NEW CLASSES OF FINITE COMMUTATIVE RINGS

A DISSERTATION SUBMITTED TO THE GRADUATE DIVISION OF THE UNIVERSITY OF HAWAII IN PARTIAL FULFILLMENT OF THE REQUIREMENTS FOR THE DEGREE OF

DOCTOR OF PHILOSOPHY

IN

MATHEMATICS

MAY 2003

By
Monika Vo

Dissertation Committee:

Thomas Craven, Chairperson
Edward Bertram
Hugh Hilden
J.B. Nation
Marc Fossorier

ACKNOWLEDGEMENTS

I would like to thank my advisor, Dr. Thomas Craven, for his continued support, friendship, and the wisdom that he provided from the time I arrived at the university. He has been an inspiration to me to finish this degree and to accomplish all that I have. I also want to extend my gratitude for the wonderful faculty of the Mathematics department at the University of Hawaii at Manoa. I have learned a lot from all of you and I will bring all these lessons with me as I embark on my career.

I must give special thanks to Dr. Bertram, Dr. Fossorier, Dr. Hilden and Dr. Nation for serving on my committee. I appreciate your valuable time and comments on my thesis. I also must express my gratitude to Dr. Little and Dr. Host Madsen for stepping in and becoming proxies.

I must at this time also thank the wonderful secretaries, Pat, Shirley and Susan. You are truly a wonderful bunch of ladies. You have been my surrogate mothers and I will miss you terribly.

In addition to the faculty in Hawaii, at this time I would like to give credit to two of my favorite professors from Kean University. Dr. James Butcher and Professor Carl Krantz encouraged me to pursue my graduate studies. Hence, I want to thank them also for their support.

However, life as a graduate student does not only revolve around studying. At times, we do have time to be with our families and friends. And so, at this time I would like to say many

thanks to all in my wonderful family, who have given me so much help and support, that they do not realize. And to my friends, your friendship, encouragement and support have been invaluable. You have all made my life truly joyous. I will miss you all.

And, last but not least, I must thank my wonderful husband, Hung. Without you, none of this could have been possible. Thank you so much for all you have done for me.

"You are a rock!" I love you and thank you for being there with me all the way.

ABSTRACT

This dissertation introduces the concept of Q-Witt rings and SQ-Witt rings. A Q-Witt ring is defined as a finite quotient of a torsion free abstract Witt ring for an elementary 2-group G. Local Q-Witt rings are characterized using topological and ring theoretic tools. Q-Witt rings of the integral group ring $\mathbb{Z}[\mathbb{Z}_2]$ are classified and several properties are shown. An SQ-Witt ring is formed as a finite quotient of torsion free Witt rings of a formally real field. Recursive construction can be used to locate all SQ-Witt rings.

TABLE OF CONTENTS

CHAPTER 1
INTRODUCTION AND NOTATION

In this paper we will work in the category of commutative rings with 1. We will be mainly interested in finite commutative rings with identity. There are many papers and books written on the topics of finite fields as well as finite commutative groups, but only a few on finite commutative rings. Thus, we will provide the reader with a substantial number of definitions, theorems and examples, so that we can understand these rings better and find ways in which they will be useful.

In Chapter 1 we will give some of the basic definitions and structure theorems for finite rings. In particular, we discuss Galois rings and chain rings. Finite chain rings are quotient rings of rings of algebraic integers in finite extensions of the rationals. Chain rings have relevance in the areas of number theory and geometry. They are used as coordinatizing rings of Hjelmslev planes [7]. In addition, there is more and more research focusing on using local rings in coding theory, mainly Galois rings and more general chain rings.

In Chapter 2 we describe abstract Witt rings, which have been defined in [10]. We offer both ring theoretic and topological descriptions of these rings as was shown in [10] and [11]. It is here that we define a special class of finite rings in the context of [10], called Q-Witt rings. We study their structure and give conditions for when we get local Q-Witt rings. In Chapter 3, we look at a very special class of Q-Witt rings, which are quotients of integral group rings of the form $\mathbb{Z}[G]$ where G is an elementary abelian 2-group. We describe the rings with $|G| = 2$ in great detail.

Chapter 4 deals with a class of finite rings, which are created as quotients of reduced Witt rings of formally real fields, called SQ-Witt rings. In order to understand this construction, we provide some background information on Witt rings of formally real fields as was described in [11].

For the remainder of this chapter, R will denote a finite commutative ring with identity different from 0, unless stated otherwise.

DEFINITION 1.1 A ring R is called *local* if it has a unique maximal ideal.

We observe that the study of finite commutative rings can be reduced to the study of finite local rings, as stated in [14, Theorem VI.2].

THEOREM 1.2 (Structure Theorem for Finite Commutative Rings)
Any finite commutative ring R with unity decomposes, up to order of summands, uniquely as a direct sum of local rings.

The proof is a nice application of the Chinese Remainder Theorem.
So, for the remainder of this chapter we will assume that R is a local ring. We let $\mathfrak{m}$ denote the unique maximal ideal of R, and $\mathbf{k} = R/\mathfrak{m}$ be the residue field associated with R. Let $\pi : R[x] \to \mathbf{k}[x]$ be the natural ring homomorphism. We denote the characteristic of R by $char(R)$, the additive group of R by R^+, the units of R by R^*, and the cardinality of R by $|R|$. The set of integers will be denoted by $\mathbb{Z}$. Then $\mathbb{Z}_n$ denotes the ring of equivalence classes of $\mathbb{Z}$ under congruence modulo a fixed positive integer n.

The structure of local rings has been presented very comprehensively by B. McDonald, so for the purposes of this paper we will simply give a short synopsis with a list of major definitions and results which we shall need later.

Let S be a finite commutative local ring, as well, with maximal ideal $\mathfrak{M}$ and residue field $\mathbb{K} = S/\mathfrak{M}$.

DEFINITION 1.3 A ring S is said to be an *extension* of R if R is a subring of S.

We note that if S is an extension of R, then S is an R-algebra with $1_R = 1_S$.
We remind the reader of [8, Corollary IV.2.12], which states that all commutative rings have the invariant dimension property. That is, every free R-module S has the property that the cardinality of any two bases is the same. The cardinal number of any basis of S is called the dimension of S over R, denoted by $\dim_R(S)$.
Since S is finite, we obtain

THEOREM 1.4 [14, Theorem XIII.1] *Let R and S be finite commutative local rings and S an extension of R. Then for any $a \in S$ there is a monic polynomial f in $R[x]$ such that $f(a) = 0$. That is, S is integral over R, in the sense that every element of S satisfies a monic polynomial in $R[x]$.*

We then have as an almost immediate consequence

LEMMA 1.5 *Let R, S, a and f be as in Theorem* 1.4. *Then there is a natural surjective R-algebra homomorphism $R[x]/(f) \to R[a]$, where $R[a]$ is the subring of S consisting of all elements of the form $p(a)$, where p is in $R[x]$.*

DEFINITION 1.6 The *enveloping algebra,* S^e, associated with an R-algebra S is the R-algebra $S \otimes_R S$.

DEFINITION 1.7 The R-algebra S is called *R-separable* or *a separable extension of* R if S is a projective S^e- module.

DEFINITION 1.8 The local ring S is called an *unramified* extension of R if $\mathfrak{M} = S\mathfrak{m}$, that is the maximal ideal $\mathfrak{m}$ of R generates the maximal ideal $\mathfrak{M}$ of S.

Next we will state a result, called the Primitive Element Theorem, which can be obtained using results from finite field extensions and Nakayama's lemma.

THEOREM 1.9 [14, Theorem XIV.7] *Let R and S be finite commutative local rings and S a separable extension of R. Then S is a simple extension of R, that is $S = R[a]$ for some a in S.*

We recall that an element a with $S = R[a]$ is called a *primitive element*.
Using a series of lemmas and theorems, McDonald showed [14, Theorem XIV.6]

THEOREM 1.10 *Let R and S be finite commutative local rings. The ring S is a separable extension of R if and only if S is an unramified extension of R.*

These characterizations are difficult to check; luckily we have another characterization of separable extensions [14, Theorem XIV.8], which will make our lives a lot easier. In order to state this theorem however, we must introduce some more vocabulary

and notation. We will use the usual definitions associated with polynomials and so we will only state the new terminology introduced by McDonald.

DEFINITION 1.11 A polynomial f in $R[x]$ is called a *regular polynomial* if f is not a zero divisor in $R[x]$.

These polynomials have a central role in the study of local rings. Therefore, we list some properties of regular polynomials, which can be easily checked using the natural ring homomorphism $\pi : R[x] \to \mathbf{k}[x]$.

THEOREM 1.12 [14, Theorems XIII.2 and XIII.7]. *Let* $f(x) = a_0 + a_1x + \ldots + a_nx^n$ *be a regular polynomial in* $R[x]$, *where* R *is a finite commutative local ring. Then*

(1) $\pi(f) \neq 0$, *which implies that for some* i, $0 \leq i \leq n$, a_i *is a unit.*

(2) If $\pi(f)$ *is irreducible in* $\mathbf{k}[x]$, *then* f *is irreducible.*

We can check that the converse of Theorem 1.12 (2) is not in general true. To see this, we consider the monic regular polynomial $p(x) = x^2 + 1$ in $\mathbb{Z}_4[x]$. Observe that p is an irreducible polynomial in $\mathbb{Z}_4[x]$; however, the image of p in $\mathbb{Z}_2[x]$ factors as $(x + 1)^2$.

DEFINITION 1.13 An irreducible polynomial $f \in R[x]$ is called *basic irreducible* provided that $\pi(f)$ is irreducible in $\mathbf{k}[x]$.

With the proper definitions stated we are now ready to state [14, Theorem XIV.8].

THEOREM 1.14 *Let R and S be finite commutative local rings. Then S is a separable extension of R if and only if $S \cong R[x]/(f)$ as an R-algebra where f is a monic basic irreducible polynomial.*

To understand Galois extensions we need to characterize the R-algebra automorphisms of $R[x]$ as well. To that end we state [14, Theorem XIII.16].

THEOREM 1.15 *Let R be a finite commutative local ring and $f(x) = a_0 + a_1x + \ldots + a_nx^n$ be a polynomial in $R[x]$. Then $\sigma_f : x \to f(x)$ induces an R-algebra automorphism of $R[x]$ if and only if a_1 is a unit and $a_2, \ldots, a_n$ are nilpotent. Each R-algebra automorphism of $R[x]$ is of the form σ_f for some such f.*

Suppose that S is an extension of R and suppose G is a group of R-algebra automorphisms of S. Let

$$S^G = \{s \in S \mid \sigma(s) = s \text{ for all } \sigma \in G\},$$

be the subring of S fixed by the R-algebra automorphisms in the group G.

DEFINITION 1.16 Let G be as above. Then we say that S is a *Galois extension* of R with Galois group G, denoted by $G_R(S)$, if

1) $S^G = R$, and

2) S is a separable extension of R.

DEFINITION 1.17 A Galois extension S of R is called a *splitting ring* for a basic irreducible f in $R[x]$ if f is a product of linear factors in $S[x]$ and S is generated over R by the zeros of f.

Now, without further ado we are ready to state the Galois theory for finite local commutative rings, as stated in [14, Theorem XV.11].

THEOREM 1.18 *Let R and S be finite local commutative rings and S a separable extension of R. Then*

1*) S is a Galois extension of R and, if $f \in R[x]$ is a monic basic irreducible such that $S \cong R[x]/(f)$, then the order of the Galois group $|G_R(S)| = \deg(f)$, S is a splitting ring of f and S is the unique Galois extension of R having R-dimension equal to $\deg(f)$.*

2*) $G_R(S)$ is cyclic, isomorphic to $G_{\mathbf{k}}(\mathbb{K})$ and generated by a power map*

$$\sigma : a \to a^{|\mathbf{k}|}$$

on a suitable primitive element a.

3*) There is a lattice preserving bijection between the subfields of $\mathbb{K}$ containing $\mathbf{k}$ and the R-separable subrings of S containing R. If T is a separable extension of R in S, then S is a separable extension of T and*

$$1 \to G_R(T) \to G_R(S) \to G_T(S) \to 1$$

is exact.

4*) S has a normal basis over R, that is, there exists an element a in S such that $\{\sigma(a) \mid \sigma \in G_R(S)\}$ is a free R-basis for S.*

EXAMPLE 1.19 Let $R = \mathbb{Z}_9$. Then $f(x) = x^2 + 1$ is an irreducible polynomial in $R[x]$. Since $\pi(f)$ is irreducible in $\mathbb{Z}_3$, f is basic irreducible. Hence, by Theorem 1.18, $S = R[x]/(f)$ is a Galois extension of R. We also know that $\deg(f) = 2$, $\dim_R(S) = 2$ and $|G_R(S)| = 2$,

which means that $G_R(S)$ is isomorphic to $\mathbb{Z}_2$ and so there are no proper R-separable subrings of S containing R.

EXAMPLE 1.20 Let $R = \mathbb{Z}_9$. Then $f(x) = x^4 + x^3 + x^2 + x + 1$ is an irreducible polynomial in $R[x]$. One can check that $\pi(f)$ is irreducible in $\mathbb{Z}_3$, so f is basic irreducible. Hence, by Theorem 1.18, $S = R[x]/(f)$ is a Galois extension of R. We also know that $\deg(f) = 4$, $\dim_R(S) = 4$ and $|G_R(S)| = 4$, which means that $G_R(S)$ is isomorphic to $\mathbb{Z}_4$. Therefore, there is an R-separable subring T of S containing R, where $T \cong R[x]/(g)$ and $g(x)$ is a quadratic monic basic irreducible. By Theorem 1.18 (1), we know T is unique, so we can choose $g(x) = x^2 + 1$.

Observe that if α is a root of f in S, then we can factor f as

$$f(x) = (x - \alpha)(x - \alpha^2)(x - \alpha^3)(x - (8\alpha^3 + 8\alpha^2 + 8\alpha + 8)).$$

The set $\{1, \alpha, \alpha^2, \alpha^3\}$ is an R-basis for S. Then if $G_R(S) = \langle\sigma\rangle$, we have

$$\sigma(\alpha) = \alpha^2$$

$$\sigma^2(\alpha) = 8\alpha^3 + 8\alpha^2 + 8\alpha + 8$$

$$\sigma^3(\alpha) = \alpha^3$$

$$\sigma^4(\alpha) = \alpha.$$

To explicitly state what T is, we need to find the fixed ring of $\langle\sigma^2\rangle$.

The polynomial $g(x) = x^2 + 1$ factors as $g(x) = (x - [\alpha^3 + \alpha^2 + 5])(x + [\alpha^3 + \alpha^2 + 5])$ and observe that

$$\sigma^2(\alpha^3 + \alpha^2 + 5) = \alpha^3 + \alpha^2 + 5$$

so $\alpha^3 + \alpha^2 + 5$ is in the fixed ring of $\langle\sigma^2\rangle$ and $T = R[\alpha^3 + \alpha^2 + 5]$.

As the reader may expect the examples we have just described belong to a very special class of local rings, which we define next.

DEFINITION 1.21 The Galois extension of degree r of the prime ring $\mathbb{Z}_{p^n}$, where p is a prime and n is a positive integer, is called a *Galois Ring* and is denoted by $GR(p^n,r)$.

We should note that Galois rings were known to Krull in 1924, and were rediscovered by Janusz and Raghavendran in 1966 and 1969 respectively [14, Pg 308].

EXAMPLE 1.22 One easily sees that the Galois ring $GR(p,r) = GF(p^r)$, the Galois field of order p^r and $GR(p^n,1) = \mathbb{Z}_{p^n}$.

EXAMPLE 1.23 In Example 1.18 S is isomorphic to the Galois ring $GR(3^2,2)$ and in Example 1.20 S is isomorphic to the Galois ring $GR(3^2,4)$ and T is isomorphic to $GR(3^2,2)$.

And finally we arrive at the highlight of this chapter which is [14, Theorem XVII.1].

THEOREM 1.24 (Structure Theorem for Finite Commutative Local Rings) *Let R be a finite local commutative ring of characteristic p^n with maximal ideal* $\mathfrak{m}$ *and residue field* $\mathbf{k}$. *Let* $[\mathbf{k} : \mathbb{Z}_p] = r$ *and* $\{m_1,\ldots m_d\}$ *be a minimal R-generating set of* $\mathfrak{m}$. *Then there exists a subring T of R such that:*

(1) $T \cong GR(p^n,r)$, T is unique and is the largest Galois extension of $\mathbb{Z}_{p^n}$ in R.

(2) R is the ring homomorphic image of $T[x_1,\ldots,x_d]$.

The Galois ring T is called the *coefficient ring* of R.

Hence, the theory of finite local commutative rings reduces to determining the primary ideals P in $GR(p^n,r)[x_1,\ldots,x_d]$ and the quotient rings $GR(p^n,r)[x_1,\ldots,x_d]/P$. This is an incredibly difficult job. Therefore, it would be very hard to actually find out how many local rings of a given order there are. Even when we restrict our attention to the class of local principal ideal rings, we do not have a complete classification.

DEFINITION 1.25 If R is a finite commutative local principal ideal ring, then R is called a *chain ring*.

We note that if R is a chain ring with maximal ideal $\mathfrak{m}$, then each ideal of R is of the form $\mathfrak{m}^i$ for some positive integer i. Hence, the ideals of R form a chain, thus the name chain ring. We finish this section by stating [14, Theorem XVII.5].

THEOREM 1.26 (Characterization of Finite Commutative Chain Rings) *Let R be a finite commutative chain ring. Suppose that b is the least positive integer such that $\mathfrak{m}^b = 0$. Also, let $char(R) = p^n$ and $r = [\mathbf{k} : \mathbb{Z}_p]$. Then there exist positive integers t and s such that*

$$R \cong GR(p^n,r)[x]/(g(x),p^{n-1}x^t)$$

where $t = b - (n-1)s > 0$ and $g(x) = x^s + p(a_{s-1}x^{s-1} + \ldots + a_1x + a_0)$

where a_0 a unit in $GR(p^n,r)$. Conversely, any such quotient ring is a finite commutative chain ring.

EXAMPLE 1.27 Using the above theorem we know that $R = \mathbb{Z}_4[x]/(x^2+2,2x)$ is a chain ring. The set R can be represented as $\{0,1,2,3,y,y+1,y+2,y+3\}$, where y satisfies

the equations $y^2 = 2$ and $2y = 0$. The maximal ideal of R is $\mathfrak{m} = \{0, y+2, 2, y\} = (y)$ which has the property that $\mathfrak{m}^3 = 0$.

The classification of chain rings is of great interest. Currently, only partial classifications have been accomplished. Clark and Liang classified all finite chain rings with invariants p, n, r, s, t up to isomorphism provided that $(p, s) = 1$ in [2], where the invariants are as in Theorem 1.25. In [7], Hou classified finite chain rings with invariants p, n, r, s, t, $(p, s) = 1$ up to isomorphism when $n = 2$ or when $p \parallel s$ but $(p-1) \nmid s$, where the invariants are as in Theorem 1.25 and $p \parallel s$ means $p \mid s$ but $p^2 \nmid s$. Therefore, the classification of finite chain rings with fixed invariants up to isomorphism is far from complete as of the writing of this paper.

The study of Galois rings as well as chain rings is also important in current research in coding theory. In [16], Norton provided among other things a solution to the classical key equation of Algebraic Coding Theory over a finite chain ring. Later, Norton with Sălăgan gave a decoding algorithm for alternant codes over a finite chain ring. Examples of such codes are BCH and Reed-solomon codes over a Galois ring. In [5] and [6], the authors showed that finite chain rings can be used to construct some useful nonlinear codes.

The goal of this thesis is to develop some new classes of finite rings. In terms of Theorem 1.24, the rings we construct in later chapters will have $r = 1$ and d arbitrarily large. We shall define abstract Witt Rings and study finite quotients of these rings.

CHAPTER 2
Q-WITT RINGS

In this chapter we introduce the reader to abstract Witt rings. In [10], Knebusch, Rosenberg and Ware defined a class of commutative rings which are residue class rings of $\mathbb{Z}[G]$ where G is an abelian torsion group. This paper gives a ring-theoretic approach to the study of Witt rings of equivalence classes of nondegenerate symmetric bilinear forms over a field of characteristic not 2. The main aim of this chapter is to define a special class of finite rings within the general context of [10]. These rings do not generally occur in quadratic form theory, but can be quotients of rings which do. This class of rings will be called Q-Witt rings. In Chapter 4 we will consider a special subclass of these we call SQ-Witt rings, which occur as quotients of Witt rings of formally real fields.

For the remainder of this section G is an elementary abelian 2-group, K a proper ideal of the integral group ring $\mathbb{Z}[G]$, and R the residue class ring $\mathbb{Z}[G]/K$. We let χ be a character of G, i.e., a homomorphism of G into $\mathbb{C}$, the field of complex numbers. Note that if G is an elementary 2-group, then since $g^2 = 1$ for all $g \in G$, we have that $\chi(g) = \pm 1$ for all χ. Every character χ gives rise to a ring homomorphism ψ_χ of $\mathbb{Z}[G]$ into $\mathbb{Z}$. Similarly, any ring homomorphism of $\mathbb{Z}[G]$ into $\mathbb{Z}$, restricted to G gives rise to a character χ of G. *RadR* denotes the radical of R, which is the intersection of all maximal ideals of R, and *NilR* denotes the set of nilpotent elements of R. R_t denotes the torsion subgroup of the additive group of R, which is an ideal of R. We will use the following notation as well. We let $R_{red} = R/NilR$. By *SpecR* we mean the set of prime ideals of R topologized by the Zariski topology, and *MaxR* and *MinR* denote the subspaces of *SpecR*

consisting of the maximal ideals and minimal prime ideals respectively. We now state a special case of [10, Lemma 3.1].

LEMMA 2.1 *The minimal prime ideals of* $\mathbb{Z}[G]$ *are the kernels* P_χ *of the ring homomorphisms* $\psi_\chi : \mathbb{Z}[G] \to \mathbb{Z}$, *with* $\mathbb{Z}[G]/P_\chi \cong \mathbb{Z}$. *The maximal ideals of* $\mathbb{Z}[G]$ *are of the form* $M = \psi_\chi^{-1}(p\mathbb{Z}) = P_\chi + p\mathbb{Z}$, *where p is a positive prime integer.*

Due to the fact that any ring homomorphism of $\mathbb{Z}[G]$ onto $\mathbb{Z}$ is completely determined by its kernel, there is a bijective correspondence between the set of characters of G and the minimal prime ideals of $\mathbb{Z}[G]$. Now we list some results from [10], which we shall need later. We shall see that the finite rings we are interested in fall under the general scope of [10], but are generally quite distinct from Witt rings of fields. They will be finite quotients of the rings analyzed in [11].

From [10, Section 3], we have

LEMMA 2.2 *Let* $R = \mathbb{Z}[G]/K$. *Then R is Jacobson; that is, each of its prime ideals is an intersection of maximal ideals,* $NilR = RadR$ *and* $R_t \supset NilR$.

LEMMA 2.3 $R_t = NilR$ *if and only if no maximal ideal of R is a minimal prime ideal, and* $R_t = R$ *if and only if all maximal ideals are minimal prime ideals.*

LEMMA 2.4 *Let p be an odd prime integer. Then the following are equivalent:*

(1) There exists a character χ *of G with* $0 \neq \psi_\chi(K) \cap \mathbb{Z} \subset p\mathbb{Z}$.

(2) R contains a minimal prime ideal M with R/M being a field of characteristic p.

(3) R has nonnilpotent p-torsion.

(4) R has nonzero p-torsion.

It is further shown in [10, Lemma 2.13] that M_0, defined as the kernel of the augmentation map $\mathbb{Z}[G] \to \mathbb{Z}$, defined by $\sum n_g g \to \sum n_g$, followed by reduction mod 2, is the unique maximal ideal of $\mathbb{Z}[G]$ containing 2. It is also proven that M_0 contains every minimal prime ideal and that each maximal ideal distinct from M_0 contains a unique minimal prime ideal.

As in [10, Definition 3.12], we are now ready to define abstract Witt rings.

DEFINITION 2.5 Let R be a commutative ring of the form $R \cong \mathbb{Z}[G]/K$ where G is an elementary abelian 2-group and K is an ideal of $\mathbb{Z}[G]$ with $\psi_\chi(K) \cap \mathbb{Z} = 0$ or $\psi_\chi(K) \cap \mathbb{Z} = 2^n\mathbb{Z}$ for all homomorphism ψ of $\mathbb{Z}[G]$ and all characters χ of G. Then R is called an *abstract Witt ring for G.*

We note that in the case of [10], the definition extends to Witt rings of abelian q-groups with q any prime. However, in this paper we will only consider Witt rings of elementary abelian 2-groups. In the future, we will investigate adopting our ideas to more general cases.

We shall finally state two characterizations [10, Proposition 3.15 and 3.16].

PROPOSITION 2.6 *Let $R = \mathbb{Z}[G]/K$ where G is an elementary 2-group. Then the following are equivalent:*

(1) $R = R_t$ is a 2-group.

(2) $\psi_\chi(K) \cap \mathbb{Z} = 2^n\mathbb{Z}$ *for all characters* χ *of G, and hence R is a Witt ring for G.*

(3) R is local with unique prime ideal M_0/K.

(4) $K \cap \mathbb{Z} = 2^n\mathbb{Z}$.

PROPOSITION 2.7 *Let* $R = \mathbb{Z}[G]/K$ *where G is an elementary 2-group. Then* $R_t = NilR$ *if and only if* $K \cap \mathbb{Z} = 0$ *and R is a Witt ring for G. In this case, R contains nonmaximal prime ideals.*

These two results precisely separate Witt rings of formally real and non-formally real fields as we shall see in Chapter 4. It is here that we depart from the standard literature, all of which has been aimed at understanding quadratic form theory. Note that any finite ring is necessarily torsion, and so almost all of the rings we construct will fall under Proposition 2.6. However, we shall concern ourselves with certain finite quotients of rings falling under Proposition 2.7. They will occur as rings of functions on *MinR* and will generally not occur as Witt rings of fields.

Assume for the moment that $R_t = Nil\ R$. The reason these Witt rings are special is that the reduced Witt ring $R_{red} = R/Nil\ R$ is still an abstract Witt ring for a subgroup of G [10, Remark 3.13]. In [11, §3], it is shown that there is a natural embedding of R_{red} into $C(X(R), \mathbb{Z})$, the ring of continuous functions from $X(R)$ to the ring of integers $\mathbb{Z}$. In $C(X(R), \mathbb{Z})$, $X(R)$ is the set of ring homomorphisms from R to $\mathbb{Z}$, or equivalently (using Lemma 2.1 and Proposition 2.7), *MinR* with the induced Zariski topology and $\mathbb{Z}$ is endowed with the discrete topology. $X(R)$ is a Boolean topological space, that is, a compact, totally disconnected Hausdorff space. As such we can conclude using

[15, Theorem 2.4 and 3.1] that $X(R)$ is normal and thus by Urysohn's lemma the points of $X(R)$ are separated by the continuous functions of $C(X(R), \mathbb{Z})$. We will denote the characteristic function of a set B by e_B. Recall that the characteristic function is defined by

$$e_B(x) = \begin{cases} 1 & if\, x \in B \\ 0 & if\, x \notin B \end{cases}.$$

Using [11, Lemma 3.5] we have that

LEMMA 2.8 *For any Boolean space X, let $\mathcal{B}$ be the basis of all clopen (closed and open) sets.*

(1) For $B_1, B_2 \in \mathcal{B}$, define

$$B_1 + B_2 = (B_1 \cup B_2) - (B_1 \cap B_2) \text{ and } B_1 B_2 = B_1 \cap B_2.$$

Then $\mathcal{B}$ is a Boolean ring with these operations.

(2) The idempotents of $C(X, \mathbb{Z})$ are the characteristic functions e_B for B in $\mathcal{B}$.

An element $f \in C(X, \mathbb{Z})$ has the form

$$f = \sum_{1}^{n} m_i e_{B_i}$$

where $m_i \in \mathbb{Z}$ and $\{B_i\}$ a partition of X by elements of $\mathcal{B}$.

(3) $\mathcal{B} \cong C(X, \mathbb{Z}_2)$ via $B \to e_B$.

(4) The units of $C(X, \mathbb{Z})$ are the functions of the form $f_B = 1 - 2e_B$ for B in $\mathcal{B}$.

Also, observe that for $B, B_1, B_2 \in \mathcal{B}$

$$f_B = \begin{cases} -1 & on\ \ B \\ 1 & on\ \ X - B \end{cases}$$

so that $f_B^2 = 1$.

(5) $f_{B_1} f_{B_2} = f_{B_1+B_2}$.

THEOREM 2.9 [11, Theorem 3.18] *Let R be a Witt ring with* $R_t = NilR$ *and let* $\psi : \mathbb{Z}[G] \to R$ *be a ring surjection for some abelian group G of exponent 2. Then*

(1) $C(X(R), \mathbb{Z})/R_{red}$ *is a 2-primary torsion group and* $C(X(R), \mathbb{Z})$ *is the integral closure of* R_{red} *in* $C(X(R), \mathbb{Q})$.

(2) The sets $H(g) = \{x \in X(R) | \psi(g)(x) = -1\}$, *where* $g \in G$, *and their complements form a subbasis* $\mathcal{H}(R)$ *of the topology of* $X(R)$.

(3) $\mathcal{H}(R)$ *is an additive subgroup of* $\mathcal{B}$, *the Boolean ring of all clopen subsets of* $X(R)$, *containing* $X(R)$.

(4) $R_{red} = \mathbb{Z} + \sum_{B \in \mathcal{H}(R)} 2\mathbb{Z} e_B$.

And now without further ado, we are ready to define the rings that are the subject of this thesis.

DEFINITION 2.10 A *Q-Witt ring* is a ring R formed by taking a finite quotient of a torsion free abstract Witt ring S for a group G of exponent 2, viewed as a subring of $C(X, \mathbb{Z})$ with $|X| < \infty$. We take the quotient by taking a function $f \in S$ to a function $\overline{f}$ in $C\left(X, \bigcup_{x \in X} \mathbb{Z}_{n_x}\right)$ such that $\overline{f}(x) \in \mathbb{Z}_{n_x}$ for each $x \in X$.

By [10, Remark 3.20] we know that $S \subset \mathbb{Z}^{|X|}$, thus it is an easy observation that a Q-Witt ring R is a subring of $\prod_{x \in X} \mathbb{Z}_{n_x}$ and hence in particular a finite ring. In view of

Theorem 1.2, it will be useful to know when a ring breaks up as a product.

We give a topological characterization in terms of the prime spectrum.

DEFINITION 2.11 A ring R is called *connected* if $SpecR$ is a connected topological space.

REMARK 2.12 From [12, Pg 79] we recall that $SpecR$ is a connected topological space if $SpecR$ is not the union of two disjoint non-empty closed/open sets.

In order for us to prove the next theorem, we will remind the reader that for each subset E of R, the closed subsets of $SpecR$, $V(E)$ are the sets consisting of all prime ideals of R containing E. Further, for any $r \in R$, the sets U_r denote the complement of $V(\{r\})$ in $SpecR$ and form a basis of open sets for the Zariski topology.

THEOREM 2.13 *Let $\phi : A \to B$ be a ring homomorphism between arbitrary commutative rings. For any $\mathcal{P} \in SpecB$, we know that $\phi^{-1}(\mathcal{P}) \in SpecA$.*

Then the induced map $\phi^\star : SpecB \to SpecA$ is continuous.

Proof. To show that $\phi^\star$ is continuous we need to show that for any open set U_a in $SpecA$, $a \in A$, $(\phi^\star)^{-1}(U_a)$ is open in $SpecB$. More specifically, we will show that $(\phi^\star)^{-1}(U_a) = U_{\phi(a)}$ in $SpecB$.

So, let $a \in A$. Then $\mathcal{P} \in U_{\phi(a)} \Leftrightarrow \phi(a) \notin \mathcal{P} \Leftrightarrow a \notin \phi^{-1}(\mathcal{P}) \subseteq A$

$\Leftrightarrow \phi^{-1}(\mathcal{P}) \in U_a \Leftrightarrow \mathcal{P} \in (\phi^\star)^{-1}(U_a)$.

THEOREM 2.14 *Let R be a finite commutative ring. Then R is a local ring if and only if R is connected.*

Proof. Suppose R is local. Then we will show that $SpecR$ can't be expressed as the union of two disjoint non-empty closed/open sets. Suppose $SpecR = A \cup B$, where A and B are two non-empty closed sets. Then we know that $A = V(I)$ and $B = V(J)$, where I and J are some ideals in R. Since R is local it contains a unique maximal ideal $\mathfrak{m}$, with $I \subseteq \mathfrak{m}$ and $J \subseteq \mathfrak{m}$, which implies that $\mathfrak{m} \in V(I) \cap V(J) = A \cap B$, so $A \cap B \neq \emptyset$.

Next, suppose R is not local. Then by Theorem 1.2 we know that we can express R as a product $R_1 \times R_2$. Then we will show that $SpecR$ is the disjoint union of the closed subsets of $SpecR$, X_1 and X_2, which are homeomorphic to $SpecR_1$ and $SpecR_2$ respectively, and so R is not connected.

Consider the surjective ring homomorphisms $\phi_i : R \to R_i$ for $i = 1,2$. Then by Theorem 2.13 the induced maps $\phi_i^\star : SpecR_i \to SpecR$ are continuous for $i = 1,2$.

We claim that for $i = 1,2$, $SpecR_i$ is homeomorphic to the closed subset $X_i = V(Ker\phi_i)$ of $SpecR$. To show this is a homeomorphism, we observe that for each i, since ϕ_i is surjective, there is a one to one correspondence between the prime ideals of R containing $Ker\phi_i$ and the prime ideals of R_i. Thus, $\phi_i^\star$ is a bijection of $SpecR_i$ and X_i for $i = 1,2$.

Also, since $\phi_i^\star : SpecR_i \to SpecR$ is continuous, if we can show that $\phi_i^\star(SpecR_i) \subseteq X_i$, then the function $\Phi_i^\star : SpecR_i \to X_i$ obtained by restricting the range of $\phi_i^\star$ is continuous as well for $i = 1,2$. Thus, for any $\mathcal{P} \in SpecR_i$, we have that $\Phi_i^\star(\mathcal{P}) = \phi_i^{-1}(\mathcal{P}) \supseteq \phi_i^\star((0)) = Ker\phi_i$, so $\phi_i^\star(\mathcal{P}) \in X_i$ or $\Phi_i^\star$ is continuous.

Similarly, $\Phi_i^\star(V(\mathcal{P})) = V(\Phi_i^\star(\mathcal{P}))$ for any $\mathcal{P} \in SpecR_i$, we have

$S \in V(\Phi_i^\star(\mathcal{P})) \Leftrightarrow S \supseteq \Phi_i^\star(\mathcal{P}) = \phi_i^{-1}(\mathcal{P}) \Leftrightarrow \phi_i(S) \supseteq \mathcal{P} \Leftrightarrow \phi_i(S) \in V(\mathcal{P})$.

Hence, Φ_i^* is a homeomorphism of $SpecR_i$ and $X_i = V(Ker\phi_i)$. Thus, we have that $X_i \subseteq SpecR$ for $i = 1,2$ and so $X_1 \cup X_2 \subseteq SpecR$.

Next, we show that $SpecR$ is the disjoint union of X_1 and X_2. First, observe that $X_1 = V(Ker\phi_1) = \{P \subseteq R_1 \times R_2 \mid P \supseteq \{0\} \times R_2\}$ and $X_2 = V(Ker\phi_2) = \{P \subseteq R_1 \times R_2 \mid P \supseteq R_1 \times \{0\}\}$. Therefore, $X_1 \cap X_2 = \emptyset$, for if $P \in X_1 \cap X_2$, then $P \supseteq \{0\} \times R_2$ and $P \supseteq R_1 \times \{0\}$, which implies that $P \supseteq R_1 \times R_2$ so $P = R_1 \times R_2$. However, that is a contradiction, since $R_1 \times R_2$ is not a prime ideal. Finally, we must show that $SpecR \subseteq X_1 \cup X_2$ to complete our proof. So, suppose $P \in SpecR$. Then since P is a prime, if $(a,b) \in P$ then either $(a,1) \in P$ or $(1,b) \in P$. If $(a,1) \in P$, then $(0,1) \in P$. Therefore, $\{0\} \times R_2 \subseteq P$, which implies that $P \in V(\{0\} \times R_2) = V(Ker\phi_1) = X_1$. On the other hand, if $(1,b) \in P$, then $(1,0) \in P$. In this event, $R_1 \times \{0\} \subseteq P$, which implies that $P \in V(R_1 \times \{0\}) = V(Ker\phi_2) = X_2$. Hence, $P \in SpecR \subseteq X_1 \cup X_2$.

At this point we observe that if R can be expressed as a product of two rings, then R is not connected (by the second part of the above proof). Hence, if R has nontrivial idempotents e and f, then R is not connected [12, Exercise 11 Page 79]. Equivalently, if R is connected, then it contains no nontrivial idempotents. Using these observations, Theorem 1.2 and [14, Theorem VII.7], we see that the only finite commutative rings with no nontrivial idempotents are local.

The main goal of the remainder of this thesis is to analyze the structure of Q-Witt rings. Due to Theorem 1.2, we know that since Q-Witt rings are finite rings, it is only necessary to find the local Q-Witt rings in order to fully understand the structure of all Q-Witt rings. We will show in the next series of theorems that if a Q-Witt ring is local then each n_x must be a power of 2, or $|X| = 1$ and n_x is a power of a prime.

THEOREM 2.15 *Let R be a Q-Witt ring, with $R \subseteq C\left(X, \bigcup_{x\in X} \mathbb{Z}_{n_x}\right)$, $X = X(R)$. If $n_x = \prod_{i=1}^{k} p_i^{a_i}$ for some $x \in X$, p_i distinct primes and $k \geq 2$, then R is not local.*

Proof. We will view R as a subring of $\prod_{x\in X} \mathbb{Z}_{n_x}$. We will show that R has more than one maximal ideal, which implies that R is not connected by Theorem 2.14. Therefore, by Theorem 1.2 the ring R decomposes as a nontrivial direct sum of local rings.

To see that R contains more than one maximal ideal, we can construct a restriction map at x by $\Psi : R \to \mathbb{Z}_{n_x}$. By the Chinese Remainder Theorem, we know that $\mathbb{Z}_{n_x} \cong \prod_{i=1}^{k} \mathbb{Z}_{p_i^{a_i}}$, which implies that there is an induced ring homomorphism $\Psi_i : R \to \mathbb{Z}_{p_i}$ for each i, $1 \leq i \leq k$. Then $R/Ker(\Psi_i)$ is isomorphic to the field $\mathbb{Z}_{p_i}$, which implies that $M_i = Ker(\Psi_i) \subseteq R$ is a maximal ideal in R for each i. Since $k \geq 2$ we know that R has at least two maximal ideals, call them M_1 and M_2. To see that M_1 is distinct from M_2 we need only to observe that $R/M_1 = R/Ker(\Psi_1) \cong \mathbb{Z}_{p_1}$ and $R/M_2 = R/Ker(\Psi_2) \cong \mathbb{Z}_{p_2}$ are not isomorphic since $p_1 \neq p_2$.

It follows from this theorem that we need only consider Q-Witt rings where each n_x is a power of a prime. In this next theorem we will investigate what happens in the event that n_x and n_y are powers of distinct primes for some $x, y \in X$.

THEOREM 2.16 *Let R be a Q-Witt ring, with* $R \subseteq C\left(X, \bigcup_{x \in X} \mathbb{Z}_{n_x}\right)$, *where*

$n_x = p^{a_x}$ *and* $n_y = q^{a_y}$ for some $x, y \in X = X(R)$ and distinct prime integers p and q.

Then R is not connected, hence is not local.

Proof. We view the ring R as a subring of $\prod_{x \in X} \mathbb{Z}_{p^{a_x}}$. Then we can construct a restriction map at x by $\Psi_x : R \to \mathbb{Z}_{p^{a_x}}$, and similarly a residue map at y by $\Psi_y : R \to \mathbb{Z}_{q^{a_y}}$.

These induce ring surjections $\Psi_x : R \to \mathbb{Z}_p$ and $\Psi_y : R \to \mathbb{Z}_q$.

Since $R/Ker(\Psi_x)$ is isomorphic to the field $\mathbb{Z}_p$ and $R/Ker(\Psi_y)$ is isomorphic to the field $\mathbb{Z}_q$, we have that $M_x = Ker(\Psi_x)$ and $M_y = Ker(\Psi_y)$ are both maximal ideals in R, and are distinct as in the previous proof.

As a result of the above theorem we can concentrate on Q-Witt rings where each n_x is a power of the same fixed prime. We will consider two cases. First, we will look at the case when each n_x is a power of an odd prime, and lastly we will show the rings we obtain when each n_x is a power of 2, actually are connected so are local.

THEOREM 2.17 *Let R be a Q-Witt ring, with* $R \subseteq C\left(X, \bigcup_{x \in X} \mathbb{Z}_{p^{a_x}}\right)$, *where*

$X = X(R)$ *and p is an odd prime. Then*

(1) if $|X| = 1$, *then R is a local ring,*

(2) if $|X| > 1$, *then R is not local.*

Proof. The proof of (1) is trivial, since $R = \mathbb{Z}_{p^{\alpha_z}}$ which is a local ring.

To show (2) we recall that R is a finite quotient of a torsion free abstract Witt ring S for a group G of exponent 2. Therefore, we have a natural ring homomorphism from $\mathbb{Z}[G]$ onto $S \subseteq C(X,\mathbb{Z})$ and thus from $\mathbb{Z}[G]$ onto $R \subseteq C(X,\bigcup_{x\in X}\mathbb{Z}_{p^{\alpha_x}})$. Let us choose $z,w \in X$ such that $\alpha_z \geq \alpha_w$. Then since we know that R separates the points of X, there is a $g \in G$ so that $z \in H(g)$ and $w \notin H(g)$ for $H(g)$ as described in Theorem 2.9. Therefore, we can construct a restriction map $\Phi : \mathbb{Z}[G] \to C(X,\bigcup_{x\in X}\mathbb{Z}_{p^{\alpha_x}})$ to $\{z,w\} \subseteq X$.

The map $\Phi : \mathbb{Z}[G] \to C(\{z,w\},\mathbb{Z}_{p^{\alpha_z}}\bigcup\mathbb{Z}_{p^{\alpha_w}})$ is defined by

$\Phi(ae+bg) = \overline{a\cdot 1 + b(1-2e_{H(g)})} \in R$. Using this ring homomorphism we will show that in fact R contains a nontrivial idempotent and thus by earlier observations, we know that R is not connected. To construct this idempotent we consider $\frac{p^{\alpha_z}+1}{2}e - \frac{p^{\alpha_z}+1}{2}g$ an element of $\mathbb{Z}[G]$. Then we claim that

$$\overline{f} = \Phi\left(\frac{p^{\alpha_z}+1}{2}e - \frac{p^{\alpha_z}+1}{2}g\right) = \overline{\frac{p^{\alpha_z}+1}{2}\cdot 1 - \frac{p^{\alpha_z}+1}{2}(1-2e_{H(g)})}$$

is an idempotent we are looking for.

To see this observe that

$\overline{f}(z) = \overline{\frac{p^{\alpha_z}+1}{2}\cdot 1 - \frac{p^{\alpha_z}+1}{2}(1-2e_{H(g)}(z))} = p^{\alpha_z}+1 = 1$ modulo p^{α_z} and

$\overline{f}(w) = \overline{\frac{p^{\alpha_z}+1}{2}\cdot 1 - \frac{p^{\alpha_z}+1}{2}(1-2e_{H(g)}(w))} = 0$ modulo p^{α_w} so

it is clear that $\overline{f}$ is a nontrivial idempotent.

In light of the above theorem, we have now only to consider the structure of the Q-Witt Rings, where each n_x is a power of 2. We will show in the next theorem that these rings are in fact local rings.

THEOREM 2.18 *Let R be a Q-Witt ring, with* $R \subseteq C\left(X, \bigcup_{x \in X} \mathbb{Z}_{2^{\alpha_x}}\right), X = X(R)$.

Then R is a local ring.

We will prove the above theorem using some lemmas, which we shall state and prove first.

LEMMA 2.19 *Suppose* $r_1, \ldots, r_n$ *are integers and n a positive integer with* $n \geq 2$.

If we let $\varepsilon_i \in \{\pm 1\}$ *for* $i = 1, \ldots, n$, *then we have that* $\sum_{i=1}^{n} r_i \equiv \sum_{i=1}^{n} \varepsilon_i r_i \pmod 2$.

Proof. Observe that for each i, $1 - \varepsilon_i = 0$ or 2, hence

$$\sum_{i=1}^{n} r_i - \sum_{i=1}^{n} \varepsilon_i r_i = \sum_{i=1}^{n} (1 - \varepsilon_i) r_i \equiv 0 \pmod 2.$$

LEMMA 2.20 *Suppose n and* $\alpha_1, \ldots, \alpha_n$ *are positive integers. Then we have the group isomorphism* $\left(\prod_{i=1}^{n} \mathbb{Z}_{2^{\alpha_i}}\right)^* \cong \prod_{i=1}^{n} \mathbb{Z}_{2^{\alpha_i}}^*$.

Proof. Let $f : \prod_{i=1}^{n} \mathbb{Z}_{2^{\alpha_i}}^* \to \left(\prod_{i=1}^{n} \mathbb{Z}_{2^{\alpha_i}}\right)^*$ be the map defined by $f((a_i)) = (a_i)$, where $a_i \in \mathbb{Z}_{2^{\alpha_i}}^*$ for each i, $1 \leq i \leq n$. Then it is easy to see that f is a group homomorphism, since for $(a_i), (b_i) \in \prod_{i=1}^{n} \mathbb{Z}_{2^{\alpha_i}}^*$, we have that

$$f((a_i)(b_i)) = f((a_i b_i)) = (a_i b_i) = (a_i)(b_i) = f((a_i))f((b_i))$$

and also $f((1_i)) = (1_i)$. f is injective, since if $(a_i) \in Ker(f)$ then $f((a_i)) = (1_i)$ implies that $(a_i) = (1_i)$ or $a_i = 1$ for each i, $1 \leq i \leq n$. Finally, we need only to show that in fact f is surjective, to show that f is an isomorphism.

So, let us suppose we have $(a_i) \in \left(\prod_{i=1}^{n} \mathbb{Z}_{2^{\alpha_i}}\right)^*$. Then we know there exists an element $(b_i) \in \left(\prod_{i=1}^{n} \mathbb{Z}_{2^{\alpha_i}}\right)^*$ so that $(a_i)(b_i) = (a_i b_i) = (1_i)$, which implies that $a_i \in \mathbb{Z}^*_{2^{\alpha_i}}$ for each i, $1 \leq i \leq n$. So, the element $(a_i) \in \prod_{i=1}^{n} \mathbb{Z}^*_{2^{\alpha_i}}$.

And now without further ado we prove Theorem 2.18.

Proof. As before, we recall that R is a finite quotient of a torsion free abstract Witt ring S for a group G of exponent 2. Therefore, by definition we know we have a natural ring homomorphism from $\mathbb{Z}[G]$ onto $S \subseteq C(X, \mathbb{Z})$ and thus from $\mathbb{Z}[G]$ onto $R \subseteq C(X, \bigcup_{x \in X} \mathbb{Z}_{2^{\alpha_x}})$. Since each $g \in G$ has exponent 2, the image of each g is a function of the form $f_g = 1 - 2e_{H(g)}$ in S as was described in Theorem 2.9. Using this observation we have a ring homomorphism $\Phi : \mathbb{Z}[G] \to S \to R \subseteq C(X, \bigcup_{x \in X} \mathbb{Z}_{2^{\alpha_x}})$ defined by $\Phi\left(\sum_{g \in G} a_g g\right) = \overline{a_{e'} + \sum_{g \in G} a_g(1 - 2e_{H(g)})} \in R$, where e' is the identity in G. Using this characterization, we will show that R has a unique maximal ideal and thus R is local. To do this, we observe that if $\overline{f} = \overline{a_{e'} + \sum_{g \in G} a_g(1 - 2e_{H(g)})} \in R$, then for each $x \in X$, by definition of the characteristic function, $1 - 2e_{H(g)}(x) \in \{\pm 1\}$. So if

we let $\varepsilon_{(x,g)} \in \{\pm 1\}$, then $\overline{f}(x) = (a_{e'} + \sum_{g\in G} \varepsilon_{(x,g)} a_g) (\mathrm{mod}\, 2^{\alpha_x})$ for each $x \in X$, where

e' is the identity of G and each $a_g \in \mathbb{Z}$.

Further, we recall that if we denote by $\mathfrak{m}_x$ the maximal ideal of $\mathbb{Z}_{2^{\alpha_x}}$, then we have that

$\mathbb{Z}_{2^{\alpha_x}} = \mathbb{Z}^*_{2^{\alpha_x}} \cup \mathfrak{m}_x$. Also, it is easy to see that either $(a_{e'} + \sum_{g\in G} \varepsilon_{(x,g)} a_g) \equiv 0 (\mathrm{mod}\, 2)$ and

so $(a_{e'} + \sum_{g\in G} \varepsilon_{(x,g)} a_g) \in \mathfrak{m}_x$ or $(a_{e'} + \sum_{g\in G} \varepsilon_{(x,g)} a_g) \equiv 1 (\mathrm{mod}\, 2)$ and so $(a_{e'} + \sum_{g\in G} \varepsilon_{(x,g)} a_g) \in \mathbb{Z}^*_{2^{\alpha_x}}$

for each $x \in X$. We can further see using Lemma 2.19 that for all $x, y \in X$, we have

that $(a_{e'} + \sum_{g\in G} \varepsilon_{(x,g)} a_g) \equiv (a_{e'} + \sum_{g\in G} \varepsilon_{(y,g)} a_g) (\mathrm{mod}\, 2)$, which implies that

either $(a_{e'} + \sum_{g\in G} \varepsilon_{(x,g)} a_g) \in \mathfrak{m}_x$ and $(a_{e'} + \sum_{g\in G} \varepsilon_{(y,g)} a_g) \in \mathfrak{m}_y$, or $(a_{e'} + \sum_{g\in G} \varepsilon_{(x,g)} a_g) \in \mathbb{Z}^*_{2^{\alpha_x}}$

and $(a_{e'} + \sum_{g\in G} \varepsilon_{(y,g)} a_g) \in \mathbb{Z}^*_{2^{\alpha_y}}$. These observations now allow us to say that $\overline{f}(x) \in \mathfrak{m}_x$ for all

x or $\overline{f}(x) \in \mathbb{Z}^*_{2^{\alpha_x}}$ for all $x \in X$. Thus, $\overline{f} \in R$ if and only if $\overline{f} \in \left(\prod_{x\in X} \mathbb{Z}^*_{2^{\alpha_x}}\right) \cup \left(\prod_{x\in X} \mathfrak{m}_x\right)$,

which by Lemma 2.20 means that $\overline{f} \in \left(\prod_{x\in X} \mathbb{Z}_{2^{\alpha_x}}\right)^* \cup \left(\prod_{x\in X} \mathfrak{m}_x\right)$. Therefore,

$R \subseteq \left(\prod_{x\in X} \mathbb{Z}_{2^{\alpha_x}}\right)^* \cup \left(\prod_{x\in X} \mathfrak{m}_x\right)$, which is clearly a local ring. This implies that R has no

nontrivial idempotents, so must also be local.

PROPOSITION 2.21 *The largest possible Q-Witt ring R, with*

$R \subseteq C\left(X, \bigcup_{x\in X} \mathbb{Z}_{2^{\alpha_x}}\right)$ *has the form* $\left(\prod_{x\in X} \mathbb{Z}_{2^{\alpha_x}}\right)^* \cup \left(\prod_{x\in X} \mathfrak{m}_x\right)$ *with* $|R| = 2\prod_{x\in X} 2^{\alpha_x - 1}$.

Proof. By [11, Example 3.9 and Theorem 3.20] the largest torsion free Witt ring

S is of the form $S = \mathbb{Z} + C(X, 2\mathbb{Z})$. Therefore, the largest possible Q-Witt ring will be

the quotient of $S = \mathbb{Z} + C(X, 2\mathbb{Z})$. By the proof of Theorem 2.18 we know that $R \subseteq \left(\prod_{x\in X} \mathbb{Z}_{2^{\alpha_x}}\right)^* \cup \left(\prod_{x\in X} \mathrm{m}_x\right)$, and since R is the largest possible such subring implies that R must be $\left(\prod_{x\in X} \mathbb{Z}_{2^{\alpha_x}}\right)^* \cup \left(\prod_{x\in X} \mathrm{m}_x\right)$. Since $|\mathbb{Z}^*_{2^{\alpha_x}}| = |\mathrm{m}_x| = 2^{\alpha_x - 1}$, we have that $\left|\left(\prod_{x\in X} \mathbb{Z}_{2^{\alpha_x}}\right)^* \cup \left(\prod_{x\in X} \mathrm{m}_x\right)\right| = 2\prod_{x\in X} 2^{\alpha_x - 1}$. Hence, $|R| = 2\prod_{x\in X} 2^{\alpha_x - 1}$.

PROPOSITION 2.22 *Let R be a Q-Witt ring, with $R \subseteq C\left(X, \bigcup_{x\in X} \mathbb{Z}_{2^{\alpha_x}}\right)$. Then R is a finite quotient of a torsion free abstract Witt ring S for a group G of exponent 2.*

(1) for $\alpha = \max_{x\in X} \alpha_x$ we have that $char(R) = 2^\alpha$ and $|R|$ divides $2\prod_{x\in X} 2^{\alpha_x - 1}$,

(2) the maximal ideal m of R is generated by $0 \leq k \leq |G|$ elements of the form $2e_{H(g)}$ for some $g \in G$, and

(3) the residue field of R is $\mathbb{Z}_2$ and R is a homomorphic image of $\mathbb{Z}_{2^\alpha}[y_1, \ldots, y_k]$, for some indeterminates $y_1, \ldots, y_k$.

Proof. The first part of part (1) is clear. To see that $|R|$ divides $2\prod_{x\in X} 2^{\alpha_x - 1}$, we need to recall from the proof of Theorem 2.18 that R is a subring of $T = \left(\prod_{x\in X} \mathbb{Z}_{2^{\alpha_x}}\right)^* \cup \left(\prod_{x\in X} \mathrm{m}_x\right)$. Thus, by Proposition 2.21 the order of R divides the order of T so $|R|$ divides $2\prod_{x\in X} 2^{\alpha_x - 1}$.

Observe that the maximal ideal of T is $\prod_{x\in X} \mathrm{m}_x$, where we denote by m_x the maximal ideal of $\mathbb{Z}_{2^{\alpha_x}}$ as in the proof of Theorem 2.18, hence $\mathrm{m} \subseteq \prod_{x\in X} \mathrm{m}_x$.

Then $\Phi(1-g) = 2e_{H(g)} \in R$ for all $g \in G$ and $2e_{H(g)}(x) \in \{0,2\}$ for each $x \in X$. Thus, $2e_{H(g)}(x) \in \mathfrak{m}_x \subseteq \prod_{x \in X} \mathfrak{m}_x$ for each $x \in X$. Therefore, the ideal generated by the set $\{2e_{H(g)} \mid \text{for some } g \in G\}$ is contained in $\mathfrak{m}$. By [10, Theorem 2.9 (iv)], we know that the unique maximal ideal containing 2, the augmentation ideal M_0 in S, is generated by the same set. Furthermore, since we have the surjection $S \to R$, and $S/M_0 \cong \mathbb{Z}_2$ and $R/\mathfrak{m} \cong \mathbb{Z}_2$, we can conclude that M_0 maps onto $\mathfrak{m}$. Thus, $\mathfrak{m}$ is contained in the ideal generated by the set $\{2e_{H(g)} \mid \text{for some } g \in G\}$, which concludes our proof of part (2). Finally, by Theorem 1.24 and parts (1) and (2) we can conclude part (3).

CHAPTER 3
GROUP RINGS

In this chapter we will focus our attention on Q-Witt rings, which are simply quotients of the integral group ring $\mathbb{Z}[G]$, where G is an elementary abelian 2-group. We recall that every abstract Witt ring for a group G in fact occurs as a quotient $\mathbb{Z}[G]/K$, where the ideal K satisfies properties as in Definition 2.5. For the remainder of this chapter we will consider the special case when the ideal K is the zero ideal. We show what all Q-Witt rings look like in the case of $|G| = 2$ and generalize some of our results for $|G| > 2$.

THEOREM 3.1 [3, Theorem 3.8 (a),(b) & (e)] *Let S be a Witt ring, $S = S_{red}$ and $|X(S)| = 2^n$, $n \geq 0$. Let $\mathcal{H}(S)$ be a subbasis for the topology of $X(S)$. Then the following are equivalent:*

(1) $S = \mathbb{Z}[G]$ (and G has order 2^n);

(2) if $H \in \mathcal{H}(S)$, $H \neq \emptyset, X$, then $|H| = 2^{n-1}$;

(3) $|\mathcal{H}(S)| = 2^{n+1}$.

Recall from Chapter 2 that all abstract Witt rings, hence Q-Witt rings, are quotient rings of Witt rings described in Theorem 3.1, that is quotients of a group ring $\mathbb{Z}[G]$. We shall see that for group rings we can do explicit computations of some of the more general results of Chapter 2.

At first, if $n = 0$, then X has only one point, say x, so $S = \mathbb{Z}$, thus $R \cong \mathbb{Z}_{n_x}$. Thus, from now on we will assume $n \geq 1$.

We consider the quotients $R \subseteq C(\{x,y\}, \mathbb{Z}_{n_x} \cup \mathbb{Z}_{n_y})$ of $\mathbb{Z}[\mathbb{Z}_2]$. We will approach this problem by considering four cases, all of which give us some different and interesting results. In our first case, both n_x and n_y are arbitrary integers with the only restriction being that $\gcd(n_x, n_y) = 1$; in our second case we shall investigate what happens when n_x and n_y are both positive odd integers with $\gcd(n_x, n_y) > 1$; thirdly we will consider what quotients we shall realize if, without loss of generality, n_x is an even positive integer and n_y is an odd positive integer. And finally, in our fourth case, we will let n_x and n_y be arbitrary even integers. Our goal of this chapter will be to generalize the findings from the case $|X| = 2$ to when $|X| = 2^n$. We shall write the group $\mathbb{Z}_2 = \{e', g\}$ and $[a]_b = a \bmod b$.

LEMMA 3.2 *Let n_x and n_y be positive integers with* $\gcd(n_x, n_y) = 1$.

Then $R \subseteq C(\{x,y\}, \mathbb{Z}_{n_x} \cup \mathbb{Z}_{n_y})$ is isomorphic to $\mathbb{Z}_{n_x} \times \mathbb{Z}_{n_y} \cong \mathbb{Z}_{n_x n_y}$.

Proof. First observe that R is naturally a subring of $\mathbb{Z}_{n_x} \times \mathbb{Z}_{n_y}$. Let θ be the homomorphism $\mathbb{Z}[\mathbb{Z}_2] \to C(\{x,y\}, \mathbb{Z}) \to C(\{x,y\}, \mathbb{Z}_{n_x} \cup \mathbb{Z}_{n_y}) \cong \mathbb{Z}_{n_x} \times \mathbb{Z}_{n_y}$. Since g is a unit in $\mathbb{Z}[\mathbb{Z}_2]$, g is mapped to a unit $f_g = 1 - 2e_{H(g)} \in C(\{x,y\}, \mathbb{Z})$, by Lemma 2.8(4), and e' is mapped to the constant function 1. We may assume that $x \notin H(g)$ and $y \in H(g)$. Then θ is defined explicitly by

$$\theta(re' + sg) = ([r+s]_{n_x}, [r-s]_{n_y}).$$

Therefore, to prove our claim we must demonstrate that θ is surjective. To do this observe that we only need that $([1]_{n_x}, [0]_{n_y})$ and $([0]_{n_x}, [1]_{n_y})$ are in the image of θ, since these elements will generate all of $\mathbb{Z}_{n_x} \times \mathbb{Z}_{n_y}$.

Now, since the $\gcd(n_x, n_y) = 1$, we know that there exist integers u, v such that $un_x + vn_y = 1$. If we let $r = vn_y$ and $s = 0$, then

$$\theta(re' + sg) = ([1 - un_x]_{n_x}, [vn_y]_{n_y}) = ([1]_{n_x}, [0]_{n_y}).$$

Similarly, if we let $r = un_x$ and $s = 0$, we find that

$$\theta(re' + sg) = ([un_x]_{n_x}, [1 - vn_y]_{n_y}) = ([0]_{n_x}, [1]_{n_y}),$$

which concludes the proof.

At this time before we discuss the other cases we would like to give an example.

EXAMPLE 3.3 We consider the quotient of $\mathbb{Z}[\mathbb{Z}_2]$, where we let $n_x = 2$ and $n_y = 3$. Then according to Theorem 3.4, $R \cong \mathbb{Z}_6$. One can easily check this, since the homomorphism which takes $re' + sg \to ([r + s]_2, [r - s]_3)$ gives us that, in this case the image of $\mathbb{Z}e'$ already is $\{(1,1),(0,2),(1,0),(0,1),(1,2),(0,0)\} \cong \mathbb{Z}_6$. We can also realize R as the quotient ring $\mathbb{Z}_6[\mathbb{Z}_2]/(e' + g)$, since this ring has exactly 6 elements due to the fact that the ideal $(e' + g) = \{e' + g, 2e' + 2g, 3e' + 3g, 4e' + 4g, 5e' + 5g, 0\}$.

REMARK 3.4 It is important for us to observe that our proof of Lemma 3.2 shows that in this case R is the image of $\mathbb{Z}e'$, since we were able to take $s = 0$ for both preimages.

LEMMA 3.5 *Let n_x and n_y be positive odd integers. Then $R \subseteq C(\{x,y\}, \mathbb{Z}_{n_x} \cup \mathbb{Z}_{n_y})$ is isomorphic to $\mathbb{Z}_{n_x} \times \mathbb{Z}_{n_y}$.*

Proof. As before we need to show that $\theta : \mathbb{Z}[\mathbb{Z}_2] \to \mathbb{Z}_{n_x} \times \mathbb{Z}_{n_y}$ as defined in the proof of Lemma 3.2 is an epimorphism.

This time we shall show that any element $([m]_{n_x},[k]_{n_y}) \in \mathbb{Z}_{n_x} \times \mathbb{Z}_{n_y}$, must have a pre-image in $\mathbb{Z}[\mathbb{Z}_2]$.

Let $r = \dfrac{m(n_x+1)+k(n_y+1)}{2}$ and $s = \dfrac{m(n_x+1)-k(n_y+1)}{2}$.

It is easy to see that $r,s \in \mathbb{Z}$, since $2|(n_x+1)$ and $2|(n_y+1)$.

By making the above choice for r and s, we can calculate

$$\theta(re^{'}+sg) = \theta(\frac{m(n_x+1)+k(n_y+1)}{2}e^{'} + \frac{m(n_x+1)-k(n_y+1)}{2}g) =$$

$\left([m(n_x+1)]_{n_x},[k(n_y+1)]_{n_y}\right) = ([m]_{n_x},[k]_{n_y}) \in \mathbb{Z}_{n_x} \times \mathbb{Z}_{n_y}$. So indeed θ is an epimorphism.

LEMMA 3.6 *Let n_x and n_y be positive integers with $n_x = 2k$ and $n_y = 2m+1$, where k and m are positive integers. Then $R \subseteq C(\{x,y\}, \mathbb{Z}_{n_x} \cup \mathbb{Z}_{n_y})$ is isomorphic to $\mathbb{Z}_{n_x} \times \mathbb{Z}_{n_y}$.*

Proof. As before we need to show that $\theta : \mathbb{Z}[\mathbb{Z}_2] \to \mathbb{Z}_{n_x} \times \mathbb{Z}_{n_y}$ as defined in the proof of Lemma 3.2 is an epimorphism. We will show that $([1]_{n_x},[0]_{n_y})$ and $([0]_{n_x},[1]_{n_y})$ are in the image of θ.

Now, by letting $r = k+m+1$ and $s = k-m$, we can easily check that in fact,

$$\theta(re^{'}+sg) = \theta((k+m+1)e^{'}+(k-m)g) = \left([2k+1]_{n_x},[2m+1]_{n_y}\right) =$$

$([n_x+1]_{n_x},[n_y]_{n_y}) = \left([1]_{n_x},[0]_{n_y}\right) \in \mathbb{Z}_{n_x} \times \mathbb{Z}_{n_y}$.

Similarly, by letting $r = k+m+1$ and $s = k-m-1$, we can see that

$$\theta(re^{'}+sg) = \theta((k+m+1)e^{'}+(k-m-1)g) = \left([2k]_{n_x},[2m+2]_{n_y}\right) =$$

$([n_x]_{n_x},[n_y+1]_{n_y}) = \left([0]_{n_x},[1]_{n_y}\right) \in \mathbb{Z}_{n_x} \times \mathbb{Z}_{n_y}$.

So indeed θ is an epimorphism.

The above two types of Q-Witt rings are special cases of Q-Witt rings, which we proved in Chapter 2 to be not connected. We confirmed this of course by specifically proving what their ring structure is. In both of the above cases the image of the Witt rings turned out to be the product $\mathbb{Z}_{n_x} \times \mathbb{Z}_{n_y}$, which are rings that are well understood. We point out that these rings are mentioned in [10, Theorem 3.8] but are not Witt rings for the group $\mathbb{Z}_2$, since they do not meet the conditions of Definition 2.5. So while our Q-Witt rings do sometimes fall outside the category of abstract Witt rings of [10], Chapter 2 shows that this occurs only via a product with quotients of $\mathbb{Z}$.

In order for us to discuss the last cases we need to introduce some new notation. Suppose k is a positive integer, say $k = 2m$, where m is a positive integer. The set $\mathbb{Z}_k = \{0, 1, \ldots, k-1\}$ can be written as the union of $E(\mathbb{Z}_k)$ and $O(\mathbb{Z}_k)$, where $E(\mathbb{Z}_k) = \{0, 2, \ldots, k-2\}$ and $O(\mathbb{Z}_k) = \{1, 3, \ldots, k-1\}$. Clearly, we have that $E(\mathbb{Z}_k) \cap O(\mathbb{Z}_k) = \emptyset$. Also, using elementary number theory, it is easy to show that if k_1 and k_2 are even positive integers, then $(O(\mathbb{Z}_{k_1}) \times O(\mathbb{Z}_{k_2})) \cup (E(\mathbb{Z}_{k_1}) \times E(\mathbb{Z}_{k_2}))$ is a subring of $\mathbb{Z}_{k_1} \times \mathbb{Z}_{k_2}$. In fact, if k_1 and k_2 are both powers of 2, this subring is connected, so local, by Theorem 2.18 and Proposition 2.21.

LEMMA 3.7 *Let n_x and n_y be positive even integers. Then $R \subseteq C(\{x,y\}, \mathbb{Z}_{n_x} \cup \mathbb{Z}_{n_y})$ is isomorphic to $(O(\mathbb{Z}_{n_x}) \times O(\mathbb{Z}_{n_y})) \cup (E(\mathbb{Z}_{n_x}) \times E(\mathbb{Z}_{n_y}))$.*

Proof. As in all the above cases, the mapping $\theta : \mathbb{Z}[\mathbb{Z}_2] \to R$ given by $\theta(re^t + sg) = ([r+s]_{n_x}, [r-s]_{n_y})$ is a ring homomorphism. For any $re^t + sg \in \mathbb{Z}[\mathbb{Z}_2]$, since $r + s \equiv r - s \bmod 2$, we have $\theta(re + sg) \in (O(\mathbb{Z}_{n_x}) \times O(\mathbb{Z}_{n_y})) \cup (E(\mathbb{Z}_{n_x}) \times E(\mathbb{Z}_{n_y}))$.

To see that θ is surjective, let us first suppose $([a]_{n_x},[b]_{n_y}) \in O(\mathbb{Z}_{n_x}) \times O(\mathbb{Z}_{n_y})$. Then there exist integers $i \in \{0,1,\ldots,\frac{n_x-2}{2}\}$ and $j \in \{0,1,\ldots,\frac{n_y-2}{2}\}$, such that $a = 2i+1$ and $b = 2j+1$. By letting $r = i+j+1$ and $s = i-j$, we can see that

$$\theta(re' + sg) = ([(i+j+1)+(i-j)]_{n_x},[(i+j+1)-(i-j)]_{n_y}) = \left([a]_{n_x},[b]_{n_y}\right).$$

Next, suppose $([a]_{n_x},[b]_{n_y}) \in E(\mathbb{Z}_{n_x}) \times E(\mathbb{Z}_{n_y})$. Then there exist integers $k \in \{0,1,\ldots,\frac{n_x-2}{2}\}$ and $l \in \{0,1,\ldots,\frac{n_y-2}{2}\}$, such that $a = 2k$ and $b = 2l$. By letting $r = k+l$ and $s = k-l$, we can see that

$$\theta(re' + sg) = ([k+l)+(k-l)]_{n_x},[(k+l)-(k-l)]_{n_y}) = \left([a]_{n_x},[b]_{n_y}\right),$$

and hence θ is indeed onto.

EXAMPLE 3.8 We consider the Q-Witt ring R to be the quotient of $\mathbb{Z}[\mathbb{Z}_2]$, where $X = \{x,y\}$ and take $n_x = 4$ and $n_y = 6$. We view R as a subring of $\mathbb{Z}_4 \times \mathbb{Z}_6$. Then using the map $\theta : \mathbb{Z}[\mathbb{Z}_2] \to \mathbb{Z}_4 \times \mathbb{Z}_6$ defined in Lemma 3.2, we find that

$$R = \{(1,1),(2,2),(3,3),(0,4),(1,5),(2,0),(3,1),(0,2),(1,3),(2,4),(3,5),(0,0)\}.$$

Observe that R is not connected, since the element $(1,3)$ is a nontrivial idempotent. Hence, this ring is not a local ring. Also, since $|R| = 12$ and $char(R) = 12$, R must be isomorphic to $\mathbb{Z}_{12}[G]/(e'+g)$, since the ideal $(e'+g) = \{0, e+g, \ldots, 11e+11g\}$ has 12 elements. (Compare this to Example 3.11 below.) More familiarly, R is just $\mathbb{Z}_{12}$.

In this event R is the image of $\mathbb{Z}e'$, however, this is not the case in general for the Q-Witt rings which are of the form described in Lemma 3.7. Therefore, at this point we would like to find the ring structure of all the Q-Witt rings that occur as in Lemma 3.7.

LEMMA 3.9 *Let n_x and n_y be positive even integers. Then*

if $k = \dfrac{n_x n_y}{\gcd(n_x, n_y)} = \operatorname{lcm}(n_x, n_y)$ *and* $m = \dfrac{\gcd(n_x, n_y)}{2}$,

then $R \subseteq C(X, \mathbb{Z}_{n_x} \cup \mathbb{Z}_{n_y})$ *is isomorphic to* $\mathbb{Z}_k[\mathbb{Z}_2]/(me + mg)$ and $|R| = \frac{n_x n_y}{2} = km$.

Proof. Using the map $\theta : \mathbb{Z}[\mathbb{Z}_2] \to \mathbb{Z}_{n_x} \times \mathbb{Z}_{n_y}$ defined in Lemma 3.2, we find that

$$R = \mathbb{Z}_k \cup (\mathbb{Z}_k + \theta(g)) \cup \ldots \cup (\mathbb{Z}_k + (m-1)\theta(g)),$$

where if q is determined by writing $2m = \gcd(n_x, n_y) = rn_x + qn_y$, then

$m\theta(g) = ([m]_{n_x}, [-m]_{n_y}) = (qn_y - m)([1]_{n_x}, [1]_{n_y})$ since $qn_y - m = m - rn_x$.

Therefore, it is clear that $char(R) = k$, which implies that R must be isomorphic to a quotient of $\mathbb{Z}_k[\mathbb{Z}_2]$. Also, by counting we obtain

$|R| = km = \dfrac{n_x, n_y}{\gcd(n_x, n_y)} \dfrac{\gcd(n_x, n_y)}{2} = \dfrac{n_x, n_y}{2}$. These two observations together suggest that R must be isomorphic to $\mathbb{Z}_k[\mathbb{Z}_2]/(me + mg)$, since the ideal $(me + mg) = \{me + mg, \ldots, \frac{k}{m}(me + mg) = 0\}$ clearly has order $\frac{k}{m}$.

It is no surprise that the Q-Witt rings we just characterized are once again not local and thus not connected in all cases except for the following special case as we showed in Chapter 2.

COROLLARY 3.10 *Let* $n_x = 2^n$ *and* $n_y = 2^m$, *where* n, m *are positive integers with* $m \geq n$. *Then* $R \subseteq C(\{x,y\}, \mathbb{Z}_{n_x} \cup \mathbb{Z}_{n_y})$ *is isomorphic to* $(\mathbb{Z}_{2^n}^* \times \mathbb{Z}_{2^m}^*) \cup ((2\mathbb{Z}_{2^n}) \times (2\mathbb{Z}_{2^m}))$ *and therefore to* $\mathbb{Z}_{2^m}[\mathbb{Z}_2]/(2^{n-1}(e' + g))$ *and* $|R| = 2^{n+m-1}$.

EXAMPLE 3.11 We consider the Q-Witt ring R to be the quotient of $\mathbb{Z}[\mathbb{Z}_2]$, where $X = \{x,y\}$ and take $n_x = 2^2$ and $n_y = 2^3$. Then we view R as a subring of $\mathbb{Z}_4 \times \mathbb{Z}_8$. Using the map $\theta : \mathbb{Z}[\mathbb{Z}_2] \to \mathbb{Z}_4 \times \mathbb{Z}_8$ defined in Lemma 3.2, we find that

$$R = \{(1,1),(2,2),(3,3),(0,4),(1,5),(2,6),(3,7),(0,0),$$

$$\theta(g) = (1,7),(2,0),(3,1),(0,2),(1,3),(2,4),(3,5),(0,6)\}$$

so we can express $R = \mathbb{Z}_8 \cup (\mathbb{Z}_8 + \theta(g))$. This ring R has characteristic 8, so it is easy to see that R is a quotient of $\mathbb{Z}_8[\mathbb{Z}_2]$. Furthermore, it is easy to check that since R has 16 elements R is isomorphic to $\mathbb{Z}_8[\mathbb{Z}_2]/(2e' + 2g)$, where

$$(2e' + 2g) = \{2e' + 2g, 4e' + 4g, 6e' + 6g, 0\}$$

as was established in Corollary 3.10. Further, we can observe that the units of R, $R^* = \{(1,1),(1,3),(1,5),(1,7),(3,1),(3,3),(3,5),(3,7)\}$ have the property that each has order equal to 2. In addition, the maximal ideal of R,

$\mathfrak{m} = \{(0,0),(0,2),(0,4),(0,6),(2,0),(2,2),(2,4),(2,6)\} = ((0,2),(2,0))$.

We can also easily check that $\mathfrak{m}$ is the unique prime ideal of R. We can also conclude that this R is not a chain ring, since the maximal ideal $\mathfrak{m}$ is not a principal ideal.

Using the above example we can further list some interesting properties of the Q-Witt rings of the type described in Corollary 3.10.

PROPOSITION 3.12 *Let* $R \cong (\mathbb{Z}_{2^n}^* \times \mathbb{Z}_{2^m}^*) \cup ((2\mathbb{Z}_{2^n}) \times (2\mathbb{Z}_{2^m}))$ or $R \cong \mathbb{Z}_{2^m}[\mathbb{Z}_2]/(2^{n-1}(e^l + g))$. *Then the units of* R, $R^* = \mathbb{Z}_{2^n}^* \times \mathbb{Z}_{2^m}^*$ *each have 2-power order.*

Proof. To convince ourself of the above we need to only observe that $\mathbb{Z}_{2^n}^*$ is a multiplicative subgroup of $\mathbb{Z}_{2^n}$ and so each element of $\mathbb{Z}_{2^n}^*$ has order, which divides 2^{n-1}. Similarly, we can say that each element of $\mathbb{Z}_{2^m}^*$ has order, which divides 2^{m-1}. Therefore, we can state that every unit of R has 2-power order.

Next we will show you a nice calculation, which could be very useful in certain areas. We will show explicitly what the ideals are in R and discuss their properties. Before we do so, we introduce a definition.

DEFINITION 3.13 Let I be an ideal of a ring R. Then the *nilpotency* of I is defined to be the smallest positive integer r with $I^r = 0$.

PROPOSITION 3.14 *Let* $R \cong (\mathbb{Z}_{2^n}^* \times \mathbb{Z}_{2^m}^*) \cup ((2\mathbb{Z}_{2^n}) \times (2\mathbb{Z}_{2^m}))$. *Then*

(1) if $n = m = 1$, *then* $R \cong \mathbb{Z}_2$ *has only the trivial ideals and the zero ideal* (0) *is the maximal ideal and its nilpotency is clearly* 1, so R is a chain ring.

(2) if $m > n = 1$, *then* $R \cong \mathbb{Z}_{2^m}$ *has* $m + 1$ *ideals, each of the form* $(2^i) = 2^i\mathbb{Z}_{2^m}$, *where* $0 \leq i \leq m$; *with maximal ideal* (2) *with nilpotency* m, *so* R *is a chain ring.*

(3) if $m \geq n > 1$, *then* R *has exactly* $2n + m - 1$ *ideals, and the unique maximal and prime ideal* $\mathfrak{m}$ *is not principal and has nilpotency* m, *so* R *is a local ring, but is not a chain ring.*

Proof. Part (1) and (2) are clear. To show part (3) we need to recall that each ideal in $\mathbb{Z}_{2^k}$, where k is a positive integer, is of the form $(2^i) = 2^i\mathbb{Z}_{2^k}$ with $0 \leq i \leq k$, where $(2^0) = \mathbb{Z}_{2^k}$ and $(2^k) = (0)$. Hence, there are exactly $k-1$ nontrivial proper ideals of $\mathbb{Z}_{2^k}$, which are all additive subgroups of $2\mathbb{Z}_{2^k}$. Also, it is clear that the nilpotency of the proper ideal (2^i) is $\frac{k}{i}$. And, finally $(2^0) \supseteq (2^1) \supseteq \ldots (2^i) \supseteq \ldots \supseteq (2^k)$ for each i with $0 \leq i \leq k$.

Using this observation, we can easily see that if we set $I_n = ((2,0))$ and $I_m = ((0,2))$, then I_n, I_m are both principal ideals of R where the nilpotency of I_n is n, and of I_m is m. These ideals are very well behaved. Observe that $I_n I_m = ((0,0))$, which implies that $(I_n + I_m)^i = I_n^i + I_m^i$ for all positive integers i. Similarly, $I_n^i \cap I_m^i = (0,0)$ for all positive integers. And finally, we have that $I_n^i \cap I_n^j = I_n^{\max(i,j)}$ as well as $I_m^i \cap I_m^j = I_m^{\max(i,j)}$ for each positive integer i,j.

Now, to show that the nilpotency of $\mathfrak{m}$ is m, first we observe that

$$(I_n + I_m)^m = I_n^m + I_m^m = 0.$$

To convince us that m is the least positive integer with this property suppose k is a positive integer less than m with $(I_n + I_m)^k = 0$. Then

$$(I_n + I_m)^k = I_n^k + I_m^k = 0,$$

which is a contradiction, since even if $I_n^k = 0$, the nilpotency of I_m is m which means $I_m^k \neq 0$ for any positive integer less than k.

Seeing all of the above, we can now state that the set of all ideals I_R of R consists of $(0), R, I_n, \ldots, I_n^{n-1}, I_m, \ldots, I_m^{m-1}, \mathfrak{m} = I_n + I_m, \ldots, I_n^{n-1} + I_m^{n-1}$, whence $|I_R| = 2 + (n-1) + (m-1) + (n-1) = 2n + m - 1$.

At this point we generalize some of our findings to the Q-Witt rings R, which are quotients (in the sense of Definition 2.10) of arbitrary group rings. That is, we will construct the rings $R \subseteq C(X, \bigcup_{x \in X} \mathbb{Z}_{n_x})$ which are quotients of $\mathbb{Z}[G]$, where $|G| = |X| = 2^n$ with $n \geq 2$ and certain conditions on each n_x. We will generalize the first two cases that we presented earlier in this chapter. And we will also show the ring structure of $R \subseteq C(X, \bigcup_{x \in X} \mathbb{Z}_{n_x})$, where each n_x is some positive integer power of 2.

In our next Propositions, we will generalize Lemma 3.2 and Lemma 3.9.

PROPOSITION 3.15 *Let n_x be positive integers with* $\gcd(n_x, n_y) = 1$ *for each $x,y \in X$. Then $R \subseteq C(X(S), \bigcup_{x \in X} \mathbb{Z}_{n_x})$ is isomorphic to $\prod_{x \in X} \mathbb{Z}_{n_x}$.*

Proof. First we observe that R is naturally a subring of $\prod_{x \in X} \mathbb{Z}_{n_x}$. Next, we show that the map $\theta : \mathbb{Z}[G] \to \prod_{x \in X} \mathbb{Z}_{n_x}$, induced by $\mathbb{Z}[G] \to C(X(S), \bigcup_{x \in X} \mathbb{Z}_{n_x})$ is a ring epimorphism. To see this we observe that $\prod_{x \in X} \mathbb{Z}_{n_x}$ is the image of $\mathbb{Z}e^1$, which follows from the Chinese Remainder Theorem.

PROPOSITION 3.16 *Let n_x be a positive odd integer for each $x \in X$. Then $R \subseteq C(X, \bigcup_{x \in X} \mathbb{Z}_{n_x})$ is isomorphic to $\prod_{x \in X} \mathbb{Z}_{n_x}$.*

Proof. Recall that R is a finite quotient of a torsion free abstract Witt ring S for a group $|G| = 2^n$. Therefore, we have a natural ring homomorphism from $\mathbb{Z}[G]$ onto $S \subseteq C(X, \mathbb{Z})$ and thus we have $\Phi : \mathbb{Z}[G] \to R \subseteq C(X, \bigcup_{x \in X} \mathbb{Z}_{n_x}) \subseteq \prod_{x \in X} \mathbb{Z}_{n_x}$ defined as in the proof of Theorem 2.18.

To show that Φ is an epimorphism, let $x \in X$. Then by [3, Lemma 3.7], there are $g_1,\ldots,g_n \in G$ such that $\{x\} = \bigcap_{i=1}^{n} H(g_i)$,. Observe that for each such g_i, $\Phi(1 - g_i) = \overline{2e_{H(g_i)}}$ and so $\Phi(\prod_{i=1}^{n}(1 - g_i)) = \overline{2^n \prod_{i=1}^{n} e_{H(g_i)}} = \overline{f}$. Notice that $\overline{f}(x) = 2^n$ and $\overline{f}(y) = 0$ for all $x \neq y \in X$. Now, since $\gcd(n_x, 2^n) = 1$, we know that $2^n \in \mathbb{Z}_{n_x}^{\star}$. Thus, there is an $a \in \mathbb{Z}_{n_x}^{\star}$ so that $a2^n \equiv 1 (\mathrm{mod}\, n_x)$, which implies that the element $(m)_{z \in X}$ with $m \equiv 1 (\mathrm{mod}\, n_x)$ and $m \equiv 0 (\mathrm{mod}\, n_y)$ for all $x \neq y \in X$ is in the image of Φ.

Since we chose x arbitrarily from X, we just showed that all elements of the form $(m)_{z \in X}$ with $m \equiv 1 (\mathrm{mod}\, n_x)$ and $m \equiv 0 (\mathrm{mod}\, n_y)$ for all $x \neq y \in X$ are in the image of Φ, which will generate $\prod_{x \in X} \mathbb{Z}_{n_x}$.

In light of our findings in Chapter 2, we know that in the case of $n \geq 1$, the only local Q-Witt rings are those rings R such that $R \subseteq C(X, \bigcup_{x \in X} \mathbb{Z}_{n_x})$, where each n_x is some positive integer power of 2 and $n_x \geq |X|$. Therefore, for the remainder of this chapter we will concentrate on the local Q-Witt rings. First, we give the ring structure of some local Q-Witt rings and determine the order of those local Q-Witt rings, where each n_x is the same power of 2 which is greater than the order of the group G.

THEOREM 3.18 *Let R be the image of $\mathbb{Z}[G]$ in $C(X, \bigcup_{x \in X} \mathbb{Z}_{n_x})$. Let $n_x = 2^{\alpha_x}$ with α_x a positive integer for each $x \in X$ and each $n_x \geq |G| = 2^n$.*

Then R is isomorphic to $\mathbb{Z}_{2^\alpha}[G]/(2^{\alpha_x - n}(\prod_{i=1}^{n}(e' + \varepsilon_{(i,x)}g_i)), x \in X)$

where $\alpha = \max_{x \in X} \alpha_x$, *and* $\{g_1, \ldots, g_n\}$ *is a fixed* $\mathbb{Z}_2$*-basis for* G, *and the* $\pm$ *signs* $\varepsilon_{(i,x)}$ *are chosen depending on* $x \in X$, *so that* $\{x\} = \bigcap_{i=1}^{n} H(-\varepsilon_i g_i)$.

Proof. Recall that we have a natural ring homomorphism from $S = \mathbb{Z}[G]$ into $C(X, \mathbb{Z})$ and thus from $S = \mathbb{Z}[G]$ into $C(X, \bigcup_{x \in X} \mathbb{Z}_{n_x})$ where $|X| = 2^n = |G|$, $n \geq 2$. Then as in the proof of Theorem 2.18, we define $\Phi : \mathbb{Z}[G] \to R \subseteq C(X, \bigcup_{x \in X} \mathbb{Z}_{n_x})$ by $\Phi(\sum_{g \in G} a_g g) = \overline{a_{e'} + a_g \sum_{g \in G} (1 - 2e_{H(g)})} \in R$, where e' is the identity in G. First, we note that, for a fixed $x \in X$, the function f_x induced by $2^{\alpha_x - n} \prod_{i=1}^{n} (e' + \varepsilon_{(i,x)} g_i)$ in $C(X, \mathbb{Z})$ is such that $f_x(x) = 2^{\alpha_x}$ at x and $f_x(y) = 0$ at all $x \neq y \in X$. Therefore, $f_x \in Ker\Phi$ for each $x \in X$. Hence, we have that $(2^{\alpha_x - n}(\prod_{i=1}^{n} (e' + \varepsilon_{(i,x)} g_i)), x \in X) \subseteq Ker\Phi$. Next we observe that the kernel of Φ consists of all $f \in C(X, \mathbb{Z})$ in the image of the Witt ring, which satisfy $f(x) \equiv 0 (\mathrm{mod}\, 2^{\alpha_x})$ for each $x \in X$. Observe that any such function is clearly a $\mathbb{Z}$-linear combination of functions $h \in C(X, \mathbb{Z})$ with $h(x) = 2^{\alpha_x}$ for a fixed $x \in X$ and $h(y) = 0$ for all $x \neq y \in X$. These functions h are precisely the ones we have included as generators fot the kernel of Φ. Thus, we can conclude that if $2^{\alpha_x} \geq 2^n$, then R is isomorphic to $\mathbb{Z}_{2^\alpha}[G]/(2^{\alpha_x - n}(\prod_{i=1}^{n} (e' + \varepsilon_{(i,x)} g_i)), x \in X)$ where $\alpha = \max_{x \in X} \alpha_x$.

The general case needs to be further investigated. However, we do have results in the special case when n_x is the same constant as a special case of the above Theorem.

COROLLARY 3.19 *Suppose R is as above. Let* $n_x = 2^\alpha \geq |G| = 2^n$ *for each* $x \in X$, *where* α *is a positive integer. Then* $R \cong \mathbb{Z}_{2^\alpha}[G]/I$ *where*

$I = \left(2^{\alpha-r} \prod_{g_{k_i} \in G_r^k} (e^l - g_{k_i}), \text{ for each } r, \text{ with } 0 \leq r \leq n,\ 1 \leq k \leq \binom{n}{r} \right)$, *where the* $\binom{n}{r}$ *r-subsets of* $\{g_1, .., g_n\}$, *a fixed* $\mathbb{Z}_2$*-basis for G, can be indexed as* $G_r^k = \{g_{k_1}, \ldots, g_{k_r}\}$ *for* $1 \leq k \leq \binom{n}{r}$. *Furthermore* $|R| = 2^{(2\alpha-n)2^{n-1}}$.

Proof. First we observe that as a special case of Theorem 3.18, we have that $\mathbb{Z}_{2^\alpha}[G]/(2^{\alpha-n}(\prod_{i=1}^{n}(e^l + \varepsilon_{(i,x)}g_i)),\ x \in X)$. Therefore, we need only to prove that the ideal $(2^{\alpha-n}(\prod_{i=1}^{n}(e^l + \varepsilon_{(i,x)}g_i)),\ x \in X)$ is the same as the ideal I. To show this once again we will use $\Phi : \mathbb{Z}[G] \to R \subseteq C(X, \bigcup_{x \in X} \mathbb{Z}_{n_x})$ as in the proof of Theorem 2.18. By [3, Lemma 3.7], for any $r,\ 0 \leq r \leq n$, we have $H(g_{k_1}), \ldots, H(g_{k_r})$ in $\mathcal{H}(\mathbb{Z}[G])$, so that $\left| \bigcap_{g_{k_i} \in G_r^k} H(g_{k_i}) \right| = 2^{n-r}$ for some G_r^k. Then we can conclude that

$\Phi(\prod_{g_{k_i} \in G_r^k} (e^l - g_{k_i})) = \overline{2^r \prod_{g_{k_i} \in G_r^k} e_{H(g_{k_i})}}$ so that $\overline{2^r \prod_{g_{k_i} \in G_r^k} e_{H(g_{k_i})}}(x) = 2^r$ at each $x \in \bigcap_{g_{k_i} \in G_r^k} H(g_{k_i})$ and $\overline{2^r \prod_{g_{k_i} \in G_r^k} e_{H(g_{k_i})}}(y) = 0$ at each $y \in X - \bigcap_{g_{k_i} \in G_r^k} H(g_{k_i})$.

Therefore, we can conclude that all the elements of the form $2^{\alpha-r} \prod_{g_{k_i} \in G_r^k} (e^l - g_{k_i}) \in \mathbb{Z}[G]$ will have images of the form $h \in C(X, \mathbb{Z})$, with $h(x) = 2^\alpha$ at each $x \in \bigcap_{g_{k_i} \in G_r^k} H(g_{k_i})$ and $h(y) = 0$ at each $y \in X - \bigcap_{g_{k_i} \in G_r^k} H(g_{k_i})$.

Thus, I is contained in $(2^{\alpha-n}(\prod_{i=1}^{n}(e^{l}+\varepsilon_{(i,x)}g_i)),\ x \in X)$.

To show the inclusion in the other direction, we show that the generators of the ideal $(2^{\alpha-n}(\prod_{i=1}^{n}(e^{l}+\varepsilon_{(i,x)}g_i)),\ x \in X)$ can be expressed as $\mathbb{Z}_{2^\alpha}$-linear combination of elements of the ideal I. So, let $2^{\alpha-n}(\prod_{i=1}^{n}(e^{l}+\varepsilon_{(i,x)}g_i))$ be an arbitrary generator. Observe that if $\varepsilon_{(i,x)} = -1$ for each (i,x), then $2^{\alpha-n}(\prod_{i=1}^{n}(e^{l}+\varepsilon_{(i,x)}g_i)) = 2^{\alpha-n}(\prod_{i=1}^{n}(e^{l}-g_i)) \in I$.

So, we can assume that $\varepsilon_{(i,x)} = 1$ for some (i,x). Without loss of generality we will assume that $\varepsilon_{(i,x)} = 1$ for $1 \le i \le m \le n$, then

$2^{\alpha-n}(\prod_{i=1}^{n}(e^{l}+\varepsilon_{(i,x)}g_i)) = 2^{\alpha-n}(\prod_{i=1}^{m}(e^{l}+g_i)(\prod_{i=m+1}^{n}(e^{l}-g_i)))$. So, it suffices for us to show each term of the form $2^{\alpha-n}(\prod_{i=1}^{m}(e^{l}+g_i)(\prod_{i=m+1}^{n}(e^{l}-g_i)))$ with $1 \le i \le m \le n$, can be expressed as $\mathbb{Z}_{2^\alpha}$-linear combination of elements of the ideal I. We will do so using induction on m.

First, suppose $m = 1$. Then $e^{l}+g = -(e^{l}-g)+2e^{l}$, so we can conclude that

$$2^{\alpha-n}((e^{l}+g)(\prod_{i=m+1}^{n}(e^{l}-g_i))) =$$

$$-2^{\alpha-n}(e^{l}-g)(\prod_{i=m+1}^{n}(e^{l}-g_i)) + 2^{\alpha-n+1}(\prod_{i=m+1}^{n}(e^{l}-g_i)) \in I.$$

Next, suppose that $\prod_{i=1}^{m-1}(e^{l}+g_i) = \sum a_{(k,r)} \prod_{g_{k_i} \in G_r^k}(e^{l}-g_{k_i})$, where $a_{(k,r)} \in \mathbb{Z}_{2^\alpha}$. Then using case 1, we can write that

$$\prod_{i=1}^{m}(e^l + g_i) = (e^l + g_m)\sum a_{(k,r)} \prod_{g_{k_i} \in G_r^k} (e^l - g_{k_i})$$

$= \sum(-a_{(k,r)})(e^l - g_m) \prod_{g_{k_i} \in G_r^k} (e^l - g_{k_i}) + \sum 2a_{(k,r)} \prod_{g_{k_i} \in G_r^k} (e^l - g_{k_i})$. Therefore,

$$2^{\alpha-n}(\prod_{i=1}^{m}(e^l + g_i)(\prod_{i=m+1}^{n}(e^l - g_i))) =$$

$$2^{\alpha-n}(\sum(-a_{(k,r)})(e^l - g_m) \prod_{g_{k_i} \in G_r^k} (e^l - g_{k_i}))(\prod_{i=m+1}^{n}(e^l - g_i))) +$$

$$2^{\alpha-n}((\sum 2a_{(k,r)} \prod_{g_{k_i} \in G_r^k} (e^l - g_{k_i}))(\prod_{i=m+1}^{n}(e^l - g_i))) \in I.$$

To complete our proof we need to find the order of this ideal I.

Since there are $\binom{n}{r}$ r-subsets G_r^k of $\{g_1, \ldots, g_n\}$, there are $\binom{n}{r}$ elements of the form $2^{\alpha-r} \prod_{g_i \in G_r} (e^l - g_i)$ in I, which implies that

$|I| = 2^n(2^{n-1})^{\binom{n}{1}}(2^{n-2})^{\binom{n}{2}} \cdots (2)^{\binom{n}{n-1}} = 2^{n2^{n-1}}$, since

$n\binom{n}{0} + (n-1)\binom{n}{1} + \ldots + 1\binom{n}{n-1} = n(\binom{n-1}{0} + \binom{n-1}{1} + \ldots + 1\binom{n-1}{n-1}) = n2^{n-1}$.

Therefore, we can conclude that since $|\mathbb{Z}_{2^\alpha}[G]| = (2^\alpha)^{2^n} = 2^{\alpha 2^n}$,

$$|R| = \frac{|\mathbb{Z}_{2^\alpha}[G]|}{|I|} = \frac{2^{\alpha 2^n}}{2^{n2^{n-1}}} = 2^{(2\alpha-n)2^{n-1}}.$$

CHAPTER 4
SQ-WITT RINGS

In this chapter, we will define a special class of Q-Witt rings, SQ-Witt rings, which occur naturally as quotients of Witt rings of formally real fields. Finitely generated reduced Witt rings of a formally real field are very well understood. Craven in [4] showed that these rings can all be constructed by a very concrete recursive process. The advantage of this observation is that theorems about them can be proven by induction via that recursion. It is hoped that the quotient rings we describe will provide interesting classes of finite rings with possible applications to coding theory.

We will show that all SQ-Witt rings arise from a recursive construction.

We will now give some background and definitions so we understand the Witt ring of a formally real field. By a Witt ring $W(F)$, we mean a ring of equivalence classes of nonde-generate symmetric bilinear forms over the field F and $W_{red}(F) = W(F)/NilW(F)$. For further developments and definitions on Witt rings we found [13] to be very detailed.

For the remainder of this thesis we will let F be a formally real field, i.e., a field where -1 is not a sum of squares. A nice example of a formally real field is of course the set of real numbers $\mathbb{R}$ and similarly one easily sees that the set of complex numbers $\mathbb{C}$ is not formally real. It is important to also observe that a formally real field by virtue of its definition, must have characteristic 0.

By an ordering of a field F one means a subset P of F, which satisfies

1) $0 \notin P$, 2) If $0 \neq x \in F$, then either $x \in P$ or $-x \in P$, and 3) $P + P \subset P$ and

$PP \subset P$ [13, Definition 1.2 Page 224]. From [11, Remark 2.7] we know that the set of orderings on F can be identified with the ring homomorphisms $W(F) \to \mathbb{Z}$ or equivalently with the minimal prime ideals of $W(F)$ as was observed in [11, Remark 2.7]. Therefore if $W(F)$ is Witt ring of a formally real field F then X_F may be identified with the set of all orderings of F. Observe that the map $W(F) \to C(X_F, \mathbb{Z})$ is defined by taking a representative $\sum a_i x_i^2$ for a class in $W(F)$ and finding the signature of the form at each ordering of F, where the signature is defined to be the number of positive a_i's minus the number of negative a_i's.

As noted earlier, Witt rings of fields occur as special classes of the abstract Witt rings as they were defined in [10], that is as a quotient ring of the integral group ring $\mathbb{Z}[G]$, where G is a group of exponent 2. We now also note that for a formally real field F, the group G is isomorphic to $F^*/(\sum F^{*2})$, where $\sum F^{*2}$ is the group of nonzero sums of squares in F.

DEFINITION 4.1 Let R be a an abstract Witt ring for an elementary abelian 2-group. Then we say that R satisfies the *weak approximation property* (WAP) if $\mathcal{H}(R)$, the subbasis for the topology of $X(R)$, is a basis, and R satisfies the *strong approximation property* (SAP) if $\mathcal{H}(R)$ is the entire Boolean algebra of clopen sets in $X(R)$.

COROLLARY 4.2 [11, Corollary 3.21] *Let F be a formally real field, X_F the "Boolean space" of all orderings of F, and $W(F)$ the Witt ring of F. Then the following statements are equivalent.*

(1) $W_{red}(F) \cong \mathbb{Z} + C(X_F, 2\mathbb{Z})$.

(2) $C(X_F, \mathbb{Z})/W_{red}(F)$ *is a group of exponent* 2.

(3) If U is a clopen subset of X_F *there exists an element a of* F^* *such that an ordering* $<$ *is in U if and only if* $a < 0$.

(4) (Approximation). Given any two disjoint closed sets Y_1, Y_2 *of orderings of F there is an element a in* F^* *with* $a < 0$ *for* $<$ *in* Y_1 *and* $0 < a$ *for* $<$ *in* Y_2.

We note that a Witt ring of F, $W(F)$, which satisfies part (3) of the above theorem also satisfies SAP, and one which satisfies part (4) of the above theorem also satisfies WAP. Further, the SAP case gives the largest possible abstract Witt ring for a given size $|X|$. (See proof of Proposition 2.21 and Proposition 4.4.)

DEFINITION 4.3 An *SQ-Witt Ring* is a ring R formed by taking the quotient ring of a torsion free Witt ring $W(F)$, viewed as a subring of $C(X_F, \mathbb{Z})$ with $|X_F| < \infty$, by taking the function $f \in W(F)$ to a function $\overline{f} \in C(X_F, \bigcup_{x \in X_F} \mathbb{Z}_{n_x})$ such that $\overline{f}(x) \in \mathbb{Z}_{n_x}$ for each $x \in X_F$. That is, the restriction mapping to a point $x \in X_F$ becomes the signature at the ordering associated with x composed with the quotient map $\mathbb{Z} \to \mathbb{Z}_{n_x}$.

Let R be an SQ-Witt ring; that is, the quotient of a torsion free Witt ring $S = W(F)$, for some formally real field F with space of orderings X. By [4], the ring S can be constructed recursively from the ring of integers $\mathbb{Z}$ using two operations:

(1) Group extension: given a ring R_0, form the group ring $R_0[\mathbb{Z}_2]$.

(2) Direct product (in the category of torsion free Witt rings): given two rings in the

category $R_i = \mathbb{Z} + \mathfrak{m}_i$, $i = 1,2$ the product is $\mathbb{Z} + \mathfrak{m}_1 \times \mathfrak{m}_2$. Here $\mathfrak{m}_i$ denotes the unique maximal ideal of R_i and is viewed as a subset of the functions $C(X_i, 2\mathbb{Z})$.

Thus any such ring is a subring of the largest possible allowed collection of functions, that of a SAP field, as in Corollary 4.2. Indeed, this is also the largest possibility for the preimage of a Q-Witt ring. We refer the reader to [1] for a much more general discussion of the torsion free rings and generalizations. Most expositions of [4, Theorem 2.1], such as that in [1], emphasize the effect on the sets of minimal prime ideals. For group extension, the space X is duplicated, with the nontrivial group element being +1 on one copy and -1 on the other. For the product, one obtains the disjoint union of X_1 and X_2.

This recursive construction is almost unique. The only non-uniqueness arises in forming the group ring $\mathbb{Z}[\mathbb{Z}_2]$, which also occurs as the product of $\mathbb{Z}$ with itself in this category. That is, there are two ways to form the ring with $|X| = 2$, whose quotients were carefully analyzed in Chapter 3.

It is now somewhat clear that a recursive construction can be used to create any SQ-Witt ring, but there are complications. For example, we can take $n = \max_{x \in X} n_x$, begin with $\mathbb{Z}_n$ in place of $\mathbb{Z}$ and use the constructions above. Then at the end, factor out the additional amount needed at each point $x \in X$. We cannot, however, build the SQ-Witt ring R with all factorizations in place as we go. This is not a problem for products, as the product construction commutes with our quotient ring construction. But the group ring construction does not. For example, if we work with $S = \mathbb{Z}[\mathbb{Z}_2 \times \mathbb{Z}_2]$, the set X has four elements. Forming R from a quotient of $\mathbb{Z}$, then forming a group ring will make all values n_x the same, and

forming it from a quotient of $R_0[\mathbb{Z}_2]$, where R_0 is a Q-Witt quotient of $\mathbb{Z}[\mathbb{Z}_2]$, will make them equal in pairs. We can only obtain the full generality we want by making an additional quotient construction at the end. While this largely loses any uniqueness for our constructions, it does still allow most of the power of the recursive construction for proofs and for computations. There is one further complication as is evident in the special case of Corollary 3.13; group ring constructions do not inject into the ring of functions, but rather have a two element kernel ($\frac{charR}{2}(e+g)$).

This is a fundamental fact of our situation since we cannot distinguish the group elements modulo 2, as they are functions taking values ± 1. This discussion shows now that we have the following theorem.

THEOREM 4.4 *The collection of all SQ-Witt rings with only 2-torsion is precisely the set $\mathcal{M}$ of rings constructed as follows*:

(1) The rings $\mathbb{Z}/2^n\mathbb{Z} \in \mathcal{M}$ for each $n = 1,2,\ldots$

(2) Given any $R \in \mathcal{M}$, the quotient of the group ring $R[\{e,g\}]/(\frac{charR}{2}(e+g)) \in \mathcal{M}$.

(3) Given $R_i = \mathbb{Z}_{n_i} + \mathfrak{m}_i \in \mathcal{M}$, the product, $\mathbb{Z}_{\max(n_1,n_2)} + \mathfrak{m}_1 \times \mathfrak{m}_2 \in \mathcal{M}$.

(4) Given $R \in \mathcal{M}$, any further quotient as in Definition 2.10 is in $\mathcal{M}$.

The restriction to having only 2-torsion is a technicality which was mentioned in Chapter 2. Any SQ-Witt ring is a product of a finite set of rings in $\mathcal{M}$ and a finite set of rings $\mathbb{Z}_n$, n odd, where either of the sets may be empty.

As an example of the power of the recursive construction, we point out how to count the number of elements in an SQ-Witt ring. Two cases have been done earlier.

PROPOSITION 4.5 *Let R be the quotient of a SAP Witt ring $\mathbb{Z} + C(X, 2\mathbb{Z})$, with values n_x, $x \in X$. Then*

$$|R| = 2\prod_{x \in X} 2^{n_x - 1}.$$

Proof. By the remark following Corollary 4.2, we know that the SAP case gives the largest possible abstract Witt ring for a given size $|X|$. Therefore, by Proposition 2.21 we have that $|R| = 2\prod_{x \in X} 2^{n_x - 1}$.

PROPOSITION 4.6 *Let R be a quotient of a group ring $\mathbb{Z}[\mathbb{Z}_2]$, with all values of $n_x = 2^\alpha$. Then $|R| = 2^{2\alpha - 1}$.*

Proof. This is just Corollary 3.10.

These are the two extreme cases for Q-Witt rings. That is, if $|X| = 2^n$ for any ring R, then $|R|$ is between the lower bound of the group ring as in Proposition 4.6 and the upper bound given in Proposition 4.5. We have no better result for an arbitrary Q-Witt ring. But if R is an SQ-Witt ring, we can compute its size recursively (until the final quotient, if needed).

THEOREM 4.7

(1) If R is the product of R_1 and R_2, then $|R| = \frac{|R_1||R_2|}{2}$.

(2) If $R = R_0[\{e,g\}]/(\frac{charR}{2}(e+g))$, *then* $|R| = \frac{|R_0|^2}{2}$.

Proof. (1) By Proposition 2.21, we have $|R_i| = 2|M_i|$, $i = 1, 2$, and so

$|R| = 2|M_1 \times M_2| = 2|M_1||M_1| = \frac{|R_1||R_2|}{2}$.

(2) This is clear since $|R_0[\{e,g\}]| = |R_0|^2$ and the ideal $(\frac{charR}{2}(e+g))$ has 2 elements.

REFERENCES

1. Andradas, C., Bröcker, L. & Ruiz, J. (1996). *Constructible sets in real geometry*. Berlin: Springer Verlag.

2. Clark, W.E. & Liang, J.J. (1973). Enumeration of finite commutative chain rings. *J. Algebra,* 27, 445-453.

3. Craven, T. (1977). Stability in Witt rings. *Transactions of the American Mathematical Society,* 225, 227-242.

4. Craven, T. (1978). Characterizing reduced Witt rings of fields. *J. Algebra,* 53, 68-77.

5. Greferath, M. & Schmidt, S. E. (1999). Gray Isometries for Finite Chain Rings and a Nonlinear Ternary $(36,3^{12},15)$ Code. *IEEE Transactions on Information Theory, Vol.* 45, *No.* 7, 2522-2524.

6. Greferath, M. & Viterbo, E. (1999). On $\mathbb{Z}_4$- and $\mathbb{Z}_9$-Linear Lifts of the Golay Codes. *IEEE Transactions on Information Theory, Vol.* 45, *No.* 7, 2524-2527.

7. Hou, X. (2001). Finite Commutative Chain Rings. *Finite Fields and Their Applications,* 7, 382-396.

8. Hungerford, T. W. (1974). *Algebra.* New York: Holt, Rinehart and Winston, Inc..

9. Jacobson, N. (1974). *Basic Algebra I.* San Fransisco: W. H. Freeman and Company.

10. Knebusch, M., Rosenberg, A., & Ware, R. (1972). Structure of Witt rings and quotients of abelian group rings. *American J. Math., 94,* 119-155.

11. Knebusch, M., Rosenberg, A., & Ware,R. (1973). Signatures on Semilocal rings. *J. Algebra,* 26, 208-250.

12. Lang, S. (1984). *Algebra.* Redwood City, CA: Addision-Wesley Publishing Company, Inc..

13. Lam, T.Y. (1973). The Algebraic Theory of Quadratic Forms. Reading, MA: W. A. Benjamin, Inc..

14. McDonald, B. R. (1974). *Finite Rings with Identity.* New York: Marcel Dekker, Inc..

15. Munkres, J. R. (1975). *Topology A First Course.* Englewood Cliffs, NJ: Prentice Hall.

16. Norton, G. (1999). On Minimal Realization Over a Finite Chain Ring. *Designs, Codes and Cryptography,* 16, 161-178.

17. Norton, G. & Sălăgean, A. (2000). On the Key Equation Over a Commutative Ring. *Designs, Codes and Cryptography,* 20, 125-141.

DEPARTMENT OF MATHEMATICS, UNIVERSITY OF HAWAII, HONOLULU, HI 96822-2273

E-mail address: mvo@hawaii.edu