University of California

Santa Barbara

On Abstract Witt Rings and Quadratic Extensions

A thesis submitted in partial satisfaction

of the requirements for the degree

Master of Arts

in

Mathematics

by

Jiajie Luo

Committee in charge:

Professor William Jacob, Chair

Professor Jon McCammond

Professor Yitang Zhang

June 2019

The thesis of Jiajie Luo is approved.

Professor Jon McCammond

Professor Yitang Zhang

Professor William Jacob, Chair

May 2019

On Abstract Witt Rings and Quadratic Extensions

Jiajie Luo

To my family.

Acknowledgements

To my advisor, Bill Jacob: thank you for your support and guidance over the years. Without you, my interest in algebra, much less this thesis, would never have existed.

To my committee members, Jon McCammond and Yitang (Tom) Zhang: thank you for your time and assistance in assembling this thesis, as well as excellent experiences in the classroom. I'm grateful for all the advice you've given me along the way, regarding both the thesis and otherwise.

To all the (other) mathematics faculty members who have supported me along my journey and helped shape my mathematical foundations and interests (to varying degrees), including Padraic Bartlett, Maribel Bueno Cachadina, Denis Labutin, Andrew Cotton-Clay, Jeffrey Stopple, Daryl Cooper, Darren Long, Birge Huisgen-Zimmermann, Stephen Bigelow, Charles Akemann, Paul Atzberger, and Hector Ceniceros (I almost definitely left people out; my dearest apologies if I forgot you!): thank you for all your support. Without you, I certainly would not be where I am today.

To Peter Garfield: thank you for being available to chat during my duration in the masters program, as well as all the formatting and LaTeX help you've provided for this thesis.

To my Isla Vista Church family: thank you for everything. There are WAY too many of you for me to list, so I won't even try. To put it (extremely) lightly, my time here would not have been the same without any of you.

To my family: thank you for everything, from taking care of me, to providing for me and supporting me, and so much more. Any attempt at words on my end will fail to describe just how thankful I actually am.

Psalm 63:3

Colossians 3:17

Abstract

On Abstract Witt Rings and Quadratic Extensions

by

Jiajie Luo

The Witt ring of a field gives the structure of the isometry classes of quadratic forms over that field. In particular, the Witt ring provides an algebraic invariant for fields away from characteristic 2, which also allow us to study the orderings we can put on that field. During the latter quarter of the 20th century, abstract Witt rings, a wider class of rings that had the structure of a Witt ring but constructed independently from fields, were introduced. In this thesis, we will use what is known about the structure of Witt rings over quadratic extensions of fields in order to come up with an analog that extends over to abstract Witt rings.

Contents

Chapter 1

Introduction

The theory of quadratic forms has been studied since antiquity. Indeed, there have been Babylonian tablets tracing back the second millennium BC mentioning integer solutions to certain quadratic forms. More recently, the study of quadratic forms has been hugely motivated by number theory, including the study of diophantine equations and lattices over $\mathbb{Z}$.

The algebraic theory of quadratic forms was largely pioneered by Ernst Witt in the 1930s. Witt introduced the study of quadratic forms over arbitrary fields, not necessarily that of number theoretic origin. Among his contributions included the development of the Witt ring of fields, which will be an important topic later discussed in this thesis.

Much of what Witt built went dormant for many years until a series of paper by Albreich Pfister in the 1960s led to a resurgence in the topic. In the 1970s, the idea of an abstract Witt ring was introduced by Manfried Knebusch, Alex Rosenberg, and Roger Ware, which axiomatically gave the structure of Witt rings independently from fields. This abstract theory, which encompassed the theory of quadratic forms over fields, was later developed by Murray Marshall. Marshall was also motivated by the space of orderings, which he introduced as a generalization of the quadratic form theory over fields. In fact, there is a correspondence between abstract Witt rings and spaces of orderings.

T. Y. Lam's book, *Quadratic Forms over Fields*, discusses the theory of Witt rings over quadratic extensions of fields. In particular, a sequence of Witt rings (viewed as modules) is presented, which satisfies the condition of reciprocity. In this thesis, we will explore the analog of Witt rings of quadratic extensions in the abstract setting. Namely, we want our "quadratic extensions" to behave in the way prescribed for the field case.

One important motivation for abstracting the Witt ring of a quadratic field extension is to help relate abstract Witt rings with pro-2 Galois groups. Given a field F, and its quadratic closure F_q, one can determine $Gal(F_q/F)$ from the structure of $W(F)$. From this, given F' in between F and F_q (ie. $F \subset F' \subset F_q$), we can compute $W(F')$, from which we can determine $Gal(F_q, F')$. By understanding the analog of 'quadratic extensions' of abstract Witt rings, we are able to determine the analog of the profinite 2-groups associated with abstract Witt rings.

Chapter 2

Background

In this section, we will go over the background information, given by Lam [3] and Marshall [4].

2.1 Preliminary Definitions

Let F be a field of characteristic not equal to 2.

Definition 2.1.1. *A* ***quadratic form****, $f : F^n \to F$, of dimension n over F is a second-degree homogeneous polynomial, of the form $f = \sum_{1 \le i \le j \le n} a_{ij} x_i x_j$, where $a_{ij} \in F$. f is* ***isotropic*** *if there is some nonzero $x \in F^n$ such that $f(x) = 0$, otherwise, f is* ***anisotropic****.*

Definition 2.1.2. *For a nonzero f, we say that $y \in F^*$ is* ***represented*** *by f if there is some $x \in F^n$ such that $f(x) = y$, and we denote $D(f)$ as the elements in F that are represented.*

Definition 2.1.3. *We say two forms f and g of the same dimension are* ***isometric*** *if $f(x) = g(T(x))$, for some isomorphism $T : F^n \to F^n$, where n is the dimension of f and g.*

Remark 2.1.1. *If f and g are isometric, then $D(f) = D(g)$.*

We may also view quadratic forms in terms of matrices. Given a quadratic form $f = \sum_{i \leq i \leq j \leq n} a_{ij} x_i x_j$ of dimension n, we form the $n \times n$ matrix M_f such that

$$(M_f)_{ij} = \begin{cases} a_{ij} & i = j \\ \frac{1}{2} a_{ij} & i < j \\ \frac{1}{2} a_{ji} & i > j \end{cases}.$$

It can be easily seen that M_f will always be symmetric, and it is clear how to recover f from M_f. In fact, given *any* $n \times n$ symmetric matrix M, we can find a unique corresponding quadratic form of degree n given by

$$f_M(x) = xMx^T$$

where x is viewed as a row vector.

Definition 2.1.4. *The **discriminant** of f is defined as $disc(f) = \det(M_f)$. We say that f is **degenerate** if $disc(f) = 0$. Otherwise, f is **nondegenerate**.*

Remark 2.1.2. *There is a one-to-one correspondence between symmetric matrices over F and quadratic forms.*

From here on out, we assume our quadratic forms are all nondegenerate.

2.2 Basic Results

In this section, we will go over some standard basic results.

Theorem 2.2.1. *All quadratic forms can be diagonalized. That is, any quadratic form f is isometric to some form $\bar{f}$ where $\bar{f} = \sum_{j=1}^{n} a_j x_j^2$. In this case, we note that $M_{\bar{f}}$ is a diagonal matrix.*

From here on out, we will represent the isometry classes of nondegenerate quadratic forms by a diagonalized representative. Notationally, we refer to the form $\sum_{j=1}^{n} a_j x_j^2$ as $\langle a_1, a_2, \cdots, a_n \rangle$.

Theorem 2.2.2.

1. $f \cong g \implies dim(f) = dim(g)$ *and* $disc(f) \cong disc(g) \mod F^{*2}$
2. $f \cong g \implies af \cong ag$ *for every* $a \in F^*$.
3. $\langle a_1 b_1^2, \cdots, a_n b_n^2 \rangle \cong \langle a_1, \cdots, a_n \rangle$.
4. *For any permutation* $\pi \in S_n$, $\langle a_1, \cdots, a_n \rangle \cong \langle a_{\pi(1)}, \cdots, a_{\pi(n)} \rangle$.
5. *If* $\langle a_1, \cdots, a_k \rangle \cong \langle b_1, \cdots, b_k \rangle$ *and* $\langle a_{k+1}, \cdots, a_n \rangle \cong \langle b_{k+1}, \cdots, b_n \rangle$, *then* $\langle a_1, \cdots, a_n \rangle \cong \langle b_1, \cdots, b_n \rangle$.

The following lemma characterizes isometry of one dimensional and two dimensional forms:

Lemma 2.2.1. *Let* $a, b, c, d \in F^*$. *Then*

1. $\langle a \rangle \cong \langle b \rangle$ *if and only if* $a \cong b \mod F^{*2}$
2. $\langle a, b \rangle \cong \langle c, d \rangle$ *if and only if* $ab \equiv cd \mod F^{*2}$ *and there are* $x, y \in F$ *such that* $c = ax^2 + by^2$.

Theorem 2.2.3. *The form* $\langle 1, -1 \rangle$ *is universal. That is,* $D(\langle 1, -1 \rangle) = F$.

This can be easily seen, as for any $a \in F$, we can find $x, y \in F$ such that $x - y = 1$ and $x + y = a$, which would mean $x^2 - y^2 = a$.

As a consequence of some of the above theorems, we have the following result:

Corollary 2.2.1. *For any* $a \in F^*$, $\langle a, -a \rangle \cong \langle 1, -1 \rangle$.

We now discuss the relation of the form $\langle 1, -1\rangle$ to isotropic forms.

Theorem 2.2.4. *For $n \geq 3$, $f = \langle a_1, \cdots, a_n\rangle$ is isotropic, if and only if there exists $b_3, \cdots, b_n$ such that $f \cong \langle 1, -1, b_3, \cdots, b_n\rangle$.*

We denote $\langle 1, -1\rangle$ by $\mathbb{H}$, which we call the hyperbolic form. This form has an important role in the theory of quadratic forms, as it plays the role of 0 in the Witt ring.

Now, we state Witt's Cancellation Theorem, which is central in the development of the Witt Ring.

Theorem 2.2.5 (Witt's Cancellation Theorem)**.** *Suppose $\langle a_1 \cdots, a_n\rangle \cong \langle b_1, \cdots, b_n\rangle$ and $a_1 = b_1$. Then $\langle a_2 \cdots, a_n\rangle \cong \langle b_2, \cdots, b_n\rangle$.*

2.3 The Witt Ring over Fields

In this section, we show the construction of the Witt ring over a field F.

Let $M(F)$ be the set of isometry classes of nondegenerate forms over F. As before, we represent our isometry classes with diagonal representations.

Definition 2.3.1. *Given quadratic forms $f = \langle a_1, \cdots, a_n\rangle$ and $g = \langle b_1, \cdots, b_m\rangle$, the **perpendicular sum** (also known as the **direct sum**) of f and g, denoted as $f \perp g = \langle a_1, \cdots, a_n, b_1, \cdots, b_m\rangle$. The **tensor product** of f and g is given by $f \otimes g = \langle a_1b_1, \cdots, a_1b_n, \cdots, a_nb_1, \cdots, a_nb_m\rangle$.*

Lemma 2.3.1. *With $\perp$ as addition and $\otimes$ as multiplication, $(M(F), \perp, \otimes)$ is a semiring.*

It is easy to see that $M(F)$ does not form a group under addition, since additive inverses don't exist. To remedy this, we construct the Witt-Grothendieck ring, $\hat{W}(F)$ by using the classical construction due to Grothendieck.

Definition 2.3.2. *Let $\sim$ be an equivalence relationship on $M(F)\times M(F)$, where $(f,g)\sim(f',g')$ if $f\perp g'\cong f'\perp g$ (the congruence here is isometry). The* ***Witt-Grothendieck ring*** *of F, $\hat{W}(F)$, is defined as $M(F)\times M(F)/\sim$.*

We note that an elements of $\hat{W}(F)$, (f,g), can be thought of as $f-g$. We can make the identification of $M(F)\hookrightarrow\hat{W}(F)$ by $f\mapsto(f,0)$.

Theorem 2.3.1. *We define the* ***Witt Ring*** *of F by $W(F)=\hat{W}(F)/\langle\mathbb{H}\rangle$, where $\mathbb{H}$ is the hyperbolic form.*

Remark 2.3.1. *We note that in $W(F)$, $-\langle a\rangle=\langle -a\rangle$.*

2.4 The Abstract Witt Ring

Let us now discuss the abstract Witt ring, a generalization of Witt rings over fields.

Definition 2.4.1. *Let G is an abelian 2-group (ie. $x^2=1$ for all $x\in G$) and Q be a pointed set with distinguised point denoted 0. Then $q:G\times G\to Q$ is a* ***quaternionic pairing*** *if it is a surjective mapping satisfying*

Q1: *(Symmetry) $q(a,b)=q(b,a)$*

Q2: $q(a,-a)=0$

Q3: *(Weak Bilinearity) $q(a,b)=q(a,c)$ if and only if $q(a,bc)=0$*

Q4: *(Linkage) If $q(a,b)=q(c,d)$, then there's some $x\in G$ such that $q(a,b)=q(a,x)$ and $q(c,d)=q(c,x)$.*

We define such a triple (G,Q,q) as a ***quaternionic structure*** *(**Q-structure** for short).*

The following consequences arise as a result of these axioms:

Lemma 2.4.1. *For all $a, b \in G$, we have*

1. $q(a, 1) = 0$
2. $q(a, a) = q(a, -1)$
3. $q(a, -ab) = q(a, b)$

We in fact have a theory of quadratic forms associated for Q-structures that mirror the theory of quadratic forms over fields.

Definition 2.4.2. *Given a Q-structure (G, Q, q), a **quadratic form** of dimension n over G is an n-tuple $f = \langle a_1, \cdots, a_n \rangle$, where $a_i \in G$. The discriminant of $f = \langle a_1, \cdots, a_n \rangle$ is $disc(f) = a_1 \cdots a_n$.*

As before we refer to $\langle 1, -1 \rangle$ as the hyperbolic form.

We now define isometry as follow:

Definition 2.4.3. *Two forms are n dimensional forms are **isometric** if*

1. *For $n = 1$, we say that $\langle a \rangle \cong \langle b \rangle$ if and only $a = b$.*
2. *For $n = 2$, we say that $\langle a, b \rangle \cong \langle c, d \rangle$ if and only if $ab = cd$ and $q(a, b) = q(c, d)$.*
3. *For $n > 2$, isometry is inductively defined by $\langle a_1, \cdots, a_n \rangle \cong \langle b_1, \cdots, b_n \rangle$ if and only if there's $a, b, c_3, \cdots, c_n \in G$ such that*
   $\langle a_2, \cdots, a_n \rangle \cong \langle a, c_3, \cdots, c_n \rangle$, $\langle b_2, \cdots, b_n \rangle \cong \langle b, c_3, \cdots, c_n \rangle$, and
   $\langle a_1, a \rangle \cong \langle b_1, b \rangle$.

As before, isometry can be shown to be an equivalence relation.

Remark 2.4.1. *These properties are shown to hold for the field case.*

Much of the relevant results made about quadratic forms over fields can be ported over to the setting of quadratic forms over Q-structures. Here are some relevant definitions and results that are analogous to Witt rings over fields.

Definition 2.4.4. *We say that a form f* ***represents*** *$x \in G$ if there are $x_2, \cdots, x_n \in G$ such that $f \cong \langle x, x_2, \cdots, x_n \rangle$.*

We also have an analogous notion of isotropy, with $\langle 1, -1 \rangle$ being our hyperbolic form:

Definition 2.4.5. *We say a form f is* ***isotropic*** *if $f \cong \langle 1, -1 \rangle \perp g$, for another form g. Otherwise, f is* ***anisotropic****.*

In particular, we have an analog on Witt cancellation:

Theorem 2.4.1 (Witt's Cancellation)**.** *Given forms f, g, g' over G, we have $g \cong g'$ if and only if $f \perp g' \cong f \perp g$. In fact, given f, f', g, g' where $f \cong f'$, we have $f \perp g \cong f' \perp g'$.*

Here, $\perp$ is exactly what it was in the field case. In fact, we can define addition and multiplication of quadratic forms over (G, Q, q) the same way it was defined for quadratic forms over a field. Now that we have a notion of quadratic forms and isometries, the (abstract) Witt ring over (G, Q, q) can be constructed the same way it was for quadratic forms over fields.

Proposition 2.4.1. *If we define $G(F) = F^*/F^{*2}$, $Q(F)$ as the set of quadratic forms over F that are of the form $\langle 1, -a, -b, ab \rangle$, and $q_F : G \times G \to Q$ by*
$q_F(a, b) = \langle 1, -a, -b, ab \rangle$, then the abstract Witt ring over $(G(F), Q(F), q_F)$ is exactly $W(F)$.

Remark 2.4.2. *Given a Q-structure (G, Q, q), and its abstract Witt ring R, we will refer to G (which we may also denote $S(R)$) as the square class group of R.*

2.5 Building up Bigger Abstract Witt Rings

We will now discuss how to build abstract Witt rings from existing ones.

The first construction is to use the direct product in the category of abstract Witt rings.

Definition 2.5.1. *Let R_1 and R_2 be abstract Witt rings. Then the* ***fiber product*** *over $\mathbb{Z}/2\mathbb{Z}$ is given by*

$$R_1 \coprod_{Z/2\mathbb{Z}} R_2 = \{(a,b) | a \in R_1, b \in R_2, \dim(a) \cong \dim(b) \mod 2\}.$$

We can extend this definition for an arbitrary number of abstract Witt rings.

Proposition 2.5.1. *The fiber product of abstract Witt rings over $\mathbb{Z}/2\mathbb{Z}$ is the direct product in the category of Witt rings. We will abbreviate this to just $\coprod$. In this case, Given abstract Witt rings R_i for $i \in I$, we have $S(\coprod_{i\in I} R_i) = \prod_{i\in I} S(R_i)$.*

Another way we can construct abstract Witt rings is by extending by 2-groups.

Proposition 2.5.2. *Let R be an abstract Witt ring, and let $\Delta_n = (\mathbb{Z}/2\mathbb{Z})^n$. Then the group ring $R[\Delta_n]$ is an abstract Witt ring, with $S(R[\Delta_n]) = S(R) \times \Delta_n$.*

Definition 2.5.2. *Let R be an abstract Witt ring with square class group G. We say that $a \in G$ is* ***rigid*** *if $D(\langle 1, a\rangle) = \{1, a\}$.*

Lemma 2.5.1. *Let $R = R_1[\Delta_n]$, and let H denote the subgroup of $S(R)$ that corresponds to $S(R_1)$. Then, we every element of $S(R) \setminus H$ is rigid.*

2.6 Witt Ring of Algebraic Extensions

We now discuss some results regarding Witt rings of algebraic field extensions. In particular, we will focus on the Witt rings of quadratic extensions.

We begin by introducing the transfer map. Let F be a field and K be an algebraic extension of F. Let $r : F \hookrightarrow K$ be the inclusion map of F into K. We denote $r^* : W(F) \to W(K)$ as the induced map by r (in the categorical sense). Namely, for a form q, $r^*(q) = q_K$ is given by the same form (that is, the form with the same coefficients, but now seen as elements of K) in $W(K)$.

Now, consider a nonzero F-linear functional $s : K \to F$. Since s is nonzero and linear, we see that s is surjective. Similarly, we denote $s_* : W(K) \to W(F)$ as the map induced by s. More specifically, given a quadratic space V over K with corresponding form q, we have that $s_*(q)(v) = s(q(v)) \in F$ (to see this is well defined, see Lam).

Theorem 2.6.1 (Springer's Theorem on Odd-degree extensions)**.** *Let K/F be an odd degree extension. If a quadratic form $q \in W(F)$ is anisotropic over F, then $q \in W(K)$ is anisotropic over K.*

In other words, if K/F is an odd degree extension, the mapping $r^* : W(F) \to W(K)$ is injective. This does not carry over for even degree extensions. For example, if we consider $\mathbb{R} \subset \mathbb{C}$, the form $\langle 1, 1\rangle$ is anisotropic in $\mathbb{R}$, but hyperbolic in $\mathbb{C}$.

Theorem 2.6.2. *(Frobenius Reciprocity) Let K be an algebraic extension of F. Let $f \in W(F)$ and $g \in W(K)$. Then $s_*(r^*(f) \otimes g) = f \otimes s_*(g)$.*

Now, we will discuss the Witt ring of quadratic extensions (ie. extension of degree 2). Suppose $K = F(\sqrt{d})$, where d is not a square in F. We denote the form $\delta = \langle 1, -d\rangle$.

Theorem 2.6.3. *Let $F \subset K$ be defined as above. Suppose q is anisotropic in F. Then q_K is hyperbolic over K if and only if there is some form θ such that $q_F \cong \delta \otimes \theta$. This means the kernel of $r^* : W(F) \to W(K)$ is the ideal (δ).*

Theorem 2.6.4. *Using the notation defined above, let $s : K \to F$ be the linear map defined by $s(1) = 0$ and $s(\sqrt{d}) = 1$. Let s_* be the transfer map defined by s. Then the following sequence is exact:*

$$0 \to W(F) \cdot \delta \to W(F) \xrightarrow{r^*} W(K) \xrightarrow{s_*} W(F) \xrightarrow{t} W(F) \cdot \delta \to 0,$$

where $t : W(F) \to W(F)$ is defined by $q \mapsto q \otimes \delta$. Consequently, we have the short exact sequence

$$0 \to \operatorname{coker}(t) \xrightarrow{r^*} W(K) \xrightarrow{s_*} \ker(t) \to 0.$$

Remark 2.6.1. *The above short exact sequence splits.*

Remark 2.6.2. *In order to show reciprocity in this context, it is enough to define a lift $l : \ker(t) \to W(K)$ and show that given $f \in W(F)$ and $g \in \ker(t)$, we have $l(f \otimes g) = r(f) \otimes l(g)$. This is how we will be showing reciprocity.*

Here, we see that $coker(t) = W(R)/\delta \otimes W(R)$, and $\ker(t) = ann(\langle 1, -d\rangle)$. We will use following result in the setting of abstract Witt rings:

Theorem 2.6.5. *Given a form f, $ann(f)$ is generated by all forms of the form $\langle 1, -x\rangle$, for $x \in D(f)$.*

The above exact sequence is enough to determine the $W(F)$-module structure of $W(K)$. The ring structure, however, requires knowledge of the structure of K.

2.7 Formulating our Problem

In this thesis, we will work to extend the theory of Witt rings of quadratic extensions of fields to the setting of abstract Witt rings. To set this up, take an abstract Witt ring R, with its corresponding square class group $S(R)$. Let $d \in S(R)$ be nontrivial, and let $\delta = \langle 1, -d\rangle$. We will consider the possible ring structures on R' that fit into an exact

sequence

$$0 \to R \cdot \delta \hookrightarrow R \xrightarrow{r} R' \xrightarrow{s} R \xrightarrow{t} R \cdot \delta \to 0,$$

for suitable r and s, where r is a ring homomorphism, s is a R-module homomorphism, and t is the map given by multiplication by δ. This is equivalent to finding the structures of R' where we have the (split) short exact sequence

$$0 \to coker(t) \xrightarrow{r} R' \xrightarrow{s} \ker(t) \to 0$$

for suitable r and s, and a lift $l : \ker(t) \to R'$.

We will set another condition to the structure of R', given below:

We note that $coker(t)$ (a quotient ring of R) and $\ker(t)$ (an ideal of R) are both R-modules, which means our split short exact sequence is of R-modules. This means that as an R-module, $R' \cong coker(t) \oplus \ker(t)$. So, R', which we may also refer to as $R[\sqrt{d}]$, can be written as $M \oplus N$, where M, which is the image of r, is a subring of R' isomorphic to a quotient ring of R, and N, the image of l, is another R-module. Furthermore, we note that the $coker(t)$ action (by multiplication) on $\ker(t)$ induced by the action of R (by multiplication) is well defined, as $coker(t) = R/R \cdot \delta$, while $\ker(t) = ann(\delta)$. Specifically, given $q, q' \in R$ such that $\overline{q} = \overline{q'}$ in $coker(t)$, we see that q and q' act in the same way. Thus, the $coker(t)$ action on $\ker(t)$ should be mirrored in the multiplication between elements of M and N.

The maps $r : coker(t) \to R'$ and $l : \ker(t) \to R'$ allows us to see view $coker(t)$ and $\ker(t)$ as the two summands of $R[\sqrt{a}]$. Here, there is a natural way for elements in M and N to multiply, which is given by the $coker(t)$ action on $\ker(t)$. We want this action to be compatible with how the multiplication in R' works. That is, given $\overline{q} \in coker(t)$ and $f \in \ker(t)$, we want $r(\overline{q}) \otimes l(f) = l(q \otimes f)$.

Remark 2.7.1. *This compatibility of module action with the lift is simply Frobenius reciprocity.*

Chapter 3

A Motivating Example

Let us now discuss an important example as well as a generalization that follows from it.

3.1 Field of Laurent Series

Definition 3.1.1. *Let F be a field. We define*

$$F((t)) = \left\{ \sum_{N}^{\infty} a_n x^n | N \in \mathbb{Z}, a_j \in F \right\}.$$

as the ***Laurent series field*** *over F.*

By using an iterated Newton's method, it can be shown that all series with more than one term can be written as a square. In fact, one can show the following:

Proposition 3.1.1. *$F((t))$ forms a field. The square class is given by*

$$F((t))^*/(F((t))^*)^2 = F^*/F^{*2} \oplus \langle t \rangle.$$

From this, we have an analogous result in terms of the Witt rings of Laurent fields.

Theorem 3.1.1 (Springer)**.** *Let F be a field away from characteristic 2. We have the following isomorphism: $W(F((t))) \cong W(F)[\Delta_1]$. In fact, we may extend this to $W(F((t_1, \cdots, t_n))) \cong W(F)[\Delta_n]$. (where $\Delta_n = (\mathbb{Z}/2\mathbb{Z})^n$).*

3.2 Taking the Square Root of t

Let us now consider what happens when we take the square root of t. That is, we have the quadratic extension $F((t))(\sqrt{t}) = F((\sqrt{t}))$, which is isomorphic to $F((t))$. This means that $W(F((t))) \cong W(F((\sqrt{t})))$. Thus, we see that taking the square root of t in this context yields an isomorphic Witt ring. We will use the details of this example to explore what happens in the abstract case.

We note that we can write $W(F((t))) = W(F) \oplus W(F) \cdot \langle t \rangle$ (as a direct sum of $W(F((t)))$-modules). Moreover, we note that $W(F((t))) \cdot \langle 1, -t \rangle = W(F) \cdot \langle 1, -t \rangle$, since $\langle t \rangle \otimes \langle 1, -t \rangle = -\langle 1, -t \rangle$. Similarly, we have $W(F((t))) \cdot \langle 1, t \rangle = W(F) \cdot \langle 1, t \rangle$.

In this subsection, we will denote $s : W(F((t))) \to W(F((t)))$ as the map $q \mapsto q \otimes \langle 1, -t \rangle$. Here, we note that $coker(s) = W(F((t)))/W(F((t)))$ while $\ker(t) = W(F((t))) \cdot \langle 1, a \rangle$ $(= W(F) \cdot \langle 1, a \rangle)$, since $D(\langle 1, -t \rangle) = \{1, -t\}$. From this, we have the following short exact sequence:

$$0 \to W(F((t)))/W(F((t))) \cdot \langle 1, -t \rangle \xrightarrow{r^*} W(F((\sqrt{t}))) \xrightarrow{s_*} W(F) \cdot \langle 1, t \rangle \to 0.$$

We can view $W(F((\sqrt{t})))$ as $W(F) \oplus W(F) \cdot \langle \sqrt{t} \rangle$. When we look at $r^* : W(F((t))) \to W(F((\sqrt{t})))$, we note that the image of r^* is the $W(F)$ summand of the codomain. Thus, when we view r^* as a map with domain $W(F((t)))/W(F((t))) \cdot \langle 1, -t \rangle$, r^* maps isomorphically onto the $W(F)$ summand of $W(F((\sqrt{t})))$.

Now, let us look at $s_* : W(F((\sqrt{t}))) \to W(F((t)))$. By our choice of s (where $1 \mapsto 0$ and $\sqrt{t} \mapsto 1$), we see that $\ker(s_*)$ is exactly the $W(F)$ summand of $W(F((\sqrt{t})))$. Thus, we see that s_* isomorphically maps the $W(F) \cdot \langle t \rangle$ summand to
$W(F) \cdot \langle 1, t \rangle$ $(= W(F((t))) \cdot \langle 1, t \rangle)$.

Thus, we have the following short exact sequence

$$0 \to W(F((t)))/W(F((t))) \cdot \langle 1, -t \rangle \xrightarrow{r^*} W(F) \oplus W(F) \cdot \langle \sqrt{t} \rangle \xrightarrow{s_*} W(F) \cdot \langle 1, t \rangle \to 0$$

where we see that in the middle, the $W(F)$ summand is the image of r^* and the kernel of

s_*, while the $W(F)\cdot\langle\sqrt{t}\rangle$ summand maps isomorphically to $W(F)\cdot\langle 1,t\rangle$. This is because we may view both these summands as $W(F((t)))$ modules.

We now construct a lift $l : W(F)\cdot\langle 1,t\rangle$ where $\overline{q}\otimes\langle 1,t\rangle \mapsto q\otimes\langle\sqrt{t}\rangle$. Let us check that our module action is preserved with this lift. That is, given $q \in coker(s)$ and $f\otimes\langle 1,t\rangle$, we have $l(f\otimes\langle 1,t\rangle)\otimes r_*(q) = l(q\otimes f\otimes\langle 1,t\rangle)$. We may take q to be the representative of the form where there are no t's present (ie. viewing it as an element of $W(F)$), as in $coker(t)$, we have $\overline{\langle 1\rangle} = \overline{\langle t\rangle}$. Similarly, we may $r^*(q) \in W(F((\sqrt{t})))$ also as an element of $W(F)$, and moreover, with $r^*(q) = q$.

Thus, as desired, we have

$$\begin{aligned} l(f\otimes\langle 1,t\rangle)\otimes r_*(q) &= q\otimes l(f\otimes\langle 1,t\rangle) \\ &= q\otimes f\otimes\langle\sqrt{t}\rangle \\ &= l(q\otimes f\otimes\langle 1,t\rangle). \end{aligned}$$

3.3 Generalizing the Previous Finding

We will now use our previous observation to make the following claim:

Theorem 3.3.1. *Let R be any abstract Witt ring. Given $R[\Delta_1]$, where Δ_1 is generated by t, then $R[\Delta_1][\sqrt{t}] \cong R[\Delta_1]$.*

Proof. First, we see that $S(R[\Delta_1]) = S(R)\oplus\langle t\rangle$.

Here, we can express $R[\Delta_1] = R\oplus R\cdot\langle t\rangle$ as a direct sum of modules. We will denote our claimed quadratic extension as $R' = R\oplus R\cdot\langle\sqrt{t}\rangle$, where $t = 1$ in $S(R')$. We want to find r and s such that we have the following exact sequence, with our desired module action to be preserved:

$$0 \to (R\oplus R\cdot\langle t\rangle)/((R\oplus R\langle t\rangle)\cdot\langle 1,-t\rangle) \xrightarrow{r} R\oplus R\cdot\langle\sqrt{t}\rangle \xrightarrow{s} ann\langle 1,-t\rangle \to 0.$$

We note that $(R\oplus R\cdot\langle t\rangle)/(R\oplus R\cdot\langle t\rangle)\cdot\langle 1,-t\rangle \cong R$, as in this ring, we have that $\overline{\langle 1\rangle} = \overline{\langle t\rangle}$. Let us now find $ann(\langle 1,-t\rangle)$. We note that in this case, $-t$ is rigid, and as

such, $D(\langle 1,-t\rangle) = \{1,-t\}$, in which case, $ann(\langle 1,-t\rangle)$ is generated by $\langle 1,t\rangle$ and the hyperbolic form, so $ann(\langle 1,-t\rangle) = (R \oplus R\langle t\rangle)\cdot\langle 1,t\rangle$. As $\langle t\rangle \otimes \langle 1,t\rangle = \langle 1,t\rangle$, we see that this can be written $R\cdot\langle 1,t\rangle$.

Let us now construct our map $r : (R\oplus R\cdot\langle t\rangle)/((R\oplus R\langle t\rangle)\cdot\langle 1,-t\rangle) \to R\oplus R\cdot\langle\sqrt{t}\rangle$. We first notice that we can represent each element of $(R\oplus R\cdot\langle t\rangle)/((R\oplus R\langle t\rangle)\cdot\langle 1,-t\rangle)$ by $\overline{\langle q\rangle}$, for $q\in R$. Thus, to construct r, we simply map $\overline{\langle q\rangle}\mapsto q$. Well definition of this map is clear, as $\overline{\langle 1,-t\rangle}\mapsto 0$.

Similarly, we construct $s : R\oplus R\cdot\langle\sqrt{t}\rangle \to R\cdot\langle 1,t\rangle$ by sending $q\mapsto 0$ and $q'\otimes\langle\sqrt{t}\rangle \mapsto q'\langle 1,t\rangle$, for $q,q'\in R$.

From this, we have the following split short exact sequence of modules as desired:

$$0\to (R\oplus R\cdot\langle t\rangle)/((R\oplus R\langle t\rangle)\cdot\langle 1,-t\rangle) \xrightarrow{r} R\oplus R\cdot\langle\sqrt{t}\rangle \xrightarrow{s} R\cdot\langle 1,t\rangle\to 0.$$

As before, we may have the first map mapping isomorphically onto the R summand, while the second map has the R summand as its kernel and maps the $R\cdot\langle\sqrt{t}\rangle$ summand isomorphically onto $R\cdot\langle 1,t\rangle$ by $\langle\sqrt{t}\rangle\mapsto\langle 1,t\rangle$.

We now construct an analogous lift as before: let $l : R\cdot\langle 1,t\rangle \to R\oplus R\cdot\langle\sqrt{t}\rangle$ map $q\cdot\langle 1,t\rangle\mapsto q\cdot\langle\sqrt{t}\rangle$.

Let us now show the module action is preserved. That is, given $\overline{q}\in(R\oplus R\cdot\langle t\rangle)/((R\oplus R\langle t\rangle)\cdot\langle 1,-t\rangle)$ and $f\otimes\langle 1,t\rangle \in R\cdot\langle 1,t\rangle$, we want to show that $r(\overline{q})l(f\otimes\langle 1,t\rangle) = l(q\otimes f\otimes\langle 1,t\rangle)$. As before, we may take q to be the representative without any t's (ie. viewing it as a member of R). Similarly, we may view $r(q)=q$ as the same member, but of the R-summand.

So, as desired, we see

$$\begin{aligned} l(f\otimes\langle 1,t\rangle)\otimes r_*(q) &= q\otimes l(f\otimes\langle 1,t\rangle)\\ &= q\otimes f\otimes\langle\sqrt{t}\rangle\\ &= l(q\otimes f\otimes\langle 1,t\rangle).\end{aligned}$$

■

We may take our result one step forward with the following corollary:

Corollary 3.3.1. *Let R be any abstract Witt ring. Let Δ_n be generated by $t_1, \cdots, t_n$. $R[\Delta_n][\sqrt{t_{i_1} \cdots t_{i_k}}] \cong R[\Delta_n]$, where $1 \leq i_1 < \cdots < i_k \leq n$.*

Proof. Let $\tilde{R} = R[\Delta_{n-1}]$, where Δ_{n-1} is generated by $t_1, \cdots, t_{i_1-1}, t_{i_1+1}, \cdots, t_n$. It is easy to see that $R[\Delta_n] \cong \tilde{R}[\Delta_1]$, where Δ_1 is generated by $t_{i_1} \cdots t_{i_k}$. By applying our theorem above to $\tilde{R}[\Delta_1]$, we are done. ■

Chapter 4

Another Motivating Example

Let $R = \mathbb{Z} \coprod \mathbb{Z} \coprod \mathbb{Z}$, and let $\beta_1 = (-1, 1, 1)$, $\beta_2 = (1, -1, 1)$, and $\beta_3 = (1, 1, -1)$. We also refer to $(1, 1, 1)$ as 1. We note that in this case, the only thing we need to take the square root of are β_1 and $\beta_1\beta_2$, as all the other elements from the square class that we can take the square root of can be done similarly.

4.1 Taking the root of β_1

We note that we can write $R = \mathbb{Z} \cdot \langle 1 \rangle \oplus \mathbb{Z} \cdot \langle 1, -\beta_1 \rangle \oplus \mathbb{Z} \cdot \langle 1, -\beta_2 \rangle$. Letting $t : R \to R$ as defined by multiplication of $\langle 1, -\beta_1 \rangle$. Let us first look at the kernel and cokernel of t.

First, let us look at $coker(t) = R/R \cdot \langle 1, -\beta_1 \rangle$. In this quotient ring, we have $\langle \overline{\beta_1} \rangle = \langle \overline{1} \rangle$, $\langle \overline{\beta_2} \rangle = \langle \overline{\beta_1\beta_2} \rangle$, and $\langle \overline{\beta_3} \rangle = \langle \overline{\beta_1\beta_3} \rangle$. In particular, we note that we originally had $\beta_1\beta_2\beta_3 = -1$, which tells us $\overline{\beta_2\beta_3} = \overline{-1}$ in our quotient, or in other words, $\overline{\beta_2} = -\overline{\beta_3}$.

So, we see that

$$coker(t) = \mathbb{Z} \cdot \overline{\langle 1 \rangle} \oplus \mathbb{Z} \cdot \overline{\langle 1, -\beta_2 \rangle}.$$

Now, let us look at $\ker(t)$, which is simply the annihilator of $\langle 1, -\beta_1 \rangle$. First, we note that $\langle 1, -\beta_1 \rangle$ represents $(1, \pm 1, \pm 1)$, in which case, the annihilator is generated by $\langle 1, -(1, \pm 1, \pm 1) = \langle 1, (-1, \pm 1, \pm 1) \rangle$, or in other words, generated by $\langle 1, \beta_1 \rangle$, $\langle 1, \beta_1\beta_2 \rangle =$

$\langle 1, -\beta_3\rangle$, $\langle 1, \beta_1\beta_3\rangle = \langle 1, -\beta_2\rangle$, $\langle 1, \beta_1\beta_2\beta_3\rangle$ (the last of which can be checked to be the hyperbolic form). We observe that $\langle 1, -\beta_i\rangle \otimes \langle 1, -\beta_j\rangle = 0$ for $i \neq j$. From this, we note that $\langle 1, -\beta_3\rangle \perp \langle 1, -\beta_2\rangle = \langle 1, -\beta_3, -\beta_2, \beta_2\beta_3\rangle \perp \langle 1, -\beta_2\beta_3\rangle = \langle 1, \beta_1\rangle$. So, as an R-module, $ann(\langle 1, -\beta_1\rangle)$ is generated by $\langle 1, -\beta_2\rangle$ and $\langle 1, -\beta_3\rangle$. In fact, it can be checked that $ann(\langle 1, -\beta_1\rangle) = \mathbb{Z} \cdot \langle 1, -\beta_2\rangle \oplus \mathbb{Z} \cdot \langle 1, -\beta_3\rangle$

Theorem 4.1.1. *Given $R = \mathbb{Z} \coprod \mathbb{Z} \coprod \mathbb{Z}$, we have $R[\sqrt{\beta_1}] \cong \mathbb{Z} \coprod \mathbb{Z} \coprod \mathbb{Z} \coprod \mathbb{Z}$.*

Proof. We note that $R[\sqrt{\beta_1}]$ must be a direct sum of two R-modules, which are isomorphic to $R/R \cdot \langle 1, -\beta_1\rangle$ and $ann(\langle 1, -\beta_1\rangle)$. We note that as $\beta_1 = (-1, 1, 1)$, we see two orders extend (while one does not) in two ways, and thus, $R[\sqrt{\beta_1}]$ has four orders. To see the rank of the group of square classes $R\sqrt{\beta_1}$ must have, we first note that $R/R \cdot \langle 1, -\beta_1\rangle$ eliminates one of the square classes, leaving behind two. We note that $ann(\langle 1, -\beta_1\rangle)$ is generated by $\langle 1, \beta_1\rangle$ and $\langle 1, \beta_1\beta_2\rangle$, which translates another two generators. Thus, $R[\sqrt{\beta_1}]$ must have four square classes, which is also the number of its orders. Thus, heuristically, we have $R[\sqrt{\beta_1}] \cong \mathbb{Z} \coprod \mathbb{Z} \coprod \mathbb{Z} \coprod \mathbb{Z}$.

What is left is to write down the maps from $R/R \cdot \langle 1, -\beta_1\rangle \to \mathbb{Z} \coprod \mathbb{Z} \coprod \mathbb{Z} \coprod \mathbb{Z} \to ann(\langle 1, -\delta_1\rangle)$ that preserver exactness.

We can write $\mathbb{Z} \coprod \mathbb{Z} \coprod \mathbb{Z} \coprod \mathbb{Z} = \mathbb{Z}\langle 1\rangle \oplus \mathbb{Z} \cdot q_1 \oplus \mathbb{Z} \cdot q_2 \oplus \mathbb{Z} \cdot q_3$, where $q_1 = \langle 1, -\gamma_1\rangle$, $q_2 = \langle 1, -\gamma_2\rangle$, and $q_3 = \langle 1, -\gamma_3\rangle$. Note that, $q_1 = (2, 0, 0, 0)$, $q_2 = (0, 2, 0, 0)$ and $q_3 = (0, 0, 2, 0)$ when viewed as a ring element. Here, we note that $q_i \otimes q_j = 0$, for $i \neq j$. We also note we can write $\mathbb{Z} \coprod \mathbb{Z} \coprod \mathbb{Z} \coprod \mathbb{Z} = \mathbb{Z} \cdot \langle 1\rangle \oplus \mathbb{Z} \cdot q_1 \oplus \mathbb{Z} \cdot q_2 \oplus \mathbb{Z} \cdot q_3$. Here, we construct the map $r : R/R \cdot \langle 1, -\beta_1\rangle \to \mathbb{Z} \coprod \mathbb{Z} \coprod \mathbb{Z} \coprod \mathbb{Z}$ where we take $\langle \overline{1}\rangle \mapsto \langle 1\rangle$ and $\langle \overline{\beta_2}\rangle \mapsto \langle \gamma_1\rangle$. Since $q_2 = \langle 1, -\gamma_1\rangle$, we note that the image of r is the $\mathbb{Z} \cdot \langle 1\rangle \oplus \mathbb{Z} \cdot q_1$ summand. We define our map $s : \mathbb{Z} \coprod \mathbb{Z} \coprod \mathbb{Z} \coprod \mathbb{Z} = \mathbb{Z} \cdot \langle 1\rangle \oplus \mathbb{Z} \cdot q_1 \oplus \mathbb{Z} \cdot q_2 \oplus \mathbb{Z} \cdot q_3 \to ann(\langle 1, -\beta_1\rangle)$ by $\langle 1\rangle \mapsto 0, q_1 \mapsto 0$, $q_2 \mapsto -\langle 1, -\beta_2\rangle$, and $q_3 \mapsto \langle 1, -\beta_3\rangle$. Indeed, this gives us exactness as we desired. Here, the corresponding lift is given by $l : ann(\langle 1, -\beta_1\rangle) \to \mathbb{Z} \cdot \langle 1\rangle \oplus \mathbb{Z} \cdot q_1 \oplus \mathbb{Z} \cdot q_2 \oplus \mathbb{Z} \cdot q_3$ where $\langle 1, -\beta_2\rangle \mapsto -q_2$ and $\langle 1, -\beta_3\rangle \mapsto q_3$. Moreover, we see that multiplying elements

between $\mathbb{Z}\cdot\langle 1\rangle \oplus \mathbb{Z}\cdot q_1$ and $\mathbb{Z}\cdot q_2 \oplus \mathbb{Z}\cdot q_3$ stays in $\mathbb{Z}\cdot q_2 \oplus \mathbb{Z}\cdot q_3$: given $p_1 \in \mathbb{Z}\cdot\langle 1\rangle \oplus \mathbb{Z}\cdot q_1$ and $p_2 \in \mathbb{Z}\cdot q_2 \oplus \mathbb{Z}\cdot q_3$, we have that $p_1 \otimes p_2 \in \mathbb{Z}\cdot q_2 \oplus \mathbb{Z}\cdot q_3$, since $\langle 1\rangle \otimes q_2 = q_2$ (and similarly for q_3), while $q_1 \otimes q_2 = q_1 \otimes q_3 = 0$. To see that the module action is preserved, we note that $\langle\overline{\beta_2}\rangle \otimes \langle 1, -\beta_2\rangle = \langle\beta_2, -1\rangle = -\langle 1, -\beta_2\rangle$, while $r(\langle\overline{\beta_2}\rangle) \otimes l(\langle 1, -\beta_2\rangle) = \langle\gamma_1\rangle \otimes (-q_2) = \langle\gamma_1\rangle \otimes (-\langle 1, -\gamma_2\rangle) = -\langle\gamma_1, -\gamma_1\gamma_2\rangle$. Since $\langle 1, -\gamma_1, -\gamma_2, \gamma_1\gamma_2\rangle = 0$, we see that $-\langle\gamma_1, -\gamma_1\gamma_2\rangle = -\langle 1, -\gamma_2\rangle$. So we see $l(\langle\overline{\beta_2}\rangle \otimes \langle 1, -\beta_2\rangle) = -l(\langle 1, -\beta_2\rangle) = -\langle 1, -\gamma_2\rangle = l(\langle 1, -\beta_2\rangle) \otimes r(\langle\overline{\beta_2}\rangle)$. With a similar computation, we can show that $l(\langle\overline{\beta_2}\rangle \otimes \langle 1, -\beta_3\rangle) = l(\langle 1, -\beta_3\rangle) \otimes r(\langle\overline{\beta_2}\rangle)$, which tells us indeed that the module action is respected. ■

4.2 Taking the root of $\beta_1\beta_2$

With $t : R \to R$ be multiplication by $\langle 1, -\beta_1\beta_2\rangle$, let us first look at $\ker(t)$ and $coker(t)$.

We begin with $coker(t) = R/R\cdot\langle 1, -\beta_1\beta_2\rangle$. We note that if we write $R = \mathbb{Z}\cdot\langle 1\rangle \oplus \mathbb{Z}\cdot\langle\beta_1\rangle \oplus \mathbb{Z}\cdot\langle\beta_1\beta_2\rangle$, we see that $R\cdot\langle 1, -\beta_1\beta_2\rangle = \mathbb{Z}\cdot\langle 1, -\beta_1\beta_2\rangle + \mathbb{Z}\cdot\langle\beta_1, -\beta_2\rangle$. This tells us that in $R/R\cdot\langle 1, -\beta_1\beta_2\rangle$, we have $\langle\overline{\beta_1}\rangle = \langle\overline{\beta_2}\rangle$, and that $\langle\overline{1}\rangle = \langle\overline{\beta_1\beta_2}\rangle$. From this, we see that $R/R\cdot\langle 1, -\beta_1\beta_2\rangle$ is generated by $\langle\overline{1}\rangle$ and $\langle\overline{\beta_1}\rangle$, which equivalently, can be generated by $\langle\overline{1}\rangle$ and $\langle 1, -\overline{\beta_1}\rangle$. We note that $\langle 1, -\overline{\beta_1}\rangle$ has torsion, since $\langle 1, -\overline{\beta_1}\rangle \perp \langle 1, -\overline{\beta_1}\rangle = \langle 1, -\overline{\beta_1}, 1, -\overline{\beta_1}\rangle = \langle 1, -\overline{\beta_1}, \overline{\beta_2}, -\overline{\beta_1\beta_2}\rangle = \langle 1, -\overline{\beta_1\beta_2}\rangle \perp \langle\overline{\beta_1}, -\overline{\beta_2}\rangle = 0$ (indeed, these are elements in $R\cdot\langle 1, -\beta_1\beta_2\rangle$). We know that $\langle 1\rangle$ is torsion free, which means we can write $R/R\cdot\langle 1, -\beta_1\beta_2\rangle = \mathbb{Z}\cdot\langle 1\rangle \oplus (\mathbb{Z}/2\mathbb{Z})\cdot\langle 1, -\beta_1\rangle$

Let us now examine $ann\langle 1, -\beta_1\beta_2\rangle$. We note that
$\langle 1, -\beta_1\beta_2\rangle = \langle 1, -(-1, -1, 1)\rangle = \langle 1, (1, 1, -1)\rangle$, which tells us that it represents $(1, 1, \pm 1)$. This tells us that $ann\langle 1, -\beta_1\beta_2\rangle$ is generated by $\langle 1, -(1, 1, -\pm 1)\rangle$, thus amounting to $\langle 1, (-1, -1, \pm 1)\rangle$. This is precisely $\langle 1, \beta_1\beta_2\rangle$ and the hyperbolic form, which tells us that $ann\langle 1, -\beta_1\rangle$ is generated by $\langle 1, \beta_1\beta_2\rangle$ as an R-module. In fact, it can be easily verified to be $\mathbb{Z}\cdot\langle 1, \beta_1\beta_2\rangle$.

Now, since we are taking the square root of $\beta_1\beta_2$, which is $(-1, -1, 1)$ in our ring,

we note that only one order extends (into two), while the first two do not. As we are quotienting by $R \cdot \langle 1, -\beta_1\beta_2 \rangle$, we are losing one of our square class generators. However, since $ann\langle 1, -\beta_1\beta_2 \rangle = \mathbb{Z} \cdot \langle 1, \beta_1\beta_2 \rangle$, we are gaining a square class generator. Thus, in $R[\sqrt{\beta_1\beta_2}]$, we have two orders and three square classes. Thus, heuristically, we have three fiber product factors, two of which are $\mathbb{Z}$ and one of which is singly generated and has torsion. So heuristically, we have $R[\sqrt{\beta_1\beta_2}] \cong \mathbb{Z} \coprod \mathbb{Z} \coprod \mathbb{Z}/4\mathbb{Z}$.

Theorem 4.2.1. *With $R = \mathbb{Z} \coprod \mathbb{Z} \coprod \mathbb{Z}$, we have $R[\sqrt{\beta_1\beta_2}] \cong \mathbb{Z} \coprod \mathbb{Z} \coprod \mathbb{Z}/4\mathbb{Z}$.*

Proof. Let us now look at $\mathbb{Z} \coprod \mathbb{Z} \coprod \mathbb{Z}/4\mathbb{Z}$. Denote $1 = (1,1,1)$, $\gamma_1 = (-1,1,1)$, $\gamma_2 = (1,-1,1)$, and $\gamma_3 = (1,1,-1)$. We know that elements here look like $(even, even, even)$ or (odd, odd, odd). We can check that $\mathbb{Z} \coprod \mathbb{Z} \coprod \mathbb{Z}/4$ is generated by $\langle 1 \rangle$, $\langle 1, -\gamma_2 \rangle$, and $\langle 1, -\gamma_3 \rangle$. We note that this corresponds to $(1,1,1), (0,2,0)$, and $(0,0,2)$ as generators. We can readily check $\langle 1, -\gamma_3 \rangle \perp \langle 1, -\gamma_3 \rangle = 0$. So, we can express $\mathbb{Z} \coprod \mathbb{Z} \coprod \mathbb{Z}/4\mathbb{Z} = \mathbb{Z} \cdot \langle 1 \rangle \oplus \mathbb{Z} \cdot \langle 1, -\gamma_2 \rangle \oplus (\mathbb{Z}/2\mathbb{Z}) \cdot \langle 1, -\gamma_3 \rangle$.

Let us now construct our maps. Let $r : R/R \cdot \langle 1, -\beta_1\beta_2 \rangle \to \mathbb{Z} \coprod \mathbb{Z} \coprod \mathbb{Z}/4\mathbb{Z}$ $(= \mathbb{Z} \cdot \langle 1 \rangle \oplus \mathbb{Z} \cdot \langle 1, -\gamma_1 \rangle \oplus (\mathbb{Z}/2\mathbb{Z}) \cdot \langle 1, -\gamma_3 \rangle)$ be define by $\langle \overline{1} \rangle \mapsto \langle 1 \rangle$, and $\overline{\langle 1, -\beta_1 \rangle} \mapsto \langle 1, -\gamma_3 \rangle$ (note that $\langle \overline{\beta_1} \rangle \mapsto \langle \gamma_3 \rangle$). We can easily see that r is injective with its image being $\mathbb{Z} \cdot \langle 1 \rangle \oplus \mathbb{Z}/2\mathbb{Z} \cdot \langle 1, -\gamma_3 \rangle$. Let $s : \mathbb{Z} \coprod \mathbb{Z} \coprod \mathbb{Z}/4\mathbb{Z} \, (= \mathbb{Z} \cdot \langle 1 \rangle \oplus \mathbb{Z} \cdot \langle 1, -\gamma_2 \rangle \oplus (\mathbb{Z}/2\mathbb{Z}) \cdot \langle 1, -\gamma_3 \rangle)$ $\to ann(\langle 1, -\beta_1\beta_2 \rangle)$ be defined by $\langle 1 \rangle \mapsto 0$, $\langle 1, -\gamma_3 \rangle \mapsto 0$, and $\langle 1, -\gamma_2 \rangle \mapsto \langle 1, \beta_1\beta_2 \rangle$. By construction, it is easy to see that the following is a short exact sequence:

$$0 \to R/R \cdot \langle 1, -\beta_1\beta_2 \rangle \xrightarrow{r} \mathbb{Z} \coprod \mathbb{Z} \coprod \mathbb{Z}/4\mathbb{Z} \xrightarrow{s} ann(\langle 1, -\beta_1\beta_2 \rangle) \to 0.$$

The corresponding lift is $l : ann(\langle 1, -\beta_1\beta_2 \rangle) \to \mathbb{Z} \coprod \mathbb{Z} \coprod \mathbb{Z}/4\mathbb{Z}$ by $\langle 1, \beta_1\beta_2 \rangle \mapsto \langle 1, -\gamma_2 \rangle$. It is easy to see that the image of r acts on the image of l, since $\langle 1 \rangle \otimes \langle 1, -\gamma_2 \rangle = \langle 1, -\gamma_2 \rangle$ and $\langle \gamma_1 \rangle \otimes \langle 1, -\gamma_2 \rangle = \langle \gamma_1, -\gamma_1\gamma_2 \rangle = \langle 1, -\gamma_2 \rangle$. To see that our life l is indeed compatible with the module action, we note that

$$\begin{aligned} l(\langle 1, \beta_1\beta_2\rangle) \otimes r(\langle\overline{\beta_1}\rangle) &= \langle 1, -\gamma_2\rangle \otimes \langle\gamma_3\rangle \\ &= \langle\gamma_3, -\gamma_2\gamma_3\rangle \\ &= \langle 1, -\gamma_2\rangle \end{aligned}$$

as well as

$$\begin{aligned} l(\langle 1, \beta_1\beta_2\rangle \otimes \langle\beta_1\rangle) &= l(\langle\beta_1, \beta_2\rangle) \\ &= l(\langle 1, \beta_1\beta_2\rangle) \\ &= \langle 1, -\gamma_2\rangle \end{aligned}$$

so indeed, $l(\langle 1, \beta_1\beta_2\rangle) \otimes r(\langle\beta_1\rangle) = l(\langle 1, \beta_1\beta_2\rangle \otimes \langle\beta_1\rangle)$.

Thus, we have shown that the module action is respected, so indeed, our candidate ring fits into the short exact sequence as $R[\sqrt{\beta_1\beta_2}]$. ■

Chapter 5

Generalizing the Previous Findings

In this section, we generalize some of the results we found above. Let $R = \coprod_{i=1}^{n} \mathbb{Z}$. As before, let β_i be the element with -1 on the ith spot and 1 everywhere else.

5.1 The Case of $n = 2$

We begin by examining the easiest case: when $n = 2$. That is, we look at the abstract Witt ring $\mathbb{Z} \coprod \mathbb{Z}$.

Lemma 5.1.1. *We have the following isomorphism:* $\mathbb{Z} \coprod \mathbb{Z} \cong \mathbb{Z}[\Delta_1]$.

Proof. Let $\mathbb{Z}[\Delta_1] = \mathbb{Z} \cdot \langle 1 \rangle \oplus \mathbb{Z} \cdot \langle t \rangle$, where t generates Δ_1. Let $\beta = (1, -1) \in \mathbb{Z} \coprod \mathbb{Z}$. We notice that we may write

$$\mathbb{Z} \coprod \mathbb{Z} = \mathbb{Z} \cdot \langle 1 \rangle \oplus \mathbb{Z}\langle \beta \rangle.$$

With that, we construct

$$\phi : \mathbb{Z} \coprod \mathbb{Z} \to \mathbb{Z}[\Delta_1]$$

where $\langle 1 \rangle \mapsto \langle 1 \rangle$ and $\langle \beta \rangle \mapsto \langle t \rangle$. It is easy to see that ϕ is a ring isomorphism. ■

From the above lemma, we notice that taking the square root of β in $\mathbb{Z} \coprod \mathbb{Z}$ is analogous to taking the square root of t in $\mathbb{Z}[\Delta_1]$. From this, we get the following corollary:

Corollary 5.1.1. *Let $R = \mathbb{Z} \coprod \mathbb{Z}$, and let $\beta = (1, -1)$. Then $R[\sqrt{\beta}] \cong R$.*

Proof. We note that $R \cong \mathbb{Z}[\Delta_1]$, and we are taking the square root of β, which is analogous to t in $\mathbb{Z}[\Delta_1]$. By Theorem 3.3.1, we are done. ■

5.2 Taking the square root of β_1

As before, we may write

$$R = \mathbb{Z} \cdot \langle 1 \rangle \oplus \mathbb{Z} \cdot \langle 1, -\beta_1 \rangle \oplus \cdots \oplus \mathbb{Z} \cdot \langle 1, -\beta_{n-1} \rangle.$$

From this, we can write

$$R/R \cdot \langle 1, -\beta_1 \rangle = \mathbb{Z} \cdot \overline{\langle 1 \rangle} \oplus \mathbb{Z} \cdot \overline{\langle 1, -\beta_2 \rangle} \oplus \cdots \oplus \mathbb{Z} \cdot \overline{\langle 1, -\beta_{n-1} \rangle}.$$

Now, let us look at $ann(\langle 1, -\beta_1 \rangle)$. We note that $D\langle 1, -\beta_1 \rangle = D\langle 1, -(-1, 1, \cdots, 1) \rangle = \{(1, \pm 1, \cdots, \pm 1)\}$. As such, we see that $ann(\langle 1, -\beta_1 \rangle)$ is generated by $\langle 1, -(1, \pm 1, \cdots, \pm 1) \rangle$. Furthermore, we can show that $ann(\langle 1, -\beta_1 \rangle) = \mathbb{Z} \cdot \langle 1, -\beta_2 \rangle \oplus \cdots \oplus \mathbb{Z} \cdot \langle 1, -\beta_n \rangle$.

In this section, we show that $R[\sqrt{\beta_1}] \cong \coprod_{i=1}^{2n-2} \mathbb{Z}$. The heuristics behind this is as follows. When we take the square root of β_1, all but one order extends in two ways, resulting in $2n-2$ orders. Now, we notice that by taking the square root of β_1, we lose a square class generator. However as $ann(\langle 1, -\beta_1 \rangle)$ has rank $n-1$, we gain another $n-1$, thus giving us $2n-2$ square classes, which is also the numbers of orders we have.

Theorem 5.2.1. *Let $R = \coprod_{i=1}^{n} \mathbb{Z}$, for $n > 1$. Then*

$$R[\sqrt{\beta_1}] \cong \coprod_{i=1}^{2n-2} \mathbb{Z}.$$

Proof. Indeed, we have shown this to be true for $n = 2, 3$. Let us show this for $n > 3$.

Let us write

$$\coprod_{i=1}^{2n-2} \mathbb{Z} = \mathbb{Z} \cdot \langle 1 \rangle \oplus \mathbb{Z} \cdot \langle 1, \gamma_2\gamma_n \rangle \oplus \cdots \oplus \mathbb{Z} \cdot \langle 1, \gamma_{n-1}\gamma_{2n-3} \rangle$$
$$\oplus \mathbb{Z} \cdot \langle 1, -\gamma_n \rangle \oplus \cdots \oplus \mathbb{Z} \cdot \langle 1, -\gamma_{2n-2} \rangle.$$

Since $\langle 1, \gamma_j\gamma_{j+n-2} \rangle = \langle \gamma_j, \gamma_{j+n-2} \rangle$, it can be readily verified that our direct sum is indeed a direct sum.

First, we construct our map

$$r : R/R \cdot \langle 1, -\beta_1 \rangle \left(= \mathbb{Z} \cdot \overline{\langle 1 \rangle} \oplus \mathbb{Z} \cdot \overline{\langle 1, -\beta_2 \rangle} \oplus \cdots \oplus \mathbb{Z} \cdot \overline{\langle 1, -\beta_{n-1} \rangle} \right)$$
$$\to \coprod_{i=1}^{2n-2} \mathbb{Z} \big(= \mathbb{Z} \cdot \langle 1 \rangle \oplus \mathbb{Z} \cdot \langle 1, \gamma_2\gamma_n \rangle \oplus \cdots \oplus \mathbb{Z} \cdot \langle 1, \gamma_{n-1}\gamma_{2n-3} \rangle$$
$$\oplus \mathbb{Z} \cdot \langle 1, -\gamma_n \rangle \oplus \cdots \oplus \mathbb{Z} \cdot \langle 1, -\gamma_{2n-2} \rangle \big)$$

as follows: $\overline{\langle 1 \rangle} \mapsto \langle 1 \rangle$, and for j between 2 and $n-1$, we send $\overline{\langle \beta_j \rangle} \mapsto \langle \gamma_j\gamma_{j+n-2\rangle}$. Here, it can be readily checked that this is an injective ring homomorphism. Here, the image is

$$\mathbb{Z} \cdot \langle 1 \rangle \oplus \mathbb{Z} \cdot \langle 1, \gamma_2\gamma_n \rangle \oplus \cdots \oplus \mathbb{Z} \cdot \langle 1, \gamma_{n-1}\gamma_{2n-3} \rangle.$$

Now, we construct

$$s : \coprod_{i=1}^{2n-2} \mathbb{Z} \big(= \mathbb{Z} \cdot \langle 1 \rangle \oplus \mathbb{Z} \cdot \langle 1, \gamma_2\gamma_n \rangle \oplus \cdots \oplus \mathbb{Z} \cdot \langle 1, \gamma_{n-1}\gamma_{2n-3} \rangle$$
$$\oplus \mathbb{Z} \cdot \langle 1, -\gamma_n \rangle \oplus \cdots \oplus \mathbb{Z} \cdot \langle 1, -\gamma_{2n-2} \rangle \big)$$
$$\to ann(\langle 1, -\beta_1 \rangle) \, (= \mathbb{Z} \cdot \langle 1, -\beta_2 \rangle \oplus \cdots \oplus \mathbb{Z} \cdot \langle 1, -\beta_n \rangle)$$

Here, we send $\langle 1 \rangle \mapsto 0$, $\langle 1, \gamma_j\gamma_{j+n-2} \rangle \mapsto 0$ for all $2 \leq j \leq n-1$, and for $j \geq n$, we have $\langle 1, -\gamma_j \rangle \mapsto \langle 1, -\beta_{j-n+2} \rangle$ (e.g. $\langle 1, -\gamma_n \rangle \mapsto \langle 1, -\beta_2 \rangle$). By construction, it is clear that

$$0 \to R/R \cdot \langle 1, -\beta_1 \rangle \to \coprod_{i=1}^{2n-2} \mathbb{Z} \to ann(\langle 1, -\beta_1 \rangle) \to 0$$

is exact. So, we have the corresponding lift $\langle 1, -\beta_j \rangle \mapsto \langle 1, -\gamma_{j+n-2} \rangle$.

Let us now show that the module action is respected. It is clear that $r(\langle 1 \rangle) \otimes l(\langle 1, -\beta_j \rangle) = l(\langle 1 \rangle \otimes \langle 1, -\beta_j \rangle)$. To see the rest of the generators behave as expected, we first show that for all (suitable) j, we have $r(\langle \beta_j \rangle) \otimes l(\langle 1, -\beta_j \rangle) = l(\langle \beta_j \rangle \otimes \langle 1, -\beta_j \rangle)$:

$$\begin{aligned} r(\langle\beta_j\rangle) \otimes l(\langle 1, -\beta_j\rangle) &= \langle\gamma_j\gamma_{j+n-2}\rangle \otimes \langle 1, -\gamma_{j+n-2}\rangle \\ &= \langle\gamma_j\gamma_{j+n-2}, -\gamma_j\rangle \\ &= -\langle 1, -\gamma_{j+n-2}\rangle \end{aligned}$$

$$\begin{aligned} l(\langle\beta_j\rangle \otimes \langle 1, -\beta_j\rangle) &= l(\langle\beta_j, -1\rangle) \\ &= l(-\langle 1, -\beta_j\rangle) \\ &= -l(\langle 1, -\beta_j\rangle) \\ &= -\langle 1, -\gamma_{j+n-2}\rangle \end{aligned}$$

So indeed, we have $r(\langle\beta_j\rangle) \otimes l(\langle 1, -\beta_j\rangle) = l(\langle\beta_j\rangle \otimes \langle 1, -\beta_j\rangle)$ for all (suitable) j.

Now, for $i \neq j$, let us show $r(\langle\beta_i\rangle) \otimes l(\langle 1, -\beta_j\rangle) = l(\langle\beta_i\rangle \otimes \langle 1, -\beta_j\rangle)$:

$$\begin{aligned} r(\langle\beta_i\rangle) \otimes l(\langle 1, -\beta_j\rangle) &= \langle\gamma_i\gamma_{i+n-2}\rangle \otimes \langle 1, -\gamma_{j+n-2}\rangle \\ &= \langle\gamma_i\gamma_{i+n-2}, -\gamma_i\gamma_{i+n-2}\gamma_{j+n-2}\rangle \\ &= \langle 1, -\gamma_{j+n-2}\rangle \end{aligned}$$

$$\begin{aligned} l(\langle\beta_i\rangle \otimes \langle 1, -\beta_j\rangle) &= l(\langle\beta_i, -\beta_i\beta_j\rangle) \\ &= l(\langle 1, -\beta_j\rangle) \\ &= l(\langle 1, -\beta_j\rangle) \\ &= \langle 1, -\gamma_{j+n-2}\rangle \end{aligned}$$

So indeed, our module action is respected. ■

5.3 Taking the square root of $\beta_1 \cdots \beta_{n-1} (= -\beta_n)$

We note that $\beta_1 \cdots \beta_{n-1} = -\beta_n = (-1, -1, \cdots, -1, 1)$. Heuristically, taking the square root would extend one of the orders to two orders, while the rest do not extend. We note that quotienting by $\langle 1, \beta_1\rangle$ would eliminate one of the square class generators. However, we also note that $ann(\langle 1, \beta_n\rangle) = \mathbb{Z}\cdot\langle 1, -\beta_n\rangle$, since $D(\langle 1, \beta_n\rangle) = D(\langle 1, (1, 1, \cdots, 1, -1)\rangle) = (1, 1, 1 \cdots, 1, \pm 1)$. Thus, $ann(\langle 1, \beta_n\rangle) = \mathbb{Z}\cdot\langle 1, \beta_n\rangle$. This also means that we gain another square class, and so, we have n generators for our square class. Thus, we expect to have the following theorem:

Theorem 5.3.1. *Let $R = \coprod_{i=1}^{n} \mathbb{Z}$, for $n > 1$. Then*

$$R[\sqrt{-\beta_n}] \cong \mathbb{Z} \coprod \mathbb{Z} \coprod \left(\coprod_{i=3}^{n} \mathbb{Z}/4\mathbb{Z} \right).$$

Proof. Let us write $R = \mathbb{Z} \cdot \langle 1 \rangle \oplus \mathbb{Z} \cdot \langle \beta_1 \rangle \oplus \cdots \oplus \mathbb{Z} \cdot \langle \beta_{n-1} \rangle$. Since $R \cdot \langle 1, \beta_n \rangle$ gives us $\mathbb{Z} \cdot \langle 1, \beta_n \rangle + \mathbb{Z} \cdot \langle \beta_n, \beta_1\beta_n \rangle + \cdots + \mathbb{Z} \cdot \langle \beta_n, \beta_{n-1}\beta_n \rangle$, which tells us that in $R/R \cdot \langle 1, \beta_n \rangle$, we have $\overline{\langle \beta_n \rangle} = -\overline{\langle 1 \rangle}$. This also means $\overline{\langle \beta_1\beta_2 \cdots \beta_{n-1} \rangle} = \overline{\langle 1 \rangle}$. We also see that for any $0 < i < n$,

$$\begin{aligned}
\overline{\langle 1, -\beta_i \rangle} \perp \overline{\langle 1, -\beta_i \rangle} &= \overline{\langle 1, -\beta_i, 1, -\beta_i \rangle} \\
&= \overline{\langle 1, -\beta_i, -\beta_n, -\beta_i \rangle} \\
&= \overline{\langle -\beta_i, -\beta_i\beta_n \rangle} \\
&= \overline{\langle -\beta_i \rangle} \otimes \overline{\langle 1, \beta_n \rangle} \\
&= 0
\end{aligned}$$

which tells us that each $\overline{\langle 1, -\beta_i \rangle}$ in $R/R \cdot \langle 1, \beta_n \rangle$ has 2-torsion. Moreover, we note that

$$\begin{aligned}
\overline{\langle 1, -\beta_1 \rangle} \perp \overline{\langle 1, -\beta_2 \rangle} \perp \cdots \perp \overline{\langle 1, -\beta_[n-1] \rangle} &= \overline{\langle 1, -\beta_1\beta_2 \cdots \beta_{n-1} \rangle} \\
&= \overline{\langle 1, \beta_n \rangle} \\
&= 0
\end{aligned}$$

which tells us that $\overline{\langle 1, -\beta_1 \rangle}$ can be written as a sum of the other $\overline{\langle 1, -\beta_i \rangle}$. So, we can write

$$R/R \cdot \langle 1, \beta_n \rangle = \mathbb{Z}\langle 1 \rangle \oplus (\mathbb{Z}/2\mathbb{Z})\langle 1, -\beta_2 \rangle \oplus \cdots \oplus (\mathbb{Z}/2\mathbb{Z})\langle 1, -\beta_{n-1} \rangle.$$

Let us write $\mathbb{Z} \coprod \mathbb{Z} \coprod \left(\coprod_{i=3}^{n} \mathbb{Z}/4\mathbb{Z} \right)$
$= \mathbb{Z} \cdot \langle 1 \rangle \oplus \mathbb{Z} \cdot \langle 1, -\gamma_1 \rangle \oplus (\mathbb{Z}/2\mathbb{Z}) \cdot \langle 1, -\gamma_2 \rangle \oplus \cdots \oplus (\mathbb{Z}/2\mathbb{Z}) \cdot \langle 1, -\gamma_{n-1} \rangle$.

We observe that $\langle 1, -\gamma_i \rangle \perp \langle 1, -\gamma_i \rangle = 0$ for $i \geq 2$. With this in mind, we construct our map

$$\begin{aligned}
r : R/R \cdot \langle 1, \beta_1 \rangle \, (&= \mathbb{Z}\langle 1 \rangle \oplus (\mathbb{Z}/2\mathbb{Z})\langle 1, -\beta_2 \rangle \oplus \cdots \oplus (\mathbb{Z}/2\mathbb{Z})\langle 1, -\beta_{n-1} \rangle) \\
&\to \mathbb{Z} \cdot \langle 1 \rangle \oplus \mathbb{Z} \cdot \langle 1, -\gamma_1 \rangle \oplus (\mathbb{Z}/2\mathbb{Z}) \cdot \langle 1, -\gamma_2 \rangle \oplus \cdots \oplus (\mathbb{Z}/2\mathbb{Z}) \cdot \langle 1, -\gamma_{n-1} \rangle
\end{aligned}$$

by sending $\langle 1\rangle \mapsto \langle 1\rangle$ and for $1 < i < n$, we send $\langle \beta_i\rangle \mapsto \langle \gamma_i\rangle$. Here, the image of r is

$$\mathbb{Z}\cdot\langle 1\rangle \oplus (\mathbb{Z}/2\mathbb{Z})\cdot\langle 1,-\gamma_2\rangle \oplus \cdots \oplus (\mathbb{Z}/2\mathbb{Z})\cdot\langle 1,-\gamma_{n-1}\rangle.$$

We define

$$\begin{aligned} s : \mathbb{Z}\cdot\langle 1\rangle \oplus \mathbb{Z}\cdot\langle 1,-\gamma_1\rangle \oplus (\mathbb{Z}/2\mathbb{Z})\cdot\langle 1,-\gamma_2\rangle \oplus \cdots \oplus (\mathbb{Z}/2\mathbb{Z})\cdot\langle 1,-\gamma_{n-1}\rangle \\ \to ann(\langle 1,\beta_n\rangle)\,(= \mathbb{Z}\cdot\langle 1,-\beta_n\rangle) \end{aligned}$$

by $\langle 1\rangle \mapsto 0$, $\langle 1,-\gamma_i\rangle \mapsto 0$ for $i \neq 1$, and $\langle 1,-\gamma_1\rangle \mapsto \langle 1,-\beta_n\rangle$.

It is clear by construction that

$$0 \to R/R\cdot\langle 1,\beta_n\rangle \to \mathbb{Z}\coprod\mathbb{Z}\coprod\left(\coprod_{i=3}^{n}\mathbb{Z}/4\mathbb{Z}\right) \to ann(\langle 1,\beta_n\rangle) \to 0$$

is exact, with the corresponding lift $l : ann(\langle 1,\beta_n\rangle) \to \mathbb{Z}\cdot\langle 1\rangle \oplus \mathbb{Z}\cdot\langle 1,-\gamma_1\rangle \oplus (\mathbb{Z}/2\mathbb{Z})\cdot\langle 1,-\gamma_2\rangle \oplus \cdots \oplus (\mathbb{Z}/2\mathbb{Z})\cdot\langle 1,-\gamma_{n-1}\rangle$ given by $\langle 1,-\beta_n\rangle \mapsto \langle 1,-\gamma_1\rangle$.

Let us now show that the module action is respected. Clearly, we have that $r(\langle 1\rangle)\otimes l(\langle 1,-\gamma_n\rangle) = l(r(\langle 1\rangle)\otimes\langle 1,-\gamma_n\rangle)$. Let us show that $r(\langle\beta_i\rangle)\otimes l(\langle 1,-\gamma_n\rangle) = l(\langle\beta_i\rangle\otimes\langle 1,-\gamma_n\rangle)$, for $1 < i < n$. To see this, we observe

$$\begin{aligned} r(\langle\beta_i\rangle)\otimes l(\langle 1,-\beta_n\rangle) &= \langle\gamma_i\rangle\otimes\langle 1,-\gamma_1\rangle \\ &= \langle\gamma_i,-\gamma_1\gamma_i\rangle \\ &= \langle 1,-\gamma_1\rangle \end{aligned}$$

$$\begin{aligned} l(\langle\beta_i\rangle\otimes\langle 1,-\beta_n\rangle) &= l(\langle\beta_i,-\beta_i\beta_n\rangle) \\ &= l(\langle 1,-\beta_n\rangle) \\ &= \langle 1,-\gamma_1\rangle \end{aligned}$$

So indeed, $r(\langle\beta_i\rangle)\otimes l(\langle 1,-\gamma_n\rangle) = l(\langle\beta_i\rangle\otimes\langle 1,-\gamma_n\rangle)$. Since $\langle 1\rangle$ and $\langle 1,-\beta_i\rangle$ for $1 < i < n$ are the generators for $R/R\cdot\langle 1,\beta_n\rangle$, the above computation shows that the module action is preserved. ■

5.4 Taking the square root of $\beta_1\cdots\beta_k$, for $k < n$

Taking inspiration from our previous cases, we prove the following theorem:

Theorem 5.4.1. *Let $R = \coprod_{i=1}^{n} \mathbb{Z}$, where $n \geq 2$. For $k < n$, we have*

$$R[\sqrt{\beta_1\beta_2\cdots\beta_{k-1}\beta_k}] \cong \left(\coprod_{i=1}^{2(n-k)} \mathbb{Z}\right) \coprod \left(\coprod_{i=2(n-k)+1}^{2n-(k+1)} \mathbb{Z}/4\mathbb{Z}\right).$$

Proof. First, let us look at $R/R \cdot \langle 1, -\beta_1 \cdots \beta_k\rangle$. We note that $\overline{\langle 1\rangle} = \overline{\langle \beta_1 \cdots \beta_k\rangle}$ in $R/R \cdot \langle 1, -\beta_1 \cdots \beta_k\rangle$. This means that $\overline{\langle \beta_{k+1} \cdots \beta_n\rangle} = -1$, and so, for any $1 \leq i \leq k$, we see that

$$\begin{aligned}
\overline{\langle 1, -\beta_i\rangle} \perp \overline{\langle 1, -\beta_i\rangle} &= \overline{\langle 1, -\beta_i, 1, -\beta_i\rangle} \\
&= \overline{\langle 1, -\beta_i, -\beta_1 \cdots \beta_{i-1}\beta_{i+1} \cdots \beta_k, 1\rangle} \\
&= \overline{\langle 1, -\beta_i, -\beta_1 \cdots \beta_{i-1}\beta_{i+1} \cdots \beta_k, \beta_1 \cdots \beta_k\rangle} \\
&= 0
\end{aligned}$$

Thus, we see that $\overline{\langle 1, -\beta_i\rangle}$, for $i \leq k$, has 2-torsion.

We also note that

$$\begin{aligned}
\overline{\langle 1, -\beta_1\rangle} \perp \cdots \perp \overline{\langle 1, -\beta_k\rangle} &= \overline{\langle 1, -\beta_1 \cdots \beta_k\rangle} \\
&= 0
\end{aligned}$$

Since we may write $R = \mathbb{Z} \cdot \langle 1\rangle \oplus \mathbb{Z} \cdot \langle 1, -\beta_1\rangle \oplus \cdots \oplus \mathbb{Z} \cdot \langle 1, -\beta_{n-1}\rangle$, and we only need $k-1$ of our $\overline{\langle 1, -\beta_i\rangle}$, for $i \leq k$, we can represent

$$\begin{aligned}
R/R \cdot \langle 1, -\beta_1 \cdots \beta_k\rangle = \mathbb{Z} \cdot \overline{\langle 1\rangle} \oplus (\mathbb{Z}/2\mathbb{Z}) \cdot \overline{\langle 1, -\beta_2\rangle} \oplus \cdots \oplus (\mathbb{Z}/2\mathbb{Z}) \cdot \overline{\langle 1, -\beta_k\rangle} \\
\oplus \mathbb{Z} \cdot \overline{\langle 1, -\beta_{k+1}\rangle} \oplus \cdots \oplus \mathbb{Z} \cdot \overline{\langle 1, -\beta_{n-1}\rangle}.
\end{aligned}$$

Now, we see that $D(\langle 1, -\beta_1 \cdots \beta_k) = D(\langle 1, (1, \cdots, 1, -1 \cdots, -1)\rangle)$
$= (1, \cdots, 1, \pm 1, \cdots, \pm 1)$, where the first k are 1 and the last $n-k$ is ± 1. This means $ann(\langle 1, -\beta_1 \cdots \beta_k\rangle)$ can be additively generated by $\langle 1, -\beta_i\rangle$, for $k+1 \leq i \leq n$, and so, we may write

$$ann(\langle 1, -\beta_1 \cdots \beta_k\rangle) = \mathbb{Z} \cdots \langle 1, -\beta_{k+1}\rangle \oplus \cdots \oplus \mathbb{Z} \cdot \langle 1, -\beta_n\rangle.$$

For our candidate ring, let us write

$$\left(\coprod_{i=1}^{2(n-k)} \mathbb{Z}\right) \coprod \left(\coprod_{i=2(n-k)+1}^{2n-(k+1)} \mathbb{Z}/4\mathbb{Z}\right)$$
$$= \mathbb{Z} \cdot \langle 1 \rangle \oplus \mathbb{Z} \cdot \langle 1, \gamma_2\gamma_{n-k+1} \rangle \oplus \cdots \oplus \mathbb{Z} \cdot \langle 1, \gamma_{n-k}\gamma_{2(n-k)-1} \rangle$$
$$\oplus \mathbb{Z} \cdot \langle 1, -\gamma_{n-k+1} \rangle \oplus \cdots \oplus \mathbb{Z} \cdot \langle 1, -\gamma_{2n-2k} \rangle$$
$$\oplus (\mathbb{Z}/2\mathbb{Z}) \cdot \langle 1, -\gamma_{2(n-k)+1} \oplus \cdots \oplus (\mathbb{Z}/2\mathbb{Z}) \cdot \langle 1, -\gamma_{2n-(k+1)} \rangle.$$

Indeed, we see that this is a direct sum, since $\langle 1, \gamma_j\gamma_{j+n-k-1} \rangle = \langle \gamma_j, \gamma_{j+n-k-1} \rangle$.

We now construct

$$r : R/R \cdot \langle 1, -\beta_1 \cdots \beta_k \rangle \to \left(\coprod_{i=1}^{2(n-k)} \mathbb{Z}\right) \coprod \left(\coprod_{i=2(n-k)+1}^{2n-(k+1)} \mathbb{Z}/4\mathbb{Z}\right)$$

as follows: We send $\overline{\langle 1 \rangle} \mapsto \langle 1 \rangle$, for $2 \leq i \leq k$, we send $\overline{\langle \beta_i \rangle} \mapsto \langle \gamma_{2(n-k)-1+i} \rangle$, and for $i \geq k+1$, we send $\overline{\langle \beta_i \rangle} \mapsto \langle \gamma_{i-(k-1)}\gamma_{i+n-2k} \rangle$. By noting that for $i \neq j$, we have $\langle 1, -\beta_i \rangle \perp \langle 1, -\beta_j \rangle = \langle 1, -\beta_i\beta_j \rangle$ (similarly for the corresponding γ's in the codomain), it is readily checked that this map is a ring homomorphism, and that the image of r is

$\mathbb{Z} \cdot \langle 1 \rangle \oplus \mathbb{Z} \cdot \langle 1, \gamma_2\gamma_{n-k+1} \rangle \oplus \cdots \oplus \mathbb{Z} \cdot \langle 1, \gamma_{n-k}\gamma_{2(n-k)-1} \rangle$

$\oplus (\mathbb{Z}/2\mathbb{Z}) \cdot \langle 1, -\gamma_{2(n-k)+1} \oplus \cdots \oplus (\mathbb{Z}/2\mathbb{Z}) \cdot \langle 1, -\gamma_{2n-(k+1)} \rangle$.

Let us now construct

$$s : \left(\coprod_{i=1}^{2(n-k)} \mathbb{Z}\right) \coprod \left(\coprod_{i=2(n-k)+1}^{2n-(k+1)} \mathbb{Z}/4\mathbb{Z}\right) \to ann(\langle 1, -\beta_1 \cdots \beta_k \rangle)$$

as follows: We send $\langle 1 \rangle \mapsto 0$, $\langle 1, \gamma_i\gamma_{i+n-k-1} \rangle \mapsto 0$ for $2 \leq j \leq n-k$, and $\langle 1, -\gamma_k \rangle \mapsto \langle 1, -\beta_{j-(n-2k)} \rangle$ for $j \geq n-k+1$.

By our construction, it is easy to see that

$$0 \to R/R \cdot \langle 1, -\beta_1 \cdots \beta_k \rangle \xrightarrow{r} \left(\coprod_{i=1}^{2(n-k)} \mathbb{Z}\right) \coprod \left(\coprod_{i=2(n-k)+1}^{2n-(k+1)} \mathbb{Z}/4\mathbb{Z}\right)$$
$$\xrightarrow{s} ann(\langle 1, -\beta_1 \cdots \beta_k \rangle) \to 0$$

is exact. Here, the corresponding lift is give by $l : \langle 1, -\beta_j \rangle \mapsto \langle 1, -\gamma_{j+(n-2k)} \rangle$.

What is left is to show that the module actions is respected. That is, we need to show

that $r(\overline{\langle\beta_i\rangle}) \otimes l(\langle 1, -\beta_j\rangle) = l(\langle\beta_i\rangle \otimes \langle 1, -\beta_j\rangle)$, for all i, j.

Let us first consider the case when $i \leq k$. Since $j \geq k+1$, we see $i \neq j$. In this case, we see that

$$\begin{aligned} r(\overline{\langle\beta_i\rangle}) \otimes l(\langle 1, -\beta_j\rangle) &= \langle 1, -\gamma_{j+n-2k}\rangle \otimes \langle \gamma_{2(n-k)+1+i}\rangle \\ &= \langle \gamma_{2(n-k)+1+i}, -\gamma_{2(n-k)+1+i}\gamma_{j+n-2k}\rangle \\ &= \langle 1, -\gamma_{j+n-2k}\rangle. \end{aligned}$$

$$\begin{aligned} l(\langle 1, -\beta_j\rangle \otimes \langle\beta_i\rangle) &= l(\langle\beta_i, -\beta_i\beta_j\rangle) \\ &= l(\langle 1, -\beta_j\rangle \\ &= \langle 1, -\gamma_{j+n-2k}\rangle \end{aligned}$$

so indeed, when $i \leq k$, we have $r(\overline{\langle\beta_i\rangle}) \otimes l(\langle 1, -\beta_j\rangle) = l(\langle\beta_i\rangle \otimes \langle 1, -\beta_j\rangle)$.

Now, we consider the case when $i \geq k+1$, and $i \neq j$. In this case, we see that

$$\begin{aligned} r(\overline{\langle\beta_i\rangle}) \otimes l(\langle 1, -\beta_j\rangle) &= \langle 1, -\gamma_{j+n-2k}\rangle \otimes \langle \gamma_{i-(k-1)}\gamma_{i+n-2k}\rangle \\ &= \langle \gamma_{i-(k-1)}\gamma_{i+n-2k}, -\gamma_{j+n-2k}\gamma_{i-(k-1)}\gamma_{i+n-2k}\rangle \\ &= \langle 1, -\gamma_{j+n-2k}\rangle \end{aligned}$$

$$\begin{aligned} l(\langle 1, -\beta_j\rangle \otimes \langle\beta_i\rangle) &= l(\langle\beta_i, -\beta_i\beta_j\rangle) \\ &= l(\langle 1, -\beta_j\rangle \\ &= \langle 1, -\gamma_{j+n-2k}\rangle \end{aligned}$$

so indeed, when $i \geq k+1$ and $i \neq j$, we have $r(\overline{\langle\beta_i\rangle}) \otimes l(\langle 1, -\beta_j\rangle) = l(\langle\beta_i\rangle \otimes \langle 1, -\beta_j\rangle)$.

Now, it is left to show that $r(\overline{\langle\beta_j\rangle}) \otimes l(\langle 1, -\beta_j\rangle) = l(\langle\beta_j\rangle \otimes \langle 1, -\beta_j\rangle)$.

Here, we see that

$$\begin{aligned} r(\overline{\langle\beta_j\rangle}) \otimes l(\langle 1, -\beta_j\rangle) &= \langle 1, -\gamma_{j+n-2k}\rangle \otimes \langle \gamma_{j-(k-1)}\gamma_{j+n-2k}\rangle \\ &= \langle \gamma_{j-(k-1)}\gamma_{j+n-2k}, -\gamma_{j-(k-1)}\rangle \\ &= -\langle 1, -\gamma_{j+n-2k}\rangle \end{aligned}$$

$$\begin{aligned} l(\langle 1, -\beta_j\rangle \otimes \langle\beta_j\rangle) &= l(\langle\beta_j, -1\rangle) \\ &= -l(\langle 1, -\beta_i\rangle) \\ &= -\langle 1, -\gamma_{j+n-2k}\rangle \end{aligned}$$

This indeed shows that $r(\overline{\langle\beta_i\rangle}) \otimes l(\langle 1, -\beta_j\rangle) = l(\langle\beta_i\rangle \otimes \langle 1, -\beta_j\rangle)$, for all i, j, so our module action is respected. ■

5.5 Taking the square root of $\beta_1 \cdots \beta_n (= -1)$

In this section, we finally consider the case when we take the square root of $\beta_1 \cdots \beta_n$, which is -1.

Theorem 5.5.1. *Given $R = \coprod_{i=1}^{n} \mathbb{Z}$, we have*

$$R[\sqrt{-1}] = \coprod_{i=1}^{n-1} \mathbb{Z}/2\mathbb{Z}[\Delta_1]$$

Proof. First, we note that $ann(\langle 1, -\beta_1 \cdots \beta_n \rangle) = ann(\langle 1, 1 \rangle) = 0$. To see this, we note that $D(\langle 1, 1 \rangle) = (1, 1, \cdots, 1)$, which means $ann(\langle 1, 1 \rangle)$ is generated by $\langle 1, -1 \rangle$, the hyperbolic form. This tells us that $R[\sqrt{-1}] \cong R/R \cdot \langle 1, 1 \rangle$.

So, let us look at $R/R \cdot \langle 1, 1 \rangle$. First, we see that in this ring, $\langle 1 \rangle = -\langle 1 \rangle$. From this, we see that $R/R \cdot \langle 1, 1 \rangle = (\mathbb{Z}/2\mathbb{Z}) \cdot \overline{\langle 1 \rangle} \oplus (\mathbb{Z}/2\mathbb{Z}) \cdot \overline{\langle 1, -\beta_1 \rangle} \oplus \cdots \oplus (\mathbb{Z}/2\mathbb{Z}) \cdot \overline{\langle 1, -\beta_{n-1} \rangle}$. We claim that this ring is isomorphic to $\coprod_{i=1}^{n-1} \mathbb{Z}/2\mathbb{Z}[\Delta_1]$.

Looking at $\coprod_{i=1}^{n-1} \mathbb{Z}/2\mathbb{Z}[\Delta_1]$, we note the elements have entries that are entirely 0 and $1 + \Delta$ or 1 and Δ. Denote γ_i as the element with 1's everywhere except for Δ on the ith spot. We note that we can write

$$\coprod_{i=1}^{n-1} \mathbb{Z}/2\mathbb{Z}[\Delta_1] \cong (\mathbb{Z}/2\mathbb{Z}) \cdot \langle 1 \rangle \oplus (\mathbb{Z}/2\mathbb{Z}) \cdot \langle 1, -\gamma_1 \rangle \oplus \cdots \oplus (\mathbb{Z}/2\mathbb{Z}) \cdot \langle 1, -\gamma_{n-1} \rangle.$$

So we define an isomorphism $\phi : R/R \cdot \langle 1, 1 \rangle \to \coprod_{i=1}^{n-1} \mathbb{Z}/2\mathbb{Z}[\Delta_1]$ where $\overline{\langle 1 \rangle} \mapsto \langle 1 \rangle$, and $\overline{\langle 1, -\beta_i \rangle} \mapsto \langle 1, -\gamma_i \rangle$. It is clear to see that this extends to a bijection preserving addition. It is also easy to see that this is multiplication is preserved, in that $\overline{\langle 1, -\beta_i \rangle} \otimes \overline{\langle 1, -\beta_j \rangle} = 0$ for $i \neq j$, and similarly, $\langle 1, -\gamma_i \rangle \otimes \langle 1, -\gamma_j \rangle = 0$ for $i \neq j$. Thus, we see that here, $R[\sqrt{-1}] = \coprod_{i=1}^{n-1} \mathbb{Z}/2\mathbb{Z}[\Delta_1]$.

■

5.6 One Ring (Isomorphism) to Rule Them All!

In this section, we refer to the following theorem from Marshall's text to unify the work we have above.

Theorem 5.6.1. *If R is an abstract Witt ring away from characteristic 2, then*

$$R \coprod \mathbb{Z}/4\mathbb{Z} \cong R \coprod \mathbb{Z}[\Delta_1].$$

This ring isomorphism gives us the following unifying corollary:

Corollary 5.6.1. *Let $R = \coprod_{i=1}^{n} \mathbb{Z}$, where $n \geq 2$. For $k \leq n$, we have*

$$R[\sqrt{\beta_1\beta_2\cdots\beta_{k-1}\beta_k}] \cong \left(\coprod_{i=1}^{2(n-k)} \mathbb{Z} \right) \coprod \left(\coprod_{i=2(n-k)+1}^{2n-(k+1)} \mathbb{Z}/2\mathbb{Z}[\Delta_1] \right).$$

Chapter 6

Rings of the form $R_1 \coprod R_2$

Given abstract Witt rings R_1 and R_2, with corresponding quadratic extensions $R_1[\sqrt{\alpha_1}]$ and $R_2[\sqrt{\alpha_2}]$, we show that

$$(R_1 \coprod R_2)[\sqrt{(\alpha_1, \alpha_2)}] = R_1[\sqrt{\alpha_1}] \coprod R_2[\sqrt{\alpha_2}] \coprod \hat{R}$$

, where either $\hat{R} = \mathbb{Z}/2\mathbb{Z}[\Delta_1]$, with Δ_1 generated by Δ, or $\hat{R} = \mathbb{Z}/4\mathbb{Z}$.

6.1 The general case of $R_1 = \coprod_{i=1}^{n_1} \mathbb{Z}$ and $R_2 = \coprod_{j=1}^{n_2} \mathbb{Z}$

We first show this to be true for the case where R_1 and R_2 are fiber products of $\mathbb{Z}$.

Theorem 6.1.1. *Let $R_1 = \coprod_{i=1}^{n_1} \mathbb{Z}$ and $R_2 = \coprod_{j=1}^{n_2} \mathbb{Z}$, where $\beta_{k_1} \in R_1$ and $\beta_{k_2} \in R_2$. Then*

$$R_1 \coprod R_2[\sqrt{(\beta_{k_1}, \beta_{k_2})}] \cong R_1[\sqrt{\beta_{k_1}}] \coprod R_2[\sqrt{\beta_{k_2}}] \coprod \mathbb{Z}/2\mathbb{Z}[\Delta_1].$$

Proof. Given $\beta_{k_1} \in R_1$ and $\beta_{k_2} \in R_2$, we have shown that the

$$R_1[\sqrt{\beta_{k_1}}] \cong \left(\coprod_{i=1}^{2(n_1-k_1)} \mathbb{Z} \right) \coprod \left(\coprod_{i=2(n_1-k_1)+1}^{2n_1-(k_1+1)} \mathbb{Z}/2\mathbb{Z}[\Delta_1] \right)$$

and

$$R_2[\sqrt{\beta_{k_2}}] \cong \left(\coprod_{i=1}^{2(n_2-k_2)} \mathbb{Z} \right) \coprod \left(\coprod_{i=2(n_2-k_2)+1}^{2n_2-(k_2+1)} \mathbb{Z}/2\mathbb{Z}[\Delta_1] \right).$$

Now, we note that $R_1 \coprod R_2 = \coprod_{i=1}^{n_1+n_2} \mathbb{Z}$, and taking the square root of $(\beta_{k_1}, \beta_{k_2})$ will result in a ring isomorphic to what would be obtained by taking the square root of $\beta_{k_1+k_2}$. So here, we see that

$$\begin{aligned}
&(R_1 \coprod R_2)[\sqrt{(\beta_{k_1}, \beta_{k_2})}] \\
&\cong \left(\coprod_{i=1}^{2(n_1+n_2-k_1-k_2)} \mathbb{Z} \right) \coprod \left(\coprod_{i=2(n_1+n_2-k_1-k_2)+1}^{2n_1+n_2-(k_1+k_2+1)} \mathbb{Z}/2\mathbb{Z}[\Delta_1] \right)
\end{aligned}$$

Here, it can be readily checked that

$$(R_1 \coprod R_2)[\sqrt{(\alpha_1, \alpha_2)}] = R_1[\sqrt{\alpha_1}] \coprod R_2[\sqrt{\alpha_2}] \coprod \mathbb{Z}/2\mathbb{Z}[\Delta_1].$$

■

6.2 The case of $\mathbb{Z}[\Delta_2] \coprod \mathbb{Z}[\Delta_2]$

We begin by exploring the basic case of when both $R_1 = R_2 = \mathbb{Z}[\Delta_2]$. This will give us intuition when neither R_1 or R_2 are fiber products of $\mathbb{Z}$. We recall that $\mathbb{Z}[\Delta_1] \cong \mathbb{Z} \coprod \mathbb{Z}$, which is why we adjoin Δ_2.

We recall that from Corollary 3.3.1 that $\mathbb{Z}[\Delta_2][\sqrt{\delta_1}] \cong \mathbb{Z}[\Delta_2]$.

Theorem 6.2.1. *Let $R = \mathbb{Z}[\Delta_2] \coprod \mathbb{Z}[\Delta_2]$, where Δ_2 is the Klein-4 group (generated by δ_1 and δ_2). Then*

$$R[\sqrt{[\delta_1, \delta_1]}] \cong R[\sqrt{\delta_1}] \coprod R[\sqrt{\delta_1}] \coprod \mathbb{Z}/2\mathbb{Z}[\Delta_1].$$

Proof. First, we note that R has, as a $\mathbb{Z}$-basis, $\{[1,1] = 1, [1,-1] = \beta, [\delta_1, 1] = \delta_1, [\delta_2, 1] = \delta_2, [\delta_1\delta_2, 1] = \delta_1\delta_2, [1, \delta_1] = \delta_1', [1, \delta_2] = \delta_2', [1, \delta_1\delta_2] = \delta_1'\delta_2'\}$.

Let us now examine $R/R \cdot \langle 1, -\beta_1\beta_1' \rangle$. We notice that in this quotient, we have

$\overline{\langle 1\rangle} = \overline{\langle \beta_1\beta_1'\rangle}$, which tells us that $\overline{\langle \beta_\rangle} = \overline{\langle \beta_1'\rangle}$. Furthermore, we notice that $\overline{\langle \beta_1\beta_2\rangle} = \overline{[\beta_1\beta_2, 1]} = \overline{[\beta_2, \beta_1]} = \overline{[\beta_2, 1]} + \overline{[1, \beta_1]} - \overline{[1, 1]} = \overline{\langle \beta_2, \beta_1', -1\rangle}$. We can similarly show that $\overline{\langle \delta_1'\delta_2'\rangle} = \overline{\langle \delta_1, \delta_2', -1\rangle}$. Furthermore, we note that

$$\begin{aligned}
\overline{\langle \delta_1\rangle} + \overline{\langle \delta_1\rangle} - \overline{\langle 1\rangle} &= \overline{[\delta_1, 1]} + \overline{[\delta_1, 1]} - \overline{[1, 1]} \\
&= \overline{[\delta_1, 1]} + \overline{[1, \delta_1]} - \overline{[1, 1]} \\
&= \overline{[\delta_1, \delta_1]} \\
&= \overline{[1, 1]} \\
&= \overline{\langle 1\rangle}
\end{aligned}$$

which tells us that $\overline{\langle 1, -\delta_1\rangle}$ has 2-torsion in our quotient.

From all of this, we may write

$$R/R \cdot \langle 1, -\delta_1\delta_1\rangle = \mathbb{Z} \cdot \overline{\langle 1\rangle} \oplus \mathbb{Z} \cdot \overline{\langle 1, -\beta\rangle} \oplus \mathbb{Z} \cdot \overline{\langle 1, -\delta_2\rangle} \oplus \mathbb{Z} \cdot \overline{\langle 1, -\delta_2'\rangle} \oplus (\mathbb{Z}/2\mathbb{Z}) \cdot \overline{\langle 1, -\beta_1\rangle}.$$

Let us now examine $ann(\langle 1, -\delta_1\delta_1'\rangle)$. So, we first look at $D(\langle 1, -\delta_1\delta_1'\rangle)$. We notice that

$$D(\langle 1, -\delta_1\delta_1'\rangle) = D(\langle 1, [-\delta_1, \delta_1]\rangle) = \{[-\delta_1, 1], [1, -\delta_1], [1, 1], [-\delta_1, -\delta_1]\},$$

which tells us that $ann(\langle 1, -\delta_1\delta_1'\rangle)$ is generated by $(1, -1)$ (which is hyperbolic),
$\langle 1, -[-\delta_1, 1]\rangle = \langle 1, \beta\delta_1\rangle$, $\langle 1, -[1, -\delta_1]\rangle = \langle 1, -\beta\delta_1'\rangle$, and
$\langle 1, -[-\delta_1, -\delta_1]\rangle = \langle 1, \delta_1\delta_1'\rangle$. We note that $\langle 1, \beta\delta_1\rangle \perp \langle 1, -\beta\delta_1'\rangle = [1 + \delta_1, 0] + [0, 1 + \delta_1] = [1 + \delta_1, 1 + \delta_1] = \langle 1, \delta_1\delta_1'\rangle$, which tells us that as an ideal, $ann(\langle 1, -\delta_1\delta_1'\rangle) = (\langle 1, \beta\delta_1\rangle, \langle 1, -\beta\delta_1'\rangle)$.

It can be readily checked that

$$ann(\langle 1, -\delta_1\delta_1'\rangle = \mathbb{Z} \cdot \langle 1, \beta\delta_1\rangle \oplus \mathbb{Z} \cdot \langle \delta_2, \beta\delta_1\delta_2\rangle \oplus \mathbb{Z} \cdot \langle 1, -\beta\delta_1'\rangle \oplus \mathbb{Z} \cdot \langle \delta_2', -\beta\delta_1'\delta_2'\rangle.$$

Furthermore, we note that $\delta_1', \delta_2', \beta, \delta_1$ fixes $\langle 1, \beta\delta_1\rangle$ and $\langle \delta_2, \beta\delta_1\delta_2\rangle$, while δ_2 swaps them. Similarly, $\delta_1, \delta_2, -\beta, \delta_1'$ fixes $\langle 1, -\beta\delta_1'\rangle$ and $\langle \delta_2', -\beta\delta_1'\delta_2'\rangle$, while δ_2' swaps them.

We note that $\mathbb{Z}[\Delta_2][\sqrt{\beta_1}] \cong \mathbb{Z}[\Delta_2]$, in which case, our quadratic extension should be

$R' = \mathbb{Z}[\Delta_2] \coprod \mathbb{Z}[\Delta_2] \coprod \mathbb{Z}/2\mathbb{Z}[\Delta_1]$. Here, we denote γ_1, γ_2 as the generators for each $\mathbb{Z}[\Delta_2]$. R' can be additively generated by $1 = [1,1,1]$, $\beta = [1,-1,1]$, $\epsilon = [1,1,\Delta]$, $\gamma_1 = [\gamma_1,1,1]$, $\gamma_2 = [\gamma_2,1,1]$, $\gamma_1\gamma_2 = [\gamma_1\gamma_2,1,1]$, $\gamma_1' = [1,\gamma_1,1]$, $\gamma_2' = [1,\gamma_2,1]$, and $\gamma_1'\gamma_2' = [1,\gamma_1\gamma_2,1]$ as a basis over $\mathbb{Z}$. Indeed, it can be readily checked that

$$R' = \mathbb{Z}\cdot\langle 1\rangle \oplus \mathbb{Z}\cdot\langle 1,-\beta\rangle \oplus \mathbb{Z}\cdot\langle 1,-\gamma_2\rangle \oplus \mathbb{Z}\cdot\langle 1,-\gamma_2'\rangle \oplus (\mathbb{Z}/2\mathbb{Z})\cdot\langle 1,-\epsilon\rangle$$
$$\oplus \mathbb{Z}\dot{\langle} 1,\beta\gamma_1\rangle \oplus \mathbb{Z}\cdot\langle 1,-\beta\gamma_1'\rangle \oplus \mathbb{Z}\cdot\langle \gamma_2,\beta\gamma_1\gamma_2\rangle \oplus \mathbb{Z}\cdot\langle \gamma_2',-\beta\gamma_1'\gamma_2'\rangle.$$

Let us now construct $r : R/R\cdot\langle 1,-\delta_1\delta_1'\rangle \to R'$ as follows: $\overline{\langle 1\rangle} \mapsto \langle 1\rangle$, $\overline{\langle\beta\rangle} \mapsto \langle\beta\rangle$, $\overline{\langle\delta_2\rangle} \mapsto \langle\gamma_2\rangle$, $\overline{\langle\delta_2'\rangle} \mapsto \langle\gamma_2'\rangle$, $\overline{\langle\delta_1\rangle} \mapsto \langle\epsilon\rangle$. It is readily checked that this map is injective, multiplication is preserved (thus, it is a ring homomorphism), and that furthermore, the image is

$$\mathbb{Z}\cdot\langle 1\rangle \oplus \mathbb{Z}\cdot\langle 1,-\beta\rangle \oplus \mathbb{Z}\cdot\langle 1,-\gamma_2\rangle \oplus \mathbb{Z}\cdot\langle 1,-\gamma_2'\rangle \oplus (\mathbb{Z}/2\mathbb{Z})\cdot\langle 1,-\epsilon\rangle.$$

We now construct $s : R' \to ann(\langle 1,-\delta_1\delta_1'\rangle$ as follows: $\langle 1,\beta\gamma_1\rangle \mapsto \langle 1,\beta\delta_1\rangle$, $\langle 1,-\beta\gamma_1'\rangle \mapsto \langle 1,-\beta\delta_1'\rangle$, $\langle \gamma_2,\beta\gamma_1\gamma_2\rangle \mapsto \langle\delta_2,\beta\delta_1\delta_2\rangle$, $\langle\gamma_2',-\beta\gamma_1'\gamma_2'\rangle \mapsto \langle\delta_2',-\beta\delta_1'\delta_2'\rangle$,
while $\langle 1\rangle, \langle 1,-\beta\rangle, \langle 1,-\gamma_2\rangle, \langle 1,-\gamma_2'\rangle, \langle 1,-\epsilon\rangle$ all go to 0. It is clear that this map is onto.

Thus, by construction, we see that

$$0 \to R/R\cdot\langle 1,-\delta_1\delta_1'\rangle \to R' \to ann(\langle 1,-\delta_1\delta_1'\rangle) \to 0$$

is exact. Here, the corresponding lift is $l : ann(\langle 1,-\delta_1\delta_1'\rangle) \to R'$ is given by $\langle 1,\beta\delta_1\rangle \mapsto \langle 1,\beta\gamma_1\rangle$, $\langle 1,-\beta\delta_1'\rangle \mapsto \langle 1,-\beta\gamma_1'\rangle$, $\langle\delta_2,\beta\delta_1\delta_2\rangle \mapsto \langle\gamma_2,\beta\gamma_1\gamma_2\rangle$, $\langle\delta_2',-\beta\delta_1'\delta_2'\rangle \mapsto \langle\gamma_2',-\beta\gamma_1'\gamma_2'\rangle$. What is left is to show that the module action is preserved.

First, we show $l(\langle\delta_1\rangle \otimes \langle 1,\beta\delta_1\rangle) = r(\overline{\langle\delta_1\rangle}) \otimes l(\langle 1,\beta\delta_1\rangle)$. To see this, we note that

$$\begin{aligned} l(\langle\delta_1\rangle \otimes \langle 1,\beta\delta_1\rangle) &= l(\langle 1,\beta\delta_1\rangle) \\ &= \langle 1,\beta\gamma_1\rangle \end{aligned}$$

$$\begin{aligned} r(\overline{\langle\delta_1\rangle}) \otimes l(\langle 1,\beta\delta_1\rangle) &= \langle\epsilon\rangle \otimes \langle 1,\beta\gamma_1\rangle \\ &= \langle 1,\beta\gamma_1\rangle \end{aligned}$$

so indeed, equality is shown.

We now show $l(\langle\delta_2\rangle \otimes \langle 1, \beta\delta_1\rangle) = r(\overline{\langle\delta_2\rangle}) \otimes l(\langle 1, \beta\delta_1\rangle)$. To see this, we note that

$$\begin{aligned} l(\langle\delta_2\rangle \otimes \langle 1, \beta\delta_1\rangle) &= l(\langle\delta_2, \beta\delta_1\delta_2\rangle) \\ &= \langle\gamma_2, \beta\gamma_1\gamma_2\rangle \end{aligned}$$

$$\begin{aligned} r(\overline{\langle\delta_2\rangle}) \otimes l(\langle 1, \beta\delta_1\rangle) &= \langle\gamma_2\rangle \otimes \langle 1, \beta\gamma_1\rangle \\ &= \langle\gamma_2, \beta\gamma_1\gamma_2\rangle \end{aligned}$$

so indeed, equality is shown.

Let us finally show $l(\langle\beta\rangle \otimes \langle 1, \beta\delta_1\rangle) = r(\overline{\langle\delta_1\rangle}) \otimes l(\langle 1, \beta\delta_1\rangle)$. To see this, we note that

$$\begin{aligned} l(\langle\beta\rangle \otimes \langle 1, \beta\delta_1\rangle) &= l(\langle 1, \beta\delta_1\rangle) \\ &= \langle 1, \beta\gamma_1\rangle \end{aligned}$$

$$\begin{aligned} r(\overline{\langle\delta_1\rangle}) \otimes l(\langle 1, \beta\delta_1\rangle) &= \langle\beta\rangle \otimes \langle 1, \beta\gamma_1\rangle \\ &= \langle 1, \beta\gamma_1\rangle \end{aligned}$$

so indeed, equality is shown.

Thus, we see the action on $\langle 1, \beta\gamma_1\rangle$ is preserved. We can similarly show that the action $\langle 1, -\beta\gamma_1'\rangle$, $\langle\gamma_2, \beta\gamma_1\gamma_2\rangle$, and $\langle\gamma_2', -\beta\gamma_1'\gamma_2'\rangle$ are preserved. ■

6.3 The general case of $\mathbb{Z}[\Delta_n] \coprod \mathbb{Z}[\Delta_m]$, where $n, m > 1$

Let us now consider when $R_1 = \mathbb{Z}[\Delta_n]$ and $R_2 = \mathbb{Z}[\Delta_m]$, where $n, m > 1$, and Δ_k is the torsion-2 group with k generators. Indeed, we can focus on when $n, m > 1$ as $\mathbb{Z}[\Delta_1] \cong \mathbb{Z} \coprod \mathbb{Z}$. Let $\delta_1, \cdots, \delta_n$ generate Δ_n and $\delta_1', \cdots, \delta_m$' generate Δ_m. Let $R = R_1 \coprod R_2$.

We recall again that by Corollary 3.3.1, we have $R_1[\sqrt{\delta_1}] \cong R_1$ and $R_2[\sqrt{\delta_1'}] \cong R_2$.

Theorem 6.3.1. *Let $R_1 = \mathbb{Z}[\Delta_n]$ and $R_2 = \mathbb{Z}[\Delta_m]$, where $n, m > 1$, and Δ_k is as above. Let $R = R_1 \coprod R_2$. Then*

$$R[\sqrt{(\beta_1, \beta_1')}] \cong R_1[\sqrt{\beta_1}] \coprod R_2[\sqrt{\beta_1'}] \coprod \mathbb{Z}/2\mathbb{Z}[\Delta_1].$$

Proof. We note that R can be expressed with a $\mathbb{Z}$-basis $\{1 = [1,1], \beta = [1,-1], \delta_{i_1} \cdots \delta_{i_j} = [\delta_{i_1} \cdots \delta_{i_j}, 1]$ for $1 \leq i_1 < \cdots < \imath_j \leq n$, and $\delta'_{i_1} \cdots \delta'_{i_k} = [1, \delta'_{i_1} \cdots \delta'_{i_k}]$ for $1 \leq i_1 < \cdots < i_k \leq m\}$. Thus, we see that R has rank $2^n + 2^m$, and can be represented as

$$R = \mathbb{Z} \cdot \langle 1 \rangle \oplus \mathbb{Z} \cdot \langle 1, -\beta \rangle \oplus \bigoplus_{1 \leq i_1 < \cdots < i_j \leq n} \mathbb{Z} \cdot \langle 1, -\delta_{i_1} \cdots \delta_{i_j} \rangle$$
$$\oplus \bigoplus_{1 \leq i_1 < \cdots < i_k \leq m} \mathbb{Z} \cdot \langle 1, -\delta'_{i_1} \cdots \delta'_{i_k} \rangle.$$

Let us now look at taking the square root of (δ_1, δ'_1). So, let us examine $R/R \cdot \langle 1, -\delta_1 \delta'_1 \rangle$. As before, we have $\overline{\langle \delta_1 \delta'_1 \rangle} = \overline{\langle 1 \rangle}$ in our quotient, and so, $\overline{\langle \delta_1 \rangle} = \overline{\langle \delta'_1 \rangle}$. As before, we can also show that $\overline{\langle 1, -\delta_1 \rangle}$ has 2-torsion, and that given $1 < i_1 < \cdots < i_j \leq n$, we have $\overline{\langle \delta_1 \delta_{i_1} \cdots \delta_{i_j} \rangle} = \overline{[\delta_1 \delta_{i_1} \cdots \delta_{i_j}, 1]} = \overline{[\delta_{i_1} \cdots \delta_{i_j}, \delta'_1]} = \langle \delta_{i_1} \cdots \delta_{i_j} \rangle \perp \langle \delta'_1 \rangle - \langle 1 \rangle$, which means $\overline{\langle \delta_1 \delta_{i_1} \cdots \delta_{i_j} \rangle}$ can be represented as a linear combination of the other generators. The same can be said about $\overline{\langle \delta'_1 \delta'_{i_1} \cdots \delta'_{i_j} \rangle}$, in which case, we can write

$$R/R \cdot \langle 1, -\delta_1 \delta'_1 \rangle = \mathbb{Z} \cdot \overline{\langle 1 \rangle} \oplus \mathbb{Z} \cdot \overline{\langle 1, -\beta \rangle} \oplus \bigoplus_{1 < i_1 < \cdots < i_j \leq n} \mathbb{Z} \cdot \overline{\langle 1, -\delta_{i_1} \cdots \delta_{i_j} \rangle}$$
$$\oplus \bigoplus_{1 < i_1 < \cdots < i_k \leq m} \mathbb{Z} \cdot \overline{\langle 1, -\delta'_{i_1} \cdots \delta'_{i_k} \rangle} \oplus (\mathbb{Z}/2\mathbb{Z}) \cdot \overline{\langle 1, -\delta_1 \rangle}.$$

Let us now examine $ann(\langle 1, -\delta_1 \delta'_1 \rangle)$. As before, we can show $ann(\langle 1, -\delta_1 \delta'_1 \rangle) = (\langle 1, \beta \delta_1 \rangle, \langle 1, -\beta \delta'_1 \rangle)$. In fact, we can also write

$$ann(\langle 1, -\delta_1 \delta'_1 \rangle) = \mathbb{Z} \cdot \langle 1, \beta \delta_1 \rangle \oplus \bigoplus_{1 < i_1 < \cdots < i_j \leq n} \langle \delta_{i_1} \cdots \delta_{i_j}, \beta \delta_1 \delta_{i_1} \cdots \delta_{i_j} \rangle$$
$$\oplus \mathbb{Z} \cdot \langle 1, -\beta \delta'_1 \rangle \oplus \bigoplus_{1 < i_1 < \cdots < i_k \leq m} \langle \delta'_{i_1} \cdots \delta'_{i_j}, -\beta \delta'_1 \delta_{i_1} \cdots \delta'_{i_k} \rangle.$$

As $\mathbb{Z}[\Delta_k][\sqrt{\beta_1}] \cong \mathbb{Z}[\Delta_k]$, our quadratic extension should be $\mathbb{Z}[\Delta_n] \coprod \mathbb{Z}[\Delta_m] \coprod \mathbb{Z}/2\mathbb{Z}[\Delta_1]$. Again, we will use γ_i and γ'_i instead of δ_i and δ'_i to denote our generators for Δ_n and Δ_m R' can be additively generated by $1 = [1,1,1]$, $\beta = [1,-1,1]$, $\epsilon = [1,1,\Delta]$, $\gamma_{i_1} \cdots \gamma_{i_j} = [\gamma_{i_1} \cdots \gamma_{i_j}, 1, 1]$ for $1 \leq i_1 < \cdots < i_j \leq n$, and $\gamma'_{i_1} \cdots \gamma'_{i_k} = [1, \gamma'_{i_1} \cdots \gamma'_{i_k}, 1]$ for $1 \leq i_1 < \cdots < i_k \leq m$. In fact, we can write

$$
\begin{aligned}
R' = {} & \mathbb{Z}\cdot\langle 1\rangle \oplus \mathbb{Z}\cdot\langle 1,-\beta\rangle \\
& \oplus \bigoplus_{1<i_1<\cdots<i_j\le n} \mathbb{Z}\cdot\langle 1,-\gamma_{i_1}\cdots\gamma_{i_j}\rangle \oplus \bigoplus_{1<i_1<\cdots<i_k\le m} \mathbb{Z}\cdot\langle 1,-\gamma'_{i_1}\cdots\gamma'_{i_k}\rangle \\
& \oplus \mathbb{Z}\cdot\langle 1,\beta\gamma_1\rangle \oplus \bigoplus_{1<i_1<\cdots<i_j\le n} \langle \gamma_{i_1}\cdots\gamma_{i_j}, \beta\gamma_1\gamma_{i_1}\cdots\gamma_{i_j}\rangle \\
& \oplus \mathbb{Z}\cdot\langle 1,-\beta\gamma'_1\rangle \oplus \bigoplus_{1<i_1<\cdots<i_k\le m} \langle \gamma'_{i_1}\cdots\gamma'_{i_j}, -\beta\gamma'_1\gamma_{i_1}\cdots\gamma'_{i_k}\rangle \\
& \oplus (\mathbb{Z}/2\mathbb{Z})\cdot\langle 1,-\epsilon\rangle.
\end{aligned}
$$

We now construct $r : R/R\cdot\langle 1,-\delta_1\delta'_1\rangle \to R'$ as follows:

- $\overline{\langle 1\rangle} \mapsto \langle 1\rangle$
- $\overline{\langle 1,-\beta\rangle} \mapsto \langle 1,-\beta\rangle$
- $\overline{\langle 1,-\delta_{i_1}\cdots\delta_{i_j}\rangle} \mapsto \langle 1,-\gamma_{i_1}\cdots\gamma_{i_j}\rangle$ for $1<i_1<\cdots<i_j\le n$
- $\overline{\langle 1,-\delta'_{i_1}\cdots\delta'_{i_k}\rangle} \mapsto \langle 1,-\gamma'_{i_1}\cdots\gamma'_{i_k}\rangle$ for $1<i_1<\cdots<i_k\le m$
- and $\overline{\langle 1,-\gamma_1\rangle} \mapsto \langle 1,-\epsilon\rangle$.

It is readily checked that this map is injective, multiplication is preserved, with the image

$$
\begin{aligned}
\mathbb{Z}\cdot\langle 1\rangle \oplus \mathbb{Z}\cdot\langle 1,-\beta\rangle \oplus & \bigoplus_{1<i_1<\cdots<i_j\le n} \mathbb{Z}\cdot\langle 1,-\gamma_{i_1}\cdots\gamma_{i_j}\rangle \\
& \oplus \bigoplus_{1<i_1<\cdots<i_k\le m} \mathbb{Z}\cdot\langle 1,-\gamma'_{i_1}\cdots\gamma'_{i_k}\rangle \oplus (\mathbb{Z}/2\mathbb{Z})\cdot\langle 1,-\epsilon\rangle.
\end{aligned}
$$

We now construct $s : R' \to ann(\langle 1,-\delta_1\delta'_1\rangle)$ defined as follows:

- $\langle 1,\beta\gamma_1\rangle \mapsto \langle 1,\beta\delta_1\rangle$
- $\langle \gamma_{i_1}\cdots\gamma_{i_j}, \beta\gamma_1\gamma_{i_1}\cdots\gamma_{i_j}\rangle \mapsto \langle \delta_{i_1}\cdots\delta_{i_j}, \beta\delta_1\delta_{i_1}\cdots\delta_{i_j}\rangle$ for $1<i_1<\cdots<i_j\le n$
- $\langle 1,-\beta\gamma'_1\rangle \mapsto \langle 1,-\beta\delta'_1\rangle$
- $\langle \gamma'_{i_1}\cdots\gamma'_{i_j}, -\beta\gamma'_1\gamma_{i_1}\cdots\gamma'_{i_k}\rangle \mapsto \langle \delta'_{i_1}\cdots\delta'_{i_j}, -\beta\delta'_1\delta_{i_1}\cdots\delta'_{i_k}\rangle$ for $1<i_1<\cdots<i_k\le m$
- $\langle 1\rangle$, $\langle 1,-\beta\rangle$, $\langle 1,-\gamma_{i_1}\cdots\gamma_{i_j}\rangle \mapsto 0$ for $1<i_1<\cdots<i_j\le n$

- $\langle 1, -\gamma_{i_1} \cdots \gamma_{i_k} \rangle \mapsto 0$ for $1 < i_1 < \cdots < i_k \leq m$

It is clear that this map is onto.

By construction, we see that $0 \to R/R \cdot \langle 1, -\delta_1 \delta_1' \rangle \to R' \to ann(\langle 1, -\delta_1 \delta_1' \rangle) \to 0$ is exact. Here, the corresponding lift is $l : ann(\langle 1, -\delta_1 \delta_1' \rangle) \to R'$ given by $\langle 1, \beta\delta_1 \rangle \mapsto \langle 1, \beta\gamma_1 \rangle$, $\langle \delta_{i_1} \cdots \delta_{i_j}, \beta\delta_1\delta_{i_1} \cdots \delta_{i_j} \rangle \mapsto \langle \gamma_{i_1} \cdots \gamma_{i_j}, \beta\gamma_1\gamma_{i_1} \cdots \gamma_{i_j} \rangle$ for $1 < i_1 < \cdots < i_j \leq n$, $\langle 1, -\beta\delta_1' \rangle \mapsto \langle 1, -\beta\gamma_1' \rangle$, and $\langle \delta_{i_1}' \cdots \delta_{i_j}', -\beta\delta_1'\delta_{i_1} \cdots \delta_{i_k}' \rangle \mapsto \langle \gamma_{i_1}' \cdots \gamma_{i_j}', -\beta\gamma_1'\gamma_{i_1} \cdots \gamma_{i_k}' \rangle$ for $1 < i_1 < \cdots < i_k \leq m$. What is left is to show that the module action is preserved.

First, we show $l(\langle \delta_1 \rangle \otimes \langle 1, \beta\delta_1 \rangle) = r(\overline{\langle \delta_1 \rangle}) \otimes l(\langle 1, \beta\delta_1 \rangle)$. To see this, we note that

$$\begin{aligned} l(\langle \delta_1 \rangle \otimes \langle 1, \beta\delta_1 \rangle) &= l(\langle 1, \beta\delta_1 \rangle) \\ &= \langle 1, \beta\gamma_1 \rangle \end{aligned}$$

$$\begin{aligned} r(\overline{\langle \delta_1 \rangle}) \otimes l(\langle 1, \beta\delta_1 \rangle) &= \langle \epsilon \rangle \otimes \langle 1, \beta\gamma_1 \rangle \\ &= \langle 1, \beta\gamma_1 \rangle \end{aligned}$$

so indeed, equality is shown.

We now show $l(\langle \delta_k \rangle \otimes \langle 1, \beta\delta_1 \rangle) = r(\overline{\langle \delta_k \rangle}) \otimes l(\langle 1, \beta\delta_1 \rangle)$ for $k > 1$. To see this, we note that

$$\begin{aligned} l(\langle \delta_k \rangle \otimes \langle 1, \beta\delta_1 \rangle) &= l(\langle \delta_k, \beta\delta_1\delta_k \rangle) \\ &= \langle \gamma_k, \beta\gamma_1\gamma_k \rangle \end{aligned}$$

$$\begin{aligned} r(\overline{\langle \delta_k \rangle}) \otimes l(\langle 1, \beta\delta_1 \rangle) &= \langle \gamma_k \rangle \otimes \langle 1, \beta\gamma_1 \rangle \\ &= \langle \gamma_k, \beta\gamma_1\gamma_k \rangle \end{aligned}$$

so indeed, equality is shown.

Let us finally show $l(\langle \beta \rangle \otimes \langle 1, \beta\delta_1 \rangle) = r(\overline{\langle \delta_1 \rangle}) \otimes l(\langle 1, \beta\delta_1 \rangle)$. To see this, we note that

$$\begin{aligned} l(\langle \beta \rangle \otimes \langle 1, \beta\delta_1 \rangle) &= l(\langle 1, \beta\delta_1 \rangle) \\ &= \langle 1, \beta\gamma_1 \rangle \end{aligned}$$

$$\begin{aligned} r(\overline{\langle \delta_1 \rangle}) \otimes l(\langle 1, \beta\delta_1 \rangle) &= \langle \beta \rangle \otimes \langle 1, \beta\gamma_1 \rangle \\ &= \langle 1, \beta\gamma_1 \rangle \end{aligned}$$

so indeed, equality is shown.

Thus, we see the action on $\langle 1, \beta\gamma_1\rangle$ is preserved. We can similarly show that module action is preserved for all the other $\mathbb{Z}$-generators of $ann(\langle 1, -\delta_1\delta_1'\rangle)$ as well, so we are done. ■

6.4 The General Case of $R = R_1 \coprod R_2$

We may extend what we have above to a more general setting. Let R_1 and R_2 be abstract Witt rings with square class groups $S(R_1) = \langle \beta_1, \cdots, \beta_n\rangle$ and $S(R_2) = \langle \beta_1', \cdots, \beta_m'\rangle$. Suppose $\tilde{R_1}$ and $\tilde{R_2}$ are quadratic extensions of R_1 (with respect to β_1) and R_2 (with respect to β_1'). We make the additional assumption that we are away from the case of $\beta_1 = -1$ in R_1 and R_2 is characteristic 2 (ie. -1 is a square) and vice versa.

Theorem 6.4.1. *Let R_1 and R_2 be abstract Witt rings, and let $\beta_1 \in S(R_1)$ and $\beta_1' \in S(R_2)$. Assuming the conditions we have above, we have*

$$(R_1 \coprod R_2)[\sqrt{[\beta_1, \beta_1']}] \cong \tilde{R_1} \coprod \tilde{R_2} \coprod \mathbb{Z}/2\mathbb{Z}[\Delta_1].$$

Proof. Per our assumptions, we have the following short exact sequences:

$$0 \to R_1/R_1 \cdot \langle 1, -\beta_1\rangle \xrightarrow{r_1} \tilde{R_1} \xrightarrow{s_1} ann(\langle 1, -\beta_1\rangle) \to 0$$

$$0 \to R_2/R_2 \cdot \langle 1, -\beta_1'\rangle \xrightarrow{r_2} \tilde{R_2} \xrightarrow{s_2} ann(\langle 1, -\beta_1'\rangle) \to 0$$

with the corresponding lifts $l_1 : ann(\langle 1, -\beta_1\rangle) \to R_1$ and $l_2 : ann(\langle 1, -\beta_1'\rangle) \to R_2$. Without loss of generality, we may assume the outputs of l_1 and l_2 are both even dimensional. In fact, we can ensure that on the generators of $ann(\langle 1, -\beta_1\rangle)$, the output of l_1 would be two dimensional (similarly for l_2).

Here, we note that given $R = R_1 \coprod R_2$, we have $S(R) = S(R_1) \times S(R_2)$. So, in R, we denote $\langle \beta_i\rangle = [\beta_i, 1]$ and $\langle \beta_j'\rangle = [1, \beta_j']$. Let us now look at $R/R \cdot \langle 1, -\beta_1\beta_1'\rangle$. Here, we note that $\overline{\langle 1, -\beta_1\beta_1'\rangle} = 0$, which means $\overline{\langle \beta_1\rangle} = \overline{\langle \beta_1'\rangle}$. We notice that $\overline{\langle \beta_1\beta_{i_1}\cdots\beta_{i_k}\rangle} = \overline{(\beta_1\beta_{i_1}\cdots\beta_{i_k}, 1)} = \overline{(\beta_{i_1}\cdots\beta_{i_k}, \beta_1')} = \overline{(\beta_{i_1}\cdots\beta_{i_k}, 1)} + \overline{(1, \beta_1')} - \overline{(1,1)} = \overline{\langle \beta_{i_1}\cdots\beta_{i_k}\rangle} + \overline{\langle \beta_1'\rangle} -$

$\overline{\langle 1\rangle}$. As before, we can show $\overline{\langle 1, -\beta_1\rangle}$ has 2-torsion. From this, we see that $S(R)$ can be generated by $\beta, \beta_1, \cdots, \beta_n, \beta'_1, \cdots, \beta'_m$. So for $R/R \cdot \langle 1, -\beta_1\beta'_1\rangle$, what we have is that $\overline{\langle \beta_1\rangle} = \overline{\langle \beta'_1\rangle}$.

We now look at $R' = \tilde{R_1} \coprod \tilde{R_2} \coprod \mathbb{Z}/2\mathbb{Z}[\Delta_1]$, which is what we want to show to be the quadratic extension of R. We notice that for $S(\tilde{R_1})$ can be generated by $\langle r_1(\beta_2) \cdots, r_1(\beta_n), \gamma_1, \cdots, \gamma_p\rangle$, for $\gamma_i \in S(R_1)$. Similarly, $S(\tilde{R_2})$ can be generated by $\langle r_2(\beta'_2) \cdots, r_2(\beta'_n), \gamma'_1, \cdots, \gamma'_q\rangle$, for $\gamma'_j \in S(R_2)$. In this context, we denote $\langle\epsilon\rangle = [1, 1, \Delta]$, $r_1(\langle\beta_i\rangle) = [r_1(\langle\beta_i\rangle), 1, 1]$, $\langle\gamma_i\rangle = [\gamma_i, 1, 1]$, $r_2(\langle\beta'_j\rangle) = [1, r_2(\langle\beta'_j\rangle), 1]$, and $\langle\gamma'_j\rangle = [1, \gamma'_j, 1]$. So here, as $S(R') = S(\tilde{R_1}) \times S(\tilde{R_2}) \times S(\mathbb{Z}/2\mathbb{Z}[\Delta_1])$, we can generate $S(R')$ with

$$r_1(\beta_2), \cdots, r_1(\beta_n), r_2(\beta'_2), \cdots, r_2(\beta'_m), \gamma_1, \cdots, \gamma_p, \gamma'_1, \cdots, \gamma'_q, \epsilon.$$

Let us now construct $r : R_1 \coprod R_1 \to \tilde{R} \coprod \tilde{R'} \coprod \mathbb{Z}/2\mathbb{Z}[\Delta_1]$ as follows: $\overline{\langle 1\rangle} \mapsto \langle 1\rangle$, $\overline{\langle\beta_i\rangle} \mapsto \langle r_1(\langle\beta_i\rangle)\rangle$ for $1 < i \leq n$, $\overline{\langle\beta'_j\rangle} \mapsto \langle r_2(\langle\beta'_j\rangle)\rangle$ for $1 < i \leq n$, and $\overline{\langle\beta_1\rangle} \mapsto \langle\epsilon\rangle$. However, if $\beta_1 = -1$ in R_1, and $\beta'_j = -1$ in R_2 for some $j > 1$, then we instead send $\overline{\langle\beta'_j\rangle} \mapsto -\langle\epsilon\rangle$ (since in this case, we would have $\overline{\langle\beta'_j\rangle} = [1, -1] = -[-1, 1] = -\overline{\langle\beta_1\rangle}$). Similarly, if $\beta'_1 = -1$ in R_2 and $\beta_k = -1$ in R_1 for $k > 1$, then we instead send $\overline{\langle\beta_k\rangle} \mapsto -\langle\epsilon\rangle$. It can be seen that this is an injection, since r_1 and r_2 are injections (in particular, we note r takes forms such as $\overline{\langle 1, -\beta_j\rangle}$ to $\langle 1, -r_1(\langle\beta_j\rangle)\rangle = [1 - r_1(\langle\beta_j\rangle), 0, 0]$, which nicely corresponds to the two dimensional form $r_1(\overline{\langle 1, -\beta_i\rangle})$ in $\tilde{R_1}$).

To show that r is well defined, we need to consider when any of the β_i or β'_j are -1 in their respective domains, since in this case, we have $[-1, 1] = -[1, -1]$. If $\beta_i = -1$ in R_1 and $\beta'_j = -1$ in R_2 for $i, j > 1$, we need to show that $r(\overline{\langle\beta_i\rangle}) = -r(\overline{\langle\beta'_j\rangle})$ (since $-[1, -1] = [-1, 1]$). Indeed, we see that $r(\overline{\langle\beta_i\rangle}) = [r_1(\langle -1\rangle), 1, 1] = [-1, 1, 1] = -[1, -1, 1] = -[1, r(\overline{\langle\beta'_j\rangle}), 1]$. We note that we are away from the case of $\beta_1 = -1$ and $\beta'_j \neq -1$ in R_2 for all j (similarly if $\beta_i \neq -1$ in R_1 for all i). If $\beta_1 = -1$ in R_1 and $\beta'_j = -1$ in R_2 for $j > 1$, well definition comes for free by construction. If $\beta_1 = \beta'_1 = -1$ in their respective rings, then we see that $r(\overline{\beta_1}) = r(\overline{\beta'_1})$. However, we note that in this

situation, $\tilde{R_1}$, $\tilde{R_2}$, and $\mathbb{Z}/2\mathbb{Z}[\Delta_1]$ all have characteristic 2, and thus, $r(\overline{\beta_1}) = -r(\overline{\beta_1})$, so indeed, we have $r(\overline{\beta_1}) = -r(\overline{\beta_1'})$.

We now inspect $ann(\langle 1, -\beta_1\beta_1'\rangle)$. It easy to see that this is simply $ann(\langle 1, -\beta_1) \oplus ann(\langle 1, -\beta_1')\rangle$, since anything in $ann(\langle 1, -\beta_1)$ and $ann(\langle 1, -\beta_1')$ are even dimensional. Moreover, we see that $ann(\langle 1, -\beta_1\beta_1'\rangle)$ can be generated by the following: $[q, 0]$ where $q \in ann(\langle 1, -\beta_1)\rangle$ is an additive generator, and $[0, q']$ where $q' \in ann(\langle 1, -\beta_1'\rangle)$ is an additive generator.

Now, we construct $s : R' \to ann(\langle 1, -\beta_1\beta_1'\rangle)$, as follows:

- $\langle 1\rangle \mapsto 0$
- $\langle \epsilon\rangle \mapsto 0$
- $\langle r_1(\beta_{i_1} \cdots \beta_{i_k})\rangle \mapsto 0$ for $1 < i_1 < \cdots < i_k \leq n$
- $\langle r_2(\beta'_{i_1} \cdots \beta'_{i_j})\rangle \mapsto 0$ for $1 < i_1 < \cdots < i_j \leq m$
- $\langle 1, -\gamma_{i_1} \cdots \gamma_{i_c}\rangle \mapsto [s_1(\langle 1, -\gamma_{i_1} \cdots \gamma_{i_c}\rangle), 0]$
  (ie. $\langle \gamma_{i_1} \cdots \gamma_{i_c}\rangle \mapsto [s_1(\langle \gamma_{i_1} \cdots \gamma_{i_c}\rangle), 0]$) for $1 \leq i_1 < \cdots < i_c \leq p$
- $\langle 1, -\gamma'_{i_1} \cdots \gamma'_{i_d}\rangle$
  $\mapsto [0, s_2(\langle 1, -\gamma'_{i_1} \cdots \gamma'_{i_d}\rangle)]$
  (ie. $\langle \gamma'_{i_1} \cdots \gamma'_{i_d}\rangle \mapsto [0, s_2(\langle \gamma'_{i_1} \cdots \gamma'_{i_d}\rangle)]$) for $1 \leq i_1 < \cdots < i_d \leq q$
- $\langle r_1(\beta_{i_1} \cdots \beta_{i_k})\gamma_{i_1} \cdots \gamma_{i_c}\rangle$
  $\mapsto [\beta_{i_1} \cdots \beta_{i_k} s_1(\gamma_{j_1} \cdots \gamma_{j_c}), 0]$ $(= [\beta_{i_1} \cdots \beta_{i_k}, 1] \otimes [s_1(\gamma_{j_1} \cdots \gamma_{j_c}), 0])$
  for $1 < i_1 < \cdots < i_j \leq n$ and $1 \leq j_1 < \cdots < j_c \leq p$
- $\langle r_2(\beta'_{i_1} \cdots \beta'_{i_j})\gamma'_{i_1} \cdots \gamma'_{i_c}\rangle$
  $\mapsto [0, \beta'_{i_1} \cdots \beta'_{i_j} s_2(\gamma'_{j_1} \cdots \gamma'_{j_d})]$ $\left(= [1, \beta'_{i_1} \cdots \beta'_{i_j}] \otimes [0, s_2(\gamma'_{j_1} \cdots \gamma'_{j_d})]\right)$
  for $1 < i_1 < \cdots < i_j \leq m$ and $1 \leq j_1 < \cdots < j_d \leq q$.

Since s_1 and s_2, we see that s is also onto.

By our construction of r and s, it is readily checked that the following sequence is exact:

$$0 \to R/R \cdot \langle 1, -\beta_1\beta_1' \rangle \xrightarrow{r} R' \xrightarrow{s} ann(\langle 1, -\beta_1\beta_1' \rangle) \to 0.$$

We have the corresponding lift $l : ann(\langle 1, -\beta_1\beta_1' \rangle) \to R'$ defined as follows: for a generator of the form $[q, 0]$, where q is a generator of $ann(\langle 1, -\beta_1 \rangle)$, we have $[q, 0] \mapsto [l_1(q), 0, 0]$ (indeed, $l_1(q)$ is even dimensional), and given a generator of the form $[0, q']$, we send $[0, q'] \mapsto [0, l_2(q'), 0]$. What is left is to show that this lift preserves the module action.

Let us take a generator $[q, 0]$ of $ann(\langle 1, -\beta_1\beta_1' \rangle)$, where q is a generator of $ann(\langle 1, -\beta_1 \rangle)$. We first show that $l(\langle \beta_i \rangle \otimes [q, 0]) = r(\overline{\langle \beta_i \rangle}) l([q, 0])$, for $i > 1$, such that if $\beta_1' = -1$ in R_2, our $\beta_i \neq -1$ in R_1. Indeed, we have that

$$\begin{aligned} l(\langle \beta_i \rangle \otimes [q, 0]) &= l([\langle \beta_i \rangle, 1] \cdot [q, 0]) \\ &= l([\langle \beta_i \rangle \otimes q, 0]) \\ &= [l_1(\langle \beta_i \rangle \otimes q), 0, 0] \\ &= [r_1(\overline{\langle \beta_i \rangle}) \otimes l_1(q), 0, 0] \\ &= [r_1(\overline{\langle \beta_i \rangle}), 1, 1] \otimes [l_1(q), 0, 0] \\ &= r(\overline{\langle \beta_i \rangle}) \otimes l([q, 0]) \end{aligned}$$

Now, if $\beta_1' = -1$ in R_2 and $\beta_i = -1$ in R_1, we see that

$$\begin{aligned} l(\langle \beta_i \rangle \otimes [q, 0]) &= l([-1, 1] \cdot [q, 0]) \\ &= l([-q, 0]) \\ &= -l([q, 0]) \\ &= [-l_1(q), 0, 0] \\ &= [-1, -1, \Delta] \otimes [l_1(q), 0, 0] \\ &= -\langle \epsilon \rangle \otimes l([q, 0]) \\ &= r(\overline{\langle \beta_i \rangle}) \otimes l([q, 0]) \end{aligned}$$

Let us now show that $l(\langle \beta_i' \rangle \otimes [q, 0]) = r(\overline{\langle \beta_i' \rangle}) l([q, 0])$, for $i > 1$, such that if $\beta_1 = -1$ in R_1, our $\beta_i' \neq -1$ in R_2. To see this, we see

$$\begin{aligned} l(\langle\beta_i'\rangle \otimes [q,0]) &= l([1,\langle\beta_i'\rangle] \otimes [q,0]) \\ &= l([q,0]) \\ &= [l_1(q),0,0] \\ &= [l_1(q),0,0] \otimes [1, r_1(\overline{\langle\beta_i'\rangle}),1] \\ &= r(\overline{\langle\beta_i'\rangle}) \otimes l([q,0]) \end{aligned}$$

Now, if $\beta_1 = -1$ in R_1 and $\beta_i' = -1$ in R_2, we see that

$$\begin{aligned} l(\langle\beta_i'\rangle \otimes [q,0]) &= l([1,-1] \cdot [q,0]) \\ &= l([q,0]) \\ &= [l_1(q),0,0] \end{aligned}$$

On the other hand, we have

$$\begin{aligned} l(\overline{\beta_i}) \otimes l([q,0]) &= -\langle\epsilon\rangle \otimes l([q,0]) \\ &= -[1,1,\Delta] \otimes [l_1(q),0,0] \\ &= [-l_1(q),0,0] \end{aligned}$$

However, as $\tilde{R_1}$ is characteristic 2 (as we are taking the square root of -1), we have $l_1(q) = -l_1(q)$ in R_1, and as such, we do indeed have $l(\langle\beta_i'\rangle \otimes [q,0]) = l(\overline{\beta_i}) \otimes l([q,0])$.

Finally, we check $l(\langle\beta_1\rangle \otimes [q,0]) = r(\overline{\langle\beta_1\rangle})l([q,0])$. To see this, we note that since $\langle 1, -\beta_1\rangle \otimes q = 0$, then $\langle\beta_1\rangle \otimes q = q$.

$$\begin{aligned} l(\langle\beta_1\rangle \otimes [q,0]) &= l([\langle\beta_1\rangle,1] \cdot [q,0]) \\ &= l([\langle\beta_1\rangle \otimes q,0]) \\ &= l([q,0]) \\ &= [l_1(q),0,0] \\ &= [l_1(q),0,0] \otimes [1,1,\Delta] \\ &= l(q) \otimes \langle\epsilon\rangle \\ &= r(\overline{\langle\beta_1\rangle}) \otimes l([q,0]) \end{aligned}$$

Thus, we see that the module action is preserved on generators of the form $[q,0]$. We can similarly show this for generators of the form $[0,q']$, and so, we are done. ■

6.5 Settling an Edge Case

We now assume we are in the situation that we avoided above, where $\beta_1 = -1$ and R_2 is characteristic 2 (ie. $\beta'_j \neq -1$ for all j).

Theorem 6.5.1. *Let R_1 and R_2 be abstract Witt rings, and let $\beta_1 \in S(R_1)$ and $\beta'_1 \in S(R_2)$. Suppose $\beta_1 = -1$ and R_2 is of characteristic 2. Then*

$$(R_1 \coprod R_2)[\sqrt{(-1, \beta'_1)}] \cong \tilde{R_1} \coprod \tilde{R_2} \coprod \mathbb{Z}/4\mathbb{Z}.$$

Proof. As before, we have the following short exact sequences:

$$0 \to R_1/R_1 \cdot \langle 1, -\beta_1 \rangle \xrightarrow{r} \tilde{R_1} \xrightarrow{s} ann(\langle 1, -\beta_1 \rangle) \to 0$$

$$0 \to R_2/R_2 \cdot \langle 1, -\beta'_1 \rangle \xrightarrow{r'} \tilde{R_2} \xrightarrow{s'} ann(\langle 1, -\beta'_1 \rangle) \to 0$$

with the corresponding lifts $l_1 : ann(\langle 1, -\beta_1 \rangle) \to R_1$ and $l_2 : ann(\langle 1, -\beta'_1 \rangle) \to R_2$. Without loss of generality, we may assume the outputs of l_1 and l_2 are both even dimensional. In fact, we can ensure that on the generators of $ann(\langle 1, -\beta_1 \rangle)$, the output of l_1 would be two dimensional (similarly for l_2). In this case, however, we show that the quadratic extension in respect to $[-1, \beta'_1]$ is $\tilde{R_1} \coprod \tilde{R_2} \coprod \mathbb{Z}/4\mathbb{Z}$.

We now look at $R' = \tilde{R_1} \coprod \tilde{R_2} \coprod \mathbb{Z}/4\mathbb{Z}$, which is what we want to show to be the quadratic extension of R. We notice that for $S(\tilde{R_1})$ can be generated by $\langle r_1(\beta_2) \cdots, r_1(\beta_n), \gamma_1, \cdots, \gamma_p \rangle$, for $\gamma_i \in S(R_1)$. Similarly, $S(\tilde{R_2})$ can be generated by $\langle r_2(\beta'_2) \cdots, r_2(\beta'_n), \gamma'_1, \cdots, \gamma'_q \rangle$, for $\gamma'_j \in S(R_2)$. In this context, we denote $\langle \epsilon \rangle = [1, 1, -1]$, $r_1(\langle \beta_i \rangle) = [r_1(\langle \beta_i \rangle), 1, 1]$, $\langle \gamma_i \rangle = [\gamma_i, 1, 1]$, $r_2(\langle \beta'_j \rangle) = [1, r_2(\langle \beta'_j \rangle), 1]$, and $\langle \gamma'_j \rangle = [1, \gamma'_j, 1]$. So here, as $S(R') = S(\tilde{R_1}) \times S(\tilde{R_2}) \times S(\mathbb{Z}/2\mathbb{Z}[\Delta_1])$, we can generate $S(R')$ with $r_1(\beta_2), \cdots, r_1(\beta_n), r_2(\beta'_2), \cdots, r_2(\beta'_m), \gamma_1, \cdots, \gamma_p, \gamma'_1, \cdots, \gamma'_q, \epsilon$.

Let us now construct $r : R_1 \coprod R_1 \to \tilde{R} \coprod \tilde{R'} \coprod \mathbb{Z}/4\mathbb{Z}$ in the same way we did above, as follows: $\overline{\langle 1 \rangle} \mapsto \langle 1 \rangle$, $\overline{\langle \beta_i \rangle} \mapsto \langle r_1(\langle \beta_i \rangle) \rangle$ for $1 < i \leq n$, $\overline{\langle \beta'_j \rangle} \mapsto \langle r_2(\langle \beta'_j \rangle) \rangle$ for $1 < i \leq n$, and $\overline{\langle \beta_1 \rangle} \mapsto \langle \epsilon \rangle$. It can be seen that this is an injection, since r_1 and r_2 are injections (in

particular, we note r takes forms such as $\overline{\langle 1, -\beta_j \rangle}$ to $\langle 1, -r_1(\langle \beta_j \rangle) \rangle = [1 - r_1(\langle \beta_j \rangle), 0, 0]$, which nicely corresponds to the two dimensional form $r_1(\overline{\langle 1, -\beta_i \rangle})$ in $\tilde{R}_1$). It is also worth noting that in this case, $\overline{\langle \beta_1 \rangle} = [-1, 1] = \langle -1 \rangle$, since R_2 is characteristic 2, which maps to $\langle \epsilon \rangle = [1, 1, -1]$, which is also $\langle -1 \rangle$ in R', as $\tilde{R}_1$ and $\tilde{R}_2$ is characteristic 2.

The construction of $s : R' \to ann(\langle 1, -\beta_1 \beta_1' \rangle)$ is also akin to the above, as follows:

- $\langle 1 \rangle \mapsto 0$
- $\langle \epsilon \rangle \mapsto 0$
- $\langle r_1(\beta_{i_1} \cdots \beta_{i_k}) \rangle \mapsto 0$ for $1 < i_1 < \cdots < i_k \leq n$
- $\langle r_2(\beta'_{i_1} \cdots \beta'_{i_j}) \rangle \mapsto 0$ for $1 < i_1 < \cdots < i_j \leq m$
- $\langle 1, -\gamma_{i_1} \cdots \gamma_{i_c} \rangle \mapsto [s_1(\langle 1, -\gamma_{i_1} \cdots \gamma_{i_c} \rangle), 0]$ (ie. $\langle \gamma_{i_1} \cdots \gamma_{i_c} \rangle$ $\mapsto [s_1(\langle \gamma_{i_1} \cdots \gamma_{i_c} \rangle), 0]$) for $1 \leq i_1 < \cdots < i_c \leq p$
- $\langle 1, -\gamma'_{i_1} \cdots \gamma'_{i_d} \rangle \mapsto [0, s_2(\langle 1, -\gamma'_{i_1} \cdots \gamma'_{i_d} \rangle)]$ (ie. $\langle \gamma'_{i_1} \cdots \gamma'_{i_d} \rangle \mapsto [0, s_2(\langle \gamma'_{i_1} \cdots \gamma'_{i_d} \rangle)]$) for $1 \leq i_1 < \cdots < i_d \leq q$
- $\langle r_1(\beta_{i_1} \cdots \beta_{i_k}) \gamma_{i_1} \cdots \gamma_{i_c} \rangle$ $\mapsto [\beta_{i_1} \cdots \beta_{i_k} s_1(\gamma_{j_1} \cdots \gamma_{j_c}), 0]$ $(= [\beta_{i_1} \cdots \beta_{i_k}, 1] \otimes [s_1(\gamma_{j_1} \cdots \gamma_{j_c}), 0])$ for $1 < i_1 < \cdots < i_j \leq n$ and $1 \leq j_1 < \cdots < j_c \leq p$
- $\langle r_2(\beta'_{i_1} \cdots \beta'_{i_j}) \gamma'_{i_1} \cdots \gamma'_{i_c} \rangle$ $\mapsto [0, \beta'_{i_1} \cdots \beta'_{i_j} s_2(\gamma'_{j_1} \cdots \gamma'_{j_d})]$ $\Big(= [1, \beta'_{i_1} \cdots \beta'_{i_j}] \otimes [0, s_2(\gamma'_{j_1} \cdots \gamma'_{j_d})]\Big)$ for $1 < i_1 < \cdots < i_j \leq m$ and $1 \leq j_1 < \cdots < j_d \leq q$.

Since s_1 and s_2, we see that s is also onto.

As before, by our construction of r and s, it is readily checked that the following sequence is exact:

$$0 \to R/R \cdot \langle 1, -\beta_1 \beta_1' \rangle \xrightarrow{r} R' \xrightarrow{s} ann(\langle 1, -\beta_1 \beta_1' \rangle) \to 0.$$

We have the corresponding lift $l : ann(\langle 1, -\beta_1\beta_1'\rangle) \to R'$ defined as follows: for a generator of the form $[q, 0]$, where q is a generator of $ann(\langle 1, -\beta_1\rangle)$, we have $[q, 0] \mapsto [l_1(q), 0, 0]$ (indeed, $l_1(q)$ is even dimensional, and given a generator of the form $[0, q']$, we send $[0, q'] \mapsto [0, l_2(q'), 0]$. The preservation of the module action can be shown in the exact way as we did above. ■

Remark 6.5.1. *We note that in this case, $R/R\cdot\langle 1, -[-1, \alpha]\rangle$ does not have characteristic 2, in which case, we would not be able to inject it into $\tilde{R_1} \coprod \tilde{R_2} \coprod \mathbb{Z}/2\mathbb{Z}[\Delta_1]$, which does have characteristic 2.*

6.6 The Case of $\beta_1 = 1$

So far, what we've been doing is taking the square root of $[\beta_1, \beta_1']$, where both β_1, β_1' are not squares in their respective ring. In this section, we discuss what taking the square root of $[1, \beta_1']$ would yield (where $\beta_1' \in S(R_2)$ is not 1).

In this section, we show that given $R = R_1 \coprod R_2$, if we take the square root of $[1, \beta_1']$, we get $R_1 \coprod R_1 \coprod \tilde{R_2}$, with $\tilde{R_2}$ being the quadratic extension of R_2 with β_1.

Theorem 6.6.1. *Let R_1 and R_2 be abstract Witt rings, and let $\beta_1' \in S(R_2)$ be not 1. Let $\tilde{R_2}$ be the quadratic extension of R_2 by β_1'. Let $R = R_1 \coprod R_2$. Then*

$$R[\sqrt{[1, \beta_1']}] \cong R_1 \coprod R_1 \coprod \tilde{R_2}.$$

Proof. We note that we have the short exact sequence given by $0 \to R_2/R_2 \cdot \langle 1, -\beta_1'\rangle \xrightarrow{r_2} \tilde{R_2} \xrightarrow{s_2} ann(\langle 1, -\beta_1'\rangle) \to 0$. We also have a corresponding lift $l_2 : ann(\langle 1, -\beta_1'\rangle) \to \tilde{R_2}$. As before, we assume the outputs of l_2 are even dimensional. In fact, we can ensure that on the generators of $ann(\langle 1, -\beta_1\rangle)$, the output of l_2 would be two dimensional.

First, let us look at $R/R \cdot \langle 1, -[1, \beta_1']\rangle$ and $ann(\langle 1, -[1, -\beta_1']\rangle)$. We note that we are quotienting by the ideal generated $[1, 1] - [1, \beta_1'] = [0, 1 - \beta_1']$. It can be readily checked

that this is isomorphic to $R_1 \coprod (R_2/R_2 \cdot \langle 1, -\beta_1' \rangle)$ using the obvious isomorphism. We can easily check that $ann(\langle 1, -[1, \beta_1'] \rangle) = R_1 \coprod ann(\langle 1, -\beta_1' \rangle)$.

With this, let us construct $r : R_1 \coprod (R_2/R_2 \cdot \langle 1, -\beta_1' \rangle \to R_1 \coprod R_1 \coprod \tilde{R}_2)$ by $[a, b] \mapsto [a, a, r_2(b)]$. It is clear that r is injective, as r_2 is injective. We also construct $s : R_1 \coprod R_1 \coprod \tilde{R}_2 \to R_1 \coprod ann(\langle 1, -\beta_1 \rangle)$ with $[a, a', b] \mapsto [a - a', s(b)]$. From this, it is readily checked that $0 \to R_1 \coprod (R_2/R_2 \cdot \langle 1, -\beta_1' \rangle) \xrightarrow{r} R_1 \coprod R_1 \coprod \tilde{R}_2 \xrightarrow{s} R_1 \coprod ann(\langle 1, -\beta_1' \rangle) \to 0$ is an exact sequence.

Here, we have a corresponding lift $l : R_1 \coprod ann(\langle 1, -\beta_1' \rangle) \to R_1 \coprod R_1 \coprod \tilde{R}_2$ such that $[a, b] \mapsto [a, 0, l(b)]$. What is left is to check the module action is preserved.

Take $\overline{[a, b]} \in R_1 \coprod R_2/R_2 \cdot \langle 1, -\beta_1' \rangle$ and $[a', b'] \in R_1 \coprod ann(\langle 1, -\beta_1' \rangle)$. Let us show that $r(\overline{[a, b]}) \otimes l([a', b']) = l([a, b] \otimes [a', b'])$.

$$\begin{aligned} r(\overline{[a, b]}) \otimes l([a', b']) &= [a, a, r_2(b)] \otimes [a', 0, l(b')] \\ &= [aa', 0, r_2(b) l(b')] \\ &= [aa', 0, l(bb')] \\ &= l([aa', bb']) \\ &= l([a, b] \otimes [a', b']) \end{aligned}$$

■

Chapter 7

Future Directions

In this section, we discuss further work to bring this problem to completion, and other work related to this problem.

7.1 Witt Rings of Local Type

There is a class of Witt rings that we have not yet discussed: Witt rings of local type. These rings can be described by its quaternionic structure, where the pairing can be represented as a skew-symmetric matrix. More intuitively, they can be realized as the Witt ring a finite (possibly non-proper) extension of some p-adic field.

Definition 7.1.1. *An finitely generated abstract Witt ring is of* ***elementary type*** *if it can be constructed from* $\mathbb{Z}$*,* $\mathbb{Z}/4\mathbb{Z}$*,* $\mathbb{Z}/2\mathbb{Z}$*, and Witt rings of local type by taking fiber products and group rings.*

By extending our theory to Witt rings of local type, we would be able to find the quadratic extension of any Witt ring of elementary type. It's been conjectured that every finitely generated abstract Witt ring is of elementary type, and as such, finding the structure of quadratic extensions of abstract Witt rings of elementary type is of interest.

7.2 Uniqueness of Quadratic Extension

It is worth noting that the way we defined the quadratic extension for an abstract Witt ring does not say anything about uniqueness. In particular, we defined the quadratic extension to be an abstract Witt ring that fits into a certain exact sequence, with a certain module action being respected. But, given an abstract Witt ring R, and $a \in S(R)$, can there be two (non-isomorphic) abstract Witt rings R_1 and R_2, along with corresponding maps, such that we have exact sequences

$$0 \to R/R \cdot \langle 1, -a \rangle \xrightarrow{r_1} R_1 \xrightarrow{s_1} ann(\langle 1, -b \rangle) \to 0$$

$$0 \to R/R \cdot \langle 1, -a \rangle \xrightarrow{r_2} R_2 \xrightarrow{s_2} ann(\langle 1, -b \rangle) \to 0$$

along with our desired module action being respected? If so, how are the two related?

7.3 Relation to Profinite Groups

As mentioned in the introduction, one of the motivations for abstracting the Witt ring of quadratic field extensions is to further study the relation between Witt rings and their corresponding profinite groups. In the field case, we can determine all possible structures on profinite Galois group $Gal(F_q/F)$ from $W(F)$, where F_q is the quadratic closure of F. By starting off with an abstract Witt ring (ie. without a field), we can more abstractly study the relation between Witt rings and profinite groups.

Bibliography

[1] B. Jacob and R. Ware. Realizing dyadic factors of elementary type Witt rings and pro-2 Galois groups. Mathematische Zeitschrift vol. 208 issue 1, 1991.

[2] L. Gerstein, Basic Quadratic Forms, American Mathematical Society, Graduate Studies in Mathematics vol. 90, 2008.

[3] T. Y. Lam, Quadratic Forms over Fields, American Mathematical Society, Graduate Studies in Mathematics vol. 67, 2005.

[4] M. Marshall, Abstract Witt Rings, Queen's Papers in Pure and Applied Mathematics # 57, 1980.