \delta$. Hence F is a commutative quasiregular ring. □

[Note: At first glance there appears to be a difference in the way that we construct quasifields as in Section 2.2 and the construction we have introduced here. For quasifields, the functions which comprise the elements of the ring take the value of 1 on the minimal elements of the poset, and the circle operation is defined via a convolution; here, the elements of the ring take the value 0 on the zero of the monoid and it is multiplication which is defined in terms of a convolution. It turns out that the two approaches are equivalent if we regard the zero of the monoid as being the only minimal element and the monoid operation as analogous to the behaviour of the w and c functions. For example, suppose f and g are elements of a ring, F, constructed on a monoid, S. Then, for non-minimal (i.e. non-zero) $s \in S$ we have $(f \circ g)(s) = (f + g + fg)(s) = f(s) + g(s) + \sum_{(y,z)\in X_s} f(y)g(z) = \sum_{(y,z)\in X_s} f^*(y)g^*(z) = (f^* \circ g^*)(s)$ in the quasifield constructed where, for $h \in F$ the function h^* in the quasifield is given by $h^*(s) = h(s)$ for non-zero s, and $h^*(0) = 1$. We have retained the two operations for purely historical reasons: the quasifields of Kesava Menon and Haukkanen, in [22] and [18] respectively, use convolution for the circle operation and define their ring elements with a value of 1 on minimal poset elements; while Ribenboim, in [32] and [33], uses the approach we have applied in this section.]

As mentioned earlier there are a number of naturally occurring examples of collapsing monoids; we shall present some of them here.

Example 8.1.2 *Any cancellative commutative semigroup S having $|X_s|$ finite for all $s \in S$ and with only the trivial subgroup is a collapsing monoid.*

Proof: We need only check condition (CM3). Suppose that we are given $u \neq s$ such that there exists at least one value of $t \in S$ satisfying $(t, u) \in X_s$. Choose one such t and define the function $p_t : X_u \to X_s$ via $p_t((a, b)) = (a, b+t)$ for $(a, b) \in X_u$. Suppose now that (a, b) and (c, d) are elements of X_u with $(a, b) \neq (c, d)$. Then if $a \neq c$ we have $p_t((a, b)) = (a, b+t) \neq (c, d+t) = p_t((c, d))$.

On the other hand, if $a = c$ then we can only have $p_t((a,b)) = (a, b+t) = (c, d+t) = p_t((c,d))$ if $b + t = d + t$. However, cancellativity would then imply that $b = d$ which contradicts $(a,b) \neq (c,d)$. Thus p_t is injective and so $|X_u| \leq |X_s|$. Now $(s,0) \in X_s$ and in order to have $p_t((a,b)) = (a, b+t) = (s,0)$ we must have $a = s$ and $b = t = 0$ (since the monoid has only the trivial subgroup). However, this would imply that $(s,0) \in X_u$ which leads to the contradictory conclusion that $u = s + 0 = s$. Consequently, p_t is not a bijection and so $|X_u| < |X_s|$ as required. Finally, it is obvious that S satisfies (CM4). □

It turns out, however, that any *cancellative* collapsing monoid can be turned into a poset suitable for the quasifield constructions of Section 2.2. Let S be such a monoid and define an order operation on S via $u \leq s$ if there exists $t \in S$ such that $u + t = s$. It is straightforward to show that this is a partial order, with (CM1) used in proving that $a \leq b$ and $b \leq a$ imply $a = b$. Furthermore, 0 is the least element in this ordering. Cancellativity implies that if (t,u) and (t,v) are elements of X_s then $u = v$ and so $|X_s|$ — which is finite by (CM2) — gives the number of elements less than or equal to s so that the poset is locally finite. If $u \leq s$ then define the function w on S via $w(s,u) = t$ where $u + t = s$, cancellativity implying that such a t is unique. It is then routine to verify that the four conditions $(w1)$ to $(w4)$ are satisfied (with $(w4)$ using (CM3)), and that the function $c(x,y) = x + y$ defined from $S \times S$ to S satisfies the conditions $(c1)$ and $(c2)$ described in Section 2.2. Thus there should be no surprise that the set of whole numbers under the operation of addition — which is a cancellative collapsing monoid — produces a quasiregular ring under the construction described in Theorem 8.1.1 which corresponds to the Cauchy convolution quasifield (or, equivalently, to the power series ring with zero constant term), while the set of natural numbers under the operation of multiplication will yield a ring isomorphic to the Dirichlet convolution quasifield.

However, there are also *non*-cancellative collapsing monoids to which Theorem 8.1.1 above can be applied, as is shown in the next example.

Example 8.1.3 *There is a collapsing monoid which is not cancellative.*

Proof: Consider the natural numbers under the following operation, $\star$.

$$1 \star x = x = x \star 1 \text{ for all } x \in \mathbf{N}$$
$$a \star b = \lceil a \rceil_2 \times \lceil b \rceil_2 \text{ otherwise,}$$

where by $\lceil x \rceil_2$ we mean the smallest power of 2 greater than or equal to x. Since $\lceil \lceil a \rceil_2 \times \lceil b \rceil_2 \rceil_2 = \lceil a \rceil_2 \times \lceil b \rceil_2$ (as both $\lceil a \rceil_2$ and $\lceil b \rceil_2$ are already powers of 2 and the same applies to their product) it is straightforward to show that $(\mathbf{N}, \star)$ is a commutative monoid with identity 1. We have $X_1 = \{(1,1)\}$ and so (CM1) holds. Furthermore,

$$X_s = \begin{cases} \{(1,s),(s,1)\} \text{ if } s \text{ is not a power of 2;} \\ \{(1,s),(s,1)\} \cup \bigcup_{i,2^i \mid s} \{(a,b) \mid 2^{i-1} < a \leq 2^i, 2^{n-i-1} < b \leq 2^{n-i}\} \text{ if } s = 2^n \end{cases}$$

from which it follows that both (CM2) and (CM3) are satisfied. Finally, it is clear that if $a \star b = b$ then $a = 1$ and so (CM4) also applies. However, this is not a cancellative collapsing monoid because, for instance, $5 \star 6 = 64 = 5 \star 7$. □

Thus the collapsing monoid construction subsumes some of the examples given in the quasifield construction of Section 2.2. On the other hand, there are non-cancellative collapsing monoids as indicated by Example 8.1.3. In such a monoid there is no analogue of the w and c functions, since there is no uniqueness associated with finding z such that $y + z = x$ (where z would be the value given to $w(x,y)$). Consequently we have examples in addition to those obtained as quasifields. Furthermore, the quasifield construction allows the partially ordered set (the analogue of the monoid) to have many minimal elements, in contrast to the single identity element of the monoid. Consequently, there is overlap in

the examples obtained by the two methods, but there are also examples which can only be obtained in one of the contexts.

Given a collapsing monoid it may be possible to take a finite restriction to obtain a smaller collapsing monoid. For instance, in Example 8.1.3, we can take the set of natural numbers between 1 and 2^n for some n. All four collapsing monoid properties will still hold; in particular, the main requirement of such a restriction is that the restricted monoid is still closed under the operation. This has implications for the results on nilpotence which will be considered shortly.

[We should point out here that the generalised power series rings of [32] and [33] cannot be used directly to produce examples. This is because the functions which are the elements of such rings are defined to have artinian and narrow support. In producing quasi-inverses there is no guarantee that this condition is maintained.]

The rings formed on collapsing monoids behave similarly to quasifields in certain respects as the next lemma shows.

Lemma 8.1.4 *Let F be the ring constructed as above on a collapsing monoid S which satisfies (CM4). If $f_1, f_2, \ldots f_n \in F$ then $(f_1 f_2 \cdots f_n)(s) = 0$ for all $s \in S$ such that $|X_s| \leq n$.*

Proof: As in Lemma 3.2.1 (to which this lemma is similar) we shall proceed by induction on n. The only element $S \in S$ with $|X_s| \leq 1$ is 0, and $f(0) = 0$ for all $f \in F$. Assume that $(f_1 f_2 \cdots f_k)(s) = 0$ for all $s \in S$ such that $|X_s| \leq k$ and for all $f_1, f_2, \ldots f_k \in F$.

Now consider $f_1, f_2, \ldots f_{k+1} \in F$ and suppose $s \in S$ satisfies $|X_s| \leq k+1$. Then

$$\begin{aligned}
&(f_1 f_2 \cdots f_{k+1})(s) \\
&\quad = \sum_{(t,u)\in X_s} f_1(t)(f_2 \cdots f_{k+1})(u)
\end{aligned}$$

$$= \sum_{(t,u)\in X_s, t,u\neq s} f_1(t)(f_2\cdots f_{k+1})(u) + \sum_{(s,u)\in X_s} f_1(s)(f_2\cdots f_{k+1})(u) + \sum_{(t,s)\in X_s} f_1(t)(f_2\cdots f_{k+1})(s)$$

$$= \sum_{(t,u)\in X_s, t,u\neq s} f_1(t)(f_2\cdots f_{k+1})(u) + f_1(s)(f_2\cdots f_{k+1})(0) + f_1(0)(f_2\cdots f_{k+1})(s) \qquad \text{(by (CM4))}$$

$$= \sum_{(t,u)\in X_s, t,u\neq s} f_1(t)(f_2\cdots f_{k+1})(u)$$

since $f(0) = 0$ for all $f \in F$. For any $u \neq s$ satisfying $(t,u) \in X_s$ we have $|X_u| < |X_s| \leq k+1$. Thus $|X_u| \leq k$ and so by the inductive hypothesis $(f_2 \cdots f_{k+1})(u) = 0$ and so it follows that $(f_1 f_2 \cdots f_{k+1})(s) = 0$. The principle of mathematical induction yields the desired conclusion. □

Corollary 8.1.5 *If there exists a natural number n such that $|X_s| \leq n$ for all $s \in S$ then F is nilpotent.*

Proof: From the previous Lemma we have $F^n = \{0\}$. □

Finite collapsing monoids certainly satisfy the requirements of this corollary.

Note that (CM3) implies something roughly equivalent to $(w5)$ to the extent that Corollary 6.1.6), with some modifications, can probably be applied to collapsing monoids.

It should be pointed out that there are examples of commutative monoids which satisfy (CM1) and (CM2) but not (CM3). The following is a modification of [38].

Example 8.1.6 *There are commutative monoids which satisfy conditions (CM1) and (CM2) but not (CM3).*

Proof: Let S be the semigroup constructed as follows. Let N be an n element null semigroup with null element u (that is, $a + b = u$ for all $a, b \in N$).

On $S = \{0, s, f\} \cup N$ define the rest of the addition operation, commutatively, via

$$\begin{aligned} 0 + a &= a \text{ for all } a \in S \\ f + a &= f \text{ for all } a \in S \\ s + s &= f \\ s + x &= s \text{ for all } x \in N \end{aligned}$$

It can be verified that S is associative. Clearly $X_0 = \{(0, 0)\}$, and since S is finite it is obvious that X_s is finite for all $s \in S$, and thus (CM1) and (CM2) hold. From the definition of addition $|X_s| = 2n$, while $|X_u| = n^2$, and yet $s + u = s$. Thus provided $n \geq 3$ we have $|X_u| > |X_s|$ even though $(s, u) \in X_s$ with $u \neq s$, and hence (CM3) does not hold. □

In the next section will show that there are commutative monoids which satisfy (CM1) to (CM3) but not (CM4).

8.2 Rings in which $(R, \circ)$ is a regular semigroup

In this section we will demonstrate the construction of some rings which have regular circle composition semigroups and are thus, in the terminology of [14], *adjoint regular*. Our approach will be similar to the previous section, but instead of using collapsing monoids we will consider commutative monoids which satisfy (CM1), (CM2) and (CM3) (but not (CM4)) and which, in addition, satisfy (CM5).

(CM5): $(s, s) \in X_s$.

Of course, (CM5) is equivalent to saying that S is a band (every element is an idempotent), so we shall call such commutative monoids *almost collapsing*

semilattices. Before we consider the construction of the rings we shall show that there are a number of naturally occurring examples of such monoids.

[Note that the lemmas before Examples 8.2.3 and 8.2.5 are combinatorical in nature. It may be that they are corollaries of more general results and/or are known to the *cognoscenti*; but, if so, their origins could not be determined and so we include the proofs for completeness.]

Example 8.2.1 *The set of natural numbers with the operation* $\max(a, b)$ *is an almost collapsing semilattice.*

Proof: The operation max is clearly associative and commutative, and 1 is the identity element since $\max(1, n) = n$ for all $n \in \mathbf{N}$. The only pair (a, b) such that $\max(a, b) = 1$ is $(1, 1)$ so that $X_1 = \{(1, 1)\}$ as required. Given $s \in \mathbf{N}$ we have $X_s = \{(t, u) \mid \max(t, u) = s\} = \{(t, s), (s, u) \mid t, u \leq s\}$. Thus $|X_s| = 2s - 1$, since there are s natural numbers less than or equal to s but we do not want to count (s, s) twice. Hence $|X_s|$ is finite; moreover, if $(t, u) \in X_s$ and $u \neq s$ then ($t = s$ and) $u < s$ whence $|X_u| = 2u - 1 < 2s - 1 = |X_s|$. Finally, $\max(s, s) = s$ and so (CM5) holds. Consequently the natural numbers form an almost collapsing semilattice with the operation $\max(a, b)$. □

Lemma 8.2.2 *If* S *is finite set with* $|S| = k$ *then the cardinality of the set* $X_S = \{(U, T) \mid U, T \subseteq S, U \cup T = S\}$ *is* 3^k.

Proof: Let $S = \{a_1, a_2, \ldots, a_k\}$. Suppose that U is a subset of S of cardinality m, and without loss of generality assume $U = \{a_1, a_2, \ldots, a_m\}$. In order to have $U \cup T = S$ we must have $T = \{a_{m+1}, a_{m+2}, \ldots, a_k\} \cup U'$ where U' is any subset of U. The number of such subsets of U is given by $\binom{m}{0} + \binom{m}{1} + \binom{m}{2} + \ldots + \binom{m}{m} = 2^m$ (by adding the number of empty sets, singletons, sets of size 2 and so on). So, for a given U with $|U| = m$ there are 2^m possibilities for T. Given that there are $\binom{k}{m}$ ways of choosing U it follows that $|X_S| = 1 + k \times 2^1 + \binom{k}{2} \times 2^2 + \ldots + \binom{k}{m} \times 2^m + \ldots + \binom{k}{k} 2^k = (1 + 2)^k = 3^k$. □

Example 8.2.3 *The set of all (finite) subsets of a (possibly infinite) set under the operation of set union is an almost collapsing semilattice. (This is a free semilattice.)*

Proof: Set union is commutative and associative, and the empty set is the identity element for this operation. Furthermore, $s \cup s = s$, so $(s, s) \in X_s$. It is also clear that $X_\emptyset = \{(\emptyset, \emptyset)\}$. If s is a set having k elements then by the previous lemma $|X_s| = 3^k$ and so the finiteness condition is satisfied. If u is a proper subset of s then u will have fewer elements than s (since all the sets involved are finite) and so $|X_u| < |X_s|$ as required. □

Lemma 8.2.4 *If $s \in \mathbf{N}$ has prime factorization $s = p_1^{k_1} p_2^{k_2} \dots p_n^{k_n}$ then the set $X_s = \{(u, t) \,|\, \mathrm{lcm}(u, t) = s\}$ has cardinality $(2k_1 + 1)(2k_2 + 1) \cdots (2k_n + 1)$.*

Proof: In what follows we will say that u is *deficient* in the prime p_i if, in comparison with $s = p_1^{k_1} p_2^{k_2} \dots p_n^{k_n}$, we have $u = p_1^{j_1} p_2^{j_2} \dots p_n^{j_n}$ with $j_i < k_i$. Suppose that u divides s. Then u is deficient some of the primes that are present in the factorization of s (unless, of course, $u = s$). Suppose that there are m different primes which are deficient. Then, in order to have $\mathrm{lcm}(u, t) = s$ the choice of t cannot be deficient in those primes (in comparison to s), while it can be deficient in any of the others. Now there are $\binom{n}{m}$ ways of choosing u so that it is deficient in m primes; moreover, if p_r is one of those primes then it can be deficient in k_r ways (not present in the factorization at all, only one factor present, and so on, up to $p_r^{k_r - 1}$ being a factor). Thus if $p_{i_1}, p_{i_2}, \dots, p_{i_m}$ are the deficient primes then there are $k_{i_1} k_{i_2} \cdots k_{i_m}$ ways of choosing u. Furthermore, given such a u we have observed that t must have the u's deficient primes completely present (so there is no choice here), but we can include any of the remaining primes from s's factorization in t, either deficiently or completely. Thus there are $(k_{i_{m+1}} + 1)(k_{i_{m+2}} + 1) \cdots (k_{i_n} + 1)$ ways of choosing t given u.

Thus the number of ordered pairs (u,t) in X_s is given by

$$\begin{aligned}|X_s| &= (k_1+1)(k_2+1)\cdots(k_n+1) \qquad \text{Term } 0\\ &\quad + \sum k_{i_1}(k_{i_2}+1)(k_{i_3}+1)\cdots(k_{i_n}+1) \qquad \text{Term } 1\\ &\quad + \sum k_{i_1}k_{i_2}(k_{i_3}+1)\cdots(k_{i_n}+1) \qquad \text{Term } 2\\ &\quad + \ldots + k_{i_1}k_{i_2}k_{i_3}\cdots k_{i_n} \qquad \text{Term } n\end{aligned}$$

where there are $\binom{n}{m}$ terms in the expression associated with the m^{th} term.

We will show that this expression equals $(2k_1+1)(2k_2+1)\cdots(2k_n+1)$. Now, we have

$$\begin{aligned}&(a_1+1)(a_2+1)\cdots(a_n+1)\\ &\quad = 1 + \sum a_j + \sum_{j_1<j_2} a_{j_1}a_{j_2} + \sum_{j_1<j_2<j_3} a_{j_1}a_{j_2}a_{j_3} + \ldots + a_1a_2\cdots a_n\end{aligned}$$

from which it follows that

$$\begin{aligned}&(2k_1+1)(2k_2+1)\cdots(2k_n+1)\\ &\quad = 1 + 2\sum k_j + 2^2 \sum_{j_1<j_2} k_{j_1}k_{j_2} + 2^3 \sum_{j_1<j_2<j_3} k_{j_1}k_{j_2}k_{j_3} + \ldots + 2^n k_1k_2\cdots k_n.\end{aligned}$$

Returning to our expansion, we note that the only constant term comes from Term 0 and is 1 as required. Singletons come from Term 0, where we have $\sum k_j$ from the expansion there, and also from Term 1, where expanding gives $k_{i_1}\times 1$ for each k_{i_1}, yielding the requisite $2\sum k_j$. Products of pairs come from Term 0 (where we have $\sum_{j_1<j_2} k_{j_1}k_{j_2}$), from Term 1 (where each pair $k_{i_1}k_{i_2}$ appears twice: once in the expansion of $k_{i_1}\prod_{b\neq i_1}(k_b+1)$ and once in the expansion of $k_{i_2}\prod_{b\neq i_2}(k_b+1)$) and finally in Term 2 (where a given $k_{i_1}k_{i_2}$ appears once in the expansion of $k_{i_1}k_{i_2}\prod_{b\neq i_1,i_2}(k_b+1)$). We thus have

$$[\tbinom{2}{0}+\tbinom{2}{1}+\tbinom{2}{2}]\sum_{j_1<j_2} k_{j_1}k_{j_2} = 2^2\sum_{j_1<j_2} k_{j_1}k_{j_2}.$$

For triples, Term 0 has $\binom{3}{0}\sum k_{j_1}k_{j_2}k_{j_3}$; Term 1 has $\binom{3}{1}\sum k_{j_1}k_{j_2}k_{j_3}$ (as a given $k_{i_1}k_{i_2}k_{i_3}$ appears once in each of $k_{i_1}\prod_{b\neq i_1}(k_b+1)$, $k_{i_2}\prod_{b\neq i_2}(k_b+1)$ and

$k_{i_3}\prod_{b\neq i_3}(k_b+1)$); Term 2 has $\binom{3}{2}\sum k_{j_1}k_{j_2}k_{j_3}$ (since $k_{i_1}k_{i_2}k_{i_3}$ arises in each of $k_{i_1}k_{i_2}\prod_{b\neq i_1,i_2}(k_b+1)$, $k_{i_1}k_{i_3}\prod_{b\neq i_1,i_3}(k_b+1)$ and $k_{i_2}k_{i_3}\prod_{b\neq i_2,i_3}(k_b+1)$); and finally Term 3 has $\binom{3}{3}\sum k_{j_1}k_{j_2}k_{j_3}$ (because any $k_{i_1}k_{i_2}k_{i_3}$ occurs just once, in $k_{i_1}k_{i_2}k_{i_3}\prod_{b\neq i_1,i_2,i_3}(k_b+1)$). Adding these gives $2^3\sum k_{j_1}k_{j_2}k_{j_3}$. Continuing to argue combinatorially (with implicit induction) produces the required result. □

Example 8.2.5 *The natural numbers with the operation* $\mathrm{lcm}(a,b)$ *(that is, the least common multiple of a and b) is an almost collapsing semilattice.*

Proof: Determining the least common multiple of two numbers is a commutative and associative operation. The natural number 1 is the identity element since $\mathrm{lcm}(1,n)=n$ for all $n\in\mathbf{N}$, and $X_1=\{(1,1)\}$. Clearly (CM5) holds. Finally, the previous lemma shows that if $s\in\mathbf{N}$ has the prime factorization $s=p_1^{k_1}p_2^{k_2}\cdots p_n^{k_n}$ then $|X_s|=(2k_1+1)(2k_2+1)\cdots(2k_n+1)$ and so $|X_s|$ is finite. (This conclusion was probably obvious from the start, but the lemma proves it explicitly.) If $u\neq s$ is such that $\mathrm{lcm}(t,u)=s$ then u must divide s. It follows that u must have the prime factorization $u=p_1^{i_1}p_2^{i_2}\cdots p_n^{i_n}$ with at least one $i_m<k_m$ (and all the others no greater than k_m). Thus we have $|X_u|=(2i_1+1)(2i_2+1)\cdots(2i_n+1)<|X_s|$ from which we can conclude that the natural numbers with $\mathrm{lcm}(a,b)$ as the binary operation form an almost collapsing semilattice. □

As was the case for the posets used in the quasifield construction and the collapsing monoids used in the previous Section, it is possible to have finite restrictions of these monoids. By this we mean we choose a finite subset of the almost collapsing band which is still closed under the operation, and for which X_s contains exactly the same elements as would be the case for the unrestricted semilattice. For instance, we can take the first five powers of 2 (including 1) with binary operation of least common multiple as in Example 8.2.5. This satisfies (CM1)–(CM3) and (CM5) as required.

Let us return to the ring construction. Let F denote the set of all mappings $f : S \to K$, where K is a field (which contrasts with the previous Section, where K was a ring), with the added condition that $f(0) = 0$.

We are going to try to obtain an analogue of Theorem 8.1.1; certainly, the conclusion that F is a ring carries over directly. The main issue is what happens with respect to circle inverses. In fact, in order to show that $(F, \circ)$ is regular (rather than showing F is quasiregular), what we want is to show that for each $f \in F$ there exists an element f' such that $f \circ f' \circ f = f$.

Define f' as follows: $f'(0) = 0$ and, for $s \neq 0$,

$$f'(s) = \frac{-f(s) - f^2(s) - \sum_{(t,u)\in X_s, u\neq s}(2f(t) + f^2(t))f'(u)}{1 + \sum_{(t,s)\in X_s}(2f(t) + f^2(t))}.$$

Now it is conceivable that the denominator of this expression could be zero, which is problematic. However, for the moment, let us suppose that f is such that $1 + \sum_{(t,s)\in X_s}(2f(t) + f^2(t)) \neq 0$ for all $s \in S$. As in Theorem 8.1.1 f' is defined *via* an inductive definition; this is possible since the values of $f'(u)$ in the numerator are known by (CM3).

It is clear from the definitions of addition and multiplication and the fact that $f(0) = f^2(0) = 0$ that $(f \circ f' \circ f)(0) = 0$. For non-zero $s \in S$ we have

$$\begin{aligned}
&(f \circ f' \circ f)(s) \\
&\quad = \quad (2f + f^2 + f' + 2ff' + f^2f')(s) \\
&\quad = \quad 2f(s) + f^2(s) + f'(s) + 2\sum_{(t,u)\in X_s} f(t)f'(u) + \sum_{(t,u)\in X_s} f^2(t)f'(u) \\
&\quad = \quad 2f(s) + f^2(s) + f'(s) + 2\sum_{(t,u)\in X_s, u\neq s} f(t)f'(u) + \\
&\qquad\qquad 2\sum_{(t,s)\in X_s} f(t)f'(s) + \sum_{(t,u)\in X_s, u\neq s} f^2(t)f'(u) + \sum_{(t,s)\in X_s} f^2(t)f'(s) \\
&\quad = \quad 2f(s) + f^2(s) + 2\sum_{(t,u)\in X_s, u\neq s} f(t)f'(u) + \sum_{(t,u)\in X_s, u\neq s} f^2(t)f'(u) \\
&\qquad\qquad f'(s)(1 + 2\sum_{(t,s)\in X_s} f(t) + \sum_{(t,s)\in X_s} f^2(t))
\end{aligned}$$

$$
\begin{aligned}
&= 2f(s) + f^2(s) + 2 \sum_{(t,u)\in X_s, u\neq s} f(t)f'(u) + \sum_{(t,u)\in X_s, u\neq s} f^2(t)f'(u) \\
&\quad + \frac{-f(s) - f^2(s) - \sum_{(t,u)\in X_s, u\neq s}(2f(t) + f^2(t))f'(u)}{1 + \sum_{(t,s)\in X_s}(2f(t) + f^2(t))} \times \\
&\quad (1 + \sum_{(t,s)\in X_s} (2f(t) + f^2(t))) \\
&= 2f(s) + f^2(s) + 2 \sum_{(t,u)\in X_s, u\neq s} f(t)f'(u) + \sum_{(t,u)\in X_s, u\neq s} f^2(t)f'(u) \\
&\quad -f(s) - f^2(s) - \sum_{(t,u)\in X_s, u\neq s} (2f(t) + f^2(t))f'(u) \\
&= f(s)
\end{aligned}
$$

so that $f \circ f' \circ f = f$ as required, *provided* that $1 + \sum_{(t,s)\in X_s}(2f(t) + f^2(t)) \neq 0$ for all $s \in S$. Observe that up until this point we have not invoked (CM5).

The question remains, what happens if there *is* a function, $f \in F$, for which there exists some $s \in S$ where $1 + \sum_{(t,s)\in X_s}(2f(t) + f^2(t)) = 0$? The answer is not (yet) entirely clear, but we do have the following result.

Theorem 8.2.6 *Let F be the ring constructed on an almost collapsing semilattice, S, with underlying field $K = \mathbf{Z}_p$ where p is a prime. Then $(F, \circ)$ is regular.*

Proof: Since p is a prime, we know that $p| \binom{p}{i}$ for all $i \neq 0, p$, and as $f^{\circ p} = \sum_{i=1}^{p} \binom{p}{i} f^i = \sum_{i=1}^{p-1} \binom{p}{i} f^i + f^p$ it follows that $f^{\circ p} = f^p$ for all $f \in F$. Given $s \in S$ the definition of multiplication in F implies that $f^p(s) = \sum f(t_1)f(t_2)\cdots f(t_p)$ where $t_1 + t_2 + \ldots + t_p = s$. Now consider such a list of semilattice elements, $S' = \{t_1, t_2, \ldots, t_p\}$ (it is not a set as t_i may equal t_j for some i and j). We want to determine how many different arrangements of these can contribute to the sum — for example, if $f(t_1)f(t_2)f(t_3)\cdots f(t_p)$ is present in the sum then so is $f(t_2)f(t_1)f(t_3)\cdots f(t_p)$ *provided* t_1 and t_2 are not equal. Partition S' into separate lists of equal elements:

$$
\begin{aligned}
S' &= \{t_1, \ldots, t_{s_1}\} \cup \{t_{n_1+1}, \ldots, t_{n_1+n_2}\} \cup \\
&\qquad \{t_{n_1+n_2+1}, \ldots, t_{n_1+n_2+n_3}\} \cup \ldots \cup \{t_{\sum n_i+1}, \ldots, t_p\},
\end{aligned}
$$

where $t_1 = t_2 = \ldots = t_{n_1}$, $t_{n_1+1} = \ldots = t_{n_2}$ and so on, and we have relabelled the elements if necessary. There are then $\binom{p}{n_1}$ ways of arranging the first set of n_1 elements into the p spaces available in the product; $\binom{p-n_1}{n_2}$ ways of arranging the next n_2 elements into the remaining $p - n_1$ spaces; etc. Thus the number of different ways of arranging the elements of S' into the product is

$$\binom{p}{n_1}\binom{p-n_1}{n_2}\binom{p-n_1-n_2}{n_3}\cdots\binom{p-\sum n_i}{p-\sum n_i}$$

and, as p is prime and all the values of n_i are less than p it follows that p is a factor of this. There is one exception to this, because $f(s)f(s)\cdots f(s)$ is a term of the big summation (by CM5), and it only appears once. For all other sets, S', the above arguments lead us to conclude that given the existence of one set $\{t_1, \ldots t_p\}$ which satisfies $t_1 + \ldots + t_p = s$ and thus contributes a term to the sum, then the number of rearrangements of it (including itself) which will also contribute to the summation is a multiple of p. However, because the underlying ring is commutative the terms that appear in the summation from these rearrangements are all equal, and so vanish because the underlying rings is $\mathbf{Z}_p$. There is only one term that remains and so $f^p(s) = (f(s))^p$. Fermat's little theorem implies that $a^p = a$ in $\mathbf{Z}_p$ and hence $f^{\circ p}(s) = f^p(s) = f(s)$. Consequently, $f^{\circ p} = f$. If $p = 2$ we have $f \circ f \circ f = f \circ f = f$; while for $p > 2$ we have $f \circ f^{\circ(p-2)} \circ f = f$. In either case, F is regular. □

Since the ring satisfies the condition $f^{\circ p} = f = f^p$ the *ring* is also regular.

We note that $(F, \circ)$ is not a group. If it were, $f^{\circ p} = f$ would imply $f^{\circ(p-1)} = 0$ for all $f \in F$. Suppose $s \in S$ has the property that $X_s = \{(s, 0), (0, s), (s, s)\}$ (such an s exists by (CM2), (CM3) and (CM5)). Then

$$f^{\circ(p-1)}(s) = (\sum_{i=1}^{p-1}\binom{p-1}{i}f^i)(s) = \sum_{i=1}^{p-1}\binom{p-1}{i}(f(s))^i = (1 + f(s))^{p-1} - 1$$

by (CM5) and the fact that $f(0) = 0$. If we choose $f \in F$ such that $f(s) = p-1$

then we would have

$$f^{\circ(p-1)}(s) = \sum_{i=1}^{p-1} \binom{p-1}{i} (f(s))^i = (1 + (p-1))^{p-1} - 1 = p^{p-1} - 1 \neq 0$$

and so $f^{\circ(p-1)} \neq 0$. Thus $(F, \circ)$ is not a group and hence not a quasiregular ring.

Note that in the first part of the proof of the previous theorem we showed that if the characteristic of a ring is p then $x^{\circ p} = x^p$ for all x in the ring. Thus if $(R, \circ)$ is "p-periodic" then so is $(R, \cdot)$, and *vice versa*. However, without *requiring* a ring to have characteristic 2 we have the following result.

Proposition 8.2.7 *If R is a ring then $x^{\circ 2} = x$ for all $x \in R$ if and only if $x^2 = x$ for all $x \in R$.*

Proof: Suppose $x^{\circ 2} = x$ for all $x \in R$. Then we have $-x = (-x) \circ (-x) = -x - x + x^2$, so $0 = -x + x^2$, whence $x = x^2$. On the other hand, if $x^2 = x$ for all $x \in R$ then R is Boolean, and, as is well known, the ring is commutative and of characteristic 2. Here $x \circ x = x + x + x^2 = 3x = x$. □

So, in fact, having $x^{\circ 2} = x$ for all $x \in R$ implies that the ring is Boolean and thus has characteristic 2.

8.3 The classes of generalized radical and adjoint regular rings are not radical classes

We conclude this thesis by considering classes of rings in which the circle composition semigroup has particular semigroup properties. In arbitrary rings of course, $(R, \circ)$ is a semigroup. It is well known that the class of rings having the property that $(R, \circ)$ is a group is a radical class: the Jacobson radical class. If $(R, \circ)$ has some semigroup property approaching being a group then we can ask does the class of rings with that property form a radical class?

Generalized radical rings — in which the circle composition semigroup is a union of groups — have been investigated in [7] and [13], while adjoint regular rings — where the circle semigroup is regular — were studied in [14] and examples were presented in the previous section. As the following example shows, neither of these classes of rings, nor the class of rings having an inverse circle semigroup, is a radical class.

Consider, for example, the ring R with operation tables as below.

Addition

	0	a	b	c
0	0	a	b	c
a	a	0	c	b
b	b	c	0	a
c	c	b	a	0

Circle Composition

	0	a	b	c
0	0	a	b	c
a	a	b	b	a
b	b	b	b	b
c	c	a	b	0

Multiplication

	0	a	b	c
0	0	0	0	0
a	0	b	a	c
b	0	a	b	c
c	0	c	c	0

Then $I = \{0, c\}$ is an ideal of R which is a zero ring whose circle composition group is isomorphic to $\mathbf{Z}_2$ and is thus a group, and hence also a union of groups, an inverse semigroup and a regular semigroup. The factor ring R/I has $I \circ I = I$ and $(a + I) \circ I = I \circ (a + I) = (a + I) \circ (a + I) = a + I$ so that $((R/I), \circ)$ is a union of groups (and similarly an inverse and regular semigroup). However, R is not even regular (let alone inverse or a union of groups), because, for example, there exists no $x \in R$ such that $a \circ x \circ a = a$.

Thus the property of having $(R, \circ)$ a union of groups is not closed under extensions and so rings having that property do not form a radical class. The same example yields the same conclusion for rings having $(R, \circ)$ inverse and those having $(R, \circ)$ regular.

Bibliography

[1] B. Amberg and O. Dickenschied. On the adjoint group of a radical ring, *Canad. Math. Bull.*, **38** (1995), 262–270.

[2] V. A. Andrunakievich. Semi-radical rings, *Izv. Akad. Nauk SSSR* **12** (1948), 129–178 (in Russian).

[3] C. C. Chang and H. J. Keisler. *Model Theory* (Second edition), Studies in Logic and the Foundations of Mathematics **73**, North-Holland Publishing Co., Amsterdam, 1977.

[4] H. L. Chick. Quasi-division rings — Some examples of quasiregular rings, in *Theory of Radicals*, Ed. L. Márki and R. Wiegandt (Proc. Conf. Szekszárd, 1991), Colloq. Math. Soc. J. Bolyai, 61, North-Holland, Amsterdam, 1993, 35–59.

[5] H. L. Chick. Rings with isomorphic additive and circle composition groups, in *Rings and radicals — Proceedings of the International Conference, Shijiazhuang '94*, Ed. B. J. Gardner, Liu Shaoxue and R. Wiegandt, Pitman Research NOtes in Mathematics Series **346**, Longman, 1996, 160–169.

[6] H. L. Chick. The properties of some rings having isomorphic additive and circle composition groups, Aust. Math. Soc. Gaz. **23** (1996), 112–117.

[7] W. Edwin Clark. Generalized radical rings, *Canad. J. Math.* **20** (1968), 88–94.

[8] Al. Climescu. Anneaux faibles (Weak rings), *Bull. Inst. Politehn. Iaşi* **7 (11)** (1961), 1–6 (in French).

[9] Al. Climescu. O nouá clasá de inele slabe (A new class of weak rings), *Bull. Inst. Politehn. Iaşi* **10 (14)** (1964), 1–4 (in Romanian).

[10] Ǧ. Čupona. On quasirings, *Bull. Soc. Math. Phys. Macédoine* **20** (1969), 19–22 (in Macedonian).

[11] N. J. Divinsky. *Rings and Radicals* George Allen & Unwin Ltd., London, 1965.

[12] J. Duncan and I. D. Macdonald. Some factorable nil rings of characteristic two. *Proc. Roy. Soc. Edin.* **82A** (1979), 193–199.

[13] Du Xiankun. The structure of generalized radical rings, *Northeastern Math. J.* **4(1)** (1988), 101–114.

[14] Du Xiankun. The rings with regular adjoint semigroups, *Northeastern Math. J.* **4(4)** (1988), 463–468.

[15] I. Fischer and K. E. Eldridge. Artinian rings with a cyclic quasi-regular group, *Duke Math. J.* **36** (1969), 43–47.

[16] L. Fuchs. *Infinite Abelian Groups (Volume 1)*, Pure and applied mathematics **36**, Academic Press, New York, 1970.

[17] F. Haimo. Radical and antiradical groups, *Rocky Mountain J. of Math.* **3** (1973), 91–106.

[18] P. Haukkanen. Some classes of quasifields having isomorphic additive and multiplicative groups, *Rend. Mat. (Series VII)* **7** (1987), 181–192.

[19] A. G. Heinicke. Subdirect sums, hereditary radicals, and structure spaces, *Proc. Amer. Math. Soc.* **25** (1970), 29–33.

[20] T. W. Hungerford. *Algebra*, Holt, Rinehart and Winston, Inc., New York, 1974.

[21] G. Karpilovsky. *Field Theory: Classical Foundations and Multiplicative Groups*, Monographs and textbooks in pure and applied mathematics **120**, Marcel Dekker, New York, 1988.

[22] P. Kesava Menon. A class of quasifields having isomorphic additive and multiplicative groups. *J. Indian Math. Soc.* **27** (1963), 71–90.

[23] N. Koblitz. *p-adic Numbers, p-adic Analysis, and Zeta-Functions*, Graduate Texts in Mathematics **58**, Springer Verlag, New York, 1977.

[24] E. Kreyszig. *Introductory Functional Analysis with Applications*, John Wiley and Sons, New York, 1978.

[25] R. L. Kruse. A note on the adjoint group of a finitely generated radical ring, *J. London Math. Soc. (2)* **1** (1969), 743–744.

[26] R. L. Kruse and D. T. Price. *Nilpotent Rings*, Notes on Mathematics and its Applications, Gordon and Breach, New York, 1969.

[27] T. Y. Lam. *A First Course in Noncommutative Rings*, Graduate Texts in Mathematics **131**, Springer Verlag, New York, 1991.

[28] P. J. McCarthy. *Introduction to Arithmetical Functions*, Springer-Verlag, New York, 1986.

[29] I. Niven. Formal power series, *Amer. Math. Monthly* **76** (1969), 871–889.

[30] M. Petrich. *Introduction to Semigroups*, Charles E. Merrill Publishing Co., Columbus, Ohio, 1973.

[31] D. Rearick. Operators on algebras of arithmetic functions, *Duke Math. J.* **35** (1968), 761–766.

[32] P. Ribenboim. Rings of generalized power series: Nilpotent elements, *Abh. Math. Sem. Univ. Hamburg* **61** (1991), 15–33.

[33] P. Ribenboim. Rings of generalized power series II: Units and zero-divisors. *Journal of Algebra* **168** (1994), 71–89.

[34] J. J. Rotman. *The Theory of Groups*, Allyn & Bacon, Boston, 1973.

[35] W. H. Schikhof. *Ultrametric Calculus: An Introduction to p-adic Analysis*, Cambridge Studies in Advanced Mathematics **4**, Cambridge University Press, Cambridge, 1984.

[36] R. P. Stanley. *Enumerative Combinatorics, Volume I*, Wadsworth & Brooks/ Cole Advanced Books & Software, Monterey, California, 1986.

[37] M. Ştefănescu. A generalization of the concept of near ring: infra-near rings, *An. Şt. Univ. "Al. I. Cuza" Iaşi* **25** (1979), 45–56.

[38] P. G. Trotter. Private communication, 1995.

[39] T. Szele. Gruppentheoretische Beziehungen bei gewissen Ringkonstructionen, *Math. Z.* **54** (1951), 168–180.

[40] R. Wiegandt. On the general theory of the Möbius inversion formula and Möbius product, *Acta Sci. Math.* **20** (1959), 164–180.

[41] R. Wiegandt. *Radical and semisimple classes of rings*, Queen's Papers in Pure and Applied Mathematics **37**, Kingston, Ontario, 1974.

[42] W. Wyss. The quasi-multiplication on rings and algebras, *Letters in Mathematical Physics* **2** (1978), 207–217.

Index