Embeddings of Integral Quadratic Forms

Rick Miranda
Colorado State University
David R. Morrison
University of California, Santa Barbara

Preface

The authors ran a seminar on Integral Quadratic Forms at the Institute for Advanced Study in the Spring of 1982, and worked on a book-length manuscript reporting on the topic throughout the 1980's and early 1990's. Some new results which are proved in the manuscript were announced in two brief papers in the *Proceedings of the Japan Academy of Sciences* in 1985 and 1986.

We are making this preliminary version of the manuscript available at this time in the hope that it will be useful. Still to do before the manuscript is in final form: final editing of some portions, completion of the bibliography, and the addition of a chapter on the application to K3 surfaces.

Rick Miranda
David R. Morrison
Fort Collins and Santa Barbara
November, 2009

Contents

CHAPTER I

Quadratic Forms and Orthogonal Groups

1. Symmetric Bilinear Forms

Let R be a commutative ring with identity, and let F be an R-module.

DEFINITION 1.1. An *F-valued symmetric bilinear form over R* is a pair
$(L, \langle -, - \rangle)$, where L is an R-module, and $\langle -, - \rangle : L \times L \to F$ is a symmetric function which is R-linear in each variable. We will often abuse language and refer to $\langle\ ,\ \rangle$ as the bilinear form, and say that $\langle\ ,\ \rangle$ is a symmetric bilinear form over R *on* L.

A symmetric bilinear form is also sometimes referred to as an *inner product*.

Let $\operatorname{Symm}^2 L$ be the quotient of $L \otimes_R L$ by the submodule generated by all tensors of the form $x \otimes y - y \otimes x$; $\operatorname{Symm}^2 L$ is the 2^{nd} *symmetric power* of L. An F-valued symmetric bilinear form over R on L can also be defined as an R-linear map from $\operatorname{Symm}^2 L$ to F.

The first example of such a form is the R-valued symmetric bilinear form on R, which is the multiplication map.

DEFINITION 1.2. Let $(L, \langle\ ,\ \rangle)$ be an F-valued symmetric bilinear form over R. The *adjoint map* to $(L, \langle\ ,\ \rangle)$ (or to $\langle\ ,\ \rangle$), denoted by Ad, is the R-linear map from L to $\operatorname{Hom}_R(L, F)$ defined by $\operatorname{Ad}(x)(y) = \langle x, y \rangle$. We will say that

$\langle\ ,\ \rangle$ is *nondegenerate* if Ad is injective, and

$\langle\ ,\ \rangle$ is *unimodular* if Ad is an isomorphism.

The *kernel of* $\langle\ ,\ \rangle$, denoted by $\operatorname{Ker}\langle\ ,\ \rangle$ (or $\operatorname{Ker} L$ if no confusion is possible) is the kernel of Ad.

Note that $\langle\ ,\ \rangle$ is nondegenerate if and only if $\operatorname{Ker}\langle\ ,\ \rangle = (0)$. If $\bar{L} = L/\operatorname{Ker}\langle\ ,\ \rangle$, then $\langle\ ,\ \rangle$ descends to a nondegenerate form on $\bar{L}$. In this book we will deal primarily with nondegenerate forms, and we will largely ignore questions involving nondegeneracy. By modding out the kernel, one can usually reduce a problem to the nondegenerate case, so we feel that this is not a serious limitation.

In this book we will often deal with the special case of an R-valued bilinear form on a free R-module. We give this type of form a special name.

DEFINITION 1.3. An *inner product R-module*, or *inner product module over R*, is a nondegenerate R-valued symmetric bilinear form $(L, \langle -, - \rangle)$ over R such that L is a finitely generated free R-module. If R is a field, this is usually referred to as a *inner product vector space over R*. We sometimes abuse notation and refer to L as the inner product module; the bilinear form $\langle -, - \rangle$ is assumed to be given.

2. Quadratic Forms

Let R be a commutative ring, and let F be an R-module.

DEFINITION 2.1. An *F-valued quadratic form over R* is a pair (L, Q), where L is an R-module and $Q : L \to F$ is a function satisfying

(i) $Q(r\ell) = r^2 Q(\ell)$ for all $r \in R$ and $\ell \in L$
(ii) the function $\langle\ ,\ \rangle_Q : L \times L \to F$ defined by

$$\langle x, y \rangle_Q = Q(x + y) - Q(x) - Q(y)$$

is an F-valued symmetric bilinear form on L.

Again we often refer to Q as the *form on L*. The *adjoint map* Ad_Q *of Q* is simply the adjoint map of $\langle\ ,\ \rangle_Q$. We say Q is nondegenerate (respectively, unimodular) if $\langle\ ,\ \rangle_Q$ is. The bilinear form $\langle\ ,\ \rangle_Q$ is called the *associated bilinear form* to Q.

We denote the kernel of $\langle\ ,\ \rangle_Q$ by $\mathrm{Ker}(L, Q)$ (or just by $\mathrm{Ker}(L)$ or $\mathrm{Ker}(Q)$ when that is convenient). The kernel of a quadratic form has a refinement called the *q-radical* of (L, Q). This is defined to be

$$\mathrm{Rad}_q(L, Q) = \{x \in \mathrm{Ker}(L, Q) | Q(x) = 0\}.$$

(We denote the q-radical by $\mathrm{Rad}_q(L)$ or $\mathrm{Rad}_q(Q)$ when convenient.) Notice that $2Q(x) = \langle x, x \rangle_Q = 0$ for $x \in \mathrm{Ker}(L, Q)$, so that if multiplication by 2 is injective in F, then the q-radical coincides with the kernel.

When restricted to the kernel of Q, Q is $\mathbb{Z}$-linear, and its q-radical is just the kernel of $Q|_{\mathrm{Ker}(Q)}$. Also, since $2Q(x) = 0$ for $x \in \mathrm{Ker}(Q)$, the image of $Q|_{\mathrm{Ker}(Q)}$ is contained in the kernel of multiplication by 2 on F. If this kernel is finite of order N, then the "index" of the q-radical of Q in the kernel of Q is a divisor of N.

Note that if $\bar{\bar{L}} = L/\mathrm{Rad}_q(L)$, then Q descends to a quadratic form on $\bar{\bar{L}}$ with trivial q-radical.

The reader will note the difference between our definition of $\langle\ ,\ \rangle_Q$ and the more usual $\frac{1}{2}[Q(x+y)-Q(x)-Q(y)]$; this definition requires multiplication by 2 to be an isomorphism on F, and we do not want to restrict ourselves to this case. The price we pay is that not every symmetric bilinear form can occur as the associated bilinear form to some quadratic form.

DEFINITION 2.2. An F-valued symmetric bilinear form $(L, \langle\ ,\ \rangle)$ over R is *even* if there exists an F-valued quadratic form Q over R on L such that $\langle\ ,\ \rangle = \langle\ ,\ \rangle_Q$.

The reason for this terminology is that if $\langle\ ,\ \rangle$ is an even form, then $\langle x, x\rangle$ is divisible by 2 in F.

LEMMA 2.3. *Let $\langle\ ,\ \rangle$ be an even F-valued symmetric bilinear form over R on L. Assume that $r^2 \equiv r \mod 2R$ for all r in R. Let $\bar{R} = R/2R$ and $\bar{L} = L/2L$. Let $K = \{f \in F \mid 2f = 0\}$. Then the set of F-valued quadratic forms Q over R on L such that $\langle\ ,\ \rangle = \langle\ ,\ \rangle_Q$ is in 1-1 correspondence with* $\mathrm{Hom}_{\bar{R}}(\bar{L}, K)$.

PROOF. Fix an F-valued quadratic form Q_0 on L such that $\langle\ ,\ \rangle = \langle\ ,\ \rangle_{Q_0}$. Let $\phi \in \mathrm{Hom}_{\bar{R}}(\bar{L}, K)$, and let $\pi : L \to \bar{L}$ be the quotient map. Then $Q_0 + \pi \circ \phi = Q_1$ is an F-valued quadratic form on L, and $\langle\ ,\ \rangle_{Q_0} = \langle\ ,\ \rangle_{Q_1}$. Conversely, if Q is an F-valued quadratic form on L with $\langle\ ,\ \rangle = \langle\ ,\ \rangle_Q$, then $\alpha = Q - Q_0 : L \to F$ is $\mathbb{Z}$-linear. Moreover, $2\alpha(x) = \alpha(2x) = 4\alpha(x)$, so $2\alpha(x) = 0$ for all x in L; hence α maps L to K. Since $\alpha(2L) = 0$, α factors through a group homomorphism $\phi : \bar{L} \to K$. Finally, if $\bar{x} \in \bar{L}$, and $r \in R$, then $\phi(r\bar{x}) = r^2\phi(\bar{x}) = r\phi(\bar{x})$ by our assumption on R. Hence, ϕ is R-linear and $\bar{R}$-linear also. Q.E.D.

Most of the rings occurring in this book satisfy the hypothesis of the previous lemma. In particular, any field of characteristic $\neq 2$ does, $\mathbb{Z}$ does, $\mathbb{Z}_p$ does (for any p), etc.

COROLLARY 2.4. *Let $\langle\ ,\ \rangle$ be an even F-valued symmetric bilinear form over R on L. Assume that multiplication by 2 is injective on F. Then there is a unique F-valued quadratic form Q over R on L such that $\langle\ ,\ \rangle = \langle\ ,\ \rangle_Q$.*

PROOF. In this case $K = \{f \in F \mid 2f = 0\}$ is trivial. Let Q_1 and Q_2 be two F-valued quadratic forms over R on L with associated bilinear forms $\langle\ ,\ \rangle$. Then $\alpha = Q_1 - Q_2$ is a $\mathbb{Z}$-linear map from L to F, and as in the proof of the previous lemma α has values in K. Hence $\alpha = 0$ and $Q_1 = Q_2$. Q.E.D.

COROLLARY 2.5. *Assume that 2 is a unit in R. Then any F-valued symmetric bilinear form $\langle\ ,\ \rangle$ over R is even, and there is a unique F-valued quadratic form Q over R such that $\langle\ ,\ \rangle = \langle\ ,\ \rangle_Q$.*

PROOF. $\langle\ ,\ \rangle$ is even, since $Q(x) = \frac{1}{2}\langle x, x\rangle$ is the required quadratic form. Q is unique by the previous corollary. Q.E.D.

3. Quadratic Modules

In this book we will be dealing with the following special case of the previous definitions. Let R be a commutative ring with identity.

DEFINITION 3.1. A *quadratic R-module*, or *quadratic module over R*, is a nondegenerate R-valued quadratic form (L, Q) over R such that L is a finitely generated free R-module. If R is a field, this is usually referred to as a *quadratic vector space over R*. We sometimes abuse notation and refer to L as the quadratic module; the form Q is assumed to be given.

Note that if (L, Q) is a quadratic R-module, and if $\langle -, -\rangle$ is the associated bilinear form to Q, then $(L, \langle -, -\rangle)$ is an (even) inner product module over R.

As is usual with free modules, many of the concepts can be expressed in terms of matrices. Let us review this part of the theory now.

Let Q be a quadratic form on R^N, with values in R, endowing R^N with the structure of a quadratic R-module. Let $\langle\ ,\ \rangle = \langle\ ,\ \rangle_Q$ be the associated bilinear form. The *matrix* of Q (or of $\langle\ ,\ \rangle$) is the $N \times N$ symmetric matrix A over R, whose $i-j^{th}$ entry is $\langle e_i, e_j\rangle$, where $\{e_1, \ldots, e_N\}$ is the standard basis of R^N. With this notation, if X and Y are column vectors in R^N, then $\langle X, Y\rangle = X^\top AY$. Note that since $\langle\ ,\ \rangle$ is even, the diagonal entries of A are in 2R.

In more generality, let (L, Q) be a quadratic R-module, and let $S = \{s_1, \ldots, s_N\}$ be a basis for L over R. The *matrix of Q* (or of $\langle\ ,\ \rangle$) *with respect to S* is the $N \times N$ symmetric matrix $A = (\langle s_i, s_j\rangle)$.

Of course, giving an ordered basis S for L is equivalent to giving an isomorphism $\alpha : L \to R^N$ (sending s_i to e_i). With this notation, we have $\langle x, y\rangle = \alpha(x)^\top A\alpha(y)$.

Note that for a quadratic R-module (L, Q), the adjoint map Ad_Q maps L to its dual $L^\# = \mathrm{Hom}_R(L, R)$, and by our convention Ad_Q is injective.

If L has basis $S = \{s_1, \ldots, s_N\}$, then $L^\#$ has dual basis $S^\# = \{s_1^\#, \ldots, s_N^\#\}$, defined by $s_i^\#(s_j) = \delta_{ij}$, the Kronecker delta.

LEMMA 3.2. *Let (L, Q) be a quadratic R-module with basis S. Let A be the matrix of Q with respect to S. Then the matrix of* $\mathrm{Ad}_Q : L \to L^\#$ *with respect to S and $S^\#$ is also A.*

PROOF. Let $C = (c_{ij})$ denote the matrix of Ad_Q, so that $\mathrm{Ad}_Q(e_j) = \sum_k c_{k_j} e_k^\#$. Then $\mathrm{Ad}_Q(e_j)(e_i) = \sum_k c_{k_j} e_k^\#(e_i) = c_{ij}$, so that $\langle e_i, e_j \rangle = \langle e_j, e_i \rangle = \mathrm{Ad}_Q(e_j)(e_i) = c_{ij}$, proving that $A = C$. Q.E.D.

COROLLARY 3.3. *With the notations of Lemma 3.2, we have:*

(3.3.1) det(A) is not a zero divisor in R,

(3.3.2) Q is unimodular if and only if $\det(A)$ *is a unit in R.*

Let us assume that (L, Q) is a quadratic R-module with two bases S and T, inducing isomorphisms α_S and $\alpha_T : L \to R^N$. Let A_S and A_T be the matrices of Q with respect to S and T, respectively, and let P be the matrix of the isomorphism $\alpha_S \circ \alpha_T^{-1} : R^N \to R^N$.

LEMMA 3.4. *With the above notations, $A_T = P^\top A_S P$.*

PROOF. For any x in L, $\alpha_S(x) = P\alpha_T(x)$, or $\alpha_T(x) = P^{-1}\alpha_S(x)$. Hence $\langle x, y \rangle = \alpha_S(x)^\top A_S \alpha_S(y) = \alpha_S(x)^\top (P^{-1})^\top P^\top A_S P P^{-1} \alpha_S(x) = \alpha_T(x)^\top (P^\top A_S P) \alpha_T(x)$, so that $A_T = P^\top A_S P$. Q.E.D.

We will use the notation $R^\times$ for the units of a ring R. The above lemma leads us to the following.

DEFINITION 3.5. Let (L, Q) be a quadratic R-module. The *discriminant of* (L, Q) (or *of* L, or *of* Q) is the class of $\det(A)$ in $R/(R^\times)^2$, where A is the matrix of Q with respect to some basis of L.

A few remarks are in order. Firstly, the discriminant of L (denoted by $\mathrm{disc}(L)$, or $\mathrm{disc}(Q)$) is well defined by Lemma 3.4. Secondly, by Corollary (3.3.1), $\mathrm{disc}(L)$ in fact lies in $\{\text{non-zero divisors of } R\}/(R^\times)^2$. In particular, if R is an integral domain, then $\mathrm{disc}(L) \in (R - \{0\})/(R^\times)^2$. Furthermore, if R is a field, then $\mathrm{disc}(L) \in R^\times/(R^\times)^2$. In this case, the values for $\mathrm{disc}(L)$ form a group.

In general, Q is unimodular if and only if $\mathrm{disc}(Q) \in R^\times/(R^\times)^2$. Note that any quadratic R-module is unimodular when R is a field.

The value group $R^\times/(R^\times)^2$ occurs so often in this book that we will use the following notation for it. If R is any commutative ring with identity, define $\mathcal{D}(R) = R^\times/(R^\times)^2$; $\mathcal{D}(R)$ is an abelian group, every nontrivial element having order 2.

It will be useful to collect these value sets for the discriminant in the following important cases.

LEMMA 3.6.

(3.6.1) $\mathbb{Z} - \{0\}/(\mathbb{Z}^\times)^2 = \mathbb{Z} - \{0\}$.
Hence any quadratic $\mathbb{Z}$-module has a nonzero rational integer as discriminant.

(3.6.2) *$\mathcal{D}(\mathbb{Q})$ is a free $\mathbb{Z}/2$-module on the set $\{-1\} \cup \{p > 1 \,|\, p$ is a prime in $\mathbb{Z}\}$.*

(3.6.3) *$\mathcal{D}(\mathbb{R})$ is a cyclic group of order 2, generated by the class of -1.*

(3.6.4) *$\mathcal{D}(\mathbb{C})$ is a trivial group.*

(3.6.5) *Recall that $\mathbb{Z}_p^\times = \{u \in \mathbb{Z}_p \,|\, \|u\|_p = 1\}$. Then:*

(a) *If p is odd, $\mathcal{D}(\mathbb{Z}_p)$ is a cyclic group of order two, generated by the class of a non-square mod p. In this case, a unit $u \in \mathbb{Z}_p^\times$ is a square if and only if u is a square mod p.*

(b) *If $p = 2$, $\mathcal{D}(\mathbb{Z}_2)$ is a Klein 4-group, consisting of the classes of 1, 3, 5 and 7. A unit $u \in \mathbb{Z}_2^\times$ is a square if and only if $u = 1 \mod 8$.*

Since every element of $\mathbb{Z}_p - \{0\}$ can be uniquely written as $p^e u$, with $e \geq 0$ and $u \in \mathbb{Z}_p^\times$, the discriminants of quadratic $\mathbb{Z}_p$-modules lie in $\mathbb{Z}_p - \{0\}/(\mathbb{Z}_p^\times)^2 \cong \mathbb{N} \times (\mathbb{Z}_p^\times)/(\mathbb{Z}_p^\times)^2 \cong$
$$\begin{cases} \mathbb{N} \times \mathbb{Z}/2 & \text{if } p \text{ is odd} \\ \mathbb{N} \times \mathbb{Z}/2 \times \mathbb{Z}/2 & \text{if } p = 2. \end{cases}$$

(3.6.6) *Every element of $\mathbb{Q}_p^\times$ can be uniquely written as $p^e u$, with $e \in \mathbb{Z}$ and $u \in \mathbb{Z}_p^\times$. Hence*

$$\mathcal{D}(\mathbb{Q}_p) = \begin{cases} \mathbb{Z}/2 \times \mathbb{Z}/2 & \text{if } p \text{ is odd} \\ \mathbb{Z}/2 \times \mathbb{Z}/2 \times \mathbb{Z}/2 & \text{if } p = 2. \end{cases}$$

(3.6.7) *(a) If p is odd, $\mathcal{D}(\mathbb{Z}/p^e)$ is a cyclic group of order 2, generated by the class of a nonsquare mod p. Again, a unit $u \in (\mathbb{Z}/p^e)^\times$ is a square if and only if u is a square mod p.*

(b) If $p = 2$, we have

$$\mathcal{D}(\mathbb{Z}/2^e) = \begin{cases} \text{trivial} & \text{if } e = 1 \\ \text{cyclic of order 2} & \text{if } e = 2 \\ \text{a Klein 4-group} & \text{if } e \geq 3. \end{cases}$$

We leave the elementary proofs of these computations to the reader.

Because of its pervasive usage, we will often use the notation $\mathbb{U}_p$ for $\mathbb{Z}_p^\times$.

We would like to identify these value groups in the p-adic and p-primary cases with "standard" groups. We do this via the following isomorphisms, all of which we call χ.

For $R = \mathbb{R}$, $\chi : \mathcal{D}(\mathbb{R}) \to \{\pm 1\}$ is the obvious isomorphism.

For $R = \mathbb{Z}_p$, p odd, $\chi : \mathcal{D}(\mathbb{Z}_p) \to \{\pm 1\}$ is the Legendre symbol; for $u \in \mathbb{U}_|$,

$$\chi(u) = \left(\frac{u}{p}\right) = \begin{cases} +1 & \text{if } u \text{ is a square} \\ -1 & \text{if } u \text{ is a non-square.} \end{cases}$$

For $R = \mathbb{Z}/p^e$, p odd, $\chi : \mathcal{D}(\mathbb{Z}/p^e) \to \{\pm 1\}$ is the Legendre symbol.
For $R = \mathbb{Z}_2$, $\chi : \mathcal{D}(\mathbb{Z}_2) \to (\mathbb{Z}/8)^\times$ is the "mod 8" map.
For $R = \mathbb{Z}/2^e$, $e \geq 3$, $\chi : \mathcal{D}(\mathbb{Z}/2^e) \to (\mathbb{Z}/8)^\times$ is the mod 8 map.
For $R = \mathbb{Z}/4$, $\chi : \mathcal{D}(\mathbb{Z}/4) \to (\mathbb{Z}/4)^\times$ is the identity.
For $R = \mathbb{Z}/2$, $\chi : \mathcal{D}(\mathbb{Z}/2) \to (\mathbb{Z}/2)^\times$ is the identity.

Note that for any prime p, we have a commutative square

$$\begin{array}{ccc} \mathcal{D}(\mathbb{Z}_p) & \xrightarrow{\chi} & \text{standard group} \\ \downarrow & & \downarrow \\ \mathcal{D}(\mathbb{Z}/p^e) & \xrightarrow{\chi} & \text{standard group} \end{array}$$

in addition the squares

$$\begin{array}{ccc} \mathcal{D}(\mathbb{Z}/p^{e_1}) & \xrightarrow{\chi} & \text{standard group} \\ \downarrow & & \downarrow \\ \mathcal{D}(\mathbb{Z}/p^{e_2}) & \xrightarrow{\chi} & \text{standard group} \end{array}$$

commute, where $e_2 \leq e_1$. In both cases the vertical maps are the natural quotient maps.

We will extend this notation to $\mathcal{D}(\mathbb{Q}_p)$ by defining

$$\chi(p^e u \bmod (\mathbb{Q}_p^\times)^2) = \chi(u \bmod \mathbb{U}_p^{\not\in}),$$

where $e \in \mathbb{Z}$ and $u \in \mathbb{U}_p$. In this case

$$\chi : \mathcal{D}(\mathbb{Q}_p) \to \{\pm 1\} \text{ if } p \text{ is odd}$$

and

$$\chi : \mathcal{D}(\mathbb{Q}_2) \to (\mathbb{Z}/8)^\times$$

are only group homomorphisms, with kernel of order 2, generated by the prime p in each case.

In case $R = \mathbb{Z}$, a quadratic $\mathbb{Z}$-module will be referred to as an *integral quadratic form*, justifying the title of this book. Similarly, if $R = \mathbb{Q}$, $\mathbb{R}$ or $\mathbb{C}$, a quadratic R-module will be called a *rational, real* or *complex quadratic form*, respectively. An *integral p-adic quadratic form* is a quadratic $\mathbb{Z}_p$-module, and a *rational p-adic quadratic form* is a quadratic $\mathbb{Q}_p$-module.

4. Torsion Forms over Integral Domains

The central construction dealt with in this book is a special case of the following type of quadratic form. Throughout this section, let R denote an integral domain, and let K denote its fraction field.

DEFINITION 4.1. A *torsion quadratic form over R* is a K/R-valued quadratic form over R on a finitely generated torsion R-module.

Similarly, a *torsion bilinear form over R* is a K/R-valued bilinear form over R on a finitely generated torsion R-module.

Note that there is no requirement of nondegeneracy in the above definition.

If G is a torsion R-module, define $G^{\#} = \mathrm{Hom}_R(G, K/R)$, so that if (G, q) is a torsion quadratic form over R, the adjoint map Ad_q maps G to $G^{\#}$. In case G is cyclic, these groups are isomorphic:

LEMMA 4.2. *Assume $a \in R$, $a \neq 0$. Then the map $\alpha : R/a \to \mathrm{Hom}_R(R/a, K/R)$ defined by*

$$\alpha(x \bmod (a))(y \bmod (a)) = \frac{xy}{a} \mod R$$

is an isomorphism of R-modules.

PROOF. It is clear that α is well defined, and is an R-map. Assume $\alpha(x \bmod (a)) = 0$. Then $\alpha(x \bmod (a))(1 \bmod (a)) = \frac{x}{a} \mod R$ will be 0 in K/R, i.e., $\frac{x}{a} \in R$, or $a|x$; hence $x \bmod (a) = 0$ in R/a. Therefore, α is 1-1. Let $\phi \in (R/a)^{\#}$, and write $\phi(1 \bmod (a)) = \frac{p}{q} \mod R$. Since $0 = \phi(0) = \phi(a \bmod (a)) = a\phi(1 \bmod (a)) = \frac{ap}{q} \mod R$, $q|ap$ in R. Write $ap = rq$; then $\frac{p}{q} = \frac{r}{a}$ in K so that $\phi(1 \bmod (a)) = \frac{r}{a} \mod R$, and $\phi = \alpha(r \bmod (a))$ by linearity. Hence α is onto. Q.E.D.

This leads to the following result which is well known in case $R = \mathbb{Z}$. As is standard, we will abbreviate "principal ideal domain" to P.I.D.

LEMMA 4.3. *Assume R is a P.I.D. and G is a finitely generated torsion R-module. Then $G \cong G^{\#}$ as R-modules.*

PROOF. By hypothesis on R, G is a direct sum of cyclic torsion R-modules. Since $(\bigoplus_i G_i)^{\#} \cong \bigoplus_i G_i^{\#}$, the result follows from Lemma 4.2. Q.E.D.

COROLLARY 4.4. *Assume R is a P.I.D. and let (G, q) be a torsion quadratic form over R. Then G is nondegenerate if and only if G is unimodular.*

Two special cases will be of particular interest to us. Firstly, if $R = \mathbb{Z}$, then a torsion quadratic form (G, q) over $\mathbb{Z}$ will be called a *finite quadratic form;* the group G is a finite abelian group, and the values of q lie in $\mathbb{Q}/\mathbb{Z}$. A *finite bilinear form* is a torsion bilinear form over $\mathbb{Z}$.

Secondly, if $R = \mathbb{Z}_p$, then a torsion quadratic form (G, q) over $\mathbb{Z}_p$ will be called a *p-primary quadratic form.* In this case the group G is

a finite abelian p-group and the values of q lie in $\mathbb{Q}_p/\mathbb{Z}_p$. A *p-primary bilinear form* is a torsion bilinear form over $\mathbb{Z}_p$.

The value group $\mathbb{Q}_p/\mathbb{Z}_p$ for a p-primary quadratic form is isomorphic to a sub-quotient group of $\mathbb{Q}$. Let $\mathbb{Q}^{(p)} \subset \mathbb{Q}$ denote the set of all rational numbers with denominator a power of p.

LEMMA 4.5. *There is a natural isomorphism between $\mathbb{Q}_p/\mathbb{Z}_p$ and $\mathbb{Q}^{(p)}/\mathbb{Z}$.*

PROOF. Represent elements of $\mathbb{Q}_p$ as Laurent series in p, with coefficients in $\{0, 1, \ldots, p-1\}$. Define $\beta : \mathbb{Q}_p \to \mathbb{Q}^{(p)}/\mathbb{Z}$ by $\beta(\sum a_i p^i) = (\sum_{i<0} a_i p^i) \mod \mathbb{Z}$. Then β is a surjective group homomorphism with kernel $\mathbb{Z}_p$. Q.E.D.

5. Orthogonality and Splitting

Let (L_1, Q_1) and (L_2, Q_2) be two F-valued quadratic forms over R.

DEFINITION 5.1. The *direct sum* (or *orthogonal* direct sum) of (L_1, Q_1) and (L_2, Q_2) is the pair $(L_1 \oplus L_2, Q_1 + Q_2)$. (The function $Q_1 + Q_2 : L_1 \oplus L_2 \to F$ is defined by $(Q_1 + Q_2)(x_1, x_2) = Q_1(x_1) + Q_2(x_2)$.)

It is trivial to check that $(L_1 \oplus L_2, Q_1 + Q_2)$ is an F-valued quadratic form over R. In addition, we have the following.

LEMMA 5.2. *Using the above notations,*

(5.2.1) *$Q_1 + Q_2$ is nondegenerate if and only if Q_1 and Q_2 are.*
(5.2.2) *$Q_1 + Q_2$ is unimodular if and only if Q_1 and Q_2 are.*

PROOF. This follows immediately from the formula $\mathrm{Ad}_{Q_1+Q_2} = \mathrm{Ad}_{Q_1} \oplus \mathrm{Ad}_{Q_2}$, and the fact that direct sums commute with Hom. Q.E.D.

LEMMA 5.3. *Assume that (L_1, Q_1) and (L_2, Q_2) are quadratic R-modules. Then*

(5.3.1) *$(L_1 \oplus L_2, Q_1 + Q_2)$ is a quadratic R-module.*
(5.3.2) *Assume S_1 and S_2 are bases for L_1 and L_2, respectively, so that A_1 and A_2 are the matrices of Q_1 and Q_2 with respect to S_1 and S_2, respectively. Then $S_1 \cup S_2 = \{(s_1, 0) \mid s_1 \in S_1\} \cup \{(0, s_2) \mid s_2 \in S_2\}$ is a basis for $L_1 \oplus L_2$ over R, and the matrix of $Q_1 + Q_2$ with respect to $S_1 \cup S_2$ is $\left(\begin{smallmatrix} A_1 & 0 \\ 0 & A_2 \end{smallmatrix}\right)$.*
(5.3.3) $\mathrm{disc}(Q_1 + Q_2) = \mathrm{disc}(Q_1)\,\mathrm{disc}(Q_2)$.

PROOF. The first statement follows immediately from the definitions and

Lemma (5.2.1). The second statement is clear by the following calculation:

$$\begin{aligned}\langle (x_1,x_2),(y_1,y_2)\rangle_{Q_1+Q_2} &= (Q_1+Q_2)(x_1+y_1,x_2+y_2)\\ &\quad -(Q_1+Q_2)(x_1,x_2)-(Q_1+Q_2)(y_1,y_2)\\ &= Q_1(x_1+y_1)+Q_2(x_2+y_2)\\ &\quad -Q_1(x_1)-Q_2(x_2)-Q_1(y_1)-Q_2(y_2)\\ &= \langle x_1,y_1\rangle_{Q_1}+\langle x_2,y_2\rangle_{Q_2}.\end{aligned}$$

Finally, the last statement follows from the second. Q.E.D.

The above construction is sometimes referred to as an *external* direct sum. There is, of course, a notion of *internal* direct sum, also.

Definition 5.4. Let (L,Q) be an F-valued quadratic form over R, with associated bilinear form $\langle\ ,\ \rangle$.

(5.4.1) Two elements x, $y \in L$ are said to be *orthogonal,* or *perpendicular* if $\langle x,y\rangle = 0$.

(5.4.2) An element $x \in L$ is *isotropic* if $Q(x) = 0$; x is *anisotropic* if $Q(x) \neq 0$.

(5.4.3) If $X \subset L$ is a subset of L, the *perpendicular module to* X, denoted by $X^\perp$, is the set $\{y \in L \mid \langle x,y\rangle = 0 \text{ for all } x \text{ in } L\}$.

(5.4.4) A subset $X \subset L$ is *totally anisotropic* if each element of X is isotropic. This implies that $X \subset X^\perp$.

Note that $\langle x,x\rangle = 0$ does not imply that x is isotropic, unless multiplication by 2 is injective on F. Similarly, $X \subset X^\perp$ does not imply that X is totally isotropic.

Also note that if X is any set, $X^\perp$ is a submodule of L. Moreover, $X \subset (X^\perp)^\perp$ always.

Definition 5.5. Let (L,Q) be an F-valued quadratic form over R. A *splitting* of (L,Q) is a direct sum decomposition $L = M \oplus N$ of L such that every element of M is orthogonal to each element of N. If M is a submodule of L, we say that M *splits off* L if M is a direct summand of L, and there exists a submodule N of L such that $L = M \oplus N$ is a splitting.

Note that if $L = M \oplus N$ is a splitting of L, then (L,Q) is isomorphic to the orthogonal direct sum of $(M, Q|_M)$ and $(N, Q|_N)$.

There is one simple but important criterion for a submodule of L to split off.

Proposition 5.6. *Let (L,Q) be an F-valued quadratic form over R and let M be a submodule of L. Assume that $(M, Q|_M)$ is unimodular. Then M splits off L. In fact, $L = M \oplus M^\perp$ is a splitting of L.*

PROOF. Since M is unimodular, $M \cap M^{\perp} = \{0\}$; hence, it suffices to show that $L = M + M^{\perp}$. Restriction gives an R-map res : $\mathrm{Hom}_R(L, F) \to \mathrm{Hom}_R(M, F)$. Let $\alpha = \mathrm{res} \circ \mathrm{Ad}_L : L \to \mathrm{Hom}_R(M, F)$. Note that $\alpha|_M = \mathrm{Ad}_M$, so by the unimodularity of M, $\alpha|_M$ is an isomorphism; hence, α is onto. The kernel of α is exactly $M^{\perp}$, so we have an exact sequence of R-modules

$$0 \to M^{\perp} \to L \xrightarrow{\alpha} \mathrm{Hom}_R(M, F) \to 0.$$

Let $x \in L$. Since $\alpha|_M$ is an isomorphism, there is an element $m \in M$ such that $\alpha(m) = \alpha(x)$; hence $x - m \in M^{\perp}$. Therefore $x = m + (x - m) \in M + M^{\perp}$. Q.E.D.

There is a generalization of the above proposition for R a discrete valuation ring which will be discussed later.

DEFINITION 5.7. An F-valued quadratic form (L, Q) over R is *indecomposable* if L does not split as the direct sum of two proper nonzero submodules. A quadratic R-module (L, Q) is *diagonalizable* if L splits as the direct sum of rank one submodules.

PROPOSITION 5.8. *Assume that R is a field of characteristic $\neq 2$, and let (L, Q) be a quadratic R-module. Then (L, Q) is diagonalizable.*

PROOF. The proof is by induction on the rank of L. If $\mathrm{rank}(L) = 1$, there is nothing to do; assume $\mathrm{rank}(L) \geq 2$. If $x \in L$ and $Q(x) \neq 0$, then $M =$ span of x splits off L, and by induction $M^{\perp}$ is diagonalizable; hence, $L = M \oplus M^{\perp}$ is diagonalizable. Therefore, we need only show that there is a vector x in L with $Q(x) \neq 0$. However, if $Q(x) = 0$ for every x in L, Q is degenerate. Q.E.D.

6. Homomorphisms

DEFINITION 6.1. Let (L_1, Q_1) and (L_2, Q_2) be two F-valued quadratic forms over R. A *homomorphism* ϕ from (L_1, Q_1) to (L_2, Q_2) (or, for convenience, from L_1 to L_2) is an R-map $\phi : L_1 \to L_2$ such that $Q_2 \circ \phi = Q_1$. If ϕ is 1-1, ϕ is called an *embedding*.

This is, of course, just what one would expect. Note that if (L, Q) is an F-valued quadratic form over R, and $M \subset L$ is a submodule, then the inclusion map inc : $M \to L$ is an embedding of $(M, Q|_M)$ into (L, Q).

The reader should also note that if L splits as $L = M \oplus N$, then the projection map $\pi : L \to M$ is *not* a homomorphism in general; it is only if $Q|_N \equiv 0$.

The composition of homomorphisms is a homomorphism.

LEMMA 6.2. *Let $\phi : (L_1, Q_1) \to (L_2, Q_2)$ be a homomorphism of F-valued quadratic forms over R. Assume $x \in L_1$ and $\phi(x) = 0$. Then $\mathrm{Ad}_{Q_1}(x) = 0$ and $Q_1(x) = 0$.*

PROOF. By assumption, $Q_1(x) = Q_2(\phi(x)) = Q_2(0) = 0$, so we need only check that $\mathrm{Ad}_{Q_1}(x) = 0$. Let $y \in L_1$. Then $Q_1(x + y) = Q_2(\phi(x+y)) = Q_2(\phi(y)) = Q_1(y)$, so that $Q_1(x+y)-Q_1(y) = 0$. Since $Q_1(x) = 0$ also, we have $\langle x, y\rangle_{Q_1} = Q_1(x + y) - Q_1(x) - Q_1(y) = 0$, so that $\mathrm{Ad}_{Q_1}(x) = 0$. Q.E.D.

COROLLARY 6.3. *Let $\phi : (L_1, Q_1) \to (L_2, Q_2)$ be a homomorphism of F-valued quadratic forms over R. Assume that L_1 is nondegenerate. Then ϕ is an embedding.*

COROLLARY 6.4. *Let $\phi : (L_1, Q_1) \to (L_2, Q_2)$ be a homomorphism of quadratic R-modules. Then ϕ is an embedding.*

These corollaries follow immediately from Lemma 6.2.

Note that if ϕ is a bijective homomorphism of F-valued quadratic forms over R, then ϕ^{-1} is also a homomorphism.

DEFINITION 6.5. An *isomorphism* (or *isometry*) of F-valued quadratic forms is a bijective homomorphism. An *automorphism* is a self-isometry. Two F-valued quadratic forms (L_1, Q_1) and (L_2, Q_2) are *isomorphic* (or *isometric*) if there exists an isomorphism between them, and we use the usual notation $(L_1, Q_1) \cong (L_2, Q_2)$ in this case. (We will often abbreviate this to $L_1 \cong L_2$ or $Q_1 \cong Q_2$.)

The following "equivalence relation" on F-valued quadratic forms is coarser than isomorphism, but still is quite rich.

DEFINITION 6.6. Two F-valued quadratic forms (L_1, Q_1) and (L_2, Q_2) over R are *stably isomorphic* if there exist two unimodular F-valued quadratic forms over R, M_1 and M_2, such that $L_1 \oplus M_1 \cong L_2 \oplus M_2$. We denote this by $L_1 \sim_S L_2$ (or $Q_1 \sim_S Q_2$).

It will be useful to consider the following special class of homomorphisms, whose importance is motivated by the above.

DEFINITION 6.7. A homomorphism $\phi : L_1 \to L_2$ of F-valued quadratic forms over R is *stable* if $L_2 = \phi(L_1) \oplus \phi(L_1)^\perp$, and $\phi(L_1)^\perp$ is unimodular.

Note that if M is unimodular, the inclusion of L into $L \oplus M$ is a stable homomorphism. We leave to the reader to check that the smallest equivalence relation on F-valued quadratic forms over R such that if there exists a stable homomorphism $\phi : L_1 \to L_2$, then L_1 is equivalent to L_2, is stable isomorphism.

7. Examples

We will collect in this section the fundamental examples of bilinear and quadratic forms which are needed in this book. These examples will all be either quadratic R-modules, or torsion quadratic forms.

EXAMPLE 7.1. *Rank 1 quadratic R-modules.*

Let R be any commutative ring with identity, and let $a \in R$. Let L be a free rank-one R-module with basis $S = \{s\}$. Define $Q : L \to R$ by $Q(rs) = ar^2$. The associated bilinear form is then $\langle xs, ys\rangle = 2xya$, so the matrix of $\langle\ ,\ \rangle$ with respect to S is the 1×1 matrix (2a). Hence $\langle\ ,\ \rangle$ is nondegenerate if and only if 2a is not a zero-divisor in R; if this is the case, then (L, Q) is a quadratic R-module of rank 1. We denote by $\langle a\rangle_R$ the isomorphism class of this quadratic R-module. The form $\langle 1\rangle_R$ will usually be denoted by $\mathbf{1}_R$.

Note that $\langle a\rangle_R \cong \langle b\rangle_R$ if and only if there is a unit $u \in R^\times$ such that $a = u^2 b$. Hence, if multiplication by 2 in injective on R, then rank-one quadratic R-modules are classified by $\{\text{non-zero divisors of } R\}/(R^\times)^2$. In particular, if R is an integral domain, rank-one quadratic R-modules are classified by $(R - \{0\})/(R^\times)^2$.

We will use a special notation in case $R = \mathbb{Z}$ or $\mathbb{Z}_p$.

If $a \neq 0$, $a \in \mathbb{Z}$, then $\langle a\rangle_{\mathbb{Z}}$ will be denoted simply by $\langle a\rangle$, if no confusion is possible.

If $a \in \mathbb{Z}_p$, $a \neq 0$, then we can write $2a = p^k u$, where $k \geq 0$ and $u \in \mathbb{U}_{\text{ı}}$. The isomorphism class of the form $\langle a\rangle_{\mathbb{Z}_p} = \langle \frac{1}{2} p^k u\rangle_{\mathbb{Z}_p}$ will be denoted by $W^{\varepsilon}_{p,k}$, where $\varepsilon = \chi(u)$.

Note that $\langle a\rangle \cong \langle b\rangle$ if and only if $a = b$, and $W^{\varepsilon}_{p,k} \cong W^{\eta}_{p,\ell}$ if and only if $\varepsilon = \eta$ and $k = \ell$.

Also, $\operatorname{disc}(\langle a\rangle) = 2a$ and $\operatorname{disc}(W^{\varepsilon}_{p,k}) = p^k u \mod \mathbb{U}^{\text{ı}}_{\text{ı}}$, where $\chi(u) = \varepsilon$.

Finally, note that if $p = 2$, the quadratic $\mathbb{Z}_2$-modules $W^{\varepsilon}_{2,0}$ are not defined as quadratic modules; the quadratic form has values in $\frac{1}{2} BbbZ_2$, not in $BbbZ_2$. However, we can define the associated bilinear form $\langle -, -\rangle$, which does have values in $BbbZ_2$; if s is the generator of the free module L, this bilinear form is $\langle xs, ys\rangle = xyu$, where $\chi(u) = \varepsilon$. With this definition we have an (odd) inner product module over $\mathbb{Z}_2$.

EXAMPLE 7.2. *The hyperbolic plane.*

Let R be a commutative ring with identity, and let L be a free rank 2 R-module with basis $S = \{s_1, s_2\}$. Define $Q : L \to R$ by $Q(r_1 s_1 + r_2 s_2) = r_1 r_2$. The associated bilinear form is then

$$\langle r_1 s_1 + r_2 s_2, r'_1 s_1 + r'_2 s_2\rangle = r_1 r'_2 + r_2 r'_1,$$

and the matrix of Q with respect to S is $\left(\begin{smallmatrix}0 & 1\\ 1 & 0\end{smallmatrix}\right)$. Hence, Q is nondegenerate and is in fact unimodular. The isomorphism class of this quadratic R-module (L, Q) of rank 2 will be denoted by U_R, or simply U if no confusion is possible; it is called the *hyperbolic plane over* R. Note that $\operatorname{disc}(U_R) = -1 \mod (R^\times)^2$.

LEMMA 7.3.

(7.3.1) If 2 is a unit in R, then U_R splits as $\langle 2\rangle_R \oplus \langle 2\rangle_R$.
(7.3.2) If 2 is not a unit in R, then U_R is indecomposable.

PROOF. The first statement is easily seen, using the new basis $\{s_1 + s_2, s_1 - s_2\}$. Assume 2 is not a unit in R. If U_R splits, it must split as a direct sum of 2 rank 1 quadratic R-modules, so $U_R \cong \langle a\rangle_R \oplus \langle b\rangle_R$ for some a, $b \in R$, in which case $\operatorname{disc}(U_R) = 4ab \mod (R^\times)^2$. Therefore, $4ab = -1 \mod (R^\times)^2$, so 2 must be a unit in R. Q.E.D.

EXAMPLE 7.4. *A_N, D_N, E_N and T_{pqr}.*

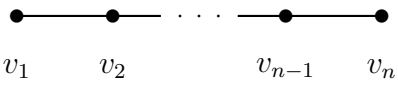
Let $R = \mathbb{Z}$ and let L be a free rank N $\mathbb{Z}$-module with basis $S = \{s_1, \dots, s_N\}$. Define a symmetric bilinear form $\langle -, -\rangle$ on L by setting $\langle s_i, s_i\rangle = -2$ for every i, $\langle s_i, s_{i+1}\rangle = 1$ for $i = 1, \dots, N-1$, and all other values $= 0$. This is an even bilinear form, so by 2.4, there is a unique quadratic form q on L inducing $\langle -, -\rangle$. The isomorphism class of this form is denoted by A_N.

The matrix of A_N in the above basis is tri-diagonal, with -2 entries on the main diagonal, $+1$ entries on the sub- and super-diagonals, and 0's elsewhere. Clearly $\operatorname{disc}(A_1) = -2$ and $\operatorname{disc}(A_2) = \det\left(\begin{smallmatrix}-2 & 1\\ 1 & -2\end{smallmatrix}\right) = +3$. By expansion along the first row, one easily checks that $\operatorname{disc}(A_{N+2}) = -2\operatorname{disc}(A_{N+1}) - \operatorname{disc}(A_N)$. Therefore, $\operatorname{disc}(A_N) = (-1)^N(N+1)$ for all N, as is easily proved by induction.

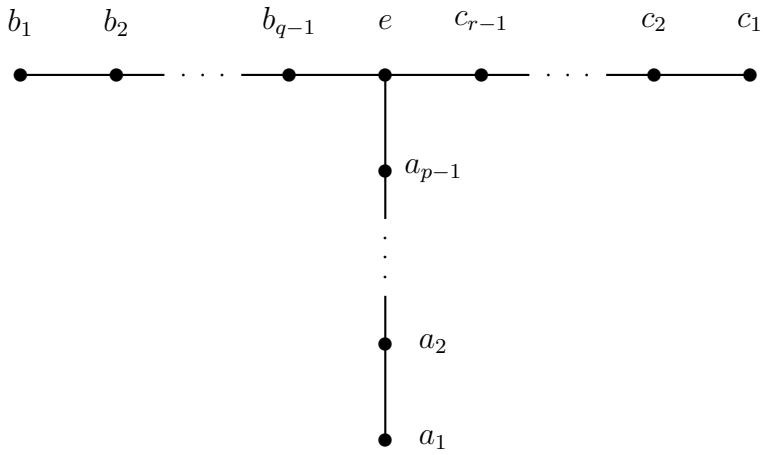
The A_N quadratic form is a special case of a more general construction. Let G be a simple graph, i.e., one without loops or multiple edges. Let L be the free $\mathbb{Z}$-module on the set of vertices. Define a bilinear form $\langle -, -\rangle$ on L by setting

$$\langle v, w\rangle = \begin{cases} -2 & \text{if } v = w \\ 1 & \text{if } v \neq w \text{ but } v \text{ and } w \text{ are adjacent in } G \\ 0 & \text{if } v \neq w \text{ and } v \text{ is not adjacent to } w \text{ in } G \end{cases}$$

for vertices v, w in G and extending by linearity. The form $\langle -, -\rangle$ is even and defines a quadratic form on L. The A_N form arises from the graph which is simply a path on N vertices:



The next level of complexity is obtained with the so-called T_{pqr} graphs, defined as the graph on $p+q+r-2$ vertices, labeled $a_1, \ldots, a_{p-1}, b_1, \ldots, b_{q-1}, c_1, \ldots, c_{r-}$ joined as follows:



Here p, q, $r \geq 1$, although if any equal 1, the graph reduces to a path, giving the A_N form. We usually order the indices so that $p \leq q \leq r$. In this case the T_{1qr} form is the A_{q+r-1} form. The matrix for the T_{222} form is $\begin{pmatrix} -2 & & & 1 \\ & -2 & & 1 \\ & & -2 & 1 \\ 1 & 1 & 1 & -2 \end{pmatrix}$, whose determinant is $+4$. In general, the same expansion as in the A_N case above yields

$$\operatorname{disc}(T_{p,q,r+2}) = -2\operatorname{disc}(T_{p,q,r+1}) - \operatorname{disc}(T_{p,q,r}).$$

Induction now easily shows that

$$\begin{aligned} \operatorname{disc}(T_{pqr}) &= (-1)^{p+q+r+1}[pqr - pq - pr - qr] \\ &= (-1)^{p+q+r+1}pqr\left[1 - \frac{1}{p} - \frac{1}{q} - \frac{1}{r}\right]. \end{aligned}$$

Note that this formula holds in case $p = 1$ also, i.e., for the A_N case.

Let us note when the T_{pqr} is degenerate and when it is unimodular. Firstly, T_{pqr} is degenerate if and only if $\operatorname{disc}(T_{pqr}) = 0$, i.e., when $1 = \frac{1}{p} + \frac{1}{q} + \frac{1}{r}$. Clearly T_{333} is degenerate and no T_{pqr} with $(p, q, r) > (3, 3, 3)$ (ordered lexicographically) is degenerate. Therefore, all other degenerate T_{pqr}'s have $p = 2$; an easy computation shows that T_{244} and T_{236} are the only other examples. These forms have special names: T_{333} is denoted by $\widetilde{E}_6$; T_{244} by $\widetilde{E}_7$; and T_{236} by $\widetilde{E}_8$.

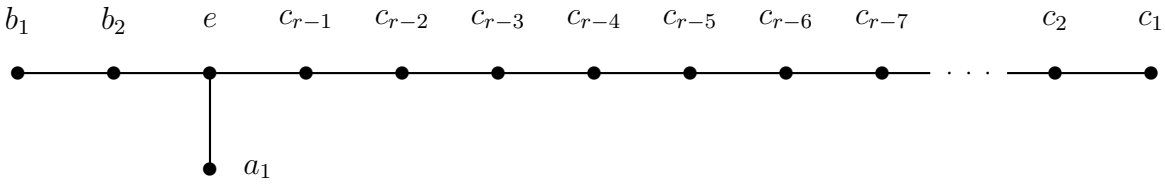
For T_{pqr} to be unimodular, we must have $pqr = pq + pr + qr \pm 1$; there are no solutions to this if $p \geq 3$; hence $p = 2$ and we must have

$qr = 2q + 2r \pm 1$, forcing $q \geq 3$. Therefore, $r = (2q \pm 1)/(q-2)$, and $r \geq q$ implies $q \leq 4$. For $q = 3$, $r = 5$ and $r = 7$ is a solution; there is none for $q = 4$. Hence the unimodular T_{pqr} forms are T_{235} and T_{237}; these are denoted by E_8 and E_{10}, respectively.

In general, T_{22r} is denoted by D_{r+2} and T_{23r} by E_{r+3}. Note that $\widetilde{E}_8 = E_9$.

The forms above which are negative definite are the A_N's, the D_N's, E_6, E_7 and E_8. All other nondegenerate T_{pqr} forms are indefinite. The graphs for these negative definite forms are the *Dynkin diagrams*.

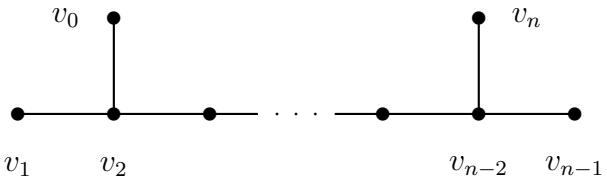
There are some non-obvious relationships among these forms. For example, if $r \geq 7$, $E_{r+3} = T_{23r} \cong E_8 \oplus U \oplus A_{r-7}$ (where, for $r = 7$, A_0 is the trivial form of rank 0). The graph for E_{r+3} is



The E_8 submodule is generated by a_1, b_1, b_2, c_{r-4}, c_{r-3}, c_{r-2}, c_{r-1} and e. Let $f = 3a_1 + 2b_1 + 4b_2 + 2c_{r-4} + 3c_{r-3} + 4c_{r-2} + 5c_{r-1} + 6e$. Then the U submodule is generated by $c_{r-5} + f$ and $c_{r-5} + c_{r-6} + f$. Since $\langle f, f\rangle = -2$, $\langle f, c_{r-5}\rangle = 2$, and $\langle f, c_{r-6}\rangle = 0$, $U \subset E_8^{\perp}$. Finally the A_{r-7} submodule is generated by $c_{r-7} - c_{r-5} - f, c_{r-6}, \ldots, c_2, c_1$, all of which are in $(U \oplus E_8)^{\perp}$.

Note that, in particular, the unimodular form E_{10} is isomorphic to $E_8 \oplus U$.

The forms $\widetilde{E}_6$, $\widetilde{E}_7$ and $\widetilde{E}_8$ all have exactly a rank one radical; modulo their radicals, they are isomorphic to E_6, E_7 and E_8, respectively. They are called the *extended* diagrams for E_6, E_7 and E_8. There are also extended diagrams for the other negative definite forms A_N and D_N, denoted also by $\widetilde{A}_N$ and $\widetilde{D}_N$. $\widetilde{A}_N$ is defined by the graph which is a cycle of $N+1$ vertices. $\widetilde{D}_N$ is defined by the following graph with $N+1$ vertices:



As is the case with $\widetilde{E}_6$, $\widetilde{E}_7$ and $\widetilde{E}_8$, these extended diagrams each have a rank-one radical and modulo their radicals $\widetilde{A}_N$ is isomorphic to A_N and $\widetilde{D}_N$ is isomorphic to D_N.

As special cases of the discriminant formula for the T_{pqr} forms, we have

$$\operatorname{disc}(D_N) = (-1)^N \cdot 4$$

and

$$\operatorname{disc}(E_N) = (-1)^{N+1}(N-9).$$

EXAMPLE 7.5. *Indecomposable rank-2 quadratic $\mathbb{Z}_2$-modules.*

Let L be a free rank 2 $\mathbb{Z}_2$-module with basis $S = \{s_1, s_2\}$. Define $Q : L \to \mathbb{Z}_2$ by $Q(a_1s_1 + a_2s_2) = 2^k a_1 a_2$. The associated bilinear form has matrix $\begin{pmatrix} 0 & 2^k \\ 2^k & 0 \end{pmatrix}$, and so Q is nondegenerate, and unimodular if $k = 0$. The isomorphism class of this quadratic form will be denoted by U_k.

Using the same $\mathbb{Z}_2$-module L and basis S, define a different quadratic form by $Q(a_1s_1+a_2s_2) = 2^k(a_1^2+a_1a_2+a_2^2)$. The associated bilinear form has matrix $\begin{pmatrix} 2^{k+1} & 2^k \\ 2^k & 2^{k+1} \end{pmatrix}$ with respect to S, so Q is nondegenerate and unimodular if $k = 0$. The isomorphism class of this quadratic form will be denoted by V_k.

Note that $\operatorname{disc}(U_k) = -2^{2k} \mod \mathbb{U}_{\not 2}^{\not 2}$ and $\operatorname{disc}(V_k) = 3 \cdot 2^{2k} \mod \mathbb{U}_{\not 2}^{\not 2}$; hence, none of these forms are isomorphic to any other.

LEMMA 7.6. *For all $k \geq 0$, U_k and V_k are indecomposable.*

PROOF. We will only prove that U_k is indecomposable, leaving the (similar) argument for the V_k's to the reader. Assume that U_k is represented by (L, Q) as above, and that (L, Q) splits as $M \oplus N$ where M and N are rank-1 quadratic $\mathbb{Z}_2$-modules generated by m and n, respectively. The set $T = \{m, n\}$ is then a basis for L and the matrix of Q with respect to T is $\begin{pmatrix} 2Q(m) & 0 \\ 0 & 2Q(n) \end{pmatrix}$, so that $\operatorname{disc}(U_k) = 4Q(m)Q(n) \mod \mathbb{U}_{\not 2}^{\not 2}$. Since 2^k divides every value of Q, 2^{2k+2} divides $\operatorname{disc}(U_k)$. Since $\operatorname{disc}(U_k) = -2^{2k} \mod \mathbb{U}_{\not 2}^{\not 2}$, this contradiction proves the indecomposability. Q.E.D.

Let us show that these are the only indecomposable rank-2 quadratic $\mathbb{Z}_2$-modules, up to isomorphism.

LEMMA 7.7. *Let (L, Q) be an indecomposable rank-2 quadratic $\mathbb{Z}_2$-module.*

(7.7.1) Assume that there is a nonzero $x \in L$ with $Q(x) = 0$. Then $(L, Q) \cong U_k$ for some $k \geq 0$.

(7.7.2) Assume that there is no nonzero x in L with $Q(x) = 0$. Then $(L, Q) \cong V_k$ for some $k \geq 0$.

(7.7.3) As an alternate characterization, $(L, Q) \cong U_k$ if and only if $\mathrm{disc}(L, Q) = 2^{2k} \cdot \delta$ for some odd δ with $\left(\frac{2}{\delta}\right) = 1$, while $(L, Q) \cong V_k$ if and only if $\mathrm{disc}(L, Q) = 2^{2k} \cdot \delta$ for some odd δ with $\left(\frac{2}{\delta}\right) = -1$.

PROOF. To prove the first statement, let $Q(x) = 0$. We may assume $x \notin 2L$, so $\{x\}$ can be extended to a basis $\{x, y\}$ for L over $\mathbb{Z}_2$. Let $\langle x, y\rangle = 2^k u$, with $u \in \mathbb{U}_{\not 2}$; by replacing y by $u^{-1}y$, we may assume $\langle x, y\rangle = 2^k$ for some $k \geq 0$. Write $\langle y, y\rangle = r$. If $r|2^k$, then the span of y splits off L: $\{y\}^\perp =$ span of $x-(2^k/r)y$, and $\{x-(2^k/r)y, y\}$ also forms a basis for L. Since L is indecomposable, $2^{k+1}|r$, and by replacing y by $y - (r/2^{k+1})x$, the matrix for Q becomes $\left(\begin{smallmatrix} 0 & 2^k \\ 2^k & 0 \end{smallmatrix}\right)$; hence, by Corollary 2.5, $(L, Q) \cong U_k$.

For the second statement, we may assume that there is a basis $S = \{x, y\}$ for L such that the matrix of Q with respect to S is $\left(\begin{smallmatrix} r & 2^k \\ 2^k & s \end{smallmatrix}\right)$. If $r|2^k$, then the span of x splits off L and if $s|2^k$, the span of y splits off L by an argument similar to the above. Hence, we may assume 2^{k+1} divides both r and s. Therefore, 2^k divides every value of Q; by replacing Q by $2^{-k}Q$, we may assume $k = 0$. We must show that (L, Q) represents V_0. Now the matrix of Q with respect for S is $\left(\begin{smallmatrix} r & 1 \\ 1 & s \end{smallmatrix}\right)$, with r and s even; write $r = 2u$ and $s = 2v$.

Claim: u and v are both odd.

Assume, for example, that v is even; write $v = 2^L w$, where w is a unit and $L \geq 1$. Replace y by $y' = 2^L x + (1 - 2^{L+1}u)y$. Then $\langle x, y'\rangle = 2^L \cdot 2u + (1 - 2^{L+1}u) \cdot 1 = 1$ still, and

$$\begin{aligned} \langle y', y'\rangle &= 2^{2L} \cdot 2u + 2 \cdot 2^L(1 - 2^{L+1}u) + (1 - 2^{L+1}u)^2 \cdot 2^{L+1}w \\ &= 2^{L+1}[2^L u + 1 - 2^{L+1}u + w - 2^{L+2}uw + 2^{2l+2}u^2] \end{aligned}$$

which is divisible by 2^{L+2} since w is odd. By iterating this operation, we achieve a sequence of bases $\{x, y^{(i)}\}$ such that $\|\langle y^{(i)}, y^{(i)}\rangle\|_2 \to 0$. Moreover, the sequence $y^{(i)}$ converges to y_∞ in L and $Q(y_\infty) = 0$, contradicting the hypotheses on L. This proves the claim.

Write $v = 1+2^L w$ where w is a unit in $\mathbb{Z}_2$ and $L \geq 1$. Again replace y by $y' = 2^L x + (1 - 2^{L+1}u)y$. We still have $\langle x, y' \rangle = 1$ and

$$\begin{aligned} \langle y', y' \rangle &= 2^{2L} \cdot 2u + 2^{L+1}(1 - 2^{L+1}u) + (1 - 2^{L+1}u)^2 \cdot 2(1 + 2^L w) \\ &= 2[2^{2L}u + 2^L - 2^{2L+1}u + 1 - 2^{L+1}u + 2^L w - 2^{2L+1}uw] \\ &= 2[1 + 2^{L+1}w'] \end{aligned}$$

since w is odd.

By iterating this operation, we obtain a sequence of bases $\{x, y^{(i)}\}$ such that

$$\|\langle y^{(i)}, y^{(i)} \rangle - 2\|_2 \to 0.$$

Moreover, the sequence $y^{(i)}$ converges to y_∞ in L, $\{x, y_\infty\}$ is a basis for L, and the matrix of Q with respect to this basis is $\left(\begin{smallmatrix} r & \frac{1}{2} \\ 1 & \end{smallmatrix}\right)$.

By reversing the roles of x and y, we obtain (again by iteration) a basis $\{x_\infty, y_\infty\}$ for L such that the matrix of Q with respect to this basis is $\left(\begin{smallmatrix} 2 & \frac{1}{2} \\ 1 & \end{smallmatrix}\right)$, proving the second statement by Corollary 2.5.

To prove the alternate characterization in the third part, note that (L, Q) must be isomorphic to U_k or V_k for some k. But $\mathrm{disc}(U_k) = 2^{2k} \cdot (-1)$ and $\left(\frac{2}{-1}\right) = 1$, while $\mathrm{disc}(V_k) = 2^{2k} \cdot 3$ and $\left(\frac{2}{3}\right) = -1$. Thus, the isomorphism classes of these forms are determined by the discriminant. Q.E.D.

Example 7.8. *Cyclic torsion bilinear forms over $\mathbb{Z}$.*

In this section we want to briefly introduce the nondegenerate $\mathbb{Q}/\mathbb{Z}$-valued symmetric bilinear forms over $\mathbb{Z}$ on $G \cong \mathbb{Z}/\ell$. If g generates G, then any such bilinear form must be of the form $\langle xg, yg \rangle = xya/\ell \mod \mathbb{Z}$, where $(a, \ell) = 1$, $a \in \mathbb{Z}$. The form $\langle\ ,\ \rangle$ depends only on the class of $a \mod \ell$), so we may consider $a \in (\mathbb{Z}/\ell)^\times$. Moreover, a and a' induce isomorphic bilinear forms if and only if there is a unit $u \in (\mathbb{Z}/\ell)^\times$ such that $a' = u^2 a \mod \ell$. Therefore, these bilinear forms are classified by $(\mathbb{Z}/\ell)^\times/((\mathbb{Z}/\ell)^\times)^2 = \mathcal{D}(\mathbb{Z}/\ell)$. This form will be denoted by $\bar{z}_\ell^a$.

Again we want to be more specific in case ℓ is a prime power $\ell = p^k$. First assume p is odd. Assume that the bilinear form has the form $\langle xg, yg \rangle = xya/p^k$, for a generator g of $\mathbb{Z}/p^k$. We denote this form by $\bar{w}_{p,k}^\varepsilon$, where $\varepsilon = \left(\frac{a}{p}\right) = \chi(a)$. Here $\varepsilon \in \{\pm 1\}$.

Assume $p = 2$. Then the bilinear form has the form $\langle xg, yg \rangle = xya/2^k$. We denote this form by $\bar{w}_{2,k}^\varepsilon$, where $\varepsilon = \chi(a \bmod 2^k)$. Here $\varepsilon \in (\mathbb{Z}/2)^\times = \{1\}$ if $k = 1$; $\varepsilon \in (\mathbb{Z}/4)^\times = \{1, 3\}$ if $k = 2$; and $\varepsilon \in (\mathbb{Z}/8)^\times = \{1, 3, 5, 7\}$ if $k \geq 3$.

Example 7.9. *Cyclic torsion quadratic forms over $\mathbb{Z}$.*

Let $G = \mathbb{Z}/\ell$ be a cyclic group of order ℓ with generator g. Fix $a \in \mathbb{Z}$ with (a, ℓ) = 1 and $a\ell \in 2\mathbb{Z}$. Define $q : G \to \mathbb{Q}/\mathbb{Z}$ by $q(rg) = r^2 a/2\ell \mod \mathbb{Z}$. This is well defined since $a\ell$ is even. The associated bilinear form $\langle xg, yg\rangle = xya/\ell \mod \mathbb{Z}$ is nondegenerate since (a, ℓ) = 1, so q is nondegenerate, hence unimodular. The isomorphism class of this finite quadratic form will be denoted by z_ℓ^a.

Note that if $a \equiv b \mod 2\ell$, then $z_\ell^a \cong z_\ell^b$, so z_ℓ^a only depends on the class of a mod 2ℓ. If ℓ is even, then there are $2\varphi(\ell)$ possible classes for a mod 2ℓ satisfying (a, ℓ) = $1(a\ell \in 2\mathbb{Z}$ is automatic); if ℓ is odd, there are $\varphi(\ell)$ possibilities for a mod 2ℓ, since in addition to (a, ℓ) = 1, a must be even. ($\varphi(\ell)$ is the Euler phi function.)

For these possible values for a mod 2ℓ, multiplication by squares of units in $\mathbb{Z}/\ell$ is well defined. To check this, let $u \in (\mathbb{Z}/\ell)^\times$ and first assume ℓ is even. Then

$$\begin{aligned}(u+\ell)^2 a \mod 2\ell &= u^2 a + 2\ell u a + \ell^2 a \mod 2\ell \\ &= u^2 a + \ell^2 a \mod 2\ell \\ &= u^2 a \mod 2\ell\end{aligned}$$

since for ℓ even, $\ell^2 \equiv 0 \mod 2\ell$. Now assume ℓ is odd; then $(u+\ell)^2 a \mod 2\ell = u^2 a + \ell^2 a \mod 2\ell = u^2 a \mod 2\ell$ since a is even.

Therefore, if a and b are allowable values as above, then $z_\ell^a \cong z_\ell^b$ if and only if there is a unit $u \in (\mathbb{Z}/\ell)^\times$ such that $b = u^2 a \mod 2\ell$.

We can be more specific if ℓ is a prime power, say $\ell = p^k$.

If $p = 2$, then the allowable values for $a \mod 2^{k+1}$ are the units $(\mathbb{Z}/2^{k+1})^\times$, and the class of $a \mod ((\mathbb{Z}/2^k)^\times)^2$ determines the isomorphism class of the form $z_{2^k}^a$. Hence the set $(\mathbb{Z}/2^{k+1})^\times/((\mathbb{Z}/2^k)^\times)^2$ classifies finite quadratic form on $\mathbb{Z}/2^k$. Note that this set is in 1-1 correspondence with $\mathcal{D}(\mathbb{Z}/2^{k+1})$; hence we will use this group to classify the finite quadratic forms in this case. We denote the isomorphism class of $z_{2^k}^a$ by $w_{2,k}^\varepsilon$, where $\varepsilon = \chi(a)$. Hence if $k = 1$, $\varepsilon \in (\mathbb{Z}/4)^\times = \{1, 3\}$; if $k \geq 2$, $\varepsilon \in (\mathbb{Z}/8)^\times = \{1, 3, 5, 7\}$.

If p is odd, the allowable values for $a \mod 2p^k$ are the even units of $(\mathbb{Z}/2p^k)^\times$, which are in 1-1 correspondence with the units of $\mathbb{Z}/p^k$. Hence, the group $\mathcal{D}(\mathbb{Z}/p^k)$ classifies finite quadratic forms on $\mathbb{Z}/p^k$. We denote the isomorphism class of $z_{p^k}^a$ by $w_{p,k}^\varepsilon$, where $\varepsilon = \chi(a \bmod p^k)$.

With this notation, we have that the associated bilinear form to $w_{p,k}^\varepsilon$ is $\bar{w}_{p,k}^\varepsilon$, where if $p = 2$ and $k \leq 2$, the ε's are only "equal" mod 2^k.

EXAMPLE 7.10. *Indecomposable finite quadratic forms on* $\mathbb{Z}/2^k \times \mathbb{Z}/2^k$.

Let $G = \mathbb{Z}/2^k \times \mathbb{Z}/2^k$, with generators x, y of order 2^k. Define $q : G \to \mathbb{Q}/\mathbb{Z}$ by $q(ax + by) = 2^{-k}ab \mod \mathbb{Z}$. The reader can check that q is a well-defined nondegenerate quadratic form on G, which is in fact indecomposable. The isomorphism class of this quadratic form will be denoted by u_k.

On the same group G, define a different quadratic form $q : G \to \mathbb{Q}/\mathbb{Z}$ by $q(ax+by) = 2^{-k}(a^2+ab+b^2) \mod \mathbb{Z}$. This form is well defined and nondegenerate and is also indecomposable; its isomorphism class will be denoted by v_k.

In keeping with the notations of Examples 7.8 and 7.9, we will denote by $\bar{u}_k$ (respectively $\bar{v}_k$) the isomorphism class of the associated bilinear form on G to u_k (respectively to v_k).

EXAMPLE 7.11. *Negation.*

Let (L, Q) be an F-valued quadratic form over R. Then $(L, -Q)$ is also an F-valued quadratic form over R, which is nondegenerate (respectively unimodular) if (L, Q) is. If (L, Q) is denoted by L, then $(L, -Q)$ will be denoted by $-L$.

Note that $-\langle a\rangle_R \cong \langle -a\rangle_R$ and $-U_R \cong U_R$. For $R = \mathbb{Z}_2$, we have $-U_k \cong U_k$ and $-V_k \cong V_k$; for $R = \mathbb{Z}_p$, $-W^{\varepsilon}_{p,k} \cong W^{-\varepsilon}_{p,k}$. For the finite quadratic forms, we have $-w^{\varepsilon}_{p,k} \cong w^{-\varepsilon}_{p,k}$, $-u_k \cong u_k$ and $-v_k \cong v_k$.

We now want to briefly discuss the elementary theory of quadratic vector spaces over $\mathbb{R}$. By Proposition (5.8), Lemma (3.6.3), and Example 7.1, every such form is isomorphic to $\langle 1\rangle_{\mathbb{R}}^{\oplus s_+} \oplus \langle -1\rangle_{\mathbb{R}}^{\oplus s_-}$ for integers $s_+, s_- \geq 0$. By Sylvester's theorem, the pair (s_+, s_-) is determined by the form.

DEFINITION 7.12. Let (L, Q) be a quadratic vector space over $\mathbb{R}$. Assume that $(L, Q) \cong \langle 1\rangle_{\mathbb{R}}^{\oplus s_+} \oplus \langle -1\rangle_{\mathbb{R}}^{\oplus s_-}$. The *signature* of (L, Q) is the pair (s_+, s_-). (L, Q) is *positive definite* if $s_- = 0$, (L, Q) is *negative definite* if $s_+ = 0$, and (L, Q) is *definite* if $s_+ s_- = 0$; (L, Q) is *indefinite* if $s_+ s_- \neq 0$.

COROLLARY 7.13. *Two quadratic vector spaces over* $\mathbb{R}$ *are isomorphic if and only if they have the same rank and signature.*

With the above language at our disposal, the signature of a quadratic vector space (L, Q) over $\mathbb{R}$ can be described as follows: s_+ is the dimension of a maximal subspace $P \subset L$ on which Q is positive definite; s_- is the dimension of a maximal subspace $N \subset L$ on which Q is negative definite.

Ring	Notation	Rank	Definition	Discriminant
R	$\langle a\rangle_R$	1	$Q(r) = ar^2$	$2a \mod (R^\times)^2$
$\mathbb{Z}$	$\langle a\rangle$	1	$Q(r) = ar^2$	$2a$
$\mathbb{Z}_p$, p odd	$W^1_{p,k}$	1	$Q(r) = p^k r^2/2$	$p^k \mod \mathbb{U}_{\text{ı}}^{\not\square}$
$\mathbb{Z}_p$, p odd	$W^{-1}_{p,k}$	1	$Q(r) = p^k r^2 u/2$, $u \in \mathbb{U}_{\text{ı}} - \mathbb{U}_{\text{ı}}^{\not\square}$	$p^k u \mod \mathbb{U}_{\text{ı}}^{\not\square}$
$\mathbb{Z}_2$	$W^1_{2,k}$	1	$Q(r) = 2^{k-1} r^2$	$2^k \mod \mathbb{U}_{\not\square}^{\not\square}$
$\mathbb{Z}_2$	$W^3_{2,k}$	1	$Q(r) = 3 \cdot 2^{k-1} r^2$	$3 \cdot 2^k \mod \mathbb{U}_{\not\square}^{\not\square}$
$\mathbb{Z}_2$	$W^5_{2,k}$	1	$Q(r) = 5 \cdot 2^{k-1} r^2$	$5 \cdot 2^k \mod \mathbb{U}_{\not\square}^{\not\square}$
$\mathbb{Z}_2$	$W^7_{2,k}$	1	$Q(r) = 7 \cdot 2^{k-1} r^2$	$7 \cdot 2^k \mod \mathbb{U}_{\not\square}^{\not\square}$
R	U_R	2	$Q(r,s) = rs$	$-1 \mod (R^\times)^2$
$\mathbb{Z}_2$	U_k	2	$Q(r,s) = 2^k rs$	$-2^{2k} \mod \mathbb{U}_{\not\square}^{\not\square}$
$\mathbb{Z}_2$	V_k	2	$Q(r,s) = 2^k(r^2 + rs + s^2)$	$3 \cdot 2^{2k} \mod \mathbb{U}_{\not\square}^{\not\square}$

TABLE 7.1. Basic Examples of Quadratic R-modules

Note that (L, Q) is positive (respectively negative) definite if and only if whenever $x \in L$ and $x \neq 0$, then $Q(x) \gneqq 0$ (respectively $Q(x) \lneqq 0$).

EXAMPLE 7.14. *Expansion.*

Let (L, Q) be an F-valued quadratic form over R, and let $r \in R$. Then (L, rQ) is an F-valued quadratic form over R. If r is a unit of R, then rQ is nondegenerate if Q is, and rQ is unimodular if Q is. If multiplication by r is injective on F, then rQ is nondegenerate if Q is. If the symbol A denotes the isomorphism class of (L, Q), we will use the symbol $A(r)$ for the isomorphism class of (L, rQ).

For example, $\langle a\rangle_R(r) \cong \langle ar\rangle_R$. In particular, $U_k(2^L) \cong U_{k+L}$ and $V_k(2^L) \cong V_{k+L}$.

We collect the examples of this section in the nearby tables for convenience.

8. Change of Rings

Let $(L,\ Q)$ be an F-valued quadratic form over R. Let S be an R-algebra. Define $Q_S : L \otimes_R S \to F \otimes_R S$ by

$$Q_S(\sum_i x_i \otimes s_i) = \sum_{i<j} \langle x_i, x_j\rangle_Q \otimes s_i s_j + \sum_i Q(x_i) \otimes s_i^2.$$

We leave it to the reader to verify that Q_S is well defined, and that it is an $(F \otimes_R S)$-valued quadratic form over S on $L \otimes_R S$. The associated bilinear form to Q_S has the form $\langle x \otimes s, y \otimes t\rangle_{Q_S} = \langle x, y\rangle_Q \otimes st$. It is immediate that the adjoint map $\operatorname{Ad} Q_S : L \otimes_R S \to \operatorname{Hom}_S(L \otimes_R S, F \otimes_R$

G	Notation	Definition
$\mathbb{Z}/\ell = \langle g \rangle$	$\bar{z}^a_\ell$	$\langle xg, yg \rangle = xya/\ell$
$\mathbb{Z}/p^k$, p odd	$\bar{w}^1_{p,k}$	$\langle xg, yg \rangle = xy/p^k$
$\mathbb{Z}/p^k$, p odd	$\bar{w}^{-1}_{p,k}$	$\langle xg, yg \rangle = xya/p^k$ where a is not a square mod p
$\mathbb{Z}/2$	$\bar{w}^1_{2,1}$	$\langle xg, yg \rangle = xy/2$
$\mathbb{Z}/4$	$\bar{w}^1_{2,2}$	$\langle xg, yg \rangle = xy/4$
$\mathbb{Z}/4$	$\bar{w}^3_{2,2}$	$\langle xg, yg \rangle = 3xy/4$
$\mathbb{Z}/2^k$, $k \geq 3$	$\bar{w}^1_{2,k}$	$\langle xg, yg \rangle = xy/2^k$
$\mathbb{Z}/2^k$, $k \geq 3$	$\bar{w}^3_{2,k}$	$\langle xg, yg \rangle = 3xy/2^k$
$\mathbb{Z}/2^k$, $k \geq 3$	$\bar{w}^5_{2,k}$	$\langle xg, yg \rangle = 5xy/2^k$
$\mathbb{Z}/2^k$, $k \geq 3$	$\bar{w}^7_{2,k}$	$\langle xg, yg \rangle = 7xy/2^k$
$\mathbb{Z}/2^k \times \mathbb{Z}/2^k$	$\bar{u}_k$	$\langle (x_1, x_2), (y_1 y_2) \rangle = (x_1 y_2 + x_2 y_1)/2^k$
$\mathbb{Z}/2^k \times \mathbb{Z}/2^k$	$\bar{v}_k$	$\langle (x_1, x_2), (y_1, y_2) \rangle = (2x_1 y_1 + 2x_2 y_2 + x_1 y_2 + x_2 y_1)/2^k$

TABLE 7.2. Basic Examples of Torsion Bilinear Forms
$\langle -, - \rangle : G \times G \to \mathbb{Q}/\mathbb{Z}$ over $\mathbb{Z}$

G	Notation	Definition
$\mathbb{Z}/\ell = \langle g \rangle$	z^a_ℓ	$q(rg) = r^2 a/2\ell$, $(a, \ell) = 1$ and $a\ell \in 2\mathbb{Z}$
$\mathbb{Z}/p^k$, p odd	$w^1_{p,k}$	$q(rg) = r^2 u/p^k$ where 2u is a square mod p
$\mathbb{Z}/p^k$, p odd	$w^{-1}_{p,k}$	$q(rg) = r^2 u/p^k$ where 2u is not a square mod p
$\mathbb{Z}/2$	$w^1_{2,1}$	$q(rg) = r^2/4$
$\mathbb{Z}/2$	$w^3_{2,1}$	$q(rg) = 3r^r/4$
$\mathbb{Z}/2^k$, $k \geq 2$	$w^1_{2,k}$	$q(rg) = r^2/2^{k+1}$
$\mathbb{Z}/2^k$, $k \geq 2$	$w^3_{2,k}$	$q(rg) = 3r^2/2^{k+1}$
$\mathbb{Z}/2^k$, $k \geq 2$	$w^5_{2,k}$	$q(rg) = 5r^2/2^{k+1}$
$\mathbb{Z}/2^k$, $k \geq 2$	$w^7_{2,k}$	$q(rg) = 7r^2/2^{k+1}$
$\mathbb{Z}/2^k \times \mathbb{Z}/2^k$	u_k	$q(r, s) = rs/2^k$
$\mathbb{Z}/2^k \times \mathbb{Z}/2^k$	v_k	$q(r, s) = (r^2 + rs + s^2)/2^k$

TABLE 7.3. Basic Examples of Torsion Quadratic Forms
$q : G \to \mathbb{Q}/\mathbb{Z}$ over $\mathbb{Z}$

S) is simply the composition of $\operatorname{Ad} Q \otimes 1 : L \otimes_R S \to \operatorname{Hom}_R(L, F) \otimes_R S$ with the natural map $\alpha : \operatorname{Hom}_R(L, F) \otimes_R S \to \operatorname{Hom}_S(L \otimes_R S, F \otimes_R S)$. Therefore, if α is injective, then Q nondegenerate implies Q_S is nondegenerate. Moreover, if α is an isomorphism then Q unimodular implies Q_S is unimodular. Fortunately, these are often the case. In particular, if L is a finitely generated free R-module and $F = R$, then α is an isomorphism. Therefore:

PROPOSITION 8.1. *If (L, Q) is a quadratic R-module, then $(L \otimes_R S, Q_S)$ is a quadratic S-module. Moreover, if (L, Q) is unimodular, so is $(L \otimes_R S, Q_S)$.*

We will often abbreviate $L \otimes_R S$ to L_S.

We should also analyze the behavior of the discriminant under change of rings. Let $f : R \to S$ be the structure map. We'll assume that both R and S are integral domains. The map f induces a natural map from $R^\times$ to $S^\times$, sending $(R^\times)^2$ into $(S^\times)^2$, so we get a natural function

$$\bar{f} : (R - \{0\})/(R^\times)^2 \to (S - \{0\})/(S^\times)^2.$$

LEMMA 8.2. *Let (L, Q) be a quadratic R-module. Then $\bar{f}(\mathrm{disc}(L)) = \mathrm{disc}(L_S)$.*

PROOF. Let $E = \{e_1, \ldots, e_N\}$ be a basis for L over R and assume that the matrix of Q with respect to E is $A = (a_{ij})$. Then $E \otimes 1 = \{e_1 \otimes 1, \ldots, e_N \otimes 1\}$ is a basis for L_S over S, and the matrix of Q_S with respect to $E \otimes 1$ is $A_S = (f(a_{ij}))$. Then

$$\begin{aligned} \mathrm{disc}(L_S) &= \det\ A_S \mod (S^\times)^2 \\ &= f(\det\ A) \mod (S^\times)^2 \\ &= \bar{f}(\mathrm{disc}(L)). \end{aligned}$$

Q.E.D.

We will again use special notation in the most important cases. If $R = \mathbb{Z}$ and $S = \mathbb{Z}_p$, we will denote by L_p the quadratic $\mathbb{Z}_p$-module $L \otimes_{\mathbb{Z}} \mathbb{Z}_p$.

It will also be useful, when dealing with the change of rings from $\mathbb{Z}$ to $\mathbb{Z}_p$, or $\mathbb{Z}$ to $\mathbb{Q}$, or $\mathbb{Z}$ to $\mathbb{R}$, etc., to consider L as embedded in L_p, $L_{\mathbb{Q}}$ or $L_{\mathbb{R}}$, and the original quadratic form Q as the restriction of Q_p, $Q_{\mathbb{Q}}$ or $Q_{\mathbb{R}}$.

DEFINITION 8.3. Let (L, Q) be an integral quadratic form. The *signature* of (L, Q) is the signature of $(L_{\mathbb{R}}, Q_{\mathbb{R}})$.

Finally, let us analyze the behavior of finite quadratic forms under the change of rings from $\mathbb{Z}$ to $\mathbb{Z}_p$. Let (G, q) be a finite quadratic form with values in $\mathbb{Q}/\mathbb{Z}$. Then $G \otimes_{\mathbb{Z}} \mathbb{Z}_p = G_p$ is the Sylow p-subgroup of G and $\mathbb{Q}/\mathbb{Z} \otimes_{\mathbb{Z}} \mathbb{Z}_p \cong \mathbb{Q}^{(p)}/\mathbb{Z} (\cong \mathbb{Q}_p/\mathbb{Z}_p)$; the induced form (G_p, q_p) upon change of rings from $\mathbb{Z}$ to $\mathbb{Z}_p$ is simply the restriction of q to G_p, with values considered in $\mathbb{Q}^{(p)}/\mathbb{Z}$.

9. Isometries

Let (L, Q) be an F-valued quadratic form over R.

DEFINITION 9.1. The *orthogonal group of* L, denoted by $\mathcal{O}(L)$ (or $\mathcal{O}(Q)$, or $\mathcal{O}(L, Q)$) is the group of automorphisms of (L, Q), i.e., the group of self-isometries under composition.

As usual, in case (L, Q) is a quadratic R-module, $\mathcal{O}(L)$ can be described in terms of matrices.

LEMMA 9.2. *Assume 2 is not a zero-divisor in R. Let (L, Q) be a quadratic R-module with basis S and let A be the $N \times N$ matrix of Q with respect to S. Then $\mathcal{O}(L, Q)$ is isomorphic to the group of invertible $N \times N$ matrices B over R satisfying $B^\top AB = A$.*

PROOF. These matrices are the matrices of automorphisms of L which preserve the associated bilinear form to Q. Since 2 is not a zero-divisor in R, any automorphism of $\langle\ ,\ \rangle_Q$ will automatically be an automorphism of Q. Q.E.D.

COROLLARY 9.3. *Let R be an integral domain and (L, Q) a quadratic R-module. Assume $\sigma \in \mathcal{O}(L)$. Then the determinant of σ is either 1 or -1.*

PROOF. Let B be the matrix of σ with respect to a basis S of L so that $B^\top AB = A$, where A is the matrix of Q with respect to S. Then $\det(B)^2 \det(A) = \det(A)$, so $\det(B)^2 = 1$ or $\det(B) = \pm 1$ since R is a domain. Q.E.D.

Let us collect in the following Lemma the orthogonal groups of the standard quadratic R-modules from Section 7.

LEMMA 9.4.

(9.4.1) $\mathcal{O}(W_{p,k}^{\varepsilon}) = \pm I$

(9.4.2) $\mathcal{O}(U_k) = \left\{ \begin{pmatrix} u & 0 \\ 0 & u^{-1} \end{pmatrix}, \begin{pmatrix} 0 & u \\ u^{-1} & 0 \end{pmatrix} | u \in \mathbb{U}_{\not\models} \right\}$

(9.4.3) $\mathcal{O}(V_k) = \left\{ \begin{pmatrix} a & -c \\ c & a+c \end{pmatrix}, \begin{pmatrix} a & a+c \\ c & -a \end{pmatrix} | a, c \in \mathbb{Z}_{\not\models}, \beth^{\not\models} + \beth + \daleth^{\not\models} = \daleth \not\models \right\}$

PROOF. The first statement is obvious, and the second follows easily by noting that if one chooses a basis $\{x, y\}$ such that the form is $Q(rx, sy) = 2^k rs$, then the only elements z of U_k with $Q(z) = 0$ are multiples of x and y. The final statement is a bit more involved. Choose a basis $\{x, y\}$ of V_k such that the form is $Q(rx + sy) = 2^k(r^2 + rs + s^2)$. Assume $\sigma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathcal{O}(V_k)$. From the equations $Q(x) = Q(\sigma(x))$,

$Q(y) = Q(\sigma(y))$, and $Q(x+y) = Q(\sigma(x+y))$, we are led to the equations

$$a^2 + ac + c^2 = 1,$$
$$b^2 + bd + d^2 = 1,$$
$$ad + bc + 2ab + 2cd = 1.$$

Therefore at least one of a or c must be odd. Let us assume first that a is odd. The third equation may be written as

$$b(c+2a) + d(a+2c) = 1;$$

since a is odd, $a+2c$ is a unit, so that

$$d = (a+2c)^{-1}(1 - bc - 2ab).$$

Substitute this in for d in the second equation, multiply through by $(a+2c)^2$, and collect terms; one obtains

$$a^2 + 4ac + 4c^2 = 3a^2b^2 + 3ab^2c + 3b^2c^2 - 3ab + 1,$$

so that

$$3ac + 3c^2 = 3b^2 - 3ab,$$

using the first equation. Dividing by 3and re-arranging gives $(b+c)(b-a-c) = 0$. Now one of $b+c$ and $b-a-c$ must be a unit: if both were even, then their difference $a+2c$ would be even, contrary to hypothesis. Therefore either $b+c=0$ or $b=a+c$; these two possibilities lead to the matrix forms given above.

If a is even, then c must be odd, and the analogous argument with the roles of a and c, b and d reversed, gives the same result. Q.E.D.

Essentially identical arguments serve to compute the orthogonal groups for the standard torsion quadratic forms introduced in Section 7. We just present the results, leaving the details to the reader.

LEMMA 9.5.

(9.5.1) $\mathcal{O}(w_{2,1}^{\varepsilon})$ *is a trivial group.*

(9.5.2) $\mathcal{O}(w_{p,k}^{\varepsilon}) = \pm I$ *if* p *is odd or if* $k \geq 2$.

(9.5.3) $\mathcal{O}(u_k) = \left\{ \begin{pmatrix} u & 0 \\ 0 & u^{-1} \end{pmatrix}, \begin{pmatrix} 0 & u \\ u^{-1} & 0 \end{pmatrix} | u \in (\mathbb{Z}/\not\vDash^{\urcorner}\mathbb{Z})^{\otimes} \right\}$

(9.5.4) $\mathcal{O}(v_k) = \left\{ \begin{pmatrix} a & -c \\ c & a+c \end{pmatrix}, \begin{pmatrix} a & a+c \\ c & -a \end{pmatrix} | a, c \in \mathbb{Z}/\not\vDash^{\urcorner}\mathbb{Z}, \supset^{\not\vDash} + \supset + {}^{\not\vDash} = \not\Vdash \right\}$

DEFINITION 9.6. Let (L, Q) be a quadratic R-module where R is an integral domain. Let $\sigma \in \mathcal{O}(L)$. Define $\det(\sigma) = \begin{cases} + & \text{if the determinant of } \sigma \text{ is 1} \\ - & \text{if the determinant of } \sigma \text{ is -1.} \end{cases}$ Hence, $\det(\sigma)$ takes values in the 2-element group $\{+, -\}$ with identity $+$. (We use this notation simply for the convenience of using $+$ and $-$

as super- and sub-scripts to denote various subgroups of $\mathcal{O}(L)$. This will be explained further in Sections 10 and 11.) Note that det is a group homomorphism from $\mathcal{O}(L)$ to $\{+,-\}$. The kernel of det will be denoted by $\mathcal{O})^+(L,Q)$.

There is one type of isometry of fundamental importance, namely the reflection. Let R be an integral domain where $2 \neq 0$, (L,Q) a quadratic R-module, and x an element of L such that $Q(x)$ divides $\langle x,y\rangle$ for all y in L.

DEFINITION 9.7. The *reflection of* x, denoted by τ_x, is the map $\tau_x : L \to L$ defined by $\tau_x(y) = y - \frac{\langle x,y\rangle}{Q(x)}x$.

LEMMA 9.8.

(9.8.1) τ_x *is an isometry of* L *of order 2.*
(9.8.2) $\det(\tau_x) = -$.
(9.8.3) If $y \in \{x\}^\perp$, *then* $\tau_x(y) = y$.
(9.8.4) $\tau_x(x) = -x$.
(9.8.5) For any $\lambda \in R^\times$, $\tau_{\lambda x} = \tau_x$.

PROOF. Statements (9.8.3) and (9.8.5) are immediate and statement (9.8.4) follows from $\langle x,x\rangle = 2Q(x)$. Clearly τ_x is R-linear and

$$\tau_x(\tau_x(y)) = \tau_x(y - \frac{\langle x,y\rangle}{Q(x)}x) = \tau_x(y) - \frac{\langle x,y\rangle}{Q(x)}\tau_x(x) = y,$$

so τ_x is of order 2 and hence is a bijection. To see that τ_x is an isometry, compute

$$\begin{aligned} Q(\tau_x(y)) &= Q(y - \frac{\langle x,y\rangle}{Q(x)}x) \\ &= \langle y, \frac{-\langle x,y\rangle}{Q(x)}x\rangle + Q(y) + Q\left(\frac{-\langle x,y\rangle}{Q(x)}x\right) \\ &= \frac{-\langle x,y\rangle}{Q(x)}\langle y,x\rangle + Q(y) + \frac{\langle x,y\rangle^2}{Q(x)^2}Q(x) \\ &= Q(y). \end{aligned}$$

This proves (9.8.1).

To prove (9.8.2), we may tensor with the fraction field K of R; the determinant of τ_x is unchanged by this. We claim in this case that $L \otimes_R K$ splits as $M \oplus M^\perp$, where M is the span of x. To see that $L = M + M^\perp$, let $\ell \in L$. By assumption on x, $\langle x,x\rangle = 2Q(x) \neq 0$, so it divides $\langle x,\ell\rangle$ (in K); set $a = \frac{\langle x,\ell\rangle}{\langle x,x\rangle}$. Then $\langle \ell - ax, x\rangle = \langle \ell, x\rangle - a\langle x,x\rangle = 0$, so $\ell = ax + (\ell - ax)$ is in $M + M^\perp$. Assume $\ell \in M \cap M^\perp$; write $\ell = ax$. Then $a\langle x,x\rangle = 0$, which is a contradiction unless $a = 0$. Hence

$M \cap M^\perp = \{0\}$ and $L \otimes_R K = M \oplus M^\perp$. Since the determinant of τ_x is the product of the determinants of τ_x restricted to M and to $M^\perp$, and τ_x is the identity on $M^\perp$, we have $\det(\tau_x) = \det(\tau_x|_M) = -1$ since τ_x is -1 on M. Q.E.D.

Note that in particular τ_x exists if $Q(x)$ is a units of R. More particularly, if R is a field of characteristic $\neq 2$ and $Q(x) \neq 0$ then τ_x exists. In this case note also that the two properties (9.8.3) and (9.8.4) determine τ_x, since when R is a field we have $L \cong Rx \oplus x^\perp$.

The importance of reflections is attested to by the theorem of Cartan and Dieudonne, which roughly says that all isometries are products of reflections.

We require a preliminary lemma.

LEMMA 9.9. *Let (L, Q) be a quadratic vector space over a field R of characteristic $\neq 2$. Let $v, w \in L$ with $Q(v) = Q(w) \neq 0$. Then at least one of τ_{v-w} and $\tau_{v+w}\tau_v$ is well-defined, and gives an element $\sigma \in O(V, B)$ such that $\sigma(v) = w$.*

PROOF. We have that $\tau_v \in (L, Q)$ since v is anisotropic; thus we must show that either τ_{v-w} or τ_{v+w} is well-defined, i.e., that $v - w$ or $v + w$ is anisotropic. But if $Q(v - w) = Q(v + w) = 0$, then

$$O = Q(v - w) + Q(v + w) = 2Q(v) + 2Q(w) = 4Q(v) \neq 0,$$

giving a contradiction; so at least one of τ_{v-w} and $\tau_{v+w}\tau_v$ is defined.

It remains to show that $\tau_{v-w}(v) = w$ and $\tau_{v+w}\tau_v(v) = w$ (whenever these are defined.)

Now

$$\begin{aligned} Q(v \pm w) &= Q(v) \pm \langle v, w\rangle + Q(w) \\ &= 2Q(v) \pm \langle v, w\rangle \\ &= \langle v, v \pm w\rangle \end{aligned}$$

so that

$$Q(v - w) = \langle v - w, v\rangle$$

and

$$Q(v + w) = \langle v + w, v\rangle.$$

Thus, if $Q(v - w) \neq 0$ then

$$\begin{aligned} \tau_{v-w}(v) &= v - \frac{\langle v - w, v\rangle}{Q(v - w)}(v - w) \\ &= v - (v - w) = w \end{aligned}$$

while if $Q(v+w) \neq 0$ then

$$\begin{aligned}\tau_{v+w}\tau_v(v) &= \tau_{v+w}(-v) \\ &= -v - \frac{\langle v+w, -v\rangle}{Q(v+w)}(v+w) \\ &= -v + (v+w) = w.\end{aligned}$$

Q.E.D.

THEOREM 9.10 (Cartan-Dieudonné). *Assume R is a field of characteristic $\neq 2$, and (L, Q) is a quadratic vector space over R. Then every element of $\mathcal{O}(L)$ is a product of reflections.*

PROOF. We use induction on the dimension of L. Let $\rho \in \mathcal{O}(L)$, choose some $w \in V$ with $Q(w) \neq 0$, and let $v = \rho(w)$. Then $Q(v) = Q(\rho(w)) = Q(w) \neq 0$ and we may apply the preceding lemma: there is some $\sigma \in \mathcal{O}(L)$ which is a product of reflections such that $\sigma\rho(w) = w$. But this means that $\sigma\rho \in \mathcal{O}(w^\perp, Q\mid_{w^\perp})$; by the inductive hypothesis, we have that $\sigma\rho$ is a product of reflections. Hence $\rho = \sigma^{-1}(\sigma\rho)$ is as well. Q.E.D.

In fact, if $\dim L = N$, at most N reflections is required; see [**Cassels 78**, Chapter 2, Example 8].

As a final remark, we should mention the map on orthogonal groups for a change of rings. Let us assume that $f : R \to S$ is a monomorphism of integral domains, in which $2 \neq 0$, and let (L, Q) be a quadratic R-module. Then there is a 1-1 homomorphism of groups $g : \mathcal{O}(L) \to \mathcal{O}(L_S)$ sending σ to $\sigma \otimes 1$. In this situation we often abuse notation and consider $\mathcal{O}(L) \subset \mathcal{O}(L_S)$ if $R \subset S$.

10. The Spinor Norm

Let K be a field of characteristic $\neq 2$ and let (L, Q) be a quadratic vector space over K. If $\sigma \in \mathcal{O}(L)$, write $\sigma = \tau_{v_1}\tau_{v_2}\ldots\tau_{v_r}$, where v_i is a vector in L with $Q(v_i) \neq 0$; this is possible by Theorem (9.10).

DEFINITION 10.1. With the above notations, define a function

$$\text{spin} : \mathcal{O}(L) \to K^\times/(K^\times)^2$$

by

$$\text{spin}(\sigma) = \prod Q(v_i) \mod (K^\times)^2.$$

THEOREM 10.2. *Let K be a field of characteristic $\neq 2$ and let (L, Q) be a quadratic vector space over K. Then* $\text{spin} : \mathcal{O}(L) \to K^\times/(K^\times)^2$ *is a well defined group homomorphism.*

PROOF. By Theorem 9.10, any $\sigma \in \mathcal{O}(L)$ can be written in the form $\sigma = \tau_{v_1} \dots \tau_{v_r}$ for some anistropic vectors $v_1, \dots, v_r$; if $\sigma = \tau_{w_1} \dots \tau_{w_s}$ is another such expression, then

$$\tau_{v_1} \dots \tau_{v_r} \tau_{w_s} \dots \tau_{w_1} = \sigma\sigma^{-1} = 1 \text{ in } \mathcal{O}(L),$$

so that

$$Q(v_1) \dots Q(v_r) Q(w_s) \dots Q(w_1) \in (K^\times)^2,$$

or

$$Q(v_1) \dots Q(v_r) \equiv Q(w_1) \dots Q(w_s) \mod (K^\times)^2.$$

This proves that spin is well-defined; the homomorphism property is immediate. Q.E.D.

The homomorphism spin is called the *spinor norm* map. An alternative approach to the spinor norm can be found in Zassenhaus (1962).

If R is an integral domain in which $2 \neq 0$ and (L, Q) is a quadratic R-module, then, as remarked in the previous section, $\mathcal{O}(L)$ may be considered as a subgroup of $\mathcal{O}(L \otimes_R K)$ and hence spin : $\mathcal{O}(L) \to K^\times/(K^\times)^2$ is defined by restriction. Note that to compute $\text{spin}(\sigma)$ for $\sigma \in \mathcal{O}(L)$, one must factor σ into a product of reflections inside $\mathcal{O}(L \otimes_R K)$; such a factorization may not be possible in $\mathcal{O}(L)$.

We wish to introduce some special subgroups of $\mathcal{O}(V)$ in case V is a quadratic vector space over $\mathbb{R}$. In this case spin takes values in $\mathbb{R}^\times/(\mathbb{R}^\times)^2$, which is cyclic of order 2; we identify this group with $\{+, -\}$. Hence we have a group homomorphism $(\det, \text{spin}) : \mathcal{O}(V) \to \{+, -\} \times \{+, -\}$, and the kernel of $(\det, \text{spin})$ will be denoted by $\mathcal{O}_{++}(V)$.

For $\alpha, \beta \in \{+, -\}$ with $(\alpha, \beta) \neq (+, +)$ we then define a group $\mathcal{O}_{\alpha\beta}(V)$ containing $\mathcal{O}_{++}(V)$ by specifying that $\mathcal{O}_{\alpha\beta}(V)/\mathcal{O}_{++}(V)$ be generated by any element $\sigma \in \mathcal{O}(V)$ such that $\det(\sigma) = \alpha$ and $\text{spin}(\sigma) = \beta$. (If no such element exists, we set $\mathcal{O}_{\alpha\beta}(V) = \mathcal{O}_{++}(V)$.) Note that the index of $\mathcal{O}_{++}(V)$ in $\mathcal{O}_{\alpha\beta}(V)$ is either 1 or 2. With this notation, we have the following descriptions of the groups $\mathcal{O}_{\alpha\beta}(V)$:

$$\mathcal{O}_{++}(V) = \{\sigma \in \mathcal{O}(V) \mid \det(\sigma) = \text{spin}(\sigma) = +\} = \text{Ker}(\det, \text{spin})$$

$$\mathcal{O}_{+-}(V) = \{\sigma \in \mathcal{O}(V) \mid \det(\sigma) = +\} = \text{Ker}(\det)$$

$$\mathcal{O}_{-+}(V) = \{\sigma \in \mathcal{O}(V) \mid \text{spin}(\sigma) = +\} = \text{Ker}(\text{spin})$$

$$\mathcal{O}_{--}(V) = \{\sigma \in \mathcal{O}(V) \mid \det(\sigma) = \text{spin}(\sigma)\} = \text{Ker}(\det \cdot \text{spin}).$$

Let L be an integral quadratic form. In the same spirit as the above, we define $\mathcal{O}_{\alpha\beta}(L)$ by

$$\mathcal{O}_{\alpha\beta}(L) = \mathcal{O}(L) \cap \mathcal{O}_{\alpha\beta}(L \otimes_{\mathbb{Z}} \mathbb{R})$$

for $(\alpha, \beta) \in \{+, -\} \times \{+, -\}$.

The elements of $\mathcal{O}_{\alpha\beta}(L)$ (or of $\mathcal{O}_{\alpha\beta}(L \otimes_{\mathbb{Z}} \mathbb{R})$) will be referred to as (α, β)-isometries.

11. Sign Structures and Orientations

Let V be a real vector space of dimension N. An *ordered basis* S of V is an N-tuple $(v_1, \ldots, v_N)$ of vectors of V whose elements form a basis for V. Define an "orienting" equivalence relation on the set of ordered bases for V by declaring $S = (v_1, \ldots, v_N)$ equivalent to $T = (w_1, \ldots, w_N)$ if the change of basis matrix from S to T has positive determinant.

Definition 11.1. An *orientation* on V is an equivalence class of ordered bases of V.

Unless $V = (0)$, each finite-dimensional real vector space has exactly two orientations. Any ordered basis of V determines a unique orientation on V. V is said to be *oriented* if an orientation for V has been chosen.

Now let (V, Q) be a quadratic vector space over $\mathbb{R}$, with signature (r_+, r_-). The set

$$\mathrm{GR}^+ = \{r_+\text{-dimensional oriented subspace } W \subset V \,|\, Q|_W \text{ is positive definite}\}$$

has either one or two connected components, one if V is negative definite, two otherwise. If V is not negative definite, the two components exchange if one switches orientation.

Similar statements hold for the set

$$\mathrm{GR}^- = \{r_-\text{-dimensional oriented subspace } W \subset V \,|\, Q|_W \text{ is negative definite}\}$$

Following Looijenga and Wahl [], we make the following:

Definition 11.2. A *positive* (respectively *negative*) *sign structure* on V is a choice of a connected component of GR^+ (respectively GR^-). A *total sign structure* on V is a positive and a negative sign structure on V.

Note that a positive (respectively negative) sign structure on V is determined by a choice of any element of GR^+ (respectively GR^-), i.e., an orientation on any r_+- (respectively r_--) dimensional subspace W of V on which $Q|_W$ is positive (respectively negative) definite.

A total sign structure on V determines an orientation on V by the rule that if W_+ (respectively W_-) belongs to the positive (respectively negative) sign structure, then $W_+ \wedge W_-$ defines the orientation. In other words, if $(v_1, \ldots, v_{r_+})$ is an ordered basis of W_+ and $(w_1, \ldots, w_{r_-})$ is

an ordered basis of W_- inducing their orientations, then the ordered basis $(v_1, \ldots, v_{r_+}, w_1, \ldots, w_{r_-})$ induces the orientation of V.

Note that if V is positive definite, there is only one possible negative sign structure and a total sign structure on V is positive sign structure, which is an orientation. Similar remarks hold if V is negative definite. If V is indefinite, all of these notions are distinct. In particular, an orientation does not induce a total sign structure in this case.

If (L, Q) is an integral quadratic form, a positive (respectively negative, respectively total) sign structure on L is by definition one on $L \otimes_{\mathbb{Z}} \mathbb{R}$; an orientation on L is one on $L \otimes \mathbb{R}$, also.

If $\sigma \in \mathcal{O}(V)$, σ acts on the sets GR^+, GR^- and the sets of ordered bases of V, so it makes sense to say that σ preserves positive, negative or total sign structures on V, or that σ preserves orientations on V. We use the same language for elements of $\mathcal{O}(L)$ where L is an integral quadratic form. With this language, we have the following descriptions of the groups $\mathcal{O}_{\alpha\beta}(L)$.

PROPOSITION 11.3. *Let L be an integral quadratic form or a real quadratic vector space. Then*

(11.3.1) $\mathcal{O}_{++}(L) = \{\sigma \in \mathcal{O}(L) \,|\, \sigma$ *preserves total sign structures*$\}$
(11.3.2) $\mathcal{O}_{+-}(L) = \{\sigma \in \mathcal{O}(L) \,|\, \sigma$ *preserves orientations*$\}$
(11.3.3) $\mathcal{O}_{-+}(L) = \{\sigma \in \mathcal{O}(L) \,|\, \sigma$ *preserves negative sign structures*$\}$
(11.3.4) $\mathcal{O}_{--}(L) = \{\sigma \in \mathcal{O}(L) \,|\, \sigma$ *preserves positive sign structures*$\}$.

PROOF. From the definition of orientation, it is immediate that $\sigma \in \mathcal{O}(L)$ preserves orientations if and only if $\det(\sigma) = +$. This proves (11.3.2) and we seek a similar statement characterizing the kernel of spin.

Let Q be the form on L (and on $V = L \otimes \mathbb{R}$) and assume L has signature (r_+, r_-). Note that if $x \in V$ is anisotropic, then $\mathrm{spin}(\tau_x) = +if\ Q(x) > 0$ and $\mathrm{spin}(\tau_x) = -$ if $Q(x) < 0$. Also, given any $x \in V$ with $Q(x) > 0$ (respectively < 0), there is an r_+-(respectively r_-−) dimensional subspace $W \subset V$ containing x, on which Q is positive (respectively negative) definite. Therefore, if $Q(x) > 0$, i.e., $\mathrm{spin}(\tau_x) = +$, then τ_x switches positive sign structures and preserves negative sign structures. On the other hand, if $Q(x) < 0$, i.e., $\mathrm{spin}(\tau_x) = -$, then τ_x preserves positive sign structures and switches negative sign structures.

By writing $\sigma \in \mathcal{O}(L)$ as a product of reflections in $\mathcal{O}(V)$, we see immediately that σ preserves negative sign structures if and only if $\mathrm{spin}(\sigma) = +$, proving statement (11.3.3).

If $\sigma \in \mathcal{O}(L)$ preserves orientations *and* negative sign structures, it must also preserve positive sign structures, hence total sign structures.

Therefore, σ preserves total sign structures if and only if $\det(\sigma) = \mathrm{spin}(\sigma) = +$, which is statement (11.3.1).

Note that $\sigma \in \mathcal{O}(L)$ preserves positive sign structures if and only if S either preserves both orientations and negative sign structures or switches both. Therefore, σ preserves positive sign structures if and only if either $\det(\sigma) = \mathrm{spin}(\sigma) = +$ or $\det(\sigma) = \mathrm{spin}(\sigma) = -$, i.e., if and only if $\det(\sigma) = \mathrm{spin}(\sigma)$, proving (11.3.4). Q.E.D.

Due to this proposition, we refer to a total sign structure, orientation, negative sign structure, and positive sign structure as a $(+,+)$-structure, $(+,-)$-structure, $(-,+)$-structure, and $(-,-)$-structure, respectively. With this language, the elements of $\mathcal{O}_{\alpha\beta}(L)$ are exactly those isometries which preserve (α,β)-structures, for any $(\alpha,\beta) \in \{+,-\}\times\{+,-\}$.

CHAPTER II

Quadratic Forms over Integral Domains

1. Torsion Modules over a Principal Ideal Domain

In this section, and indeed throughout this entire chapter, R will denote a principal ideal domain with quotient field K, of characteristic unequal to 2. We will also assume that all R-modules discussed are finitely generated, except of course for the module K/R. Let G be a torsion R-module. A finite subset $E = \{g_1, \ldots, g_n\}$ of $G - \{0\}$ is *independent* if whenever $\sum r_i g_i = 0$ in G, with $r_i \in R$, then $r_i g_i = 0$ for every i. A *basis* for G is an independent set of nonzero elements of G which generates G. A basis $E = \{g_1, \ldots, g_n\}$ is an *ordered basis* if $\mathrm{Ann}_R(g_i) \supseteq \mathrm{Ann}_R(g_{i+1})$ for every i; if we set $(d_i) = \mathrm{Ann}_R(g_i)$, this condition is equivalent to $d_i | d_{i+1}$ for every i.

For example, $\{2, 3\}$ is a basis for $\mathbb{Z}/6\mathbb{Z}$ over $\mathbb{Z}$, but it is not an ordered basis; $\{1\}$ is an ordered basis.

From the classification theorem for finitely generated modules over a principal ideal domain, any two ordered bases of a torsion R-module G have the same cardinality. This cardinality is the minimum among all subsets of G which generate G; it called the *length* of G, and is denoted by $\ell(G)$.

Any two ordered bases for G also have the same sequence of annihilator ideals $\mathrm{Ann}_R(g_i)$. Generators $d_i \in R$ for these ideals are unique up to a unit factor in $R^\times$, and are called the *invariant factors*, or simply the *invariants*, of G. Any collection $\{d_1, \ldots, d_n\}$ of elements of R such that d_1 is not a unit and $d_i | d_{i+1}$ for every i can occur as the invariants of a torsion R-module G, and they determine G as an R-module up to isomorphism:

$$G \cong R/(d_1) \oplus \cdots \oplus R/(d_n).$$

The product $\Delta = \prod d_i$ of the invariants of G is the *order* of G; it is well defined up to a unit factor. If $R = \mathbb{Z}$ we will always take $\Delta > 0$, so that $\Delta = |G|$.

Let $p \in R$ be a prime element, and let R_p be the localization of R at the prime ideal (p). If G is a torsion R-module, then $G \otimes_R R_p$ is a torsion R_p-module, whose invariants are all powers of p. Conversely, if G is a torsion R-module whose invariants are all powers of p, then

G is naturally an R_p-module also, and $G \cong G \otimes_R R_p$ as R_p-modules. Such a module will be called a *p-primary* R-module. If $R = \mathbb{Z}$, then a p-primary $\mathbb{Z}$-module will be simply called a finite abelian p-group.

Let $G_p = \{x \in G \,|\, p^k x = 0 \text{ for some } k \geq 0\}$. G_p is an R-submodule of G, is p-primary, and is in fact isomorphic to $G \otimes_R R_p$. G_p will be called the *p-part* of G. Note that $G = \bigoplus_p G_p$ is an internal direct sum decomposition of G.

PROPOSITION 1.1. *Let $\langle -, - \rangle$ be a torsion bilinear form on G, i.e., a symmetric bilinear form on G with values in K/R. Then the decomposition $G = \bigoplus_p G_p$ is an orthogonal direct sum decomposition, i.e., a splitting of G.*

PROOF. Let p_1 and p_2 be two non-associate primes of R, and let $x_i \in G_p$. Assume $p_1^\alpha x_1 = 0$ and $p_2^\beta x_2 = 0$; since p_1 and p_2 are relatively prime, so are p_1^α and p_2^β, and there exist elements a and b in R such that $ap_1^\alpha + bp_2^\beta = 1$. Therefore,

$$\begin{aligned} \langle x_1, x_2 \rangle &= (ap_1^\alpha + bp_2^\beta)\langle x_1, x_2 \rangle \\ &= ap_1^\alpha \langle x_1, x_2 \rangle + bp_2^\beta \langle x_1, x_2 \rangle \\ &= a\langle p_1^\alpha x_1, x_2 \rangle + b\langle x_1, p_2^\beta x_2 \rangle \\ &= 0 \mod R. \end{aligned}$$

Q.E.D.

This splitting of G is called the *Sylow-splitting* of G.

Let G be a nontrivial p-primary torsion R-module, with invariants $d_1 = p^{e_1}, \ldots, d_n = p^{e_n}$. We define the *exponent* of G to be $d_n = p^{e_n}$, and the *scale* of G to be $d_1 = p^{e_1}$. Note that the exponent of G is p^e if $p^e G = 0$ but $p^{e-1} G \neq 0$; the scale of G is the minimum order among elements of G which are not divisible by p. Alternatively, the exponent is the largest order which appears in any decomposition of G into cyclic R-modules, and the scale is the smallest order so appearing. If G is trivial, we define its exponent and scale to be 1.

A p-primary torsion R-module H is *homogeneous* if its exponent is equal to its scale. This is equivalent to $H \cong (R/(p^e))^s$ for some e and $s \in \mathbb{N}$. The integer e is the exponent (and scale) of H, and the integer s is the *rank* of H.

Note that any p-primary torsion R-module G is isomorphic to $\bigoplus_{e \geq 1} (R/(p^e))^{s_e}$, where $(s_e)_{e \geq 1}$ is a collection of nonnegative integers, all but finitely many equal to zero. The s_e's are determined by G. If G is nontrivial, then the exponent of G is $p^{\max\{e \,|\, s_e \neq 0\}}$ and the scale of G is $p^{\min\{e \,|\, s_e \neq 0\}}$. G is homogeneous if $s_e \neq 0$ for at most one e, and that s_e is its rank.

If G is any torsion R-module, the decomposition $G = \bigoplus_p (\bigoplus_e (R/(p^e))^{s_{p,e}})$ will be called the *prime power decomposition* of G. It is often more useful than the invariant factor decomposition $G = \bigoplus_{i=1}^n R/(d_i)$.

Note that any basis of a p-primary torsion R-module can be ordered to become an ordered basis; hence, we will always assume (in the p-primary case) that any basis is so ordered.

Finally note that $(G_p)^* = (G^*)_p$, where $G^* = \mathrm{Hom}_R(G, K/R)$ for a torsion R-module G.

2. The Functors ρ_k

Fix a prime p of R, and let G be a torsion R-module.

DEFINITION 2.1. $G_{p,k} = \{x \in G \mid p^k x = 0\}$.

The following is immediate.

LEMMA 2.2.

(2.2.1) $G_{p,0} = (0)$

(2.2.2) $G_{p,k-1} \subseteq G_{p,k}$ *for all* $k \geq 1$

(2.2.3) $pG_{p,k+1} \subseteq G_{p,k}$ *for all* $k \geq 0$

(2.2.4) For k *sufficiently large,* $G_{p,k} = G_{p,k+1}$ *and* $G_p = \bigcup_{k \geq 0} G_{p,k}$.

If G is a p-primary, we will often denote $G_{p,k}$ by simply G_k. With this notation, $G_{p,k} = (G_p)_k$.

DEFINITION 2.3. $\rho_{p,k}(G) = G_{p,k}/(G_{p,k-1} + pG_{p,k+1})$

If G is p-primary, $\rho_{p,k}$ will be denoted by ρ_k. We note that $\rho_{p,k}(G) = \rho_k(G_p)$.

We have the following elementary properties of this construction.

LEMMA 2.4.

(2.4.1) $\rho_{p,k}$ *is a covariant functor from the category of torsion* R*-modules to* p*-primary torsion* R*-modules.*

(2.4.2) $\rho_{p,k}$ *is additive, i.e.*

$$\rho_{p,k}(G \oplus H) \cong \rho_{p,k}(G) \oplus \rho_{p,k}(H).$$

(2.4.3) $\rho_{p,k}(G)$ *is either trivial or is homogeneous with exponent* p.

(2.4.4) If G *is homogeneous with exponent* p^e *and rank* s*, then*

$$\rho_k(G) \cong \begin{cases} \{0\} & \text{if } k \neq e \\ (R/(p))^s & \text{if } k = e. \end{cases}$$

(2.4.5) If G *is* p*-primary and* $G \cong \bigoplus_{e \geq 1} (R/(p^e))^{s_e}$*, then* $\rho_k(G) \cong (R/(p))^{s_k}$.

(2.4.6) $\rho_{p,k}(G^*) \cong \rho_{p,k}(G)^*$.

PROOF. Since $G_{p,k}$ is p-primary, so is $\rho_{p,k}(G)$. Hence (2.4.1) follows from remarking that if $\phi : G \to H$ is an R-map, then $\phi(G_{p,k}) \subseteq H_{p,k}$, so ϕ induces an R_p-map $\delta_{p,k}(\phi)$ from $\rho_{p,k}(G)$ to $\rho_{p,k}(H)$. Statement (2.4.2) is obvious, and (2.4.3) follows from (2.2.3). To prove (2.4.4), it suffices to assume G has rank 1, so that $G \cong R/(p^e)$. Then G_k is generated by p^{e-k} for $k \leq e$ and $G_k = G$ for $k \geq e$; hence, $pG_{k+1} = G_k$ for $k > e$, so that $\rho_k(G) = 0$ if $k \neq$ e. Finally, $\rho_e(G)$ is generated by $1 \mod p^e$ which is of order p in $\rho_e(G)$. Statement (2.4.5) follows from (2.4.4) and the additivity of ρ_k. Finally, (2.4.6) is a direct consequence of the isomorphism $(G_p)^* \equiv (G^*)_p$; we leave the details to the reader. Q.E.D.

The functor ρ_k exactly "picks out" the exponent p^k piece of a p-primary torsion module G and can reduce many questions about torsion R-modules to homogeneous p-primary torsion R-modules. For instance, if $G \cong \bigoplus_e (R/(p^e))^{s_e}$, then $s_e = \mathrm{rank}_{R/p}(\rho_e(G))$, showing that the ranks s_e are uniquely determined by G. This is the crucial observation to make, to prove the uniqueness of the prime power decomposition and the invariant factor decomposition of a torsion R-module G.

Our interest in ρ_k goes a bit deeper, though: if G has a bilinear form on it, then $\rho_k(G)$ inherits the form.

LEMMA 2.5. *Let G be a p-primary torsion R-module, and let $\langle -, - \rangle$ be a torsion bilinear form on G, i.e., a symmetric bilinear form with values in K/R. For $x \in G_k$, denote by $\bar{x}$ its class in $\rho_k(G)$. Define $\langle -, - \rangle_k$ on $\rho_k(G)$ by $\langle \bar{x}, \bar{y} \rangle_k = p^{k-1}\langle x, y \rangle$. Then $\langle -, - \rangle_k$ is a well-defined torsion bilinear form on $\rho_k(G)$, which is nondegenerate if $\langle -, - \rangle$ is nondegenerate on G.*

PROOF. To check that $\langle -, - \rangle_k$ is well defined, we need only check that $G_{k-1} + pG_{k+1}$ is contained in the kernel of $\langle -, - \rangle|_{G_k}$. Let $z \in G_{k-1}$, $y \in G_k$, and $w \in G_{k+1}$; then

$$\begin{aligned} p^{k-1}\langle z + pw, y \rangle &= p^{k-1}\langle z, y \rangle + p^k \langle w, y \rangle \\ &= \langle p^{k-1}z, y \rangle + \langle w, p^k y \rangle \\ &= \langle 0, y \rangle + \langle w, 0 \rangle \\ &= 0. \end{aligned}$$

This proves that $\langle -, - \rangle_k$ is well defined since it is clearly symmetric and bilinear.

If $\langle -, - \rangle$ is nondegenerate, then the adjoint map $\mathrm{Ad} : G \to G^*$ is an isomorphism; by the functoriality of ρ_k, $\rho_k(\mathrm{Ad}) : \rho_k(G) \to \rho_k(G^*)$ is also an isomorphism. Since $\rho_k(G^*) \cong \rho_k(G)^*$ and $\rho_k(\mathrm{Ad})$ corresponds to the adjoint map of $\langle -, - \rangle_k$, this induced form $\langle -, - \rangle_k$ is also nondegenerate. Q.E.D.

If H is a homogeneous R-module, we can be more explicit.

LEMMA 2.6. *Let H be a homogeneous p-primary torsion R-module with exponent p^k and rank s. Let $\{e_1, \dots, e_s\}$ be a basis for H. Let $\langle -, - \rangle$ be a torsion bilinear form on H.*

(2.6.1) For every i and j, $\langle e_i, e_j \rangle = p^{-k} a_{ij} \mod R$ with $a_{ij} \in R$.

(2.6.2) $\langle -, - \rangle$ is nondegenerate on $H \Leftrightarrow \det(a_{ij})$ is prime to p. If so, the class of $\det(a_{ij})$ in $(R/p^k)^\times/((R/p^k)^\times)^2$ is uniquely determined by $\langle -, - \rangle$.

(2.6.3) $\langle -, - \rangle$ is nondegenerate on $H \Leftrightarrow \langle -, - \rangle_k$ is nondegenerate on $\rho_k(H)$.

(2.6.4) Any splitting of H induces a splitting of $\rho_k(H)$.

(2.6.5) If $\langle -, - \rangle$ is nondegenerate on H, then any splitting of $\rho_k(H)$ can be lifted to a splitting of H.

PROOF. Since p^k annihilates $H, p^k \langle e_i, e_j \rangle$ must be $0 \mod R$, proving (2.6.1). Let $\{e_1^*, \dots, e_s^*\}$ be the dual basis for H^*, i.e., $e_i^*(e_j) = \delta_{ij} p^{-k}$. Then the matrix for the adjoint map Ad to $\langle -, - \rangle$ with respect to these bases is (a_{ij}); hence Ad is an isomorphism if and only if $\det(a_{ij})$ is a unit in R/p^k, i.e., $p \not| \det(a_{ij})$. If so, a change of basis (via a matrix M in $\mathrm{GL}(s, R/p^k)$) changes $\det(a_{ij})$ by $(\det M)^2$, proving (2.6.2). If $\bar{e}_i$ is the class of e_i in $\rho_k(H)$, then $\{\bar{e}_i\}$ is a basis for $\rho_k(H)$ over R/p, and since $\langle \bar{e}_i, \bar{e}_j \rangle_k = p^{-1} a_{ij} \mod R$, the matrix for the adjoint map to $\langle -, - \rangle_k$ is also (a_{ij}). This proves (2.6.3), using (2.6.2). Statement (2.6.4) is now clear; a splitting for H corresponds to a certain block form for the matrix (a_{ij}), and this block form is still present, of course, when considering the (a_{ij}) matrix as the matrix for the induced form $\langle -, - \rangle_k$.

To prove (2.6.5), let $\{\bar{e}_1, \dots, \bar{e}_m\}$ generate an orthogonal direct summand $\bar{A}$ of $\rho_k(H)$. Lift each $\bar{e}_i$ to e_i in H and let A be the submodule of H generated by $e_1, \dots, e_m$, so that $\rho_k(A) = \bar{A}$. Since $\langle -, - \rangle$ is nondegenerate, so is $\langle -, - \rangle_k$, and since $\bar{A}$ is an orthogonal direct summand of $\rho_k(H)$, so is $\langle -, - \rangle_k|_{\bar{A}}$. But $\langle -, - \rangle_k|_{\bar{A}} = (\langle -, - \rangle|_A)_k$, so by (2.6.3) applied to A, $\langle -, - \rangle|_A$ is nondegenerate. By (I.4.4), $\langle -, - \rangle|_A$ is unimodular, so A splits off H by (I.5.6). This splitting induces the given splitting of $\rho_k(H)$. Q.E.D.

Let us present ρ_k for the relevant examples in (I, section 7); we leave the computations to the reader.

LEMMA 2.7.

(2.7.1) $\rho_k(\bar{w}_{2,k}^\varepsilon) = \bar{w}_{2,1}^1$ for every ε.

(2.7.2) If p is odd, $\rho_k(\bar{w}_{p,k}^\varepsilon) = \bar{w}_{p,1}^\varepsilon$ for each $\varepsilon = \pm 1$.

(2.7.3) $\rho_k(\bar{u}_k) = \bar{u}_1$ *and* $\rho_k(\bar{v}_k) = \bar{v}_1$*; note that* $\bar{u}_1 \cong \bar{v}_1$.

As an application of this construction, we have the following.

PROPOSITION 2.8. *Let* $\langle -,- \rangle$ *be a torsion bilinear form on a p-primary torsion R-module G.*

(2.8.1) If $\langle -,- \rangle$ *is nondegenerate, then G splits into homogeneous orthogonal direct summands.*

(2.8.2) $\langle -,- \rangle$ *is nondegenerate on* $G \Leftrightarrow \langle -,- \rangle_k$ *is nondegenerate on* $\rho_k(G)$ *for all k.*

PROOF. Assume $\langle -,- \rangle$ is nondegenerate, and let the exponent of G be p^k. Write $G = H \oplus K$, where H is homogeneous of exponent p^k and the exponent of K is strictly less than p^k; the sum need not be orthogonal. Since $\rho_k(H) = \rho_k(G)$ and $\langle -,- \rangle_k$ is nondegenerate on $\rho_k(G)$ by (2.5), then $\langle -,- \rangle|_H$ is nondegenerate on H by (2.6.3). Hence H splits off G by (I.5.6). Statement (2.8.1) then follows by induction on the exponent.

One direction of (2.8.2) follows from (2.5). To finish, assume that each $\rho_k(G)$ is nondegenerate. Again write $G = H \oplus K$ as above; then $\langle -,- \rangle_k$ on $\rho_k(H) = \rho_k(G)$ is nondegenerate, so $\langle -,- \rangle|_H$ is nondegenerate on H. Hence H splits off G and by induction G is the orthogonal direct sum of nondegenerate homogeneous modules. Hence $\langle -,- \rangle$ on G is nondegenerate by (I.5.2). Q.E.D.

COROLLARY 2.9. *Let G be a torsion R-module and* $\langle -,- \rangle$ *a nondegenerate symmetric torsion bilinear form on G. Then* $(G, \langle -,- \rangle)$ *splits into nondegenerate homogeneous p-primary torsion bilinear forms. If q is a nondegenerate torsion quadratic form on G, then* (G, q) *splits into nondegenerate homogeneous p-primary torsion quadratic forms.*

The above follows directly from the previous proposition and the Sylow splitting of G.

3. The Discriminant of a Torsion Bilinear Form

Let G be a torsion R-module, with ordered basis $\{g_1, \ldots, g_n\}$ and invariants $\{d_1, \ldots, d_n\}$. If $\langle -,- \rangle$ is a torsion bilinear form on G (with values in K/R), then one can choose representatives $B_{ij} \in K$ for $\langle g_i, g_j \rangle$; these representatives must satisfy

$$d_i B_{ij} \in R \text{ and } d_j B_{ij} \in R \text{ for all } i, j. \tag{3.1}$$

Conversely, if (B_{ij}) is an $n \times n$ matrix over K satisfying (3.1), then the torsion bilinear form $\langle -,- \rangle$ on G defined by $\langle g_i, g_j \rangle = B_{ij} \mod R$ is well defined.

Note that the choice of the B_{ij}'s in K is exactly a lifting of the torsion bilinear form on G to a K-valued bilinear form on the free R-module on the set $\{g_1, \ldots, g_n\}$.

LEMMA 3.2. *Let $(G, \langle -, - \rangle)$ be a torsion bilinear form over R, and let*
$\{g_1, \ldots, g_n\}$ be an ordered basis of G. Assume that the invariants of G are
$\{d_1, \ldots, d_n\}$, and let $\Delta = \prod d_i$ be the order of G.

(3.2.1) If $(B_{ij}) \in K$ is any lifting of $(\langle g_i, g_j \rangle)$, then $\Delta \cdot \det(B_{ij}) \in R$.

(3.2.2) If (B_{ij}) and (B'_{ij}) are two such liftings, then

$$\Delta \cdot [\det(B_{ij}) - \det(B'_{ij})] \in d_1 R.$$

(3.2.3) If $\langle -, - \rangle$ is nondegenerate, then $\Delta \cdot \det(B_{ij}) \in R$ is relatively prime to d_1.

PROOF. Note that $\det(B_{ij})$ is a sum of terms of the form

$$\pm B_{1\sigma(1)} B_{2\sigma(2)} \ldots B_{n\sigma(n)},$$

where $\sigma \in S_n$ is a permutation. By (3.1), $d_i B_{i\sigma(i)} \in R$ for every i; hence,

$$\Delta \cdot B_{1\sigma(1)} \ldots B_{n\sigma(n)} = d_1 B_{1\sigma(1)} d_2 B_{2\sigma(2)} \ldots d_n B_{n\sigma(n)} \in R.$$

Therefore,

$$\Delta \cdot \det(B_{ij}) \in R,$$

proving (3.2.1).

To prove the second statement, we may assume that $B'_{ij} = B_{ij}$ except for one pair of subscripts i_0, j_0, and that $B'_{i_0 j_0} = B_{i_0 j_0} + r$, where $r \in R$. Let $\sigma \in S_n$ be a permutation. If $\sigma(i_0) \neq j_0$, then $\prod_i B_{i\sigma(i)} = \prod_i B'_{i\sigma(i)}$; if $\sigma(i_0) = j_0$, then

$$\begin{aligned}
\Delta \cdot \prod_i B'_{i\sigma(i)} &= \Delta \cdot \left(\prod_{i \neq i_0} B_{i\sigma(i)} \right) (B_{i_0 j_0} + r) \\
&= \Delta \cdot \prod_i B_{i\sigma(i)} + \Delta \cdot \left(\prod_{i \neq i_0} B_{i\sigma(i)} \right) r \\
&= \Delta \cdot \prod_i B_{i\sigma(i)} + \left(\prod_{i \neq i_0} (d_i B_{i\sigma(i)}) \right) d_{i_0} r.
\end{aligned}$$

Therefore, by (3.1)

$$\Delta \cdot \left[\prod_i B_{i\sigma(i)} - \prod_i B'_{i\sigma(i)} \right] \in d_{i_0} R \subseteq d_1 R.$$

Hence, in all cases every term of $\Delta \cdot [\det(B_{ij}) - \det(B'_{ij})]$ is in $d_1 R$, proving (3.2.2).

Finally, assume $\langle -, - \rangle$ is nondegenerate and let p be a prime of R dividing d_1. Assume p also divides $\Delta \cdot \det(B_{ij})$. Since $\Delta \cdot \det(B_{ij}) = \det(d_i B_{ij})$, the matrix $(d_i B_{ij} \mod p)$ is singular over R/p. Let $(r_1 \mod p, \ldots, r_n \mod p)$ be a nonzero null vector for $(d_i B_{ij} \mod p)$, so that $(d_i B_{ij}) \begin{pmatrix} r_1 \\ \vdots \\ r_n \end{pmatrix} = 0 \mod p$. Let $x = \sum_i \frac{d_i}{p} r_i g_i \in G$. Since there exists at least one i such that $r_i \neq 0 \mod p$, $x \neq 0$ in G. However,

$$\langle x, g_j \rangle = \langle \sum_i \frac{d_i}{p} r_i g_i, g_j \rangle = \frac{1}{p} \sum_i d_i r_i B_{ij} \mod R_j$$

since p divides $\sum d_i r_i B_{ij}$, $\langle x, g_j \rangle = 0 \mod R$ for every j, so that $\mathrm{Ad}(x) = 0$. Hence, $\langle -, - \rangle$ is degenerate. Q.E.D.

From (3.2.2), given the ordered basis $\{g_i\}$ of G, the class of $\Delta \cdot \det(B_{ij}) \in R/d_1 R$ is well defined. We would like to have an invariant which is also independent of the choice of ordered basis. For this we need the following.

LEMMA 3.3. *Let G be a torsion R-module with ordered basis $\{g_1, \ldots, g_n\}$ and first invariant d_1, and let σ be an R-automorphism of G. Let L be the free R-module on the set $\{g_i\}$, and let $\widetilde{\sigma} : L \to L$ be an R-endomorphism of L which induces σ. Then $\det(\widetilde{\sigma}) \in R$ is relatively prime to d_1.*

PROOF. Let p be a prime of R dividing d_1 and assume p also divides $\det(\widetilde{\sigma})$. We get an induced R/p-automorphism $\sigma_p : G/pG \to G/pG$ and an induced (R/p)-endomorphism $\widetilde{\sigma}_p : L/pG \to L/pG$ such that $\det(\widetilde{\sigma}_p) = 0$ and $\widetilde{\sigma}_p$ induces σ_p. However, since $p | d_1$, the natural projection from L/pL to G/pG is an R/p-isomorphism; therefore, $\sigma_p = \widetilde{\sigma}_p$ and since $\det(\widetilde{\sigma}_p) = 0, \sigma_p$ cannot be an automorphism. Q.E.D.

COROLLARY 3.4. *Let $(G, \langle -, - \rangle)$ be a torsion bilinear form over R with invariants $\{d_1, \ldots, d_n\}$ and order Δ. If $\{g_i\}$ and $\{g'_i\}$ are two ordered bases for G and (B_{ij}) and (B'_{ij}) are liftings to K of $(\langle g_i, g_j \rangle)$ and $(\langle g'_i, g'_j \rangle)$, respectively, then*

$$\Delta \cdot \det(B'_{ij}) = u^2 \Delta \cdot \det(B_{ij}) \text{ in } R/d_1 R$$

for some unit $u \in (R/d_1 R)^\times$.

PROOF. Let $\sigma : G \to G$ be the change of basis automorphism of G from $\{g_i\}$ to $\{g'_i\}$. Let L be the free R-module on $\{g_i\}$ and let $\widetilde{\sigma}$

p	d_1	Δ	representatives in $\frac{1}{\Delta}\mathbb{Z}$ for $\frac{1}{\Delta}(\mathbb{Z}/d_1)^\times/((\mathbb{Z}/d_1)^\times)^2$
odd	p^{e_1}	p^k	$\{p^{-k}, p^{-k}u\}$ where u is a non-square mod p
2	$2^{e_1} \geq 8$	2^k	$\{2^{-k}, 3\cdot 2^{-k}, 5\cdot 2^{-k}, 7\cdot 2^{-k}\}$
2	4	2^k	$\{2^{-k}, 3\cdot 2^{-k}\}$
2	2	2^k	$\{2^{-k}\}$

TABLE 3.1. representatives for $\frac{1}{\Delta}(\mathbb{Z}/d_1)^\times/((\mathbb{Z}/d_1)^\times)^2$

be a lifting of σ to an R-endomorphism of L. Let M be the matrix of $\widetilde{\sigma}$; then we may assume $(B'_{ij}) = M^T B_{ij} M$, since they are both liftings of $\langle g'_i, g'_j\rangle$ and the class $\Delta\cdot\det(B'_{ij})$ is independent of this lifting. By taking determinants, we see that $\Delta\cdot\det(B'_{ij}) = (\det M)^2\Delta\cdot\det(B_{ij})$ mod d_1R and moreover, $u = \det M$ is a unit in R/d_1R by the previous lemma. Q.E.D.

Hence, $\Delta\cdot\det(B_{ij})$ is well defined in $((R/d_1)^\times)^2\backslash R/d_1R$ and is an invariant of the bilinear form alone. Equivalently, we know

$$\det(B_{ij}) \in ((R/d_1)^\times)^2\backslash\frac{1}{\Delta}R/\frac{d_1}{\Delta}R$$

is well defined.

DEFINITION 3.5. Let $(G, \langle -,-\rangle)$ be a torsion bilinear form over R. The *discriminant* of $(G, \langle -,-\rangle)$, denoted by $\mathrm{disc}(G, \langle -,-\rangle)$ (or simply $\mathrm{disc}(G)$ or $\mathrm{disc}\langle -,-\rangle$), is the class of $\det(B_{ij})$ in $((R/d_1)^\times)^2\backslash\frac{1}{\Delta}R/\frac{d_1}{\Delta}R$.

We will often only need to consider the discriminants of nondegenerate forms, in which case the discriminant takes values in a subset of the above, namely

$$((R/d_1)^\times)^2\backslash\frac{1}{\Delta}(\text{elements of } R \text{ prime to } d_1)/\frac{d_1}{\Delta}(\text{elements of } R \text{ prime to } d_1)$$

which we will by abuse of notation denote by

$$\frac{1}{\Delta}(R/d_1)^\times/((R/d_1)^\times)^2 = \frac{1}{\Delta}\mathcal{D}(R/d_1).$$

If $R = \mathbb{Z}$ and G is p-primary for some prime number p, then $d_1 = p^{e_1}$ and $\Delta = p^k$ for two integers $1 \leq e_1 \leq k$. In this case the above set of values for $\mathrm{disc}(G)$ is readily calculated; we leave the computations to the reader and present the results in Table 3.1.

The values for the discriminant of the standard examples from (I, section 7) are given in Table 3.2.

The discriminant, although well defined for any torsion bilinear form over R, behaves more nicely in the case of p-primary forms. For

$(G, \langle -,- \rangle)$	$\operatorname{disc}(\langle -,- \rangle)$
$\bar{w}^1_{p,k}$, p odd	p^{-k}
$\bar{w}^{-1}_{p,k}$, p odd	$p^{-k}u$, where u is a non-square mod p
$\bar{w}^{\varepsilon}_{2,k}$, $k \geq 3$	$2^{-k}u$, where $\chi(u) = \varepsilon \mod 8$
$\bar{w}^{\varepsilon}_{2,2}$	$2^{-4}u$, where $\chi(u) = \varepsilon \mod 4$
$\bar{w}^1_{2,1}$	2^{-2}
$\bar{u}_k$	-2^{-2k}
$\bar{v}_k$	$3 \cdot 2^{-2k}$

TABLE 3.2. discriminants of finite bilinear forms

example, we have an "additivity" property. This is a little awkward to define, since the values of the discriminant lie in different sets, depending on the torsion module. However, if d_1 and d_1' are the first invariants, and Δ and Δ' are the orders of two torsion modules, there is a natural "product"

$$\left[((R/d_1)^\times)^2 \backslash \frac{1}{\Delta} R / \frac{d_1}{\Delta} R\right] \times \left[((R/d_1')^\times)^2 \backslash \frac{1}{\Delta'} R / \frac{d_1'}{\Delta'} R\right] \to ((R/d)^\times)^2 \backslash \frac{1}{\Delta\Delta'} R / \frac{d}{\Delta\Delta'} R$$

where $d = \gcd(d_1, d_1')$, induced by the ordinary multiplication map $\frac{1}{\Delta}R \times \frac{1}{\Delta'}R \to \frac{1}{\Delta\Delta'}$R. With this in mind, we have the following.

LEMMA 3.6. *Fix a prime p of R and let $(G, \langle -,- \rangle)$ and $(G', \langle -,- \rangle)$ be two p-primary torsion bilinear forms over R; let $G \oplus G'$ denote their orthogonal direct sum. Then* $\operatorname{disc}(G \oplus G') = \operatorname{disc}(G)\operatorname{disc}(G')$*, where the product of the discriminants is defined as above.*

PROOF. Firstly, note that because G and G' are p-primary, the first invariant d of $G \oplus G'$ is simply the "smaller" of the two first invariants d_1 and d_1' for G and G', i.e.,

$$d = \gcd(d_1, d_1') = \begin{cases} d_1 & \text{if } d_1 | d' \\ d_1' & \text{if } d' | d_1. \end{cases}$$

Since the order of $G \oplus G' = \Delta \cdot \Delta'$ (where Δ and Δ' are the orders for G and G'), both sides of the equality live in the same set.

The equality is now clear; after re-ordering, the representing matrix for $G \oplus G'$ can be chosen as the block form matrix consisting of two blocks, namely the representing matrices for G and G'. Q.E.D.

For p-primary forms, there is also a converse to (3.2.3).

LEMMA 3.7. *Let $(G, \langle -,- \rangle)$ be a p-primary torsion bilinear form with order Δ and let $B_{ij} \in K$ be such that $B_{ij} \mod R = \langle g_i, g_j \rangle$ for*

some ordered basis $\{g_i\}$ *for* G. *Then* $(G, \langle -, - \rangle)$ *is nondegenerate if and only if* $p \not| \Delta \cdot \det(B_{ij})$.

PROOF. By the additivity (3.6) and (2.8.1), we may assume G is homogeneous, say of exponent p^k and of rank s. Then by (2.6.1), $B_{ij} = p^{-k} a_{ij}$ for some $a_{ij} \in R$ and $\Delta = p^{sk}$; hence, $\Delta \cdot \det(B_{ij}) = p^{sk} \det(p^{-k} a_{ij}) = \det(a_{ij})$. The result now follows from (2.6.2). Q.E.D.

In the above case, we will abuse language and say that if $p \not| \Delta \cdot \det B_{ij}$, the *discriminant is a unit*.

Finally, there is a localization statement. Again this is slightly awkward to formulate. Note however that for a p-primary form, the values for the discriminant can equally well be taken in

$$((R_p/d_1)^\times)^2 \backslash \frac{1}{\Delta} R_p / \frac{d_1}{\Delta} R_p$$

instead of

$$((R/d_1)^\times)^2 \backslash \frac{1}{\Delta} R / \frac{d_1}{\Delta} R,$$

which are naturally isomorphic if d_1 and Δ are powers of p. In any case, there is for any d_1 and Δ a natural localization map

$$((R/d_1)^\times)^2 \backslash \frac{1}{\Delta} R / \frac{d_1}{\Delta} R \to ((R_p/d_1)^\times)^2 \backslash \frac{1}{\Delta} R_p / \frac{d_1}{\Delta} R_p$$

and if $\mathrm{disc}(G)$ is in the left-hand set, its image in the right-hand set will be denoted by $(\mathrm{disc}(G))_p$, the "p-part of the discriminant". The following lemma can now be stated.

LEMMA 3.8. *Let* $(G, \langle -, - \rangle)$ *be a torsion bilinear form over* R *and fix a prime* p. *Assume that* G *and* G_p *have the same length, i.e.,* p *divides the first invariant of* G. *Then* $\mathrm{disc}(G_p) = (\mathrm{disc}\, G)_p$.

PROOF. The point is that if $\ell(G) = \ell(G_p)$, the same representing matrix (B_{ij}) for $\langle -, - \rangle$ on G over R also represents $\langle -, - \rangle$ on G_p over R_p. Indeed, if $\{g_i\}$ is an ordered basis for G, then $g_i \otimes_R R_p \in G_p$ is an ordered basis for G_p, and the result follows immediately. Q.E.D.

4. The Discriminant of a Torsion Quadratic Form

Let G be a torsion R-module. If $q : G \to K/R$ is a quadratic form on G, the associated bilinear form $\langle -, - \rangle$ to q is always symmetric. We can use this and the extra information obtained in passing from the bilinear form $\langle -, - \rangle$ to the quadratic form q to define a more refined discriminant for q than for $\langle -, - \rangle$.

Assume that (G, q) is a torsion quadratic form over R with ordered basis $\{g_i\}$, invariants $\{d_i\}$, and associated bilinear form $\langle -, - \rangle$. One

can choose "symmetric" representatives for the values of q as follows. If $i < j$ let $B_{ij} \in K$ be a lift of $\langle g_i, g_j \rangle \in K/\mathrm{R}$. For the diagonal elements, let B_{ii} be two times a lift of $q(g_i) \in K/\mathrm{R}$. If $i > j$, set $B_{ij} = B_{ji}$. In this way we produce a matrix (B_{ij}) over K satisfying

$$\begin{aligned} B_{ij} = B_{ji} \text{ for every } i \text{ and } j, \text{ and} \\ d_i B_{ij} \in R \text{ if } i \neq j. \end{aligned} \tag{4.1}$$

Note that $B_{ii} \in K$ is actually well defined $\mod 2R$, since $B_{ii} = 2q(g_i)$, and $q(g_i)$ is well defined $\mod R$. The matrix (B_{ij}) over K will be called a *representing matrix* for q. We have the following analogue of (3.2).

LEMMA 4.2. *Let (G, q) be a torsion quadratic form over R and let $\{g_1, \ldots, g_n\}$ be an ordered basis of G. Assume that the invariants of G are $\{d_1, \ldots, d_n\}$ and let $\Delta = \prod d_i$ be the order of G.*

(4.2.1) If (B_{ij}) is any representing matrix for q, then $\Delta \cdot \det(B_{ij}) \in R$.

(4.2.2) If (B_{ij}) and (B'_{ij}) are two representing matrices for q, then

$$\Delta \cdot [\det B_{ij} - \det B'_{ij}] \in \alpha d_1 R,$$

where $\alpha = \gcd(2, d_1)$.

(4.2.3) If q is nondegenerate, then $\Delta \cdot \det(B_{ij}) \in R$ is relatively prime to αd_1.

PROOF. The first statement follows immediately from (3.2.1), since (B_{ij}) is a lift of $(\langle g_i, g_j \rangle)$, where $\langle -, - \rangle$ is the associated bilinear form to q. To prove the second statement, let us introduce some notation. Let E_{ij} be the $n \times n$ matrix over K with all 0's as entries, except in the $i - j^{\text{th}}$ position, where the entry is 1. Denote by $M[i, j]$ the matrix obtained from a matrix M by deleting the i^{th} row and j^{th} column. Note that if M is a square matrix,

$$\det(M + rE_{ij}) = \det M + (-1)^{i+j} \det M[i, j], \tag{4.3}$$

as is easily seen by expansion along the i^{th} row.

We may assume that the two representing matrices B' and B for q differ in only one entry on or above the main diagonal (recall that both are symmetric). There are two cases to consider.

Case 1: $B' = B + 2rE_{i_0 i_0}$ for some i_0.

This case occurs if B' and B differ in one entry on the main diagonal, since the entries on the main diagonal of a representing matrix for q is

well defined $\mod 2R$. Then

$$\begin{aligned}\Delta \cdot [\det B' - \det B] &= \Delta \cdot [\det(B + 2rE_{i_0 i_0}) - \det B] \\ &= \Delta \cdot (2r \det B[i_0, i_0]) \text{ by (4.3)} \\ &= 2d_{i_0} r \left(\prod_{i \neq i_0} d_i \right) \det B[i_0, i_0]\end{aligned}$$

which is in $2d_1R$, since $\left(\prod_{i\neq i_0} d_i\right) \det B[i_0, i_0] \in R$ by (4.2.1) applied to the subgroup of G generated by $\{g_i\}_{i\neq i_0}$. Since $2d_1R \subseteq \alpha d_1 R$, this case is clear.

Case 2: $B' = B + rE_{i_0 j_0} + rE_{j_0 i_0}$ for some $i_0 \lneqq j_0$.

In this case

$$\begin{aligned}\Delta \cdot [\det B' - \det B] &= \Delta \cdot [\det(B + rE_{i_0 j_0} + rE_{j_0 i_0}) - \det B] \\ &= \Delta \cdot (\det(B + rE_{i_0 j_0}) \\ &\quad + (-1)^{i_0 + j_0} r \det((B + rE_{i_0 j_0})[j_0, i_0]) \\ &\quad - \det B) \\ &= \Delta \cdot (\det B + (-1)^{i_0 j_0} r \det B[i_0, j_0] \\ &\quad + (-1)^{i_0 + j_0} r \det B[j_0, i_0] + r^2 \det(B[j_0, i_0][i_0, j_0]) \\ &\quad - \det B) \\ &= \Delta \cdot (2r(-1)^{i_0 + j_0} \det B[i_0, j_0] + r^2 \det(B[j_0, i_0][i_0, j_0])) \\ &= 2d_{i_0} r (-1)^{i_0 + j_0} \left(\prod_{i \neq i_0} d_i \right) \det B[i_0, j_0] \\ &\quad + d_{i_0} d_{j_0} r^2 \left(\prod_{i \neq i_0, j_0} d_i \right) \det(B[j_0, i_0][i_0, j_0]).\end{aligned}$$

Now $\left(\prod_{i\neq i_0} d_i\right) \det B[i_0, j_0] \in R$ by (4.1) and the same analysis as in the proof of (3.2.1); $\left(\prod_{i\neq i_0, j_0} d_i\right) \det(B[j_0, i_0][i_0, j_0]) \in R$ by applying (4.2.1) to the subgroup of G generated by $\{g_i\}_{i\neq i_0, j_0}$. Therefore,

$$\Delta \cdot [\det B' - \det B] \in 2d_{i_0} R + d_{i_0} d_{j_0} R \subseteq 2d_1 R + d_1^2 R \subseteq \alpha d_1 R,$$

proving (4.2.2).

Finally, (4.2.3) follows from (3.2.3), after noting that any $r \in R$ which is relatively prime to d_1 is relatively prime to αd_1 (and conversely). Q.E.D.

p	d_1	Δ	α	representatives in $\frac{1}{\Delta}\mathbb{Z}$ for $\frac{1}{\Delta}(\mathbb{Z}/\alpha d_1)^\times/((\mathbb{Z}/\alpha d_1)^\times)^2$
odd	p^{e_1}	p^k	1	$\{p^{-k}, p^{-k}u\}$ where u is a non-square mod p
2	$2^{e_1} \geq 4$	2^k	2	$\{2^{-k}, 3\cdot 2^{-k}, 5\cdot 2^{-k}, 7\cdot 2^{-k}\}$
2	2	2^k	2	$\{2^{-k}, 3\cdot 2^{-k}\}$

TABLE 4.1. representatives for $\frac{1}{\Delta}(\mathbb{Z}/\alpha d_1)^\times/((\mathbb{Z}/\alpha d_1)^\times)^2$

(G,q)	disc(q)
$w^1_{p,k}$, p odd	p^{-k}
$w^{-1}_{p,k}$, p odd	$p^{-k}u$, where u is a non-square mod p
$w^{\varepsilon}_{2,k}$, $k \geq 2$	$2^{-k}u$, where $\chi(u) = \varepsilon \mod 8$
$w^{\varepsilon}_{2,1}$	$2^{-1}u$, where $\chi(u) = \varepsilon \mod 4$
u_k	-2^{-2k}
v_k	$3\cdot 2^{-2k}$

TABLE 4.2. discriminants of finite quadratic forms

Corollary (3.4) applies in our situation as well, and, recalling that $\left(\frac{R}{d_1}\right)^\times \cong \left(\frac{R}{\alpha d_1}\right)^\times$, we obtain a well-defined element

$$\det(B_{ij}) \in ((R/\alpha d_1)^\times)^2 \backslash \frac{1}{\Delta}R/\frac{\alpha d_1}{\Delta}R$$

DEFINITION 4.4. Let (G,q) be a torsion quadratic form over R. The *discriminant* of (G,q), denoted by disc(G,q) (or disc(G), or disc(q)) is the class of $\det B$ in $((R/\alpha d_1)^\times)^2\backslash\frac{1}{\Delta}R/\frac{\alpha d_1}{\Delta}R$, where B is any representing matrix for q.

Again, by (4.2.3), if q is nondegenerate, disc(q) takes values in

$$\frac{1}{\Delta}\left(\frac{R}{\alpha d_1}\right)^\times / \left(\left(\frac{R}{\alpha d_1}\right)^\times\right)^2 = \frac{1}{\Delta}\mathcal{D}\left(\frac{R}{\alpha d_1}\right).$$

If $R = \mathbb{Z}$ and G is p-primary, then $d_1 = p^{e_1}$ and $\Delta = p^k$ for two integers $1 \leq e_1 \leq k$. In this case we have the values shown in Table 4.1 for disc(q) in the nondegenerate case:

The values for the discriminants of the standard examples from (I, section 7) are given in Table 4.2.

We will again find it useful to employ the χ notation to factor out the powers of p in the p-primary situations.

If p is odd, and $d \in \frac{1}{p^k}(\mathbb{Z}/p^{e_1})^\times/((\mathbb{Z}/p^{e_1})^\times)^2$ is a discriminant value, we set $\chi(d) = 1$ if $d \equiv p^{-k}$, and $\chi(d) = -1$ if $d \equiv p^{-k}u$ for a non-square

$u \bmod p$. Note that abusing the notation somewhat this formula reads that $\chi(d) = \chi(p^k d)$.

With this same abuse of notation, if $p = 2$, and $\Delta = 2^k$, then we set $\chi(d) = \chi(2^k d)$ which is a unit $\bmod 8$ if $k \geq 2$, and is a unit $\bmod 4$ if $k = 1$.

The discriminant for a torsion quadratic form satisfies similar properties as does the discriminant for a torsion bilinear form. We present these below, leaving the proofs (which are entirely analogous to the bilinear case) to the reader. We also employ the same notational conventions used in the previous section.

PROPOSITION 4.5.

(4.5.1) Fix a prime p of R and let (G, q) and (G', q') be two p-primary torsion quadratic forms over R; let $(G \oplus G', q + q')$ denote their orthogonal direct sum. Then $\operatorname{disc}(q + q') = \operatorname{disc}(q) \operatorname{disc}(q')$.

(4.5.2) Let (G, q) be a p-primary quadratic form with order Δ and let B be a representing matrix for q. Then (G, q) is nondegenerate if and only if $p \not| \Delta \cdot \det(B)$, i.e., if $\operatorname{disc}(q)$ *is a unit.*

(4.5.3) Let (G, q) be a torsion quadratic form over R and fix a prime p. Assume that G and G_p have the same length, i.e., p divides the first invariant of G. Then $\operatorname{disc}(G_p, q_p) = (\operatorname{disc}(G, q))_p$, *where $q_p = q|_{G_p}$ is the induced quadratic form on G_p.*

Finally, the discriminant of a torsion quadratic form is compatible with the discriminant of the associated bilinear form in the following sense. There is a natural map

$$((R/\alpha d_1)^\times)^2 \backslash \frac{1}{\Delta} R / \frac{\alpha d_1}{\Delta} R \to ((R/d_1)^\times)^2 \backslash \frac{1}{\Delta} R / \frac{d_1}{\Delta} R$$

namely, the " $\bmod d_1$" map. It sends values for $\operatorname{disc}(q)$ to values for $\operatorname{disc}(\langle -, - \rangle)$.

LEMMA 4.6. *Let (G, q) be a torsion quadratic form with associated bilinear form $\langle -, - \rangle$. Then* $\operatorname{disc}(q) = \operatorname{disc}\langle -, - \rangle \bmod d_1$.

The proof is immediate.

5. The Functor τ

In this section we will define another useful functor, the τ functor, which will be used in the sequel to refine the discriminant of a quadratic form in certain cases. We begin with a description of these "special" forms.

DEFINITION 5.1. Let G be a torsion R-module.

(5.1.1) A torsion bilinear form $\langle -, - \rangle$ on G is *special* if whenever $x \in G$ and $2x = 0$ then $\langle x, x \rangle = 0$.

(5.1.2) A torsion quadratic form q on G is *special* if its associated bilinear form is, i.e., whenever $x \in G$ and $2x = 0$ then $2q(x) = 0$.

(5.1.3) A torsion bilinear form $\langle -, - \rangle$ on G is *extraspecial* if it is special, and whenever $x \in G$ and $4x = 0$ then $2\langle x, x \rangle = 0$.

Recall that for a torsion R-module G, the subgroup $G_{2,1} = \{x \in G \,|\, 2x = 0\}$ is defined (2.1). Hence, a torsion form $\langle -, - \rangle$ on G is special if $x \in G_{2,1}$ implies $\langle x, x \rangle = 0$. Note that if $x, y \in G_{2,1}$, then $\langle x + y, x + y \rangle = \langle x, x \rangle + \langle y, y \rangle$, so to check whether $\langle -, - \rangle$ is special it suffices to check that $\langle f_i, f_i \rangle = 0$ for a generating set $\{f_i\}$ for $G_{2,1}$.

We will adopt the notation that, for a torsion R-module G, G' will denote the quotient module $G' = \frac{G}{G_{2,1}}$. Given $x \in G$, x' will denote its image in G'; given $x' \in G$, x will denote a lift of x' to G.

Definition 5.2. Let $(G, \langle -, - \rangle)$ be a special torsion symmetric bilinear form over R. Define $\tau(G, \langle -, - \rangle) = (G', q')$ to be the torsion quadratic form defined on G' by

$$q'(x) = \langle x, x \rangle.$$

To see that q' is well defined, suppose that $z \in G_{2,1}$; then $\langle x, 2z \rangle = 0$ and $\langle z, z \rangle = 0$ since $\langle -, - \rangle$ is special. Therefore, $\langle x + z, x + z \rangle = \langle x, x \rangle$. To see that q' is quadratic, note that $q'(rx') = \langle rx, rx \rangle = r^2 \langle x, x \rangle = r^2 q'(x')$; in addition, the associated bilinear form to q'is $\langle -, - \rangle'$ where

$$\begin{aligned} \langle x', y' \rangle &= q'(x' + y') - q'(x') - q'(y') \\ &= \langle x + y, x + y \rangle - \langle x, x \rangle - \langle y, y \rangle \\ &= 2\langle x, y \rangle \end{aligned}$$

which is bilinear.

Lemma 5.3.

(5.3.1) If $(G, \langle -, - \rangle)$ is nondegenerate, then $\tau(G, \langle -, - \rangle)$ is nondegenerate.

(5.3.2) $(G, \langle -, - \rangle)$ is extra special $\Leftrightarrow$ $\tau(G, \langle -, - \rangle)$ is special.

(5.3.3) τ is additive.

Proof. Suppose $x' \in \operatorname{Ker} \mathrm{Ad}_{\langle -, - \rangle'}$; then for all $y \in G$,

$$\langle 2x, y \rangle = 2\langle x, y \rangle = \langle x', y' \rangle = 0.$$

Since $\langle -, - \rangle$ is nondegenerate, $2x = 0$ in G, so $x \in G_{2,1}$ and $x' = 0$. This proves (5.3.1); the last statements are obvious. Q.E.D.

Our first task is to show that any torsion quadratic form can be obtained as τ of a special torsion bilinear form.

LEMMA 5.4. *Let (G', q') be a torsion quadratic form over R and let $\{e'_i\}$ be an ordered basis of G' with invariants $\{d'_i\}$. For each i, define*

$$d_i = \begin{cases} d'_i & \text{if } (d'_i, 2) = 1 \\ 2d'_i & \text{if } (d'_i, 2) \neq 1 \end{cases}$$

and let G be the torsion R-module with ordered basis $\{e_i\}$ and invariants $\{d_i\}$. (Note that $\frac{G}{G_{2,1}} \cong G'$, the isomorphism induced by sending e_i to e'_i; hence, there should be no confusion with the notation.) Then there is a special symmetric bilinear form $\langle -, - \rangle$ on G such that $\tau(G, \langle -, - \rangle) \cong (G', q')$.

PROOF. Choose elements $b'_{ij} \in K$ such that

(1) $b'_{ji} = b'_{ij}$

(2) $b'_{ij} = \langle e'_i, e'_j \rangle'$ mod R, where $\langle -, - \rangle'$ is the associated bilinear form to q'

(3) $\frac{1}{2} b'_{ii} = q'(e'_i)$ mod R

(4) If $(d'_i, 2) = 1$ and $i \leq j$ then $\frac{1}{2} d'_i b'_{ij} \in R$.

Only property (4) needs justification. If $(d'_i, 2) = 1$ and $i \leq j$, then $d'_i b'_{ij} \equiv \langle d'_i e'_i, e'_j \rangle = 0$ mod R, so that $b'_{ij} = \frac{a'_{ij}}{d'_i}$ for some a'_{ij} in R. Since $(d'_i, 2) = 1$, there exist α_i, β_i in R with $2\alpha_i + d'_i \beta_i = 1$. Then $\frac{a'_{ij}}{d'_i} - \beta_i a'_{ij} = \frac{2\alpha_i a'_{ij}}{d'_i}$; thus, choosing appropriate representatives of $\langle e'_i, e'_j \rangle$ in K, we may ensure that the numerators $2\alpha_i a'_{ij}$ are even (divisible by 2).

We now define $\langle -, - \rangle$ on G by setting $\langle e_i, e_j \rangle = \frac{1}{2} b'_{ij}$ mod R and extending by linearity.

To see that $\langle -, - \rangle$ is well defined, we must check that $\langle d_i e_i, e_j \rangle = 0$ mod R for every i and j.

If $(d_i, 2) \neq 1$, then $d_i = 2d'_i$, so that $\langle d_i e_i, e_j \rangle = \frac{1}{2} d_i b'_{ij} = d'_i b'_{ij} = \langle d'_i e'_i, e'_j \rangle' = 0$ mod R.

If $(d_i, 2) = 1$ and $i \leq j$, then $d_i = d'_i$, so that $\langle d_i e_i, e_j \rangle = \frac{1}{2} d'_i b'_{ij} = \frac{1}{2} d'_i b'_{ij} = 0$ mod R by property (4).

If $(d_i, 2) = 1$ and $i > j$, then $d_j | d_i$, $d_i = d'_i$ and $d_j = d'_j$, so that $\langle d_i e_i, e_j \rangle = \frac{1}{2} d_i b'_{ij} = \frac{d_i}{d_j} \cdot \frac{1}{2} d'_j b'_{ji} = 0$ mod R, again by (4).

Therefore, $\langle -,- \rangle$ is well defined. To see that $\langle -,- \rangle$ is special, note that $G_{2,1}$ has $\{d'_i e_i\}$ as a generating set. Therefore, since

$$\begin{aligned} \langle d'_i e_i, d'_i e_i \rangle &= (d'_i)^2 \langle e_i, e_i \rangle \\ &= (d'_i)^2 \frac{1}{2} b'_{ii} \\ &= (d'_i)^2 q'(e'_i) \\ &= q'(d'_i e'_i) \\ &= 0 \mod R, \end{aligned}$$

$\langle -,- \rangle$ is indeed special.

Finally, note that $\tau(G, \langle -,- \rangle) = (G', q')$, since

$$\begin{aligned} q'\left(\sum_i n_i e'_i\right) &= \sum_i n_i^2 q'(e'_i) + \sum_{i<j} n_i n_j \langle e'_i, e'_j \rangle' \\ &= \frac{1}{2} \sum_i n_i^2 b'_{ii} + \sum_{i<j} n_i n_j b'_{ij} \\ &= \sum_i n_i^2 \langle e_i, e_i \rangle + 2 \sum_{i<j} n_i n_j \langle e_i, e_j \rangle \\ &= \langle \sum_i n_i e_i, \sum_i n_i e_i \rangle. \end{aligned}$$

Q.E.D.

The structure of $G_{2,1}$ and G' are obviously of some importance for the functor τ. We need the following language.

DEFINITION 5.5. A torsion R-module G is *good* if $G_{2,1}$ is homogeneous with annihilator $2R$ and is *better* if whenever $x \in G_{2,1}$, then $x = 2y$ for some $y \in G$.

LEMMA 5.6.

(5.6.1) Assume G has invariants $\{d_i\}$. Then

G is good $\Leftrightarrow$ whenever $(d_i, 2) \neq 1$, then $2|d_i$

and

G is better $\Leftrightarrow$ whenever $(d_i, 4) \neq 1$, then $4|d_i$.

Hence G better $\Rightarrow$ G good.

(5.6.2) If G is better then $G' = \frac{G}{G_{2,1}}$ is good. Conversely, for any good module G' there is a better module G such that $\frac{G}{G_{2,1}} \cong G'$.

(5.6.3) If $\langle -,- \rangle$ is a symmetric bilinear form on a better module G, then $\langle -,- \rangle$ is special.

(5.6.4) If 2 is either a prime or a unit in R, then every torsion R-module is good.

PROOF. The first statement (5.6.1) is clear. The first part of (5.6.2) is also clear, and the second part is the construction introduced in Lemma (5.4). To see (5.6.3), assume $2x = 0$; then $x = 2y$ for some y, so that $\langle x, x\rangle = \langle 2y, 2y\rangle = 4\langle y, y\rangle = \langle 4y, y\rangle = 0$. Finally, the last statement is immediate from (5.6.1). Q.E.D.

LEMMA 5.7. *Suppose $(G, \langle -, -\rangle)$ is a torsion bilinear form and G is better. If $\tau(G, \langle -, -\rangle)$ is nondegenerate, then $(G, \langle -, -\rangle)$ is nondegenerate.*

PROOF. Let $x \in \operatorname{Ker} \mathrm{Ad}_{\langle -,-\rangle}$. Then $\langle x', z'\rangle = 2\langle x, z\rangle = 0$ for all $z' \in G'$, so that $x' \in \operatorname{Ker} \mathrm{Ad}_{\langle -,-\rangle'}$, forcing $x' = 0$ so that $x \in G_{2,1}$. Since G is better, $x = 2y$ for some $y \in G$. Assume $x \neq 0$; then $y' \in G$ is not zero, so there exists $z' \in G$ with $\langle y', z'\rangle \neq 0$. For some $z \in G$ mapping to z', $\langle x, z\rangle = \langle 2y, z\rangle = 2\langle y, z\rangle = \langle y', z'\rangle' \neq 0$, *a* contradiction. Hence, $x = 0$ and $\langle -, -\rangle$ is nondegenerate. Q.E.D.

There is also a uniqueness statement related to (5.6.2).

LEMMA 5.8. *Suppose G is a torsion R-module, and $\langle -, -\rangle_1$ and $\langle -, -\rangle_2$ are two special torsion symmetric bilinear forms on G such that*

$$\tau(G, \langle -, -\rangle) = \tau(G, \langle -, -\rangle_2), \text{ and}$$
$$(G', q') = \tau(G, \langle -, -\rangle_i) \text{is nondegenerate.}$$

Then there is an isometry $\psi : (G, \langle -, -\rangle_1) \to (G, \langle -, -\rangle_2)$.

PROOF. By (5.7), each $\langle -, -\rangle_i$ is nondegenerate. Consider the symmetric bilinear form $\beta(x, y) = \langle x, y\rangle_1 - \langle x, y\rangle_2$. Note that

$$2\beta(x, y) = 2\langle x, y\rangle_1 - 2\langle x, y\rangle_2 = \langle x', y'\rangle' - \langle x', y'\rangle' = 0$$

for every $x, y \in G$, and

$$\beta(x, x) = \langle x, x\rangle_1 - \langle x, x\rangle_2 = q'(x') - q'(x') = 0$$

for every $x \in G$.

These two properties guarantee the existence of a (non-symmetric) bilinear form γ on G such that $\beta(x, y) = \gamma(x, y) + \gamma(y, x)$ and $2\gamma(x, y) = 0$. For example, if $\{e_i\}$ is an ordered basis of G, we may set

$$\gamma(e_i, e_j) = \begin{cases} \beta(e_i, e_j) & \text{if } i<j \\ 0 & \text{if } i \geq j. \end{cases}$$

γ measures the difference between the two forms and by induction on the length of G we may assume there exist I, J such that $\gamma(e_i, e_j) = 0$ when $i = I$ and $j = \mathrm{J}$.

Let $\varphi = (\mathrm{Ad}_{\langle -,-\rangle_2})^{-1}\,\mathrm{Ad}_\gamma$, so that $\gamma(x,z) = \langle \varphi(x), z\rangle$ for all x and z, and define $\psi(x) = x + \varphi(x)$.

Note that $\langle 2y(x), z\rangle_2 = 2\gamma(x,z) = 0$ for all z, so that $2\varphi(x) = 0$. If $i \neq I$, then $\varphi(e_i) = 0$; hence, $\langle \varphi(e_i), \varphi(e_j)\rangle_2 = 0$ unless $i = j = \mathrm{I}$. But since $\langle -,-\rangle_2$ is special and $2\varphi(e_I) = 0, \langle \varphi(e_I), \varphi(e_I)\rangle_2 = 0$, also. Hence, $\langle \varphi(x), \varphi(y)\rangle_2 = 0$ for every x and y; therefore,

$$\begin{aligned}\langle \psi(x), \psi(y)\rangle_2 &= \langle x,y\rangle_2 + \langle \varphi(x), y\rangle_2 + \langle \varphi(y), x\rangle_2 + \langle \varphi(x), \varphi(y)\rangle_2 \\ &= \langle x,y\rangle_2 + \gamma(x,y) + \gamma(y,x) \\ &= \langle x,y\rangle_2 + \beta(x,y) \\ &= \langle x,y\rangle_1\end{aligned}$$

so that $\psi : G \to G$ maps $\langle -,-\rangle_1$ to $\langle -,-\rangle_2$. Moreover, if $x \in \operatorname{Ker}\psi$ then $\langle x,y\rangle_1 = \langle \psi(x), \psi(y)\rangle_2 = \langle 0, \psi(y)\rangle_2 = 0$ for every y, forcing $x = 0$. Therefore, ψ is an isomorphism of R-modules, hence an isometry. Q.E.D.

By applying (5.6.3), we have

Corollary 5.9.

(5.9.1) Suppose G is a better torsion R-module, and $\langle -,-\rangle_1$ and $\langle -,-\rangle_2$ are two torsion symmetric bilinear forms on G such that

$$\tau(G, \langle -,-\rangle_1) = \tau(G, \langle -,-\rangle_2), \textit{and}$$

$$(G', q') = \tau(G, \langle -,-\rangle_i) \textit{is nondegenerate.}$$

Then there is an isometry $\psi : (G, \langle -,-\rangle_1) \to \tau(G, \langle -,-\rangle_2)$.

(5.9.2) τ establishes a 1-1 correspondence between

$$\left\{\begin{matrix}\textit{isometry classes of nonde-}\\ \textit{generate symmetric bilinear}\\ \textit{forms on better } R\textit{-modules}\end{matrix}\right\} \textit{ and } \left\{\begin{matrix}\textit{isometry classes of nonde-}\\ \textit{generate quadratic forms on}\\ \textit{good } R\textit{-modules}\end{matrix}\right\}$$

Under this correspondence, extraspecial bilinear forms on better modules correspond to special quadratic forms.

Let us display in Table 5.1 the "standard" torsion R-modules and the behavior of the functor τ on them.

6. The Discriminant of a Good Special Torsion Quadratic Form

There is a refinement of the discriminant for a torsion quadratic form (defined in section 4) in case the form is good and special. We first treat the case of a torsion bilinear form which is better and extra special. In this section we work only over $R = \mathbb{Z}_2$.

R	$(G, \langle -, - \rangle)$	good/better?	special?	$\tau(G, \langle -, - \rangle)$
$\mathbb{Z}_p$, p odd	$\bar{w}^{\varepsilon}_{p,k}$	better	extra special	$w^{\varepsilon}_{p,k}$
$\mathbb{Z}_2$	$\bar{w}^{\varepsilon}_{2,1}$	good	no	(0)
$\mathbb{Z}_2$	$\bar{w}^{\varepsilon}_{2,2}$	better	special	$w^{\varepsilon}_{2,1}$
$\mathbb{Z}_2$	$\bar{w}^{\varepsilon}_{2,k}$, $k \geq 3$	better	extra special	$w^{\varepsilon}_{2,k-1}$
$\mathbb{Z}_2$	$\bar{u}_1$	good	extra special	(0)
$\mathbb{Z}_2$	$\bar{v}_1$	good	extra special	(0)
$\mathbb{Z}_2$	$\bar{u}_k$, $k \geq 2$	better	extra special	u_{k-1}
$\mathbb{Z}_2$	$\bar{v}_k$, $k \geq 2$	better	extra special	v_{k-1}

TABLE 5.1. the functor τ

Let $(G, \langle -, - \rangle)$ be a better and extra special nondegenerate torsion bilinear form over $\mathbb{Z}_2$. As in section 4, let $\{g_i\}$ be an ordered basis for G, with invariants $\{d_i\}$ and choose "symmetric" representatives $\{B_{ij}\}$ in $K = \mathbb{Q}_2$ for the values of $\langle -, - \rangle$ so that $\langle g_i, g_j \rangle \equiv B_{ij} \mod R$, with $B_{ij} = B_{ji}$. Since G is better, $d_1 \geq 4$. The extra special assumption means that if $d_i = 4$, then $2B_{ii} \in R$.

We have the following analogue of (4.2).

LEMMA 6.1. *Let $\Delta = \prod_i d_i$ and assume $\{B_{ij}\}$ is as above.*

(6.1.1) $\Delta \cdot \det(B_{ij}) \in R$

(6.1.2) If (B_{ij}) and (B'_{ij}) are two such symmetric matrices, then

$$\Delta \cdot [\det(B_{ij}) - \det(B'_{ij})] \in 8R.$$

PROOF. The first statement is simply (3.2.1) again. The proof of (6.1.2) is along the lines of that of (4.2.2). Firstly, if $d_1 \geq 8$, we are done by (3.2.2). Therefore, we may assume $d_1 = 4$, which implies $2B_{11} \in R$. We may further assume that (B_{ij}) and (B'_{ij}) differ only in one entry on or above the diagonal.

If $B' = B + rE_{i_0 i_0}$ for some i_0 and $r \in R$, then

$$\Delta \cdot [\det B' - \det B] = d_{i_0} r \left(\prod_{i \neq i_0} d_i \right) \det B[i_0, i_0],$$

which is in $8R$ if $d_{i_0} \geq 8$. Assume then that $d_{i_0} = 4$, or equivalently that $i_0 = 1$. If $\left(\prod_{i \neq i_0} d_i \right) (\det B[i_0, i_0])$ is a unit in $\mathbb{Z}_2$, then the subgroup H of G generated by $\{g_2, \ldots, g_n\}$ is nondegenerate, thus splitting off of G; therefore, G has an orthogonal direct summand which is cyclic of order 4, namely the complement of H. This order 4 subgroup must

$(G, \langle -,- \rangle)$ or (G, q)	$\operatorname{disc}_8 G$
$\bar{w}^{\varepsilon}_{2,k}$, $k \geq 3$	ε
$\bar{u}_k$, $k \geq 2$	7
$\bar{v}_k$, $k \geq 2$	3
$w^{\varepsilon}_{2,k}$, $k \geq 2$	ε
u_k	7
v_k	3

TABLE 6.1. the mod 8 discriminant

be nondegenerate, since G is; however, this contradicts the extra specialness of G. Therefore, $\left(\prod_{i \neq i_0} d_i\right)(\det B[i_0, i_0])$ is divisible by 2, so that $\Delta \cdot [\det B' - \det B] \in 8R$ as required.

If $B' = B + rE_{i_0 j_0} + rE_{j_0 i_0}$ for some $i_0 \lneqq j_0$ and $r \in R$, the calculation in the proof of (4.2.2) shows that $\Delta \cdot [\det B_{ij} - \det B'_{ij}] \in 8\mathrm{R}$. Q.E.D.

Since $((\mathbb{Z}/8)^{\times})^2 = \{1\}$, the above lemma gives us a well-defined element $\Delta \cdot \det(B_{ij})$ in $(\mathbb{Z}/8)^{\times}$.

DEFINITION 6.2. Let $(G, \langle -,- \rangle)$ be a better and extra special nondegenerate torsion biliniear form over $\mathbb{Z}_2$. The *mod 8 discriminant* of $(G, \langle -,- \rangle)$, denoted by $\operatorname{disc}_8(G, \langle -,- \rangle)$ (or $\operatorname{disc}_8(G)$, or $\operatorname{disc}_8\langle -,- \rangle$) is the element $\Delta \cdot \det(B_{ij})$ in $(\mathbb{Z}/8)^{\times}$.

Using the functor τ, we can extend this mod 8 discriminant to good and special nondegenerate quadratic forms. Let (G', q') be such a form over $\mathbb{Z}_2$. Let $(G, \langle -,- \rangle)$ be the unique better and extra special nondegenerate torsion bilinear form over $\mathbb{Z}_2$ (unique up to isometry, by (5.9)) with $\tau(G, \langle -,- \rangle) = (G', q')$.

DEFINITION 6.3. The *mod 8 discriminant* of (G', q'), denoted by $\operatorname{disc}_8(G', q')$ (or $\operatorname{disc}_8 G'$, or $\operatorname{disc}_8 q'$) is the mod 8 discriminant of $(G, \langle -,- \rangle)$.

Table 6.1 shows the mod 8 discriminants for the standard examples.

Comparing these values to those of Table (4.2), at first glance it may seem that we haven't gained much; these values are simply $|G|$ times the values for the ordinary discriminant. However, for u_1, and v_1 the above values are defined mod 8, while the ordinary discriminant is only defined mod 4.

7. The Discriminant-Form Construction

In this section R will be an integral domain and K its quotient field.

DEFINITION 7.1. Let M be a finite-dimensional vector space over the quotient field K. An *R-lattice in M* is a free finitely generated R-submodule L of M such that the natural map from $L \otimes_R K$ to M is an isomorphism. An *R-lattice* is an R-lattice in M for some finite-dimensional vector space M over K.

The rank of the R-lattice over R is the same as the dimension of M over K; every R-lattice in M can be given as the R-span of a K-basis of M. If L is a finitely generated free R-module, then one can consider L as being naturally an R-lattice in $L_K = L \otimes_R \mathrm{K}$.

Let L be a finitely generated free R-module and let $\langle -, - \rangle$ be a K-valued symmetric bilinear form on L, which is nondegenerate. The extension $L_K = L \otimes_R K$ inherits the bilinear form; simply set $\langle l_1 \otimes k_1, l_2 \otimes k_2 \rangle_K = k_1 k_2 \langle l_1, l_2 \rangle$. In this way $(L_K, \langle -, - \rangle_K)$ is a K-valued symmetric bilinear form over K, and is also nondegenerate.

Conversely, suppose a K-valued symmetric bilinear form is given on a finite-dimensional vector space M over K. If L is any R-lattice in M, then the restriction of the form to L is a K-valued symmetric bilinear form on L, nondegenerate if the original form is. This operation is inverse to the previous extension operation.

In this situation there is a natural notion of duality.

DEFINITION 7.2. Let $(M, \langle -, - \rangle)$ be a nondegenerate symmetric K-valued bilinear form on a finite-dimensional vector space M over K. For any R-lattice L in M, define its *dual lattice* $L^\#$ in M by

$$L^\# = \{ m \in M \mid \langle m, l \rangle \in R \text{ for every } l \in L \}.$$

If $(L, \langle -, - \rangle)$ is a nondegenerate symmetric K-valued bilinear form on a free f.g. R-module L, its dual lattice $L^\#$ will denote its dual lattice in L_K.

The first thing to check is that in fact $L^\#$ is a lattice in M. It is enough to consider the case when $M = L_K$.

The R-dual $L^* = \mathrm{Hom}_R(L, R)$ of L is, of course, also a finitely generated free R-module with the same rank.

LEMMA 7.3. *Assume $(L, \langle -, - \rangle)$ is a nondegenerate K-valued symmetric bilinear form over R as above. Then the map $\alpha : L^\# \to L^*$ defined by sending x to $\mathrm{Ad}_{L_K}(x)|_L = \langle x, - \rangle$ is an isomorphism of R-modules.*

PROOF. It is clear that the above map α is well-defined, and maps $L^\#$ to L^*. Let us first show that α is onto. Choose any f in L^* and consider the extension $\widetilde{f}$ of f in $L_K^* = \mathrm{Hom}_K(L_K, K)$. Let $x =$

$\mathrm{Ad}_{L_K}^{-1}(\widetilde{f})$, i.e., $x \in L_K$ and $\widetilde{f}(y) = \langle x, y\rangle$ for every $y \in L_K$. Since $\widetilde{f}$ extends f, and f is in L^*, x must be in $L^\#$. Since $\alpha(x) = f$, we have proved α is onto.

Since L is nondegenerate, Ad_{L_K} is an isomorphism, so the restriction $\alpha = \mathrm{Ad}_{L_K}|_L = \mathrm{Ad}_{L^\#}$ is injective. Q.E.D.

The above lemma suffices to show that $L^\#$ is an R-lattice in L_K. It of course inherits a K-valued bilinear form (denoted $\langle -, -\rangle_{L^\#}$) from the induced form on L_K. It is nondegenerate, since the form on L_K is.

If $\{e_i\}$ is a basis for L over R, define a "dual basis" $\{e_i^\#\}$ for $L^\#$ by transporting the dual basis $\{e_i^*\}$ of L^* via $\alpha : e_i^\# = \alpha^{-1}(e_i^*)$. The vectors $e_i^\#$ can also be defined by the property that $\langle e_i^\#, e_j\rangle_{L_K} = \delta_{ij}$, the Kronecker delta.

A special case of the above situation is afforded when $(L, \langle -, -\rangle)$ is an *R-valued* form over R. In this case, as lattices in $L_K, L \subseteq L^\#$. In particular, if (L, Q) is a quadratic R-module, then $L \subseteq L^\#$. The adjoint map Ad_L from L to L^* can be viewed as the composition of the inclusion of L into $L^\#$, followed by the isomorphism α of the previous lemma.

Definition 7.4. Let (L, Q) be a quadratic R-module. The *discriminant-form module* of (L, Q) is the torsion R-module $G_L = L^\#/L$.

By Lemma (I.3.2), a matrix for Ad_L is given by a matrix for Q, so that if $R = \mathbb{Z}, G_L$ is a finite abelian group of order equal to $|\operatorname{disc}(L)|$. If $R = \mathbb{Z}_p$ and $\operatorname{disc}(L) = p^e u \mod \mathbb{U}_p^2$, where $u \in \mathbb{U}_p$, then G_L is a finite abelian p-group of order p^e, using similar considerations. In general, if R is a P.I.D. and $\{d_1, \ldots, d_n\}$ are the invariants of G, with $\Delta = \prod d_i$, then $\Delta \equiv \operatorname{disc}(L) \mod \frac{R^\times}{(R^\times)^2}$ in the value group $\frac{(R-\{0\})}{(R^\times)^2}$.

The quadratic form Q on L induces one, Q_K, on $L_K(I, (8.1))$. The restriction of Q_K to $L^\#$ induces a K-valued quadratic form $Q_\#$ on $L^\#$, which is also nondegenerate.

The plot now thickens: the discriminant-form module also inherits the quadratic form by defining

$$q_L(x + L) = Q_\#(x) \mod R \in K/R.$$

Proposition 7.5. *Let (L, Q) be a quadratic R-module. Then (G_L, q_L) is a well-defined nondegenerate torsion quadratic form over R.*

PROOF. Assume $x, y \in L^\#$ with $x - y \in L$; write $x = y + l$. Then

$$\begin{aligned} q_L(x+L) &= Q_\#(x) \mod R \\ &= Q_\#(y+l) \mod R \\ &= Q_\#(y) + Q_\#(l) + \langle y, l\rangle_\# \mod R \\ &= Q_\#(y) + Q(l) \mod R \text{ since } \langle y, l\rangle_\# \in R \\ &= Q_\#(y) \mod R \text{ since } Q(l) \in R \\ &= q_L(y+L); \end{aligned}$$

hence, q_L is well defined. It is trivial to check that it is a quadratic form. Finally, to see that it is nondegenerate, assume $x + L$ is in the kernel of Ad_{G_L}. Let [-,-] denote the associated bilinear form to q_L on G_L. Then $[x+L, y+L] = 0$ for all y in $L^\#$; however, from the definition of q_L, $[x+L, y+L] = \langle x, y\rangle \mod R$, so that $\langle x, y\rangle_\# \in R$ for all y in $L^\#$. Since $(L^\#)^\# = L$, this implies $x \in L$, so that $x + L = 0$ in G_L. Q.E.D.

We will usually denote the associated bilinear form to q_L on G_L by $\langle -, -\rangle_{G_L}$.

Note that $G_L = (0)$ if and only if L is unimodular. Also, any splitting of L induces one of $G_L : G_{L\oplus M} \cong G_L \oplus G_M$ as torsion forms over R.

As an example, assume $\mathrm{char}(R) \neq 2$ and let $L = \langle a\rangle_R$. (That is, L is a rank-one R-module generated by $e \in L$, and $Q(e) = a$.) The dual $L^\# \subset L_K$ is generated by $e^\# = (1/2a)\cdot e$, and $Q_\#(e^\#) = (1/4a^2)\cdot Q(e) = 1/4a \in K$. The adjoint map sends e to $2ae^\#$, so that $G_L \cong R/(2a)$ is generated by the class of $e^\#$ mod L. Since $q(e^\#) = 1/2 \cdot 2a \mod R$, we see that $(G_L, q_L) \cong z^1_{2a}$.

A related example is this. Consider the form $(L, Q) = \langle a\rangle_{\mathbb{Z}_{(}} = \langle (1/2)p^k u\rangle_{\mathbb{Z}_{(}}$ (whose isomorphism class is $W^\varepsilon_{p,k}$, where $\varepsilon = \chi(u)$). If e generates the rank-one $\mathbb{Z}_{(}$-module L, with $Q(e) = (1/2)p^k u$, then $p^{-k}e$ generates $L^\# \subset L_K$. We have $G_L \cong \mathbb{Z}_{(}/(\ulcorner)$, and $Q_\#(p^{-k}e) = p^{-2k}\cdot Q(e) = u/2p^k$, so that $(G_L, q_L) \cong z^u_{p^k}$. Since $\chi(u) = \varepsilon$, this is the form whose isomorphism class was denoted by $w^\varepsilon_{p,k}$.

Similar calculations for U_k and V_k will enable the reader to complete the verification of Table 7.1, which shows the discriminant-form modules for the standard examples of Chapter I.

As one application of discriminant-forms, we give a characterization of indecomposable torsion quadratic forms over $\mathbb{Z}_{\not 2}$ of rank two.

LEMMA 7.6. *Let (G, q) be a nondegenerate indecomposable torsion quadratic form over $\mathbb{Z}_{\not 2}$ of rank two. (Note that (G, q) is necessarily good and special.) Let $\delta = \mathrm{disc}_8(G, q)$. Then $(G, q) \cong u_k$ if and only if*

R	(L,Q)	(G_L,q_L)
$\mathbb{Z}$	$\langle a\rangle$	z^1_{2a}
$\mathbb{Z}_{(}$, p odd	$W^1_{p,k}$	$w^1_{p,k}$
$\mathbb{Z}_{(}$, p odd	$W^{-1}_{p,k}$	$w^{-1}_{p,k}$
$\mathbb{Z}_{\not 2}$	$W^{\varepsilon}_{2,k}$	$w^{\varepsilon}_{2,k}$
$\mathbb{Z}_{\not 2}$	U_k	u_k
$\mathbb{Z}_{\not 2}$	V_k	v_k

TABLE 7.1. discriminant-form modules

(G,q) has scale 2^k and $\left(\frac{2}{\delta}\right)=1$, while $(G,q)\cong v_k$ if and only if (G,q) has scale 2^k and $\left(\frac{2}{\delta}\right)=-1$.

PROOF. There clearly exists a nondegenerate quadratic $\mathbb{Z}_{\not 2}$-module of rank two (L,Q) whose discriminant-form is (G,q). If (L,Q) were decomposable, the orthogonal direct sum decomposition into two cyclic pieces would induce an orthogonal direct sum decomposition of (G,q), contrary to hypothesis. Thus, (L,Q) is indecomposable, so by lemma (7.7) of chapter I, (L,Q) must be isomorphic to U_k or V_k for some k. But Then by table (7.1), (G,q) is isomorphic to u_k or v_k for some k. Since u_k and v_k each have scale 2^k and satisfy the given conditions on the mod-8 discriminants, these two properties characterize their isomorphism classes: the scale of (G,q) identifies k, and the mod-8 discriminant distinguishes between u_k and v_k. Q.E.D.

COROLLARY 7.7. *If we multiply all the values of the quadratic form u_k or v_k by a fixed unit in $\mathbb{Z}_{\not 2}$, the isomorphism class does not change.*

PROOF. The scale is not affected (being a property of the group), and the mod-8 discriminant is simply multiplied by the square of the fixed unit, and so remains unchanged. Q.E.D.

Returning to the free R-modules L and $L^{\#}$, assume that the matrix of Q_L with respect to a basis $\{e_i\}$ for L is A.

LEMMA 7.8. *The matrix for $Q_{L^{\#}}$ with respect to the dual basis $\{e_i^{\#}\}$ for $L^{\#}$ is A^{-1}.*

PROOF. Write $e_i^{\#}=\sum c_{ij}e_j$, with $c_{ij}\in K$ and let $C=(c_{ij})$ be the associated matrix. Note that $\sum_j c_{kj}\langle e_j,e_i\rangle_L=\langle\sum_j c_{kj}e_j,e_i\rangle_L=\langle e_k^{\#},e_i\rangle_{L_K}=\delta_{ik}$. Hence, CA is the identity matrix. Since A is symmetric, so is C; moreover, if B is the matrix for $Q_{L^{\#}}$, then $B=C^TAC=C^T=C=A^{-1}$. Q.E.D.

COROLLARY 7.9. *Let L be a quadratic R-module. Then*

$$\operatorname{disc}(L)\operatorname{disc}(L^{\#}) = 1.$$

Note that $\operatorname{disc}(L) \in \frac{R-\{0\}}{(R^{\times})^2}$ while $\operatorname{disc}(L^{\#}) \in \frac{K-\{0\}}{(R^{\times})^2}$; hence, the product makes sense, in $\frac{K-\{0\}}{(R^{\times})^2}$.

Let us close this section with the calculation of the discriminant-form groups for the examples of (I, section 7.4), namely, the A_N, D_N, E_N and T_{pqr} forms. We take up the case of the A_N forms first. Label the vertices of the path graph $v_1, \ldots, v_N$ in order so that they form a basis for the $\mathbb{Z}$-module L. Denote the dual basis of $L^{\#}$ by $v_1^{\#}, \ldots, v_N^{\#}$. For $0 \leq m \leq N-1$, define $\alpha_m = \sum_{i=m+1}^{N}(i-m)v_i; \alpha_m \in L$ for every m. Note that if $m \geq 1$, we have

$$\langle \alpha_m, v_j \rangle = \begin{cases} 0 & \text{if } j < m \\ 1 & \text{if } j = m \\ 0 & \text{if } m < j < N \\ 0 & \text{if } j = N, \end{cases}$$

so that $v_m^{\#} = \alpha_m + (N+1-m)v_N^{\#}$ if $1 \leq m \leq N-1$. Therefore, $v_N^{\#}$ generates $G_L = L^{\#}/\mathrm{L}$. Furthermore, we have

$$\langle \alpha_0, v_j \rangle = \begin{cases} 0 & \text{if } j < N \\ -N-1 & \text{if } j = N, \end{cases}$$

so that $v_N^{\#} = \frac{-1}{N+1}\alpha_0$. Since

$$\begin{aligned} Q_{\#}(v_N^{\#}) &= Q_{\#}\left(\frac{-1}{N+1}\alpha_0\right) \\ &= \frac{1}{2(N+1)^2}\langle \alpha_0, \alpha_0 \rangle \\ &= \frac{1}{2(N+1)^2}\left[-2\sum_{i=1}^{N}(i^2) + 2\sum_{i=1}^{N-1} i(i+1)\right] \\ &= \frac{1}{2(N+1)^2}[-2N^2 + N(N-1)] \\ &= \frac{1}{2(N+1)^2}[-N^2 - N] \\ &= \frac{-N}{2(N+1)}, \end{aligned}$$

we have

$$q_L(v_1^{\#} + L) = \frac{-N}{2(N+1)} \mod \mathbb{Z}.$$

Therefore, the discriminant-form group for A_N is isomorphic to z_{N+1}^{-N}.

The same techniques can be used to discover the discriminant-form groups for the T_{pqr} forms. Label the vertices of the T_{pqr} graph by $a_1, \ldots, a_{p-1}, b_1, \ldots, b_{q-1}, c_1, \ldots, c_{r-1}$, and e as in (I, section 7.4). Define

$$\alpha_m = \sum_{i=m+1}^{p-1} (i-m)a_i \text{ for } 0 \le m \le p-2$$

$$\beta_m = \sum_{i=m+1}^{q-1} (i-m)b_i \text{ for } 0 \le m \le q-2, \text{ and}$$

$$\gamma_m = \sum_{i=m+1}^{r-1} (i-m)c_i \text{ for } 0 \le m \le r-2.$$

As above,

$$a_m^\# = \alpha_m + (p-m)a_{p-1}^\# \text{ for } 1 \le m \le p-2,$$

$$b_m^\# = \beta_m + (q-m)b_{q-1}^\# \text{ for } 1 \le m \le q-2, \text{ and}$$

$$c_m^\# = \gamma_m + (r-m)c_{r-1}^\# \text{ for } 1 \le m \le r-2,$$

so that $\{a_{p-1}^\#, b_{q-1}^\#, c_{r-1}^\#, e^\#\}$ generates $G_L = L^\#/L$.

Next, note that $\langle \alpha_0, \alpha_{p-1} \rangle = -p$, $\langle \alpha_0, e \rangle = p-1$ and

$$\langle \alpha_0, \text{any other basis vector of } L \rangle = 0,$$

so that

$$\begin{aligned} \alpha_0 &= (p-1)e^\# - pa_{p-1}^\#; \text{ similarly,} \\ \beta_0 &= (q-1)e^\# - qb_{q-1}^\#, \text{ and} \\ \gamma_0 &= (r-1)e^\# - rc_{r-1}^\#. \end{aligned} \tag{7.10}$$

Also, $\langle e, e \rangle = -2$, $\langle e, a_{p-1} \rangle = \langle e, b_{q-1} \rangle = \langle e, c_{r-1} \rangle = 1$ and

$$\langle e, \text{other basis vector of } L \rangle = 0$$

so that

$$e = -2e^\# + a_{p-1}^\# + b_{p-1}^\# + c_{r-1}^\#. \tag{7.11}$$

Therefore, in $L^\#/L$, we have the four relations

$$
\begin{aligned}
(p-1)e^{\#} - pa^{\#}_{p-1} &= 0 \\
(q-1)e^{\#} - qb^{\#}_{q-1} &= 0 \\
(r-1)e^{\#} - rc^{\#}_{r-1} &= 0 \\
-2e^{\#} + a^{\#}_{p-1} + b^{\#}_{q-1} + c^{\#}_{r-1} &= 0.
\end{aligned} \tag{7.12}
$$

Since the determinant

$$
\begin{vmatrix}
(p-1) & -p & 0 & 0 \\
(q-1) & 0 & -q & 0 \\
(r-1) & 0 & 0 & -r \\
-2 & 1 & 1 & 1
\end{vmatrix} = pqr - pq - pr - qr,
$$

which is the order of $L^{\#}/L$ for T_{pqr}, there are no other independent relations among the generators $e^{\#}, a^{\#}_{p-1}, b^{\#}_{q-1}$ and $c^{\#}_{r-1}$ of $G_{T_{pqr}}$; hence we have given generators and relations for $G_{T_{pqr}}$.

The most straightforward way to compute the form on $G_{T_{pqr}}$ is to first write the given generators in terms of e, α_0, β_0 and γ_0 by using (7.11) and (7.12), i.e., by inverting the above 4×4 matrix. We get

$$
\begin{aligned}
e^{\#} &= \frac{1}{D}\left[pqre + qr\alpha_0 + pr\beta_0 + pq\gamma_0\right] \\
a^{\#}_{p-1} &= \frac{1}{D}\left[(pqr - qr)e + (q+r)\alpha_0 + (pr - r)\beta_0 + (pq - q)\gamma_0\right] \\
b^{\#}_{q-1} &= \frac{1}{D}\left[(pqr - pr)e + (qr - r)\alpha_0 + (p+r)\beta_0 + (pq - p)\gamma_0\right] \\
c^{\#}_{r-1} &= \frac{1}{D}\left[(pqr - pq)e + (qr - q)\alpha_0 + (pr - p)\beta_0 + (p+q)\gamma_0\right]
\end{aligned} \tag{7.13}
$$

where $D = |G_{T_{pqr}}| =$ pqr $-pq - pr$ - qr.

The values of the bilinear form for e, α_0, β_0 and γ_0 are given below.

(7.14)

$\langle -, - \rangle$	e	α_0	β_0	γ_0
e	-2	$p-1$	$q-1$	$r-1$
α_0	$p-1$	$-p(p-1)$	0	0
β_0	$q-1$	0	$-q(q-1)$	0
γ_0	$r-1$	0	0	$-r(r-1)$

In principle, (7.13) and (7.14) suffice to calculate the quadratic form q on $G_{T_{pqr}}$. We will be satisfied at this time with calculating q for the D_N and E_N forms.

For $D_N, p = q = 2, r = N - 2$, and $D = 4$. Assume first that N is even, say $N = 2\mathrm{M}$. From (7.13) we have

$$e^{\#} = 0$$
$$a_1^{\#} = \frac{M}{2}\alpha_0 - \frac{M-1}{2}\beta_0 - \frac{1}{2}\gamma_0$$
$$b_1^{\#} = \frac{-M-1}{2}\alpha_0 + \frac{M}{2}\beta_0 - \frac{1}{2}\gamma_0$$
$$c_{r-1}^{\#} = -\frac{1}{2}\alpha_0 - \frac{1}{2}\beta_0$$

in G_{D_N}. Hence $G_{D_N} \cong \mathbb{Z}/2 \times \mathbb{Z}/2$, with nonzero elements $a_1^{\#}, b_1^{\#}$ and $c_{r-1}^{\#}$. Using (7.14), one finds that

$$q(a_1^{\#}) = q(b_1^{\#}) = -\frac{M}{4} \mod \mathbb{Z}$$

and

$$q(c_{r-1}^{\#}) = -\frac{1}{2} \mod \mathbb{Z}.$$

If $N \equiv 2 \mod 8$, then $\langle a_1^{\#}, b_1^{\#} \rangle_G = 0$ and G_{D_N} splits as $w_{2,1}^{-1} \oplus w_{2,1}^{-1}$. If $N \equiv 4 \mod 8$, then G_{D_N} is indecomposable; $G_{D_N} \cong v_1$. If $N \equiv 6 \mod 8$, then $\langle a_1^{\#}, b_1^{\#} \rangle_G = 0$ and G_{D_N} splits as $w_{2,1}^{1} \oplus w_{2,1}^{1}$. If $N \equiv 0 \mod 8, G$ is again indecomposable; $G_{D_N} \cong u_1$.

Now assume that N is odd, say $N = 2M + 1$. Then, using (7.13), we have

$$a_1^{\#} = \frac{1}{4}\left[2re + (r+2)\alpha_0 + r\beta_0 + 2\gamma_0\right]$$
$$= \frac{1}{4}\left[2(2M-1)e + (2M+1)\alpha_0 + (2M-1)\beta_0 + 2\gamma_0\right]$$
$$= \frac{1}{4}\left[-2e + (2M+1)\alpha_0 + (2M-1)\beta_0 + 2\gamma_0\right] \text{ in } G_{D_N},$$

and hence $a_1^{\#}$ has order 4 in G_{D_N}, so G_{D_N} is cyclic, generated by $a_1^{\#}$. Again using (7.14), we find that $q(a_1^{\#}) = \frac{-N}{8}$. Hence

$$G_{D_N} \cong w_{2,2}^{\varepsilon},$$

where $\varepsilon = -N \mod 8$.

For $E_N, p = 2, q = 3$ and $r = N-3$. We really only need to compute G_{E_N} for $N = 6$ and 7, since E_8 is unimodular, E_9 is degenerate, and $E_N \cong E_8 \oplus U \oplus A_{N-10}$ for $N \geq 10$. For $N = 6, D = 3$, so $G_{E_6} \cong \mathbb{Z}/3$. From (7.13), $b_{q-1}^{\#} = \frac{1}{3}\left[12e + 6\alpha_0 + 5\beta_0 + 4\gamma_0\right] = \frac{1}{3}\left[2\beta_0 + \gamma_0\right]$ in G_{E_6}, so $b_{q-1}^{\#} \neq 0$ and generates G_{E_6}. From (7.15??), we have $q(b_{q-1}^{\#}) = \frac{1}{3} \mod \mathbb{Z}$, so that $G_{E_6} \cong w_{3,1}^{-1}$.

quadratic $\mathbb{Z}$-module L	G	q_L	$\lvert G_L\rvert$
A_N, $N \geq 1$	$\mathbb{Z}/N+1$	z_{N+1}^{-N}	$N+1$
$D_N, N \equiv 0 \mod 8$	$(\mathbb{Z}/2)^2$	u_1	4
$D_N, N \equiv 1 \mod 8$	$\mathbb{Z}/4$	$w_{2,2}^7$	4
$D_N, N \equiv 2 \mod 8$	$(\mathbb{Z}/2)^2$	$w_{2,1}^{-1} \oplus w_{2,1}^{-1}$	4
$D_N, N \equiv 3 \mod 8$	$\mathbb{Z}/4$	$w_{2,2}^5$	4
$D_N, N \equiv 4 \mod 8$	$(\mathbb{Z}/2)^2$	v_1	4
$D_N, N \equiv 5 \mod 8$	$\mathbb{Z}/4$	$w_{2,2}^3$	4
$D_N, N \equiv 6 \mod 8$	$(\mathbb{Z}/2)^2$	$w_{2,1}^1 \oplus w_{2,1}^1$	4
$D_N, N \equiv 7 \mod 8$	$\mathbb{Z}/4$	$w_{2,1}^1$	4
E_6	$\mathbb{Z}/3$	$w_{3,1}^{-1}$	3
E_7	$\mathbb{Z}/2$	$w_{2,1}^1$	2
E_8, E_{10}	$\{1\}$	—	1
$E_N, N \geq 11$	$\mathbb{Z}/N-9$	z_{N-9}^{10-N}	$N-9$
$T_{p,q,r}$	—	—	$pqr-pq-pr-qr$

TABLE 7.2. discriminant-forms of A_N, D_N, E_N, and $T_{p,q,r}$

For $N=6, D=2$, so $G_{E_7} \cong \mathbb{Z}/2$. From (7.13), $a_{p-1}^{\#} = \frac{1}{2}[12e + 7\alpha_0 + 4\beta_0 + 3\gamma_0]$ $= \frac{1}{2}[\alpha_0 + \gamma_0]$ in G_{E_7}, so $a_{p-1}^{\#}$ generates G_{E_7}. From (7.14), we have $q(a_{p-1}^{\#}) = \frac{1}{4} \mod \mathbb{Z}$, so that $G_{E_7} \cong w_{2,1}^1$.

For completeness, we have for $N \geq 11$, $G_{E_N} \cong G_{A_{N-10}} \cong z_{N-9}^{10-N}$.

We collect what we have computed in Table 7.2.

8. The Functoriality of G_L

Again let R be an integral domain with characteristic $\neq 2$. Let L and M be two quadratic R-modules and $\Phi : L \to M$ a homomorphism of quadratic R-modules. By $(I, (6.4)), \Phi$ is an embedding; hence Φ induces an injection of vector spaces $\Phi_K : L_K \to M_K$.

How does Φ_K behave with respect to the dual lattices $L^{\#}$ and $M^{\#}$? In particular, does $\Phi_K(L^{\#}) \subseteq M^{\#}$? The answer is unfortunately no in general. For example, assume $R = \mathbb{Z}$ and $M = \mathbb{Z}^2$, with the quadratic structure of the hyperbolic plane. With the standard basis $\{e_1, e_2\}$ for M, we have $\langle e_1, e_1\rangle = \langle e_2, e_2\rangle = 0$ and $\langle e_1, e_2\rangle = 1$. Let $L \cong \mathbb{Z}$ be the submodule generated by $f = e_1 + e_2$. Note that $\langle f, f\rangle = 2$, so L is nondegenerate; in fact, $Q_L(l) = 0 \Leftrightarrow l = 0$ in L. The dual lattice $L^{\#}$ to L is generated by $f^{\#} = f/2$; however since M is unimodular, $M^{\#} = M$ and so $L^{\#}$ does not map to $M^{\#}$, since $f/2$ is not in M.

However, if the image $\Phi(L)$ of L in M *splits off* M, then it is clear that $\Phi_K(L^{\#}) \subseteq M^{\#}$. Indeed, if we write $M = \Phi(L) \oplus \Phi(L)^{\perp}$, then

$M^\#$ is $\Phi(L)^\# \oplus (\Phi(L)^\perp)^\#$. In this case we then obtain a module map $\varphi : G_L \to G_M$ induced by $\Phi|_{L^\#}$. It is not hard to see that in fact the splitting condition is necessary for $\Phi_K(L^\#)$ to lie inside $M^\#$.

The reader can easily check that in this case φ is a homomorphism of the quadratic structures on G_L and on G_M, and is in fact an injection of a direct summand (as is Φ, after all).

Therefore, if Φ is in fact a *stable homomorphism*, i.e., $\Phi(L)$ splits off M and $\Phi(L)^\perp$ is unimodular, then φ will be an isometry from G_L to G_M. The following is now immediate.

PROPOSITION 8.1. *The discriminant-form construction*

$$L \rightsquigarrow G_L$$

is a covariant functor from the category of quadratic R-modules (with stable homomorphisms) to the category of torsion quadratic forms over R (with isometries).

As the first application, we therefore have a map on orthogonal groups:

COROLLARY 8.2. *Let L be a quadratic R-module. Then there is a natural group homomorphism from $\mathcal{O}(L)$ to $\mathcal{O}(G_L)$.*

If $\sigma \in \mathcal{O}(L)$ is an isometry of L, the induced isometry of G_L will be denoted by $\overline{\sigma}$. Since the map on G_L is the reduction $\mod L$ of the induced map from $L^\#$ to $L^\#$, we have

$$\overline{\sigma}(x \mod L) = \sigma(x) \mod L \text{ for } x \text{ in } L^\#. \tag{8.3}$$

NOTATION 8.4. *If L is a quadratic R-module, the kernel of $\mathcal{O}(L) \to \mathcal{O}(G_L)$ will be denoted by $\mathcal{O}^\#(L)$.*

In terms of matrices, if the matrix of Q_L is A and the matrix of $\sigma \in \mathcal{O}(L)$ is S with respect to some basis of L, then the matrix of σ on $L^\#$ with respect to the dual basis is ASA^{-1}. Hence

$$\begin{aligned}
\sigma \in \mathcal{O}^\#(L) &\Leftrightarrow \overline{\sigma}(x \mod L) = x \mod L \text{ for all } x \text{ in } L^\# \\
&\Leftrightarrow \forall x \in L^\#, \sigma(x) - x \in L \\
&\Leftrightarrow \text{Image of } (ASA^{-1} - I) \subseteq \text{ image of } A \text{ on } R^N, \\
&\qquad \text{where } N = \operatorname{rank} L \\
&\Leftrightarrow \exists C \in \mathcal{M}_{N\times N}(R) \text{ such that } ASA^{-1} = I + AC \\
&\Leftrightarrow \exists C \in \mathcal{M}_{M\times N}(R) \text{ such that } S = I + CA
\end{aligned}$$

Therefore, $\mathcal{O}^\#(L) = \{S \in \mathcal{O}(L) \mid S = I + CA \text{ for some } C\}$, which corresponds to the set $\{C \mid I + CA \in \mathcal{O}(L)\}$.

Now $I + CA \in \mathcal{O}(L) \Leftrightarrow (I + CA)^\top A(I + CA) = A \Leftrightarrow C + C^\top + C^\top AC = 0$; therefore, we have an onto function from $\{C \,|\, C + C^\top + C^\top AC = 0\}$ to $\mathcal{O}^\#(L)$, sending C to I + AC.

The reader can easily check the following.

PROPOSITION 8.5. *Let (L, Q) be a quadratic R-module of rank N with matrix A. Let $H_A = \{C \in \mathcal{M}_{N\times N}(R) \,|\, C + C^\top + C^\top AC = 0\}$. Define an operation $*$ on H_A by setting $C_1 * C_2 = C_1 + C_2 + C_1AC_2$. Then:*

(8.5.1) $(H_A, *)$ is a group.
(8.5.2) The inverse of $C \in H_A$ is $C^\top$.
(8.5.3) The map $H_A \to \mathcal{O}^\#(L)$ defined by sending C to $I + CA$ is an isomorphism of groups.

For example, suppose L has rank 1 so that $A = (2a)$ for some $a \in R$. Then

$$\begin{aligned} H_A &= \{(c) \,|\, (c) + (c)^\top + (c)^\top (2a)(c) = 0\} \\ &= \{(c) \,|\, 2c + 2ac^2 = 0\} \\ &= \{(c) \,|\, c + ac^2 = 0\} \\ &= \{(c) \,|\, c(1 + ac) = 0\}. \end{aligned}$$

Therefore, $H_A = \{(0)\}$ if $a \notin R^\times$, and $H_A = \{(0), (-a^{-1})\}$ if $a \in R^\times$. Hence,

$$\mathcal{O}^\#(L) = \begin{cases} \{I\} & \text{if } a \notin R^\times \\ \{\pm I\} & \text{if } a \in R^\times. \end{cases}$$

It is useful to remark at this point that Lemmas (I.9.4) and (I.9.5) show that the map $\mathcal{O}(L) \to \mathcal{O}(G_L)$ is surjective for all the standard forms $W^\varepsilon_{p,k}$, U_k, and V_k.

We will close this section with a discussion of the discriminant and its behavior vis-a-vis the discriminant-form construction. The result is as follows.

PROPOSITION 8.6. *Assume R is a P.I.D. Let (L, Q) be a quadratic R-module and let (G_L, q_L) be the discriminant-form for L. Assume that the rank of L equals the length of G_L. Let d_1 be the first invariant of G_L and let $\alpha = \gcd(2, d_1)$. Then*

$$\overline{\operatorname{disc}(L)} \cdot \operatorname{disc}(G_L) = 1 \text{ in } \mathcal{D}\left(\frac{R}{\alpha d_1}\right)$$

PROOF. Before proceeding, let us remark on the meaning of this identity. The discriminant $\operatorname{disc}(L)$ lies in $(R^\times)^2\backslash(R - \{0\})$, and if $\{d_1, \ldots, d_N\}$ are the invariants of G_L and $\Delta = \prod d_i$, then in fact

$\text{disc}(L) \in (R^\times)^2/\Delta \cdot R^\times$. By $\overline{\text{disc}(L)}$ we denote its residue in $(R^\times)^2 \backslash \Delta \cdot \left(\frac{R}{\alpha d_1}\right)^\times = \Delta \mathcal{D}\left(\frac{R}{\alpha d_1}\right)$. Recall that $\text{disc}(G_L) \in \frac{1}{\Delta}\mathcal{D}\left(\frac{R}{\alpha d_1}\right)$ since q_L is nondegenerate. In the product $\overline{\text{disc}(L)} \cdot \text{disc}(G_L)$ the Δ's cancel and we get a class in $\mathcal{D}\left(\frac{R}{\alpha d_1}\right)$; we are claiming this class is 1.

Let $\{g_1, \ldots, g_N\}$ be an ordered basis for G_L; lift these generators to a basis $\{f_i\}$ for $L^\#$. Let $\{e_i\}$ be the dual basis for L and let A be the matrix of Q_L with respect to the basis $\{e_i\}$. Then $B = A^{-1}$ is the matrix of $Q_{L^\#}$ with respect to $\{f_i\}$, by (7.9). B is a matrix over K and from the definition of q, B is a representing matrix for q. Since $\text{disc}(L)$ is the class of $\det(A)$ and $\text{disc}(G_L)$ is the class of $\det(B)$, the result follows. Q.E.D.

In the case of a quadratic $\mathbb{Z}_p$-module, we can factor out the powers of p occurring in both discriminants to obtain the following.

COROLLARY 8.7. *Fix a prime p, and let L be a quadratic $\mathbb{Z}_p$-module, and let (G_L, q_L) be its discriminant-form. Assume that the rank of L equals the length of G_L. Then $\chi(\text{disc}(L)) = \chi(\text{disc}(q_L))$. (If $p = 2$ then this holds* $\bmod 8$ *if the first invariant of G is at least 4, and it holds* $\bmod 4$ *if the first invariant of G is 2.) Moreover if $p = 2$ and G is good and special, then $\chi(\text{disc}(L)) = \chi(\text{disc}_8(q_L))$.*

PROOF. This follows immediately from the above, noting that χ has values in a group all of whose elements have order two. The better and extra special case also follows by the same proof, simply noting that the relevant quantities are defined $\bmod 8$. Q.E.D.

.

9. The Discriminant-Form and Stable Isomorphism

In this section let R be a P.I.D. of characteristic $\neq 2$.

Recall that if M is a unimodular quadratic R-module, then its discriminant-form module G_M is trivial. Therefore, if L is any other quadratic R-module, then $G_{L \oplus M} \cong G_L \oplus G_M \cong G_L$, so that L and $L \oplus M$ have isomorphic discriminant-forms. This immediately implies the following.

LEMMA 9.1. *If L_1 and L_2 are quadratic R-modules, which are stably isomorphic, then $G_{L_1} \cong G_{L_2}$.*

Recall that we denote stable isomorphism by $L_1 \sim_S L_2$. It is our intention in this section to demonstrate that in fact the converse of (9.1) is true. We require one technical lemma.

LEMMA 9.2. *Let $\widetilde{L}$ and $\widetilde{M}$ be two K-valued quadratic forms over R and let $f : \widetilde{L} \to \widetilde{M}$ be an R-module homomorphism such that $Q_{\widetilde{M}}(f(x)) \equiv Q_{\widetilde{L}}(x) \mod R$ for every x in L. Then there exists a unimodular quadratic R-module N and an R-map $g : \widetilde{L} \to N$ such that $f \oplus g : \widetilde{L} \to \widetilde{M} \oplus N$ is a homomorphism of quadratic forms.*

PROOF. As is standard, let U denote the rank-2 quadratic R-module with matrix $\begin{pmatrix} 01 \\ 10 \end{pmatrix}$, i.e., the hyperbolic plane over R. Let $\{\widetilde{e}_1, \ldots, \widetilde{e}_N\}$ be a basis for $\widetilde{L}$ and let

$$r_{ij} = \langle \widetilde{e}_i, \widetilde{e}_j \rangle_{\widetilde{L}} - \langle f(\widetilde{e}_i), f(\widetilde{e}_j) \rangle_{\widetilde{M}}.$$

By hypothesis, $r_{ij} \in R$. The proof proceeds by induction on the number of nonzero r_{ij}'s. If this number is zero, then f is a homomorphism of the bilinear form structure and since R has characteristic 2, f is also a homomorphism of the quadratic structure.

It then suffices to show that, if the number of nonzero r_{ij}'s is at least one, then there exists a map $g : \widetilde{L} \to U$ such that the R-map $f \oplus g : \widetilde{L} \to \widetilde{M} \oplus U$ "corrects" exactly one r_{ij}. There are two cases to consider.

Case 1: Correct r_{kk}.

Since the bilinear forms come from quadratic forms, the diagonal elements are divisible by 2, so $r_{kk} = 2a_k$. Define

$$g : \widetilde{L} \to U \text{ by } g(\widetilde{e}_n) = \begin{cases} (a_k, 1) & \text{if } n = k \\ (0,0) & \text{if } n \neq k. \end{cases}$$

Then

$$\begin{aligned} &\langle \widetilde{e}_i, \widetilde{e}_j \rangle \widetilde{L} - \langle f(\widetilde{e}_i), f(\widetilde{e}_j) \rangle \widetilde{M} - \langle g(\widetilde{e}_i), g(\widetilde{e}_j) \rangle_U \\ &\quad = \begin{cases} r_{ij} & \text{if } i \neq k \text{ or } j \neq k \\ r_{kk} - 2a_k = 0 & \text{if } (i,j) = (k,k). \end{cases} \end{aligned}$$

Hence this corrects r_{kk}.

Case 2: Correct $r_{kl}, k \neq$ l.

In this case define $g : \widetilde{L} \to U$ by

$$g(\widetilde{e}_n) = \begin{cases} (r_{kl}, 0) & \text{if } n = k \\ (0,1) & \text{if } n = l \\ (0,0) & \text{if } n \neq k, l \end{cases}$$

Then

$$\begin{aligned} &\langle \widetilde{e}_i, \widetilde{e}_j \rangle \widetilde{L} - \langle f(\widetilde{e}_i), f(\widetilde{e}_j) \rangle \widetilde{M} - \langle g(\widetilde{e}_i), g(\widetilde{e}_j) \rangle_U \\ &\quad = \begin{cases} r_{ij} & \text{if } (i,j) \neq (k,l) \\ r_{kl} - r_{kl} \cdot 1 = 0 & \text{if } (i,j) = (k,l). \end{cases} \end{aligned}$$

Therefore, this corrects r_{kl}. Q.E.D.

Our result is this:

PROPOSITION 9.3. *Let L and M be quadratic R-modules. Then $L \sim_S M \Leftrightarrow G_L \cong G_M$ as torsion quadratic forms.*

PROOF. Lemma (9.1) is the direction $\Rightarrow$, so we will prove $\Leftarrow$. Let $\bar{f} : G_L \to G_M$ be an isomorphism of the torsion quadratic structures on G_L on G_M. Since L is a free R-module, so is $L^\#$, so $\bar{f}$ can be lifted to an R-map $f : L^\# \to M^\#$. This gives us the following commutative diagram:

$$\begin{array}{ccccccccc} 0 & \longrightarrow & L & \xrightarrow{\mathrm{Ad}_L} & L^\# & \longrightarrow & G_L & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle f|_L} & & \downarrow{\scriptstyle f} & & \cong\downarrow{\scriptstyle \bar{f}} & & \\ 0 & \longrightarrow & M & \xrightarrow{\mathrm{Ad}_M} & M^\# & \longrightarrow & G_M & \longrightarrow & 0 \end{array}$$

Since $\bar{f}$ is an isomorphism, we have $Q_{M^\#}(f(x)) = Q_{L^\#}(x) \mod R$ for every x in $L^\#$. By the previous lemma, there exists a unimodular quadratic R-module N and an R-map $g : L^\# \to N$ such that $h = f \oplus g : L^\# \to M^\# \oplus N$ is a quadratic form homomorphism, hence an embedding. Restricting h to L gives the isomorphism $h : L \to M \oplus$N.

We claim that $h(L) \oplus h(L)^\perp = M \oplus N$, i.e. that $h(L)$ splits off $M \oplus$ N. Certainly $h(L) \oplus h(L)^\perp \subseteq M \oplus$ N. To prove the reverse inclusion, let $y \in M \oplus$ N. Consider the linear map $\langle y, - \rangle_{M^\# \oplus N}$ on $M^\# \oplus N$, restricted to $h(L^\#)$. Since h is 1-1, this linear map is induced, via the adjoint map, from a unique element of $h(L^\#)^\# = h(L)$, say $h(l)$. Let $z = y - h(l)$, so that $y = h(l) +$ z. We need only show that $z \in h(L)^\perp$, i.e., for every l' in L, $\langle z, h(l') \rangle_{M \oplus N} = 0$. But

$$\begin{aligned} \langle z, h(l') \rangle_{M \oplus N} &= \langle y - h(l), h(l') \rangle_{M \oplus N} \\ &= \langle y, h(l') \rangle_{M \oplus N} - \langle h(l), h(l') \rangle_{M \oplus N} \\ &= \langle y, h(l') \rangle_{M \oplus N} - \langle l, l' \rangle_L \\ &= 0 \text{ by the choice of l.} \end{aligned}$$

This proves that $h(L) \oplus h(L)^\perp = M \oplus$ N. Hence

$$\mathrm{disc}(h(l)) \, \mathrm{disc}(h(L)^\perp = \mathrm{disc}(M) \, \mathrm{disc}(N) = \mathrm{disc}(M) \mod \frac{R^\times}{(R^\times)^2}$$

since N is unimodular. However, $\mathrm{disc}(h(L)) = \mathrm{disc}(L) = \mathrm{disc}(M)$ mod $\frac{R^\times}{(R^\times)^2}$, since $G_L \cong G_M$. Therefore, $\mathrm{disc}(h(L)^\perp$ is in $\frac{R^\times}{(R^\times)^2}$, so that $h(L)^\perp$ is unimodular. This proves that $L \sim_S M$. Q.E.D.

Note that we have actually proved a slightly stronger result:

PROPOSITION 9.4. *Let L and M be quadratic R-modules. Then any isomorphism $\bar{f} : G_L \to G_M$ can be lifted to a stable homomorphism from L to $M \oplus N$, for some unimodular quadratic R-module N.*

10. Discriminant-forms and overlattices

One of the primary uses for discriminant forms is the following construction. Let L be a quadratic R-module, and suppose that M is a submodule of $L^\# \subset L_K$ which contains L such that $Q_\#$ is R-valued on M. We then get a chain of inclusions

$$L \subset M \subset M^\# \subset L^\#$$

which induce inclusions

$$M/L \subset M^\#/L \subset L^\#/L = G_L.$$

Let $I = M/L$. Now since $Q_\#$ is R-valued on M, q_L vanishes identically on I. Moreover, the definition of $M^\#$ implies that $M^\#/L = I^\perp$ in G_L. Thus, to each overlattice M of L corresponds a totally isotropic subspace I of G_L, and $G_M = I^\perp/I$. The converse statement (that each totally isotropic I corresponds to an overlattice) is also easy to see.

As an example of this construction, consider the finite quadratic form $(G, q) = w^1_{2,k+1} \overset{\perp}{\oplus} w^3_{2,k+1}$, and let x and y be generators of the first and second factors, respectively. Now $q(2^k x + 2^k y) = 2^k \mod \mathbb{Z}$, so that $2^k x + 2^k y$ generates an isotropic subgroup H of order 2. To find $H^\perp$, we compute $\langle ax + by, 2^k x + 2^k y\rangle = (a + 3b)/2$; thus, $ax + by \in H^\perp$ if and only if $a + 3b$ is an even integer. Thus, $H^\perp$ is generated by $2x$ and $x + y$; in $H^\perp/H$, these each have order 2^k, and there are no other relations. Now $q(2x) = 2^{-k}$, $\langle 2x, x + y\rangle = 2^{-k-1}$, and $q(x + y) = 2^{-k}$, which shows that $H^\perp/H$ is isomorphic to v_k.

Thus, the quadratic $\mathbb{Z}_{\not 2}$-module

$$W^1_{2,k+1} \bigoplus W^3_{2,k+1}$$

has an overlattice whose discriminant-form is isomorphic to v_k. In fact, from Lemma (I.7.7.2) it can be seen that this overlattice is isomorphic to V_k.

11. Quadratic forms over a discrete valuation ring

Let R be a discrete valuation ring, and let F be an R-module. We say that F is *quasi-principal* if every finitely generated submodule of F can be generated by a single element. The primary examples of quasi-principal R-modules which will interest us are R itself, and K/R, where K is the fraction field of R.

We note two properties of a quasi-principal R-module.

LEMMA 11.1. *Let F be a quasi-principal R-module.*

(11.1.1) Any submodule H of a finitely generated submodule G of F is itself finitely generated.

(11.1.2) For any subset $\{x_i\}_{i\in I}$ which generates a finitely generated submodule of F, there is some $j \in I$ such that x_j generates the same submodule as $\{x_i\}_{i\in I}$.

PROOF. Let π be a uniformizing parameter for R.

(11.1.1) If G is a finitely generated submodule of F, then G can be generated by a single element g of G. Every other element of g can then be written in the form $\pi^e u \cdot g$ for some $e \geq 0$ and some unit u of R. If we define $\nu(H) = \min\{e|\pi^e u \cdot g \in H \text{ for some unit } u \text{ of } R\}$, then H is generated by $\pi^e \cdot g$.

(11.1.2) Let G be the submodule generated by $\{x_i\}_{i\in I}$ and let g be a generator of G as before. Then for each $i \in I$, we can write $x_i = \pi^{e_i} u_i \cdot g$ as before. There must be some j such that $e_j = 0$ (else $\{x_i\}_{i\in I}$ would not generate G). But then x_j generates G. Q.E.D.

Now suppose we are given a quadratic form $Q : L \to F$ over R, where R is a discrete valuation ring, L is a finitely generated R-module, and F is a quasi-principal R-module. Under these conditions, we define $\mathrm{Im}(\langle , \rangle)$ to be the submodule of F generated by $\{\langle x, y\rangle\}_{x,y\in L}$ (where $\langle -, -\rangle$ denotes the associated bilinear form of Q) and $\mathrm{Im}(Q)$ to be the submodule generated by $\{Q(x)\}_{x\in L}$. Notice that since $2Q(x) = \langle x, x\rangle$, we have $2 \cdot \mathrm{Im}(Q) \subset \mathrm{Im}(\langle , \rangle)$.

LEMMA 11.2.

(11.2.1) Suppose that $2 \cdot \mathrm{Im}(Q) = \mathrm{Im}(\langle , \rangle)$, and that $Q(x)$ generates $\mathrm{Im}(Q)$. Then the submodule of L generated by x splits as an orthogonal direct summand of L.

(11.2.2) Suppose that $2 \cdot \mathrm{Im}(Q) \neq \mathrm{Im}(\langle , \rangle)$, and that $\langle x, y\rangle$ generates $\mathrm{Im}(\langle , \rangle)$. Then the submodule of L generated by x and y splits as an orthogonal direct summand of L.

PROOF. (11.2.1) $\langle x, x\rangle = 2Q(x)$ must generate $\mathrm{Im}(\langle , \rangle)$. Thus, for any $z \in L$, we may write $\langle z, x\rangle = \alpha_z \langle x, x\rangle$ for some $\alpha_z \in L$. But then

$z = (z - \alpha_z x) + \alpha_z x$ and $z - \alpha_z x$ lies in $x^\perp$. It follows that the submodule of L generated by x splits as an orthogonal direct summand of L.

(11.2.2) Let π be a uniformizing parameter for R. Since $2 \cdot \mathrm{Im}(Q) \neq \mathrm{Im}(\langle , \rangle)$, there exist ξ and $\eta \in R$ such that $2Q(x) = \langle x, x\rangle = \pi\xi\langle x, y\rangle$, and $2Q(y) = \langle y, y\rangle = \pi\eta\langle x, y\rangle$. ($\pi$ divides each coefficient since $2 \cdot \mathrm{Im}(Q)$

is a proper submodule of $\mathrm{Im}(\langle,\rangle)$.) Then $u = 1 - \pi^2\xi\eta$ is a unit in R. Now for any $z \in L$, there exist $\alpha_z, \beta_z \in R$ such that $\langle z, x\rangle = \alpha_z\langle x, y\rangle$ and $\langle z, y\rangle = \beta_z\langle x, y\rangle$. We can write

$z = [z + u^{-1}(\pi\eta\alpha_z - \beta_z)x + u^{-1}(\pi\xi\beta_z - \alpha_z)y]+$

$u^{-1}(\beta_z - \pi\eta\alpha_z)x + u^{-1}(\alpha_z - \pi\xi\beta_z)y$. An easy computation shows that

$z + u^{-1}(\pi\eta\alpha_z - \beta_z)x + u^{-1}(\pi\xi\beta_z - \alpha_z)y$ is orthogonal to both x and y. Thus, the submodule of L generated by x and y splits as an orthogonal direct summand of L. Q.E.D.

LEMMA 11.3. *Suppose that R is a discrete valuation ring, that F is a quasi-principal R-module, that $Q : L \to F$ is a quadratic form, and that L is generated by x and y but cannot be generated by a single element. Then L is indecomposable if and only if $2 \cdot \mathrm{Im}(Q) \neq \mathrm{Im}(\langle,\rangle)$. Moreover, in this case $\mathrm{Im}(\langle,\rangle)$ is generated by $\langle x, y\rangle$.*

PROOF. If $2 \cdot \mathrm{Im}(Q) = \mathrm{Im}(\langle,\rangle)$, then there is some z in L such that $Q(z)$ generates $\mathrm{Im}(Q)$. By lemma (11.2)(i), the submodule of L generated by z (which is a proper submodule by assumption) splits as an orthogonal direct summand, so that L is decomposable.

Conversely, suppose that L is decomposable. Since the minimum number of generators of a finitely generated R-module is an invariant of the module which is additive under direct sum, we must have $L = L_1 \oplus L_2$, where L_1 and L_2 are cyclic. But then if z and w are the corresponding generator, $\mathrm{Im}(\langle,\rangle)$ is generated by $2Q(z)$, $2Q(w)$, and $\langle z, w\rangle = 0$. Thus, $\mathrm{Im}(\langle,\rangle)$ is generated by $2Q(z)$ and $2Q(w)$ alone, and so coincides with $2 \cdot \mathrm{Im}(Q)$.

To see the last statement, note that if $2 \cdot \mathrm{Im}(Q) \neq \mathrm{Im}(\langle,\rangle)$, then $\mathrm{Im}(\langle,\rangle)$ is generated by $2Q(x)$, $2Q(y)$, and $\langle x, y\rangle$. Now one of these three quantities must generate the module $\mathrm{Im}(\langle,\rangle)$. It cannot be either of the first two (by our assumption); thus, $\langle x, y\rangle$ generates $\mathrm{Im}(\langle,\rangle)$, as claimed. Q.E.D.

As a consequence of lemmas (11.2) and (11.3) we get

PROPOSITION 11.4. *Let R be a discrete valuation ring, let L be a finitely generated R-module, let F be a quasi-principal R-module, and let $Q : L \to F$ be a quadratic form. Then there is an orthogonal direct sum decomposition into indecomposable pieces $L \cong L_1 \oplus \cdots \oplus L_k$ such that $\mathrm{rank}(L_i) = 1$ or 2 for each i. Moreover, if 2 is a unit in R, then $\mathrm{rank}(L_i) = 1$ for each i.*

PROOF. Let $\{x_i\}$ is a finite generating set for L. Then $\{\langle x_i, x_j\rangle\}$ is a finite generating set for $\mathrm{Im}(\langle,\rangle)$. Moreover, since

$Q(\sum a_i x_i) = \sum a_i^2 Q(x_i) + \sum a_i a_j \langle x_i, x_j \rangle$, we see that $\mathrm{Im}(Q)$ is contained in the submodule generated by $\{Q(x_i)\}$ and $\{\langle x_i, x_j \rangle\}$, so that it is finitely generated as well.

If $2 \cdot \mathrm{Im}(Q) = \mathrm{Im}(\langle , \rangle)$ (which must be the case when 2 is a unit in R), there exists some x such that $Q(x)$ generates $\mathrm{Im}(Q)$. By lemma (11.2), the submodule of L generated by x splits as an orthogonal direct summand of L. If on the other hand $2 \cdot \mathrm{Im}(Q) \neq \mathrm{Im}(\langle , \rangle)$, there exist x and y such that $\langle x, y \rangle$ generates $\mathrm{Im}(\langle , \rangle)$. Again using lemma (11.2), the submodule of L generated by x and y splits as an orthogonal direct summand of L. By lemma (11.3), this summand is indecomposable. An easy induction on the rank of L now finishes the argument. Q.E.D.

Since R and K/R are both quasi-principal R-modules, we get an immediate corollary.

COROLLARY 11.5. *Let R be a discrete valuation ring.*

(11.5.1) If $Q : L \to R$ is a nondegenerate quadratic R-module, then there is an orthogonal direct sum decomposition into indecomposable pieces $L \cong L_1 \oplus \cdots \oplus L_k$ such that $\mathrm{rank}(L_i) = 1$ or 2 for each i. Moreover, if 2 is a unit in R, then $\mathrm{rank}(L_i) = 1$ for each i.

(11.5.2) If $q : G \to K/R$ is a nondegenerate finitely generated torsion quadratic form over R, there is an orthogonal direct sum decomposition into indecomposable pieces $G \cong G_1 \oplus \cdots \oplus G_k$ such that $\ell(G_i) = 1$ or 2 for each i. Moreover, if 2 is a unit in R, then $\ell(G_i) = 1$ for each i.

Notice that in the case of torsion quadratic forms, each G_i is homogeneous (since there is always a decomposition into homogeneous pieces).

We can give a further refinement of these decompositions which makes them compatible with the discriminant-form construction.

PROPOSITION 11.6. *Let R be a discrete valuation ring, let $Q : L \to R$ be a nondegenerate quadratic R-module, and let $q_L : G_L \to K/R$ be the discriminant-form of L. Suppose we are given an orthogonal direct sum decomposition*

$G_L \cong G_1 \oplus \cdots \oplus G_k$ where each G_i is indecomposable (so that in particular, $\ell(G_i) \leq 2$ and if 2 is a unit in R then $\ell(G_i) = 1$). Then there exists an orthogonal direct sum decomposition into indecomposable pieces

$L \cong L_1 \oplus \cdots \oplus L_k \oplus M_1 \oplus \cdots \oplus M_\ell$ such that $\mathrm{rank}(L_i) = \ell(G_i)$, the natural map induces an isomorphism $G_{L_i} \cong G_i$, and each M_j is unimodular of rank at most 2 (rank 1 if 2 is a unit).

PROOF. By induction on the rank, it suffices to show that we may split off one L_i or M_j of the appropriate type.

Suppose first that there exist $x, y \in L$ such that $\langle x, y\rangle$ is a unit in R. By lemma (11.2), either $2 \cdot \mathrm{Im}(Q) \neq \mathrm{Im}(\langle , \rangle)$ and x and y generate a submodule of L which splits as an orthogonal direct summand, or $2 \cdot \mathrm{Im}(Q) = \mathrm{Im}(\langle , \rangle)$. In the first case, we may take M_1 to be the submodule generated by x and y, since this is clearly unimodular. In the second case, 2 must be a unit in R, and there exists some z with $Q(z)$ a unit; we may take M_1 to be the submodule generated by z in this case.

Thus, we may assume that $\mathrm{Im}(\langle , \rangle) \neq R$. Let π be a uniformizing parameter for R, and let π^m generate $\mathrm{Im}(\langle , \rangle)$ with $m \geq 1$. We claim that the first invariant of G_L is π^m. For suppose that ξ is part of an ordered basis of G_L and has annihilator (π^n) with $n \leq m-1$. Let $\pi^{-n}x$ be a representative of ξ in $L^{\#}$. Then for all $z \in L$, $\langle x, z\rangle = \pi^m \alpha$ with $\alpha \in R$, so that $\langle \pi^{-n-1}x, z\rangle = \pi^{m-n-1}\alpha \in R$; this implies that $\pi^{-n-1}x \in L^{\#}$. But then if η is the image of $\pi^{-n-1}x$ in G_L, we have $\xi = \pi\eta$, a contradiction. Thus, π^m divides the first invariant of G_L. On the other hand, if we choose $x, y \in L$ such that $\langle x, y\rangle = \pi^m$, then the image of $\pi^{-m}x$ in G_L has annihilator (π^m), and cannot be divided by π in G_L. (For if it could, then for some $z \in L$ we would have $\pi^{-m-1}x + \pi^{-1}z \in L^{\#}$. But then $\langle \pi^{-m-1}x + \pi^{-1}z, y\rangle = \pi^{-1}(1 + \langle z, y\rangle) \in R$. Since π^m divides $\langle z, y\rangle$, this is impossible). Thus, $\pi^{-m}x$ may be taken as the first element of an ordered basis of G_L.

Thus, there exists some G_i whose first invariant is π^m. (The second invariant, if it has one, is also π^m, since G_i is homogenous.) Let ξ (resp. ξ, η) be an ordered basis for G_i, and let $\pi^{-m}x$ (resp. $\pi^{-m}x$ and $\pi^{-m}y$) be a lift of the basis to $L^{\#}$. In the rank one case, nondegeneracy implies that $q(\xi) = (1/2)\pi^{-m} \cdot u$ for some unit u. Thus, $Q(x) \equiv \pi^{2m}q(\xi) \equiv (1/2)\pi^m \cdot u \mod \pi^{2m}$. In the rank two case, since $2 \cdot \mathrm{Im}(Q) \neq \mathrm{Im}(\langle , \rangle)$, nondegeneracy implies that $\langle \xi, \eta\rangle = \pi^{-m} \cdot u$ for some unit u and that $\pi^m q(\xi)$ and $\pi^m q(\eta)$ are both divisible by π. Thus, $\langle x, y\rangle \equiv \pi^{2m}\langle \xi, \eta\rangle \equiv \pi^m \cdot u \mod \pi^{2m}$, while $Q(x)$ and $Q(y)$ are both divisible by π^{m+1}. So in either case, we may take L_i to be the submodule generated by x (resp. x and y); this is an orthogonal direct summand by lemma (11.2).

Q.E.D.

CHAPTER III

Gauss Sums and the Signature

1. Gauss sum invariants for finite quadratic forms

Let (G, q) be a finite quadratic form. The *Gauss sum invariant* (or *Gauss invariant*) of the form is the map

$$\gamma_G : \mathrm{Hom}_{\mathbb{Z}}(\mathbb{Q}/\mathbb{Z}, \mathbb{Q}/\mathbb{Z}) \to \mathbb{C}$$

defined by

$$\gamma_G(\varphi) = |G|^{-1/2} \sum_{x \in G} \exp(2\pi i \varphi(q(x))).$$

(We occasionally denote this by $\gamma_{(G,q)}$ or γ_q rather than γ_G.)

Note that the value of $\gamma_G(\varphi)$ depends only on the restriction of φ to the submodule of $\mathbb{Q}/\mathbb{Z}$ generated by the image of q, so that there are only a finite number of distinct values taken on by $\gamma_G(\varphi)$. These values can all be found by taking φ to be one of the homomorphisms φ_N which multiplies any element of $\mathbb{Q}/\mathbb{Z}$ by N; the resulting value $\gamma_G(\varphi_N)$ will be denoted by $\gamma_G(N)$.

Note also that $\gamma_{(G,q)}(\varphi) = \gamma_{(G,\varphi \circ q)}(1)$, so that all values of $\gamma_{(G,q)}$ can be found by varying the quadratic form on G, and computing the corresponding sums with $\varphi = \varphi_1$.

We now investigate how the Gauss invariant behaves with respect to various operations on finite quadratic forms.

LEMMA 1.1. *If* $G \cong H \overset{\perp}{\oplus} K$, *then* $\gamma_G(\varphi) = \gamma_H(\varphi)\gamma_K(\varphi)$ *for all* φ.

PROOF. This is just a computation:

$$\begin{aligned}
\gamma_G(\varphi) &= |G|^{-1/2} \sum_{x \in G} \exp(2\pi i \varphi(q(x))) \\
&= |G|^{-1/2} \sum_{y \in H, z \in K} \exp(2\pi i \varphi(q(y) + q(z))) \\
&= |H|^{-1/2} \sum_{y \in H} \exp(2\pi i \varphi(q(y))) \cdot |K|^{-1/2} \sum_{z \in K} \exp(2\pi i \varphi(q(z))) \\
&= \gamma_H(\varphi)\gamma_K(\varphi)
\end{aligned}$$

Q.E.D.

LEMMA 1.2. *Let (G,q) be a finite quadratic form, and let H be a totally isotropic subgroup of G. Then $\gamma_G(1) = |H|^{1/2}|G/H^\perp|^{-1/2}\gamma_{H^\perp/H}(1)$.*

PROOF. Let $x_1, \dots, x_m$ be a complete set of representatives for the cosets of G/H, where $m = |G/H|$. Then

$$\begin{aligned}\gamma_G(1) &= |G|^{-1/2}\sum_{x_j}\sum_{y\in H}\exp(2\pi i q(x_j+y)) \\ &= |G|^{-1/2}\sum_{x_j}\sum_{y\in H}\exp(2\pi i (q(x_j)+\langle x_j,y\rangle)) \\ &= |G|^{-1/2}\sum_{x_j}\exp(2\pi i q(x_j))\sum_{y\in H}\exp(2\pi i\langle x_j,y\rangle)\end{aligned}$$

Now $\mathrm{Ad}_q(x_j)$ defines a homomorphism from H to $\mathbb{Q}/\mathbb{Z}$; let k be the order of the image. If this homomorphism is trivial (which is the case exactly when $x_j \in H^\perp$), then $\sum_{y\in H}\exp(2\pi i\langle x_j,y\rangle) = |H|$. Otherwise, $\sum_{y\in H}\exp(2\pi i\langle x_j,y\rangle)$ is the sum all the k^{th} roots of unity, each counted $|H|/k$ times; the sum is therefore 0. Thus,

$$\begin{aligned}\gamma_G(1) &= |G|^{-1/2}|H|\sum_{x_j\in H^\perp}\exp(2\pi i q(x_j)) \\ &= |H|^{1/2}|G/H^\perp|^{-1/2}|H^\perp/H|^{-1/2}\sum_{x_j\in H^\perp}\exp(2\pi i q(x_j)) \\ &= |H|^{1/2}|G/H^\perp|^{-1/2}\gamma_{H^\perp/H}(1).\end{aligned}$$

Q.E.D.

Since $|H| = |G/H^\perp|$ when (G,q) is nondegenerate, we get:

COROLLARY 1.3. *Let (G,q) be a nondegenerate finite quadratic form, and let H be a totally isotropic subgroup. Then $\gamma_G(1) = \gamma_{H^\perp/H}(1)$.*

Recall that the *kernel* of a finite quadratic form (G,q) is $\mathrm{Ker}(G) = \mathrm{Ker}(\mathrm{Ad}_q)$, and the *q-radical* of (G,q) is

$$\mathrm{Rad}_q(G) = \{x \in \mathrm{Ker}(G) | q(x) \equiv 0 \mod \mathbb{Z}\}.$$

Note that $q|_{\mathrm{Ker}(G)}$ is $\mathbb{Z}$-linear, with values in $\frac{1}{2}\mathbb{Z}/\mathbb{Z}$.

COROLLARY 1.4. *Let $\bar{G} = G/\mathrm{Rad}_q(G)$, and let $\bar{q}$ be the induced quadratic form on $\bar{G}$. Then $\gamma_{(G,q)}(\varphi) = |\mathrm{Rad}_q(G)|^{1/2}\gamma_{(\bar{G},\bar{q})}(\varphi)$.*

PROOF. $\mathrm{Rad}_q(G)$ is an isotropic subgroup for $(G, \varphi \circ q)$, and $\mathrm{Rad}_q(G)^\perp = G$, so

$$\begin{aligned} \gamma_{(G,q)}(\varphi) &= \gamma_{(G,\varphi\circ q)}(1) \\ &= |\mathrm{Rad}_q(G)|^{1/2}\gamma_{(\bar{G},\varphi\circ\bar{q})}(1) \\ &= |\mathrm{Rad}_q(G)|^{1/2}\gamma_{(\bar{G},\bar{q})}(\varphi). \end{aligned}$$

Q.E.D.

LEMMA 1.5. *Let (G, q) be a finite quadratic form. If $\mathrm{Ker}(G) \neq \mathrm{Rad}_q(G)$, then $\gamma_G(1) = 0$.*

PROOF. By corollary (1.4), it suffices to prove the statement in the case in which the q-radical is trivial. In this case, the kernel is nontrivial, and so $\mathrm{Ker}(G) \cong \mathbb{Z}/\not{=}\mathbb{Z}$; let x be a generator of $\mathrm{Ker}(G)$. If $x = 2y$ for some $y \in G$, then $q(x) = 4q(y) = 2\langle y, y\rangle = \langle 2y, y\rangle = \langle x, y\rangle \in \mathbb{Z}$. Hence, $x \in \mathrm{Rad}_q(G)$, a contradiction.

Thus, x is not divisible by 2 in G, so there is a direct sum decomposition (as finite groups) $G \cong \mathrm{Ker}(G) \bigoplus G_0$. This is clearly an orthogonal direct sum decomposition, so it suffices by lemma (1.1) to show that $\gamma_{\mathrm{Ker}(G)}(1) = 0$. But

$$\begin{aligned} \gamma_{\mathrm{Ker}(G)}(1) &= 2^{-1/2}(\exp(2\pi i q(0)) + \exp(2\pi i q(x))) \\ &= 2^{-1/2}(e^{2\pi i} + e^{2\pi i/2}) \\ &= 0. \end{aligned}$$

Q.E.D.

We now apply these results to take a first step in computing the Gauss invariants of finite quadratic forms.

PROPOSITION 1.6. *Let p be prime, and u be relatively prime to p. Then $\gamma_{w^\varepsilon_{p,k}}(p^\ell u)$ takes the following values:*

(1.6.1) $p^{k/2}$, *if* $\ell > k$
(1.6.2) $p^{\ell/2}$, *if* $\ell = k$ *and* $p > 2$
(1.6.3) 0, *if* $\ell = k$ *and* $p = 2$
(1.6.4) $p^{\ell/2}\gamma_{z^{au}_{p^{k-\ell}}}(1)$, *if* $\ell < k$, *where* $\varepsilon = \chi(a)$.

PROOF. Recall that $w^\varepsilon_{p,k} \cong z^a_{p^k}$, where $\varepsilon = \chi(a \bmod p^k)$ if p is odd, and $\varepsilon = \chi(a \bmod 2^{k+1})$ if $p = 2$. Let (G, q) denote this form $z^a_{p^k}$. If e is a generator for G, then the annihilator of e is (p^k), and the form is given by $q(re) = r^2 a/2p^k$.

The Gauss invariant in question, which we shall denote by γ, is best computed by using the form $\widetilde{q}$ on G defined by $\widetilde{q}(x) = p^\ell u \cdot q(x)$. (For

then $\gamma = \gamma_{(G,\widetilde{q})}(1)$.) Since $\langle re, e\rangle_{\widetilde{q}} = p^\ell u \cdot ra/p^k$, we see that $\mathrm{Ker}(\widetilde{q})$ is generated by $p^{k-\ell}e$ if $\ell \le k$, and $\mathrm{Ker}(\widetilde{q}) = G$ if $\ell > k$. In fact, if $\ell > k$, then $\mathrm{Rad}_q(\widetilde{q}) = G$ as well, so that by corollary (1.4), $\gamma = |G|^{1/2} = p^{k/2}$, as claimed.

Thus, we may assume that $\ell \le k$. Now $\widetilde{q}(p^{k-\ell}e) = p^{k-\ell}au/2$. Thus, if $\ell < k$ or $p > 2$, $p^{k-\ell}e$ generates $\mathrm{Rad}_q(\widetilde{q})$ as well as $\mathrm{Ker}(\widetilde{q})$. In this case, the induced form $\bar{q}$ on $\bar{G} = G/\mathrm{Rad}_q(\widetilde{q})$ is nondegenerate and satisfies $\bar{q}(re) = r^2au/2p^{k-\ell}$; thus, $(\bar{G}, \bar{q}) \cong z^{au}_{p^{k-\ell}}$. It then follows from corollary (1.4) that $\gamma = |\mathrm{Rad}_q(\widetilde{q})|^{1/2} \cdot \gamma_{z^{au}_{p^{k-\ell}}}(1) = p^{\ell/2} \cdot \gamma_{z^{au}_{p^{k-\ell}}}(1)$, proving the formula in this case.

Finally, in the case $\ell = k$, $p = 2$, we have that $\mathrm{Ker}(\widetilde{q}) \neq \mathrm{Rad}_q(\widetilde{q})$. By lemma (1.5), $\gamma = 0$. Q.E.D.

Proposition 1.7. *Let ε be a 2-adic unit.*

(1.7.1) $\gamma_{u_k}(2^\ell\varepsilon) = 2^k$ *for* $\ell \ge k$, *and* $\gamma_{u_k}(2^\ell\varepsilon) = 2^\ell \cdot \gamma_{u_{k-\ell}}(\varepsilon)$ *for* $\ell < k$.

(1.7.2) $\gamma_{v_k}(2^\ell\varepsilon) = 2^k$ *for* $\ell \ge k$, *and* $\gamma_{v_k}(2^\ell\varepsilon) = 2^\ell \cdot \gamma_{v_{k-\ell}}(\varepsilon)$ *for* $\ell < k$.

The proof is similar to that of proposition (1.6), and is left to the reader.

2. Gauss Sums

In order to finish the computation of the Gauss invariants of the finite quadratic forms $w^\varepsilon_{p,k}$, u_k, and v_k, we need to study the properties of Gauss sums. Let a and ℓ be relatively prime integers such that $2|a\ell$. Define the *Gauss sum* $S(a,\ell)$ by

$$S(a,\ell) = |\ell|^{-1/2} \sum_{x=0}^{|\ell|-1} \exp(\pi i a x^2/\ell).$$

Note that $S(a,\ell) = \gamma_{z^a_\ell}(1)$, where (z^a_ℓ, q) is the quadratic form on $\mathbb{Z}/\ell\mathbb{Z}$ defined in section 7 of chapter I; in particular, the terms in the sum only depend on $x \bmod \ell$. Clearly, the sum $S(a,\ell)$ only depends on $a \bmod 2\ell$. Moreover, $S(-a,-\ell) = S(a,\ell)$.

The first properties of this sum follow directly from our analysis in section 1.

Corollary 2.1.

(2.1.1) *If a, ℓ, and m are relatively prime and $2|a\ell m$, then* $S(a,\ell m) = S(a\ell, m)S(am,\ell)$.

(2.1.2) *If p is an odd prime and $r \ge 2$, or if $p = 2$ and $r \ge 3$, then* $S(a,p^r) = S(a,p^{r-2})$.

PROOF. The first property follows from the direct sum decomposition $z^a_{\ell m} \cong z^{a\ell}_m \oplus z^{am}_\ell$, and the second comes from the fact that if x is a generator for $z^a_{p^r}$, then $y = p^{r-1}x$ generates a totally isotropic subgroup H, and $H^\perp/H \cong z^a_{p^{r-2}}$. Q.E.D.

There are a few additional elementary properties of Gauss sums. (We extend the definition of the Legendre symbol $\left(\frac{2}{a}\right)$ to all odd integers a by exploiting the fact that its value only depends on $a \bmod 8$; note that we then have $\left(\frac{2}{-a}\right) = \left(\frac{2}{a}\right)$.)

LEMMA 2.2.

(2.2.1) $S(a,1) = 1, S(a,2) = (1+i^a)/\sqrt{2} = \left(\frac{2}{a}\right)\exp(\pi i a/4)$, *and* $S(a,4) = \exp(\pi i a/4)$.

(2.2.2) If p is an odd prime, then $S(2b,p) = \left(\frac{b}{p}\right) S(2,p)$, *where* $\left(\text{-}\right)$ *denotes the Legendre symbol.*

PROOF. (2.2.1) follows from a direct computation, together with the formula $(1+i^a)/\sqrt{2} = \left(\frac{2}{a}\right)\exp(\pi i a/4)$, which is easy to verify. To prove (2.2.2), consider first the case in which $b \equiv j^2$ is a square $\bmod p$. Then

$$\begin{aligned} S(2b,p) &= \sum_{x=0}^{p-1} \exp(2\pi i j^2 x^2/p) \\ &= \sum_{y=0}^{p-1} \exp(2\pi i y^2/p) \\ &= S(2,p), \end{aligned}$$

proving the formula in this case.

On the other hand, if $2b$ is not a square $\bmod p$, then

$$\sqrt{p}\cdot S(2b,p) - 1 = 2\cdot \sum_{(\text{non-residues } k)} e^{2\pi i k/p},$$

while

$$\sqrt{p}\cdot S(2,p) - 1 = 2\cdot \sum_{(\text{non-zero residues } k)} e^{2\pi i k/p}.$$

Thus, $\sqrt{p}\cdot S(2b,p) - 1 + \sqrt{p}\cdot S(2,p) - 1 =$ twice the sum of all primitive p^{th} roots of unity, and so equals -2. Hence, $S(2b,p) + S(2,p) = 0$. Q.E.D.

It remains to compute $S(2,p)$ for odd primes p; to do this, we establish a general reciprocity property for Gauss sums.

PROPOSITION 2.3. *$S(a,\ell) = S(-\ell,a)\exp(\pi i\sigma/4)$, where $\sigma = a\ell/|a\ell| \in \{1,-1\}$.*

PROOF. Since $S(-a,-\ell) = S(a,\ell)$, we may assume without loss of generality that $\ell > 0$. Let

$$f(t) = \sum_{k=0}^{\ell-1} \exp(\frac{\pi i a(t+k)^2}{\ell}),$$

and Fourier expand. If

$$b_n = \int_0^1 f(t)\exp(2\pi i n t)dt,$$

then

$$f(t) = \sum_{-\infty}^{\infty} b_n \exp(-2\pi i n t)$$

and

$$S(a,\ell) = |\ell|^{-1/2} f(0) = |\ell|^{-1/2} \sum_{n=-\infty}^{\infty} b_n.$$

Now

$$b_n = \sum_{k=0}^{\ell-1} \int_0^1 \exp(2\pi i(\frac{a(t+k)^2}{2\ell} + nt))dt.$$

Complete the square:

$$\frac{a(t+k)^2}{2\ell} + nt = \frac{a(t+k+\frac{n\ell}{a})^2}{2\ell} - nk - \frac{n^2\ell}{2a}.$$

Making the substitution $s = t + k + n\ell/a$, and using the fact that $\exp(2\pi i(-nk)) = 1$, we get

$$b_n = \exp(\frac{-\pi i n^2\ell}{a}) \sum_{k=0}^{\ell-1} \int_{k+\frac{n\ell}{a}}^{k+1+\frac{n\ell}{a}} \exp(\frac{\pi i a s^2}{\ell})ds.$$

Now if $n = am + r$, then $(am+r)^2\ell/a \equiv r^2\ell/a \mod 2\mathbb{Z}$. Thus,

$$b_{am+r} = \exp(\frac{-\pi i r^2\ell}{a}) \sum_{k=0}^{\ell-1} \int_{k+m\ell+\frac{r\ell}{a}}^{k+m\ell+1+\frac{r\ell}{a}} \exp(\frac{\pi i a s^2}{\ell})ds.$$

Hence,

$$\sum_{m=-\infty}^{\infty} b_{am+r} = \exp(\frac{-\pi i r^2\ell}{a}) \int_{-\infty}^{\infty} \exp(\frac{\pi i a s^2}{\ell})ds.$$

If we make the substitution $y = |a/\ell|^{1/2}s$, then $as^2/\ell = \sigma y^2$, where $\sigma = a\ell/|a\ell|$; setting

$$I_\sigma = \int_{-\infty}^{\infty} \exp(\pi i \sigma y^2) dy,$$

we find

$$\sum_{m=-\infty}^{\infty} b_{am+r} = \exp(\frac{-\pi i r^2 \ell}{a})|\frac{\ell}{a}|^{1/2} I_\sigma$$

Thus,

$$\begin{aligned} S(a,\ell) &= |\ell|^{-1/2} \sum_{r=0}^{|a|-1} \sum_{n=-\infty}^{\infty} b_{am+r} \\ &= |a|^{-1/2} \sum_{r=0}^{|a|-1} \exp(-\pi i r^2 \ell/a) I_\sigma \\ &= S(-\ell, a) I_\sigma. \end{aligned}$$

We still need to evaluate the integrals I_σ for $\sigma = 1$ and $\sigma = -1$. But using the property already established together with Lemma (2.2) we find:

$$\begin{aligned} I_\sigma &= S(\sigma,2)/S(-2,\sigma) = S(\sigma,2)/S(-2\sigma,1) \\ &= S(\sigma,2) = \left(\frac{2}{\sigma}\right) \exp(\pi i \sigma/4) = \exp(\pi i \sigma/4). \end{aligned}$$

Q.E.D.

COROLLARY 2.4. *If p is odd, then $S(2,p) = \left(\frac{2}{p}\right) \exp(\pi i(1-p)/4)$.*

PROOF.

$$\begin{aligned} S(2,p) &= S(-p,2)\exp(\pi i/4) \\ &= \left(\frac{2}{-p}\right) \exp(\pi i(-p)/4) \exp(\pi i/4) \\ &= \left(\frac{2}{p}\right) \exp(\pi i(1-p)/4). \end{aligned}$$

Q.E.D.

These properties together allow the computation of $S(a,\ell)$ in general; we record here the results when ℓ is a prime power.

COROLLARY 2.5.

(2.5.1) If p is an odd prime, b is relatively prime to p, and $r \geq 1$, then

$$S(2b, p^r) = \left(\tfrac{2b}{p}\right)^r \left(\exp(\pi i(1-p)/4)\right)^{r^2}.$$

(2.5.2) If a is odd and $r \geq 1$, then
$$S(a, 2^r) = \left(\tfrac{2}{a}\right)^r \exp(\pi i a/4).$$

PROOF. (2.5.1) By corollary (2.1) and lemma (2.2), if r is even then $S(2b, p^r) = S(2b, 1) = 1$, while if r is odd then

$$\begin{aligned} S(2b, p^r) &= S(2b, p) \\ &= \left(\frac{b}{p}\right) \cdot S(2, p) \\ &= \left(\frac{b}{p}\right) \cdot \left(\frac{2}{p}\right) \cdot \exp(\pi i(1-p)/4) \\ &= \left(\frac{2b}{p}\right) \cdot \exp(\pi i(1-p)/4), \end{aligned}$$

where we have used corollary (2.4) to find the value of $S(2, p)$. Since $\left(\frac{2b}{p}\right) \in \{\pm 1\}$, $\exp(\pi i(1-p)/4) \in \{\pm 1, \pm i\}$, and $r^2 \equiv 0 \mod 4$ for r even while $r^2 \equiv 1 \mod 4$ for r odd, the formula follows.

(2.5.1) By corollary (2.1) and lemma (2.2), if r is even then $S(a, 2^r) = S(a, 4) = \exp(\pi i a/4)$, while if r is odd then $S(a, 2^r) = S(a, 2) = \left(\frac{2}{a}\right) \cdot \exp(\pi i a/4)$. Again since $\left(\frac{2}{a}\right) \in \{\pm 1\}$, the formula follows. Q.E.D.

We can now finish the computation of the Gauss invariants of the finite quadratic forms $w^{\varepsilon}_{p,k}$, u_k, and v_k. From proposition (1.6) and corollary (2.5) we get:

COROLLARY 2.6.

(2.6.1) If p is odd, then $\gamma_{w^{\varepsilon}_{p,k}}(p^\ell u) = p^{k/2}$ for $\ell \geq k$, and
$$\gamma_{w^{\varepsilon}_{p,k}}(p^\ell u) = p^{\ell/2} \cdot \varepsilon^{k-\ell} \left(\frac{u}{p}\right)^{k-\ell} (\exp(\pi i(1-p)/4))^{(k-\ell)^2} \text{ for } \ell < k.$$

(2.6.2) If $p = 2$, then
$\gamma_{w^{\varepsilon}_{2,k}}(2^\ell u) = 2^{k/2}$ *for* $\ell > k$,
$\gamma_{w^{\varepsilon}_{2,k}}(2^\ell u) = 0$ *for* $\ell = k$, *and*
$\gamma_{w^{\varepsilon}_{2,k}}(2^\ell u) = 2^{\ell/2} \cdot \left(\frac{2}{\varepsilon}\right)^{k-\ell} \left(\frac{2}{u}\right)^{k-\ell} \exp(\pi i \varepsilon u/4)$ *for* $\ell < k$.

PROOF. This is clear. Q.E.D.

As the final step in our computation, we prove:

PROPOSITION 2.7. *Let ε be a 2-adic unit. Then $\gamma_{u_k}(\varepsilon) = 1$ for all k, while $\gamma_{v_k}(\varepsilon) = (-1)^k$.*

PROOF. First note that by corollary (II.7.7), multiplying all values of the quadratic form u_k or v_k by a fixed unit does not change the

isomorphism type of the form; thus for ε a unit, $\gamma_{u_k}(\varepsilon) = \gamma_{u_k}(1)$ and $\gamma_{v_k}(\varepsilon) = \gamma_{v_k}(1)$.

To compute $\gamma_{u_k}(1)$, let x and y be the standard generators, and consider the subgroup H generated by x. H is an isotropic subgroup; moreover, since $\langle x, ax+by\rangle = b/2^k$, $H^\perp = H$. Thus, by corollary (1.3), $\gamma_{u_k}(1) = \gamma_{H^\perp/H}(1) = 1$.

To compute $\gamma_{v_k}(1)$, we use the example in Section (II.10). It was shown there that there exists a totally isotropic subspace H for the form $(G,q) = w^1_{2,k+1} \overset{\perp}{\oplus} w^3_{2,k+1}$ such that $H^\perp/H$ is isomorphic to v_k. Again using corollary (1.3), we see that $\gamma_{v_k}(1) = \gamma_{w^1_{2,k+1}}(1) \cdot \gamma_{w^3_{2,k+1}}(1)$. By corollary (2.6), we find

$$\gamma_{v_k}(1) = \left(\tfrac{2}{1}\right)^{k+1} \exp(\pi i/4) \cdot \left(\tfrac{2}{3}\right)^{k+1} \exp(3\pi i/4) = (-1)^k. \qquad \text{Q.E.D.}$$

Combining this with proposition (1.7), we get:

Corollary 2.8.

(2.8.1) $\gamma_{u_k}(2^\ell\varepsilon) = 2^k$ *for* $\ell \geq k$, *and*
$\gamma_{u_k}(2^\ell\varepsilon) = 2^\ell$ *for* $\ell < k$.

(2.8.2) $\gamma_{v_k}(2^\ell\varepsilon) = 2^k$ *for* $\ell \geq k$, *and*
$\gamma_{v_k}(2^\ell\varepsilon) = 2^\ell \cdot (-1)^{k-\ell}$ *for* $\ell < k$.

3. Signature invariants for torsion quadratic forms over $\mathbb{Z}_{(}$

Lemma 3.1. *Let (G,q) be a nondegenerate torsion quadratic form over $\mathbb{Z}_{(}$, let r_ℓ be the length of the homogeneous piece of G with scale p^ℓ, and define*

$$\rho(\ell) = \sum_{j\leq\ell} j \cdot r_j + \sum_{j>\ell} \ell \cdot r_j.$$

Then $\gamma_G(p^\ell)/p^{\rho(\ell)/2}$ is either 0, or an eighth root of unity.

Proof. Since the quantity $\gamma_G(p^\ell)/p^{\rho(\ell)/2}$ is multiplicative under direct sums, it suffices to verify this for the standard forms $w^\varepsilon_{p,k}$, u_k, and v_k. In the case of $w^\varepsilon_{p,k}$, $\rho(\ell) = k$ if $k \leq \ell$, and $\rho(\ell) = \ell$ if $k > \ell$; the statement follows from corollary (2.6). In the case of u_k or v_k, $\rho(\ell) = 2k$ if $k \leq \ell$, and $\rho(\ell) = 2\ell$ is $k > \ell$; this time the statement follows from Corollary (2.8). Q.E.D.

Definition 3.2. The *ℓ^{th} signature invariant* of a nondegenerate torsion quadratic form (G,q) over $\mathbb{Z}_{(}$ is the quantity

$$\sigma_\ell(G) = \gamma_G(p^\ell)/p^{\rho(\ell)/2},$$

which, as we have seen, is multiplicative under direct sum and takes values in $\{0, e^{\pi i\alpha/4}\}$.

(G,q)	$\sigma_\ell(G)$			
	$\ell < k$		$\ell = k$	$\ell > k$
	$k-\ell$ even	$k-\ell$ odd		
$w^{\varepsilon}_{p,k}$, p odd	$\varepsilon^{(k-\ell)}\exp(\pi i(1-p)(k-\ell)^2/4)$		1	1
$w^{1}_{p,k}$, p odd	1	$(-i)^{(p-1)/2}$	1	1
$w^{-1}_{p,k}$, p odd	1	$-(-i)^{(p-1)/2}$	1	1
$w^{\varepsilon}_{2,k}$	$\left(\frac{2}{\varepsilon}\right)^{(k-\ell)}\exp(\pi i\varepsilon/4)$		0	1
$w^{1}_{2,k}$	$\exp(\pi i/4)$	$\exp(\pi i/4)$	0	1
$w^{3}_{2,k}$	$\exp(3\pi i/4)$	$\exp(7\pi i/4)$	0	1
$w^{5}_{2,k}$	$\exp(5\pi i/4)$	$\exp(\pi i/4)$	0	1
$w^{7}_{2,k}$	$\exp(7\pi i/4)$	$\exp(7\pi i/4)$	0	1
u_k	1	1	1	1
v_k	1	-1	1	1

TABLE 3.1. signature invariants of the standard torsion quadratic forms

Corollaries (2.6) and (2.8) provide a computation of the signature invariants for the standard forms $w^{\varepsilon}_{p,k}$, u_k, and v_k; we present the results in Table (3.1).

4. The discriminant and the Gauss invariant

In this section, we will show how the discriminant and mod-8 discriminant are related to the Gauss invariant for nondegenerate quadratic forms on finite abelian 2-groups. Our method is to use the decomposition into indecomposable pieces whose existence is guaranteed by Corollary (II.11.5), and then to compute explicitly with those pieces. Unfortunately, we do not know direct proofs of the relations we find.

PROPOSITION 4.1. *Let (G,q) be a nondegenerate torsion quadratic form over $\mathbb{Z}_{(2)}$, let $r = \text{length}(G)$, let $\Delta = |G|$, and let $\delta = \Delta \cdot \text{disc}(G,q)$ be the unit part of the discriminant. Then*

$$\left(\frac{-1}{\delta}\right) = i^{-r}\cdot\gamma_G(1)^2.$$

Notice that δ is well-defined $\mod 4$ (at least), so that $\left(\frac{-1}{\delta}\right)$ is always well-defined.

PROOF. As remarked above, since both sides of this formula are multiplicative under orthogonal direct sum, it suffices to prove the formula for indecomposable forms of ranks one and two. By Example

(I.7.9) and Lemma (II.7.6), each such form must be isomorphic to one of the basic forms $w^{\varepsilon}_{2,k}$, u_k, and v_k.

If $(G,q) \cong w^{\varepsilon}_{2,k}$, then $\delta \equiv \varepsilon \mod 4$, while $\gamma_G(1)^2 = \left(\frac{2}{\varepsilon}\right)^{2k} \exp(2\pi i\varepsilon/4) = \exp(\pi i\varepsilon/2) = i \cdot \left(\frac{-1}{\varepsilon}\right)$, verifying the formula in this case. (The last equality, which holds for any odd ε, is easy to check.)

If $(G,q) \cong u_k$ or v_k, then $\delta \equiv 3 \mod 4$, while $r = 2$ and $\gamma_G(1) = \pm 1$. Since $i^{-2} \cdot (\pm 1)^2 = -1 = \left(\frac{-1}{3}\right)$, the formula again follows. Q.E.D.

PROPOSITION 4.2. *Let (G,q) be a good and special nondegenerate torsion quadratic form over $\mathbb{Z}_{\not 2}$, let $r = \text{length}(G)$, let $2^k = \text{exponent}(G)$, and let $\delta = \text{disc}_8(G,q)$ be the mod-8 discriminant. Then for each ℓ with $0 \le \ell < k$, we have*

$$\gamma_G(2^\ell)/\gamma_G(1) = 2^{\ell r/2} \cdot \left(\frac{2}{\delta}\right)^{\ell}.$$

In particular,

$$\left(\frac{2}{\delta}\right) = 2^{-r/2} \cdot \gamma_G(2)/\gamma_G(1).$$

Notice that $\gamma_G(1)$ is never zero for a nondegenerate form, so that the right hand side of the equation is well-defined. It is also nonzero, since $\gamma_G(2) \neq 0$ for a good and special form. Moreover, notice that $\left(\frac{2}{\delta}\right)$ only depends on $\delta \bmod 8$.

PROOF. It again suffices to verify this for the forms $w^{\varepsilon}_{2,k}$, u_k, and v_k.

If $(G,q) \cong w^{\varepsilon}_{2,k}$, then $k \ge 2$ since it is good and special, and $\delta \equiv \varepsilon \mod 8$. We find that

$$\gamma_G(2^\ell)/\gamma_G(1) = \left\{ 2^{\ell/2} \cdot \left(\frac{2}{\varepsilon}\right)^{k-\ell} \exp(\pi i\varepsilon/4) \right\} / \left\{ \left(\frac{2}{\varepsilon}\right)^{k} \exp(\pi i\varepsilon/4) \right\} = 2^{\ell/2} \cdot \left(\frac{2}{\varepsilon}\right)^{\ell},$$

so the formula holds.

If $(G,q) \cong u_k$, then $\delta \equiv 7 \mod 8$, while $r = 2$ and $\gamma_G(2^\ell)/\gamma_G(1) = 2^\ell/1 = 2^\ell = 2^\ell \cdot \left(\frac{2}{7}\right)^{\ell}$. If $(G,q) \cong v_k$, then $\delta \equiv 3 \mod 8$, while $r = 2$ and $\gamma_G(2^\ell)/\gamma_G(1) = 2^\ell \cdot (-1)^{k-\ell}/(-1)^k = 2^\ell \cdot (-1)^\ell = 2^\ell \cdot \left(\frac{2}{3}\right)^{\ell}$. Q.E.D.

These two pieces of information about the discriminant can be combined: it is easy to verify that for odd $\delta \bmod 8$ we have

$$\exp(\pi i\delta/4) = \left(\frac{2}{\delta}\right) \left\{ 1 + i \cdot \left(\frac{-1}{\delta}\right) \right\} / 2^{1/2}.$$

Thus, we get:

COROLLARY 4.3. *Let (G,q) be a good and special nondegenerate torsion quadratic form over $\mathbb{Z}_{(\not 2)}$, let $r = \text{length}(G)$, and let $\delta = \text{disc}_8(G,q)$ be the mod-8 discriminant. Then*

$$\exp(\pi i\delta/4) = 2^{-(r+1)/2} \cdot \left\{1 + i^{(1-r)} \cdot \gamma_G(1)^2\right\} \cdot \gamma_G(2)/\gamma_G(1).$$

These formulae may be more easily digestible when expressed in terms of the signature invariants. The statement, whose proof we leave to the reader, is given below; it follows either from the above statements, or by a direct computation using Tables (3.1) and (II.6.1).

PROPOSITION 4.4. *Let (G,q) be a good and special nondegenerate torsion quadratic form over $\mathbb{Z}_{(\not 2)}$, let $2^k = \text{exponent}(G)$, and let $\delta = \text{disc}_8(G,q)$ be the mod-8 discriminant. Then for each ℓ with $0 \le \ell < k$, we have*

$$\sigma_\ell(G)/\sigma_0(G) = \left(\frac{2}{\delta}\right)^\ell.$$

Although we will not have an occasion to use it, we note here a similar relation for the discriminant of a torsion quadratic forms over $\mathbb{Z}_{(}$ for p odd. The proof (which consists of checking the formula for $w^\varepsilon_{p,k}$) is left to the reader.

PROPOSITION 4.5. *Let (G,q) be a nondegenerate torsion quadratic form over $\mathbb{Z}_{(}$, p odd, let $r = \text{length}(G)$, let $\Delta = |G|$, and let $\delta = \Delta \cdot \text{disc}(G,q)$ be the unit part of the discriminant. Then*

$$\left(\frac{\delta}{p}\right) = p^{-r/2} \cdot \exp(\pi i(1-p)/4)^{-r} \cdot \gamma_G(p) \cdot \gamma_G(1).$$

5. Milgram's theorem: the signature

We now come to a fundamental result due to Milgram which relates the signature of an integral quadratic form to its Gauss invariant. First, some notation. If L is a nondegenerate integral quadratic form, we define its Gauss invariant γ_L to be the Gauss invariant γ_{G_L} of its discriminant form G_L.

THEOREM 5.1. *Let L be a nondegenerate integral quadratic form with signature (s_+, s_-), and let $s = s_+ - s_-$. Then $\gamma_L(1) = \exp(\pi i s/4)$*

PROOF. Let r be the rank of L. There exist elements $x_1, \ldots, x_r \in L$ which form a diagonal basis for the induced form on $L \otimes \mathbb{Q}$. Let L_1 be the $\mathbb{Z}$-span of $\{x_1, \ldots, x_r\}$. By the standard "overlattice" construction (section 10 of chapter II), $H = L/L_1$ is an isotropic subspace in $G_{L_1} = L_1^\#/L_1$, and $H^\perp/H = G_L$. By corollary (1.3), $\gamma_L(1) = \gamma_{L_1}(1)$.

Since L and L_1 have the same signature, to prove the theorem it suffices to prove it for L_1; hence we are reduced to the case of a diagonal form. Moreover, since the signature is additive and the Gauss invariant is multiplicative under direct sum, it suffices to prove it for a form of rank 1.

So suppose that $L = \langle a \rangle$ for some integer a. Then as shown in section 7 of chapter II, $G_L \cong z_{2a}^1$. Moreover, the signature of L is $(1,0)$ if $a > 0$, and $(0,1)$ if $a < 0$, so that $s = a/|a| \in \{\pm 1\}$. Now by the reciprocity property for Gauss sums,

$$\gamma_L(1) = S(1,2a) = S(-2a,1)\exp(\pi i s/4) = \exp(\pi i s/4).$$

Q.E.D.

CHAPTER IV

Quadratic Forms over $\mathbb{Z}_p$

In this chapter, we will give a complete description of the isomorphism classes of nondegenerate quadratic $\mathbb{Z}_p$-modules, and of nondegenerate torsion quadratic forms over $\mathbb{Z}_p$.

1. Indecomposable Forms of Ranks One and Two Over $\mathbb{Z}_p$

According to the decomposition proved in Section 11 of chapter II, all nondegenerate quadratic $\mathbb{Z}_p$-modules and all nondegenerate torsion quadratic forms over $\mathbb{Z}_p$ can be built up (using direct sums) from indecomposable forms of ranks one and two. We discuss these forms here.

In section 7 of Chapter I, we gave examples of indecomposable nondegenerate quadratic forms on both free and torsion $\mathbb{Z}_p$-modules of ranks 1 and 2. The basic quadratic $\mathbb{Z}_p$-modules are the forms $W_{p,k}^{\varepsilon}$, (for $k \geq 0$ if p is odd, and $k \geq 1$ if $p = 2$), and when $p = 2$, U_k and V_k for $k \geq 0$ on free $\mathbb{Z}_p$-modules. The basic torsion forms are the forms $w_{p,k}^{\varepsilon}$ (for $k \geq 1$ with any p) and when $p = 2$, u_k and v_k for $k \geq 1$ on torsion $\mathbb{Z}_p$-modules. The isomorphism classes for the forms of rank 1 are determined by p, ε, and k; we recall the statement from examples (I.7.1) and (I.7.9).

Lemma 1.1.

(1.1.1) Every nondegenerate quadratic form on a free $\mathbb{Z}_p$-module of rank one is isomorphic to one of the forms $W_{p,k}^{\varepsilon}$. Moreover, $W_{p,k}^{\varepsilon} \cong W_{p,\ell}^{\eta}$ if and only if $\varepsilon = \eta$ and $k = \ell$.

(1.1.2) Every nondegenerate quadratic form on a cyclic torsion $\mathbb{Z}_p$-module is isomorphic to one of the forms $w_{p,k}^{\varepsilon}$. Moreover, $w_{p,k}^{\varepsilon} \cong w_{p,\ell}^{\eta}$ if and only if either
(a) *$\varepsilon = \eta$ and $k = \ell$, or*
(b) *$p = 2$, $\varepsilon \equiv \eta \mod 4$, and $k = \ell = 1$.*

We also proved in chapter I a characterization of the indecomposable quadratic $\mathbb{Z}_2$-modules (of rank two), and extended this to the torsion case in chapter II. We recall the results (Lemma (I.7.7.3), and Lemma (II.7.6):

PROPOSITION 1.2.

(1.2.1) Let (L,Q) be a nondegenerate indecomposable quadratic $\mathbb{Z}_2$-module of rank two. Then $(L,Q) \cong U_k$ if and only if $\operatorname{disc}(L,Q) = 2^{2k}\delta$ *for some odd δ with $\left(\frac{2}{\delta}\right) = 1$, while $(L,Q) \cong V_k$ if and only if* $\operatorname{disc}(L,Q) = 2^{2k}\delta$ *for some odd δ with $\left(\frac{2}{\delta}\right) = -1$.*

(1.2.2) Let (G,q) be a nondegenerate indecomposable torsion quadratic form of rank two. (Note that (G,q) is necessarily good and special.) Let $\delta = \operatorname{disc}_8(G,q)$. Then $(G,q) \cong u_k$ if and only if (G,q) has scale 2^k and $\left(\frac{2}{\delta}\right) = 1$, while $(G,q) \cong v_k$ if and only if (G,q) has scale 2^k and $\left(\frac{2}{\delta}\right) = -1$.

We can interpret these results in the following way. Let us define $\mathcal{Q}_{\surd}$ (resp. $\mathcal{T}_{\surd}$, resp. $\mathcal{G}_{\surd}$) to be the monoid of isomorphism classes of nondegenerate quadratic $\mathbb{Z}_p$-modules (resp. nondegenerate torsion quadratic forms over $\mathbb{Z}_p$, resp. good and special nondegenerate torsion quadratic forms over $\mathbb{Z}_p$). (The operation in the monoid is direct sum.) Then for p odd, $\mathcal{Q}_{\surd}$ is generated by $\{W^{\varepsilon}_{p,k}$ for $k \geq 0\}$ and $\mathcal{T}_{\surd} = \mathcal{G}_{\surd}$ is generated by $\{w^{\varepsilon}_{p,k}$ for $k \geq 1\}$, while for $p = 2$, $\mathcal{Q}_{\in}$ is generated by $\{U_{k-1}, V_{k-1}, W^{\varepsilon}_{2,k}$ for $k \geq 1\}$, $\mathcal{T}_{\in}$ is generated by $\{u_k, v_k, w^{\varepsilon}_{2,k}$ for $k \geq 1\}$, and $\mathcal{G}_{\in}$ is generated by $\{u_{k-1}, v_{k-1}, w^{\varepsilon}_{2,k}$ for $k \geq 2\}$.

We recall one more important property of these forms of ranks one and two, which is a direct consequence of the computations in Lemmas (I.9.4) and (I.9.5).

PROPOSITION 1.3. *Let (L,Q) be one of the forms $W^{\varepsilon}_{p,k}$, U_k, or V_k. Then the natural map $\mathcal{O}(\mathcal{L}) \to \mathcal{O}(\mathcal{G}_{\mathcal{L}})$ is surjective.*

Next, we would like to offer the reader recognition criteria for deciding, given a specific rank one or rank two quadratic $\mathbb{Z}_p$-module, how it splits as a direct sum of the generators given above. This will become useful in the proof of the relations among these forms.

We begin with the rank one case, which is no more than formalizing the discussion following Example (I.7.1).

LEMMA 1.4. *Fix a prime p, and let $Q(r) = up^k r^2$ define a quadratic form on $\mathbb{Z}_p$, with u a unit* $\bmod p$.

(1.4.1) If p is odd, then $Q \cong W^{\varepsilon}_{p,k}$, where $\varepsilon = \left(\frac{2u}{p}\right)$.

(1.4.2) If p is 2, then $Q \cong W^{\varepsilon}_{2,k+1}$, where $\varepsilon \equiv u \bmod 8$.

The rank two case (which we will only discuss for $p = 2$) is more interesting. We begin with a decomposability criterion.

LEMMA 1.5. *Let $Q(r,s) = 2^k(ar^2 + brs + cs^2)$ be a quadratic form on $\mathbb{Z}_2^2$, and assume that not all of a, b, and c are even. Then Q is nondegenerate if and only if $b^2 \neq 4ac$. In this case, Q splits into two rank one forms if and only if b is even. If so, let $d = ac - b^2/4$ and write $d = 2^\ell \bar{d}$ with $\bar{d}$ odd. Then*

(1.5.1) If a is odd, then $Q \cong W_{2,k+1}^{a \bmod 8} \oplus W_{2,k+\ell+1}^{a\bar{d} \bmod 8}$.
(1.5.2) If c is odd, $Q \cong W_{2,k+1}^{c \bmod 8} \oplus W_{2,k+\ell+1}^{c\bar{d} \bmod 8}$.

PROOF. The nondegeneracy statement is clear. Suppose first that b is even. In case a is odd, let $x = (1,0)$ and $y = (-b/2, a)$; they also form a basis for $\mathbb{Z}_2^2$, and in this basis $Q(rx+sy) = Q(r - sb/2, as) = 2^k(a(r-sb/2)^2 + b(r-sb/2)(as) + c(as)^2) = 2^k(ar^2 - abrs + ab^2s^2/4 + abrs - ab^2s^2/2 + ca^2s^2) = 2^k(ar^2 + (ca^2 - ab^2/4)s^2) = 2^k ar^2 + 2^{k+\ell} a\bar{d}s^2$. This proves this case, and the other is the symmetric argument.

The converse is equivalent to proving that when the diagonal form $Q(r,s) = 2^k(ar^2 + cs^2)$ is re-written with any new basis for $\mathbb{Z}_2^2$, the resulting form has an even coefficient for the rs term. We may assume that a is odd. Let $x = (\alpha, \beta), y = (\gamma, \delta)$ be a new basis for $\mathbb{Z}_2^2$. Note that then $\alpha\delta - \beta\gamma$ is odd. In terms of this basis, Q has the form

$$Q(rx+sy) = 2^k((a\alpha^2 + c\beta^2)r^2 + 2(a\alpha\gamma + c\beta\delta)rs + (a\gamma^2 + c\delta^2)s^2)$$

and it suffices for our statement to show that at least one of the coefficients $a\alpha^2 + c\beta^2$ or $a\gamma^2 + c\delta^2$ is odd.

If α is odd and β is even, then $a\alpha^2 + c\beta^2$ is odd since a is odd. Assume α and β are both odd. Then since $\alpha\delta - \beta\gamma$ is odd, $\delta - \gamma$ must be odd, so δ and γ have opposite parity. If γ is odd and δ is even, then $a\gamma^2 + c\delta^2$ is odd. If γ is even and δ is odd, then $a\alpha^2 + c\beta^2 \equiv a + c \bmod 2$ and $a\gamma^2 + c\delta^2 \equiv c \bmod 2$, so since a is odd at least one of these is odd.

Hence we may assume α is even. This implies that both β and γ are odd, since $\alpha\delta - \beta\gamma$ is odd. If δ is even, then $a\gamma^2 + c\delta^2$ is odd. Finally, if δ is odd, then $a\alpha^2 + c\beta^2 \equiv c \bmod 2$ and $a\gamma^2 + c\delta^2 \equiv a + c \bmod 2$, so since a is odd at least one of these is odd. Q.E.D.

The recognition of the indecomposable forms is now easy.

LEMMA 1.6. *Let $Q(r,s) = 2^k(ar^2 + brs + cs^2)$ be a quadratic form on $\mathbb{Z}_2^2$, with b odd. Then Q is nondegenerate and indecomposable. Moreover,*

$$Q \cong U_k \text{ if } ac \text{ is even, and}$$

$$Q \cong V_k \text{ if } ac \text{ is odd.}$$

PROOF. Since b is odd, b^2-4ac is odd, so that Q is nondegenerate; hence it is indecomposable by Lemma (1.5). Also, since b is odd, 2^{k+1} does not divide all the values of Q, but 2^k clearly does; hence $Q \cong U_k$ or V_k. Applying Lemma (I.7.7.1), we see that $Q \cong U_k$ if and only if there is an isotropic vector. An isotropic vector for Q corresponds to a root of the quadratic equation $az^2+bz+c=0$, so we see that $Q \cong U_k$ if and only if b^2-4ac is a square, or, equivalently, if $b^2-4ac \equiv 1 \mod 8$. Since b is odd, $b^2 \equiv 1 \mod 8$, so $b^2-4ac \equiv 1 \mod 8$ if and only if ac is even. Q.E.D.

Finally let us briefly mention without proofs the relevant statements for inner product modules over $\mathbb{Z}_p$. Denote by $\mathcal{I}_p$ the monoid of isomorphism classes of inner product $\mathbb{Z}_p$-modules. Then if $p \neq 2$, we have $\mathcal{I}_p = \mathcal{Q}_p$ since every bilinear form is even. However if $p=2$, then we have the odd rank one forms $W^{\varepsilon}_{2,0}$; indeed, $\mathcal{I}_2$ is generated by $\{U_k, V_k, W^{\varepsilon}_{2,k} \text{ for } k \geq 0\}$.

2. Quadratic Forms over $\mathbb{Z}_p$, p odd

When p is odd, the relations which hold among the generators $W^{\varepsilon}_{p,k}$ of the monoid $\mathcal{Q}_{\surd}$ of isomorphism classes of nondegenerate quadratic $\mathbb{Z}_p$-modules (as well as the relations in the torsion cases $\mathcal{T}_{\surd}$ and $\mathcal{G}_{\surd}$) are quite easy to describe.

LEMMA 2.1. *Let p be an odd prime.*

(2.1.1) For all $k \geq 0$, there is an isomorphism of nondegenerate quadratic $\mathbb{Z}_p$-modules

$$W^{-1}_{p,k} \oplus W^{-1}_{p,k} \cong W^{1}_{p,k} \oplus W^{1}_{p,k}.$$

(2.1.2) For all $k \geq 1$, there is an isomorphism of torsion quadratic forms over $\mathbb{Z}_p$

$$w^{-1}_{p,k} \oplus w^{-1}_{p,k} \cong w^{1}_{p,k} \oplus w^{1}_{p,k}.$$

PROOF. Discriminant-forms allow the second statement to be deduced from the first, so we will only address the first. Choose a basis $\{x,y\}$ for $W^1_{p,k} \oplus W^1_{p,k}$ with $Q(rx+sy) = p^k(r^2+s^2)/2$. The squares mod p are not closed under addition; find two integers m and n, relatively prime to p, such that $j = m^2+n^2$ is not a square, and is still relatively prime to p. Let $x' = mx+ny$ and $y' = -nx+my$. Then $\{x', y'\}$ is also a basis for the free rank 2 module, and $Q(rx'+sy') = p^k(r^2j+s^2j)/2$. Thus the form is also isomorphic to $W^{-1}_{p,k} \oplus W^{-1}_{p,k}$. Q.E.D.

As we will see below, the relations listed here generate all relations among the generators of $\mathcal{Q}_{\surd}$ (respectively $\mathcal{T}_{\surd}$) for p odd. The first step in establishing that fact is finding a normal form for quadratic forms on p-groups.

DEFINITION 2.2. When p is odd, a decomposition of a quadratic form (G, q) on a finite abelian p-group is in *normal form* if

$$(G, q) = \bigoplus_{k\geq 1}((w_{p,k}^1)^{\oplus n(k)} \oplus (w_{p,k}^{-1})^{\oplus m(k)})$$

where $m(k) \leq 1$ for each k.

Given a normal form decomposition, we define

$$G(k) := (w_{p,k}^1)^{\oplus n(k)} \oplus (w_{p,k}^{-1})^{\oplus m(k)}.$$

LEMMA 2.3. *Every nondegenerate quadratic form (G, q) on a finite abelian p-group with p odd has a normal form decomposition.*

PROOF. (G, q) can be written as a sum of terms isomorphic to $w_{p,k}^1$ or $w_{p,k}^{-1}$. By using the isomorphism (2.1.2), we can easily guarantee that each homogeneous piece of the decomposition contains at most 1 term of type $w_{p,k}^{-1}$. Q.E.D.

It remains to show that we actually have a normal form, i.e., that the normal form is unique.

PROPOSITION 2.4. *If p is odd, a nondegenerate torsion quadratic form on a finite abelian p-group has a unique normal form decomposition.*

PROOF. Let (G, q) be such a form, and suppose that

$$(G, q) = \bigoplus_{k\geq 1}((w_{p,k}^1)^{\oplus n(k)} \oplus (w_{p,k}^{-1})^{\oplus m(k)})$$

is a normal form decomposition, i.e., the exponents $m(k)$ ar either 0 or 1 for each k. Our task is to show that the $n(k)'s$ and $m(k)'s$ are determined. Let $(G, \langle , \rangle)$ be the associated bilinear form to (G, q). Applying the functor $\rho_{p,k}$ (section II.2) to $(G, \langle , \rangle)$ gives a nondegenerate bilinear form on a homogeneous p-group of scale p, and by Lemma (II.2.7), this biliinear form is

$$\rho_{p,k}(G) = (\bar{w}_{p,1}^1)^{\oplus n(k)} \oplus (\bar{w}_{p,1}^{-1})^{\oplus m(k)}.$$

Let $r(k) = n(k) + m(k)$ be the rank of this form over $\mathbb{Z}/p$; the order of $\rho_{p,k}(G)$ is $\Delta = p^{r(k)}$. The discriminant of this form takes values in the

two-element set

$$\frac{1}{\Delta}\mathcal{D}(R/p) = \{p^{-r(k)}, p^{-r(k)}u\}$$

(where u is a non-square $\mod p$). From the computations given in Table (II.3.2),

$$disc(\rho_{p,k}(G)) = \begin{cases} p^{-r(k)} & \text{if } m(k) = 0 \\ p^{-r(k)}u & \text{if } m(k) = 1 \end{cases}$$

Therefore the discriminants of these associated bilinear forms determine $m(k)$; since the ranks $r(k)$ are also determined, the exponents $n(k)$ are invariants and the normal form is unique. Q.E.D.

Since the normal form is unique, and the construction of the normal form uses the relations of Lemma (2.1.2) only, it immediately follows that there are no other relations:

Corollary 2.5. *If p is odd, the relations listed in Lemma (2.1.2) among the generators of $\mathcal{T}_{\surd}$ (p odd) generate all the relations.*

We now deduce normal forms for decompositions of nondegenerate quadratic $\mathbb{Z}_p$-modules into rank one summands from the corresponding results for p-torsion quadratic forms. We use the discriminant-form construction, which provides a natural map $d : \mathcal{Q}_{\surd} \to \mathcal{T}_{\surd}$ assigning the isomorphism class of a quadratic $\mathbb{Z}_p$-module to that of its discriminant-form. Unfortunately, this map d fails to be an isomorphism, because of the existence of the unimodular forms $W^{\varepsilon}_{p,0}$. However, this is the only essential difference between the two monoids.

We begin by making the analogous definition of normal form for the quadratic $\mathbb{Z}_p$-modules.

Definition 2.6. If p is odd, a decomposition of a quadratic $\mathbb{Z}_p$-module (L, Q) is in *normal form* if

$$(L, Q) = \bigoplus_{k\geq 0}((W^1_{p,k})^{\oplus n(k)} \oplus (W^{-1}_{p,k})^{\oplus m(k)})$$

where $m(k) \leq 1$ for each k.

Proposition 2.7. *If p is odd, every quadratic $\mathbb{Z}_p$-module (L, Q) has a unique normal form decomposition.*

Proof. The same argument as was used in the proof of Lemma (2.3) shows that normal forms exist. To check the uniqueness, suppose that

$$(L, Q) = \bigoplus_{k\geq 0}((W^1_{p,k})^{\oplus n(k)} \oplus (W^{-1}_{p,k})^{\oplus m(k)})$$

(where $m(k) \leq 1$ for each k), is a normal form decomposition for a quadratic $\mathbb{Z}_p$-module (L, Q). Applying the discriminant-form functor d, we obtain the torsion form (G, q), and a normal form decomposition

$$(G, q) = \bigoplus_{k \geq 1} ((w_{p,k}^{1})^{\oplus n(k)} \oplus (w_{p,k}^{-1})^{\oplus m(k)})$$

and thus by the uniqueness of normal forms for the torsion forms, we have that the exponents $n(k)$ and $m(k)$ for $k \geq 1$ are all determined. It only remains to show that $n(0)$ and $m(0)$ are also determined. Their sum is determined by the rank of L, and so both are determined by either. Finally, the discriminant of L detects $m(0)$. Q.E.D.

A series of corollaries can now be immediately deduced.

COROLLARY 2.8. *If p is odd, the relations listed in Lemma (2.1.1) among the generators of $\mathcal{Q}_{\surd}$ generate all the relations.*

COROLLARY 2.9. *If p is odd, let $\mathcal{Q}_{\surd}^{(\infty)}$ be the sub-monoid of $\mathcal{Q}_{\surd}$ generated by the forms $W_{p,k}^{\varepsilon}$ with $k \geq 1$. Then the map $d : \mathcal{Q}_{\surd}^{(\infty)} \to \mathcal{T}_{\surd}$ is an isomorphism of monoids.*

PROOF. Let $\mathcal{F}$ be the free monoid on the generators $\{w_{p,k}^{\varepsilon}$ for $k \geq 1\}$ of $\mathcal{T}_{\surd}$, and define a map $e : \mathcal{F} \to \mathcal{Q}_{\surd}^{(\infty)}$ as follows: $e(w_{p,k}^{\varepsilon}) = W_{p,k}^{\varepsilon}$. Each relation among the generators of $\mathcal{T}_{\surd}$ maps under e to a valid relation among the generators of $\mathcal{Q}_{\surd}^{(\infty)}$; thus e descends to a map $\bar{e} : \mathcal{T}_{\surd} \to \mathcal{Q}_{\surd}^{(\infty)}$, which provides an inverse for d. Q.E.D.

COROLLARY 2.10. *Let p be an odd prime.*

(2.10.1) Given any torsion quadratic form (G, q) over $\mathbb{Z}_p$ there is a unique quadratic $\mathbb{Z}_p$-module $L(q)$ (up to isomorphism) such that $\operatorname{rank}(L(q)) = \ell(G)$ *and the discriminant-form of $L(q)$ is isomorphic to (G, q).*

(2.10.2) If L is any quadratic $\mathbb{Z}_p$-module whose discriminant-form is isomorphic to (G, q), then there is a unique unimodular quadratic $\mathbb{Z}_p$-module M such that $L \cong M \oplus L(q)$.

(2.10.3) $\operatorname{disc}(L(q)) \cdot \operatorname{disc}(q) = 1$.

PROOF. $L(q)$ is simply the pre-image in $\mathcal{Q}_{\surd}^{(\infty)}$ of (G, q): if we write q as a direct sum of $w_{p,k}^{\varepsilon}$'s, then $L(q)$ is isomorphic to the corresponding direct sum of $W_{p,k}^{\varepsilon}$'s. This proves the first statement, and the second follows easily from the uniqueness of the normal form.

The third statement requires some explanation, since the two discriminants lie in different groups. The discriminant of $L(q)$ lies in $\mathbb{Z}_p/(\mathbb{U}_1)^{\not\in} \cong \mathbb{N} \times \{\pm \not\in\}$, and every element can be represented as $p^n u$, for some unit u in $\mathbb{U}_1$. If G has order p^m, and scale $d_1 = p^s$, then its discriminant lies in $p^{-m}(\mathbb{Z}/p^s)^\times/((\mathbb{Z}/p^s)^\times)^2 \cong p^{-m}\{\pm 1\}$ and every element here can be thought of as $p^{-m}v$, for some unit $v \in (\mathbb{Z}/p^s)^\times$. The statement means that the p-parts of $\mathrm{disc}(L(q))$ and $\mathrm{disc}(q)$ cancel, as do the unit parts, both of which come from groups naturally identified with $\{\pm 1\}$.

The proof is now easy. Since both discriminants are multiplicative, it suffices to prove it for the rank one forms, in which case it is clear. Q.E.D.

COROLLARY 2.11. *If p is odd, a nondegenerate quadratic $\mathbb{Z}_p$-module is determined up to isomorphism by its rank, discriminant, and discriminant-form.*

PROOF. This follows from the argument given above in the proof of Proposition 2.7. Q.E.D.

A natural question now arises: for which possible ranks, discriminants, and discriminant-forms does a quadratic $\mathbb{Z}_p$-module exist? The answer when p is odd is not too difficult to arrive at; it is in fact a mild restatement of Corollary 2.10.

PROPOSITION 2.12. *Let p be an odd prime. Fix an integer r, an element $d \in \mathbb{Z}_p - \{0\}/\mathbb{U}_p^2$, and a finite p-torsion quadratic form (G, q). Then there exists a quadratic $\mathbb{Z}_p$-module L with $\mathrm{rank}(L) = r$, $\mathrm{disc}(L) = d$, and $(G_L, q_L) \cong (G, q)$ if and only if:*

(1) *$r \geq \ell(G)$,*
(2) *if $d = p^k u \mod \mathbb{U}_p^2$ with $u \in \mathbb{U}_p$, then $|G| = p^k$, and*
(3) *if $r = \ell(G)$ then $\chi(d) = \chi(\mathrm{disc}(q))$.*

Moreover, if so, then L is unique up to isomorphism.

PROOF. Clearly the first condition that $r \geq \ell(G)$ is necessary, as is the second. The third condition follows by Corollary II.8.7. To see that these conditions are sufficient, decompose (G, q) into normal form as

$$(G, q) = \bigoplus_{k \geq 1} ((w_{p,k}^1)^{\oplus n(k)} \oplus (w_{p,k}^{-1})^{\oplus m(k)}).$$

Set $\ell = \sum_{k \geq 1}(n(k) + m(k))$ which is the length of G. Then the quadratic $\mathbb{Z}_p$-module

$$(L, Q) = (W_{p,0}^1)^{r-\ell} \oplus \bigoplus_{k \geq 1} ((W_{p,k}^1)^{\oplus n(k)} \oplus (W_{p,k}^{-1})^{\oplus m(k)})$$

has the correct rank r and has discriminant-form (G, q). Moreover the power of p occurring in $\mathrm{disc}(L)$ is the order $|G|$ of the group G, and hence by the second condition the power of p in $\mathrm{disc}(L)$ is the same as the power of p in d. Therefore to finish we need only show that $\chi(\mathrm{disc}(L)) = \chi(d)$. If $r = \ell$, this is guaranteed by the third condition and Corollary II.8.7. If $r > \ell$ and this is not the case, simply replace one of the $W_{p,0}^1$ factors by a $W_{p,0}^{-1}$ factor, which does not spoil any of the other conditions.

This proves the existence of L, and the uniqueness statement is exactly Corollary 2.11. Q.E.D.

It is useful to express conditions (2) and (3) of the above Proposition by saying that $d \cdot \mathrm{disc}(q)$ is a unit, and is 1 if $r = \ell$, with the obvious abuses of notation being understood.

We close this section with a statement concerning the lifting of isometries.

THEOREM 2.13. *Let p be an odd prime, and let L_1 and L_2 be two nondegenerate quadratic $\mathbb{Z}_p$-modules such that* $\mathrm{rank}(L_1) = \mathrm{rank}(L_2)$ *and* $\mathrm{disc}(L_1) = \mathrm{disc}(L_2)$. *Suppose that $\sigma : G_{L_1} \to G_{L_2}$ is an isometry between the discriminant forms of L_1 and L_2. Then there exists an isometry $s : L_1 \to L_2$ inducing σ.*

PROOF. The assumptions imply, by Corollary (2.11), that L_1 and L_2 are isomorphic. Decompose G_{L_1} into an (internal) orthogonal direct sum of cyclic torsion forms $w_{p,k}^{\epsilon}$; denote this by

$$G_{L_1} = \oplus_i w_i^{(1)}.$$

Now transport this decomposition to G_{L_2} via the isomorphism σ, and denote this by

$$G_{L_2} = \oplus_i w_i^{(2)}.$$

Since σ is an isometry, $w_i^{(1)} \cong w_i^{(2)}$ for each i. Now by Proposition (II.11.6), both L_1 and L_2 can be decomposed compatibly with their discriminant-forms. Specifically, we have direct sum decompositions

$$L_1 = M_1 \oplus \bigoplus_i W_i^{(1)} \text{ and } L_2 = M_2 \oplus \bigoplus_i W_i^{(2)}$$

with M_1 and M_2 unimodular, $W_i^{(1)}$ and $W_i^{(2)}$ rank one for each i, and the natural inclusions inducing the obvious correspondence of discriminant-forms.

Note that by the classification of rank one forms, since $w_i^{(1)} \cong w_i^{(2)}$ for each i, the same is true for the W's: $W_i^{(1)} \cong W_i^{(2)}$ for each i. Therefore M_1 and M_2 are isomorphic, since they have the same rank

and discriminant. Therefore the pieces of the decompositions of L_1 and L_2 match up perfectly, and this allows us to define an isometry $s' : L_1 \to L_2$ by identifying the pieces.

The isometry s' induces an isometry $\sigma' : G_{L_1} \to G_{L_2}$, which preserves the decompositions. Therefore σ' and σ differ only by automorphisms of the pieces: i.e., there is an automorphism τ of G_{L_1} which preserves the decomposition, such that $\sigma = \sigma' \circ \tau$. By Proposition (1.3), the automorphism τ lifts to an automorphism t of L_1, and the desired isometry from L_1 to L_2 is then $s = s' \circ t$. Q.E.D.

Applying the above with $L_1 = L_2$ gives the following:

COROLLARY 2.14. *If p is odd, and L is a nondegenerate quadratic $\mathbb{Z}_p$-module, then the natural map $\mathcal{O}(\mathcal{L}) \to \mathcal{O}(\mathcal{G}_\mathcal{L})$ is surjective.*

3. Relations for Quadratic Forms over $\mathbb{Z}_2$

The relations which hold among the generators $W_{2,k}^{\varepsilon}$, U_k, and V_k of the monoid $\mathcal{Q}_\in$ of isomorphism classes of nondegenerate quadratic $\mathbb{Z}_2$-modules (as well as the relations in the torsion cases $\mathcal{T}_\in$ and $\mathcal{G}_\in$) are rather complicated. We begin with the quadratic $\mathbb{Z}_2$-modules.

PROPOSITION 3.1. *The following relations hold among quadratic $\mathbb{Z}_2$-modules.*

(I) *For $k \geq 1$,*

$$W_{2,k}^{\varepsilon_1} \oplus W_{2,k}^{\varepsilon_2} \cong W_{2,k}^{5\varepsilon_1} \oplus W_{2,k}^{5\varepsilon_2}$$

(II) *Let $\underline{\varepsilon} = (\varepsilon_1, \varepsilon_2, \varepsilon_3)$, $s_1(\underline{\varepsilon}) = \varepsilon_1 + \varepsilon_2 + \varepsilon_3$, and $s_2(\underline{\varepsilon}) = \varepsilon_1\varepsilon_2 + \varepsilon_2\varepsilon_3 + \varepsilon_3\varepsilon_1$. Then if $s_2(\underline{\varepsilon}) \equiv 3$, we have for $k \geq 1$*

$$W_{2,k}^{\varepsilon_1} \oplus W_{2,k}^{\varepsilon_2} \oplus W_{2,k}^{\varepsilon_3} \cong W_{2,k}^{s_1(\underline{\varepsilon})} \oplus V_k$$

while if $s_2(\underline{\varepsilon}) \equiv 7$, we have for $k \geq 1$

$$W_{2,k}^{\varepsilon_1} \oplus W_{2,k}^{\varepsilon_2} \oplus W_{2,k}^{\varepsilon_3} \cong W_{2,k}^{s_1(\underline{\varepsilon})} \oplus U_k.$$

(III) *For $k \geq 0$,*

$$U_k^{\oplus 2} \cong V_k^{\oplus 2}.$$

(IV) *For $k \geq 1$,*

$$W_{2,k}^{\varepsilon} \oplus U_k \cong (W_{2,k}^{\varepsilon})^{\oplus 2} \oplus W_{2,k}^{-\varepsilon}$$

and

$$W_{2,k}^{\varepsilon} \oplus V_k \cong (W_{2,k}^{3\varepsilon})^{\oplus 3}.$$

(V) *If $\varepsilon_1 \equiv \varepsilon_2 \mod 4$, then for $k \geq 1$,*

$$U_k \oplus W_{2,k}^{\varepsilon_1} \oplus W_{2,k}^{\varepsilon_2} \cong V_k \oplus W_{2,k}^{\varepsilon_1 - 2} \oplus W_{2,k}^{\varepsilon_2 + 2}.$$

(VI) *For $k \geq 2$,*

$$W_{2,k-1}^{\varepsilon_1} \oplus W_{2,k}^{\varepsilon_2} \cong W_{2,k-1}^{\varepsilon_1+2\varepsilon_2} \oplus W_{2,k}^{\varepsilon_2+2\varepsilon_1}.$$

(VII) *For $k \geq 2$,*

$$W_{2,k-1}^{\varepsilon} \oplus U_k \cong W_{2,k-1}^{5\varepsilon} \oplus V_k.$$

(VIII) *For $k \geq 1$,*

$$U_{k-1} \oplus W_{2,k}^{\varepsilon} \cong V_{k-1} \oplus W_{2,k}^{5\varepsilon}.$$

(IX) *If $\varepsilon_1 \equiv \varepsilon_2 \mod 4$, then for $k \geq 2$,*

$$W_{2,k-1}^{\varepsilon_1} \oplus W_{2,k-1}^{\varepsilon_2} \oplus W_{2,k}^{1} \cong W_{2,k-1}^{\varepsilon_1-2} \oplus W_{2,k-1}^{\varepsilon_2+2} \oplus W_{2,k}^{5}.$$

(X) *For $k \geq 3$,*

$$W_{2,k-2}^{\varepsilon_1} \oplus W_{2,k}^{\varepsilon_2} \cong W_{2,k-2}^{5\varepsilon_1} \oplus W_{2,k}^{5\varepsilon_2}.$$

It is worth remarking at the outset that the relations (II) and (IV) are completely equivalent (each set of relations amounts to reading the other set backwards, possibly using the relations (I)). We should also remark that the relations listed here generate all relations among the generators of $\mathcal{Q}_{\in}$, as will be proved in Section 5.

Proof. The verification of these relations is a long computation of which we will not present every detail. The proof will be given by assuming that the form presented on the left side of each relation is a sum of the standard forms on $\mathbb{Z}_p^N$ given by the formulas of Table (I.7.1), in the standard basis; our job will be to find a new basis which exhibits the decomposition on the right side of the relation.

We abuse notation and view the quantities ε for the rank one forms as being defined mod 8 when appearing in the exponents of the rank one form notation, but as being the corresponding units 1, 3, 5, or 7 in $\mathbb{Z}_2$ when appearing in other formulas. We repeatedly use the recognition criteria given in Lemmas (1.5) and (1.6).

Let us present relation (I) in detail. Let $W_{2,k}^{\varepsilon_1} \oplus W_{2,k}^{\varepsilon_2}$ have the standard basis, so that the quadratic form is given by $Q(r,s) = 2^{k-1}(\varepsilon_1 r^2 + \varepsilon_2 s^2)$. Let $u = (1,2)$ and $v = (2\varepsilon_2, -\varepsilon_1)$. The pair $\{u, v\}$ is also a basis for $\mathbb{Z}_2^2$, and in this basis we have

$$\begin{aligned} Q(ru+sv) &= Q(r(1,2) + s(2\varepsilon_2, -\varepsilon_1)) = Q(r + 2\varepsilon_2 s, 2r - \varepsilon_1 s) \\ &= 2^{k-1}(\varepsilon_1(r+2\varepsilon_2 s)^2 + \varepsilon_2(2r - \varepsilon_1 s)^2) \\ &= 2^{k-1}((\varepsilon_1 + 4\varepsilon_2)r^2 + (4\varepsilon_1\varepsilon_2^2 + \varepsilon_2\varepsilon_1^2)s^2). \end{aligned}$$

Since $\varepsilon_1 + 4\varepsilon_2 \equiv 5\varepsilon_1 \mod 8$ and $4\varepsilon_1\varepsilon_2^2 + \varepsilon_2\varepsilon_1^2 \equiv 5\varepsilon_2 \mod 8$, this basis realizes the decomposition $W_{2,k}^{5\varepsilon_1} \oplus W_{2,k}^{5\varepsilon_2}$.

For relation (II), it is useful to remark that if we write $s_3(\underline{\varepsilon}) = \varepsilon_1\varepsilon_2\varepsilon_3$, then the identity $s_1(\underline{\varepsilon})s_3(\underline{\varepsilon}) = s_2(\underline{\varepsilon})$ holds, as a check of the various cases verifies immediately. Assume that $Q(r,s,t) = 2^{k-1}(\varepsilon_1 r^2 + \varepsilon_2 s^2 + \varepsilon_3 t^2)$, and let $x = (1,1,1), y = (\varepsilon_2, -\varepsilon_1, 0)$ and $z = (\varepsilon_3, 0, -\varepsilon_1)$. Then $\{x,y,z\}$ is a new basis for $\mathbb{Z}_2^3$, and y and z are orthogonal to x. Since $Q(rx) = 2^{k-1}s_1(\underline{\varepsilon})r^2$, the span of x represents the form $W_{2,k}^{s_1(\underline{\varepsilon})}$. Now $Q(ry+sz) = Q(r\varepsilon_2 + s\varepsilon_3, -r\varepsilon_1, -s\varepsilon_1) = 2^{k-1}(\varepsilon_1(r\varepsilon_2 + s\varepsilon_3)^2 + \varepsilon_2(-r\varepsilon_1)^2 + \varepsilon_3(-s\varepsilon_1)^2) = 2^{k-1}((\varepsilon_1\varepsilon_2^2 + \varepsilon_2\varepsilon_1^2)r^2 + (2\varepsilon_1\varepsilon_2\varepsilon_3)rs + (\varepsilon_1\varepsilon_3^2 + \varepsilon_3\varepsilon_1^2)s^2)$. Note that the coefficients of r^2 and s^2 are even, so this can be written as $Q(ry+sz) = 2^k((\frac{\varepsilon_1\varepsilon_2^2+\varepsilon_2\varepsilon_1^2}{2})r^2 + (\varepsilon_1\varepsilon_2\varepsilon_3)rs + (\frac{\varepsilon_1\varepsilon_3^2+\varepsilon_3\varepsilon_1^2}{2})s^2)$. The middle coefficient is odd, so by Lemma (1.6), the span of $\{y,z\}$ is indecomposable, and we detect which form it is by the parity of $(\frac{\varepsilon_1\varepsilon_2^2+\varepsilon_2\varepsilon_1^2}{2})(\frac{\varepsilon_1\varepsilon_3^2+\varepsilon_3\varepsilon_1^2}{2})$. This quantity is exactly $(s_3^2+\varepsilon_1^2 s_1 s_3)/4$; using the identity mentioned above, this is equal to $(s_3^2+\varepsilon_1^2 s_2)/4$, and clearly its parity is determined by the value of $s_3^2 + \varepsilon_1^2 s_2 \mod 8$. Since squares are all $1 \mod 8$, this equals $1 + s_2 \mod 8$; hence the parity is even if $s_2 \equiv 7 \mod 8$ and is odd if $s_2 \equiv 3 \mod 8$. This proves relation (II).

For relation (III), write $Q(r,s,t,u) = 2^k(rs+tu)$, representing the form $U_k^{\oplus 2}$. Let $x = (1,1,0,0)$, $y = (0,1,1,1)$, $z = (1,-1,-1,0)$, and $w = (1,-1,0,-1)$. The set $\{x,y,z,w\}$ is a basis for $\mathbb{Z}_2^4$, and both z and w are orthogonal to both x and y, giving an alternate splitting of the form Q. On the span of $\{x,y\}$, Q has the form $Q(rx+sy) = Q(r, r+s, s, s) = 2^k(r^2+rs+s^2)$, which is exactly the form V_k. On the span of $\{z,w\}$, Q has the form $Q(rz+sw) = Q(r+s, -r-s, -r, -s) = 2^k((r+s)(-r-s)+rs) = 2^k(-r^2-rs-s^2)$, which also represents V_k.

As mentioned above, relation (IV) is simply (II) read backwards, so we will move on to relation (V). Write $Q(r,s,t,u) = 2^k(rs) + 2^{k-1}(\varepsilon_1 t^2 + \varepsilon_2 u^2)$. Let $x = (1,1,0,0)$, $y = (0,1,1,1)$, $z = (-\varepsilon_1, \varepsilon_1, 1, 0)$, and $w = (-\varepsilon_2, \varepsilon_2, 0, 1)$. Again the set $\{x,y,z,w\}$ is a basis for $\mathbb{Z}_2^4$, and both z and w are orthogonal to both x and y, giving an alternate splitting of the form Q. On the span of $\{x,y\}$, Q has the form $Q(rx+sy) = Q(r, r+s, s, s) = 2^k(r^2 + rs + (\frac{\varepsilon_1+\varepsilon_2}{2})s^2)$. Under the assumption that $\varepsilon_1 \equiv \varepsilon_2 \mod 4$, the quantity $\varepsilon_1 + \varepsilon_2$ is always congruent to 2 mod 4, hence the coefficient of s^2 in the above is odd; by Lemma (1.6), this represents the form V_k. On the span of $\{z,w\}$, Q has the form $Q(rz+sw) = Q(-\varepsilon_1 r - \varepsilon_2 s, \varepsilon_1 r + \varepsilon_2 s, r, s) = 2^{k-1}((-2\varepsilon_1^2 + \varepsilon_1)r^2 - (4\varepsilon_1\varepsilon_2)rs + (-2\varepsilon_2^2 + \varepsilon_2)s^2)$, which we see decomposes by Lemma (1.5). Using the notation of that Lemma, we have $a = -2\varepsilon_1^2 + \varepsilon_1$, $b = -4\varepsilon_1\varepsilon_2$, and $c = -2\varepsilon_2^2 + \varepsilon_2$; hence $d = \bar{d} = \varepsilon_1\varepsilon_2(1 - 2\varepsilon_1 - 2\varepsilon_2)$. Note that a is odd, and $a \equiv \varepsilon_1 - 2 \mod 8$. Since $\varepsilon_1 + \varepsilon_2$ is congruent to 2 mod 4, $1 - 2\varepsilon_1 - 2\varepsilon_2 \equiv 5 \mod 8$, and $a\bar{d} \equiv 5\varepsilon_2 - 2\varepsilon_1\varepsilon_2 \mod 8$. Since

$\varepsilon_1 \equiv \varepsilon_2 \mod 4$, $\varepsilon_1\varepsilon_2 \equiv 1 \mod 4$; hence $a\bar{d} \equiv 5\varepsilon_2 - 2 \mod 8$. Since $5\varepsilon - 2 \equiv \varepsilon + 2 \mod 8$ for any ε, the result follows from Lemma (1.5.1).

Relation (VI) is a bit easier. Represent the form by $Q(r,s) = 2^{k-2}\varepsilon_1 r^2 + 2^{k-1}\varepsilon_2 s^2$. Let $x = (1,1)$ and $y = (-2\varepsilon_2, \varepsilon_1)$; x and y form a new basis for $\mathbb{Z}_2^2$, and in this basis Q has the form $Q(rx+sy) = Q(r-2\varepsilon_2 s, r+\varepsilon_1 s) = 2^{k-2}\varepsilon_1(r-2\varepsilon_2 s)^2 + 2^{k-1}\varepsilon_2(r+\varepsilon_1 s)^2) = 2^{k-2}(\varepsilon_1 + 2\varepsilon_2)r^2 + 2^{k-1}(\varepsilon_2\varepsilon_1^2 + 2\varepsilon_1\varepsilon_2^2)s^2$; since $\varepsilon_2\varepsilon_1^2 + 2\varepsilon_1\varepsilon_2^2 \equiv \varepsilon_2 + 2\varepsilon_1 \mod 8$, the result follows.

For relation (VII), represent the form by $Q(r,s,t) = 2^{k-2}\varepsilon r^2 + 2^k st$. Let $x = (1,1,1)$, $y = (-2,\varepsilon,0)$, and $z = (-2,0,\varepsilon)$; they form a new basis for $\mathbb{Z}_2^3$, and both y and z are orthogonal to x. Since $Q(rx) = Q(r,r,r) = 2^{k-2}(\varepsilon+4)r^2$, and since for any ε, $\varepsilon + 4 \equiv 5\varepsilon \mod 8$, the span of x represents $W_{2,k-1}^{5\varepsilon}$. On the span of $\{y,z\}$, Q has the form $Q(ry+sz) = Q(-2r-2s, \varepsilon r, \varepsilon s) = 2^{k-2}\varepsilon(-2r-2s)^2 + 2^k\varepsilon^2 rs = 2^k(\varepsilon r^2 + (2\varepsilon+\varepsilon^2)rs + \varepsilon s^2)$, which by Lemma (1.6) represents V_k.

Relation (VIII) is similar; represent the form by $Q(r,s,t) = 2^{k-1}(rs + \varepsilon t^2)$. Let $x = (2,2,1)$, $y = (\varepsilon, 0, -1)$, and $z = (0,\varepsilon,-1)$; they form a new basis for $\mathbb{Z}_2^3$, and both y and z are orthogonal to x. Since $Q(rx) = Q(2r,2r,r) = 2^{k-1}(\varepsilon+4)r^2$, the span of x represents $W_{2,k}^{5\varepsilon}$. On the span of $\{y,z\}$, Q has the form $Q(ry+sz) = Q(\varepsilon r, \varepsilon s, -r-s) = 2^{k-1}(\varepsilon^2 rs + \varepsilon(-r-s)^2) = 2^{k-1}(\varepsilon r^2 + (2\varepsilon+\varepsilon^2)rs + \varepsilon s^2)$, which by Lemma (1.6) represents V_{k-1}.

For relation (IX), represent the form by $Q(r,s,t) = 2^{k-2}\varepsilon_1 r^2 + 2^{k-2}\varepsilon_2 s^2 + 2^{k-1}t^2$. Let $x = (1,0,1)$, $y = (-2,0,\varepsilon_1)$, and $z = (0,1,0)$; they form a new basis for $\mathbb{Z}_2^3$, and are pairwise orthogonal. Since $Q(rx) = Q(r,0,r) = 2^{k-2}(\varepsilon_1+2)r^2$, the span of x represents $W_{2,k-1}^{\varepsilon_1+2}$. Since $Q(ry) = 2^k\varepsilon_1 r^2 + 2^{k-1}\varepsilon_1^2 r^2 = 2^{k-1}(\varepsilon_1^2 + 2\varepsilon_1)r^2$, the span of y represents the form $W_{2,k}^{1+2\varepsilon_1}$. Clearly the span of z represents the form $W_{2,k-1}^{\varepsilon_2}$. Now use relation (VI), which tells us that the span of $\{y,z\}$ is isomorphic to $W_{2,k}^{1+2\varepsilon_1+2\varepsilon_2} \oplus W_{2,k-1}^{\varepsilon_2+2+4\varepsilon_1}$. Since $\varepsilon_1 \equiv \varepsilon_2 \mod 4$, $1+2\varepsilon_1+2\varepsilon_2 \equiv 5 \mod 8$, and $\varepsilon_2 + 2 + 4\varepsilon_1 \equiv \varepsilon_2 - 2$. This proves the required decomposition.

Finally, represent the form for relation (X) by $Q(r,s) = 2^{k-3}\varepsilon_1 r^2 + 2^{k-1}\varepsilon_2 s^2$. Let $x = (1,1)$ and $y = (-4\varepsilon_2, \varepsilon_1)$; they form a new basis for $\mathbb{Z}_2^2$, and are pairwise orthogonal. Since $Q(rx+sy) = Q(r - 4\varepsilon_2 s, r+\varepsilon_1 s) = 2^{k-3}\varepsilon_1(r-4\varepsilon_2 s)^2 + 2^{k-1}\varepsilon_2(r+\varepsilon_1 s)^2 = 2^{k-3}(\varepsilon_1 + 4\varepsilon_2)r^2 + 2^{k-1}(\varepsilon_2\varepsilon_1^2 + 4\varepsilon_1\varepsilon_2^2)s^2$, and $\varepsilon_1 + 4\varepsilon_2 \equiv 5\varepsilon_1 \mod 8$, and $\varepsilon_2\varepsilon_1^2 + 4\varepsilon_1\varepsilon_2^2 \equiv 5\varepsilon_2 \mod 8$, the result follows. Q.E.D.

We remark that if we want to consider the bilinear forms $W_{2,0}^{\varepsilon}$, which are not quadratic $\mathbb{Z}_2$-modules but are inner product modules over $\mathbb{Z}_2$, then all of the same relations as stated in Proposition 3.1 hold, when

they make sense. Thus for example relations (I), (II), (IV), (V), and (VIII) hold for $k \geq 0$; relations (VI), (VII), and (X) hold for $k \geq 1$; and relation (X) holds for $k \geq 2$.

From the relations in Proposition (3.1), we immediately derive the corresponding relations on discriminant forms. This gives us a large set of relations among torsion quadratic $\mathbb{Z}_2$-modules. Recall also that we know one further relation for torsion quadratic forms: by Lemma (1.1.2), $w_{2,1}^1 \cong w_{2,1}^5$ and $w_{2,1}^3 \cong w_{2,1}^7$. (This also follows from considering the discriminant forms in relation (VIII) with k = 1.) Thus we have proved:

PROPOSITION 3.2. *The following relations hold among torsion quadratic forms over* $\mathbb{Z}_2$.

(0)
$$w_{2,1}^1 \cong w_{2,1}^5 \text{ and } w_{2,1}^3 \cong w_{2,1}^7.$$

(I) *For* $k \geq 1$,
$$w_{2,k}^{\varepsilon_1} \oplus w_{2,k}^{\varepsilon_2} \cong w_{2,k}^{5\varepsilon_1} \oplus w_{2,k}^{5\varepsilon_2}.$$

(II) *Let* $\underline{\varepsilon} = (\varepsilon_1, \varepsilon_2, \varepsilon_3)$, $s_1(\underline{\varepsilon}) = \varepsilon_1 + \varepsilon_2 + \varepsilon_3$, *and* $s_2(\underline{\varepsilon}) = \varepsilon_1\varepsilon_2 + \varepsilon_2\varepsilon_3 + \varepsilon_3\varepsilon_1$. *Then if* $s_2(\underline{\varepsilon}) \equiv 3$, *we have for* $k \geq 1$
$$w_{2,k}^{\varepsilon_1} \oplus w_{2,k}^{\varepsilon_2} \oplus w_{2,k}^{\varepsilon_3} \cong w_{2,k}^{s_1(\underline{\varepsilon})} \oplus v_k$$
while if $s_2(\underline{\varepsilon}) \equiv 7$, *we have for* $k \geq 1$
$$w_{2,k}^{\varepsilon_1} \oplus w_{2,k}^{\varepsilon_2} \oplus w_{2,k}^{\varepsilon_3} \cong w_{2,k}^{s_1(\underline{\varepsilon})} \oplus u_k.$$

(III) *For* $k \geq 1$,
$$u_k^{\oplus 2} \cong v_k^{\oplus 2}.$$

(IV) *For* $k \geq 1$,
$$w_{2,k}^{\varepsilon} \oplus u_k \cong (w_{2,k}^{\varepsilon})^{\oplus 2} \oplus w_{2,k}^{-\varepsilon}$$
and
$$w_{2,k}^{\varepsilon} \oplus v_k \cong (w_{2,k}^{3\varepsilon})^{\oplus 3}.$$

(V) *If* $\varepsilon_1 \equiv \varepsilon_2 \mod 4$, *then for* $k \geq 1$,
$$v_k \oplus w_{2,k}^{\varepsilon_1} \oplus w_{2,k}^{\varepsilon_2} \cong u_k \oplus w_{2,k}^{\varepsilon_1 - 2} \oplus w_{2,k}^{\varepsilon_2 + 2}.$$

(VI) *For* $k \geq 2$,
$$w_{2,k-1}^{\varepsilon_1} \oplus w_{2,k}^{\varepsilon_2} \cong w_{2,k-1}^{\varepsilon_1 + 2\varepsilon_2} \oplus w_{2,k}^{\varepsilon_2 + 2\varepsilon_1}.$$

(VII) *For* $k \geq 2$,
$$w_{2,k-1}^{\varepsilon} \oplus v_k \cong w_{2,k-1}^{5\varepsilon} \oplus u_k.$$

(VIII) *For* $k \geq 2$,

$$v_{k-1} \oplus w_{2,k}^{\varepsilon} \cong u_{k-1} \oplus w_{2,k}^{5\varepsilon}.$$

(IX) *If* $\varepsilon_1 \equiv \varepsilon_2 \mod 4$, *then for* $k \geq 2$,

$$w_{2,k-1}^{\varepsilon_1} \oplus w_{2,k-1}^{\varepsilon_2} \oplus w_{2,k}^{5} \cong w_{2,k-1}^{\varepsilon_1-2} \oplus w_{2,k-1}^{\varepsilon_2+2} \oplus w_{2,k}^{1}.$$

(X) *For* $k \geq 3$,

$$w_{2,k-2}^{\varepsilon_1} \oplus w_{2,k}^{\varepsilon_2} \cong w_{2,k-2}^{5\varepsilon_1} \oplus w_{2,k}^{5\varepsilon_2}.$$

We will see in Section 4 that the relations listed here generate all relations among the generators of the monoid $\mathcal{T}_{\in}$ of isomorphism classes of nondegenerate 2-torsion quadratic forms.

4. Normal forms for 2-torsion quadratic forms

In this section, we will establish several normal forms for decompositions of nondegenerate quadratic forms on 2-groups into rank one and two summands. We will often refer to the relations given in Proposition (3.2) during the discussion. In addition, the signature invariants σ_ℓ introduced in Section III.3 play a crucial role. We begin with a rather crude normal form.

Definition 4.1. A decomposition of a quadratic form (G, q) on a finite abelian 2-group is in *partial normal form* if

$$(G, q) = \bigoplus_{k \geq 1} (u_k^{\oplus n(k)} \oplus v_k^{\oplus m(k)} \oplus w(k))$$

where $m(k) \leq 1$, $\operatorname{rank}(w(k)) \leq 2$, and $w(k)$ is a sum of forms of type $w_{2,k}^{\varepsilon}$.

Given a partial normal form decomposition, we define

$$G(k) := u_k^{\oplus n(k)} \oplus v_k^{\oplus m(k)} \oplus w(k),$$

and

$$x(k) := v_k^{\oplus m(k)} \oplus w(k).$$

Lemma 4.2. *Every nondegenerate quadratic form* (G, q) *on a finite abelian 2-group has a partial normal form decomposition. Moreover, the quantities* $n(k) + m(k)$ *and* $\operatorname{rank}(w(k))$ *are invariants of the form* (G, q).

Proof. Using relation (II), we can easily guarantee that each homogeneous piece of the decomposition contains at most 2 terms of type $w_{2,k}^{\varepsilon}$. Then using relation (III), we can guarantee that each homogeneous piece contains at most one v_k term. This is exactly the partial normal form.

Group A	Group B	σ_{k-1}	$disc_8(A)$	$disc_8(B)$
0	-	1	1	-
-	v_k	-1	-	3
$w^1_{2,k}$	$w^5_{2,k}$	$e^{\pi i/4}$	1	5
$v_k \oplus w^3_{2,k}$	$v_k \oplus w^7_{2,k}$	$e^{3\pi i/4}$	1	5
$v_k \oplus w^5_{2,k}$	$v_k \oplus w^1_{2,k}$	$e^{5\pi i/4}$	7	3
$w^7_{2,k}$	$w^3_{2,k}$	$e^{7\pi i/4}$	7	3
$w^1_{2,k} \oplus w^1_{2,k}$	$w^1_{2,k} \oplus w^5_{2,k}$	i	1	5
$v_k \oplus w^1_{2,k} \oplus w^3_{2,k}$	$v_k \oplus w^1_{2,k} \oplus w^7_{2,k}$	-1	1	5
$w^7_{2,k} \oplus w^7_{2,k}$	$w^3_{2,k} \oplus w^7_{2,k}$	$-i$	1	5
$w^1_{2,k} \oplus w^7_{2,k}$	$w^1_{2,k} \oplus w^3_{2,k}$	1	7	3

TABLE 4.1. Homogeneous normal forms

To see that $n(k) + m(k)$ and $\text{rank}(w(k))$ are invariants, note first that their sum $n(k) + m(k) + \text{rank}(w(k))$ is simply the $\mathbb{Z}/2$-rank of the module $\rho_k(G)$, defined in Section II.2. Hence the sum depends only on (G, q), and so either one determines both. Consulting Table (III.3.1), we see that $w(k) = 0$ if and only if $\sigma_k \neq 0$. In this case, $n(k)+m(k) = r_k/2$. Otherwise, $\text{rank}(w(k)) = 1$ or 2 depending on the parity of r_k, and $n(k) + m(k) = (r_k - \text{rank}(w(k)))/2$. Q.E.D.

This partial normal form is just a setup for the actual normal form to be described below. We next find a true normal form for each homogeneous piece.

DEFINITION 4.3. A decomposition of a quadratic form on a homogeneous abelian 2-group is in *homogeneous normal form* if it is in partial normal form, if $x(k)$ is one of the possibilities appearing in Table (4.1), and if in case $k = 1$ $x(k)$ belongs to "group A" in the table.

Before proving that this homogeneous normal form can actually be achieved, we want to point out some of the properties of Table (4.1). The value of the $(k-1)^{\text{st}}$ signature invariant σ_{k-1} has been recorded in the table, as well as the mod 8 discriminant values (which are defined if $k \geq 2$ in all cases, and for u_1 and v_1).

LEMMA 4.4.

(4.4.1) Let $x(k)$ be one of the entries in Table (4.1) such that either $k \geq 2$ or $w(k) = 0$, and let $\delta = \text{disc}_8(x(k))$. Then $\left(\frac{2}{\delta}\right) = -1$ if and only if $x(k)$ lies in group B. In particular, for $x(k)$ in group A, $\sigma_\ell(x(k)) = \sigma_{k-1}(x(k))$ for all $0 \leq \ell < k$, while for

$x(k)$ in group B, $\sigma_\ell(x(k)) = (-1)^\ell \sigma_{k-1}(x(k))$ for all $0 \le \ell < k$. (See Proposition (III.4.4)).

(4.4.2) For each $x(k)$ in group B other than $x(k) = v_k$, if we replace exactly one of the $w_{2,k}^{\varepsilon}$ summands with $w_{2,k}^{5\varepsilon}$, we get (a form isomorphic to) the entry in group A of the table in the same row.

(4.4.3) If (G, q) is in homogeneous normal form (with G homogeneous of scale 2^k) and if we know
(a) *whether $\sigma_k = 0$,*
(b) *whether $x(k)$ belongs to group A or group B, and*
(c) *the value of σ_ℓ for some ℓ with $0 \le \ell < k$,*
then we know $x(k)$. If in addition we know r_k, then we know (G, q).

PROOF. Statement (4.4.1) is clear from Table (4.1), using Proposition (III.4.4)), and (4.4.2) is a straightforward verification (occasionally using relation (I)). To prove (4.4.3), note first that (G, q) and $x(k)$ have the same signature invariants, since all signature invariants of u_k are 1. Next note that whether $\operatorname{rank}(w(k))$ is zero or not is determined by (a), and that if the rank is zero, then $x(k)$ is either 0 or v_k, and so is determined by (b). If $\operatorname{rank}(w(k)) \ge 1$, then (b) and (c) determine the value of $\sigma_{k-1}(x(k))$, by the formula in part (4.4.1). Now for each value of this signature invariant σ_{k-1}, there is exactly one possibility for $x(k)$ in group A, and one possibility in group B. Q.E.D.

It remains to show that we actually have a normal form.

PROPOSITION 4.5. *Every quadratic form (G, q) on a homogeneous 2-group has a decomposition in homogeneous normal form, and the terms appearing in the decomposition are uniquely determined by (G, q).*

PROOF. We first show that a homogeneous normal form decomposition exists. By Lemma (4.2), we can find a decomposition in partial normal form. For each such decomposition with $\operatorname{rank}(w(k)) \le 1$, the corresponding $x(k)$ occurs in Table (4.1), so in those cases we are already in homogeneous normal form. When $\operatorname{rank}(w(k)) = 2$, there are 4 *a priori* possibilities for $w(k)$ which do not appear in Table (4.1):

$$w_{2,k}^3 \oplus w_{2,k}^3, w_{2,k}^3 \oplus w_{2,k}^5, w_{2,k}^5 \oplus w_{2,k}^5, \text{ and } w_{2,k}^5 \oplus w_{2,k}^7.$$

But by using relation (I), these are isomorphic to (respectively)

$$w_{2,k}^7 \oplus w_{2,k}^7, w_{2,k}^1 \oplus w_{2,k}^7, w_{2,k}^1 \oplus w_{2,k}^1, \text{ and } w_{2,k}^1 \oplus w_{2,k}^3.$$

Furthermore, among the 6 remaining rank 2 choices for $w(k)$, 4 out of the 12 *a priori* possibilities for $x(k)$ do not appear in the table:

$$v_k \oplus w^1_{2,k} \oplus w^1_{2,k}, v_k \oplus w^1_{2,k} \oplus w^5_{2,k}, v_k \oplus w^3_{2,k} \oplus w^7_{2,k}, \text{ and } v_k \oplus w^7_{2,k} \oplus w^7_{2,k}.$$

But by using relation (V), these are isomorphic to (respectively)

$$u_k \oplus w^3_{2,k} \oplus w^7_{2,k}, u_k \oplus w^7_{2,k} \oplus w^7_{2,k}, u_k \oplus w^1_{2,k} \oplus w^1_{2,k}, \text{ and } u_k \oplus w^1_{2,k} \oplus w^5_{2,k}.$$

Therefore these forms can be transformed into the forms with the u_k summands, and then the u_k term is absorbed into the other part of the normal form; hence the associated $x(k)$ terms can be made into (respectively)

$$w^3_{2,k} \oplus w^7_{2,k}, w^7_{2,k} \oplus w^7_{2,k}, w^1_{2,k} \oplus w^1_{2,k}, \text{ and } w^1_{2,k} \oplus w^5_{2,k},$$

which do appear in the table.

Finally, since $w^{\varepsilon}_{2,1} \cong w^{5\varepsilon}_{2,1}$ (relation (0)), by Lemma (4.4.2) we may ensure that $x(1)$ lies in group A. (For later convenience, we should point out that this is the only place in this section where relation (0) is used.)

We now turn to the uniqueness of the terms appearing in the homogeneous normal form. If $k = 1$, then $x(1)$ lies in group A by assumption, and so according to Lemma (4.4.3) it is determined by σ_0 and σ_1. If $k > 1$, then the invariants σ_{k-1} and σ_{k-2} are both defined and nonzero. By Lemma (4.4.1), the ratio $\sigma_{k-1}/\sigma_{k-2}$ determines the group to which $x(k)$ belongs (it is group A when the ratio is 1, and group B when the ratio is -1). Now the values of σ_k and σ_{k-1} will determine $x(k)$ (again by Lemma (4.4.3)). Therefore in all cases $x(k)$ is determined; since the remaining term $u_k^{n(k)}$ is determined by the rank, the homogeneous normal form is unique. Q.E.D.

Note that up to this point we have used only relations (0)-(V).

We come finally to the task of finding a normal form decomposition for an arbitrary quadratic form on a finite abelian 2-group, using the remaining relations (VI) - (X). Our strategy is to first attempt to limit the summands to u_k, $w^1_{2,k}$, and $w^5_{2,k}$, and then to attempt to make $x(k)$ belong to group A (and so have a discriminant δ with $\left(\frac{2}{\delta}\right) = 1$).

Definition 4.6. A decomposition

$$(G, q) = \bigoplus_{k \geq 1} (u_k^{\oplus n(k)} \oplus v_k^{\oplus m(k)} \oplus w(k))$$

with $x(k) = v_k^{\oplus m(k)} \oplus w(k)$ is in *normal form* provided that all of the following hold.

(a) Each homogeneous piece $G(k) = u_k^{\oplus n(k)} \oplus v_k^{\oplus m(k)} \oplus w(k)$ is in homogeneous normal form,
(b) If $w(k-1) \neq 0$ then $x(k) \in \{0, w_{2,k}^1, w_{2,k}^5, w_{2,k}^1 \oplus w_{2,k}^1, w_{2,k}^1 \oplus w_{2,k}^5\}$.
(c) If $n(k-1)+m(k-1) \neq 0$, or if $w(k-2) \neq 0$, or if $w(k-1)$ is in $\{w_{2,k-1}^1 \oplus w_{2,k-1}^1, w_{2,k-1}^1 \oplus w_{2,k-1}^5, w_{2,k-1}^7 \oplus w_{2,k-1}^7, w_{2,k-1}^3 \oplus w_{2,k-1}^7\}$, then either $w(k) = 0$ or $x(k)$ belongs to group A.

One convenient thing to notice about this definition is that by Table (4.1), when $k \geq 2$ the condition $w(k-1) \in \{w_{2,k-1}^1 \oplus w_{2,k-1}^1, w_{2,k-1}^1 \oplus w_{2,k-1}^5, w_{2,k-1}^7 \oplus w_{2,k-1}^7, w_{2,k-1}^3 \oplus w_{2,k-1}^7\}$ is equivalent to: $\sigma_{k-2}(G(k-1)) = \pm i$.

PROPOSITION 4.7. *Every quadratic form on a finite abelian 2-group has a normal form decomposition.*

PROOF. By proposition (4.5), we may put each homogeneous piece $G(k)$ into homogeneous normal form. Since $G(k) = 0$ for $k \gg 0$, we will use descending induction on k: we assume that the conditions specified for $G(\ell)$ (and particularly the form of $x(\ell)$) hold for all $\ell > k$, and we work on $G(k)$. It may happen that in the course of using the relations (VI) - (X), the homogeneous normal form on some lower pieces $G(\ell)$ for $\ell < k$ may be disturbed; it is understood that we restore the homogenous normal form for such pieces after each step.

By using relation (VI), if $w(k-1) \neq 0$ we may change any $w_{2,k}^3$ or $w_{2,k}^7$ to a $w_{2,k}^1$ or $w_{2,k}^5$. In addition, by using relation (VII), if $w(k-1) \neq 0$ we may change any v_k to a u_k. This leaves us with an $x(k)$ which satisfies condition (b).

To ensure that condition (c) is satisfied, note that we may assume $k \geq 2$, since $x(1)$ already belongs to group A. Under each of the three alternate hypotheses of condition (c), there is a relation (relations (VIII), (X), and (IX) respectively) which will enable us to convert a term of type $w_{2,k}^{\varepsilon}$ to a term of type $w_{2,k}^{5\varepsilon}$. By Lemma (4.4.2), then, if $w(k) \neq 0$ we may use such a relation to make $x(k)$ belong to group A.

It remains to show that the operations we have carried out have not caused any of the terms $G(\ell)$ for $\ell > k$ to fall out of normal form. Since we have changed no summands in any such terms, and since $n(k) + m(k)$, $\operatorname{rank}(w(k))$ and $\operatorname{rank}(w(k-1))$ are all invariants of the form, the only way this could have happened is if $w(k)$, while not previously in the set $\{w_{2,k}^1 \oplus w_{2,k}^1, w_{2,k}^1 \oplus w_{2,k}^5, w_{2,k}^7 \oplus w_{2,k}^7, w_{2,k}^3 \oplus w_{2,k}^7\}$, has now become an element of that set (forcing a new requirement that $x(k+1)$ be in group A). This implies that before our operations, $w(k) = w_{2,k}^{\varepsilon_1} \oplus w_{2,k}^{\varepsilon_2}$ with $\varepsilon_1 \not\equiv \varepsilon_2 \mod 4$, but that this is no longer true

after our operations. However, the only operation in our process which changes a $w_{2,k}^{\varepsilon}$ to a $w_{2,k}^{\bar{\varepsilon}}$ with $\bar{\varepsilon} \not\equiv \varepsilon \mod 4$ is the use of relation (VI) in achieving condition (b). If this relation has been used, then $w(k-1) \neq 0$; but then the conditions on the normal form for $G(k+1)$ imply that $x(k+1)$ was already in group A, so nothing has changed. Q.E.D.

We now come to the task of showing that our normal form is unique. As a corollary, we will find that the relations we have given among the standard quadratic forms on 2-groups in fact generate the full set of relations.

PROPOSITION 4.8. *The normal form decomposition of a quadratic form (G, q) on a finite abelian 2-group is unique. Moreover, the terms appearing are completely determined by the invariants $r_k(G)$ and $\sigma_k(G)$.*

PROOF. We begin with a decomposition

$$(G, q) = \bigoplus_{j \geq 1} (u_j^{\oplus n(j)} \oplus v_j^{\oplus m(j)} \oplus w(j))$$

which we assume is in normal form. We must show, then, that the invariants $r_j(G)$ and $\sigma_j(G)$ determine $x(j) = v_j^{\oplus m(j)} \oplus w(j)$ for each j. (The remaining terms $u_j^{n(j)}$ will then be determined by the ranks r_j.)

Let k be the largest index for which $G(k) \neq 0$. Our first task will be to show that $x(k)$ is determined, and then we will use a straightforward induction argument to finish the proof.

To prove that $x(k)$ is determined, we have several cases to consider. Notice for the purpose of dividing into cases that since σ_0 is always nonzero, if we assume that $\sigma_{k-1} = 0$ then automatically $k \geq 2$ so that σ_{k-2} is defined.

Case 1: $\sigma_k \neq 0$.

In this case $w(k) = 0$, so $x(k)$ is either 0 or v_k. If $\sigma_{k-1} \neq 0$, and $k = 1$, then $\sigma_1/\sigma_0 = \left(\frac{2}{\delta}\right)$ where $\delta = disc_8(G)$ distinguishes these. If $\sigma_{k-1} \neq 0$, and $k \geq 2$, then the ratio $\sigma_{k-2}/\sigma_{k-1}$ distinguishes these by Lemma (4.4.1). Finally, if $\sigma_{k-1} = 0$, then $w(k-1) \neq 0$, so $x(k)$ must be 0 by condition (b).

Case 2: $\sigma_k = 0$.

In this case we then have that $w(k) \neq 0$. This case breaks further by considering σ_{k-1}.

Case 2A: $\sigma_k = 0$ and $\sigma_{k-1} \neq 0$.

Suppose first that $k \geq 2$, $r_{k-1} = 0$, and $\sigma_{k-2} \neq 0$. Since $r_{k-1} = 0$, there are no $G(k-1)$ terms; moreover, $G(k-2)$ has only u_{k-2} and v_{k-2} terms. Hence $\sigma_{k-1} = \sigma_{k-1}(G(k))$ and $\sigma_{k-2} = \sigma_{k-2}(G(k))$. Therefore

the ratio $\sigma_{k-2}/\sigma_{k-1}$ determines whether $x(k)$ is in Group A or Group B, by Lemma (4.4.1). Therefore $x(k)$ is determined, by Lemma (4.4.3).

Next assume that either $k = 1$, $r_{k-1} \geq 1$, or $\sigma_{k-2} = 0$. We claim that under any of these hypotheses, $x(k)$ must be in Group A. If $k = 1$, then this is true by definition of the homogeneous normal form. If $r_{k-1} \geq 1$, then since $\sigma_{k-1} \neq 0$, we must have $w(k-1) = 0$. Hence $n(k-1) + m(k-1) = r_{k-1}$ is not zero, so $x(k)$ is in Group A by condition (c). Finally, if $\sigma_{k-2} = 0$, then $w(k-2) \neq 0$, so that again $x(k)$ is in Group A by condition (c).

Now that we know $x(k)$ must be in Group A, it is determined by Lemma (4.4.3).

Case 2B: $\sigma_k = 0$ and $\sigma_{k-1} = 0$.

In this case we have $w(k) \neq 0$ and $w(k-1) \neq 0$; in addition we must have $k \geq 2$. Condition (b) now forces $x(k)$ to come from the set $\{w^1_{2,k}, w^5_{2,k}, w^1_{2,k} \oplus w^1_{2,k}, w^1_{2,k} \oplus w^5_{2,k}\}$ and we must distinguish between these four forms.

If either $\sigma_{k-2} = 0$, $r_{k-1} > 2$, or $\sigma_{k-2}(G(k-1)) = \pm i$, then by condition (c) we know that $x(k)$ is in Group A, forcing $x(k)$ to be either $w^1_{2,k}$ or $w^1_{2,k} \oplus w^1_{2,k}$. The parity of the rank r_k distinguishes between these two.

Hence we may suppose that $\sigma_{k-2} \neq 0$, $r_{k-1} \leq 2$, and $\sigma_{k-2}(G(k-1)) \neq \pm i$.

Since $w(k-1) \neq 0$, and since r_{k-1} is equal to 1 or 2, $x(k-1)$ cannot have any v_{k-1} term. Therefore the only possibilities for $G(k-1)$ are the forms $w^{\varepsilon}_{2,k-1}$, $w^1_{2,k-1} \oplus w^7_{2,k-1}$, and $w^1_{2,k-1} \oplus w^3_{2,k-1}$, given that $\sigma_{k-2}(G(k-1)) \neq \pm i$. Note then that $\sigma_{k-2}(G(k-1)) \in \{e^{\pi i/4}, e^{7\pi i/4}, 1\}$, since this is true for each one of these. Since $\sigma_{k-2} \neq 0$, $w(k-2) = 0$, and so $\sigma_{k-2}(G(k-2)) = 1$; hence the value of σ_{k-2} is determined only by $x(k-1)$ and $x(k)$, i.e., $\sigma_{k-2} = \sigma_{k-2}(G(k-1)) \cdot \sigma_{k-2}(x(k))$. Since $\sigma_{k-2}(G(k-1)) \in \{e^{\pi i/4}, e^{7\pi i/4}, 1\}$, we see that σ_{k-2} and $\sigma_{k-2}(x(k))$ lie in the same complex half-plane; therefore the complex half-plane in which $\sigma_{k-2}(x(k))$ lies is determined.

The proof is now completed by noting that the possibilities for $x(k)$ with the same rank have opposite σ_{k-2}; therefore if one knows the complex half-plane in which they lie, we know $x(k)$.

This finishes the proof of the statement that $x(k)$ (and hence $G(k)$) is determined by the given invariants, and is the crux of the induction proof for the general statement.

Our inductive hypothesis is as follows. We fix an integer $k \geq 1$, and we assume that the normal form decomposition for any quadratic form on a group G' with $G'(j) = 0$ for all $j \geq k$ is unique, and is

determined by the rank and signature invariants. We must then prove the statement for a group G with $G(k) \neq 0$ but with $G(j) = 0$ for all $j > k$.

Write $G = G' \oplus G(k)$, with G' having no terms of scale 2^k or greater. By the first part of the argument, the normal form for the $G(k)$ piece is determined. Moreover, for each ℓ with $0 \leq \ell < k$, the signature invariants $\sigma_\ell(G(k))$ are all nonzero. Hence for each such ℓ we may define

$$\widetilde{\sigma}_\ell = \sigma_\ell(G)/\sigma_\ell(G(k))$$

and we have immediately that

$$\sigma_\ell(G') = \widetilde{\sigma}_\ell$$

for these ℓ. Therefore the rank and signature invariants of G' are determined from those of G. By induction, G' has a unique normal form decomposition. Hence so does G. Q.E.D.

As in the case with p odd, the uniqueness of the normal form and the construction using the relations of Proposition (3.2) only, implies that there are no other relations:

Corollary 4.9. *The relations (0) - (X) listed in Proposition (3.2) among the generators of $\mathcal{T}_\in$ generate all the relations. In addition, the relations (I) - (X) among the generators of $\mathcal{G}_\in$ generate all the relations between them.*

Note that $\mathcal{G}_\in$ is exactly the set of torsion quadratic $\mathbb{Z}_2$-modules which have no summand of type $w^\varepsilon_{2,1}$ in any decomposition.

5. Normal forms for quadratic $\mathbb{Z}_2$-modules

In this section, we will deduce normal forms for decompositions of nondegenerate quadratic $\mathbb{Z}_2$-modules into rank one and two summands from the corresponding results for 2-torsion quadratic forms. The discriminant-form construction provides a natural map $d : \mathcal{Q}_\in \to \mathcal{T}_\in$ assigning the isomorphism class of a quadratic $\mathbb{Z}_2$-module to that of its discriminant-form. This is not an isomorphism of monoids, for two reasons: firstly, the unimodular forms U_0 and V_0 have trivial discriminant-form groups, and secondly, the relation (0) $w^\varepsilon_{2,1} \cong w^{5\varepsilon}_{2,1}$ does not lift to a corresponding relation between $W^\varepsilon_{2,1}$'s.

For the purpose of finding normal forms, it is more useful to define a different map $d_2 : \mathcal{Q}_\in \to \mathcal{G}_\in$ as follows: given a quadratic $\mathbb{Z}_2$-module (L, Q), consider the form $(L(2), Q_{(2)})$, where $L(2) \cong L$ and $Q_{(2)}(x) = 2Q(x)$. Then $d_2(L, Q)$ is the isomorphism class of the

discriminant-form $(G_{L(2)}, q_{L(2)})$. Note that this discriminant form contains no summands of type $w^{\varepsilon}_{2,1}$, so that its isomorphism class lies in $\mathcal{G}_{\in}$. We have $d_2(W^{\varepsilon}_{2,k}) = w^{\varepsilon}_{2,k+1}$, $d_2(U_k) = u_{k+1}$, and $d_2(V_k) = v_{k+1}$.

PROPOSITION 5.1. *The map $d_2 : \mathcal{Q}_{\in} \to \mathcal{G}_{\in}$ is an isomorphism of monoids.*

PROOF. Let $\mathcal{F}$ be the free monoid on the generators $\{u_{k-1}, v_{k-1}, w^{\varepsilon}_{2,k}$ for $k \geq 2\}$ of $\mathcal{G}_{\in}$, and define a map $e : \mathcal{F} \to \mathcal{Q}_{\in}$ as follows: for $k \geq 2$, $e(u_{k-1}) = U_{k-2}$, $e(v_{k-1}) = V_{k-2}$, and $e(w^{\varepsilon}_{2,k}) = W^{\varepsilon}_{2,k-1}$. Each relation among the generators of $\mathcal{G}_{\in}$ maps under e to a valid relation among the generators of $\mathcal{Q}_{\in}$; thus e descends to a map $\bar{e} : \mathcal{G}_{\in} \to \mathcal{Q}_{\in}$, which provides an inverse for d_2. Q.E.D.

COROLLARY 5.2. *The relations listed in proposition (3.1) among the generators of $\mathcal{Q}_{\in}$ generate all the relations.*

PROOF. The existence of the isomorphism d_2 precludes the possibility of further relations. Q.E.D.

DEFINITION 5.3. A decomposition of a quadratic $\mathbb{Z}_2$-module (L, Q) is in *partial normal form*, or *homogeneous normal form*, or *normal form* exactly when the induced decomposition of $G_{L(2)}$ has the corresponding property.

COROLLARY 5.4. *Every nondegenerate quadratic $\mathbb{Z}_2$-module (L, Q) has a unique normal form decomposition.*

This follows directly from the corresponding statement for $\mathcal{T}_{\in}$ (and hence for $\mathcal{G}_{\in}$).

We have the following analogue of Corollary (2.11):

COROLLARY 5.5. *A nondegenerate quadratic $\mathbb{Z}_2$-module is determined up to isomorphism by its rank, discriminant, and discriminant-form.*

PROOF. Let (L, Q) be a nondegenerate quadratic $\mathbb{Z}_2$-module, and decompose it into normal form $L \cong \bigoplus_{k \geq 0} L(k)$ where for each k, $L(k)$ is a direct sum of U_k's, V_k's, and $W^{\varepsilon}_{2,k}$'s, The discriminant-form determines $L(k)$ for $k \geq 2$, and it remains to show that $L(0)$ and $L(1)$ are also determined. We have that

$$L(0) \oplus L(1) \cong U_0^{\oplus n(0)} \oplus V_0^{\oplus m(0)} \oplus U_1^{\oplus n(1)} \oplus V_1^{\oplus m(1)} \oplus W(1)$$

where $W(1)$ is either trivial or a sum of 1 or 2 rank one forms $W^{\varepsilon}_{2,1}$'s. The discriminant-form of this part of L is $u_1^{\oplus n(1)} \oplus v_1^{\oplus m(1)} \oplus w(1)$, where $w(1)$ is the corresponding sum of cyclic forms to $W(1)$. Note that the

only part of this data which is not seen by the discriminant-form is $n(0)$, $m(0)$, and the difference between $W_{2,1}^5$ and $W_{2,1}^1$, and between $W_{2,1}^7$ and $W_{2,1}^3$. Hence $n(1)$ and $m(1)$ are always determined, as is the rank of $W(1)$, by the discriminant-form: the only ambiguity in $W(1)$ is because of relation (0). Therefore also the rank of $L(0)$ is determined, by the total rank. If the rank of $W(1)$ is zero, then $L(1)$ is determined; since the rank of $L(0)$ is determined, and whether $m(0)$ is 0 or 1 is distinguished by the discriminant, we are done in this case.

Therefore assume that $W(1) \neq 0$. If $L(0) = 0$, then the normal form requires that $X(1) = V_1^{\oplus m(1)} \oplus W(1)$ come from the capital letter version of Table (4.1). In this case, the knowledge of the discriminant-form tells us which row of the table we are on; since the (capitalized) entries in each row differ in their discriminants, we are done in this case.

If $L(0) \neq 0$, then the normal form requires that $X(1) = V_1^{\oplus m(1)} \oplus W(1)$ come from the capital letter version of Group A of Table (4.1). Therefore $X(1)$ is determined by the discriminant-form. This determines $L(1)$, and the two possibilities for $L(0)$ are now distinguished by the discriminant. Q.E.D.

We also have an analogue of Corollary (2.10) in the $p = 2$ case; we leave the proof to the reader.

COROLLARY 5.6. *Let $p = 2$.*

(5.6.1) Given any torsion quadratic form (G, q) over $\mathbb{Z}_2$ in $\mathcal{G}_2$ (i,e, with no summands of the form $w_{2,1}^{\varepsilon}$) there is a unique quadratic $\mathbb{Z}_2$-module $L(q)$ (up to isomorphism) such that $\operatorname{rank}(L(q)) = \ell(G)$ *and the discriminant-form of $L(q)$ is isomorphic to (G, q).*

(5.6.2) If (G, q) is a torsion quadratic form over $\mathbb{Z}_2$ not in $\mathcal{G}_2$ (i.e., if (G, q) has a direct summand of the form $w_{2,1}^{\varepsilon}$ for some ε) then there are exactly two quadratic $\mathbb{Z}_2$-modules $L_1(q)$ and $L_2(q)$ (up to isomorphism) such that $\operatorname{rank}(L_1(q)) = \operatorname{rank}(L_2(q)) = \ell(G)$ *and the discriminant-forms of both $L_1(q)$ and $L_2(q)$ are isomorphic to (G, q). Moreover,* $\operatorname{disc}(L_1(q)) = 5 \operatorname{disc}(L_2(q)) \bmod \mathbb{U}_{\not\square}^{\not\square}$.

(5.6.3) If L is any quadratic $\mathbb{Z}_p$-module whose discriminant-form is isomorphic to (G, q), and L' is a quadratic $\mathbb{Z}_2$-module such that $\operatorname{rank}(L') = \ell(G)$ *and the discriminant-form of L' is also isomorphic to (G, q), then there is a unique unimodular quadratic $\mathbb{Z}_2$-module M such that $L \cong M \oplus L'$.*

It is useful to have at hand the analoque of Proposition 2.12:

PROPOSITION 5.7. *Fix an integer r, an element $d \in \mathbb{Z}_2 - \{0\}/\mathbb{U}_2^2$, and a finite 2-torsion quadratic form (G, q). Then there exists a quadratic $\mathbb{Z}_2$-module L with $\operatorname{rank}(L) = r$, $\operatorname{disc}(L) = d$, and $(G_L, q_L) \cong (G, q)$ if and only if:*

(1) *$r \geq \ell(G)$;*
(2) *$r \equiv \ell(G) \bmod 2$;*
(3) *if $d = 2^k u \mod \mathbb{U}_2^2$ with $u \in \mathbb{U}_2$, then $|G| = 2^k$;*
(4) *if $r = \ell(G) + 2n$ then $\chi(d) \equiv (-1)^n \chi(\operatorname{disc}(q)) \bmod 4$.*
(5) *if $r = \ell(G)$ and if G has no summand of the form $w_{2,1}^{\varepsilon}$ (i.e., G is good and special), then $\chi(d) = \chi(\operatorname{disc}_8(q))$.*

Moreover, if so, then L is unique up to isomorphism.

PROOF. Clearly the first and third conditions are necessary, and the fifth condition follows by Corollary II.8.7. The second and fourth conditions follow from Corollary 5.6.3, noting that any unimodular quadratic $\mathbb{Z}_2$-module has even rank, and decomposes completely into rank two pieces (U_0's and V_0's); these pieces have discriminants equal to $-1 \bmod 4$.

To see that these conditions are sufficient, let L' be a quadratic $\mathbb{Z}_2$-module with discriminant-form equal to (G, q) such that $\operatorname{rank}(L') = \ell(G)$; such an L' exists by Corollary 5.6, and there are two choices for L' if G contains one of the forms $w_{2,1}^{\varepsilon}$ as a summand; these two have discriminants which differ by a factor of 5. We seek the desired module L in the form

$$L = U_0^{N(0)} \oplus V_0^{e(0)} \oplus L'$$

with $e(0) \leq 1$; note that in this case $\operatorname{disc}(L) = 7^{N(0)} \cdot 3^{e(0)} \cdot \operatorname{disc}(L')$. This module L has rank $2N(0) + 2e(0) + \ell(G)$, and $\operatorname{disc}(L) = |G|u$ for some unit u. Moreover $\chi(\operatorname{disc}(L)) = 7^{N(0)} \cdot 3^{e(0)} \cdot \chi(\operatorname{disc}(q))$.

First assume that G has no summand of the form $w_{2,1}^{\varepsilon}$, so that either $\operatorname{disc}(q)$ is defined modulo 8 or the mod 8 discriminant $\operatorname{disc}_8(q)$ is defined, and L' is unique. (In the rest of this paragraph we write only $\operatorname{disc}(q)$, but if necessary the reader should use $\operatorname{disc}_8(q)$.) If $r = \ell(G)$, we may take $N(0) = e(0) = 0$, so that $L = L'$; by (3) and (5) we see that $\operatorname{disc}(L) = d$ and we are done. If $r = \ell(G) + 4n + 2$ with $n \geq 0$, then by (4) either $\chi(d) = 3\operatorname{disc}(q) \bmod 8$ or $\chi(d) = 7\operatorname{disc}(q) \bmod 8$; in the former case we take $N(0) = 2n$ and $e(0) = 1$ and in the latter case we take $N(0) = 2n + 1$ and $e(0) = 0$. If $r = \ell(G) + 4n$ with $n \geq 1$, then by (4) either $\chi(d) = \operatorname{disc}(q) \bmod 8$ or $\chi(d) = 5\operatorname{disc}(q) \bmod 8$; in the former case we take $N(0) = 2n$ and $e(0) = 0$ and in the latter case we take $N(0) = 2n - 1$ and $e(0) = 1$. Thus we are done in case G is good and special.

Suppose G has a summand of the form $w_{2,1}^{\varepsilon}$ so that $\mathrm{disc}(q)$ is only defined modulo 4. Here there are two choices for L', as noted above. Write $r = \ell(G) + 2n$, and set $N(0) = n$ and $e(0) = 0$, so that $L = U_0^n \oplus L'$. We have $\mathrm{disc}(L) = 7^n \mathrm{disc}(L')$ so that $\chi(\mathrm{disc}(L)) = \chi(d) \bmod 4$ by (4). By altering L' if necessary we can therefore achieve that $\chi(\mathrm{disc}(L)) = \chi(d) \bmod 8$, so that $\mathrm{disc}(L) = d$ as required.

This proves the existence of L, and the uniqueness statement is exactly Corollary 2.11. Q.E.D.

We note that many of the above statements hold for inner product modules over $\mathbb{Z}_2$, where we have in addition the forms $W_{2,0}^{\varepsilon}$. In particular, the relations in Proposition 3.1 generate all the relations, the partial normal form, homogeneous normal form, and normal form all make sense and exist, and the normal form decomposition is unique. We leave all the extensions of the statements and results to the monoid $\mathcal{I}_2$ to the reader.

We close this section with the analogue of Theorem (2.13) concerning the lifting of isometries.

THEOREM 5.8. *Let L_1 and L_2 be two nondegenerate quadratic $\mathbb{Z}_2$-modules such that* $\mathrm{rank}(L_1) = \mathrm{rank}(L_2)$ *and* $\mathrm{disc}(L_1) = \mathrm{disc}(L_2)$. *Suppose that $\sigma : G_{L_1} \to G_{L_2}$ is an isometry between the discriminant forms of L_1 and L_2. Then there exists an isometry $s : L_1 \to L_2$ inducing σ.*

PROOF. The proof is formally the same as that of Theorem (2.13). The assumptions imply, by Corollary (5.5), that L_1 and L_2 are isomorphic. Decompose G_{L_1} into an (internal) normal form decomposition; denote this by

$$G_{L_1} = \oplus_i g_i^{(1)}.$$

Now transport this decomposition to G_{L_2} via the isomorphism σ, and denote this by

$$G_{L_2} = \oplus_i g_i^{(2)}.$$

Since σ is an isometry, $g_i^{(1)} \cong g_i^{(2)}$ for each i. Now by Proposition (II.11.6), both L_1 and L_2 can be decomposed compatibly with their discriminant-forms. Specifically, we have direct sum decompositions

$$L_1 = M_1 \oplus \bigoplus_i L_i^{(1)} \text{ and } L_2 = M_2 \oplus \bigoplus_i L_i^{(2)}$$

with M_1 and M_2 unimodular, $L_i^{(1)}$ and $L_i^{(2)}$ indecomposable and rank one or two for each i, and the natural inclusions inducing the obvious correspondence of discriminant-forms.

Since the decompositions of the G_{L_i} are in normal form, these decompositions of the L_i are almost in normal form. They are certainly

in normal form for any pieces except possibly any $W_{2,1}^{\varepsilon}$'s,, and the unimodular pieces. The only departure from normal form is a possible failure to use relation (VIII) when $k = 1$, so that some $W_{2,1}^{\varepsilon}$ should be a $W_{2,1}^{5\varepsilon}$ at the expense of changing the unimodular part of the decomposition. (This is not visible at the discriminant-form level, because of relation (0).) If this is so, we may alter the decomposition of the L_i appropriately and still have a lifting of the G_{L_i} decomposition; thus we may assume that the decomposition of the L_i above are in normal form. Since L_1 and L_2 are isomorphic, the pieces of their decompositions (which are now in normal form) are unique and so match up perfectly. This allows us to define an isometry $s' : L_1 \to L_2$ by identifying the pieces.

The isometry s' induces an isometry $\sigma' : G_{L_1} \to G_{L_2}$, which preserves the decompositions. Therefore σ' and σ differ only by automorphisms of the pieces: i.e., there is an automorphism τ of G_{L_1} which preserves the decomposition, such that $\sigma = \sigma' \circ \tau$. By Proposition (1.3), the automorphism τ lifts to an automorphism t of L_1, and the desired isometry from L_1 to L_2 is then $s = s' \circ t$. Q.E.D.

Finally, applying the above with $L_1 = L_2$ gives the 2-adic analogue of Corollary (2.14):

COROLLARY 5.9. *If L is a nondegenerate quadratic $\mathbb{Z}_2$-module, then the natural map $\mathcal{O}(\mathcal{L}) \to \mathcal{O}(\mathcal{G}_{\mathcal{L}})$ is surjective.*

CHAPTER V

Rational Quadratic Forms

In this chapter we will collect results concerning quadratic vector spaces over the rationals $\mathbb{Q}$, the p-adic rationals $\mathbb{Q}_p$, and the reals $\mathbb{R}$. All of the definitions and results are quite standard and can be found in any number of good texts, for example, [**Cassels 78**], [**O'Meara 63**], and [**Lam 73**]. We will therefore not give proofs of all the statements, but we will give complete definitions and proofs of several of the simpler results to give the reader some feeling for the subject.

1. Forms over $\mathbb{Q}$ and $\mathbb{Q}_p$

Let K be a field of characteristic 0; in our applications, K will be either $\mathbb{Q}$ or $\mathbb{Q}_p$ for some p. (We allow $p = \infty$, where $\mathbb{Q}_\infty$ denotes the field of real numbers $\mathbb{R}$.) Let (V, Q) be a quadratic vector space over K, with associated bilinear form $\langle -, - \rangle$. If $\{e_i\}$ is a basis for V over K, let A_Q be the matrix of the form: $(A_Q)_{ij} = \langle e_i, e_j \rangle$. This matrix is a nonsingular symmetric matrix over K, with even values on the main diagonal. The determinant of A_Q is non-zero, and induces the discriminant $\mathrm{disc}(Q)$ which lies in $\mathcal{D}(K) = K^\times/(K^\times)^2$. Let us remind the reader of these value groups for the fields in question; the following comes directly from Lemma (I.3.6).

Lemma 1.1.

(1.1.1) $\mathcal{D}(\mathbb{Q})$ *is a free* $\mathbb{Z}/2$*-module on the set* $\{-1\} \cup \{p > 1 \mid p$ *is a prime in* $\mathbb{Z}\}$.

(1.1.2) $\mathcal{D}(\mathbb{R}) = \mathcal{D}(\mathbb{Q}_\infty) = \{1, -1\}$ *is a cyclic group of order 2.*

(1.1.3) If p *is an odd prime, then* $\mathcal{D}(\mathbb{Q}_p) = \{1, p, r, pr\}$ *is a Klein* 4*-group generated by the prime* p *and the class* r *of a non-square unit in* $\mathbb{Z}_p$.

(1.1.4) For $p = 2$, $\mathcal{D}(\mathbb{Q}_2) = \{1, 2, 3, 5, 6, 7, 10, 14\}$ *is isomorphic to* $(\mathbb{Z}/2)^3$*, generated by* $\{2, 3, 5\}$.

If $A_Q = (a_{ij})$ with respect to some basis $\{e_i\}$ for V over K, then the quadratic form Q can be written as

$$Q(\sum_i x_i e_i) = Q(\underline{x}) = \sum_i Q(e_i) x_i^2 + \sum_{i<j} a_{ij} x_i x_j.$$

for x_i in K. (Note that in characteristic 0, $Q(e_i) = a_{ii}/2$.) This polynomial notation for Q will be used frequently in this chapter.

With this notation, the form Q is diagonalizable if and only if there is a basis $\{e_i\}$ for V over K such that $Q(\sum_i x_i e_i) = \sum_i Q(e_i)x_i^2$.

With our hypothesis of characteristic 0 on K, we see by Proposition (I.5.8) that every quadratic K-vector space is diagonalizable.

If $a \in K$, we say that the form Q *represents* a if there is a non-zero vector v in V such that $Q(v) = a$.

2. The Hilbert norm residue symbol and the Hasse invariant

Let a and b be elements of $\mathbb{Q}_p^\times$ ($p = \infty$ is allowed).

Definition 2.1. The *Hilbert Norm Residue Symbol* $(a, b)_p$ (or simply (a, b) if no confusion is likely) is defined by

$$(a,b)_p = \begin{cases} 1 & \text{if } ax^2 + by^2 - z^2 \text{ represents } 0 \\ -1 & \text{otherwise.} \end{cases}$$

Note that the value of $(a, b)_p$ depends only on the classes of a and b modulo squares in $\mathbb{Q}_p^\times$. Hence the function $(-,-)_p$ descends to a map

$$(-,-)_p : {\mathbb{Q}_p}^\times/(\mathbb{Q}_p^\times)^2 \to \{1,-1\}.$$

The following lemma records the elementary facts concerning the Hilbert Norm Residue Symbol. For proofs, see [**Cassels 78**, Chapter 3, Section 2].

Lemma 2.2.

(2.2.1) The Hilbert Norm residue Symbol $(-,-)_p$ *is a nondegenerate bilinear function from* ${\mathbb{Q}_p}^\times/(\mathbb{Q}_p^\times)^2$ *to* $\{1,-1\}$.

(2.2.2) $(a,-a) = 1$ *for every* $a \in \mathbb{Q}_p^\times$.

(2.2.3) $(-1,-1)_\infty = -1$.

(2.2.4) If $p \neq 2, \infty$ *and* r *is a non-square unit modulo* p, *then* $(1,1)_p = (1,r)_p = (r,r)_p = 1$, $(p,r)_p = -1$, *and* $(p,p)_p = (-1)^{(p-1)/2}$.

(2.2.5) $(2,2)_2 = (3,5)_2 = (5,5)_2 = 1$ *and* $(2,3)_2 = 2,5)_2 = (3,3)_2 = -1$.

Since $\mathbb{Q} \subset \mathbb{Q}_p$ for all p, we may evaluate $(a, b)_p$ for $a, b \in \mathbb{Q}^\times$ also. The behavior of these values is governed by the so-called "Product Formula" for the Hilbert Norm Residue Symbol, which is equivalent to the law of Quadratic Reciprocity. A proof may be found in [**Cassels 78**, Chapter 3, Lemma 3.4].

Lemma 2.3. *Let* $a, b \in \mathbb{Q}^\times$. *Then*

(2.3.1) $(a,b)_p = 1$ *for all but finitely many* p.
(2.3.2) $\prod_{all\ p}(a,b)_p = 1$.

We will hereafter use the phrase "almost all p" to mean all but finitely many p.

DEFINITION 2.4. Let (V,Q) be a quadratic vector space over $\mathbb{Q}_p$, $p \leq \infty$. Choose a diagonalizing basis for V, so that in this basis Q has the form

$$Q(\sum_i x_i e_i) = \sum_i a_i x_i.$$

The *Hasse invariant* of (V,Q), denoted by $c_p(V,Q)$ (or $c_p(V)$ or $c_p(Q)$ as the situation warrants) is defined by the product

$$c_p(V,Q) = \prod_{i<j}(a_i,a_j)_p.$$

If the dimension of V is one, we define $c_p(V,Q) = 1$.

A priori of course the Hasse invariant depends on the choice of diagonalizing basis for V. In fact it is well-defined, independent of this choice. (See [**Cassels 78**, Chapter 4, Section 2].) In addition, we have the following direct sum formula for the Hasse invariant.

LEMMA 2.5. *If* (V_1,Q_1) *and* (V_2,Q_2) *are two quadratic vector spaces over* $\mathbb{Q}_p$, *then*

$$c_p(V_1 \oplus V_2) = c_p(V_1)c_p(V_2)(\mathrm{disc}(V_1),\mathrm{disc}(V_2))_p.$$

PROOF. Assume Q_1 and Q_2 are diagonalized as $Q_1(\underline{x}) = \sum_i a_i x_i$ and $Q_2(\underline{y}) = \sum_j b_j y_j$. Then $Q_1 + Q_2 = \sum_i a_i x_i + \sum_j b_j y_j$ is the quadratic form on $V_1 \oplus V_2$. Hence

$$\begin{aligned} c_p(V_1 \oplus V_2) &= \left(\prod_{i<k}(a_i,a_k)_p\right)\left(\prod_{i,j}(a_i,b_j)_p\right)\left(\prod_{j<n}(b_j,b_n)_p\right) \\ &= c_p(V_1)(\prod_i a_i, \prod_j b_j)_p c_p(V_2) \text{ by the bilinearity of } (-,-)_p \\ &= c_p(V_1)c_p(V_2)(\mathrm{disc}(V_1),\mathrm{disc}(V_2))_p. \end{aligned}$$

Q.E.D.

Recall that a quadratic vector space over $\mathbb{Q}_\infty = \mathbb{R}$ is classified by its rank and signature. The Hasse invariant can be immediately computed using Lemma (2.2.3):

LEMMA 2.6. *Let* (V,Q) *be a real quadratic vector space, with signature* (s_+,s_-). *Then* $c_\infty(V,Q) = (-1)^{\binom{s_-}{2}}$.

The main global result concerning the Hasse invariant is a consequence of the Product Formula (Lemma (2.3)) for the Hilbert Norm Residue Symbol.

LEMMA 2.7. *Let V be a quadratic vector space over $\mathbb{Q}$, and let $V_p = V \otimes \mathbb{Q}_p$ be the induced quadratic vector space over $\mathbb{Q}_p$. Then $c_p(V_p) = 1$ for almost all p, and*

$$\prod_{all\ p} c_p(V_p) = 1.$$

PROOF. Diagonalize the form Q on V as $Q(\underline{x}) = \sum_i a_i x_i$, where the a_i are fixed rational numbers. This polynomial formula is also the formula for the induced form Q_p for every p. Hence $c_p(V_p) = \prod_{i<j}(a_i, a_j)_p$ for all p. Since the a_i's are independent of p, $c_p(V_p) = 1$ for almost all p by Lemma (2.3.1). The second statement now follows from Lemma (2.3.2):

$$\prod_{\text{all } p} c_p(V_p) = \prod_{i<j} \prod_{\text{all } p} (a_i, a_j)_p = \prod_{i<j} 1 = 1.$$

Q.E.D.

3. Representations of numbers by forms over $\mathbb{Q}$ and $\mathbb{Q}_p$

Recall that a quadratic vector space (V, Q) represents a number $a \in K$ if there is a nonzero vector v in V such that $Q(v) = a$. The following observation is sometimes useful:

(3.1)
If $a \neq 0$, then V represents a if and only if $V \oplus \langle -a \rangle_K$ represents 0.

The next theorem tells when a form over $\mathbb{Q}_p$ for finite p represents a given number.

THEOREM 3.2. *Fix a prime $p \neq \infty$, and let V be a quadratic vector space over $\mathbb{Q}_p$. Let n be the rank of V, d the discriminant of V, and c_p the Hasse invariant of V. Let a be a non-zero element of $\mathbb{Q}_p$. Then V represents a if and only if one of the following holds:*

(1) $n = 1$ *and* $a \equiv d \mod (\mathbb{Q}_p^\times)^2$
(2) $n = 2$ *and* $(a, -d)_p = c_p$
(3) $n = 3$ *and* $a \neq -d \mod (\mathbb{Q}_p^\times)^2$
(4) $n = 3$, $a \equiv -d \mod (\mathbb{Q}_p^\times)^2$, *and* $(-1, -d)_p = c_p$
(5) $n \geq 4$.

The reader may find proofs of this theorem in [**Cassels 78**, Chapter 4, Section2], [**Serre 73**, Chapter IV, Section 2.2], or [**B-S 66**, Chapter 1, Section 6].

The following corollary is immediate.

COROLLARY 3.3. *Fix a prime $p \neq \infty$, and let V be a quadratic vector space over $\mathbb{Q}_p$ of rank $n \geq 3$, discriminant d, and Hasse invariant c_p. Let $a \in \mathbb{Q}_p^\times$. Then V fails to represent a if and only if $n = 3$, $a \equiv -d \mod (\mathbb{Q}_p^\times)^2$, and $(-1, -d)_p = -c_p$. In particular, V represents all but possibly one coset in $\mathbb{Q}_p^\times/(\mathbb{Q}_p^\times)^2$.*

The next corollary is an easy consequence of the previous results.

COROLLARY 3.4. *Fix a prime $p \neq \infty$, and let V be a quadratic vector space over $\mathbb{Q}_p$ of rank $n \geq 5$. Then V represents 0.*

PROOF. Not every vector of V can be isotropic, so find a nonzero vector w such that $Q(w) \neq 0$. If W is the span of w, then $W^\perp$ is of dimension 4, and so by the previous corollary $W^\perp$ represents $-Q(w)$. Since $W \cong \langle +Q(w) \rangle$, the result follows from (3.1). Q.E.D.

Of course, the situation over $\mathbb{Q}_\infty = \mathbb{R}$ is different. The following is immediate.

LEMMA 3.5. *Let V be a real quadratic vector space with $sign(V) = (s_+, s_-)$. Then V represents 0 if and only if $s_- s_+ \neq 0$, i.e., V is indefinite.*

COROLLARY 3.6. *If V is an indefinite real quadratic vector space, then V represents all real numbers.*

The Hasse-Minkowski Theorem reduces representation of numbers with quadratic forms over $\mathbb{Q}$ to representation over $\mathbb{Q}_p$ for all p. It is one of the cornerstones of the theory of rational quadratic forms.

THEOREM 3.7. *Let V be a quadratic vector space over $\mathbb{Q}$. Then V represents 0 if and only if $V \otimes \mathbb{Q}_p$ represents 0 for all $p \leq \infty$.*

Proofs of the Hasse-Minkowski Theorem appear in [**Cassels 78**, Chapter 6 Section 11], [**Serre 73**, Chapter IV, Section 3.2], and [**B-S 66**, Chapter 1, section 7].

The following corollary is often referred to as Meyer's Theorem.

COROLLARY 3.8. *Let V be an indefinite quadratic vector space over $\mathbb{Q}$ of dimension $n \geq 5$. Then V represents 0.*

4. Isometries

The rank, discriminant, and Hasse invariants serve to classify quadratic vector spaces over the fields $\mathbb{Q}_p$ for $p \neq \infty$. Expressed in terms of isometries, the precise statement is given below. (See [**Cassels 78**, Chapter 4,Theorem 1.1] or [**Serre 73**, Chapter IV, Section 2.3, Theorem 7].)

THEOREM 4.1. *Fix a finite prime p, and let V_1 and V_2 be quadratic vector spaces over $\mathbb{Q}_p$. Then there exists an isometry between V_1 and V_2 if and only if they have the same rank n, discriminant d, and Hasse invariant c_p.*

The analogous statement for $\mathbb{Q}_\infty = \mathbb{R}$ is false; for example, the forms with signature $(1, 6)$ and $(5, 2)$ have the same rank (7), the same discriminant (1) and the same Hasse invariant c_∞ (-1), but are clearly not isomorphic. If $p = \infty$, such an isometry exists if and only $\text{rank}(V_1) = \text{rank}(V_2)$ and $sign(V_1) = sign(V_2)$.

The Weak Hasse Principle state that isometries of rational forms depend only on p-adic isometries:

THEOREM 4.2. *Let V_1 and V_2 be quadratic vector spaces over $\mathbb{Q}$. Suppose that there exist isometries $\sigma_p : V_1 \otimes \mathbb{Q}_p \to V_2 \otimes \mathbb{Q}_p$ for every $p \leq \infty$. Then there exists an isometry $\sigma : V_1 \to V_2$.*

Proofs may be found in [**Cassels 78**, Chapter 6, Theorems 1.2], [**Serre 73**, Chapter IV, Section 3.3, Theorem 4], and [**B-S 66**, Chapter 1, section 7, Theorem 2].

5. Existence of forms over $\mathbb{Q}$ and $\mathbb{Q}_p$

The main result concerning the existence of quadratic vector spaces over $\mathbb{Q}_p$ is given below. (See [**Cassels 78**, Chapter 6, Theorems 1.3], or [**Serre 73**, Chapter IV, Section 2.3, Proposition 6].)

THEOREM 5.1. *Fix a finite prime p, and let $(n, d, c) \in \mathbb{N} \times \left(\mathbb{Q}_\shortmid^\times / (\mathbb{Q}_\shortmid^\times)^{\nvDash}\right) \times \{\nVdash, -\nVdash\}$ be given, such that*

(1) *if $n = 1$ then $c = 1$, and*
(2) *if $n = 2$ and $d \equiv -1 \mod (\mathbb{Q}_p^\times)^2$ then $c = 1$*

Then there exists a quadratic vector space V over $\mathbb{Q}_p$ such that $dim(V) = n$, $\text{disc}(V) \equiv d \mod (\mathbb{Q}_p^\times)^2$, and $c_p(V) = c$.

The existence of quadratic vector spaces over $\mathbb{Q}$ forms a converse to Lemma (2.7):

THEOREM 5.2. *Fix $n \geq 1$ and $d \in \mathbb{Q}^\times$. Suppose that for every $p \leq \infty$, we are given a quadratic vector space V_p over $\mathbb{Q}_p$ such that*

(1) *$dim(V_p) = n$ for every p,*
(2) $\mathrm{disc}(V_p) \equiv d \mod (\mathbb{Q}_p^\times)^2$ *for every p,*
(3) *$c_p(V_p) = 1$ for almost all p, and*
(4) $\prod_{p\le\infty} c_p(V_p) = 1$.

Then there exists a quadratic vector space V over $\mathbb{Q}$ such that $dim(V) = n$, $\mathrm{disc}(V) \equiv d \mod (\mathbb{Q}^\times)^2$. *Moreover, there exist isometries $\sigma_p : V \otimes \mathbb{Q}_p \to V_p$ for every p.*

It will be convenient to rephrase this existence theorem by singling out $p = \infty$.

COROLLARY 5.3. *Fix a pair $(s_+, s_-) \in \mathbb{N}^{\not=}$, and $d \in \mathbb{Q}^\times$, such that $d = (-1)^{s_-}|d|$. Assume that for every finite prime $p < \infty$ there is given a quadratic vector space V_p over $\mathbb{Q}_p$ of dimension $n = s_+ + s_-$, satisfying the following:*

(1) $\mathrm{disc}(V_p) \equiv d \mod (\mathbb{Q}_p^\times)^2$ *for every p,*
(2) *$c_p(V_p) = 1$ for almost all p, and*
(3) $(-1)^{\binom{s_-}{2}} \prod_{p\neq\infty} c_p(V_p) = 1$.

Then there exists a quadratic vector space V over $\mathbb{Q}$ such that $dim(V) = n$, $\mathrm{disc}(V) \equiv d \mod (\mathbb{Q}^\times)^2$, *and $sign(V) = (s_+, s_-)$. Moreover, there exist isometries $\sigma_p : V \otimes \mathbb{Q}_p \to V_p$ for every p.*

PROOF. Since $d_\infty = d/|d|$, it is necessary that $d = (-1)^{s_-}|d|$, since $d_\infty = (-1)^{s_-}$. This assures that (2) of Theorem (5.2) holds for all p; (2) is the same condition, and (3) follows from the calculation of $c_\infty(V)$ given in Lemma (2.6). Q.E.D.

6. Orthogonal Groups and the surjectivity of (det,spin)

The reader will recall from Chapter I, Section 9 the definition of a *reflection*. Let (V, Q) be a quadratic vector space over K and assume that $v \in V$ has $Q(v) \neq 0$. Then the isometry τ_v defined by

$$\tau_v(w) = w - (\langle v, w\rangle / Q(v))v$$

has $\det(\tau_v) = -$ and $\mathrm{spin}(\tau_v) = Q(v) \mod (K^\times)^2$. Moreover, every element of $\mathcal{O}(V)$ can be written as a product of reflections (see Theorem (I.9.10)).

We want to apply the theory to compute the image of the map

$$(\det, \mathrm{spin}) : \mathcal{O}(V) \to \{+, -\} \times K^\times/(K^\times)^2.$$

in case $K = \mathbb{Q}$ or $\mathbb{Q}_p$.

PROPOSITION 6.1. *Let V be a quadratic vector space over K with $dim(V) \ge 3$.*

(6.1.1) If $K = \mathbb{Q}_p$ with $p \neq \infty$ then $(\det, \mathrm{spin})$ *is surjective.*
(6.1.2) If $K = \mathbb{Q}$ and V is indefinite, then $(\det, \mathrm{spin})$ *is surjective.*

PROOF. To prove the first statement, let $k = |\mathbb{Q}_p^\times/(\mathbb{Q}_p^\times)^2|$. Note that $k = 4$ if $p \neq 2$ and $k = 8$ if $p = 2$. By Corollary (3.3), there exist $v_1, \ldots, v_{k-1} \in V$ such that the values $a_i = Q(V_i)$ range over all but one of the cosets of $\mathbb{Q}_p^\times \mod (\mathbb{Q}_p^\times)^2$. In particular, $Q(v_i) \neq 0$ for any i, so the reflections τ_{v_i} are defined. In this case

$$(\det(\tau_{v_i}), \mathrm{spin}(\tau_{v_i})) = (-1, a_i)$$

and

$$(\det(\tau_{v_1}\tau_{v_i}), \mathrm{spin}(\tau_{v_1}\tau_{v_i})) = (1, a_1 a_i)$$

and these images are all distinct. Therefore the image of $(\det, \mathrm{spin})$ contains at least $2k - 2$ elements; since the image group $\{+, -\} \times \mathbb{Q}_p^\times/(\mathbb{Q}_p^\times)^2$ has $2k$ elements, and $k \geq 4$, the surjectivity follows.

To prove the second statement, let $d = \mathrm{disc}(V)$ and $c_p = c_p(V \otimes \mathbb{Q}_p)$. By Corollary (3.3), a rational number $a \in \mathbb{Q}$ fails to be represented by $V \otimes \mathbb{Q}_p$ if and only if $n = 3$, $a \equiv -d \mod (\mathbb{Q}_p^\times)^2$, and $(-1, -d)_p = -c_p$. But $(-1, -d)_p = 1$ and $c_p = 1$ for almost all p, by Lemmas (2.3.1) and (2.7), so that $(-1, -d)_p \neq -c_p$ for almost all p. Thus, there is a finite set S of primes (those for which $(-1, -d)_p = -c_p$) such that $a \in \mathbb{Q}^\times$ fails to be represented by $V \otimes \mathbb{Q}_p$, $p \neq \infty$, if and only if $p \in S$ and $a \equiv -d \mod (\mathbb{Q}_p^\times)^2$.

For any $a \in \mathbb{Q}^\times$, by the Chinese Remainder Theorem, we can find b and c in $\mathbb{Q}^\times$ such that $a = bc$ and $b, c \neq -d \mod (\mathbb{Q}_p^\times)^2$ for all $p \in S$. Therefore b and c are represented by $V \otimes \mathbb{Q}_p$ for all $p \neq \infty$; by Corollary (3.6), since V is indefinite, both b and c are represented by $V \otimes \mathbb{Q}_\infty$ as well. Hence by the Hasse-Minkowski Theorem (3.7), there exists v and w in V such that $Q(v) = b$ and $Q(w) = c$. In particular, $\mathrm{spin}(\tau_v\tau_w) = bc = a$. This shows that $\mathrm{spin} : \mathcal{O}^+(V) \to \mathbb{Q}^\times/(\mathbb{Q}^\times)^2$ (where $\mathcal{O}^+(V)$ is the kernel of the det map) is surjective. Since $\mathcal{O}(V) \neq \mathcal{O}^+(V)$, this proves that $(\det, \mathrm{spin})$ defined on all of $\mathcal{O}(V)$ is surjective as well. Q.E.D.

7. The strong approximation theorem for the spin group

Let (V, Q) be a quadratic vector space over K. For the fields $\mathbb{Q}$ and $\mathbb{Q}_p$, the $(\det, \mathrm{spin})$ map tends to be surjective, onto a well-understood group, by the results of the previous section. Therefore computations with the orthogonal group of (V, Q) can often be reduced to the kernel of $(\det, \mathrm{spin})$.

DEFINITION 7.1. Let R be an integral domain with quotient field K, and let (L, Q) be a quadratic R-module. Let $V = L \otimes_R K$, with the induced quadratic form, also denoted Q. Note that in this situation we may consider $L \subseteq V$, and also $\mathcal{O}(L) \subseteq \mathcal{O}(V)$, and hence both det and spin are defined on $\mathcal{O}(L)$. Define

$$\Theta(L) = \mathrm{Ker}(\det, \mathrm{spin}) : \mathcal{O}(L) \to \{+, -\} \times K^\times/(K^\times)^2.$$

$\Theta(L)$ is also denoted by $\Theta(L, Q)$ or $\Theta(Q)$.

The reader should not confuse $\Theta(L)$ with $\mathcal{O}_{++}(L)$, which was defined in Section (I.10) also as the kernel of $(\det, \mathrm{spin})$. That was a slightly different spin, only over the real numbers.

The Strong Approximation Theorem for the Spin Group can now be stated.

THEOREM 7.2. *Let L be an indefinite quadratic $\mathbb{Z}$-module, of rank at least 3. Let $V = L \otimes_{\mathbb{Z}} \mathbb{Q}$ be the induced quadratic vector space over $\mathbb{Q}$. For each $p \neq \infty$, let $\mathcal{V}_p$ be a nonempty open subset (in the p-adic topology) of $\Theta(V \otimes \mathbb{Q}_p)$ such that $\mathcal{V}_p = \Theta(L \otimes \mathbb{Z}_p)$ for almost all p. Then there is an isometry $\sigma \in \Theta(V)$ such that $\sigma \in \mathcal{V}_p$ for all p.*

A proof may be found in [**Cassels 78**, Chapter 10, Section 7].

CHAPTER VI

The Existence of Integral Quadratic Forms

1. The monoids $\mathcal{Q}$ and $\mathcal{Q}_p$

Recall that an *integral quadratic form* is a free finitely generated $\mathbb{Z}$-module L together with a $\mathbb{Z}$-valued quadratic form Q defined on L. (This is a *quadratic $\mathbb{Z}$-module*.) Let $\mathcal{Q}$ be the monoid of isomorphism classes of integral quadratic forms. (The operation in the monoid is direct sum.) There are two natural maps

$$\text{rank} : \mathcal{Q} \to \mathbb{N}$$

and

$$\text{disc} : \mathcal{Q} \to \mathbb{Z}$$

defined on $\mathcal{Q}$ as we have seen.

There is another more "discriminating" function on $\mathcal{Q}$ given by the discriminant-form construction. Let $\mathcal{T}$ be the monoid of isomorphism classes of torsion quadratic $\mathbb{Z}$-modules; these are finite abelian groups G together with a $\mathbb{Q}/\mathbb{Z}$-valued quadratic form q defined on G. The discriminant-form construction gives a natural map

$$d : \mathcal{Q} \to \mathcal{T}$$

which we have investigated in the p-adic context in Chapter IV.

Namely, recall that $\mathcal{Q}_p$ denotes the monoid of isomorphism classes of quadratic $\mathbb{Z}_p$-modules, and $\mathcal{T}_p$ denotes the monoid of isomorphism classes of torsion quadratic $\mathbb{Z}_p$-modules. We have a natural map

$$d : \mathcal{Q}_p \to \mathcal{T}_p$$

defined by the discriminant-form construction for each prime p.

By the Sylow splitting (Proposition (II.1.1)), the monoid $\mathcal{T}$ is naturally the direct sum of the monoids $\mathcal{T}_p$:

$$\mathcal{T} \cong \bigoplus_p \mathcal{T}_p.$$

In addition, localization gives a map $\mathcal{Q} \to \mathcal{Q}_p$ induced by sending an integral quadratic form L to $L \otimes_{\mathbb{Z}} \mathbb{Z}_p$. For each prime p we have the

obvious commutative diagram

$$\begin{array}{ccc} \mathcal{Q} & \to & \mathcal{Q}_p \\ d\downarrow & & d\downarrow \\ \mathcal{T} & \to & \mathcal{T}_p \end{array}$$

where the vertical arrows are the discriminant-form construction, the upper horizontal arrow is the localization map, and the lower horizontal arrow is the projection onto the p-Sylow part.

If we set $\mathbb{Z}_\infty = \mathbb{R}$, the real numbers, then most of this notation can be applied to the case $p = \infty$. Let $\mathcal{Q}_\infty$ be the monoid of isomorphism classes of real quadratic vector spaces. We have the natural localization map $\mathcal{Q} \to \mathcal{Q}_\infty$ induced by sending an integral quadratic form L to $L \otimes_{\mathbb{Z}} \mathbb{R}$. (There is no analogue $\mathcal{T}_\infty$ of the monoids $\mathcal{T}_p$.) We will often use $\mathbb{Q}_\infty$ rather than $\mathbb{Z}_\infty$ to denote $\mathbb{R}$, as is more standard.

Putting these localization maps together, we obtain a natural map

$$g : \mathcal{Q} \to \bigoplus_{\text{all } p} \mathcal{Q}_p,$$

where here "all p" means that $p = \infty$ is included. This map g is the *genus* map, and a *genus* is any element of $\bigoplus_{\text{all } p} \mathcal{Q}_p$ which is in the image of g.

In this chapter we will investigate the existence of integral quadratic forms with prescribed "local" data. In the standard treatment of the theory, "local" data means essentially the genus. Our point of view is that "local" data means the discriminant-form. The existence theorem from this point of view was first proved by Nikulin in [**Nikulin 80b**]; we give this theorem in section 5. The proof depends on the corresponding theorem over $\mathbb{Q}$ (Corollary (V.5.3)), and the analyses of discriminant-forms and p-adic integral quadratic forms given in Chapters II, III, and IV.

2. The surjectivity of $\mathcal{Q} \to \mathcal{T}$

We begin the study of the existence of integral quadratic forms by showing in this section that any torsion quadratic form over $\mathbb{Z}$ (that is, a finite abelian group with a $\mathbb{Q}/\mathbb{Z}$-valued quadratic form on it) is, up to isomorphism, the discriminant-form of some integral quadratic form. In other words, we will show that the map $d : \mathcal{Q} \to \mathcal{T}$ is surjective. We begin with the following lemma.

LEMMA 2.1. *Fix $a_0, a_1, \ldots, a_m$ in $\mathbb{Q}$. Define $d_m = a_m$, $d_{m-1} = a_{m-1}d_{m-2} - 1$, and $d_{i-2} = a_{i-2}d_{i-1} - d_i$ for $2 \le i \le m$. Then the*

determinant of the tridiagonal matrix

$$\begin{pmatrix} a_0 & 1 & 0 & & & \\ 1 & a_1 & 1 & 0 & & \\ 0 & 1 & a_2 & & & \\ & & & \ddots & & \\ & & 0 & 1 & a_{m-1} & 1 \\ & & & 0 & 1 & a_m \end{pmatrix}$$

with the a_i's on the diagonal, 1's on the sub- and super-diagonals, and 0's elsewhere, is d_0.

PROOF. This is a straightforward induction on m. If $m = 0$ or $m = 1$, the result is clear. Assume then that $m \geq 2$ and that the result is true for all sizes less than m. Denote the above tridiagonal matrix by $[a_0, a_1, \ldots, a_m]$. By expanding the determinant along the first row, we see that

$$\begin{aligned} \det[a_0, a_1, \ldots, a_m] &= a_0 \det[a_1, \ldots, a_m] - \det[a_2, \ldots, a_m] \\ &= a_0 d_1 - d_2 \text{ by the inductive hypothesis} \\ &= d_0 \text{ by definition.} \end{aligned}$$

Q.E.D.

We begin by exhibiting integral qudratic forms whose discriminant-forms are equal to the cyclic generators of $\mathcal{T}_p$.

LEMMA 2.2. *Fix a prime p, and an integer $k \geq 1$. Then for any ε ($= \pm 1$ if p is odd, $= 1, 3, 5, 7$ if $p = 2$) there exists an integral quadratic form L whose discriminant-form represents $w_{p,k}^{\varepsilon}$.*

PROOF. Let $G = \mathbb{Z}/|^{\urcorner}$, and define the $\mathbb{Q}/\mathbb{Z}$-valued quadratic form q on G by setting $q(1) = p^{-k}n/2$, where $(n, p) = 1$, $|n| < p^k$, and n is even if p is odd. Any $w_{p,k}^{\varepsilon}$ is represented by such a q, and we will produce an integral quadratic form (L, Q) with discriminant-form $(G_L, q_L) \cong (G, q)$.

Write $1 = nd_1 - p^k d_2$; since $|n| < p^k$, we must have $|d_2| < |d_1|$. Certainly d_1 and d_2 cannot both be even. If they are both odd, then since n and p have opposite parity we may replace d_1 by $d_1 + p^k$ and d_2 by $d_2 + n$ to make one even and one odd. Therefore we may assume that d_1 and d_2 have opposite parity. Set $d_0 = p^{-k}$ and $a_0 = p^{-k}n$; then $d_0 = a_0 d_1 - d_2$. Recursively define sequences (a_i) and (d_i) as follows.

Given d_i and d_{i+1} with $|d_{i+1}| > 1$, choose the even number a_i so that $a_i d_{i+1}$ is the closest even multiple of d_{i+1} to d_i, and set $d_{i+2} = a_i d_{i+1} - d_i$. In this case note that

(a) $d_i = a_i d_{i+1} - d_{i+2}$
(b) $0 \neq |d_{i+2}| < |d_{i+1}|$
(c) the parity of d_i is that of d_{i+2}.

If $|d_{i+1}| = 1$, set $a_i = d_i$ and stop.

By (b) above, this construction ends, and produces sequences $(a_0, \dots, a_m)$ and $(d_0, \dots, d_m)$ ($d_{m+1} = \pm 1$). Also, since d_1 and d_2 have opposite parity, the parity of the integers d_i (for $i > 0$) alternate, by (c). Hence the last members $a_m = d_m$ are even, since d_{m+1} is odd; therefore each a_i is even, for $i \geq 1$.

Let $L^\#$ be the free $\mathbb{Z}$-module with basis $\{e_0^\#, \dots, e_m^\#\}$. Define a symmetric $\mathbb{Q}$-valued bilinear form $\langle -, - \rangle$ on $L^\#$ by setting the matrix $A^\# = (\langle e_i^\#, e_j^\# \rangle)$ equal to the tridiagonal matrix $[a_0, a_1, \dots, a_m]$ (using the notation of Lemmma (2.1)). By Lemma (2.1), the determinant of $A^\#$ is $d_0 = p^{-k}$, using (a) above. Hence by Cramer's Rule, the inverse A of $A^\#$ is integral, since every maximal minor of $A^\#$ has determinant s/p^k for some $s \in \mathbb{Z}$. (The only non-integral entry of $A^\#$ is the upper left corner entry a_0.)

Let L be the dual module to $L^\#$, i.e., $L = \{x \in L^\# \otimes \mathbb{Q} | \langle \curvearrowleft, \curvearrowright \rangle \in \mathbb{Z}$ for all $y \in L^\#\}$. By Lemma (II.7.8), the matrix of the induced bilinear form on L is A. Note that a basis for L over $\mathbb{Z}$ is $\{e_0, \dots, e_m\}$, where $e_0 = p^k e_0^\#$ and $e_i = e_i^\#$ for $i > 0$.

We next note that the matrix A has all even entries on its main diagonal. Indeed, if $i > 0$, then $\langle e_i, e_i \rangle = a_i$ and is therefore even. For the upper left entry, we have that $\langle e_0, e_0 \rangle = \langle p^k e_0^\#, p^k e_0^\# \rangle = p^k n$, which is even if p is odd since then n is even, and is obviously even if $p = 2$.

Therefore the bilinear form $\langle -, - \rangle$ on L comes from a unique $\mathbb{Z}$-valued quadratic form Q, (defined by $Q(x) = \langle x, x \rangle / 2$), and the pair (L, Q) is an integral quadratic form. The discriminant-form group $L^\#/L$ is generated by the class of $e_0^\#$, and has order p^k. Its quadratic form q_L is determined by $q_L(e_0^\# \mod L) = Q(e_0^\#) \mod \mathbb{Z} = \langle \overset{\#}{\curvearrowleft}, \overset{\#}{\curvearrowleft} \rangle / \not\Vdash \mod \mathbb{Z} = \supset_{\curvearrowleft} / \not\Vdash \mod \mathbb{Z} = \shortmid^{-} \urcorner \ltimes / \not\Vdash \mod \mathbb{Z}$. Thus $(G_L, q_L) \cong (G, q)$ as desired. Q.E.D.

The rank two indecomposable torsion forms over $\mathbb{Z}_2$ are obtainable as follows.

Lemma 2.3.

(2.3.1) The rank 2 integral form (L, Q) defined by $Q(x, y) = 2^k xy$ has u_k as discriminant-form.

(2.3.2) The rank 4 integral form (L, Q) defined by $Q(x, y, z, w) = 2^k x^2 + 2^k y^2 + az^2 + bw^2 + 2^k xy + 2^k yz + zw$, where $a = (2^k - (-1)^k)/3$ and $b = (-1)^{k-1}$, has v_k as discriminant-form.

PROOF. In the first case the dual module $L^{\#}$ is easily seen to be generated by $f_1 = (2^{-k}, 0)$ and $f_2 = (0, 2^{-k})$, and the result follows directly. In the second case, the determinant of the matrix of the form is exactly 2^{2k}, and it is easy to see that $f_1 = (2^{-k}, 0, 0, 0)$ and $f_2 = (0, 2^{-k}, 0, 0)$ are in the dual lattice $L^{\#}$. Therefore the dual lattice is generated by f_1, f_2, $(0, 0, 1, 0)$, and $(0, 0, 0, 1)$ (there is no more room left for anything bigger), and so the discriminant-form group G_L is generated by the image of f_1 and f_2. The reader can now easily check that the induced form q_L on G_L represents v_k. Q.E.D.

Since the forms $w^{\varepsilon}_{p,k}$, u_k, and v_k generate the monoids $\mathcal{T}_p$, and since $\mathcal{T} = \bigoplus_p \mathcal{T}_p$, the above lemmas suffice to prove the desired surjectivity result:

THEOREM 2.4. *The map $d : \mathcal{Q} \to \mathcal{T}$ is surjective.*

3. Hasse invariants for Integral p-adic Quadratic Forms

In this section, we compute the Hasse invariants (defined in Chapter V, section 2) for the unimodular p-adic integral quadratic forms, i.e., the unimodular quadratic $\mathbb{Z}_p$-modules. If L is a quadratic $\mathbb{Z}_p$-module, define its Hasse invariant $c_p(L) = c_p(L \otimes \mathbb{Q}_p)$.

PROPOSITION 3.1. *Let L be a unimodular p-adic integral quadratic form.*

(3.1.1) If p is odd, then $c_p(L) = 1$.

(3.1.2) If $p = 2$, write $L \cong U_0^{\oplus n} \oplus V_0^{\oplus m}$ with $m \leq 1$. Then $c_2(L) = (-1)^{m(n+1)+\binom{n}{2}}$.

PROOF. To prove the first statement, we use induction on the rank. Since any 1-dimensional form has Hasse invariant 1, the formula holds if L has rank 1.

If L has rank at least 2, then we may write $L \cong W^{\varepsilon}_{p,0} \oplus L'$ with $\varepsilon = \pm 1$ and $\operatorname{rank}(L') = \operatorname{rank}(L) - 1$. Let $d = \operatorname{disc}(W^{\varepsilon}_{p,0})$ and $d' = \operatorname{disc}(L')$. Then by Lemma (V.2.5),

$$c_p(L) = c_p(W^{\varepsilon}_{p,0}) c_p(L')(d, d')_p.$$

The first term on the right is 1 since the rank of the form is one, and the second term is 1 by the inductive hypothesis. Finally, the third term is also 1 by Lemma (V.2.2), since both d and d' are prime to p.

To prove the second statement, we use induction on n; we must start by computing $c_2(U_0)$ and $c_2(V_0)$.

U_0 has matrix $\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$, so that $U_0 \otimes \mathbb{Q}_2$ is equivalent to a form with matrix $\begin{pmatrix} 2 & 0 \\ 0 & -2 \end{pmatrix}$; hence, $\mathrm{disc}(U_0) = -1$ and $c_2(U_0) = (2,-2)_2 = 1$.

V_0 has matrix $\begin{pmatrix} 2 & 1 \\ 1 & 2 \end{pmatrix}$, so that $V_0 \otimes \mathbb{Q}_2$ is equivalent to a form with matrix $\begin{pmatrix} 2 & 0 \\ 0 & 6 \end{pmatrix}$; hence, $\mathrm{disc}(V_0) = 3$ and $c_2(V_0) = (2,6)_2 = -1$.

Therefore the result is true when $n = 0$. Assume the results holds for $n-1$, and let us show it for n. Let $L \cong U_0^{\oplus n} \oplus V_0^{\oplus m}$, with $m \leq 1$. Let $L' = U_0^{\oplus(n-1)} \oplus V_0^{\oplus m}$, so that $L \cong U_0 \oplus L'$. Then by Lemma (V.2.5),

$$\begin{aligned} c_2(L) &= c_2(U_0)c_2(L')(-1,(-1)^{n-1}3^m)_2 \\ &= 1 \cdot (-1)^{mn+\binom{n-1}{2}}(-1,-1)_2^{n-1}(-1,3)_2^m \end{aligned}$$

which gives the desired result after noting that $(-1,-1)_2 = (-1,3)_2 = -1$.

Q.E.D.

4. Localization of $\mathbb{Z}$-modules

In this section, we study a pair of free $\mathbb{Z}$-modules inside a fixed vector space over $\mathbb{Q}$, and show the extent to which they are determined by local data. The theorem we desire is the following.

THEOREM 4.1. *Let Λ be a free $\mathbb{Z}$-module of finite rank.*

(4.1.1) Suppose that there is a $\mathbb{Z}$-module $L \subset \Lambda \otimes \mathbb{Q}$ such that $L \otimes \mathbb{Q} = \Lambda \otimes \mathbb{Q}$. Then for almost all p, $L \otimes \mathbb{Z}_p = \Lambda \otimes \mathbb{Z}_p$.

(4.1.2) Suppose one is given $\mathbb{Z}_p$-modules $L_p \subset \Lambda \otimes \mathbb{Q}_p$ for all p, such that

(a) *$L_p \otimes \mathbb{Q}_p = \Lambda \otimes \mathbb{Q}_p$ for all p, and*

(b) *$L_p = \Lambda \otimes \mathbb{Z}_p$ for almost all p.*

Then there is a $\mathbb{Z}$-module $L \subset \Lambda \otimes \mathbb{Q}$ such that $L \otimes \mathbb{Z}_p = L_p$ for all p.

PROOF. The first statement is easy: let $\{x_1, \ldots, x_n\}$ and $\{y_1, \ldots, y_n\}$ be bases of L and Λ repsectively. Then there exist $a_{ij} \in \mathbb{Q}$ with $\det(a_{ij}) \neq 0$ and $x_i = \sum_j a_{ij} y_j$ for each i. If p is any prime such that $a_{ij} \in \mathbb{Z}_p$ and $\det(a_{ij}) \in \mathbb{U}_{\text{ı}}$, then $L \otimes \mathbb{Z}_p = \Lambda \otimes \mathbb{Z}_p$; this holds for almost all p.

To see the second statement, note that without loss of generality we may assume that $L_p \subset \Lambda \otimes \mathbb{Z}_p$ for all p, by replacing Λ by $a\Lambda$ for a suitable rational number $a \in \mathbb{Q}$.

Since $\Lambda \cap L_p = \Lambda \cap (\Lambda \otimes \mathbb{Z}_p) = \Lambda$ for almost all p, the intersection $\bigcap_p (\Lambda \cap L_p)$ is actually an intersection of finitely many $\mathbb{Z}$-modules; let $L = \bigcap_p (\Lambda \cap L_p)$.

There are non-negative integers $e(p)$, defined by each prime p, which are almost all 0, such that $p^{e(p)}(\Lambda \otimes \mathbb{Z}_p) \subset L_p$. Thus if we let $k = \prod_p p^{e(p)}$, we have $k\Lambda \subset L \subset \Lambda$ so that L is a free $\mathbb{Z}$-module with $L \otimes \mathbb{Q} = \Lambda \otimes \mathbb{Q}$.

By definition, $L \otimes \mathbb{Z}_p \subset L_p$ for each p. Thus, we must only show that $L_p \subset L \otimes \mathbb{Z}_p$ for each p. For this, it is enough to show that for every $x \in L_p$ and for every $\epsilon > 0$, there is a $y \in L$ such that $\| x - y \|_p < \epsilon$. Therefore fix p, and such an x and an ϵ.

Let $\{x_1, \ldots, x_n\}$ be a basis for Λ, and write $x = \sum_i a_i x_i$ where $a_i \in \mathbb{Z}_p$ since $L_p \subset \Lambda \otimes \mathbb{Z}_p$. Let $N > \max(e(p), \log_p(\sqrt{n}/\epsilon))$. By the Chinese Remainder Theorem, there exist integers $b_1, \ldots, b_n$ such that

$$b_i \equiv a_i \mod p^N$$

and

$$b_i \equiv 0 \mod q^{e(q)} \text{ for all } q \neq p.$$

(This is only finitely many conditions since $e(q) = 0$ for almost all q.)

Let $y = \sum_i b_i x_i$. Then $y \in \Lambda$ since $b_i \in \mathbb{Z}$, and for every $q \neq p$, $y \in q^{e(q)}(\Lambda \otimes \mathbb{Z}_q) \subset L_q$. Also, $x - y \in p^{e(p)}(\Lambda \otimes \mathbb{Z}_p) \subset L_p$ so that $y \in L_p$ since $x \in L_p$. Thus, by the definition of L, $y \in L$.

On the other hand,

$$\| x - y \|_p^2 = \sum \| a_i - b_i \|_p^2 \leq n p^{-2N} < \epsilon^2.$$

Q.E.D.

5. Nikulin's Existence Theorem

In this section we formulate a necessary and sufficient condition on a signature, discriminant, and discriminant-form, to guarantee the existence of an integral quadratic form having that signature, discriminant, and discriminant-form.

Recall that if L is an integral quadratic form, with discriminant-form group $G_L = L^\#/L$, and $\text{sign}(L) = (s_+, s_-)$, then $\text{disc}(L) = (-1)^{s_-}|G_L|$.

If (G, q) is any torsion quadratic form over $\mathbb{Z}$, we will denote by (G_p, q_p) the induced torsion quadratic form over $\mathbb{Z}_p$ on the p-Sylow subgroup G_p of G.

If (G_p, q_p) is a torsion quadratic form over $\mathbb{Z}_p$, denote by $L(q_p)$ a quadratic $\mathbb{Z}_p$-module with discriminant-form isomorphic to (G_p, q_p) and $\text{rank}(L(q_p)) = \ell(G_p)$. $L(q_p)$ is unique up to isomorphism if p is

odd, or if $p = 2$ and $w_{2,1}^{\varepsilon}$ does not split off q_p for any ε, by Corollaries (IV.2.10) and (IV.5.6). If $p = 2$ and $w_{2,1}^{\varepsilon}$ does split off q_2, we will write $L(q_2)$ for either of the two quadratic $\mathbb{Z}_2$-modules which are possible; this ambiguity should not cause any confusion in what follows. Recall that in this case $\mathrm{disc}(L(q_2))$ is well-defined up to multiplication by 5, mod $\mathbb{U}_{\not\equiv}^{\not\equiv}$, by Corollary (IV.5.6).

Using this terminology, we have the following necessary conditions for the existence of an integral quadratic form. Recall that $\ell(G)$ is the length of a finite abelian group, and $\gamma_L(1)$ is one of the Gauss sum invariants of an integral quadratic form, defined in Chapter 3.

PROPOSITION 5.1. *Let L be an integral quadratic form with discriminant-form (G, q), and with signature* $\mathrm{sign}(L) = (s_+, s_-)$. *Let* $r = \mathrm{rank}(L) = s_+ + s_-$. *Then*

(5.1.1) $r \geq \ell(G)$.

(5.1.2) If $s = s_+ - s_-$, *then* $\gamma_L(1) = \exp(\pi i s/4)$.

(5.1.3) If $r = \ell(G_p)$, *and if either p is odd, or if $p = 2$ and $w_{2,1}^{\varepsilon}$ does not split off q_2, then* $(-1)^{s_-}|G| = \mathrm{disc}(L(q_p))(\mod \mathbb{U}_{\shortmid}^{\not\equiv})$.

(5.1.4) If $r = \ell(G_p)$, $p = 2$, *and* $w_{2,1}^{\varepsilon}$ *does split off* q_2, *then* $(-1)^{s_-}|G| = \mathrm{disc}(L(q_2))(\mod (5, \mathbb{U}_{\shortmid}^{\not\equiv}))$.

PROOF. Since $G = L^{\#}/L$, it is generated by the classes of a basis for $L^{\#}$; since L and $L^{\#}$ have the same rank r, the first statement follows. The second statement is Milgram's Theorem, Theorem (III.5.1).

If $r = \ell(G_p)$, then $L_p = L \otimes \mathbb{Z}_p$ has rank $r = \ell(G_p)$, with discriminant-form (G_p, q_p); therefore $L_p \cong L(q_p)$, and so $\mathrm{disc}(L_p) = \mathrm{disc}(L(q_p))(\mod \mathbb{U}_{\shortmid}^{\not\equiv}$ in the situation of (5.1.3) and $\mod (5, \mathbb{U}_{\shortmid}^{\not\equiv})$ in the situation of (5.1.4). Since $\mathrm{disc}(L_p) = \mathrm{disc}(L) \mod \mathbb{U}_{\shortmid}^{\not\equiv} = (-\not\equiv)^{\sim -}|\mathbb{G}|$, the last two statements follow. Q.E.D.

Nikulin's Existence Theorem is essentially a converse to the above Proposition. It turns out that conditions (5.1.3) and (5.1.4) can be weakened slightly. The statement follows.

THEOREM 5.2. *Fix a pair of nonegative integers* $(s_+, s_-) \in \mathbb{N}^{\not\equiv}$, *and a torsion quadratic form (G, q) over $\mathbb{Z}$. Then there exists an integral quadratic form L such that* $\mathrm{sign}(L) = (s_+, s_-)$, *with discriminant-form isomorphic to (G, q), if and only if the following conditions are satisfied:*

(5.2.1) $r = s_+ + s_- \geq \ell(G)$.

(5.2.2) $\gamma_q(1) = \exp(\pi i(s_+ - s_-)/4)$.

(5.2.3) If p is odd and $r = \ell(G_p)$, then $(-1)^{s_-}|G| = \mathrm{disc}(L(q_p))(\mod \mathbb{U}_{\shortmid}^{\not\equiv})$.

(5.2.4) If $r = \ell(G_2)$ and $w^{\varepsilon}_{2,1}$ does not split off q_2 for any ε, then $|G| = \pm \operatorname{disc}(L(q_p))(\mod \mathbb{U}^{\not\rightleftharpoons})$.

PROOF. The necessity follows from the previous Proposition. Note that if we assume that the theorem is true, it follows that the above 4 conditions imply the (a priori) stronger conditions of the Proposition. This can be checked directly also, which we will leave as an exercise for the reader.

It remains to demonstrate the sufficiency of the conditions. By Theorem (2.4), there is an integral quadratic form E with discriminant-form (G, q). The problem with E is that its signature $\operatorname{sign}(E) = (e_+, e_-)$ may be wrong. Let U be hyperbolic plane over $\mathbb{Z}$; recall that this is the rank 2 integral quadratic form whose matrix is $\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$. Recall also that $\operatorname{disc}(U) = -1$ and $\operatorname{sign}(U) = (1, 1)$, so that U is unimodular and, for any $k \geq 1$, $\operatorname{sign}(E \oplus U^{\oplus k}) = (e_+ + k, e_- + k)$.

Choose k such that $e_+ + k \equiv s_+ \mod 8$, $e_- + k \equiv s_- \mod 8$, and $e_+ + e_- + 2k \geq r = s_+ + s_-$. (This is possible because of the Gauss sum condition (5.2.2).) Set $M = E \oplus U^{\oplus k}$, and write $m_\pm = e_\pm + k$, so that $\operatorname{sign}(M) = (m_+, m_-)$. Therefore

(i) $m_+ \equiv s_+ \mod 8$ and $m_- \equiv s_- \mod 8$,
(ii) $\operatorname{rank}(M) = m_+ + m_- \geq r$, and
(iii) the discriminant-form (G_M, q_M) of M is isomorphic to (G, q), and $m_+ - m_- \equiv s_+ - s_- \mod 8$, so that $\gamma_q(1) = \exp(\pi i(m_+ - m_-)/4)$.

For each prime p, write $M_p = M \otimes \mathbb{Z}_p$. By Corollaries (IV.2.10) and (IV.5.6) and the classification of unimodular quadratic $\mathbb{Z}_p$-modules, we may write

$$M_p = (W^1_{p,0})^{\oplus \alpha_p} \oplus (W^{-1}_{p,0})^{\oplus \beta_p} \oplus L(q_p)$$

if p is odd, and

$$M_2 = (U_0)^{\oplus \alpha_2} \oplus (V_0)^{\oplus \beta_2} \oplus L(q_2),$$

where $\alpha_p \geq 0$ and $\beta_p = 0$ or 1 for each p. Moreover we may assume that

(iv) $\beta_2 = 0$ if $w^{\varepsilon}_{2,1}$ splits off q_2 for some ε,

by using relation VIII of Proposition (IV.3.1) if necessary. (Note that this switches $L(q_2)$ in the above expression for M_2.)

Set

$$\gamma_p = r - \ell(G_p) - \beta_p = r - \operatorname{rank}(M) + \alpha_p$$

if p is odd, and

$$\gamma_2 = (r - \ell(G_2) - 2\beta_2)/2 = (r - \operatorname{rank}(M) + 2\alpha_2)/2$$

Since $\ell(G_2) = \operatorname{rank}(L(q_2))$, the quantity $r - \ell(G_2) - 2\beta_2 = r - \operatorname{rank}(M) + 2\alpha_2$ is even by (i); therefore γ_p is an integer for all p. In addition

(v) $\gamma_p \equiv \alpha_p \mod 8$ if p is odd, and $\gamma_2 \equiv \alpha_2 \mod 4$ if $p = 2$,

by (i).

We will next show that $\gamma_p \geq 0$ for all p. Since $r \geq \ell(G) \geq \ell(G_p)$ for all p by (5.2.1), and since $\beta_p \leq 1$ for all p, the only way that γ_p could be negative is if $r = \ell(G_p)$ and $\beta_p = 1$. Therfore fix a prime p and assume that $r = \ell(G_p)$; we will show that $\beta_p = 0$. This follows from a discriminant calculation.

If p is odd, fix a non-square $a \in \mathbb{U}_{\text{ı}}$. Then

$$\begin{aligned} \operatorname{disc}(L(q_p)) &= (-1)^{s_-}|G| \mod \mathbb{U}_{\text{ı}}^{\not\square} \text{ by (5.2.3)} \\ &= (-1)^{m_-}|G| \mod \mathbb{U}_{\text{ı}}^{\not\square} \text{ by (i)} \\ &= \operatorname{disc}(M) \mod \mathbb{U}_{\text{ı}}^{\not\square} \text{ by (iii)} \\ &= \operatorname{disc}(M_p) = a^{\beta_p} \operatorname{disc}(L(q_p)) \end{aligned}$$

by the decomposition of M_p. Therefore $a^{\beta_p} = 1 \mod \mathbb{U}_{\text{ı}}^{\not\square}$, forcing β_p to be even, hence 0.

If $p = 2$ and $w_{2,1}^{\varepsilon}$ splits off q_2, then $\beta_2 = 0$ by the assumption (iv).

Finally, if $p = 2$ and $w_{2,1}^{\varepsilon}$ does not split off q_2, then

$$\begin{aligned} \operatorname{disc}(L(q_2)) &= \pm|G| \mod \mathbb{U}_{\not\square}^{\not\square} \text{ by (5.2.4)} \\ &= \pm \operatorname{disc}(M) \mod \mathbb{U}_{\not\square}^{\not\square} \text{ by (iii)} \\ &= \pm \operatorname{disc}(M_2) = \pm(-1)^{\alpha_2} 3^{\beta_2} \operatorname{disc}(L(q_2)) \end{aligned}$$

by the decomposition of M_2. Note that these are all equalities $\mod \mathbb{U}_{\not\square}^{\not\square}$, not also $\mod 5$, since we have fixed $L(q_2)$ throughout. Therefore $(-1)^{\alpha_2} 3^{\beta_2} = \pm 1 \mod \mathbb{U}_{\not\square}^{\not\square}$, again forcing β_2 to be even, hence 0.

This proves that $\gamma_p \geq 0$ for all p.

Now define quadratic $\mathbb{Z}_p$-modules L_p for each p by setting

$$L_p = (W_{p,0}^{1})^{\oplus \gamma_p} \oplus (W_{p,0}^{-1})^{\oplus \beta_p} \oplus L(q_p)$$

if p is odd, and

$$L_2 = (U_0)^{\oplus \gamma_2} \oplus (V_0)^{\oplus \beta_2} \oplus L(q_2),$$

where we use the same $L(q_2)$ as in the decomposition of M_2.

These quadratic $\mathbb{Z}_p$-modules will be isomorphic to the localizations of the desired integral quadratic form L. Note that the discriminant-form of L_p is (G_p, q_p), and $\operatorname{rank}(L_p) = r$, for all p. Set $d = (-1)^{s_-}|G|$; then $d = (-1)^{s_-} d$. Moreover, if p is odd,

$$\operatorname{disc}(L_p) = \operatorname{disc}(M_p) = (-1)^{m_-}|G| = (-1)^{s_-}|G| = d(\mod \mathbb{U}_{\text{ı}}^{\not\square}),$$

and if $p = 2$,

$$\begin{aligned} \operatorname{disc}(L_2) &= (-1)^{\alpha_2-\gamma_2}\operatorname{disc}(M_2) \text{ since } \operatorname{disc}(U_0) = -1 \\ &= \operatorname{disc}(M_2) \text{ by (v)} \\ &= (-1)^{s_-}|G| = d \mod \mathbb{U}_{\not\in}^{\not\in} \text{ as above.} \end{aligned}$$

Hence

(vi) $\operatorname{disc}(L_p) = d \mod \mathbb{U}_{\dagger}^{\not\in}$ for every $p \neq \infty$.

The Hasse invariants of these L_p's can be calculated using Lemma (V.2.5) and Proposition (3.1).

If p is odd, then

$$\begin{aligned} c_p(L_p) &= c_p((W_{p,0}^1)^{\oplus(\alpha_p-\gamma_p)} \oplus M_p) \\ &= c_p((W_{p,0}^1)^{\alpha_p-\gamma_p})c_p(M_p)(1, \operatorname{disc}(M_p))_p \\ &= c_p(M_p). \end{aligned}$$

If $p = 2$,

$$\begin{aligned} c_2(L_2) &= c_2(U_0^{\oplus(\alpha_2-\gamma_2)} \oplus M_2) \\ &= c_2(U_0^{\oplus(\alpha_2-\gamma_2)})c_2(M_2)((-1)^{\alpha_2-\gamma_2}, \operatorname{disc}(M_2))_2 \\ &= c_2(M_2) \text{ since } \alpha_2 - \gamma_2 \equiv 0 \mod 4. \end{aligned}$$

Therefore for each p we have $c_p(L_p) = c_p(M_p)$. Hence

(vii) $c_p(L_p) = 1$ for almost all p

since this is true of the $c_p(M_p)$ by Lemma (V.2.7). Finally, we have

(viii) $(-1)^{\binom{s_-}{2}} \prod_{p\neq\infty} c_p(L_p) = 1$

since this is true for the $c_p(M_p)$, and $s_- \equiv m_- \mod 8$.

The statements (vi), (vii), and (viii) are precisely the hypotheses of Corollary (V.5.3). Hence, there is a quadratic vector space (V, Q) over $\mathbb{Q}$ such that $\operatorname{rank}(V) = r$, $\operatorname{disc}(V) = d \mod (\mathbb{Q}^\times)^{\not\in}$, and $\operatorname{sign}(V) = (s_+, s_-)$. Moreover, there are isometries $\sigma_p : V \otimes \mathbb{Q}_p \to L_p \otimes \mathbb{Q}_p$ for each $p < \infty$.

Let Λ be any $\mathbb{Z}$-module in V such that $\Lambda \otimes \mathbb{Q} = \mathbb{V}$, and define

$$L'_p = \begin{cases} \Lambda \otimes \mathbb{Z}_p \text{ if both } L_p \text{ and } \Lambda \otimes \mathbb{Z}_p \text{ are unimodular} \\ \sigma_p^{-1}(L_p) \text{ if not.} \end{cases}$$

Since $\operatorname{disc}(L_p) \equiv d \equiv \operatorname{disc}(\Lambda \otimes \mathbb{Z}_p) \mod (\mathbb{Q}_p^\times)^2$ for all p, if L_p and $\Lambda \otimes \mathbb{Z}_p$ are both unimodular then $L_p \cong \Lambda \otimes \mathbb{Z}_p$; in particular, the discriminant-forms of L'_p and of L_p are isomorphic for all $p < \infty$.

Since $L'_p \otimes \mathbb{Q}_p = \Lambda \otimes \mathbb{Q}_p$ for all p, by Theorem (4.1) there is a $\mathbb{Z}$-module $L \subset V$ such that $L \otimes \mathbb{Z}_p = L'_p$ for every p. When the form Q on V is restricted to L, it is $\mathbb{Z}$-valued, since the induced form on

L'_p is $\mathbb{Z}_p$-valued for every p. Moreover, $\text{sign}(L) = \text{sign}(V) = (s_+, s_-)$. Finally, the discriminant-form q_L of L is

$$q_L = \bigoplus_p q_{L\otimes\mathbb{Z}_p} = \bigoplus_p q_{L'_p} = q$$

as desired. Therefore L is the required integral quadratic form. Q.E.D.

6. The Genus

In this section we wish to remark that the two invariants, the signature $\text{sign}(L)$ and the discriminant-form (G_L, q_L), determine the genus of an integral quadratic form. Recall that the genus of L is the collection $\{L \otimes \mathbb{Z}_p\}$ of quadratic $\mathbb{Z}_p$-modules, for all p (including $p = \infty$), up to isomorphism.

By Sylvester's Theorem, $\text{sign}(L)$ determines $L \otimes \mathbb{Z}_\infty = L \otimes \mathbb{R}$, and the rank r of $L \otimes \mathbb{Z}_p$ for all p. Since $\text{disc}(L \otimes \mathbb{Z}_p) = (-1)^{s-}|G_L|$ and $q_{L\otimes\mathbb{Z}_p} = (q_L)_p$, both of these invariants of $L \otimes \mathbb{Z}_p$ are dtermined. Therefore, by Theorem (5.2), we have the following.

THEOREM 6.1. *The invariants* $\text{sign}(L)$ *and* (G_L, q_L) *determine the genus of an integral quadratic form* L*, and conversely.*

It is in this sense that we consider these invariants, the signature and the discriminant-form, to be "local" data for an integral quadratic form: they are equivalent to the data of the genus. There are two advantages to this approach. Firstly, the data is more compactly represented, and secondly, in many situations the signature and discriminant-form come more readily from other given data without further calculation.

CHAPTER VII

Local Orthogonal Groups

1. The Cartan-Dieudonné Theorem Recalled

In this chapter, we study the orthogonal group $\mathcal{O}(L)$ of a free quadratic $\mathbb{Z}_p$-module L. One of our goals is to give an analogue of the Cartan-Dieudonné Theorem I.9.10 for this group (and for certain subgroups of it). We begin by recalling the statement of that theorem over a field K of characteristic not 2; the proof motivates many of the calculations which follow.

Recall that if (V, Q) is a quadratic form space over K, and $v \in V$ is anisotropic, then V gives rise to $\tau_v \in \mathcal{O}(V)$, called the *reflection in* V, defined as follows:

$$\tau_v(w) = w - \frac{\langle v, w\rangle}{Q(v)}v = w - \frac{2\langle v, w\rangle}{\langle v, v\rangle}v$$

for all $w \in V$.

THEOREM 1.1 (Cartan-Dieudonné).

(1.1.1) Let (V, Q) be a quadratic form space over a field K of characteristic not 2. Let $v, w \in V$ with $Q(v) = Q(w) \neq 0$. Then at least one of τ_{v-w} and $\tau_{v+w}\tau_v$ is well-defined, and gives an element $\sigma \in \mathcal{O}(V)$ such that $\sigma(v) = w$.

(1.1.2) The orthogonal group $\mathcal{O}(V)$ is generated by reflections.

We recall that the Cartan-Dieudonné theorem was used to define the *spinor norm*, a homomorphism

$$\mathrm{spin}\colon \mathcal{O}(V) \to K^*/(K^*)^2$$

as follows: if $\rho \in \mathcal{O}(V)$, write

$$\rho = \tau_{v_1} \dots \tau_{v_r}$$

for suitable anisotropic vectors $v_1, \dots, v_r$. Then

$$\mathrm{spin}(\rho) = Q(v_1) \dots Q(v_r) \bmod (K^*)^2.$$

If R is an integral domain with quotient field K, and (L, Q) is a quadratic R-module, then $(L \otimes K, Q)$ is quadratic vector space over K

and there is a natural inclusion

$$\mathcal{O}(L,Q) \subset \mathcal{O}(L \otimes K, Q).$$

We define

$$\operatorname{spin}\colon \mathcal{O}(L,Q) \to K^*/(K^*)^2$$

by restriction; note that to compute $\operatorname{spin}\rho$ for $\rho \in \mathcal{O}(L,Q)$ we must factor ρ into a product of reflections inside $\mathcal{O}(L \otimes K, Q)$; such a factorization may not be possible in $\mathcal{O}(L,Q)$ itself.

We note at this juncture that if (L,Q) is a quadratic R-module with associated bilinear form $\langle -,- \rangle$, then the set of automorphisms of L preserving the quadratic form Q is exactly the same set as those preserving the bilinear form $\langle -,- \rangle$. Hence from this point of view there is no particular advantage to having the quadratic form available. Indeed, it is somewhat artificial to restrict oneself to studying orthogonal groups of only quadratic forms; this is equivalent to studying the orthogonal groups of the even bilinear forms. We have seen that the even-ness of the bilinear form, which allows the definition of the quadratic form, is of real importance in other areas. However for orthogonal groups this is less so, for a simple reason: one can expand, or scale, an odd bilinear form by 2 and make it even, without changing the orthogonal group. Conversely, if all values of the bilinear form are even, (so that the bilinear form is even, and is induced by a quadratic form), then one may divide all the values by 2, to produce a possibly odd bilinear form; again this has the same orthogonal group.

For these reasons we will deal in the first few sections of this chapter with inner product modules over $\mathbb{Z}_p$, not quadratic $\mathbb{Z}_p$-modules. There is of course no difference if $p \neq 2$. When $p = 2$ the only difference in the relevant decompositions is the existence of the rank one inner product $\mathbb{Z}_2$-modules $W^{\varepsilon}_{2,0}$.

We will still freely use the notation of the quadratic form, namely $Q(x)$, defined in terms of the bilinear form by $Q(x) = \frac{1}{2}\langle x, x \rangle$. When $p = 2$, it may be the case that Q has values in $\frac{1}{2}\mathbb{Z}_2$, and one should not assume that $Q(x) \in \mathbb{Z}_2$ for all $x \in L$.

2. The groups $\mathcal{O}(L)$ and $\mathcal{O}^{\#}(L)$

Let L be an inner product $\mathbb{Z}_p$-module, and let $G_L = L^{\#}/L$ be its discriminant form group. As we discussed in Chapter II, there is a natural homomorphism $\mathcal{O}(L) \to \mathcal{O}(G_L)$. We let $\mathcal{O}^{\#}(L)$ denote the kernel of this homomorphism. The homomorphisms $\det\colon \mathcal{O}(L \otimes \mathbb{Q}_p) \to \{\pm 1\}$ and $\operatorname{spin}\colon \mathcal{O}(L \otimes \mathbb{Q}_p) \to \mathbb{Q}_p^*/(\mathbb{Q}_p^*)^2$ restrict to homomorphisms of $\mathcal{O}(L)$ and $\mathcal{O}^{\#}(L)$.

The Cartan-Dieudonné theorem 1.1 tells us that elements of $\mathcal{O}(L \otimes \mathbb{Q}_p)$ can be expressed as products of reflections in $\mathcal{O}(L \otimes \mathbb{Q}_p)$. We will spend the next several sections finding analogues of this statement (and of the preliminary Lemma I.9.9) for the groups $\mathcal{O}(L)$ and $\mathcal{O}^{\#}(L)$. The goal is to find a collection of "elementary" isometries in $\mathcal{O}(L)$ or $\mathcal{O}^{\#}(L)$ which generate the group. Of course, when regarded as elements of $\mathcal{O}(L \otimes \mathbb{Q}_p)$, these "elementary" isometries will have a further factorization into a product of reflections, but this factorization does not in general hold in $\mathcal{O}(L)$ or $\mathcal{O}^{\#}(L)$.

We first consider reflections in $\mathcal{O}(L)$.

LEMMA 2.1. *Let $x \in L$ be primitive and anisotropic. Then the following are equivalent:*

(2.1.1) $\tau_x \in \mathcal{O}(L)$
(2.1.2) $\langle x, t\rangle \in Q(x)\mathbb{Z}_p$ *for all* $t \in L$
(2.1.3) there is a k *such that* $Q(x) \in p^k\mathbb{U}_p$ *and* $\langle x, t\rangle \in p^k\mathbb{Z}_p$ *for all* $t \in L$.

Moreover, if x is simply anisotropic without being primitive, then it is still the case that (2.1.2) and (2.1.3) are equivalent, and each implies (2.1.1).

PROOF. This is immediate from the formula

$$\tau_x(t) = t - \frac{\langle x, t\rangle}{Q(x)}x$$

since $\frac{\langle x,t\rangle}{Q(x)}x \in L$ if and only if $\frac{\langle x,t\rangle}{Q(x)} \in \mathbb{Z}_p$ because x is assumed to be primitive. Q.E.D.

We now turn to the group $\mathcal{O}^{\#}(L)$. If $\rho \in \mathcal{O}(L)$, then the induced $\overline{\rho} \in \mathcal{O}(G_L)$ is defined by extending ρ to $L \otimes \mathbb{Q}_p$ by linearity, then restricting to $L^{\#}$, and descending to $G_L = L^{\#}/L$. We can thus phrase the condition that ρ be in $\mathcal{O}^{\#}(L)$ as follows: for every $\xi \in L^{\#}$, the element $\rho(\xi) - \xi$ is in fact in L.

It is slightly more convenient to view the dual lattice $L^{\#}$ as being isomorphic to the dual module L^* via the adjoint mapping $\alpha : L^{\#} \to L^*$ defined by sending $x \in L^{\#}$ to the functional $\mathrm{Ad}(x)|_L = \langle x, -\rangle$. Then $G_L \cong L^*/L$, where we view $L \subset L^*$ via the adjoint mapping. With this point of view the induced map $\overline{\rho}$ acts via the adjoint; if $\xi \in L^*$ is a functional on L, then

$$\overline{\rho}(\xi \bmod \mathrm{Ad}(L)) = \rho^*(\xi) \bmod \mathrm{Ad}(L) = \xi \circ \rho \bmod \mathrm{Ad}(L)$$

Hence the condition that ρ be in $\mathcal{O}^{\#}(L)$ is as follows: for every $\xi \in L^*$, there is some $z \in L$ (depending on ξ) such that

$$\rho^*(\xi) - \xi = \mathrm{Ad}(z).$$

This observation is sufficient to give the following criterion.

LEMMA 2.2. *Let $\rho \in \mathcal{O}(L)$ and suppose that there exist $x_1, \ldots, x_k, y_1, \ldots, y_k \in L$ such that*

$$\rho(t) = t + \sum \langle y_i, t \rangle x_i$$

for all $t \in L$. Then $\rho \in \mathcal{O}^{\#}(L)$.

PROOF. Given $\xi \in L^*$, consider $z = \sum \xi(x_i) y_i$. Since $\xi(x_i) \in \mathbb{Z}_p$ and $y_i \in L$ for every i, $z \in L$. Moreover, for every $t \in L$,

$$\begin{aligned}(\rho^*(\xi) - \xi)(t) &= \xi(\rho(t)) - \xi(t) \\ &= \xi(\sum \langle y_i, t \rangle x_i) \\ &= \sum \langle y_i, t \rangle \xi(x_i) \\ &= \langle \sum \xi(x_i) y_i, t \rangle \\ &= \langle z, t \rangle\end{aligned}$$

so that $\rho^*(\xi) - \xi = \mathrm{Ad}(z)$; hence $\rho \in \mathcal{O}^{\#}(L)$. Q.E.D.

PROPOSITION 2.3. *Let $x \in L$ be primitive and anisotropic. Then $\tau_x \in \mathcal{O}^{\#}(L)$ if and only if $p \nmid Q(x)$.*

Even if x is not primitive, if x is anisotropic and $p \nmid Q(x)$ then $\tau_x \in \mathcal{O}^{\#}(L)$.

PROOF. Suppose that $p \nmid Q(x)$. Then $\frac{1}{Q(x)} \in \mathbb{Z}_p$ so that $\tau_x \in \mathcal{O}(L)$ by Lemma 2.1. Also, $\frac{-1}{Q(x)} x \in L$ so that

$$\tau_x(t) = t + \left(\frac{-1}{Q(x)} x \right) \langle x, t \rangle$$

satisfies the hypotheses of Lemma 2.2. Hence $\tau_x \in \mathcal{O}^{\#}(L)$.

Conversely, suppose that $\tau_x \in \mathcal{O}^{\#}(L)$. Since x is primitive, there is some $\xi \in L^*$ with $\xi(x) = 1$. Since $\tau_x \in \mathcal{O}^{\#}(L)$, there is then some $z \in L$ with

$$\tau_x^*(\xi) - \xi = \mathrm{Ad}(z).$$

Thus, for every $t \in L$

$$\begin{aligned}\langle z, t\rangle = \mathrm{Ad}(z)(t) &= (\tau_x^*(\xi) - \xi)(t)\\ &= \xi(\tau_x(t) - t)\\ &= -\xi(x)\langle x, t\rangle/Q(x)\\ &= \langle -x/Q(x), t\rangle\end{aligned}$$

which implies that $x/Q(x) = -z$ is in L. But since x is primitive, this can only happen if $1/Q(x) \in \mathbb{Z}_p$, i.e., if $p \nmid Q(x)$. Q.E.D.

We let $\mathcal{O}^{\mathrm{ref}}(L)$ (resp. $\mathcal{O}^{\#,\mathrm{ref}}(L)$) denote the subgroup of $\mathcal{O}(L)$ (resp. $\mathcal{O}^{\#}(L)$) generated by reflections. Lemmas 2.1 and 2.3 describe the generators of these groups.

We need one additional fact about $\mathcal{O}^{\#}(L)$. Let us say that L has *scale* $\geq k$ if $\langle x, y\rangle \in p^k\mathbb{Z}_p$ for all $x, y \in L$. We will say that L has *scale* k if L has scale $\geq k$ and does not have scale $\geq k+1$; this is equivalent to saying that L has scale $\geq k$ and there are elements $x, y \in L$ with $\langle x, y\rangle \in p^k\mathbb{U}_p$. By convention, the zero lattice has scale ∞.

Note that if L has scale ≥ 1, then $\mathrm{scale}(L) = \mathrm{scale}(G_L)$. Also note the if L has scale $\geq k$, then $Q(x) \in \frac{1}{2}p^k\mathbb{Z}_p$ for all $x \in L$. If L has scale $\geq k$, then L can be decomposed as a direct sum of the rank one forms $\{W_{p,m}^{\varepsilon}; m \geq k\}$ if $p \neq 2$, and if $p = 2$, then L can be decomposed into the pieces $\{U_m, V_m, W_{2,m}^{\varepsilon}; m \geq k\}$. In particular, if $p = 2$ and L has scale ≥ 1, then the bilinear form is even and the quadratic form in $\mathbb{Z}_2$-valued.

LEMMA 2.4. *Let L be an inner product $\mathbb{Z}_p$-module of scale $\geq k$, and let $\rho \in \mathcal{O}^{\#}(L)$. Then for all $x \in L$, $\rho(x) - x \in p^kL$.*

PROOF. We first note that $\rho^{-1} \in \mathcal{O}^{\#}(L)$ as well, and that for every $t \in L$,

$$\begin{aligned}(\rho^{-1})^*(\mathrm{Ad}\, x)(t) &= \mathrm{Ad}\, x(\rho^{-1}(t))\\ &= \langle x, \rho^{-1}(t)\rangle\\ &= \langle \rho(x), t\rangle\\ &= \mathrm{Ad}(\rho(x))(t)\end{aligned}$$

so that $(\rho^{-1})^*(\mathrm{Ad}\, x) = \mathrm{Ad}(\rho(x))$.

Now since $p^k \mid \langle x, y\rangle$ for every $x, y \in L$, we have $\frac{1}{p^k}\mathrm{Ad}(x) \in L^*$. Then there must exist some $z \in L$ with $(\rho^{-1})^*\left(\frac{1}{p^k}\mathrm{Ad}(x)\right) -$

$\left(\frac{1}{p^k}\operatorname{Ad}(x)\right) = \operatorname{Ad}(z)$. But then,

$$\begin{aligned} p^k \operatorname{Ad}(z) &= (\rho^{-1})^*(\operatorname{Ad}(x)) - \operatorname{Ad}(x) \\ &= \operatorname{Ad}(\rho(x)) - \operatorname{Ad}(x) \\ &= \operatorname{Ad}(\rho(x) - x) \end{aligned}$$

which implies that $\rho(x) - x = p^k z$. Q.E.D.

3. The Generalized Eichler Isometry

In this section, we introduce our basic "elementary" isometry for use in factoring elements of $\mathcal{O}(L)$ and $\mathcal{O}^{\#}(L)$.

PROPOSITION 3.1. *Let L be an inner product $\mathbb{Z}_p$-module, and let $x, y \in L$, such that $2 \mid \langle x, x\rangle$ and $2 \mid \langle y, y\rangle$. (I.e., $Q(x)$ and $Q(y)$ are integral.) Suppose that either*

(a) *$Q(x) = \langle x, y\rangle = 0$, or*

(b) *$1 - \langle x, y\rangle + Q(x)Q(y) \in \mathbb{U}_p$, and $Q(y) \mid \langle y, t\rangle$ for every $t \in L$.*

Define

$$\begin{aligned} E_y^x(t) = t &+ \frac{x - Q(x)y}{1 - \langle x, y\rangle + Q(x)Q(y)}\langle y, t\rangle \\ &+ \frac{-y - Q(y)x + \langle x, y\rangle y}{1 - \langle x, y\rangle + Q(x)Q(y)}\langle x, t\rangle \end{aligned}$$

Then:

(3.1.1) In case (a), we have $E_y^x(t) = t + x\langle y, t\rangle + (-y - Q(y)x)\,\langle x, t\rangle$.

(3.1.2) If $Q(y)$ divides $\langle y, t\rangle$ for all $t \in L$, (in particular, in case (b)), we have

$$\tau_y \in \mathcal{O}(L), \quad \tau_{y - Q(y)x} \in \mathcal{O}(L) \quad \text{and} \quad E_y^x = \tau_y \tau_{y - Q(y)x}.$$

(3.1.3) In both cases (a) and (b), $E_y^x \in \mathcal{O}^{\#}(L)$.

(3.1.4) If $Q(x) = \langle x, y_1\rangle = \langle x, y_2\rangle = 0$ then $E_{y_1}^x E_{y_2}^x = E_{y_1 + y_2}^x$.

(3.1.5) $\det(E_y^x) = 1$ and $\operatorname{spin}(E_y^x) = 1 - \langle x, y\rangle + Q(x)Q(y)$.

E_y^x is called a generalized Eichler isometry.

PROOF. Statement (3.1.1) is clear.

To prove (3.1.2), first notice that since $Q(y)$ divides $\langle y, t\rangle$ for all t and this is sufficient to ensure that $\tau_y \in \mathcal{O}(L)$. Also note that

$$\begin{aligned} Q\left(y - Q(y)x\right) &= Q(y) - Q(y)\langle x, y\rangle + Q(y)^2 Q(x) \\ &= Q(y)(1 - \langle x, y\rangle + Q(y)Q(x)). \end{aligned}$$

If we let $\varepsilon = 1 - \langle x, y\rangle + Q(y)Q(x)$, then $Q(y - Q(y)x) = Q(y)\varepsilon$ and we see that the assumption also implies that $Q(y - Q(y)x)$ divides $\langle y - Q(y)x, t\rangle$ for all t; hence also $\tau_{y-Q(y)x)} \in \mathcal{O}(L)$.

Next note that

$$\begin{aligned} \tau_y\left(y - Q(y)x\right) &= y - Q(y)x - \frac{\langle y, y\rangle - Q(y)\langle x, y\rangle}{Q(y)} y \\ &= y - Q(y)x - (2 - \langle x, y\rangle)y \\ &= -y - Q(y)x + \langle x, y\rangle y \end{aligned}$$

Then

$$\begin{aligned} &\tau_y\tau_{y-Q(y)x}(t) = \tau_y\left(t - \frac{\langle y, t\rangle - Q(y)\langle x, t\rangle}{Q(y)\varepsilon}\left(y - Q(y)x\right)\right) \\ &= \tau_y(t) - \frac{\langle y, t\rangle - Q(y)\langle x, t\rangle}{Q(y)\varepsilon}\tau_y(y - Q(y)x) \\ &= t - \frac{\langle y, t\rangle}{Q(y)} y - \frac{\langle y, t\rangle - Q(y)\langle x, t\rangle}{Q(y)\varepsilon}\left(-y - Q(y)x + \langle x, y\rangle y\right) \\ &= t + \frac{\langle y, t\rangle}{Q(y)\varepsilon}\left(-\varepsilon y + y + Q(y)x - \langle x, y\rangle y\right) + \frac{\langle x, t\rangle}{\varepsilon}\left(-y - Q(y)x + \langle x, y\rangle y\right) \\ &= t + \frac{\langle y, t\rangle}{Q(y)\varepsilon}\left(-Q(y)Q(x)y + Q(y)x\right) + \frac{\langle x, t\rangle}{\varepsilon}\left(-y - Q(y)x + \langle x, y\rangle y\right) \\ &= t + \frac{\langle y, t\rangle}{\varepsilon}\left(-Q(x)y + x\right) + \frac{\langle x, t\rangle}{\varepsilon}\left(-y - Q(y)x + \langle x, y\rangle y\right) \\ &= E_y^x(t). \end{aligned}$$

This completes the proof of (3.1.2).

To see (3.1.3), we first check that $E_y^x \in \mathcal{O}(L)$. In case (b), this follows from (3.1.2). In case (a), (3.1.1) shows that E_y^x maps L to L. Moreover,

$$\begin{aligned} Q(E_y^x(t)) &= Q\left(t + x\langle y, t\rangle + (-y - Q(y)x)\langle x, t\rangle\right) \\ &= Q(t) + \langle x, t\rangle^2 Q(y) + \langle y, t\rangle\langle x, t\rangle - \langle y + Q(y)x, t\rangle\langle x, t\rangle \\ &= Q(t) + \langle x, t\rangle^2 Q(y) + \langle y, t\rangle\langle x, t\rangle - \langle y, t\rangle\langle x, t\rangle - Q(y)\langle x, t\rangle^2 \\ &= Q(t) \end{aligned}$$

so that $E_y^x \in \mathcal{O}(L)$.

Now Lemma 2.2 can be used to conclude that in both cases $E_y^x \in \mathcal{O}^\#(L)$. Indeed, no further statements are necessary in case (a). In case (b) we need only note that our hypotheses guarantee that

$$\frac{x - Q(x)y}{1 - \langle x, y\rangle + Q(x)Q(y)} \text{ and } \frac{-y - Q(y)x + \langle x, y\rangle y}{1 - \langle x, y\rangle + Q(x)Q(y)}$$

are both in L, so Lemma 2.2 also applies and $E_y^x \in \mathcal{O}^\#(L)$. This finishes statement (3.1.3).

Moving on to (3.1.4), note that if $Q(x) = \langle x, y_i\rangle = 0$, then we are in case (a), and $1 - \langle x, y_i\rangle + Q(x)Q(y_i) = 1$ so that $E_{y_i}^x(t) = t + x\langle y_i, t\rangle - (y_i + Q(y_i)x)\langle x, t\rangle$ by (3.1.1).
Thus,

$$E_{y_1}^x(x) = x$$

and

$$\begin{aligned} E_{y_1}^x\left(y_2 + Q(y_2)x\right) &= E_{y_1}^x(y_2) + Q(y_2)x \\ &= y_2 + x\langle y_1, y_2\rangle + Q(y_2)x \end{aligned}$$

so that

$$\begin{aligned} E_{y_1}^x E_{y_2}^x(t) &= E_{y_1}^x\left(t + x\langle y_2, t\rangle - (y_2 + Q(y_2)x)\langle x, t\rangle\right) \\ &= t + x\langle y_1, t\rangle - (y_1 + Q(y_1)x)\langle x, t\rangle + x\langle y_2, t\rangle \\ &\quad -\langle x, t\rangle(y_2 + x\langle y_1, y_2\rangle + Q(y_2)x) \\ &= t + x\langle y_1 + y_2, t\rangle - ((y_1 + y_2) + (Q(y_1) + Q(y_2) + \langle y_1, y_2\rangle)x)\langle x, t\rangle \\ &= t + x\langle y_1 + y_2, t\rangle - ((y_1 + y_2) + Q(y_1 + y_2)x)\langle x, t\rangle \\ &= E_{y_1+y_2}^x(t). \end{aligned}$$

proving (3.1.4).

Finally we show (3.1.5). If $Q(y) \neq 0$, then as we showed in the proof of (3.1.2), $E_y^x = \tau_y\tau_{y-Q(y)x}$. Thus, $\det(E_y^x) = 1$ and $\operatorname{spin}(E_h^x) = Q(y)Q\left(y - Q(y)x\right) = Q(y)^2\left(1 - \langle x, y\rangle + Q(x)Q(y)\right)$ so $\operatorname{spin}(E_y^x) \equiv 1 - \langle x, y\rangle + Q(x)Q(y) \bmod (\mathbb{Q}_p^*)^2$.

On the other hand, if $Q(y) = 0$ then we are in case (a), and $Q(x) = \langle x, y\rangle = 0$. The non-degeneracy of L guarantees that there is some $z \in x^\perp$ such that $Q(z) \neq 0$. Choose $\lambda \in \mathbb{Z}_p$ such that

$$Q(y - \lambda z) = -\lambda\langle y, z\rangle + \lambda^2 Q(z) \neq 0$$

Then $E_{\lambda z}^x$ and $E_{y-\lambda z}^x$ are well-defined (using case (a)), and $\langle x, \lambda z\rangle = \langle x, y - \lambda z\rangle = 0$ so that

$$E_y^x = E_{y-\lambda z}^x E_{\lambda z}^x$$

by (3.1.4). But now since $Q(y-\lambda z) \neq 0$ and $Q(\lambda z) \neq 0$, we have by the previous analysis that

$$\det(E_{y-\lambda z}^{x}) = \det(E_{\lambda z}^{x}) = 1$$

and

$$\operatorname{spin}(E_{y-\lambda z}^{x}) = \operatorname{spin}(E_{\lambda z}^{x}) = 1$$

so that $\det(E_y^x) = 1$ and $\operatorname{spin}(E_y^x) = 1 (= 1 - \langle x, y\rangle + Q(x)Q(y))$. Q.E.D.

4. Factorization for Forms Containing $W_{p,k}^{\varepsilon}$

In this and the next two sections, we study factorizations of elements in the groups $\mathcal{O}(L)$ and $\mathcal{O}^{\#}(L)$. In Chapter IV, we decomposed quadratic (and inner product) $\mathbb{Z}_p$-modules L as direct sums of certain pieces $W_{p,k}^{\varepsilon}$, U_k, and V_k; our factorization proceeds by induction on the rank of L, assuming that L contains one of these pieces as a direct summand (with k minimal). We treat the case of $W_{p,k}^{\varepsilon}$ in this section, and the cases of U_k and V_k in subsequent sections.

In addition to factoring isometries, we wish to keep track of the determinants and spinor norms introduced along the way, with the ultimate goal being the calculation of the images

$$\Sigma(L) = \operatorname{Im}((\det, \operatorname{spin})\colon \mathcal{O}(L) \to \{\pm 1\} \times \mathbb{Q}_p^*/(\mathbb{Q}_p^*)^2)$$
$$\Sigma^{\#}(L) = \operatorname{Im}((\det, \operatorname{spin})\colon \mathcal{O}^{\#}(L) \to \{\pm 1\} \times \mathbb{Q}_p^*/(\mathbb{Q}_p^*)^2).$$

For this purpose, it is convenient to introduce some subgroups $\Gamma_{p,k} \subset \{\pm 1\} \times \mathbb{Q}_p^*/(\mathbb{Q}_p^*)^2$, defined as follows:

$\Gamma_{p,0} = \{(1,1), (1,u_p), (-1,1), (-1,u_p)\}$ for p odd, and some non-square $u_p \in \mathbb{U}_p$

$\Gamma_{p,k} = \{(1,1), (-1,1)\}$ for p odd, $k \geq 1$

$\Gamma_{2,0} = \{(1,1), (1,3), (1,5), (1,7), (-1,1), (-1,3), (-1,5), (-1,7)\}$

$\Gamma_{2,1} = \{(1,1), (1,3), (1,5), (1,7)\}$

$\Gamma_{2,2} = \{(1,1), (1,5)\}$

$\Gamma_{2,k} = \{(1,1)\}$ for $k \geq 3$.

THEOREM 4.1. *Let L be an inner product $\mathbb{Z}_p$-module of scale $k \geq 1$. Let $x, y \in L$ such that $x - y \in p^k L$ and $Q(x) = Q(y) \in \frac{1}{2}p^k\mathbb{U}_p$. Assume that either $p > 2$ and $k \geq 1$, or $p = 2$ and $k \geq 2$. Then there is a $\sigma \in \mathcal{O}^{\#}(L)$ such that*

(1) $\sigma(x) = y$

(2) $\det(\sigma) = 1$ *and* $\operatorname{spin}(\sigma) = 1 + \frac{Q(x-y)}{Q(x+y)}$

(3) $(\det(\sigma), \mathrm{spin}(\sigma)) \in \Gamma_{p,k}$

(4) *if* $p = 2$ *and* $(\det(\sigma), \mathrm{spin}(\sigma)) \neq (1,1)$*, then* $k = 2$ *and there is some* $z \in L$ *with* $\langle y, z\rangle = 0$ *and* $Q(z) \in 2\mathbb{U}_2$.

PROOF. Since $k \geq 1$, $x - y \in 2L$ so that $x + y \in 2L$. Define $s, t \in L$ by $x - y = p^k s$, $x + y = 2t$ and write $Q(s) = p^k\alpha/2$, $Q(t) = p^k\beta/2$ for some $\alpha, \beta \in \mathbb{Z}_p$. Then $Q(x-y) = p^{3k}\alpha/2$ and $Q(x+y) = 2p^k\beta$.

We first claim that with these assumptions β is a unit. If $p = 2$, since $k \geq 2$ we get $4p^{k+1} = 2^{k+3} \mid 2^{3k-1}\alpha$, while if $p > 2$, since $k \geq 1$ we get $4p^{k+1} \mid p^{3k}\alpha/2$; in either case $4p^{k+1} \mid Q(x-y)$. On the other hand, if $p > 2$ then $4p^{k+1} \nmid 4Q(x)$; since

$$4Q(x) = Q(x-y) + Q(x+y)$$

we have that $4p^{k+1} \nmid Q(x+y) = 2p^k\beta$. Hence $\beta \in \mathbb{U}_p$ if $p > 2$. If $p = 2$, then $4p^k \nmid 4Q(x)$; hence arguing in the same way we see that $4p^k \nmid Q(x+y) = 2p^k\beta$, so that $2 \nmid \beta$ and $\beta \in \mathbb{U}_2$.

Note that $\langle s, t\rangle = \frac{1}{2p^k}\langle x-y, x+y\rangle = 0$ since $Q(x) = Q(y)$. Thus, if we define

$$\begin{aligned}\gamma &= 1 - \langle t, -\beta^{-1}s\rangle + Q(t)Q(\beta^{-1}s)\\ &= 1 + p^{2k}\beta^{-1}\alpha/4 = 1 + \frac{Q(x-y)}{Q(x+y)}\end{aligned}$$

then our hypotheses on k guarantee that $\gamma \equiv 1 \bmod p$, and that $Q(t), Q(-\beta^{-1}s) \in 2\mathbb{Z}_p$. Also, $Q(t) = p^k\beta/2 \in \frac{1}{2}p^k\mathbb{U}_p$, and since L has scale k, $p^k \mid \langle t, z\rangle$ for all $z \in L$; in particular $Q(t) \mid \langle t, z\rangle$ for all $z \in L$. Thus case (b) of Proposition 3.1 applies, and there is a $\sigma = E_t^{-\beta^{-1}s} \in \mathcal{O}^{\#}(L)$ with $\det(\sigma) = 1$ and $\mathrm{spin}(\sigma) = \gamma$. Moreover, in $\mathcal{O}(L)$, $\sigma = \tau_t\tau_{t+Q(t)\beta^{-1}s}$. This is the desired σ, and we see that we automatically have (2). But

$$t + Q(t)\beta^{-1}s = t + p^k s/2 = \tfrac{1}{2}(x+y) + \tfrac{1}{2}(x-y) = x$$

so that

$$\sigma = \tau_{\frac{1}{2}(x+y)}\tau_x = \tau_{x+y}\tau_x$$

and this implies that $\sigma(x) = y$, giving us (1).

We must still check (3) and (4), noting that $(\det(\sigma), \mathrm{spin}(\sigma)) = (1, \gamma)$. Since $\gamma \equiv 1 \bmod p$, we have $(1,\gamma) = (1,1) \in \Gamma_{p,k}$ when $p > 2$. So we may assume that $p = 2$.

If $k \geq 3$, then $\frac{1}{4}p^{2k} = 2^{2k-2}$ is divisible by 8, so that $\gamma = 1 + \frac{1}{4}p^{2k}\beta^{-1}\alpha \equiv 1 \bmod 8$, and $(1,\gamma) = (1,1) \in \Gamma_{2,k}$.

If $k = 2$, then $\gamma = 1 + 4\beta^{-1}\alpha$ so that $\gamma \equiv 1 \bmod 4$; this implies $(1,\gamma) \in \Gamma_{2,2}$. This completes the proof of (3).

Finally, to check that (4) holds, we may assume that $p = 2$, $k = 2$, and $\gamma \equiv 5 \bmod 8$; then $\beta^{-1}\alpha \in \mathbb{U}_2$, so that $\alpha \in \mathbb{U}_2$.

Note that $\langle x, y\rangle = Q(x) + Q(y) - Q(x-y) = 2Q(y) - 16Q(s) = 2Q(y) - 32\alpha$, and that since $4 \nmid Q(y)$ we have that $Q(y) \mid 4\alpha$. Hence $8Q(y) \mid -32\alpha = \langle x, y\rangle - 2Q(y) = \langle y, x-y\rangle$; this implies that $2Q(y) \mid \langle y, s\rangle$, and we may set $\delta = \langle y, s\rangle / 2Q(y) \in \mathbb{Z}_2$ and $z = s - \delta y \in L$. Note that $\langle y, z\rangle = 0$ by the choice of δ. Let $Q(y) = 2\varepsilon$, with $\varepsilon \in \mathbb{U}_2$. Now

$$Q(z) = Q(s) - \delta^2 Q(y) = 2\alpha - 2\delta^2\varepsilon$$

so if we let $\varphi = \alpha - \delta^2\varepsilon$ then $Q(z) = 2\varphi$.

Since $x = y + 4s = (1+4\delta)y + 4z$, we get

$$2\varepsilon = Q(x) = (1+4\delta)^2(2\varepsilon) + 16(2\varphi)$$

so that $(2\delta^2 + \delta)\varepsilon + 2\varphi = 0$, which implies $2 \mid \delta$. But then $\varphi = \alpha - \delta^2\varepsilon \in \mathbb{U}_2$ since $\alpha \in \mathbb{U}_2$; in particular, $Q(z) = 2\varphi \in 2\mathbb{U}_2$. Q.E.D.

COROLLARY 4.2. *Let $L = W^{\varepsilon}_{p,k} \oplus L'$ be an inner product $\mathbb{Z}_p$-module of scale k such that either*

(1) *$p > 2$, $k \geq 1$;*

(2) *$p = k = 2$ and $Q(L') \cap 2\mathbb{U}_2 = \emptyset$; or*

(3) *$p = 2$, $k \geq 3$.*

Then for every $\rho \in \mathcal{O}^{\#}(L)$ there is a $\sigma \in \mathcal{O}^{\#}(L)$ such that $\sigma\rho \in \mathcal{O}^{\#}(L')$ and $(\det(\sigma), \mathrm{spin}(\sigma)) = (1, 1)$. In particular, $\Sigma^{\#}(L) = \Sigma^{\#}(L')$.

PROOF. Let y generate $W^{\varepsilon}_{p,k}$ and let $x = \rho(y)$. By Lemma 2.4, $x - y \in p^k L$ and we may apply Theorem 4.1. Q.E.D.

THEOREM 4.3. *Let $L = W^{\varepsilon}_{2,2} \oplus W^{\varphi}_{2,2} \oplus L'$ be an inner product $\mathbb{Z}_2$-module of scale 2. Then:*

(4.3.1) For every $\rho \in \mathcal{O}^{\#}(L)$, there is a $\sigma \in \mathcal{O}^{\#}(L)$ such that $\sigma\rho \in \mathcal{O}^{\#}(L')$ and $(\det(\sigma), \mathrm{spin}(\sigma)) \in \Gamma_{2,2}$.

(4.3.2) $\Sigma^{\#}(L) = \Gamma_{2,2} \cdot \Sigma^{\#}(L')$.

PROOF. Statement (4.3.1) follows from two applictions of Theorem 4.1, as in Corollary 4.2. From (4.3.1), we see that $\Sigma^{\#}(L) \subset \Gamma_{2,2} \cdot \Sigma^{\#}(L')$. So to prove (4.3.2), we must show that $\Gamma_{2,2} \subset \Sigma^{\#}(L)$; or in other words, that $(1, 5) \in \Sigma^{\#}(L)$.

Let s, t span $W^{\varepsilon}_{2,2}$ and $W^{\varphi}_{2,2}$ respectively, and write $Q(s) = 2\alpha$ and $Q(t) = 2\beta$ for some $\alpha, \beta \in \mathbb{U}_2$. Let $\gamma = -\alpha\beta^{-1}$. Since $\gamma^2 + 16\gamma \equiv 1 \bmod 8$, there exist two square roots of $\gamma^2 + 16\gamma$ in $\mathbb{U}_2$. Choose a square root such that $4 \nmid \gamma + \sqrt{\gamma^2 + 16\gamma}$, and let $\delta = \frac{1}{2}\left(\gamma + \sqrt{\gamma^2 + 16\gamma}\right)$; note

that $\delta \in \mathbb{U}_2$. Then δ satisfies $\delta^2 = \gamma\delta + 4\gamma$, i.e.,

$$\beta + \alpha\delta^{-1} + 4\alpha\delta^{-2} = 0.$$

Let $x = (1 + 8\delta^{-1})s + 4t$ and $y = s$. Then

$$\begin{aligned} Q(x) &= (1 + 8\delta^{-1})^2(2\alpha) + 16(2\beta) \\ &= 2\alpha + 32(\delta^{-1}\alpha + 4\delta^{-2}\alpha + \beta) \\ &= 2\alpha = Q(y) \end{aligned}$$

while $x - y = 4(2\delta^{-1}s + t) \in 4L$. We may thus apply Theorem 4.1 (with $p = 2$ and $k = 2$) to this x and y to get a $\sigma \in \mathcal{O}^{\#}(L)$ with $\det(\sigma) = 1$ and $\mathrm{spin}(\sigma) = 1 + Q(x - y)/Q(x + y)$. As shown in the proof of 4.1, $Q(x + y) \in 8\mathbb{U}_2$. On the other hand,

$$\begin{aligned} Q(x - y) &= Q(8\delta^{-1}s + 4t) \\ &= 64\delta^{-2}(2\alpha) + 16(2\beta) \\ &= 32(4\delta^{-2}\alpha + \beta) \in 32\mathbb{U}_2 \end{aligned}$$

so that $Q(x-y)/Q(x+y) \in 4\mathbb{U}_2$ and $\mathrm{spin}(\sigma) = 1+Q(x-y)/Q(x+y) \equiv 5 \bmod 8$. Q.E.D.

LEMMA 4.4. *Let L be an inner product $\mathbb{Z}_p$-module of scale k. Let $x, y \in L$ such that $x - y \in p^k L$ and $Q(x) = Q(y) \in \frac{1}{2}p^k\mathbb{U}_p$. Suppose that either*

(1) *$p > 2$ and $k = 0$; or*

(2) *$p = 2$, $k = 0$, and $2 \nmid Q(x - y)$; or*

(3) *$p = 2$ and $k = 1$.*

Then there is a $\sigma \in \mathcal{O}^{\#,ref}(L)$ such that $\sigma(x) = y$.

PROOF. Let $x - y = p^k z$ for some $z \in L$. First suppose that $p^{2k+1} \nmid Q(x - y)$. Then $p \nmid Q(z)$, so that by Proposition 2.3, $\tau_z \in \mathcal{O}^{\#,\mathrm{ref}}(L)$. Since $\tau_z = \tau_{x-y}$, $\tau_z(x) = y$ so that $\sigma = \tau_z$ works in this case.

Now suppose that $p^{2k+1} \mid Q(x - y)$; since in this case $k = 1$ when $p = 2$, this is the same as $4p \mid Q(x-y)$. We also get $x - y \in 2L$ so that $x + y \in 2L$; write $x + y = 2t$ for some $t \in L$. But now our hypotheses imply that $p \nmid Q(x)$; and since $4Q(x) = Q(2x) = Q((x+y)+(x-y)) = Q(x + y) + Q(x - y) = 4Q(t) + Q(x - y)$, we see that $p \nmid Q(t)$. Again by Proposition 2.3, $\sigma = \tau_t\tau_x \in \mathcal{O}^{\#,\mathrm{ref}}(L)$. But

$$\sigma = \tau_t\tau_x = \tau_{x+y}\tau_x$$

so that $\sigma(x) = y$ by Theorem 1.1.1. Q.E.D.

COROLLARY 4.5. *Let $L = W^{\varepsilon}_{p,k} \oplus L'$ be an inner product $\mathbb{Z}_p$-module of scale k with either $p > 2$ and $k = 0$, or $p = 2$ and $k = 1$. For every $\rho \in \mathcal{O}^{\#}(L)$, there is a $\sigma \in \mathcal{O}^{\#,ref}(L)$ such that $\sigma\rho \in \mathcal{O}^{\#}(L')$. Moreover $\Sigma^{\#}(L)$ is generated by $\Sigma^{\#}(L')$ and $\{(-1, Q(z)) \mid z \in L, p \nmid Q(z)\}$.*

PROOF. Let y span $W^{\varepsilon}_{p,k}$, $x = \rho(y)$ and apply Lemma 4.4. The last statement follows from the proof of the Lemma, in which σ was found to be a reflection τ_z with $p \nmid Q(z)$ or a product of two such reflections. Q.E.D.

COROLLARY 4.6. *Let $L = W^{\varepsilon}_{p,0} \oplus L'$ be an inner product $\mathbb{Z}_p$-module (of scale 0) with $p > 2$. For every $\rho \in \mathcal{O}(L)$, there is a $\sigma \in \mathcal{O}^{\#,ref}(L)$ such that $\sigma\rho \in \mathcal{O}(L')$. In particular, $\Sigma(L)$ is generated by $\Sigma(L')$ and $\{(-1, Q(z)) \mid z \in L, p \nmid Q(z)\}$.*

PROOF. Let y span $W^{\varepsilon}_{p,0}$ $x = \rho(y)$ and apply Lemma 4.4. Q.E.D.

LEMMA 4.7. *Let $L = L_1 \oplus L_2$ be an (odd) inner product $\mathbb{Z}_2$-module such that L_1 is odd and unimodular,* $\operatorname{rank}(L_1) \leq 2$, *and scale$(L_2) \geq 1$. Let $x, y \in L$ such that $Q(x) = Q(y) \in \frac{1}{2}\mathbb{U}_2$ and $y \in L_1$. Suppose that $2 \mid Q(x - y)$. Then for every $t \in L$, $\langle x - y, t\rangle \in 2\mathbb{Z}_2$.*

PROOF. Note that the hypotheses imply that L_1 either has rank one and is isomorphic to $W^{\varepsilon}_{2,0}$, or has rank two and decomposes as a direct sum of two $W^{\varepsilon}_{2,0}$'s. Let y, z be an orthogonal basis for L_1 (where $z = 0$ if $\operatorname{rank}(L_1) = 1$), and write

$$x = (\alpha + 1)y + \beta z + s$$

for some $\alpha, \beta \in \mathbb{Z}_2$, $s \in L_2$. Then

$$Q(x) = (\alpha + 1)^2 Q(y) + \beta^2 Q(z) + Q(s) = Q(y)$$

so that

$$(*) \qquad (\alpha^2 + 2\alpha)Q(y) + \beta^2 Q(z) + Q(s) = 0.$$

Then

$$Q(x - y) = \alpha^2 Q(y) + \beta^2 Q(z) + Q(s) = -2\alpha Q(y).$$

Since $2 \mid Q(x - y)$ and $Q(y) \in \frac{1}{2}\mathbb{U}_2$ we have that $2 \mid \alpha$; write $\alpha = 2\alpha_0$. Since L_2 has scale ≥ 1, $Q(s) \in \mathbb{Z}_2$ so that $(*)$ now implies that $\beta^2 Q(z) \in \mathbb{Z}_2$. But either $z = 0$ or $Q(z) \in \frac{1}{2}\mathbb{U}_2$, so in either case we may write $\beta = 2\beta_0$. Thus,

$$\langle x - y, t\rangle = 2\alpha_0\langle y, t\rangle + 2\beta_0\langle z, t\rangle + \langle s, t\rangle.$$

But scale$(L_2) \geq 1$ implies $\langle s, t\rangle \in 2\mathbb{Z}_2$, so that $\langle x - y, t\rangle \in 2\mathbb{Z}_2$. Q.E.D.

THEOREM 4.8. *Let $L = W^{\varepsilon}_{2,0} \oplus L'$ be an inner product $\mathbb{Z}_2$-module (of scale 0). Assume that either scale$(L') \geq 1$ or that $L' = W^{\varepsilon}_{2,0} \oplus L''$ with scale$(L'') \geq 1$. Then:*

(4.8.1) For every $\rho \in \mathcal{O}(L)$ there is a $\sigma \in \mathcal{O}^{ref}(L)$ such that $\sigma\rho \in \mathcal{O}(L')$

(4.8.2) $\Sigma(L)$ is generated by $\Sigma(L')$ and $S = \{(-1, Q(z)) \mid z \in L, 4 \nmid Q(z)$ and if $2 \mid Q(z)$ then $2 \mid \langle z, t\rangle$ for all $t \in L\}$.

PROOF. (4.8.1): Let y span $W^{\varepsilon}_{2,0}$ and let $x = \rho(y)$; we must find $\sigma \in \mathcal{O}^{\mathrm{ref}}(L)$ such that $\sigma(x) = y$.

If $2 \nmid Q(x-y)$, this follows from Lemma 4.4.2, with $\sigma \in \mathcal{O}^{\#,\mathrm{ref}}(L)$. So assume $2 \mid Q(x-y)$; then by Lemma 4.7, the functions

$$t \longmapsto \langle x - y, t\rangle$$
$$t \longmapsto \langle x + y, t\rangle$$

take on only even values for $t \in L$.

If $4 \nmid Q(x-y)$, then $\sigma = \tau_{x-y} \in \mathcal{O}^{\mathrm{ref}}(L)$ by Lemma 2.1, $Q(x-y) \in 2\mathbb{U}_2$ and $\sigma(x) = y$. On the other hand, if $4 \mid Q(x-y)$ then since $4 \nmid 4Q(x) = Q(x-y) + Q(x+y)$ we have that $4 \nmid Q(x+y)$. In this case we see that $Q(x+y) \in 2\mathbb{U}_2$, so that by Lemma 2.1, $\tau_{x+y} \in \mathcal{O}^{\mathrm{ref}}(L)$; also $\tau_x \in \mathcal{O}^{\#,\mathrm{ref}}(L)$ so that $\sigma = \tau_{x+y}\tau_x \in \mathcal{O}^{\mathrm{ref}}(L)$ and $\sigma(x) = y$.

(4.8.2): The σ constructed in the proof of (4.8.1) is a product of reflections from $\mathcal{O}^{\#,\mathrm{ref}}$, together with (perhaps) a reflection τ_z with $Q(z) \in 2\mathbb{U}_2$ and $2 \mid \langle z, t\rangle$ for all $t \in L$. Moreover all of the reflections τ_w from $\mathcal{O}^{\#,\mathrm{ref}}$ used in the above are such that $4 \nmid Q(w)$. Hence we see that $\sigma(L)$ is contained in the group generated by $\Sigma(L')$ and S.

Conversely, to see that every element of S is in $\Sigma(L)$, note that if z satisfies the conditions given in S, then $\tau_z \in \mathcal{O}(L)$ by Lemma 2.1. Thus, $(-1, Q(z)) \in \Sigma(L)$. Q.E.D.

5. Factorization for Forms Containing U_k

We now turn to the case of inner product $\mathbb{Z}_2$-modules containing a factor of U_k. If L is an inner product $\mathbb{Z}_2$-module, and $x, y \in L$, we say that x, y is a *k-hyperbolic pair* if the matrix of $\langle -, -\rangle|_{\mathrm{span}(x,y)}$ with respect to x and y is

$$\begin{pmatrix} 0 & 2^k \\ 2^k & 0 \end{pmatrix}$$

If L has scale k, then any k-hyperbolic pair splits off as a direct summand of L.

LEMMA 5.1. *Let L be an inner product $\mathbb{Z}_2$-module of scale k, let x, y be a k-hyperbolic pair in L and let $\alpha \in \mathbb{U}_2$ satisfy $\alpha \equiv 1 \bmod 2^k$. Define $\sigma\colon L \to L$ by*

$$\begin{aligned}\sigma(x) &= \alpha^{-1}x\\ \sigma(y) &= \alpha y\\ \sigma(z) &= z \text{ for all } z \in (\mathit{span}(x,y))^{\perp}\end{aligned}$$

Then $\sigma \in \mathcal{O}^{\#}(L)$ and $(\det(\sigma), \mathrm{spin}(\sigma)) = (1, \alpha)$.

PROOF. Write $\alpha = 1 + 2^k\beta$ for some $\beta \in \mathbb{Z}_2$. Then

$$\begin{aligned}&Q(\beta x) = 0 \in 2\mathbb{Z}_2\\ &Q(x-y) = -2^k \in 2^k\mathbb{U}_2\\ &\langle x-y, \beta x\rangle = -2^k\beta\\ &1 - \langle x-y, \beta x\rangle + Q(x-y)Q(\beta x) = 1 + 2^k\beta = \alpha\end{aligned}$$

Moreover, since L has scale k, $2^k \mid \langle x-y, t\rangle$ for every $t \in L$.

By case (b) of Proposition 3.1, $E^{\beta x}_{x-y} \in \mathcal{O}^{\#}(L)$ with $(\det(E^{\beta x}_{x-y}), \mathrm{spin}(E^{\beta x}_{x-y})) = (1, \alpha)$. Now for any $t \in L$,

$$\begin{aligned}E^{\beta x}_{x-y}(t) &= t + \alpha^{-1}\beta x\langle x-y, t\rangle + \alpha^{-1}((-1-2^k\beta)(x-y) + 2^k\beta x)\langle \beta x, t\rangle\\ &= t + \alpha^{-1}\beta((1+2^k\beta)x + (-1-2^k\beta)(x-y))\langle x, t\rangle - \alpha^{-1}\beta x\langle y, t\rangle\\ &= t + \beta y\langle x, t\rangle - \alpha^{-1}\beta x\langle y, t\rangle\end{aligned}$$

Thus, $E^{\beta x}_{x-y}(z) = z$ for any $z \in (\mathrm{span}(x,y))^{\perp}$, while

$$E^{\beta x}_{x-y}(x) = x - \alpha^{-1}\beta 2^k x = \alpha^{-1}x$$

and

$$E^{\beta x}_{x-y}(y) = y + 2^k\beta y = \alpha y.$$

Thus $\sigma = E^{\beta x}_{x-y}$ and has the desired properties. Q.E.D.

LEMMA 5.2. *Let L be an inner product $\mathbb{Z}_2$-module of scale k. Let x_1, y_1 and x_2, y_2 be k-hyperbolic pairs in L such that $x_1 - x_2$ and $y_1 - y_2$ are in 2^kL and $\langle x_2, y_1\rangle = 2^k$ (so that x_2 and y_1 form a k-hyperbolic pair also). Then there is a $\sigma \in \mathcal{O}^{\#}(L)$ with $(\det(\sigma), \mathrm{spin}(\sigma)) = (1,1)$, $\sigma(x_1) = x_2$ and $\sigma(y_1) = y_2$.*

PROOF. Let

$$\begin{aligned}x_2 - x_1 &= 2^k\alpha x_1 + 2^k\beta y_1 - 2^k z\\ y_2 - y_1 &= 2^k\gamma x_2 + 2^k\delta y_1 - 2^k s\end{aligned}$$

with $\alpha, \beta, \gamma, \delta \in \mathbb{Z}_2$, $z \in (\mathrm{span}(x_1, y_1))^\perp$ and $s \in (\mathrm{span}(x_2, y_1))^\perp$. Now

$$2^k = \langle x_2, y_1 \rangle = \langle (1 + 2^k\alpha)x_1 + 2^k\beta y_1 - 2^k z, y_1 \rangle = 2^k(1 + 2^k\alpha)$$

and

$$2^k = \langle x_2, y_2 \rangle = \langle x_2, 2^k\gamma x_2 + (1 + 2^k\delta)y_1 - 2^k s \rangle = 2^k(1 + 2^k\delta)$$

so that $\alpha = \delta = 0$ and

$$\begin{aligned} x_2 &= x_1 + 2^k\beta y_1 - 2^k z \\ y_2 &= 2^k\gamma x_2 + y_1 - 2^k s. \end{aligned}$$

Now

$$0 = Q(x_2) = Q(x_1 + 2^k\beta y_1) + Q(2^k z) = 2^{2k}\beta + 2^{2k}Q(z)$$

and

$$0 = Q(y_2) = Q(2^k\gamma x_2 + y_1) + Q(2^k s) = 2^{2k}\gamma + 2^{2k}Q(s)$$

so that $Q(z) = -\beta$ and $Q(s) = -\gamma$. Since we also have $\langle y_1, z \rangle = \langle x_2, s \rangle = Q(y_1) = Q(x_2) = 0$, by case (a) of Proposition 3.1, $E_s^{x_2}, E_z^{y_1} \in \mathcal{O}^\#(L)$, with determinants and spinor norms 1. Let $\sigma = E_s^{x_2} \circ E_z^{y_1}$, so that $(\det(\sigma), \mathrm{spin}(\sigma)) = (1, 1)$.

For any $t \in L$,

$$\begin{aligned} E_s^{x_2}(t) &= t + x_2\langle s, t \rangle + (-s + \gamma x_2)\langle x_2, t \rangle \\ E_z^{y_1}(t) &= t + y_1\langle z, t \rangle + (-z + \beta y_1)\langle y_1, t \rangle. \end{aligned}$$

Thus,

$$\begin{aligned} E_z^{y_1}(x_1) &= x_1 + 2^k(\beta y_1 - z) = x_2 \\ E_z^{y_1}(y_1) &= y_1 \end{aligned}$$

while

$$\begin{aligned} E_s^{x_2}(x_2) &= x_2 \\ E_s^{x_2}(y_1) &= y_1 + 2^k(-s + \gamma x_2) = y_2 \end{aligned}$$

so that $\sigma(x_1) = x_2$ and $\sigma(y_1) = y_2$ as required. Q.E.D.

LEMMA 5.3. *Let L be an inner product $\mathbb{Z}_2$-module, and suppose that $t_1, t_2 \in L$ with $Q(t_1), Q(t_2) \in \mathbb{Z}_2$ and*

$$4Q(t_1)Q(t_2) - \langle t_1, t_2 \rangle^2 \equiv 7 \bmod 8.$$

Then there is a $z \in$ span(t_1, t_2) with $Q(z) = 0$ and $\langle z, t_1 \rangle = 1$.

PROOF. The hypotheses guarantee that t_1 and t_2 span a unimodular quadratic $\mathbb{Z}_2$-module, and so their span must be isometric to U_0 or V_0. Since $\det(U_0) \equiv 7 \bmod 8$ and $\det(V_0) \equiv 3 \bmod 8$, we see that $\operatorname{span}(t_1, t_2) \cong U_0$. But then there exists a 0-hyperbolic pair z_1, z_2 which is a basis for $\operatorname{span}(t_1, t_2)$. Choose i such that $\langle t_1, z_i\rangle \in \mathbb{U}_2$; then $z = \frac{1}{\langle t_1, z_i\rangle} z_i$ has the required properties. Q.E.D.

LEMMA 5.4. *Let L be an inner product $\mathbb{Z}_2$-module of scale k, and let x_1, y_1 and x_2, y_2 be two k-hyperbolic pairs in L such that $x_1 - x_2 \in 2^k L$. Then there is a $\sigma \in \mathcal{O}^{\#}(L)$ such that $\langle x_2, \sigma(y_1)\rangle \in 2^k \mathbb{U}_2$, and $(\det(\sigma), \operatorname{spin}(\sigma)) \in \Gamma_{2,k}$.*

PROOF. If $k > 0$, we may take σ to be the identity; if $\langle x_2, y_1\rangle = 2^k\alpha$ then since $x_2 - x_1 \in 2^k L$, $2^{2k} \mid \langle x_2 - x_1, y_1\rangle = 2^k\alpha - 2^k$ so that $\alpha \equiv 1 \bmod 2^k$.

If $k = 0$, write

$$x_2 = \alpha x_1 + \beta y_1 + t_1$$
$$y_2 = \gamma x_1 + \delta y_1 + t_2$$

with $\alpha, \beta, \gamma, \delta \in \mathbb{Z}_2$, $t_1, t_2 \in (\operatorname{span}(x_1, y_1))^{\perp}$. We must consider three cases.

Case 1: $\alpha \in \mathbb{U}_2$.

Then $\langle x_2, y_1\rangle = \alpha \in \mathbb{U}_2$ so $\sigma =$ identity will suffice as above.

Case 2: $\alpha \in 2\mathbb{Z}_2$, $\beta \in \mathbb{U}_2$.

Then $Q(x_2 - x_1) = -\beta \in \mathbb{U}_2$ so that by Proposition 2.3, $\tau_{x_2 - x_1} \in \mathcal{O}^{\#}(L)$. Let $\sigma = \tau_{x_2 - x_1}$. Then $(\det(\sigma), \operatorname{spin}(\sigma)) = (-1, -\beta) \in \Gamma_{2,0}$, and

$$\langle x_2, \sigma(y_1)\rangle = \langle \sigma^{-1}(x_2), y_1\rangle = \langle x_1, y_1\rangle = 1 \in \mathbb{U}_2.$$

Case 3: $\alpha, \beta \in 2\mathbb{Z}_2$.

Then the matrix of the bilinear form $\langle -, -\rangle|_{\operatorname{span}(t_1, t_2)}$ with respect to t_1, t_2 is

$$\begin{pmatrix} -2\alpha\beta & 1 - \alpha\delta - \beta\gamma \\ 1 - \alpha\delta - \beta\gamma & -2\gamma\delta \end{pmatrix}.$$

This has determinant $4\alpha\beta\gamma\delta - (1 - \alpha\delta - \beta\gamma)^2$; since α and β are even, this determinant is congruent to 7 mod 8.

Thus, by Lemma 5.3, there is $z \in \operatorname{span}(t_1, t_2)$ with $Q(z) = 0$ and $\langle z, t_1\rangle = 1$, and hence $\langle x_2, z\rangle = 1$.

Now $Q(x_1) = Q(z) = \langle x_1, z\rangle = 0$ so that $E_z^{x_1}$ is defined using case (a) of Proposition 3.1; if $\sigma = E_z^{x_1}$, then $\sigma \in \mathcal{O}^{\#}(L)$, and $\det(\sigma) = \operatorname{spin}(\sigma) = 1$. Moreover,

$$\sigma(y_1) = y_1 + x_1\langle z, y_1\rangle - z\langle x_1, y_1\rangle = y_1 - z$$

so that $\langle x_2, \sigma(y_1)\rangle = \langle x_2, y_1 - z\rangle = \alpha - 1 \in \mathbb{U}_2$. Q.E.D.

THEOREM 5.5. *Let L be an inner product $\mathbb{Z}_2$-module of scale k. Let x_1, y_1 and x_2, y_2 be two k-hyperbolic pairs in L such that $x_1 - x_2$ and $y_1 - y_2$ are in $2^k L$. Then there is a $\sigma \in \mathcal{O}^\#(L)$ such that $\sigma(x_1) = x_2$, $\sigma(y_1) = y_2$ and $(\det(\sigma), \mathrm{spin}(\sigma)) \in \Gamma_{2,k}$.*

PROOF. By Lemma 5.4, there is a $\sigma_1 \in \mathcal{O}^\#(L)$ such that $\langle x_2, \sigma_1(y_1)\rangle \in 2^k\mathbb{U}_2$. By Lemma 2.4, $\sigma_1(t) - t \in 2^k L$ for all $t \in L$, so that

$$\sigma_1(x_1) - x_2 = (\sigma_1(x_1) - x_1) + (x_1 - x_2) \in 2^k L$$
$$\sigma_1(y_1) - y_2 = (\sigma_1(y_1) - y_1) + (y_1 - y_2) \in 2^k L$$

and the hypotheses are still satisfied by the two k-hyperbolic pairs $\sigma_1(x_1)$, $\sigma_1(y_1)$ and x_2, y_2.

Thus, if we write

$$x_2 = \alpha\sigma_1(x_1) + 2^k\beta\sigma_1(y_1) + 2^k z$$

for some $\alpha, \beta \in \mathbb{Z}_2$, with $\alpha \equiv 1 \bmod 2^k$ and $z \in (\mathrm{span}(\sigma_1(x_1), \sigma_1(y_1)))^\perp$, we have $\langle x_2, \sigma_1(y_1)\rangle = 2^k\alpha \in 2^k\mathbb{U}_2$ so that $\alpha \in \mathbb{U}_2$.

By Lemma 5.1, there is a $\sigma_2 \in \mathcal{O}^\#(L)$ with $\sigma_2(\sigma_1(x_1)) = \alpha^{-1}\sigma_1(x_1)$ and $\sigma_2(\sigma_1(y_1)) = \alpha\sigma_1(y_1)$. Again by Lemma 2.4, a similar computation to that above shows that $\sigma_2^{-1}\sigma_1(x_1)$, $\sigma_2^{-1}\sigma_1(y_1)$ and x_2, y_2 are two k-hyperbolic pairs satisfying the hypotheses of the theorem.

Now

$$\langle x_2, \sigma_2^{-1}\sigma_1(y_1)\rangle = \langle x_2, \alpha^{-1}\sigma_1(y_1)\rangle = \alpha^{-1}\langle x_2, \sigma_1(y_1)\rangle = 2^k.$$

Thus, by Lemma 5.2, there is a $\sigma_3 \in \mathcal{O}^\#(L)$ with

$$\sigma_3(\sigma_2^{-1}\sigma_1(x_1)) = x_2$$
$$\sigma_3(\sigma_2^{-1}\sigma_1(y_1)) = y_2.$$

Let $\sigma = \sigma_3\sigma_2^{-1}\sigma_1$; we of course have $\sigma(x_1) = x_2$, $\sigma(y_1) = y_2$ by definition.

The isometry σ_1 was obtained using Lemma 5.4, and therefore we have that $(\det(\sigma_1), \mathrm{spin}(\sigma_1)) \in \Gamma_{2,k}$. The isometry σ_2 was obtained using Lemma 5.1, hence $\det(\sigma_2) = 1$ and this is enough to ensure that $(\det(\sigma_2), \mathrm{spin}(\sigma_2)) \in \Gamma_{2,k}$. Finally, the isometry σ_3 was obtained using Lemma 5.2, hence $(\det(\sigma_3), \mathrm{spin}(\sigma_3)) = (1, 1)$. Since $(\det\sigma_i, \mathrm{spin}\,\sigma_i) \in \Gamma_{2,k}$ for each $i = 1, 2, 3$, $(\det(\sigma), \mathrm{spin}(\sigma)) \in \Gamma_{2,k}$. Q.E.D.

COROLLARY 5.6. *Let $L = \mathbb{U}_k \oplus L'$ be an inner product $\mathbb{Z}_2$-module of scale k. Then:*

(5.6.1) For every $\rho \in \mathcal{O}^\#(L)$ there is a $\sigma \in \mathcal{O}^\#(L)$ such that $\sigma\rho \in \mathcal{O}^\#(L')$ and $(\det(\sigma), \mathrm{spin}(\sigma)) \in \Gamma_{2,k}$.

(5.6.2) $\Sigma^{\#}(L) = \Gamma_{2,k} \cdot \Sigma^{\#}(L')$

PROOF. To see (5.6.1), let x_2, y_2 be a k-hyperbolic pair spanning U_k, and let $x_1 = \rho(x_2)$, $y_1 = \rho(y_2)$. Since $\rho \in \mathcal{O}^{\#}(L)$, by Lemma 2.4 $\rho(x_2) - x_2$ and $\rho(y_2) - y_2$ are in $2^k L$. Thus, by Theorem 5.5, there is a $\sigma \in \mathcal{O}^{\#}(L)$ with $(\det(\sigma), \mathrm{spin}(\sigma)) \in \Gamma_{2,k}$ and $\sigma(\rho(x_2)) = x_2$, $\sigma(\rho(y_2)) = y_2$. Thus, $\sigma\rho$ fixes U_k so that $\sigma\rho \in \mathcal{O}^{\#}(L')$.

To check (5.6.2), by (5.6.1), $\Sigma^{\#}(L) \subset \Gamma_{2,k} \cdot \Sigma^{\#}(L')$, so we must show that $\Gamma_{2,k} \subset \Sigma^{\#}(L)$. Let $(d, s) \in \Gamma_{2,k}$.

First suppose $d = 1$. Since $s \equiv 1 \bmod 2^k$, by Lemma 5.1 there is a $\sigma \in \mathcal{O}^{\#}(L)$ with $(\det \sigma, \mathrm{spin}\ \sigma) = (d, s)$.

The case $d = -1$ occurs only if $k = 0$. In that case, choose $z \in U_0$ such that $Q(z) = 1$. Then $\tau_z \in \mathcal{O}^{\#}(L)$ by Proposition 2.3, and $(\det(\tau_z), \mathrm{spin}(\tau_z)) = (-1, 1)$. Since $\Gamma_{2,0}$ is generated by $(-1, 1)$ and $\{(d, s) \in \Gamma_{2,0} \mid d = 1\}$, the statement follows. Q.E.D.

COROLLARY 5.7. *Let $L = U_0 \oplus L'$ be an inner product $\mathbb{Z}_2$-module (of scale 0). Then:*

(5.7.1) For every $\rho \in \mathcal{O}(L)$ there is a $\sigma \in \mathcal{O}(L)$ such that $\sigma\rho \in \mathcal{O}(L')$ and $(\det(\sigma), \mathrm{spin}(\sigma)) \in \Gamma_{2,0}$.

(5.7.2) $\Sigma(L) = \Gamma_{2,0} \cdot \Sigma(L')$.

PROOF. For (5.7.1), let x_2, y_2 be a 0-hyperbolic pair spanning U_0, and let $x_1 = \rho(x_2)$, $y_1 = \rho(y_2)$. Then $x_1 - x_2, y_1 - y_2 \in 2^0 L$ so by Theorem 5.5, there is a $\sigma \in \mathcal{O}(L)$ with $(\det(\sigma), \mathrm{spin}(\sigma)) \in \Gamma_{2,0}$ and $\sigma\rho \in \mathcal{O}(L')$.

To see (5.7.2), by (5.7.1), $\Sigma(L) \subset \Gamma_{2,0} \cdot \Sigma(L')$ and by Corollary 5.6.2, $\Gamma_{2,0} \subset \Sigma(L)$. Q.E.D.

6. Factorization for Forms Containing V_k

In this section, we factor isometries of lattices containing a copy of V_k.

LEMMA 6.1. *Let L be an inner product $\mathbb{Z}_2$-module of scale k, and suppose that $r, s, t \in L$ satisfy*

(1) $Q(t) \in 2^k \mathbb{U}_2$

(2) $\langle t, t - 2s \rangle = 0$

(3) $Q(r) = Q(s)$

(4) $r - s \in 2^k L$

(5) *if $k = 0$, either $2 \nmid Q(r - s + t)$ or $2 \mid \langle r - s, t \rangle$.*

Then there is a $\sigma \in \mathcal{O}^{\#}(L)$ *such that* $\sigma(r) = s$ *and* $(\det(\sigma), \mathrm{spin}(\sigma)) \in \Gamma_{2,k}$. *Moreover, if* $\langle r-s, t-2s\rangle = 0$, *then* $\sigma(t-2s) = t-2s$. *(Note that in the case* $\langle r-s, t-2s\rangle = 0$, *(5) is automatic since* $\langle r-s, t\rangle = 2\langle r-s, s\rangle$.*)*

PROOF. Let $r - s = 2^k z$ and $Q(t) = 2^k \alpha$ with $z \in L$ and $\alpha \in \mathbb{U}_2$. We consider two cases.

Case 1: $k = 0$ and $2 \mid Q(z+t)$.

By (5), this implies that $2 \mid \langle z, t\rangle$. Then since in this case $Q(t) \in \mathbb{U}_2$ we see that

$$Q(z) = Q(z+t) - \langle z, t\rangle - Q(t) \equiv 1 \bmod 2,$$

so that $Q(z) \in \mathbb{U}_2$. By Proposition 2.3, $\sigma = \tau_z \in \mathcal{O}^{\#}(L)$. Also, $\tau_z = \tau_{r-s}$ so that $\sigma(r) = \tau_z(r) = s$. In addition, $(\det(\sigma), \mathrm{spin}(\sigma)) = (-1, Q(z)) \in \Gamma_{2,0}$.

In the case $\langle r-s, t-2s\rangle = \langle z, t-2s\rangle = 0$, we have immediately that $\sigma(t-2s) = \tau_z(t-2s) = t-2s$.

Case 2: $k \geq 1$, or $k = 0$ and $2 \nmid Q(z+t)$.

Since L has scale k, $2^k \mid \langle t, x\rangle$ for all $x \in L$. Let

$$\begin{aligned}\beta &= 1 - \langle -\alpha^{-1} z, t\rangle + Q(-\alpha^{-1} z) Q(t) \\ &= 1 + \alpha^{-1}\langle z, t\rangle + 2^k \alpha^{-1} Q(z).\end{aligned}$$

If $k \geq 1$, $2^k \mid \langle z, t\rangle$ so that $\beta \equiv 1 \bmod 2^k$. If $k = 0$,

$$\begin{aligned}\alpha^{-1} Q(z+t) &= \alpha^{-1} Q(z) + \alpha^{-1}\langle z, t\rangle + \alpha^{-1} Q(t) \\ &= \alpha^{-1} Q(z) + \alpha^{-1}\langle z, t\rangle + 1 = \beta;\end{aligned}$$

since $2 \nmid Q(z+t)$, $\beta \in \mathbb{U}_2$.

Thus in either case, using case (b) of Proposition 3.1, we may define $\sigma = E_t^{-\alpha^{-1} z} \in \mathcal{O}^{\#}(L)$ and $(\det(\sigma), \mathrm{spin}(\sigma)) = (1, \beta) \in \Gamma_{2,k}$.

Since $Q(t) \neq 0$,

$$\sigma = \tau_t \tau_{t+2^k z} = \tau_t \tau_{t+r-s}.$$

Now using (2) and (3) we see that $Q(r) = Q(s) = Q(s-t)$ so that

$$\tau_{t+r-s}(r) = \tau_{r-(s-t)}(r) = s - t$$

and

$$\tau_t(s-t) = \tau_{s-(s-t)}(s-t) = s;$$

hence $\sigma(r) = s$.

Moreover, in the case that $\langle r-s, t-2s\rangle = 0$, then

$$\langle t + r - s, t - 2s\rangle = \langle t, t-2s\rangle + \langle r-s, t-2s\rangle = 0$$

and $\quad \langle t, t-2s\rangle = 0$

so that $\sigma(t-2s) = \tau_t\tau_{t+r-s}(t-2s) = \tau_t(t-2s) = t-2s$. Q.E.D.

THEOREM 6.2. *Let L be an inner product $\mathbb{Z}_2$-module of scale k. Let x_1, x_2, y_1, y_2 be in L such that $x_1 - x_2$ and $y_1 - y_2$ are in 2^kL, and for each $i = 1, 2$ the matrix of $\langle -, - \rangle|_{span(x_i, y_i)}$ with respect to x_i, y_i is*

$$\begin{pmatrix} 2^{k+1} & 2^k \\ 2^k & 2^{k+1} \end{pmatrix}.$$

If $k = 0$, suppose that $Q((span(x_2, y_2))^\perp) \cap \mathbb{U}_2 = \emptyset$. Then there is a $\sigma \in \mathcal{O}^\#(L)$ such that $\sigma(x_1) = x_2$, $\sigma(y_1) = y_2$, and $(\det(\sigma), \mathrm{spin}(\sigma)) \in \Gamma_{2,k}$.

PROOF. We first apply Lemma 6.1 with $r = x_1$, $s = x_2$, and $t = y_2$. To verify the hypotheses:

(1) $Q(t) = Q(y_2) = 2^{k+1}$

(2) $\langle t, t - 2s \rangle = \langle y_2, y_2 - 2x_2 \rangle = 2^{k+1} - 2^{k+1} = 0$

(3) $Q(r) = Q(x_1) = 2^k = Q(x_2) = Q(s)$

(4) $r - s = x_1 - x_2 \in 2^kL$ by assumption

(5) If $k = 0$, write

$$x_1 = (\alpha + 1)x_2 + (\beta - 1)y_2 + z$$

with $z \in (\mathrm{span}(x_2, y_2))^\perp$. Note that since $k = 0$ we have $Q(x_i) = Q(y_i) = \langle x_i, y_i \rangle = 1$ for each i. Then

$$r - s + t = x_1 - x_2 + y_2 = \alpha x_2 + \beta y_2 + z$$

so that

$$Q(r - s + t) = Q(x_1 - x_2 + y_2) = \alpha^2 + \alpha\beta + \beta^2 + Q(z)$$

and

$$\langle r - s, t \rangle = \langle x_1 - x_2, y_2 \rangle = \alpha + 2\beta - 2.$$

Suppose that $2 \nmid \langle r - s, t \rangle = \alpha + 2\beta - 2$; then α must be odd. This forces $\alpha^2 + \alpha\beta + \beta^2$ to be odd. If in addition $2 \mid Q(r - s + t) = Q(x_1 - x_2 + y_2)$ then $Q(z)$ must be odd and integral, i.e., $Q(z) \in \mathbb{U}_2$. This violates the assumption on the values of Q on $\mathrm{span}(x_2, y_2))^\perp$, and finishes the verification of (5).

Thus, by Lemma 6.1, there is a $\sigma_1 \in \mathcal{O}^\#(L)$ with $(\det(\sigma_1), \mathrm{spin}(\sigma_1)) \in \Gamma_{2k}$ and $\sigma_1(x_1) = x_2$.

We now apply Lemma 6.1 a second time with $r = \sigma_1(y_1)$, $s = y_2$, and $t = 2y_2 - x_2$. In this case,

$$\begin{aligned}\langle r - s, t - 2s\rangle &= \langle y_2 - \sigma_1(y_1), 2y_2 - x_2 - 2y_2\rangle \\ &= -\langle y_2, x_2\rangle + \langle \sigma_1(y_1), x_2\rangle \\ &= -2^k + \langle \sigma_1(y_1), \sigma_1(x_1)\rangle = 0\end{aligned}$$

so that we will invoke the last sentence of Lemma 6.1 as well (and do not need to check hypothesis (5)). To check the other hypotheses:

(1) $Q(t) = Q(2y_2 - x_2) = 3 \cdot 2^k \in 2^k\mathbb{U}_2$

(2) $\langle t, t - 2s\rangle = \langle 2y_2 - x_2, 2y_2 - x_2 - 2y_2\rangle = \langle 2y_2 - x_2, -x_2\rangle = -2^{k+1} + 2^{k+1} = 0$

(3) $Q(r) = Q(\sigma_1(y_1)) = Q(y_1) = 2^k = Q(y_2) = Q(s)$

(4) $\sigma_1(y_1) - y_2 = (\sigma_1(y_1) - y_1) + (y_1 - y_2) \in 2^k L$ by Lemma 2.4, since $\sigma_1 \in \mathcal{O}^{\#}(L)$.

Thus, by Lemma 6.1, there is a $\sigma_2 \in \mathcal{O}^{\#}(L)$ with $(\det(\sigma_2), \mathrm{spin}(\sigma_2)) \in \Gamma_{2,k}$, $\sigma_2(\sigma_1(y_1)) = y_2$; in addition, since we have checked that $\langle r - s, t - 2s\rangle = 0$, we have $\sigma_2(2y_2 - x_2 - 2y_2) = 2y_2 - x_2 - 2y_2$, i.e., $\sigma_2(x_2) = x_2$.

But then if $\sigma = \sigma_2\sigma_1$,

$$\begin{aligned}\sigma(x_1) &= \sigma_2\sigma_1(x_1) = \sigma_2(x_2) = x_2 \\ \sigma(y_1) &= \sigma_2\sigma_1(y_1) = y_2\end{aligned}$$

so that σ is the desired isometry. Q.E.D.

LEMMA 6.3. *Let L be an inner product $\mathbb{Z}_2$-module of scale k, and let $x, y \in L$ such that the matrix of $\langle -, -\rangle|_{span(x,y)}$ with respect to x, y is*

$$\begin{pmatrix} 2^{k+1} & 2^k \\ 2^k & 2^{k+1}\end{pmatrix}$$

For any $\alpha \in \mathbb{U}_2$ with $\alpha \equiv 1 \bmod 2^k$ there is a $\sigma \in \mathcal{O}^{\#}(L)$ with $(\det(\sigma), \mathrm{spin}(\sigma)) = (1, \alpha)$.

PROOF. For any $\beta \in \mathbb{U}_2$, consider

$$\begin{aligned}\gamma &= 1 - \langle x, \beta y\rangle + Q(x)Q(\beta y) \\ &= 1 - 2^k\beta + 2^{2k}\beta^2;\end{aligned}$$

note that $\gamma \in \mathbb{U}_2$. Also $Q(\beta y) = 2^k\beta^2 \in 2^k\mathbb{U}_2$; Since L has scale k, $2^k \mid \langle \beta y, t\rangle$ for every $t \in L$. Thus, using case (b) of Proposition 3.1, we may define $E^x_{\beta y} \in \mathcal{O}^{\#}(L)$ with $(\det(E^x_{\beta y}), \mathrm{spin}(E^x_{\beta y})) = (1, \gamma)$.

Since odd spinor norms are determined by their values mod8, if $\alpha \equiv 1 \bmod 8$ we may take $\sigma =$ identity to get $\text{spin}(\sigma) \equiv \alpha \bmod 8$. If $\alpha \not\equiv 1 \bmod 8$ then $k \leq 2$; unless $k = 1$ and $\alpha \equiv 5 \bmod 8$ we choose β by the following table to guarantee that $\gamma = \text{spin}(E^x_{\beta y}) \equiv \alpha \bmod 8$.

k	β	$\gamma = 1 - 2^k\beta + 2^{2k}\beta^2 \bmod 8$
0	3 5 7	7 5 3
1	1 3	7 3
2	1	5

Since $\alpha \equiv 1 \bmod 4$ when $k = 2$, all possibilities can be realized in this way unless $k = 1$ and $\alpha \equiv 5 \bmod 8$. To obtain this last case, simply compose two isometries with spinor norm 3 and 7, which exist by the table above. Q.E.D.

COROLLARY 6.4. *Let $L = V_k \oplus L'$ be an inner product $\mathbb{Z}_2$-module of scale k, and if $k = 0$ assume that $Q(L') \cap \mathbb{U}_2 = \emptyset$. Then:*

(6.4.1) For every $\rho \in \mathcal{O}^\#(L)$, there is a $\sigma \in \mathcal{O}^\#(L)$ such that

$$\sigma\rho \in \mathcal{O}^\#(L') \quad \textit{and} \quad (\det(\sigma), \text{spin}(\sigma)) \in \Gamma_{2,k}.$$

(6.4.2) $\Sigma^\#(L) = \Gamma_{2,k} \cdot \Sigma^\#(L')$.

The proof is entirely analogous to that of Corollary 5.6, using Theorem 6.2 and Lemma 6.3.

COROLLARY 6.5. *Let $L = V_0 \oplus L'$ be an inner product $\mathbb{Z}_2$-module (of scale 0) such that $Q(L') \cap \mathbb{U}_2 = \emptyset$. Then:*

(6.5.1) For every $\rho \in \mathcal{O}(L)$ there is a $\sigma \in \mathcal{O}(L)$ such that $\sigma\rho \in \mathcal{O}(L')$ and $(\det(\sigma), \text{spin}(\sigma)) \in \Gamma_{2,0}$.

(6.5.2) $\Sigma(L) = \Gamma_{2,0} \cdot \Sigma(L')$.

The proof is analogous to that of Corollary 5.7.

7. Cartan-Dieudonné-type Theorems for Quadratic $\mathbb{Z}_2$-Modules

We now combine the calculations of the last few sections to get analogues of the Cartan-Dieudonné thoerem for $\mathcal{O}^\#(L)$ and $\mathcal{O}(L)$.

It is convenient to introduce another "normal form" for a decomposition of a quadratic (or inner product) $\mathbb{Z}_2$-module into indecomposable

components. This is far from unique, but is useful for the isometry results of this section.

DEFINITION 7.1. Let L be a quadratic (or inner product) $\mathbb{Z}_2$-module. A decomposition

$$L = \bigoplus_{k\geq 0} (U_k^{\oplus N(k)} \oplus V_k^{e(k)} \oplus W(k))$$

is in *alternate normal form* if:

(a) each piece $U_k^{\oplus N(k)} \oplus V_k^{e(k)} \oplus W(k)$ of scale k is in homogeneous normal form, and
(b) for each $k \geq 1$, either $e(k-1) = 0$ or $W(k) = 0$.

It is a simple matter to put a quadratic or inner product $\mathbb{Z}_2$-module L into alternate normal form, working from the "bottom up". We take as given that each piece of scale k can be separately put into homogeneous normal form; start by putting all pieces of scale k into homogeneous normal form. Assume by induction that each piece of scale $\leq m$ is in homogeneous normal form, and that condition (b) is satisfied for all $k \leq m$. If at that point we have $e(m) = 1$ and $W(m+1) \neq 0$, use relation (VIII) of Proposition IV.3.1 to increase $N(m)$ and decrease $e(m)$. (This can always be done in such a way as not to spoil the homogeneous normal form at either the m level or the $m+1$ level.) Then proceed to the next level. Hence:

PROPOSITION 7.2. *Every quadratic (or inner product) $\mathbb{Z}_2$-module L can be decomposed into alternate normal form.*

We begin with two lemmas.

LEMMA 7.3. *Let $L = W_{2,k}^{\varepsilon} \oplus W_{2,k}^{\varphi}$. Then there is a $z \in L$ such that $Q(z) \in 2^k\mathbb{U}_2$ if and only if $\varepsilon + \varphi \not\equiv 0 \bmod 4$.*

PROOF. Choose generators x and y for $W_{2,k}^{\varepsilon}$ and $W_{2,k}^{\varphi}$, respectively, so that $Q(ax) = \varepsilon 2^{k-1}a^2$ and $Q(by) = \varphi 2^{k-1}b^2$. (Here we abuse notation slightly and consider ε and φ as coming from the set $\{1,3,5,7\} \subset \mathbb{U}_2$.) Let $z = ax + by$, so that $Q(z) = (a^2\varepsilon + b^2\varphi)2^{k-1}$. Then $2^k \mid Q(z)$ if and only if $a^2\varepsilon + b^2\varphi$ is even; this happens if and only if $a \equiv b \bmod 2$, since both ε and φ are odd. But if a and b are both even then $2^{k+1} \mid Q(z)$. Thus $Q(z) \in 2^k\mathbb{U}_2$ implies that $a, b \in \mathbb{U}_2$. In that case, $a^2\varepsilon + b^2\varphi \equiv \varepsilon + \varphi \bmod 8$, so that $a^2\varepsilon + b^2\varphi \in 2\mathbb{U}_2$ and only if $\varepsilon + \varphi$ is not divisible by 4, i.e., $\varepsilon + \varphi \not\equiv 0 \bmod 4$. Q.E.D.

LEMMA 7.4. *Let L be an inner product $\mathbb{Z}_2$-module decomposed into alternate normal form. Write*

$$L = U_0^N \oplus V_0^e \oplus W(0) \oplus L'$$

with scale$(L') \geq 1$. *If* $e \neq 0$, *then* $Q(W(0) \oplus L') \cap \mathbb{U}_2 = \emptyset$.

PROOF. Write

$$L' = U_1^{N(1)} \oplus V_1^{e(1)} \oplus W(1) \oplus L''$$

with scale$(L'') \geq 2$. Hence $Q(L'') \subset 2\mathbb{Z}_2$, so we need only worry about the values of Q on $W(0) \oplus U_1^{N(1)} \oplus V_1^{e(1)} \oplus W(1)$. Since $e = e(0) \neq 0$, we have (by the alternate normal form assumption) that $W(1) = 0$. Since the values of Q on both U_1 and V_1 are all even, we see that $Q(L') \subset 2\mathbb{Z}_2$.

Suppose there is a $z = z_1 + z_2$ with $z_1 \in W_{(0)}$ and $z_2 \in L'$, such that $Q(z) = Q(z_1) + Q(z_2) \in \mathbb{U}_2$. Then $Q(L') \subset 2\mathbb{Z}_2$ implies that so that $Q(z_1) \in \mathbb{U}_2$. If rank $W_{(0)} \leq 1$, this is clearly impossible; the values of Q on $W_{2,0}^{\varepsilon}$ have the form $\frac{1}{2}\varepsilon a^2$ for some $a \in \mathbb{Z}_2$, with $\varepsilon \in \mathbb{U}_2$, and this is never a unit. If rank $W_{(0)} = 2$, by Lemma 7.3 this can happen only if $W_{(0)} = W_{2,0}^{\varepsilon} \oplus W_{2,0}^{\varphi}$ where $\varepsilon + \varphi \not\equiv 0 \bmod 4$. But since the decomposition is in alternate normal form, in particular the piece of scale 0 is in homogeneous normal form; hence the only possibilities for (ε, φ) with $e \neq 0$ are $(1,3)$ and $(1,7)$ (see Table IV.4); this is a contradiction. Q.E.D.

THEOREM 7.5. *Let* L *be an even inner product* $\mathbb{Z}_p$*-module. (I.e., here we explicitly assume that* L *is a quadratic* $\mathbb{Z}_2$*-module, where the quadratic form* Q *takes integral values.) Then* $\mathcal{O}^{\#}(L)$ *is generated by reflections and generalized Eichler isometries.*

PROOF. We proceed by induction on the rank of L, using Corollaries 4.2, 4.5, 5.6, 6.4, and Theorem 4.3. Note that all of the isometries constructed there can be factored as products of reflections and generalized Eichler isometries. Note also that those statements take the following form: given a decomposition $L = L_1 \oplus L_2$ satisfying certain hypotheses, for every $\rho \in \mathcal{O}(L)$ there is a $\sigma \in \mathcal{O}(L)$ (which is a product of reflections and generalized Eichler isometries) such that $\sigma\rho \in \mathcal{O}(L_2)$. By the inductive hypothesis, $\sigma\rho$ will also be a product of reflections and generalized Eichler autometries.

First consider the case $p = 2$. We may assume that L is in alternate normal form. Suppose that L has scale k, and write

$$L = (U_k)^N \oplus (V_k)^e \oplus W(k) \oplus L'$$

with scale $(L') \geq k + 1$.

If $N > 0$, we may apply Corollary 5.6.

If $N = 0$ and $e > 0$, note that if $k = 0$ then $Q(W(0) \oplus L') \cap \mathbb{U}_2 = \emptyset$ by Lemma 7.4. Thus we may apply Corollary 6.4.

If $N = e = 0$, note that $k \geq 1$ since we have assumed that L is even. We may thus apply Corollary 4.5 in the case $k = 1$, and Corollary 4.2

in the case $k \geq 3$. If $k = 2$ and rank $W(2) = 1$, then $L = W^{\varepsilon}_{2,2} \oplus L'$, and since L' has scale at least 3, $Q(L') \subset 4\mathbb{Z}_2$ and we may apply Corollary 4.2 also. Finally if $k = 2$ and rank $W(2) = 2$, we apply Theorem 4.3.

If $p > 2$, we may write $L = W^{\varepsilon}_{p,k} \oplus L'$ and apply Corollary 4.5 if $k = 0$ and Corollary 4.2 if $k \geq 1$. Q.E.D.

To give an analogous theorem for $\mathcal{O}(L)$, we must discuss the effects of *scaling* on the orthogonal group. Again it is more convenient to do this with respect to the bilinear forms than the quadratic forms. Let L be an inner product $\mathbb{Z}_p$-module of scale $\geq k$, with bilinear form $\langle -, - \rangle$. Define the bilinear form $\langle -, - \rangle_1$ on L by

$$\langle x, y \rangle_1 = p^{-k} \langle x, y \rangle \quad \text{for all } x, y \in L.$$

Note that even if $\langle -, - \rangle$ is an even bilinear form, if $p = 2$ it may be the case that $\langle -, - \rangle_1$ is *not* an even bilinear form.

If $(L, \langle -, - \rangle)$ has scale k, and we decompose L as

$$(L, \langle -, - \rangle) \cong \bigoplus_{m \geq k} (U_m^{N(m)} \oplus V_m^{e(m)} \oplus W(m))$$

as usual, then we have

$$(L, \langle -, - \rangle_1) \cong \bigoplus_{m \geq 0} (U_m^{N(m+k)} \oplus V_m^{e(m+k)} \oplus W(m+k)).$$

In any case there is a natural isomorphism from $\mathcal{O}(L, \langle -, - \rangle)$ to $\mathcal{O}(L, \langle -, - \rangle_1)$. Moreover this clearly preserves the set of reflections, since a reflection can be defined purely in terms of the bilinear form also: τ_v is defined when $\langle v, v \rangle \neq 0$ and $\langle v, v \rangle \mid 2\langle v, w \rangle$ for all $w \in L$.

To see the effect on the generalized Eichler isometries, we prove the

PROPOSITION 7.6. *Let L be an inner product $\mathbb{Z}_p$-module.*

(7.6.1) Suppose $x, y \in L$ such that $Q(x) = \langle x, y \rangle = 0$, $Q(y) \in p^k \mathbb{Z}_p$, and with $p^k \mid \langle x, t \rangle$ and $p^k \mid \langle y, t \rangle$ for all $t \in L$. Define the rescaled Eichler isometry ${}^k E_y^x$ *by*

$${}^k E_y^x(t) = t + x p^{-k} \langle y, t \rangle + \left(-y - p^{-k} Q(y) x\right) p^{-k} \langle x, t \rangle$$

Then ${}^k E_y^x \in \mathcal{O}(L)$.

(7.6.2) Suppose that L has scale $\geq k$. If $\sigma \in \mathcal{O}(L, \langle -, - \rangle_1)$ is a generalized Eichler isometry then, regarded as an element of $\mathcal{O}(L, \langle -, - \rangle)$, σ is either a product of reflections or is a rescaled Eichler isometry.

PROOF. We first discuss (7.6.1). The hypotheses guarantee that ${}^kE_y^x$ maps L to L. To see that ${}^kE_y^x \in \mathcal{O}(L)$, we must check that $Q({}^kE_y^x(t)) = Q(t)$ for every $t \in L$; this is a slight modification of the calculation given in the proof of Proposition 3.1.3.

To see (7.6.2), first assume that σ satisfies hypothesis (b) of Proposition 3.1. Then σ is a product of reflections in $\mathcal{O}(L, \langle -, - \rangle_1)$; since the isomorphism between $\mathcal{O}(L, \langle -, - \rangle)$ and $\mathcal{O}(L, \langle -, - \rangle_1)$ preserves the set of reflections, this still holds in $\mathcal{O}(L, \langle -, - \rangle)$.

If $\sigma = E_y^x$ satisfies hypothesis (a) of Proposition 3.1, then

$$E_y^x(t) = t + x\langle y, t \rangle_1 + \left(-y - \tfrac{1}{2}\langle y, y \rangle_1 x\right) \langle x, t \rangle_1$$

so that in $\mathcal{O}(L, \langle -, - \rangle)$, $\sigma = {}^kE_y^x$ is a rescaled Eichler isometry. Q.E.D.

THEOREM 7.7. *Let L be an inner product $\mathbb{Z}_p$-module. Then $\mathcal{O}(L)$ is generated by reflections and rescaled Eichler isometries.*

PROOF. We gain use induction on the rank of L.

Suppose that $(L, \langle -, - \rangle)$ has scale k, let $\langle -, - \rangle_1 = p^{-k}\langle -, - \rangle$, and consider a decomposition $L = L_1 \oplus L_2$. If we can show that for every $\rho \in \mathcal{O}(L, \langle -, - \rangle_1)$ there is a $\sigma \in \mathcal{O}(L, \langle -, - \rangle_1)$ such that $\sigma\rho \in \mathcal{O}(L_2, \langle -, - \rangle_1|_{L_2})$ and σ is a product of reflections and generalized Eichler isometries, we shall be finished: regarded as elements in $\mathcal{O}(L, \langle -, - \rangle)$ and $\mathcal{O}(L_2, \langle -, - \rangle|_{L_2})$, σ and $\sigma\rho$ will be products of reflections and rescaled Eichler isometries by Proposition 7.6 and the inductive hypothesis, respectively.

If $p = 2$, we may assume that $(L, \langle -, - \rangle)$ is in alternate normal form, and write

$$(L, \langle -, - \rangle_1) = U_0^N \oplus V_0^e \oplus W(0) \oplus L'$$

with $\text{scale}(L') \geq 1$. Note that since we have rescaled, either $N \neq 0$, $e \neq 0$, or $\text{rank}\, W(0) \neq 0$.

If $N > 0$, we may apply Corollary 5.7. If $N = 0$ and $e > 0$ then by Lemma 7.4, $Q(W(0) \oplus L') \cap \mathbb{U}_2 = \emptyset$ so that we may apply Corollary 6.5. Finally, if $N = e = 0$, then $\text{rank}\, W(0) \leq 2$, and we may apply Theorem 4.8.

If $p > 2$, we may write $(L, \langle -, - \rangle_1) = W_{p,0}^{\varepsilon} \oplus L'$ and apply Corollary 4.6. Q.E.D.

8. Scaling and Spinor Norms

We turn now to the computation of the groupos $\Sigma(L)$ and $\Sigma^{\#}(L)$, defined as

$$\Sigma(L) = \mathrm{Im}\left((\det, \mathrm{spin})\colon \mathcal{O}(L) \to \{\pm 1\} \times \mathbb{Q}_p^*/(\mathbb{Q}_p^*)^2\right).$$
$$\Sigma^{\#}(L) = \mathrm{Im}\left((\det, \mathrm{spin})\colon \mathcal{O}^{\#}(L) \to \{\pm 1\} \times \mathbb{Q}_p^*/(\mathbb{Q}_p^*)^2\right)$$

We will also find it convenient to introduce

$$\Sigma^{+}(L) = \{(d,s) \in \Sigma(L) \mid d = 1\},$$
$$\Sigma^{++}(L) = \left\{(d,s) \in \Sigma(L) \mid d = 1, s \in \mathbb{U}_p \bmod (\mathbb{Q}_p^*)^2\right\}.$$

As the proof of Theorem 7.7 shows, we need to know the effect of scaling in order to compute $\Sigma(L)$.

PROPOSITION 8.1. *Let $(L, \langle -,- \rangle)$ be an inner product $\mathbb{Z}_p$-module of scale $\geq k$, and let $\langle -,- \rangle_1 = p^{-k}\langle -,- \rangle$.*

(8.1.1) If k is even, then $\Sigma(L, \langle -,- \rangle_1) = \Sigma(L, \langle -,- \rangle)$.

(8.1.2) If k is odd, then $\Sigma^{+}(L, \langle -,- \rangle_1) = \Sigma^{+}(L, \langle -,- \rangle)$, while

$$(-1, s) \in \Sigma(L, \langle -,- \rangle_1) \Longleftrightarrow (-1, ps) \in \Sigma(L, \langle -,- \rangle).$$

PROOF. Given $\rho \in \mathcal{O}(L, \langle -,- \rangle)$, decompose ρ as a product of reflections

$$\rho = \tau_{z_1} \cdots \tau_{z_r}$$

in $\mathcal{O}(L \otimes \mathbb{Q}_p, \langle -,- \rangle \otimes \mathbb{Q}_p)$. Then $\det(\rho) = (-1)^r$ while

$$\mathrm{spin}(\rho) = Q(z_1) \cdots Q(z_r).$$

The decomposition of ρ still holds if ρ is regarded as an element of $\mathcal{O}(L, \langle -,- \rangle_1)$, so that

$$\det{}_1(\rho) = (-1)^r = \det(\rho)$$

while

$$\mathrm{spin}_1(\rho) = Q_1(z_1) \ldots Q_1(z_r) = p^{-kr}\,\mathrm{spin}(\rho)$$

where we write Q_1 for the quadratic form associated to $\langle -,- \rangle_1$, and $\det_1$ and spin_1 for the values computed with respect to the rescaled forms. Thus

$$\frac{\mathrm{spin}_1(\rho)}{\mathrm{spin}(\rho)} \equiv \begin{cases} 1 & \text{if } k \text{ is even or } \det\rho = 1 \\ p & \text{if } k \text{ is odd and } \det\rho = -1. \end{cases} \quad \bmod (Q_p^*)^2$$

Q.E.D.

We shall not be overly concerned with the change in spinor norms for k odd, due to the following lemma.

LEMMA 8.2. *Let L be an inner product $\mathbb{Z}_p$-module. Then:*

(8.2.1) There exist reflections in $\mathcal{O}(L)$

(8.2.2) $[\Sigma(L)\colon \Sigma^{+}(L)] = 2$

(8.2.3) $\Sigma(L)/\Sigma^{+}(L)$ is generated by the determinant and spinor norm of any reflection in $\mathcal{O}(L)$.

PROOF. (8.2.1): Let L have scale k. Then we can write either $L = W_{p,k}^{\varepsilon} \oplus L'$, $L = U_k \oplus L'$ or $L = V_k \oplus L'$. In the first case, there is a $z \in L$ with $Q(z) \in \frac{1}{2}p^k\mathbb{U}_p$ so that $\tau_z \in \mathcal{O}(L)$ by Lemma 2.1. In the last two cases, there is a $z \in L$ with $Q(z) \in 2^k\mathbb{U}_2$ so that $\tau_z \in \mathcal{O}(L)$ by Lemma 2.1.

(8.2.2): We have $\Sigma(L)/\Sigma^{+}(L) \subset \{\pm 1\}$, and is nonempty by (8.2.1).

(8.2.3): This is obvious by the other two statements, since any reflection τ_z has determinant -1 and so $(\det(\tau_z), \mathrm{spin}(\tau_z)) \notin \Sigma^{+}(L)$. Q.E.D.

In view of this lemma, we shall concentrate on the computation of $\Sigma^{\#}(L)$ and $\Sigma^{+}(L)$ in the following sections.

9. Computation of $\Sigma^{\#}(L)$ and $\Sigma^{+}(L)$ for $p \neq 2$

In this section, we compute $\Sigma^{\#}(L)$ and $\Sigma^{+}(L)$ for quadratic $\mathbb{Z}_p$-modules with p odd. (Recall for p odd that there is no essential difference between a quadratic $\mathbb{Z}_p$-module and an inner product $\mathbb{Z}_p$-module.)

LEMMA 9.1. *Let $L = W_{p,0}^{\varepsilon} \oplus W_{p,0}^{\varphi} \oplus L'$ be a quadratic $\mathbb{Z}_p$-module with $p \neq 2$. Then*

$$\Sigma^{\#}(L) \supset \left\{(d,s) \in \{\pm 1\} \times \mathbb{Q}_p^*/(\mathbb{Q}_p^*)^2 \mid s \not\equiv 0 \bmod p\right\} = \Gamma_{p,0}$$

PROOF. Let $\alpha \in \mathbb{U}_p$ be a non-square, i.e., $\left(\frac{\alpha}{p}\right) = -1$.

By Lemma IV.2.1.1, for any ε and φ in $\{\pm 1\}$, $W_{p,0}^{\varepsilon} \oplus W_{p,0}^{\varphi} \cong W_{p,0}^{-\varepsilon} \oplus W_{p,0}^{-\varphi}$; in particular, both $W_{p,0}^{1}$ and $W_{p,0}^{-1}$ must occur as factors in some (perhaps different) decompositions of L. This means that there are elements $x, y \in L$ with $Q(x) = 1$ and $Q(y) = \alpha$; but now $\tau_x, \tau_y \in \mathcal{O}^{\#}(L)$ by Proposition 2.3, while

$$(\det \tau_x, \mathrm{spin}\, \tau_x) = (-1, 1),\ (\det \tau_y, \mathrm{spin}\, \tau_y) = (-1, \alpha).$$

But $\{(d,s) \mid s \not\equiv 0 \bmod p\} = \{(1,1), (1,\alpha), (-1,1), (-1,\alpha)\}$ is generated by $(-1,1)$ and $(-1,\alpha)$. Q.E.D.

COROLLARY 9.2. *Let $L = W^{\varepsilon}_{p,k} \oplus W^{\varphi}_{p,k} \oplus L'$ be a quadratic $\mathbb{Z}_p$-module with $p \neq 2$. Then $\Sigma(L) \supset \big\{(d,s) \in \{\pm 1\} \times \mathbb{Q}_p^*/(\mathbb{Q}_p^*)^2 \mid d = 1,\ s \not\equiv 0 \bmod p\big\}$.*

PROOF. Let $\alpha \in \mathbb{U}_p$ be a nonsquare, so that $\{(d,s) \mid d = 1,\ s \not\equiv 0 \bmod p\} = \{(1,1),(1,\alpha)\}$. Consider the quadratic module $L'' = W^{\varepsilon}_{p,0} \oplus W^{\varphi}_{p,0}$ which, up to scaling, is a direct summand of L. By Lemma 9.1, there is a $\sigma \in \mathcal{O}^{\#}(L'')$ such that $(\det(\sigma), \mathrm{spin}(\sigma)) = (1,\alpha)$. But then, regarding $\sigma \in \mathcal{O}(L)$ (acting as σ on $W^{\varepsilon}_{p,k} \oplus W^{\varphi}_{p,k}$ and as the identity on L'), we still have $(\det(\sigma), \mathrm{spin}(\sigma)) = (1,\alpha)$, (arguing as in the proof of Proposition 8.1); hence $(1,\alpha) \in \Sigma(L)$. Q.E.D.

THEOREM 9.3. *Let L be a quadratic $\mathbb{Z}_p$-module with $p \neq 2$.*

(9.3.1) If scale$(L) \geq 1$ then $\Sigma^{\#}(L) = \{(1,1)\}$.

(9.3.2) If $L = W^{\varepsilon}_{p,0} \oplus L'$ with scale$(L') \geq 1$, then

$$\Sigma^{\#}(L) = \{(1,1),(-1,2\alpha)\}, \qquad \text{where } \left(\frac{\alpha}{p}\right) = \varepsilon.$$

(9.3.3) If $L = W^{\varepsilon}_{p,0} \oplus W^{\varphi}_{p,0} \oplus L'$, then $\Sigma^{\#}(L) = \Gamma_{p,0}$.

PROOF. We proceed by induction on the rank of L. Let L have scale k, and write $L = W^{\varepsilon}_{p,k} \oplus L'$.

If $k \geq 1$, by the inductive hypothesis $\Sigma^{\#}(L') = \{(1,1)\}$. But by Corollary 4.2, $\Sigma^{\#}(L) = \Sigma^{\#}(L')$, so that $\Sigma^{\#}(L) = \{(1,1)\}$, proving (9.3.1).

If $k = 0$, by Corollary 4.5, $\Sigma^{\#}(L)$ is generated by $\Sigma^{\#}(L')$ and $\{(-1,Q(z)) \mid z \in L,\ Q(z) \in \mathbb{U}_p\}$. Since this last set is contained in $\Gamma_{p,0}$, we see that $\Sigma^{\#}(L) \subset \Gamma_{p,0}$. Now case (9.3.3) is finished by Lemma 9.1.

For case (9.3.2), we must show: for every $z \in L$ with $Q(z) \in \mathbb{U}_p$ we have $Q(z) \equiv 2\alpha \bmod (\mathbb{Q}_p^*)^2$, where α is chosen so that $\left(\frac{\alpha}{p}\right) = \varepsilon$. Let x be a basis of $W^{\varepsilon}_{p,0}$ such that $Q(x) = \alpha/2$ (which is possible since $\left(\frac{\alpha}{p}\right) = \varepsilon$). Write $z = ax + y$ with $y \in L'$. then $Q(z) = a^2\alpha/2 + Q(y) \equiv a^2\alpha \bmod p$, so that $Q(z) \equiv a^2\alpha/2 \bmod (\mathbb{Q}_p^*)^2$ and hence $Q(z) \equiv 2\alpha \bmod (\mathbb{Q}_p^*)^2$. Q.E.D.

We turn now to the computation of $\Sigma^{+}(L)$. We first consider $\Sigma + (L)/\Sigma^{++}(L)$.

LEMMA 9.4. *Let $L = W^{\varepsilon}_{p,k} \oplus W^{\varphi}_{p,\ell} \oplus L'$ be a quadratic $\mathbb{Z}_p$-module, $p \neq 2$, with $k \not\equiv \ell \bmod 2$. Then $(1,p\alpha) \in \Sigma^{+}(L)$, where $\left(\frac{\alpha}{p}\right) = \varepsilon\varphi$. In particular, $\Sigma^{+}(L) \neq \Sigma^{++}(L)$.*

PROOF. Choose $\beta \in \mathbb{U}_p$ with $\left(\frac{\beta}{p}\right) = \varepsilon$, and let $\gamma = \alpha\beta^{-1}$ so that $\left(\frac{\gamma}{p}\right) = \varphi$. then there are bases x, y for Wp, k^{ε} and $W_{p,\ell}^{\varphi}$ respectively such that $Q(x) = p^k\beta/2$ and $Q(y) = p^\ell\gamma/2$. Since $W_{p,k}^{\varepsilon}$ and $W_{p,\ell}^{\varphi}$ are direct summands, $\tau_x, \tau_y \in \mathcal{O}(L)$.

But now

$$\operatorname{spin}(\tau_x\tau_y) = \operatorname{spin}(\tau_x)\operatorname{spin}(\tau_y) = p^{k+\ell}\beta\gamma/4 \equiv p\alpha \bmod (\mathbb{Q}_p^*)^2$$

since $k + \ell \equiv 1 \bmod 2$, so that $(1, p\alpha) \in \Sigma^{+}(L)$. Q.E.D.

THEOREM 9.5. *Let L be a quadratic $\mathbb{Z}_p$-module, $p \neq 2$. Then $\Sigma^{+}(L) = \Sigma^{++}(L)$ if and only if $L = W_{p,k_1}^{\varepsilon_1} \oplus \cdots \oplus W_{p,k_r}^{\varepsilon_r}$, with $k_i \equiv k_j \bmod 2$ for all i and j.*

PROOF. Write $L = W_{p,k_1}^{\varepsilon_1} \oplus \cdots \oplus W_{p,k_r}^{\varepsilon_r}$ with $k_1 \leq k_2 \leq \cdots \leq k_r$. We will proceed by induction on $r = \operatorname{rank}(L)$. Since the statement is invariant under scaling by Proposition 8.1, we may assume that $k_1 = 0$.

If there exist i, j with $k_i \not\equiv k_j \bmod 2$, then by Lemma 9.4, $\Sigma^{+}(L) \neq \Sigma^{++}(L)$.

Conversely, suppose that $k_i = k_j \bmod 2$ for all i and j. Since we have assumed that $k_1 = 0$, this is equivalent to having all k_i even. Let $L' = W_{p,k_2}^{\varepsilon_2} \oplus \cdots \oplus W_{p,k_r}^{\varepsilon_r}$. If $r = 1$ then $\Sigma(L') = \{(1,1)\}$ by convention; if $r \geq 2$, choose $\alpha_2 \in \mathbb{U}_2$ with $\left(\frac{\alpha_2}{p}\right) = \varepsilon_2$ so that the inductive hypothesis says that $\Sigma(L')$ is generated by $(-1, \alpha_2 p^{k_2}/2)$ and $\Sigma^{+}(L') = \Sigma^{++}(L')$, i.e., by $(-1, \alpha_2/2)$ and $\Sigma^{++}(L')$, since k_2 is even. By Corollary 4.6, $\Sigma(L)$ is generated by $\Sigma(L')$ and by $\{(-1, Q(z)) \mid z \in L, Q(z) \in \mathbb{U}_p\}$. But then $\Sigma^{+}(L)$ is generated by $\Sigma^{+}(L') = \Sigma^{++}(L')$ and $\{(1, \alpha_2 Q(z)/2) \mid z \in L, Q(z) \in \mathbb{U}_p\}$; since this latter set is contained in $\Sigma^{++}(L)$, we get $\Sigma^{+}(L) = \Sigma^{++}(L)$. Q.E.D.

Since $[\Sigma^{+}(L) \colon \Sigma^{++}(L)] \leq 2$, Theorem 9.5 reduces the calculation of $\Sigma^{+}(L)$ to that of $\Sigma^{++}(L)$.

THEOREM 9.6. *Let L be a quadratic $\mathbb{Z}_p$-module with $p \neq 2$. Then*

$$\Sigma^{++}(L) = \left\{(d, s) \in \{\pm 1\} \times \mathbb{Q}_p^*/(\mathbb{Q}_p^*)^2 \mid d = 1, s \not\equiv 0 \bmod p\right\}$$

unless $L = W_{p,k_1}^{\varepsilon_1} \oplus \cdots \oplus W_{p,k_r}^{\varepsilon_r}$ with $k_1 < k_2 < \cdots < k_r$, and there exist $\alpha_+, \alpha_- \in \mathbb{U}_p$ such that $\varepsilon_i = \left(\frac{\alpha_+}{p}\right)$ if k_i is even and $\varepsilon_i = \left(\frac{\alpha_-}{p}\right)$ if k_i is odd. In this latter case, $\Sigma^{++}(L) = \{(1,1)\}$, and $\Sigma(L) \subset \{(1,1), (1, \alpha_+\alpha_- p), (-1, \alpha_+), (-1, \alpha_- p)\}$.

PROOF. Write $L = W_{p,k_1}^{\varepsilon_1} \oplus \cdots \oplus W_{p,k_r}^{\varepsilon_r}$ with $k_1 \leq k_2 \leq \cdots \leq k_r$. We again proceed by induction on $r = \operatorname{rank}(L)$. As in Theorem 9.5, the statement is invariant under scaling by Proposition 8.1, so that we may assume that $k_1 = 0$.

Let $\alpha \in \mathbb{U}_p$ be a non-square, and note that $\{(d,s) \mid d = 1, s \not\equiv 0 \bmod p\} = \{(1,1),(1,\alpha)\}$. If there exists an i with $k_i = k_{i+1}$, then $(1,\alpha) \in \Sigma^{++}(L)$ by Corollary 9.2. So we may assume that $0 = k_1 < k_2 < \cdots < k_r$.

Similarly, if there exists an i and j with $k_i \equiv k_j \bmod 2$ and $\varepsilon_i\varepsilon_j = -1$, choose bases x_i, x_j for $W_{p,k_i}^{\varepsilon_i}$ and $W_{p,k_j}^{\varepsilon_j}$ respectively. Then $\tau_{x_i}, \tau_{x_j} \in \mathcal{O}(L)$, while

$$(\det(\tau_{x_i}\tau_{x_j}), \operatorname{spin}(\tau_{x_i}\tau_{x_j})) = (1, Q(x_i)Q(x_j)) = (1, p^{k_i+k_j}\alpha) = (1,\alpha) \in \Sigma^{++}(L).$$

Thus, $\Sigma^{++}(L) = \{(1,1)\}$ also implies the existence of α_+ and α_- with the stated properties.

Suppose now that L has these properties, namely that the k_i are strictly increasing, and that appropriate α_+ and α_- exist as stated. Let $L' = W_{p,k_2}^{\varepsilon_2} \oplus \cdots \oplus W_{p,k_r}^{\varepsilon_r}$. Since L' also has these properties, $\Sigma^{++}(L') = \{(1,1)\}$ and $\Sigma(L') \subset \{(1,1),(1,\alpha_+\alpha_-p),(-1,\alpha_+),(-1,p\alpha_-)\}$ by the inductive hypothesis. By Corollary 4.6, $\Sigma(L)$ is generated by $\Sigma(L')$ and $\{(-1,Q(z)) \mid z \in L, Q(z) \in \mathbb{U}_p\}$. But since $0 = k_1 < k_2$, if $Q(z) \in \mathbb{U}_p$ then $Q(z) \equiv \alpha_+ \bmod p$, so that $\Sigma(L)$ is generated by $\Sigma(L')$ and $(-1,\alpha_+)$; hence,

$$\Sigma(L) \subset \{(1,1),(1,\alpha_+\alpha_-p),(-1,\alpha_+),(-1,\alpha_-p)\}$$

and $\Sigma^{++}(L) = \{(1,1)\}$. Q.E.D.

10. Computation of $\Sigma^{\#}(L)$ for $p = 2$

In this section we compute $\Sigma^{\#}(L)$ for a quadratic $\mathbb{Z}_2$-module L, or, equivalently, for an even inner product $\mathbb{Z}_2$-module L. To make the computation useful in applications, we express it in terms of the *partial normal form*, whose definition we now recall (cf. Definition IV.4.1).

Definition 10.1. Let L be an inner product $\mathbb{Z}_2$-module. An expression for L in terms of the generators $\{U_k, V_k, W_{2,k}^{\varepsilon}\}$ of $\mathcal{I}_2$ is in *partial normal form* if the terms with scale k can be written as

$$(U_k)^{N(k)} \oplus (V_k)^{e(k)} \oplus W(k),$$

with $N(k) \geq 0$, $e(k) = 0$ or 1, and $W(k) = 0$, $W_{2,k}^{\varepsilon}$ or $W_{2,k}^{\varepsilon} \oplus W_{2,k}^{\varphi}$.

Notice that the integers $N(k)$, $e(k)$, and $\operatorname{rank}(W(k))$ are invariants of the partial normal form, and that an expression in normal form or alternate normal form is also in partial normal form.

We will express $\Sigma^{\#}(L)$ (for most L) in terms of the groups $\Gamma_{2,k}$; we recall the definition for the reader's convenience:

$\Gamma_{2,0} = \{(1,1),(1,3),(1,5),(1,7),(-1,1),(-1,3),(-1,5),(-1,7)\}$

$\Gamma_{2,1} = \{(1,1),(1,3),(1,5),(1,7)\}$

$\Gamma_{2,2} = \{(1,1),(1,5)\}$

$\Gamma_{2,k} = \{(1,1)\}$ for $k \geq 3$.

THEOREM 10.2. *Let L be a quadratic $\mathbb{Z}_2$-module in partial normal form, and write*

$$L = U_0^{N(0)} \oplus V_0^{e(0)} \oplus U_1^{N(1)} \oplus V_1^{e(1)} \oplus W(1) \oplus U_2^{N(2)} \oplus V_2^{e(2)} \oplus W(2) \oplus L'$$

with scale $(L') \geq 3$.

(10.2.1) If $N(0) + e(0) > 0$, then $\Sigma^{\#}(L) = \Gamma_{2,0}$

(10.2.2) If $N(0) = e(0) = 0$, $N(1) + e(1) > 0$ and $\operatorname{rank}(W(1)) > 0$, then $\Sigma^{\#}(L) = \Gamma_{2,0}$.

(10.2.3) If $N(0) = e(0) = \operatorname{rank}(W(1)) = 0$ and $N(1) + e(1) > 0$, then $\Sigma^{\#}(L) = \Gamma_{2,1}$.

(10.2.4) If $N(0) = e(0) = N(1) = e(1) = 0$ and $\operatorname{rank}(W(1)) > 0$, then $\Sigma^{\#}(L) \subset \Gamma_{2,0}$.

(10.2.5) If $N(0) = e(0) = N(1) = e(1) = \operatorname{rank}(W(1)) = 0$ and $N(2) + e(2) > 0$, then $\Sigma^{\#}(L) = \Gamma_{2,2}$.

(10.2.6) If $N(0) = e(0) = N(1) = e(1) = \operatorname{rank}(W(1)) = N(2) = e(2) = 0$ and $\operatorname{rank}(W(2)) = 2$, then $\Sigma^{\#}(L) = \Gamma_{2,2}$.

(10.2.7) If $N(0) = e(0) = N(1) = e(1) = \operatorname{rank}(W(1)) = N(2) = e(2) = 0$ and $\operatorname{rank}(W(2)) \leq 1$, then $\Sigma^{\#}(L) = \{(1,1)\}$.

REMARK 10.3. We will refine the computation in case (10.2.4) in Lemma 10.6 and Theorems 10.7 and 10.8 below.

PROOF. We first notice that the statement depends only on the integers $N(k) + e(k)$ and $\operatorname{rank}(W(k))$; in particular, we may replace the given expression for L with one in alternate normal form without affecting the truth of the theorem. Therefore we will assume for the proof that L is in alternate normal form.

The proof will proceed by induction on the rank. We begin by discussing (10.2.7). Assume L has scale k, and write L as

$$L = U_k^{N(k)} \oplus V_k^{e(k)} \oplus W(k) \oplus L'$$

where either $N(k)+e(k) > 0$ or $W(k) \neq 0$ or both. By hypothesis either $k \geq 3$ or $k = 2$, $N(2) = e(2) = 0$, and $\mathrm{rank}(W(2)) = 1$. We assume by induction that $\Sigma^{\#}(L') = \{(1,1)\}$. If $(W(k)) \neq 0$ then we may use Corollary 4.2 to conclude that $\Sigma^{\#}(L) = \{(1,1)\}$. If $W(k) = 0$ and $N(k) > 0$ then $k \geq 3$ and Corollary 5.6 implies that $\Sigma^{\#}(L) = \{(1,1)\}$. Finally if $W(k) = 0$ and $N(k) = 0$ then $e(k) = 1$ and $k \geq 3$; in this case Corollary 6.4 gives that $\Sigma^{\#}(L) = \{(1,1)\}$.

This finishes the proof of (10.2.7); note that we can conclude that whenever L has scale ≥ 3, Then $\Sigma^{\#}(L) = \{(1,1)\}$.

The hypotheses of (10.2.6) imply that L may be written as

$$L = W_{2,2}^{\varepsilon} \oplus W_{2,2}^{\varphi} \oplus L'$$

with $\mathrm{scale}(L') \geq 3$. Hence $\Sigma^{\#}(L') = \{(1,1)\}$ by (10.2.7). We conclude using Theorem 4.3 that $\Sigma^{\#}(L) = \Gamma_{2,2}$ as claimed.

To see (10.2.5), in this case we have that

$$L = U_2^{N(2)} \oplus V_2^{e(2)} \oplus W(2) \oplus L',$$

with $N(2) + e(2) > 0$ and $\mathrm{scale}(L') \geq 3$. Using (10.2.6) and (10.2.7) we have that $\Sigma^{\#}(W(2) \oplus L') \subset \Gamma_{2,2}$. Now using either Corollary 5.6 or Corollary 6.4, we see that $\Sigma^{\#}(L) = \Gamma_{2,2}$.

Note that (10.2.5-7) now give us that whenever $\mathrm{scale}(L) \geq 2$, we have $\Sigma^{\#}(L) \subset \Gamma_{2,2}$.

The assumptions of (10.2.4) allow us to write L as

$$L = W(1) \oplus L'$$

with $W(1) \neq 0$ and $\mathrm{scale}(L') \geq 2$. Hence $\Sigma^{\#}(L') \subset \Gamma_{2,2}$. In this case Corollary 4.5 implies that $\Sigma^{\#}(L)$ is generated by $\Sigma^{\#}(L')$ and $\{(-1, Q(z)) \mid 2 \nmid Q(z)\}$. This set is contained in $\Gamma_{2,0}$, hence so is $\Sigma^{\#}(L)$ as claimed.

The proof of (10.2.3) is similar to that of (10.2.5); in this case we may write L as

$$L = U_1^{N(1)} \oplus V_1^{e(1)} \oplus L'$$

with $\mathrm{scale}(L') \geq 2$ and $N(1) + e(1) > 0$. Therefore we have $\Sigma^{\#}(L') \subset \Gamma_{2,2}$. Hence using either Corollary 5.6 or Corollary 6.4 we see that $\Sigma^{\#}(L) = \Gamma_{2,1}$.

To see (10.2.2), these hypotheses imply that we may write L as

$$L = W(1) \oplus L'$$

where $W(1)$ has rank one or two and L' satisfies the hypotheses of (10.2.3). Hence $\Sigma^{\#}(L') = \Gamma_{2,1}$ as shown above. In this case we use Corollary 4.5 to conclude that $\Sigma^{\#}(L)$ is generated by $\Gamma_{2,1}$ and

$\{(-1, Q(z)) \mid 2 \nmid Q(z)\}$. This set exactly generates $\Gamma_{2,0}$, since there are z's (e.g., a generator of a $W^{\varepsilon}_{2,1}$ summand) with $2 \nmid Q(z)$.

Note that at this point we have shown that if $\mathrm{scale}(L) \geq 1$, then $\Sigma^{\#}(L) \subset \Gamma_{2,0}$.

Finally the assumptions of (10.2.1) imply that we can write L as

$$L = U_0^{N(0)} \oplus V_0^{e(0)} \oplus L'$$

where $N(0)+e(0) > 0$ and $\mathrm{scale}(L') \geq 1$. Then we have $\Sigma^{\#}(L') \subset \Gamma_{2,0}$. Moreover the assumption of alternate normal form gives that if $e(0) = 1$ then $W(1) = 0$. In this case we invoke either Corollary 5.6 or Corollary 6.4 to conclude that $\Sigma^{\#}(L) = \Gamma_{2,0}$; we note that if we need to use Corollary 6.4 then $e(0) = 1$ so that $W(1) = 0$ and we have satisfied the assumptions necessary to invoke Corollary 6.4.

This completes the proof of the Theorem. Q.E.D.

In order to finish the computation in case (10.2.4) of the Theorem, we need to study the reflections in $\mathcal{O}^{\#}(L)$.

LEMMA 10.4. *Let L be an inner product $\mathbb{Z}_2$-module.*

(10.4.1) If $L = W^{\varepsilon}_{2,k} \oplus W^{\varphi}_{2,k} \oplus L'$ with $\varepsilon \not\equiv \varphi \bmod 4$, then $\Sigma(L) \supset \Gamma_{2,1}$; if $k \leq 1$, then $\Sigma^{\#}(L) \supset \Gamma_{2,1}$.

(10.4.2) If $L = W^{\varepsilon}_{2,k} \oplus W^{\varphi}_{2,k} \oplus L'$ with $\varepsilon \equiv \varphi \bmod 4$, then $(1,5) \in \Sigma(L)$; if $k \leq 1$, then $(1,5) \in \Sigma^{\#}(L)$.

(10.4.3) If $L = W^{\varepsilon}_{2,k} \oplus W^{\varphi}_{2,k+2} \oplus L'$, then $(1,5) \in \Sigma(L)$; if $k \leq 1$, then $(1,5) \in \Sigma^{\#}(L)$.

(10.4.4) If $L = W^{\varepsilon}_{2,k} \oplus W^{\varphi}_{2,k+1} \oplus L'$, then $(1, 1+2\varepsilon\varphi) \in \Sigma(L)$; if $k \leq 1$, then $(1, 1+2\varepsilon\varphi) \in \Sigma^{\#}(L)$.

PROOF. Let $L = W^{\varepsilon}_{2,k} \oplus W^{\varphi}_{2,k+\ell} \oplus L'$, and let x and y span $W^{\varepsilon}_{2,k}$ and $W^{\varphi}_{2,k+\ell}$ respectively so that $Q(x) = 2^{k-1}\varepsilon$ and $Q(y) = 2^{k+\ell-1}\varphi$.

If $\ell = 0$, by Proposition IV.3.1(I), there is some $z = ax + by$ such that $Q(z) = 2^{k-1} \cdot 5\varepsilon$. Then τ_x and τ_z are in $\mathcal{O}(L)$ (respectively $\mathcal{O}^{\#}(L)$ if $k \leq 1$ by Proposition 2.3) so that $(1, Q(x)Q(z)) = (1,5) \in \Sigma(L)$ (respectively $\Sigma^{\#}(L)$ if $k \leq 1$). This proves (10.4.2). If in addition $\varepsilon \not\equiv \varphi \bmod 4$, then $\tau_x\tau_y \in \mathcal{O}(L)$ (respectively $\mathcal{O}^{\#}(L)$ if $k \leq 1$) so that $(1, Q(x)Q(y)) = (1, \varepsilon\varphi) \in \Sigma(L)$ (respectively $\Sigma^{\#}(L)$ if $k \leq 1$). Since $\varepsilon\varphi \not\equiv 5 \bmod 8$, $(1,5)$ and $(1,\varepsilon\varphi)$ generate $\Gamma_{2,1}$, proving (10.4.1).

If $\ell = 1$, then $Q(x+y) = 2^{k-1}(\varepsilon + 2\varphi)$ so that τ_x and τ_{x+y} are in $\mathcal{O}(L)$ (respectively $\mathcal{O}^{\#}(L)$ if $k \leq 1$). Thus, $(1, Q(x)Q(x+y)) = (1, 1+2\varepsilon\varphi) \in \Sigma(L)$ (respectively $\Sigma^{\#}(L)$ if $k \leq 1$), proving (10.4.4).

Finally, if $\ell = 2$, then $Q(x+y) = 2^{k-1}(\varepsilon + 4\varphi)$ so that again τ_x and τ_{x+y} are in $\mathcal{O}(L)$ (respectively $\mathcal{O}^{\#}(L)$ if $k \le 1$) and $(1, Q(x)Q(x+y)) = (1,5) \in \Sigma(L)$ (respectively $\Sigma^{\#}(L)$ if $k \le 1$). This proves (10.4.3) and completes the proof of the lemma. Q.E.D.

LEMMA 10.5. *Let L be an inner product $\mathbb{Z}_2$-module, and let $\alpha \in \mathbb{U}_p$.*

(10.5.1) If $L = W_{2,k}^{\varepsilon} \oplus W_{2,k}^{\varphi} \oplus U_{k+1}^{N(k+1)} \oplus V_{k+1}^{e(k+1)} \oplus L'$ with scale$(L') \ge k+2$, if $\varepsilon \equiv \varphi \bmod 4$, and if $x \in L$ such that $Q(x) = 2^{k-1}\alpha$, then $\alpha \equiv \varepsilon$ or $5\varepsilon \bmod 8$.

(10.5.2) If $L = W_{2,k}^{\varepsilon} \oplus U_{k+1}^{N(k+1)} \oplus V_{k+1}^{e(k+1)} \oplus L'$ with scale$(L') \ge k+2$ and if $x \in L$ such that $Q(x) = 2^{k-1}\alpha$, then $\alpha \equiv \varepsilon$ or $5\varepsilon \bmod 8$.

(10.5.3) If $L = W_{2,k}^{\varepsilon} \oplus W_{2,k+1}^{\varphi} \oplus U_{k+2}^{N(k+2)} \oplus V_{k+2}^{N(k+2)} \oplus L'$ with scale$(L') \ge k+3$, and if $x \in L$ such that $Q(x) = 2^{k-1}\alpha$, then $\alpha \equiv \varepsilon$ or $(1+2\varepsilon\varphi)\varepsilon \bmod 8$.

(10.5.4) If $L = W_{2,k}^{\varepsilon} \oplus U_{k+2}^{N(k+2)} \oplus V_{k+2}^{N(k+2)} \oplus L'$ with scale$(L') \ge k+3$, and if $x \in L$ such that $Q(x) = 2^{k-1}\alpha$, then $\alpha \equiv \varepsilon \bmod 8$.

PROOF. Write $x = y+z$, with $y \in$ (sum of W's), $z \in$ (sum of U, V, L').

In the cases (10.5.1) and (10.5.2), we have $Q(z) \in 2^{k+1}\mathbb{Z}_2$ so that $2^{1-k}Q(x) \equiv 2^{1-k}Q(y) \bmod 4$. Our claim then becomes: for every $y \in$ (sum of W's) with $Q(y) \in 2^{k-1}\mathbb{U}_2$ we have $2^{1-k}Q(y) \equiv \varepsilon \bmod 4$.

In cases (10.5.3) and (10.5.4), $Q(z) \in 2^{k+2}\mathbb{Z}_2$ so that $2^{1-k}Q(x) \equiv 2^{1-k}Q(y) \bmod 8$. Our claim is then: for every $y \in$ (sum of W's) with $Q(y) \in 2^{k-1}\mathbb{U}_2$ we have $2^{1-k}Q(y) \equiv \varepsilon$ or $(1+2\varepsilon\varphi)\varepsilon \bmod 8$ in case (10.5.3), and $2^{1-k}Q(y) \equiv \varepsilon \bmod 8$ in case (10.5.4).

Now any such y must split off from the sum of the W's, and so gives as relation among the W's; all such relations were given in Proposition IV.3.1. In case (10.5.4) there is no relevant relation which could apply, and we conclude that $2^{1-k}Q(y) \equiv \varepsilon \bmod 8$.

In case (10.5.2), again there is only one W, and the only relevant relation is relation (VII):

$$W_{2,k}^{\varepsilon} \oplus U_k \cong W_{2,k}^{5\varepsilon} \oplus V_k.$$

We may therefore conclude that $2^{1-k}Q(y) = \varepsilon$ or $5\varepsilon \bmod 8$ as required.

In case (10.5.1), we have this relation above, and in addition the relation (I):

$$W_{2,k}^{\varepsilon} \oplus W_{2,k}^{\varphi} \cong W_{2,k}^{5\varepsilon} \oplus W_{2,k}^{5\varphi}.$$

We again conclude that $2^{1-k}Q(y) = \varepsilon$ or $5\varepsilon \bmod 8$ as required.

Finally in case (10.5.3), the only relevant relation is (VI):

$$W_{2,k}^{\varepsilon} \oplus W_{2,k+1}^{\varphi} \cong W_{2,k}^{\varepsilon+2\varphi} \oplus W_{2,k+1}^{\varphi+2\varepsilon}$$

which shows that $2^{1-k}Q(y) \equiv \varepsilon$ or $\varepsilon + 2\varphi = (1+2\varepsilon\varphi)\varepsilon \bmod 8$. Q.E.D.

We are now ready to finish the computation of $\Sigma^{\#}(L)$ in case (10.2.4) of Theorem 10.2. Define

$$\Sigma^{\#,+}(L) = \left\{(d,s) \in \Sigma^{\#}(L) \mid d = 1\right\}.$$

We first compute the quotient $\Sigma^{\#}(L)/\Sigma^{\#,+}(L)$.

LEMMA 10.6. *Let $L = W_{2,1}^{\varepsilon} \oplus L'$ be a quadratic $\mathbb{Z}_2$-module. Then the index $\left[\Sigma^{\#}(L)\colon \Sigma^{\#,+}(L)\right] = 2$, and $\Sigma^{\#}(L)/\Sigma^{\#,+}(L)$ is generated by $(-1,\varepsilon)$.*

PROOF. In any case, $\left[\Sigma^{\#}(L)\colon \Sigma^{\#,+}(L)\right] \leq 2$, so we merely must find something in $\Sigma^{\#}(L) - \Sigma^{\#,+}(L)$. Let x span $W_{2,1}^{\varepsilon}$ with $Q(x) = \varepsilon$. Then $\tau_x \in \mathcal{O}^{\#}(L)$, while $(\det(\tau_x), \operatorname{spin}(\tau_x)) = (-1,\varepsilon)$. Q.E.D.

THEOREM 10.7. *Let $L = W_{2,1}^{\varepsilon} \oplus L'$ be a quadratic $\mathbb{Z}_2$-module in partial normal form with scale $(L') \geq 2$, and write*

$$L' = U_2^{N(2)} \oplus V_2^{e(2)} \oplus W(2) \oplus U_3^{N(3)} \oplus V_3^{e(3)} \oplus W(3) \oplus L''$$

where scale$(L'') \geq 4$.

(10.7.1) If $N(2) + e(2) + \operatorname{rank}(W(3)) > 0$ and $\operatorname{rank}(W(2)) > 0$, then $\Sigma^{\#}(L') \subset \Gamma_{2,2}$ and $\Sigma^{\#,+}(L) = \Gamma_{2,1}$.

(10.7.2) If $N(2) + e(2) + \operatorname{rank}(W(3)) > 0$ and $\operatorname{rank}(W(2)) = 0$, then $\Sigma^{\#}(L') \subset \Gamma_{2,2}$ and $\Sigma^{\#,+}(L) = \Gamma_{2,2}$.

(10.7.3) If $N(2) = e(2) = \operatorname{rank}(W(3)) = 0$ and $\operatorname{rank}(W(2)) = 2$, then $\Sigma^{\#}(L') = \Gamma_{2,2}$ and $\Sigma^{\#,+}(L) = \Gamma_{2,1}$.

(10.7.4) If $N(2) = e(2) = \operatorname{rank}(W(3)) = 0$ and $W(2) = W_{2,2}^{\varphi}$, then $\Sigma^{\#}(L') = \{(1,1)\}$ and $\Sigma^{\#,+}(L) = \{(1,1),(1,1+2\varepsilon\varphi)\}$.

(10.7.5) If $N(2) = e(2) = \operatorname{rank}(W(2)) = \operatorname{rank}(W(3)) = 0$, then $\Sigma^{\#}(L') = \{(1,1)\}$ and $\Sigma^{\#,+}(L) = \{(1,1)\}$.

PROOF. By Corollary 4.5, $\Sigma^{\#}(L)$ is generated by $\Sigma^{\#}(L')$ and $\{(-1,Q(x)) \mid x \in L, Q(x) \in \mathbb{U}_2\}$. In each case we can bound or actually compute $\Sigma^{\#}(L')$ using Theorem 10.2; we get the results stated above. Note that in each case $\Sigma^{\#,+}(L') = \Sigma^{\#}(L')$, i.e., there are no $d = -1$ elements in $\Sigma^{\#}(L')$.

Thus the group $\Sigma^{\#,+}(L)$ is generated by $\Sigma^{\#}(L')$ and $\{(1, Q(x)Q(y)) \mid x, y \in L, Q(x), Q(y) \in \mathbb{U}_2\}$. Hence we simply need to find the possible set of reflections.

(10.7.1): If $N(2) + e(2) > 0$ then $\Sigma^{\#,+}(L') = \Gamma_{2,2}$ by (10.2.5). On the other hand, if $\mathrm{rank}(W(3)) > 0$, then $(1,5) \in \Sigma^{\#,+}(L)$ by (10.4.3). So $(1,5) \in \Sigma^{\#,+}(L)$ in either case. Also, since $\mathrm{rank}(W(2)) > 0$, by (10.4.4), either $(1,3)$ or $(1,7) \in \Sigma^{\#,+}(L)$. But this implies that $\Sigma^{\#,+}(L) = \Gamma_{2,1}$.

(10.7.2): As in (10.7.1), $(1,5) \in \Sigma^{\#,+}(L)$. On the other hand, $\Sigma^{\#,+}(L') \subset \Gamma_{2,2}$ by (10.2.5-7). Now for every $x \in L$ with $Q(x) \in \mathbb{U}_2$, $Q(x) \equiv \varepsilon$ or $5\varepsilon \bmod 8$ by (10.5.2). Therefore the extra generators $(1, Q(x)Q(y))$ of $\Sigma^{\#,+}(L)$ lie in $\Gamma_{2,2}$. Since $(1,5) \in \Sigma^{\#,+}(L)$, we conclude that $\Sigma^{\#,+}(L) = \Gamma_{2,2}$.

(10.7.3): Note that either $(1,3)$ or $(1,7) \in \Sigma^{\#,+}(L)$ by (10.4.4). On the other hand $\Sigma^{\#}(L') = \Gamma_{2,2}$. Hence we conclude that $\Sigma^{\#,+}(L) = \Gamma_{2,1}$.

(10.7.4): By (10.4.4), $(1, 1 + 2\varepsilon\varphi) \in \Sigma^{\#,+}(L)$. Also, we have $\Sigma^{\#,+}(L') = \{(1,1)\}$. Now for every $x \in L$ with $Q(x) \in \mathbb{U}_2$, $Q(x) \equiv \varepsilon$ or $(1 + 2\varepsilon\varphi)\varepsilon \bmod 8$ by (10.5.3). Therefore the extra generators $(1, Q(x)Q(y))$ of $\Sigma^{\#,+}(L)$ lie in $\{(1,1), (1, 1+2\varepsilon\varphi)\}$, and so $\Sigma^{\#,+}(L) = \{(1,1), (1, 1 + 2\varepsilon\varphi)\}$.

(10.7.5): We see that $\Sigma^{\#,+}(L') = \{(1,1)\}$ by (10.2.7), and by (10.5.4) we see that for every $x \in L$ with $Q(x) \in \mathbb{U}_2$, $Q(x) \equiv \varepsilon \bmod 8$. Hence the extra generators are all $(1,1)$, and so $\Sigma^{\#,+}(L) = \{(1,1)\}$. Q.E.D.

THEOREM 10.8. *Let $L = W_{2,1}^{\varepsilon} \oplus W_{2,1}^{\varphi} \oplus L'$ be a quadratic $\mathbb{Z}_p$-module in partial normal form with scale$(L') \geq 2$, and write*

$$L' = U_2^{N(2)} \oplus V_2^{e(2)} \oplus W(2) \oplus L''$$

where scale$(L'') \geq 3$.

(10.8.1) If $\varepsilon \not\equiv \varphi \bmod 4$, then $\Sigma^{\#,+}(L) = \Gamma_{2,1}$.

(10.8.2) If $\varepsilon \equiv \varphi \bmod 4$ and $\mathrm{rank}(W(2)) > 0$, then $\Sigma^{\#,+}(L) = \Gamma_{2,1}$.

(10.8.3) If $\varepsilon \equiv \varphi \bmod 4$ and $\mathrm{rank}(W(2)) = 0$, then $\Sigma^{\#,+}(L) = \Gamma_{2,2}$.

PROOF. First note that by (10.4.1-2), $(1,5) \in \Sigma^{\#,+}(L)$. We proceed as in the proof of Theorem 10.7: note that by Corollary 4.5 and Lemma 10.6, $\Sigma^{\#,+}(L)$ is generated by $\Sigma^{\#,+}(W_{2,1}^{\varphi} \oplus L')$ and $\{(1, \varepsilon Q(x)) \mid x \in L, Q(x) \in \mathbb{U}_2\}$; and with our assumptions, we obtain information about $\Sigma^{\#,+}(W_{2,1}^{\varphi} \oplus L')$ from Theorem 10.7.

(10.8.1): In this case, $\Sigma^{\#,+}(L) = \Gamma_{2,1}$ by (10.4.1).

(10.8.2): In this case, by (10.4.4), either $(1,3)$ or $(1,7) \in \Sigma^{\#,+}(L)$; since we already know $(1,5) \in \Sigma^{\#,+}(L)$, we get $\Sigma^{\#,+}(L) = \Gamma_{2,1}$.

(10.8.3): By (10.7.2) and (10.7.5), $\Sigma^{\#,+}(W_{2,1}^{\varphi} \oplus L') \subset \Gamma_{2,2}$, and we already know that $\Gamma_{2,2} \subset \Sigma^{\#,+}(L)$. So we must show: for every $x \in L$ with $Q(x) \in \mathbb{U}_2$, $\varepsilon Q(x) \equiv 1$ or $5 \bmod 8$. This is the content of (10.5.1). Q.E.D.

11. Computation of $\Sigma^+(L)$ for $p = 2$

In this section, we compute $\Sigma^+(L)$ for an inner product $\mathbb{Z}_2$-module L. We begin by considering $\Sigma^+(L)/\Sigma^{++}(L)$.

For elements s of $\mathbb{Q}_2^*/(\mathbb{Q}_2^*)^2$, we will say that s is a *unit* if $s \in \mathbb{U}_2 \bmod (\mathbb{Q}_2^*)^2$, and that s is a *non-unit* (or is not a unit) if not (i.e., $s \in 2\mathbb{U}_2 \bmod (\mathbb{Q}_2^*)^2$).

LEMMA 11.1. *Let L be an inner product $\mathbb{Z}_2$-module, and suppose that either $L = U_k \oplus L'$, $L = V_k \oplus L'$ or $L = W_{2,k+1}^{\varepsilon} \oplus L'$. Then there exists some $(-1,s) \in \Sigma(L)$ such that if $k \equiv 0 \bmod 2$ then s is a unit, while if $k \equiv 1 \bmod 2$ then s is a non-unit.*

PROOF. In any of these cases, there is some $x \in U_k$ (respectively V_k, $W_{2,k+1}^{\varepsilon}$) such that $Q(x) \in 2^k\mathbb{U}_2$ and for every $t \in L$, $\langle x,t\rangle \in 2^k\mathbb{Z}_2$. By Lemma 2.1, $\tau_x \in \mathcal{O}(L)$. But then $\det(\tau_x) = -1$, and if $k \equiv 0 \bmod 2$, then $\operatorname{spin}(\tau_x) \equiv 2^{-k}Q(x) \in \mathbb{U}_2$ while if $k \equiv 1 \bmod 2$ then $\operatorname{spin}(\tau_x) \equiv 2^{-k+1}Q(x) \in 2\mathbb{U}_2$. Q.E.D.

THEOREM 11.2. *Let L be an inner product $\mathbb{Z}_2$-module in partial normal form. Then $\Sigma^+(L) = \Sigma^{++}(L)$ if and only if there is some $\ell \in \mathbb{Z}/2\mathbb{Z}$ such that:*

(1) *If $k \equiv \ell \bmod 2$, then $W(k) = 0$*

(2) *If $k \not\equiv \ell \bmod 2$, then $N(k) = e(k) = 0$. If in addition $\operatorname{rank}(W(k)) = 2$, then $W(k) = W_{2,k}^{\varepsilon} \oplus W_{2,k}^{\varphi}$ with $\varepsilon + \varphi \equiv 0 \bmod 4$.*

Moreover, if such an ℓ exists, and if $(-1,s) \in \Sigma(L)$, then s is always a unit in the case $\ell = 0$, while s is never a unit in the case $\ell = 1$.

REMARK 11.3. If $\Sigma^{++}(L) = \Gamma_{2,1}$, then in the case $\Sigma^+(L) \neq \Sigma^{++}(L)$, we have that $\Sigma^+(L)/\Sigma^{++}(L)$ can be generated by $(1,2)$, for example. When we compute $\Sigma^{++}(L)$ in Theorems 11.4 and 11.6 below, we shall give potential generators for $\Sigma^+(L)/\Sigma^{++}(L)$ in those cases in which $\Sigma^{++}(L) \neq \Gamma_{2,1}$.

PROOF. Since by Lemma 8.2 there are reflections in $\mathcal{O}(L)$, and hence there are elements of the form $(-1,s) \in \Sigma(L)$, we see that $\Sigma^+(L) = \Sigma^{++}(L)$ if and only if either for all $(-1,s) \in \Sigma(L)$ we have

that s is a unit or for all $(-1,s) \in \Sigma(L)$ we have that s is a non-unit. Thus, Lemma 11.1 shows that any module L with $\Sigma^+(L) = \Sigma^{++}(L)$ must satisfy all statements in the Theorem, including the Moreover, except perhaps the last sentence of (2). But if there is a $k \not\equiv \ell \bmod 2$ with $W(k) = W^{\varepsilon}_{2,k} \oplus W^{\varphi}_{2,k}$ and $\varepsilon + \varphi \not\equiv 0 \bmod 4$, by Lemma 7.3 there is some $z \in L$ with $Q(z) \in 2^k\mathbb{U}_2$. If x spans $W^{\varepsilon}_{2,k}$, then $(\det(\tau_x\tau_z), \mathrm{spin}(\tau_x\tau_z)) \notin \Sigma^{++}(L)$, a contradiction since it is obviously in $\Sigma^+(L)$. Hence, any L with $\Sigma^+(L) = \Sigma^{++}(L)$ satisfies all the stated conditions.

Conversely, suppose that L satisfies (1) and (2). To show that $\Sigma^+(L) = \Sigma^{++}(L)$, we proceed by induction on the rank. By Proposition 8.1, the statement of the theorem is invariant under scaling, so we may assume that L has scale 0. It is not hard to see that we may also assume without loss of generality that L is in alternate normal form.

Suppose first that $\ell = 0$. Then $L = U_0^{N(0)} \oplus V_0^{e(0)} \oplus L'$ with scale $L' \geq 1$ and $N(0)+e(0) > 0$. If $N(0) > 0$, then by Corollary 5.7, $\Sigma(L) = \Gamma_{2,0}\cdot\Sigma(L')$. If $N(0) = 0$ and $e(0) > 0$, then since L is in alternate normal form, Lemma 7.4 guarantees that we may apply Corollary 6.5 to again get $\Sigma(L) = \Gamma_{2,0}\cdot\Sigma(L')$. But now for every $(-1,s) \in \Gamma_{2,0}$, s is a unit; this also holds for $(-1,s) \in \Sigma(L')$ by the inductive hypothesis, and so holds for every $(-1,s) \in \Sigma(L)$. But that implies that $\Sigma^+(L) = \Sigma^{++}(L)$.

Suppose instead that $\ell = 1$. Then we may write $L = W^{\varepsilon}_{2,0} \oplus L' \oplus L''$ with $\mathrm{scale}(L'') \geq 1$, $Q(L'') \subset 2\mathbb{Z}_2$ and either $L' = 0$ or $L' = W^{\varphi}_{2,0}$ with $\varepsilon + \varphi \equiv 0 \bmod 4$. By Theorem 4.8, $\Sigma(L)$ is generated by $\Sigma(L' \oplus L'')$ and by

$$\{(-1, Q(z)) \mid z \in L, 4 \nmid Q(z), \text{ and if } 2 \mid Q(z) \text{ then } 2 \mid \langle z,t\rangle \text{ for all } t \in L\}.$$

By the inductive hypothesis, if $(-1,s) \in \Sigma(L' \oplus L'')$ then s is not a unit. Also, if $Q(z) \in \frac{1}{2}\mathbb{U}_2$ (respectively $2\mathbb{U}_2$) then $Q(z)$ in a non-unit (considered as an element of $\mathbb{Q}_2^*/(\mathbb{Q}_2^*)^2$). Thus, we only need to show that for every $z \in L$, $Q(z) \notin \mathbb{U}_2$.

Let x span $W^{\varepsilon}_{2,0}$ with $Q(x) = \varepsilon/2$. If $L' = 0$, then $z = ax + t$ for some $t \in L''$ and $Q(z) = a^2\varepsilon/2 + Q(t)$; since $t \in L''$, $2 \mid Q(t)$ which implies that $Q(z)$ is not in $\mathbb{U}_2$. If $L' = W^{\varphi}_{2,0}$, let y span L' with $Q(y) = \varphi/2$. Then $z = ax + by + t$ for some $t \in L''$, and $Q(z) = a^2\varepsilon/2 + b^2\varphi/2 + Q(t)$, and since $2 \mid Q(t)$, we see that $Q(z) \in \mathbb{U}_2$ if and only if $Q(ax+by) = (a^2\varepsilon + b^2\varphi)/2 \in \mathbb{U}_2$. But since $\varepsilon + \varphi \equiv 0 \bmod 4$, by Lemma 7.3, $Q(ax+by) \notin \mathbb{U}_2$. Q.E.D.

We now turn to the computation of $\Sigma^{++}(L)$.

THEOREM 11.4. *Let L be an inner product $\mathbb{Z}_2$-module such that $L = U_k \oplus L'$ or $L = V_k \oplus L'$. Then $\Sigma^{++}(L) = \Gamma_{2,1}$.*

PROOF. Since $\Sigma^{++}(L) \subset \Gamma_{2,1}$, it suffices to show that $\Sigma^{++}(U_k) = \Sigma^{++}(V_k) = \Gamma_{2,1}$. Since Σ^{++} is invariant under scaling by Proposition 8.1, we only need to show $\Sigma^{++}(U_0) = \Gamma_{2,1}$ and $\Sigma^{++}(V_0) = \Gamma_{2,1}$. The first follows from Corollary 5.7, and the second from Corollary 6.5. Q.E.D.

LEMMA 11.5. *Let L be an inner product $\mathbb{Z}_2$-module.*

(11.5.1) If $L = W^{\varepsilon}_{2,k} \oplus W^{\varphi}_{2,k+3} \oplus L'$, then $(1, 1 + 2\varepsilon\varphi) \in \Sigma(L)$.

(11.5.2) If $L = W^{\varepsilon}_{2,k} \oplus W^{\varphi}_{2,k+4} \oplus L'$, then $(1, 5) \in \Sigma(L)$.

(11.5.3) If $L = W^{\varepsilon}_{2,k} \oplus W^{\varphi}_{2,k} \oplus L'$ with $\varepsilon \equiv \varphi \bmod 4$, then $(1, 1 + \varepsilon\varphi) \in \Sigma(L)$.

(11.5.4) If $L = W^{\varepsilon}_{2,k} \oplus W^{\varphi}_{2,k} \oplus W^{\psi}_{2,k+2} \oplus L'$ with $\varepsilon \equiv \varphi \equiv \psi \bmod 4$, then $\Sigma^{++}(L) = \Gamma_{2,1}$.

(11.5.5) If $L = W^{\varepsilon}_{2,k} \oplus W^{\varphi}_{2,k+2} \oplus W^{\psi}_{2,k+2} \oplus L'$ with $\varepsilon \equiv \varphi \equiv \psi \bmod 4$, then $\Sigma^{++}(L) = \Gamma_{2,1}$.

PROOF. (11.5.1): Let x, y span $W^{\varepsilon}_{2,k}$ and $W^{\varphi}_{2,k+3}$, respectively, with $Q(x) = 2^{k-1}\varepsilon$, $Q(y) = 2^{k+2}\varphi$. Then $Q(2x + y) = 2^{k+1}(\varepsilon + 2\varphi)$ and for every $t \in L$, $\langle 2x + y, t\rangle \in 2^{k+1}\mathbb{Z}_2$. Thus $\tau_{2x+y} \in \mathcal{O}(L)$; since $\tau_x \in \mathcal{O}(L)$, we get $(1, \mathrm{spin}(\tau_x\tau_{2x+y})) \in \Sigma(L)$. But

$$\mathrm{spin}(\tau_x\tau_{2x+y}) = Q(x)Q(2x + y) = 2^{2k}\varepsilon(\varepsilon + 2\varphi) \equiv 1 + 2\varepsilon\varphi \bmod (\mathbb{Q}_2^*)^2.$$

(11.5.2): Let x, y span $W^{\varepsilon}_{2,k}$ and $W^{\varphi}_{2,k+4}$, respectively, with $Q(x) = 2^{k-1}\varepsilon$, $Q(y) = 2^{k+3}\varphi$. Then $Q(2x + y) = 2^{k+1}(\varepsilon + 4\varphi)$ and for every $t \in L$, $\langle 2x + y, t\rangle \in 2^{k+1}\mathbb{Z}_2$. Thus $\tau_{2x+y} \in \mathcal{O}(L)$; since $\tau_x \in \mathcal{O}(L)$, we get $(1, \mathrm{spin}(\tau_x\tau_{2x+y})) \in \Sigma(L)$. But

$$\mathrm{spin}(\tau_x\tau_{2x+y}) = Q(x)Q(2x + y) = 2^{2k}\varepsilon(\varepsilon + 4\varphi) \equiv 1 + 4\varphi\varepsilon \bmod (\mathbb{Q}_2^*)^2$$

and $1 + 4\varphi\varepsilon \equiv 5 \bmod 8$.

(11.5.3): Let x, y span $W^{\varepsilon}_{2,k}$ and $W^{\varphi}_{2,k}$, respectively, with $Q(x) = 2^{k-1}\varepsilon$, $Q(y) = 2^{k-1}\varphi$. Then $Q(x + y) = 2^{k-1}(\varepsilon + \varphi) \equiv 2^k \bmod 2^{k+1}$ since $\varepsilon \equiv \varphi \bmod 4$ (and hence $\varepsilon + \varphi \equiv 2 \bmod 4$). Also, for every $t \in L$, $\langle x + y, t\rangle \in 2^k\mathbb{Z}_2$, so that $\tau_{x+y} \in \mathcal{O}(L)$; since $\tau_x \in \mathcal{O}(L)$, we get $(1, \mathrm{spin}(\tau_x\tau_{x+y})) \in \Sigma(L)$. But

$$\mathrm{spin}(\tau_x\tau_{x+y}) = Q(x)Q(x + y) = 2^{2k-2}\varepsilon(\varepsilon + \varphi) \equiv 1 + \varepsilon\varphi \bmod (\mathbb{Q}_2^*)^2$$

so that $(1, 1 + \varepsilon\varphi) \in \Sigma(L)$.

(11.5.4): Let x, y, and z span $W^{\varepsilon}_{2,k}$, $W^{\varphi}_{2,k}$ and $W^{\psi}_{2,k+2}$, respectively, with $Q(x) = 2^{k-1}\varepsilon$, $Q(y) = 2^{k-1}\varphi$ and $Q(z) = 2^{k+1}\psi$. Then $Q(2x+2y+$

$z) = 2^{k+1}(\varepsilon+\varphi+\psi)$ and for every $t \in L$, $\langle 2x+2y+z, t\rangle \in 2^{k+1}\mathbb{Z}_2$. Thus $\tau_{2x+2y+z} \in \mathcal{O}(L)$; since $\tau_x \in \mathcal{O}(L)$ we get $(1, \mathrm{spin}(\tau_x\tau_{2x+2y+z})) \in \Sigma(L)$. But

$$\mathrm{spin}(\tau_x\tau_{2x+2y+z}) = Q(x)Q(2x+2y+z) = 2^{2k}\varepsilon(\varepsilon+\varphi+\psi) \equiv \varepsilon(\varepsilon+\varphi+\psi) \bmod (\mathbb{Q}_2^*)^2$$

and $\varepsilon(\varepsilon+\varphi+\psi) \equiv 3 \bmod 4$ since $\varepsilon \equiv \varphi \equiv \psi \bmod 4$. Thus, either $(1,3)$ or $(1,7) \in \Sigma(L)$. But by Lemma 10.4.2, $(1,5) \in \Sigma(L)$. Thus, $\Sigma(L) \supset \Gamma_{2,1}$ so $\Sigma^{++}(L) = \Gamma_{2,1}$.

(11.5.5): Let x, y, z span $W^{\varepsilon}_{2,k}$, $W^{\varphi}_{2,k+2}$ and $W^{\psi}_{2,k+2}$, respectively, with $Q(x) = 2^{k-1}\varepsilon$, $Q(y) = 2^{k+1}\varphi$ and $Q(z) = 2^{k+1}\psi$. Then $Q(2x+y+z) = 2^{k+1}(\varepsilon+\varphi+\psi)$ and for every $t \in L$, $\langle 2x+y+z, t\rangle \in 2^{k+1}\mathbb{Z}_2$. Therefore as above $\tau_x, \tau_{2x+y+z} \in \mathcal{O}(L)$ so that

$$\mathrm{spin}(\tau_x\tau_{2x+2y+z}) \equiv \varepsilon(\varepsilon+\varphi+\psi) \equiv 3 \bmod 4.$$

Hence as above, $(1,3)$ or $(1,7) \in \Sigma(L)$; again by Lemma 10.4.2, $(1,5) \in \Sigma(L)$ so that $\Sigma^{++}(L) = \Gamma_{2,1}$. Q.E.D.

In view of Theorem 11.4, we may restrict our attention to diagonal lattices $L = W^{\varepsilon_1}_{2,k_1} \oplus \cdots \oplus W^{\varepsilon_r}_{2,k_r}$ with $k_1 \le \cdots \le k_r$ and $k_i < k_{i+2}$ for each i.

THEOREM 11.6. *Let $L = W^{\varepsilon_1}_{2,k_1} \oplus \cdots \oplus W^{\varepsilon_r}_{2,k_r}$ be an inner product $\mathbb{Z}_2$-module with $k_1 \le \cdots \le k_r$ and $k_i < k_{i+2}$ for each i. Then $\Sigma^{++}(L) = \Gamma_{2,1}$ unless there is an $\ell \in \mathbb{Z}/4\mathbb{Z}$ and $\varepsilon_+, \varepsilon_- \in \mathbb{U}_2$ such that:*

(1) *For all i,*

$$\varepsilon_i = \begin{cases} \varepsilon_+ \text{ or } (2\ell+1)\varepsilon_+ \bmod 8, & \text{if } k_i \text{ is even} \\ \varepsilon_- \text{ or } (2\ell+1)\varepsilon_- \bmod 8, & \text{if } k_i \text{ is odd.} \end{cases}$$

(2) *Suppose there exist $i \ne j$ with $|k_i - k_j| \le 4$. Then $\ell \ne 0$ and $|k_i - k_j| \equiv \ell \bmod 2$. If in addition ℓ is odd, then*

$$\varepsilon_i\varepsilon_j \equiv \ell \bmod 4.$$

(3) *If there exists an i with $k_i = k_{i+1}$, then $\ell = 2$, $|k_i - k_j| \ge 4$ for all $j \ne i, i+1$ and $1 + \varepsilon_i\varepsilon_{i+1} \equiv 2\varepsilon_+\varepsilon_- \bmod 8$.*

(4) *If $\ell \ne 0$, either there exist i, j with $i \ne j$ and $|k_i - k_j| \le 4$, or there exist i and j with $k_i \equiv k_j \bmod 2$ and $\varepsilon_i \equiv (2\ell+1)\varepsilon_j \bmod 8$.*

In this case, $\Sigma^{++}(L) = \{(1,1), (1, 2\ell+1)\}$. Moreover, $\Sigma^{+}(L)/\Sigma^{++}(L)$ is either trivial or generated by $(1, 2\varepsilon_+\varepsilon_-)$.

PROOF. We first show that if $\Sigma^{++}(L) \neq \Gamma_{2,1}$, then the desired ℓ, ε_+, and ε_- exist, and that for such an L, $(1, 2\ell+1) \in \Sigma^{++}(L)$; we will use induction on the rank at one step.

First note then that if L has rank one, we may take $\ell = 0$, and $\Sigma^+(L) = \Sigma^{++}(L) = \{(1,1)\}$; in particular, the theorem holds.

Consider next $S = \{\varepsilon_i \mid k_i \text{ is even}\}$. Then for any $\varepsilon', \varepsilon'' \in S$, $(1, \varepsilon'\varepsilon'') \in \Sigma^{++}(L)$ (using a product of reflections in the appropriate generators). In particular, if S contains more than two classes mod 8, then $\Sigma^{++}(L) = \Gamma_{2,1}$, which is a contradiction. Since any one or two classes may be written as ε_+ and $(2\ell+1)\varepsilon_+$ for some ℓ mod 4, we may assume that there is an ℓ and an ε_+ with $\varepsilon_i \equiv \varepsilon_+$ or $(2\ell+1)\varepsilon_+$ mod 8 whenever k_i is even. Note that we have in this case that $(1, 2\ell+1) \in \Sigma^{++}(L)$.

Similarly, by considering the set $S' = \{\varepsilon_i \mid k_i \text{ is odd }\}$, we see that if $\Sigma^{++}(L) \neq \Gamma_{2,1}$, there is an ℓ' and an ε_- with $\varepsilon_i \equiv \varepsilon_-$ or $(2\ell'+1)\varepsilon_-$ mod 8 whenever k_i is odd. In this case we also have that $(1, 2\ell'+1) \in \Sigma^{++}(L)$.

If $\ell' \neq \ell$, and if neither one is 0, then $\Sigma^{++}(L) = \Gamma_{2,1}$; thus, either $\ell = \ell'$ or one of ℓ, ℓ' is 0. If one is 0 and the other is not, we may replace the 0 value by the other value and assume that $\ell = \ell'$ without loss of generality. (The $\ell = 0$ case is subsumed in any $\ell \neq 0$ case for (1).) Hence we have shown at this point that if $\Sigma^{++}(L) \neq \Gamma_{2,1}$, then an ℓ and $\varepsilon_+, \varepsilon_-$ exist satisfying (1) and with $(1, 2\ell+1) \in \Sigma^{++}(L)$.

Note that if $\ell \neq 0$ then there is still some freedom left in the choices of ε_+ and ε_-; they can be multiplied by $2\ell+1$, independently, and we still have (1). Moreover if S (respectively S') is empty, then we need not choose ε_+ (respectively ε_-) just yet.

Next, suppose there exist i, j with $i \neq j$ and $0 \leq m = |k_i - k_j| \leq 4$. If $m = 0$ (respectively 2, 4), then $(1,5) \in \Sigma^{++}(L)$ by Lemma 10.4.2 (respectively Lemma 10.4.3, Lemma 11.5.2). Thus, if $\ell \neq 0$ or 2, $\Sigma^{++}(L) = \Gamma_{2,1}$, since in this case $(1,5)$ and $(1, 2\ell+1)$ will generate $\Gamma_{2,1}$. Therefore if m is even we conclude ℓ is 0 or 2.

If $m = 1$ (resp. 3) then by Lemma 10.4.4 (respectively Lemma 11.5.1), we see that $(1, 1 + 2\varepsilon_i\varepsilon_j) \in \Sigma^{++}(L)$. If $\varepsilon_i\varepsilon_j \not\equiv \ell$ mod 4, and $\ell \neq 0$, then we would again have $\Sigma^{++}(L) = \Gamma_{2,1}$. Therefore if m is odd we conclude that either $\ell = 0$ or $\ell = \varepsilon_+\varepsilon_-$ mod 4.

We claim that it cannot happen that both m even and m odd occur (with different i, j pairs). If m even occurs, then we have seen above that $(1,5) \in \Sigma^{++}(L)$; if m odd occurs, then we have seen that $(1, 1 + 2\varepsilon_+\varepsilon_-) \in \Sigma^{++}(L)$. Since ε_+ and ε_- are both odd, $1+2\varepsilon_+\varepsilon_- \equiv 3$ mod 4; hence we would have $\Sigma^{++}(L) = \Gamma_{2,1}$, violating our assumption.

Now if m even is the case that occurs, we have that $\ell = 0$ or 2; if $\ell = 0$, we may change to $\ell = 2$ without spoiling the previous results.

If m odd is the case that occurs, then $\ell = 0$ or $\ell = \varepsilon_i\varepsilon_j$; again we may change if necessary and assume $\ell = \varepsilon_i\varepsilon_j$.

At this point we have ℓ, ε_+, and ε_- satisfying (1) and (2), and in addition $(1, 2\ell + 1) \in \Sigma^{++}(L)$.

Next note that the only reason so far to have needed an $\ell \neq 0$ is in case either the set S or the set S' has two classes, (so that there is a pair $i \neq j$ with $k_i = k_j \bmod 2$ and $\varepsilon_i = (2\ell + 1)\varepsilon_j$) or if there is a pair $i \neq j$ with $|k_i - k_j| \leq 4$. Therefore in addition to (1) and (2) we see that (4) is also satisfied.

Finally, suppose there is some i with $k_i = k_{i+1}$ and assume $\Sigma^{++}(L) \neq \Gamma_{2,1}$. As we saw above, $(1, 5) \in \Sigma^{++}(L)$ (this is an m even case) so that we must have $\ell = 2$, and $\Sigma^{++}(L) = \{(1, 1), (1, 5)\} = \Gamma_{2,2}$.

If there is some $j \neq i, i+1$ such that $|k_i - k_j| < 4$, then $|k_i - k_j| = 2$ since $\ell = 2$ and no 3 of the k's are equal. Since $\ell = 2$, (1) implies then that $\varepsilon_i \equiv \varepsilon_{i+1} \equiv \varepsilon_j \bmod 4$; but in this case, by Lemma 11.5.4 and 11.5.5, $\Sigma^{++}(L) = \Gamma_{2,1}$, a contradiction. Thus, $|k_i - k_j| \geq 4$ for all $j \neq i, i + 1$.

Let $L' = \bigoplus_{j\neq i} W_{2,k_j}^{\varepsilon_j}$.

Suppose that $\Sigma^{+}(L') = \Sigma^{++}(L'')$; this can only happen if all k_j's (for $j \neq i$) have the same parity (else the product of two reflections in generators of summands with opposite k parity will give an element in $\Sigma^{+}(L) - \Sigma^{++}(L)$). Since $k_i = k_{i+1}$, we see that all k_j (including k_i) have the same parity. If all the k's are even, then ε_- has not yet been determined; if all the k's are odd, then ε_+ has not yet been determined. In either case we may choose the undetermined one so that $1 + \varepsilon_i\varepsilon_{i+1} \equiv 2\varepsilon_+\varepsilon_- \bmod 8$.

Suppose that $\Sigma^{+}(L') \neq \Sigma^{++}(L')$. Since $\Sigma^{++}(L') \neq \Gamma_{2,1}$ (it is not for the larger lattice L), we see that $(1, 2\varepsilon_+\varepsilon_-) \in \Sigma^{+}(L')$ by the inductive hypothesis, and hence $(1, 2\varepsilon_+\varepsilon_-) \in \Sigma^{+}(L) - \Sigma^{++}(L)$ also. Now by Lemma 11.5.3, $(1, 1 + \varepsilon_i\varepsilon_{i+1}) \in \Sigma^{+}(L) - \Sigma^{++}(L)$. Thus, $(1, \frac{1}{2}\varepsilon_+\varepsilon_-(1 + \varepsilon_i\varepsilon_{i+1})) \in \Sigma^{++}(L)$. But since $\Sigma^{++}(L) = \{(1, 1), (1, 5)\}$, this implies $\frac{1}{2}\varepsilon_+\varepsilon_-(1 + \varepsilon_i\varepsilon_{i+1}) \equiv 1 \bmod 4$, or $1 + \varepsilon_i\varepsilon_{i+1} \equiv 2\varepsilon_+\varepsilon_- \bmod 8$.

This finishes the first part of the proof.

Conversely, suppose that L satisfies (1)–(4). We will proceed by induction on the rank of L, and write $L = W_{2,k_1}^{\varepsilon_1} \oplus L'$. Since the statement of the theorem is invariant under scaling by Proposition 8.1, we may assume that $\mathrm{scale}(L) = 0$, i.e., that $k_1 = 0$.

By Theorem 4.8, $\Sigma(L)$ is generated by $\Sigma(L')$ and by

$$\{(-1, Q(z)) \mid z \in L, 4 \nmid Q(z) \text{ and if } 2 \mid Q(z) \text{ then } 2 \mid \langle z, t\rangle \text{ for all } t \in L\}.$$

Thus, since the reflection with respect to the generator of the first summand gives the class $(-1, \varepsilon_1/2)$ in $\Sigma(L) - \Sigma^+(L)$, $\Sigma^+(L)$ is generated by $\Sigma^+(L')$ and by

$$\{(1, \varepsilon_1 Q(z)/2) \mid z \in L, 4 \nmid Q(z \text{ and if } 2 \mid Q(z) \text{ then } 2 \mid \langle z, t\rangle \text{ for all } t \in L\}.$$

Since we know that $(1, 2\ell{+}1) \in \Sigma^{++}(L)$, and that $\Sigma^{++}(L') = \{(1,1), (1, 2\ell+1)\}$ by the inductive hypothesis, and in addition that $\Sigma^+(L')$ is either equal to $\Sigma^{++}(L)$ or can be generated over $\Sigma^{++}(L')$ by $(1, 2\varepsilon_+\varepsilon_-)$, we must only show that these extra generators do not give any more elements, i.e., that whenever z satisfies the conditions above, we have that $\varepsilon_1 Q(z)/2 \equiv 1$ or $2\ell + 1$ or $2\varepsilon_+\varepsilon_-$ or $(2\ell + 1)2\varepsilon_+\varepsilon_-$ in $\mathbb{Q}_2^*/(\mathbb{Q}_2^*)^2$. This is equivalent to the following:

(i) if $Q(z) \in \frac{1}{2}\mathbb{U}_2$, then $2Q(z) \equiv \varepsilon_+$ or $(2\ell + 1)\varepsilon_+$ mod 8,

(ii) if $Q(z) \in \mathbb{U}_2$, then $Q(z) \equiv \varepsilon_-$ or $(2\ell + 1)\varepsilon_-$ mod 8, and

(iii) if $Q(z) \in 2\mathbb{U}_2$ and $\langle z, t\rangle \in 2\mathbb{Z}_2$ for all $t \in L$, then

$$\frac{1}{2}Q(z) \equiv \varepsilon_+ \text{ or } (2\ell + 1)\varepsilon_+ \text{ mod } 8.$$

(All these statements come from noting that since $k_1 = 0$ is even, $\varepsilon_1 \equiv \varepsilon_+$ or $(2\ell{+}1)\varepsilon_+$ mod 8; statements (i) and (iii) follow since in these cases we must have $\varepsilon_1 Q(z)/2 \equiv 1$ or $2\ell + 1$, and statement (ii) follows since in this case we must have $\varepsilon_1 Q(z)/2 \equiv 2\varepsilon_+\varepsilon_-$ or $(2\ell + 1)2\varepsilon_+\varepsilon_-$.)

First suppose that scale$(L') \geq 5$, and let x span $W_{2,0}^{\varepsilon_1}$ with $Q(x) = \varepsilon_1/2$. Write $z = ax + t$ with $t \in L'$. then $Q(z) = a^2\varepsilon_1/2 + Q(t) \equiv a^2\varepsilon_1/2$ mod 16. If $Q(z) \in \frac{1}{2}\mathbb{U}_2$, then $2Q(z) \equiv a^2\varepsilon_1 \equiv \varepsilon_+$ or $(2\ell + 1)\varepsilon_+$ mod 8. If $Q(z) \in \mathbb{Z}_2$ then $a = 2a_0$ and $2 \mid Q(z)$. If $Q(z) \in 2\mathbb{U}_2$, then $\frac{1}{2}Q(z) \equiv a_0^2\varepsilon_1$ mod $8 \equiv \varepsilon_1$ mod $8 \equiv \varepsilon_+$ or $(2\ell + 1)\varepsilon_+$ mod 8, proving the theorem in this case.

Now suppose that scale$(L') \leq 4$, and write $L' = W_{2,k_2}^{\varepsilon_2} \oplus L''$, with scale$(L'') = s + 1 \geq k_2$. Let x, y span $W_{2,0}^{\varepsilon_1}$, $W_{2,k_2}^{\varepsilon_2}$, respectively, with $Q(x) = \varepsilon_1/2$ and $Q(y) = 2^{k_2-1}\varepsilon_2$. Write $z = ax + by + t$ with $t \in L''$, so that $Q(z) \equiv a^2\varepsilon_1/2 + 2^{k_2-1}b^2\varepsilon_2$ mod 2^s. We consider several cases.

Case 1: $k_2 = 0$. Then by (3), $\ell = 2$ and we have $s \geq 3$. Hence we have $Q(z) \equiv a^2\varepsilon_1/2 + b^2\varepsilon_2/2$ mod 8. In this case, statement (i) is Lemma 10.5.1. For (ii), in order that $Q(z) \in \mathbb{U}_2$, we must have a and b both odd; then $Q(z) \equiv a^2\varepsilon_1/2 + b^2\varepsilon_2/2$ mod $8 \equiv (\varepsilon_1 + \varepsilon_2)/2$ mod 4 so that $Q(z) \equiv \varepsilon_-$ mod 4 using (3) since $\varepsilon_1 \equiv \varepsilon_2 \equiv \varepsilon_+$ mod 4. But this means $Q(z) \equiv \varepsilon_-$ or $5\varepsilon_-$ mod 8 as required since $\ell = 2$.

For (iii), since $Q(z) \in 2\mathbb{U}_2$ we must have $a = 2a_0$, $b = 2b_0$ so that $\frac{1}{2}Q(z) \equiv a_0^2\varepsilon_1 + b_0^2\varepsilon_2$ mod 4. Since $\frac{1}{2}Q(z) \in \mathbb{U}_2$, exactly one of a_0, b_0

is odd; thus $\frac{1}{2}Q(z) \equiv \varepsilon_1$ or $\varepsilon_2 \bmod 4$. Since these are both equal to $\varepsilon_+ \bmod 4$, we have that $\frac{1}{2}Q(z) \equiv \varepsilon_+$ or $5\varepsilon_+ \bmod 8$ as required since $\ell = 2$.

Case 2: $k_2 = 1$. Then by (2), ℓ is odd and we have $s \geq 5$. Hence we have $Q(z) \equiv a^2\varepsilon_1/2 + b^2\varepsilon_2 \bmod 32$. Here, (i) is Lemma 10.5.3. For (ii), $a = 2a_0$ and b is odd, so that $Q(z) \equiv 2a_0^2\varepsilon_1 + b^2\varepsilon_2 \bmod 32$; thus, $Q(z) \equiv \varepsilon_2$ or $\varepsilon_2 + 2\varepsilon_1 \bmod 8$. Since $\varepsilon_2(\varepsilon_2 + 2\varepsilon_1) \equiv 1 + 2\varepsilon_1\varepsilon_2 \equiv 2\ell + 1 \bmod 8$, and since $\varepsilon_2 \equiv \varepsilon_-$ or $(2\ell+1)\varepsilon_- \bmod 8$, $Q(z) \equiv \varepsilon_-$ or $(2\ell+1)\varepsilon_- \bmod 8$.

For (iii), we must have $a = 2a_0$ with a_0 odd and $b = 2b_0$. Then $\frac{1}{2}Q(z) \equiv a_0^2\varepsilon_1 + 2b_0^2\varepsilon_2 \bmod 16$ so that $\frac{1}{2}Q(z) \equiv \varepsilon_1$ or $\varepsilon_1 + 2\varepsilon_2 \bmod 8$. Again, $\varepsilon_1(\varepsilon_1+2\varepsilon_2) \equiv 1+2\varepsilon_1\varepsilon_2 \equiv 2\ell+1 \bmod 8$ by (3) so that $\frac{1}{2}Q(z) \equiv \varepsilon_+$ or $(2\ell + 1)\varepsilon_+ \bmod 8$.

Case 3: $k_2 = 2$. Then by (2), $\ell = 2$ and we have $s \geq 3$. Hence we have $Q(z) \equiv a^2\varepsilon_1/2 + 2b^2\varepsilon_2 \bmod 8$. Then (i) is Lemma 10.5.2, and (ii) does not occur. For (iii), we must have $a = 2a_0$. Then $\frac{1}{2}Q(z) \equiv a_0^2\varepsilon_1 + b^2\varepsilon_2 \bmod 4$. Exactly one of a_0 and b is even, so that $\frac{1}{2}Q(z) \equiv \varepsilon_1$ or $\varepsilon_2 \bmod 4$, which implies that $\frac{1}{2}Q(z) \equiv \varepsilon_+$ or $5\varepsilon_+ \bmod 8$.

Case 4: $k_2 = 3$. Then by (2), ℓ is odd and we have $s \geq 5$. Hence we have $Q(z) \equiv a^2\varepsilon_1/2 + 4b^2\varepsilon_2 \bmod 32$. Statement (i) is Lemma 10.5.4, and again (ii) does not occur. For (iii), we must have $a = 2a_0$ with a_0 odd. Then $\frac{1}{2}Q(z) \equiv a_0^2\varepsilon_1 + 2b^2\varepsilon_2 \bmod 16$ so that $\frac{1}{2}Q(z) \equiv \varepsilon_1$ or $\varepsilon_1 + 2\varepsilon_2 \bmod 8$. Since $\varepsilon_1(\varepsilon_1 + 2\varepsilon_1) \equiv 2\ell + 1 \bmod 8$, we see that $\frac{1}{2}Q(z) \equiv \varepsilon_+$ or $(2\ell + 1)\varepsilon_+ \bmod 8$.

Case 5: $k_2 = 4$. Then by (2), $\ell = 2$ and we have $s \geq 3$. Hence we have $Q(z) \equiv a^2\varepsilon_1/2 \bmod 8$. Then again (i) is Lemma 10.5.4, and (ii) does not occur. For (iii), we must have $a = 2a_0$ with a_0 odd. Then $\frac{1}{2}Q(z) \equiv a_0^2\varepsilon_1 \equiv \varepsilon_1 \bmod 4$ so that $\frac{1}{2}Q(z) \equiv \varepsilon_+$ or $5\varepsilon_+ \bmod 8$.

This completes the proof of the theorem. Q.E.D.

12. $\Sigma(L)$, $\Sigma^{\#}(L)$ and $\Sigma_0^{\#}(L)$ in Terms of the Discriminant-Form

In this section, we will express our computations of $\Sigma(L)$ and $\Sigma^{\#}(L)$ for quadratic $\mathbb{Z}_p$-modules (i.e., for *even* inner product $\mathbb{Z}_p$-modules) in terms of the rank, discriminant and discriminant-form group alone. (We will also compute a subgroup $\Sigma_0^{\#}(L)$ of $\Sigma^{\#}(L)$, defined below.) We assume as given an integer $\mathrm{rk}(L)$, a "discriminant" $\mathrm{disc}(L) \in \mathbb{Z}_p - \{0\}/\mathbb{U}_p^2$ and a finite p-primary torsion quadratic form $(G, q) \in \mathcal{T}_p$.

Let us first recall the conditions for the existence of a quadratic $\mathbb{Z}_p$-module with this rank, discriminant, and discriminant-form. To

fix notation, we may write the element $\mathrm{disc}(L)$ as $\mathrm{disc}(L) = p^k u$ for some $u \in \mathbb{U}_p \mod \mathbb{U}_p^2$. The length of the discriminant-form (G, q), which is the minimum number of generators of G, is denoted by $\ell(q)$. If p is odd, and if G has order p^k and first invariant p^{e_1}, then the discriminant $\mathrm{disc}(q)$ takes values in $p^{-k}(\mathbb{Z}/p^{e_1})^\times/((\mathbb{Z}/p^{e_1})^\times)^2$; it may be written as $p^{-k}v$, where v comes from the above group of order two, and $\chi(v) = \pm 1$. If $p = 2$ and if G has order 2^k and first invariant 2^{e_1}, then the discriminant $\mathrm{disc}(q)$ takes values in $2^{-k}(\mathbb{Z}/p^{e_1+1})^\times/((\mathbb{Z}/p^{e_1+1})^\times)^2$; it may be written as $2^{-k}v$, where v is odd and is well-defined modulo 4; it is well-defined modulo 8 if $e_1 \geq 2$. Finally, if $p = 2$ and q has no summand of the form $w_{2,1}^{\varepsilon}$ (i.e., q is good and special), then the mod 8 discriminant $\mathrm{disc}_8(q)$ is well-defined.

Now we assume that the three quantities $\mathrm{rank}(L)$, $\mathrm{disc}(L)$, and (G, q) satisfy the following conditions

(1) $\mathrm{rk}(L) \geq \ell(q)$, and if $p = 2$ then $\mathrm{rk}(L) \equiv \ell(q) \bmod 2$;

(2) if $\mathrm{disc}(L) = p^k u \mod \mathbb{U}_p^2$ with $u \in \mathbb{U}_p$, then $|G| = p^k$;

(3) if $p > 2$ and $r = \ell(q)$ then $\chi(\mathrm{disc}(L)) = \chi(\mathrm{disc}(q))$.

(4) if $p = 2$ and $r = \ell(q)+2n$ then $\chi(\mathrm{disc}(L)) \equiv (-1)^n \chi(\mathrm{disc}(q)) \bmod 4$.

(5) if $p = 2$ and $r = \ell(q)$ and if G has no summand of the form $w_{2,1}^{\varepsilon}$ (i.e., G is good and special), then $\chi(\mathrm{disc}(L)) = \mathrm{disc}_8(q)$.

These conditions guarantee the existence of a unique quadratic $\mathbb{Z}_p$-module L with rank $\mathrm{rk}(L)$, discriminant $\mathrm{disc}(L)$ and discriminant-form (G, q), by Propositions IV.2.12 and IV.5.7. In this section it is $\Sigma^{\#}(L)$ and $\Sigma(L)$ which we will compute; however, our conditions will not involve L itself in any way, simply these three invariants.

For each odd p, we fix once and for all a non-square $u_p \in \mathbb{U}_p$. Then the groups we are computing are subgroups of $\{\pm 1\} \times \mathbb{Q}_p^\times/(\mathbb{Q}_p^\times)^2$, which we denote by Γ_p. We will also have occasion to consider

$$\Gamma_p^+ = \{(d, s) \in \Gamma_p \mid d = 1\}$$
$$\Gamma_p^{++} = \{(d, s) \in \Gamma_p \mid d = 1, s \in \mathbb{U}_p \bmod (\mathbb{Q}_p^*)^2\}$$

and the $\Gamma_{p,k}$'s which we defined in Section 4. For p odd, Γ_p^{++} is generated by $(1, u_p)$, Γ_p^+ by $(1, u_p)$ and $(1, p)$ and Γ_p by $(1, u_p)$, $(1, p)$ and $(-1, 1)$. Similar statements hold for $p = 2$ if we allow u_p to range over $(\mathbb{Z}/8\mathbb{Z})^\times$. Note that $\Gamma_2^{++} = \Gamma_{2,1}$. Also note that for any p, $\Gamma_{p,0} = \{\pm 1\} \times \mathbb{U}_p/\mathbb{U}_p^2$.

We will compute the groups $\Sigma^{\#}(L)$ and $\Sigma(L)$, which are both a priori subgroups of Γ_p. (In fact, $\Sigma^{\#}(L) \subset \Gamma_{p,0}$ always.) For this purpose, it is convenient to consider the auxiliary groups

$$\Sigma^{+}(L) = \Sigma(L) \cap \Gamma_p^{+}$$
$$\text{and} \quad \Sigma^{++}(L) = \Sigma(L) \cap \Gamma_p^{++}$$

which were defined in Section 8. We will also compute a new group $\Sigma_0^{\#}(L)$, defined as follows. Let

$$\Gamma_0 = \{(1,1),(1,-1),(-1,1),(-1,-1)\} \in \{\pm 1\} \times \mathbb{Q}^{\times}/(\mathbb{Q}^{\times})^2.$$

The natural map $\mathbb{Q}^{\times}/(\mathbb{Q}^{\times})^2 \to \mathbb{Q}_p^{\times}/(\mathbb{Q}_p^{\times})^2$ induces a map

$$\varphi_p \colon \Gamma_0 \to \Gamma_{p,0}$$

which to be completely explicit has the following values:

p	$\varphi_p(1,1)$	$\varphi_p(1,-1)$	$\varphi_p(-1,1)$	$\varphi_p(-1,-1)$
2	$(1,1)$	$(1,7)$	$(-1,1)$	$(-1,7)$
1 mod 4	$(1,1)$	$(1,1)$	$(-1,1)$	$(-1,1)$
3 mod 4	$(1,1)$	$(1,u_p)$	$(-1,1)$	$(-1,u_p)$

We define

$$\Sigma_0^{\#}(L) = \varphi_p^{-1}(\Sigma^{\#}(L)) = \big\{(d,s) \in \Gamma_0 \mid \varphi_p(d,s) \in \Sigma^{\#}(L)\big\}$$

The usefulness of knowing $\Sigma_0^{\#}(L)$ will become apparent in the next chapter; for now, we simply remark that it is completely a function of $\Sigma^{\#}(L)$ (and p), and we are merely recording its values below for later reference.

In the statements which follow, we assume that q is in partial normal form (whenever $p = 2$). We begin with the computations of $\Sigma^{\#}(L)$ and $\Sigma_0^{\#}(L)$.

THEOREM 12.1. *Let $p \neq 2$.*

(12.1.1) If $\mathrm{rk}(L) = \ell(q)$ then $\Sigma^{\#}(L) = \{(1,1)\}$ and

$$\Sigma_0^{\#}(L) = \begin{cases} \{(1,1)\} & \text{if } p \equiv 3 \bmod 4 \\ \{(1,1),(1,-1)\} & \text{if } p \equiv 1 \bmod 4 \end{cases}$$

(12.1.2) If $\mathrm{rk}(L) = \ell(q) + 1$, let $\delta = \mathrm{disc}(L)\,\mathrm{disc}(q) \in \mathbb{U}_p/\mathbb{U}_p^2$. Then

$$\Sigma^{\#}(L) = \{(1,1),(-1,2\delta)\}$$

and

$$\Sigma_0^{\#}(L) = \begin{cases} \Gamma_0 & \text{if } p \equiv 1 \bmod 8 \text{ and } \chi(\delta) = 1 \\ & \underline{\text{or}}\ p \equiv 5 \bmod 8 \text{ and } \chi(\delta) = -1 \\ \{(1,1),(-1,-1)\} & \text{if } p \equiv 3 \bmod 8 \text{ and } \chi(\delta) = 1 \\ & \underline{\text{or}}\ p \equiv 7 \bmod 8 \text{ and } \chi(\delta) = -1 \\ \{(1,1),(1,-1)\} & \text{if } p \equiv 5 \bmod 8 \text{ and } \chi(\delta) = 1 \\ & \underline{\text{or}}\ p \equiv 1 \bmod 8 \text{ and } \chi(\delta) = -1 \\ \{(1,1),(-1,1)\} & \text{if } p \equiv 7 \bmod 8 \text{ and } \chi(\delta) = 1 \\ & \underline{\text{or}}\ p \equiv 3 \bmod 8 \text{ and } \chi(\delta) = -1 \end{cases}$$

(12.1.3) If $\mathrm{rk}(L) \geq \ell(q) + 2$ *then* $\Sigma^{\#}(L) = \Gamma_{p,0}$ *and* $\Sigma_0^{\#}(L) = \Gamma_0$.

PROOF. Statement (12.1.1) is Theorem 9.3.1, which applies since if $\mathrm{rk}(L) = \ell(q)$ then $\mathrm{scale}(L) \geq 1$. The other two statements (12.1.2,3) follow exactly from Theorem 9.3.2,3.

The reader is advised that the well-known facts $\chi(-1) = \left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}}$ and $\chi(2) = \left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}$ when p is odd (cf. Serre (1970), Chap. I, §3) are invaluable in verifying the results above. Q.E.D.

THEOREM 12.2. *Let* $p = 2$*, and write* q *in partial normal form as*

$$q = u_1^{N(1)} \oplus v_1^{e(1)} \oplus w(1) \oplus u_2^{N(2)} \oplus v_2^{e(2)} \oplus w(2) \oplus q'$$

with $\mathrm{scale}(q') \geq 3$*. Then* $\Sigma^{\#}(L)$ *and* $\Sigma_0^{\#}(L)$ *are given by the following table, and by Theorems 12.3 and 12.4 below.*

$\mathrm{rk}(L) - \ell(q)$	$N(1) + e(1)$	$\ell(w(1))$	$N(2) + e(2)$	$\ell(w(2))$	$\Sigma^{\#}(L)$	$\Sigma_0^{\#}(L)$
> 0					$\Gamma_{2,0}$	Γ_0
0	> 0	> 0			$\Gamma_{2,0}$	Γ_0
0	> 0	0			$\Gamma_{2,1}$	$\{(1,\pm 1)\}$
0	0	2			*see Thm. 12.3*	
0	0	1			*see Thm. 12.4*	
0	0	0	> 0		$\Gamma_{2,2}$	$\{(1,1)\}$
0	0	0	0	2	$\Gamma_{2,2}$	$\{(1,1)\}$
0	0	0	0	≤ 1	$\{(1,1)\}$	$\{(1,1)\}$

PROOF. This is the content of Theorem 10.2. Q.E.D.

THEOREM 12.3. *Suppose that* $p = 2$, $\mathrm{rk}(L) = \ell(q)$ *and*

$$q = w_{2,1}^{\varepsilon} \oplus w_{2,1}^{\varphi} \oplus u_2^{N(2)} \oplus v_2^{e(2)} \oplus w_{(2)} \oplus q'$$

with scale$(q') \geq 3$. Then $\Sigma^{\#}(L)$ and $\Sigma_0^{\#}(L)$ are given by the following table:

$\varepsilon\varphi \bmod 4$	$\ell(w(2))$	$\Sigma^{\#}(L)$	$\varepsilon \bmod 4$	$\Sigma_0^{\#}(L)$
3		$\Gamma_{2,0}$		Γ_0
1	> 0	$\Gamma_{2,0}$		Γ_0
1	0	$\left\{ \begin{array}{l} (1,1),(1,5) \\ (-1,\varepsilon),(-1,5\varepsilon) \end{array} \right\}$	1	$\{(1,1),(-1,1)\}$
			3	$\{(1,1),(-1,-1)\}$

Proof. Theorem 10.8 computes $\Sigma^{\#,+}(L)$ in these cases; then we use Lemma 10.6 to compute $\Sigma^{\#}(L)$. Q.E.D.

Theorem 12.4. *Suppose that $p = 2$, $\mathrm{rk}(L) = \ell(q)$ and $q = w_{2,1}^{\varepsilon} \oplus q'$ with*

$$q' = u_2^{N(2)} \oplus v_2^{e(2)} \oplus w(2) \oplus u_3^{N(3)} \oplus v_3^{e(3)} \oplus w(3) \oplus q''$$

with scale$(q'') \geq 4$. Let $\delta = \chi(\mathrm{disc}(L))/\operatorname{disc}_8(q')$, which is well-defined (given this partial normal form) since $q' \in \mathcal{G}_2$. Then $\Sigma^{\#}(L)$ and $\Sigma_0^{\#}(L)$ are given by the following table:

$N(2)+e(2)$ $+\ell(w(3))$	$w(2)$	$\Sigma^{\#}(L)$	$\delta \bmod 8$	$\Sigma_0^{\#}(L)$
> 0	$\neq 0$	$\Gamma_{2,0}$		Γ_0
> 0	0	$\left\{ \begin{array}{l} (1,1),(1,5) \\ (-1,\delta),(-1,5\delta) \end{array} \right\}$	$1,5$	$\{(1,1),(-1,1)\}$
			$3,7$	$\{(1,1),(-1,-1)\}$
0	rank 2	$\Gamma_{2,0}$		Γ_0
0	$w_{2,2}^{\varphi}$, $\varepsilon\varphi \equiv 3 \bmod 4$	$\left\{ \begin{array}{l} (1,1),(1,7) \\ (-1,\delta),(-1,7\delta) \end{array} \right\}$	$1,7$	Γ_0
			$3,5$	$\{(1,1),(1,-1)\}$
0	$w_{2,2}^{\varphi}$ $\varepsilon\varphi \equiv 1 \bmod 4$	$\left\{ \begin{array}{l} (1,1),(1,3) \\ (-1,\delta),(-1,3\delta) \end{array} \right\}$	$1,3$	$\{(1,1),(-1,1)\}$
			$5,7$	$\{(1,1),(-1,-1)\}$
0	0	$\{(1,1),(-1,\delta)\}$	1	$\{(1,1),(-1,1)\}$
			7	$\{(1,1),(-1,-1)\}$
			$3,5$	$\{(1,1)\}$

Proof. Let us remark that the definition of δ implies that L may be written as $L = W_{2,1}^{\delta} \oplus L'$, with $q_{L'} = q'$. Then Theorem 10.7

computes $\Sigma^{\#,+}(L)$ in these cases, and we use Lemma 10.6 to compute $\Sigma^{\#}(L)$.

Note that since the partial normal form is not unique, the form q' and hence also the value of δ are not determined solely by q and $\mathrm{disc}(L)$, but by the partial normal form. However it is an exercise to check that the answers in the table above do not depend on the specific partial normal form decomposition. Q.E.D.

We next turn to the computation of $\Sigma(L)$. We will compute this in three stages: first, we compute $\Sigma^{++}(L)$ and a group whose order is twice that of $\Sigma^{++}(L)$ which contains $\Sigma^{+}(L)$ (so that $\Sigma^{+}(L)$ is that group if and only if $\Sigma^{+}(L) \neq \Sigma^{++}(L)$). Second, we give conditions which decide whether $\Sigma^{+}(L) = \Sigma^{++}(L)$ or $\Sigma^{+}(L) \neq \Sigma^{++}(L)$. Third, we describe a generator for the group $\Sigma(L)/\Sigma^{+}(L)$ of order 2.

THEOREM 12.5. *Let $p \neq 2$. We have, of course, $\Sigma^{++}(L) \subseteq \Gamma_p^{++}$ and $\Sigma + (L) \subseteq \Gamma_p^{+}$.*

Then $\Sigma^{++}(L) \neq \Gamma_p^{++}$ if and only if there exist $\varepsilon_+, \varepsilon_- \in \{\pm 1\}$ such that if we write $q = w_{p,k_1}^{\varepsilon_1} \oplus \cdots \oplus w_{p,k_r}^{\varepsilon_r}$ then

(1) *$k_1 < k_2 < \cdots < k_r$ and $\mathrm{rk}(L) - \ell(q) \leq 1$,*

(2) *$\varepsilon_i = \varepsilon_+$ if k_i is even and $\varepsilon_i = \varepsilon_-$ if k_i is odd; moreover if $\mathrm{rk}(L) = \ell(q) + 1$ and we let $\delta = \chi(\mathrm{disc}(L))/\chi(\mathrm{disc}(q))$ then $\left(\frac{\delta}{p}\right) = \varepsilon_+$.*

In this latter case, $\Sigma^{++}(L) = \{(1,1)\}$ and $\Sigma^{+}(L) \subset \{(1,1),(1,p\alpha)\}$ where α satisfies $\left(\frac{\alpha}{p}\right) = \varepsilon_+\varepsilon_-$.

PROOF. The condition that $\mathrm{rk}(L) \leq \ell(q) + 1$ implies that L may be written as

$$L = W(0) \oplus W_{p,k_1}^{\varepsilon_1} \oplus \cdots \oplus W_{p,k_r}^{\varepsilon_r}$$

where $W(0)$ has rank at most one; if it has rank one the $W(0) = W_{p,0}^{\delta}$. In this form we see that the hypotheses of Theorem 9.6 hold and this theorem gives the results stated above. Q.E.D.

THEOREM 12.6. *Let $p = 2$. Again, $\Sigma^{++}(L) \subseteq \Gamma_2^{++}$ and $\Sigma^{+}(L) \subseteq \Gamma_2^{+}$. Then $\Sigma^{++}(L) \neq \Gamma_2^{++}$ if and only if $\mathrm{rk}(L) = \ell(q)$, q has the form*

$$q = w_{2,k_1}^{\varepsilon_1} \oplus \cdots \oplus w_{2,k_r}^{\varepsilon_r}$$

with $k_1 \leq \cdots \leq k_r$ and $k_i < k_{i+2}$ for each i, and there exist $n \in \mathbb{Z}/4\mathbb{Z}$ and $\varepsilon_+, \varepsilon_- \in (\mathbb{Z}/8\mathbb{Z})^{\times}$ with the following properties:

(1) $\varepsilon_i \equiv \varepsilon_+$ *or* $(2n+1)\varepsilon_+ \bmod 8$ *if* k_i *is even,* $\varepsilon_i \equiv \varepsilon_-$ *or* $(2n+1)\varepsilon_- \bmod 8$ *if* $k_i \geq 3$ *is odd, and if* $1 = k_1 < k_2$ *then*

$$\delta_1 = \frac{\chi(\mathrm{disc}(L))}{\prod_{j>1} \varepsilon_j} \equiv \varepsilon_- \quad or \quad (2n+1)\varepsilon_- \bmod 8.$$

(2) *Suppose there exist* $i \neq j$ *such that* $|k_i - k_j| \leq 4$. *Then* $n \neq 0$ *and* $|k_i - k_j| \equiv n \bmod 2$. *If in addition* n *is odd, then* $\varepsilon_i\varepsilon_j \equiv n \bmod 4$.

(3) *If there exists an* i *with* $k_i = k_{i+1} \geq 2$, *then* $n = 2$, $|k_i - k_j| \geq 4$ *for all* $j \neq i, i+1$ *and* $1+\varepsilon_i\varepsilon_{i+1} \equiv 2\varepsilon_+\varepsilon_- \bmod 8$. *If* $k_1 = k_2 = 1$, *then* $n = 2$, $|k_j - k_1| \geq 4$ *for all* $j \geq 3$, $\varepsilon_1 \equiv \varepsilon_2 \bmod 4$ *and*

$$1 + \frac{\chi(\mathrm{disc}(L))}{\prod_{j>2} \varepsilon_j} \equiv 2\varepsilon_+\varepsilon_- \bmod 8.$$

(4) *If* $n \neq 0$, *either there exist* i, j *with* $i \neq j$ *and* $|k_i - k_j| \leq 4$, *or there exist* i *and* j *with* $k_i, k_j \geq 2$, $k_i \equiv k_j \bmod 2$ *and* $\varepsilon_i \equiv (2n+1)\varepsilon_j \bmod 8$, *or* $1 = k_1 < k_2$ *and there exists* $i > 1$ *with* $k_i \equiv 1 \bmod 2$ *and*

$$\frac{\chi(\mathrm{disc}(L))}{\prod_{j>1} \varepsilon_j} \equiv (2n+1) \bmod 8.$$

In this latter case, $\Sigma^{++}(L) = \{(1,1),(1,2n+1)\}$ *(which has order* 1 *if* $n = 0$*) and* $\Sigma^{+}(L) \subset \{(1,1),(1,2n+1),(1,2\varepsilon_+\varepsilon_-),(1,2\varepsilon_+\varepsilon_-(2n+1))\}$.

Proof. This is a re-statement of Theorems 11.4 and 11.6. The only variation in the statements occurs in case L has scale 1; then $L = W_{2,1}^{\delta_1} \oplus L'$ and $q = w_{2,1}^{\varepsilon_1} \oplus q'$ and since ε_1 is only defined modulo 4 we must resort to describing δ_1 in terms of the discriminant as in (1) and (4). In (3), we use the discriminant to write the product $\delta_1\delta_2$ where in this case $L = W_{2,1}^{\delta_1} \oplus W_{2,1}^{\delta_2} \oplus L''$.

In verifying the hypotheses the relation (I) of Proposition IV.3.1 is needed at a couple of stages. Q.E.D.

At this point we have computed $\Sigma^{++}(L)$ in all cases. We now turn to computing $\Sigma^{+}(L)$. As noted above, we have in every case given a group which contains $\Sigma^{+}(L)$ and has order at most twice that of $\Sigma^{++}(L)$. Therefore $\Sigma^{+}(L)$ is determined if we know whether $\Sigma^{+}(L) = \Sigma^{++}(L)$ or not, and it is this to which we now turn.

THEOREM 12.7. *Let $p \neq 2$. Then $\Sigma^+(L) = \Sigma^{++}(L)$ if and only if, writing*

$$q = w_{p,k_1}^{\varepsilon_1} \oplus \cdots \oplus w_{p,k_r}^{\varepsilon_r},$$

(1) *$k_i \equiv k_j \bmod 2$ for each i, j*

(2) *if $\operatorname{rk}(L) \neq \ell(q)$ then $k_i \equiv 0 \bmod 2$ for all i.*

PROOF. This is Theorem 9.5. Q.E.D.

THEOREM 12.8. *Let $p = 2$. Then $\Sigma^+(L) = \Sigma^{++}(L)$ if and only if there exists an $n \in \mathbb{Z}/2\mathbb{Z}$ such that, writing q in partial normal form*

$$q = \cdots \oplus u_k^{N(k)} \oplus v_k^{e(k)} \oplus w(k) \oplus \cdots$$

we have

(1) *$k \equiv n \bmod 2 \Rightarrow w(k) = 0$*

(2) *$k \not\equiv n \bmod 2 \Rightarrow N(k) = e(k) = 0$. If in addition $\ell(w(k)) = 2$, then $w(k) = w_{2,k}^{\varepsilon} \oplus w_{2,k}^{\varphi}$ with $\varepsilon + \varphi \equiv 0 \bmod 4$.*

(3) *if $\operatorname{rk}(L) \neq \ell(q)$ then $n \equiv 0 \bmod 2$.*

PROOF. This follows from Theorem 11.4. Q.E.D.

At this point we have determined both $\Sigma^+(L)$ and $\Sigma^{++}(L)$ from the rank, discriminant, and discriminant-form data. To finish the description of $\Sigma(L)$, we note that $[\Sigma(L) : \Sigma^+(L)] = 2$ by Lemma 8.2; hence if we give an element in $\Sigma(L) - \Sigma^+(L)$, this element will generate $\Sigma(L)/\Sigma^+(L)$, and we will be done.

THEOREM 12.9. *Let $p \neq 2$.*

(12.9.1) If $\ell(q) = 0$ then $\Sigma(L)/\Sigma^+(L)$ is generated by $(-1, 2\operatorname{disc}(L))$.

(12.9.2) If $\ell(q) \neq 0$ and $q = w_{p,2k}^{\varepsilon} \oplus q'$ then $\Sigma(L)/\Sigma^+(L)$ is generated by $(-1, 2\alpha)$, where $\left(\frac{\alpha}{p}\right) = \varepsilon$.

(12.9.3) If $\ell(q) \neq 0$ and $q = w_{p,2k+1}^{\varepsilon} \oplus q'$ then $\Sigma(L)/\Sigma^+(L)$ is generated by $(-1, 2\alpha p)$, where $\left(\frac{\alpha}{p}\right) = \varepsilon$.

PROOF. To see (12.9.1), we note that in this case L is unimodular, of the form

$$L = \bigoplus_i W_{p,0}^{\varepsilon_i}.$$

In this case by Theorem 9.6 $\Sigma^{++}(L) = \Gamma_p^{++}$ unless $\operatorname{rk}(L) = 1$, in which case $\Sigma^{++}(L) = \{(1,1)\}$. Moreover by Theorem 12.7 we have

$\Sigma^+(L) = \Sigma^{++}(L)$. Therefore $\Sigma(L)$ is generated over $\Sigma^+(L)$ by the determinant and spinor norm of any reflection, and in this case there are such giving a class of the form $(-1, u)$ for some unit u. If $\Sigma^+(L) = \Gamma_p^{++}$, then any unit u will generate the same group, namely $\{\pm 1\} \times \mathbb{U}_p/\mathbb{U}_p^2$; we might as well take $u = 2\,\mathrm{disc}(L)$. If $\mathrm{rk}(L) = 1$, then $L = W_{p,0}^{\varepsilon}$, and letting x be a generator of L with $Q(x) = \alpha/2$, where $\chi(\alpha) = \varepsilon$, so that $\tau_x = -\text{identity}$ is defined, we see that $(\det(\tau_x), \mathrm{spin}(\tau_x)) = (-1, \alpha/2) \equiv (-1, 2\alpha)$; Since in this case $\mathrm{disc}(L) = \alpha$, the result follows.

The last two statement follow in the same way, by considering the reflection τ_x through a generator of the corresponding summand of L. Q.E.D.

THEOREM 12.10. *Let $p = 2$.*

(12.10.1) If $\mathrm{rk}(L) \neq \ell(q)$, or $q = u_{2k} \oplus q'$ or $v_{2k} \oplus q'$ then $\Sigma(L)/\Sigma^+(L)$ is generated by $(-1, 1)$.

(12.10.2) If $q = u_{2k+1} \oplus q'$ or $v_{2k+1} \oplus q'$ then $\Sigma(L)/\Sigma^+(L)$ is generated by $(-1, 2)$.

(12.10.3) If $q = w_{2,2k}^{\varepsilon} \oplus q'$, then $\Sigma(L)/\Sigma^+(L)$ is generated by $(-1, 2\varepsilon)$.

(12.10.4) If $q = w_{2,2k+1}^{\varepsilon} \oplus q'$ with $2k + 1 > 1$, then $\Sigma(L)/\Sigma^+(L)$ is generated by $(-1, \varepsilon)$.

(12.10.5) If $\mathrm{rk}(L) = \ell(q)$ and $q = w_{2,1}^{\varepsilon} \oplus w_{2,1}^{\varphi} \oplus q'$, then $\Sigma(L)/\Sigma^+(L)$ is generated by $(-1, \delta)$ where δ is either of the elements of $\mathbb{U}_2/\mathbb{U}_2^2$ such that $\delta \equiv \varepsilon \bmod 4$.

(12.10.6) If $\mathrm{rk}(L) = \ell(q)$ and $q = w_{2,1}^{\varepsilon} \oplus q'$, with $q' \in \mathcal{G}_2$, then $\Sigma(L)/\Sigma^+(L)$ is generated by $(-1, \delta)$, where $\delta = \chi(\mathrm{disc}(L))/\,\mathrm{disc}_8(q')$.

PROOF. Again this is just a matter of identifying spinor norms of appropriate reflections; we simply need to identify $Q(x)$ for an appropriate reflecting element x, and then $(-1, Q(x))$ will generate $\Sigma(L)/\Sigma^+(L)$.

For (12.10.1), we have either a summand U_{2k} or V_{2k} of L. In either case there is a reflecting element x such that $Q(x) = 2^{2k}$. Then $(-1, 2^{2k}) \equiv (-1, 1)$ in the group $\Sigma(L)$.

For (12.10.2), we have either a summand U_{2k+1} or V_{2k+1} of L, and again there is a reflecting element x such that $Q(x) = 2^{2k+1}$. Then $(-1, 2^{2k+1}) \equiv (-1, 2)$ in the group $\Sigma(L)$.

For (12.10.3), we have a summand $W^{\varepsilon}_{2,2k}$ of L, and again there is a reflecting element x such that $Q(x) = 2^{2k-1}\varepsilon$. Then $(-1, 2^{2k-1}\varepsilon) \equiv (-1, 2\varepsilon)$ in the group $\Sigma(L)$.

Similarly, for (12.10.4), we have that ε is defined modulo 8 (since $2k+1 \geq 3$) so there is a summand $W^{\varepsilon}_{2,2k+1}$ of L, and there is a reflecting element x such that $Q(x) = 2^{2k}\varepsilon$. Then $(-1, 2^{2k}\varepsilon) \equiv (-1, \varepsilon)$ in the group $\Sigma(L)$.

To see (12.10.5), note that $W^{\delta}_{2,1}$ is a summand of L, for some $\delta \equiv \varepsilon \bmod 4$. Letting x be a generator of this summand with $Q(x) = \delta$, we see that $(-1, \delta) \in \Sigma(L)$. However by Theorem 12.6, we also have that the element $(1, 5) \in \Sigma^{++}(L)$. Therefore $(-1, 5\delta)$ is also in $\Sigma(L)$, which gives the result.

Finally the definition of δ given in (12.10.6) ensures that $W^{\delta}_{2,1}$ is a summand of L; considering the reflection through a generator x with $Q(x) = \delta$ now finishes the proof. Q.E.D.

Corollary 12.11. *Let L be an quadratic $\mathbb{Z}_p$-module.*

(12.11.1) If $\mathrm{rk}(L) \geq \ell(q_L) + 2$, *then* $\Sigma^{\#}(L) = \Gamma_{p,0}$.

(12.11.2) If $\mathrm{rk}(L) \geq 2$ *and L is unimodular, then* $\Sigma^{\#}(L) = \Sigma(L) = \Gamma_{p,0}$.

Proof. Statement (12.11.1) follows from Theorem 12.1.3 if $p \neq 2$, and the first line of the table in Theorem 12.2 if $p = 2$.

The statement in (12.11.2) about $\Sigma^{\#}(L)$ follows from (12.11.1). Since $\mathrm{rk}(L) \geq 2$ and $\ell(q) = 0$, we get $\Sigma^{++}(L) = \Gamma_p^{++}$ by Theorem 12.5 if $p \neq 2$ and by Theorem 12.6 if $p = 2$. Moreover, $\Sigma^{+}(L) = \Sigma^{++}(L)$ by Theorem 12.7 if $p \neq 2$ and Theorem 12.8 if $p = 2$. Since Γ_p^{++} has index 2 in $\Gamma_{p,0}$, we only need to show that the generator of $\Sigma(L)/\Sigma^{+}(L)$ lies in $\Gamma_{p,0}$, i.e., is of the form $(-1, u)$ for some unit u. If $p \neq 2$, by Theorem 12.9.1 this generator is $(-1, 2\,\mathrm{disc}(L))$ which is in $\Gamma_{p,0}$ since $2\,\mathrm{disc}(L)$ is a unit. If $p = 2$, by Theorem 12.10.1, this generator is $(-1, 1) \in \Gamma_{2,0}$. Q.E.D.

Bibliographical note for Chapter VII

The spinor norm and the Eichler isometries were first introduced in Eichler (1952). The analogue of the Cartan-Dieudonné Theorem for $\mathcal{O}(L)$ (our 7.7) is fairly standard when p is odd (cf. O'Meara (1963) 92:4, for example) and is due to O'Meara and Pollak (1965) when $p = 2$. The corresponding theorem for $\mathcal{O}^{\#}(L)$ (7.5) is new. The calculations is Sections 4, 5, and 6 were directly inspired by O'Meara and Pollak's proof.

The computation of $\Sigma(L)$ is due to Kneser (1956) when p is odd, and Earnest and Hsia (1975) when $p = 2$ (in slightly different form). The computations of $\Sigma^{\#}(L)$ and $\Sigma_0^{\#}(L)$ are new.

CHAPTER VIII

Uniqueness of Integral Quadratic Forms

1. Discriminant Forms and Rational Quadratic Forms

If L is an integral quadratic form, we let G_L denote the discriminant quadratic form of L and $\text{sign}(L) = (s_+, s_-)$ denote the signature of $L \otimes \mathbb{R}$.

THEOREM 1.1. *Let L and Λ be integral quadratic forms. Suppose that $G_L \simeq G_\Lambda$ and $\text{sign}(L) = \text{sign}(\Lambda)$. Then there is an isometry $\sigma : L \otimes \mathbb{Q} \to \Lambda \otimes \mathbb{Q}$ of quadratic form spaces over $\mathbb{Q}$.*

PROOF. First note that since $\text{sign}(L) = \text{sign}(\Lambda)$, by Corollary I.7.13 there is an isometry $\sigma_\infty : L \otimes \mathbb{Q}_\infty \to \Lambda \otimes \mathbb{Q}_\infty$, where $\mathbb{Q}_\infty$ denotes $\mathbb{R}$.

Now recall that for an integral quadratic form L, $\text{disc}(L) = (-1)^{s_-}|G_L|$. Thus, $\text{disc}(L \otimes \mathbb{Z}_p) = \text{disc}(\Lambda \otimes \mathbb{Z}_p)$ for all $p < \infty$. Moreover, $G_{L \otimes \mathbb{Z}_p} \simeq G_{\Lambda \otimes \mathbb{Z}_p}$ since each is the p-part of the corresponding group. By Theorem III.5.8, there exist isometries $\sigma_p : L \otimes \mathbb{Z}_p \times \Lambda \otimes \mathbb{Z}_p$ for each $p < \infty$.

But now we have isometries $\sigma_p : L \otimes \mathbb{Q}_p \to \Lambda \otimes \mathbb{Q}_p$ for each $p \leq \infty$. By the weak Hasse principle (Theorem V.4.2), there is then an isometry $\sigma : L \otimes \mathbb{Q} \to \Lambda \otimes \mathbb{Q}$. Q.E.D.

COROLLARY 1.2. *Let L be an integral quadratic form with signature (s_+, s_-). Then any integral quadratic form whose signature is (s_+, s_-) and whose discriminant form is isomorphic to G_L is isometric to an integral quadratic form Λ such that*

(1) $\Lambda \subset L \otimes \mathbb{Q}$
(2) *for each $p < \infty$, there exists $\sigma_p \in \mathcal{O}(L \otimes \mathbb{Q}_p)$ such that $\sigma_p(L \otimes \mathbb{Q}_p) = \Lambda \otimes \mathbb{Z}_p$.*

PROOF. (1) is immediate. For (2), note that we constructed isometries $\sigma_p : L \otimes \mathbb{Z}_p \to \Lambda \otimes \mathbb{Z}_p$ in the proof of Theorem 1.1. Then σ_p induces an isometry $\sigma_p : L \otimes \mathbb{Q}_p \to \Lambda \otimes \mathbb{Q}_p$; since $\Lambda \otimes \mathbb{Q}_p = L \otimes \mathbb{Q}_p$, and σ_p may be regarded as an element of $\mathcal{O}(L \otimes \mathbb{Q}_p)$. Q.E.D.

The following is immediate from Theorem VI.4.1.

THEOREM 1.3. *Let L be an integral quadratic form.*

(1) *Suppose* $\Lambda \subset L \otimes \mathbb{Q}$ *is a* $\mathbb{Z}$*-lattice such that there exist* $\sigma_p \in \mathcal{O}(L \otimes \mathbb{Q}_p)$ *with* $\sigma_p(L \otimes \mathbb{Z}_p) = \Lambda \otimes \mathbb{Z}_p$ *for all* p*. Then for almost all* $p, \sigma_p \in \mathcal{O}(L \otimes \mathbb{Z}_p)$*.*
(2) *Suppose one is given* $\sigma_p \in \mathcal{O}(L \otimes \mathbb{Q}_p)$ *for all* p *such that* $\sigma_p \in \mathcal{O}(L \otimes \mathbb{Z}_p)$ *for almost all* p*. Then there is a* $\mathbb{Z}$*-lattice* $\Lambda \subset L \otimes \mathbb{Q}$ *such that* $\sigma_p(L \otimes \mathbb{Z}_p) = \Lambda \otimes \mathbb{Z}_p$ *for all* p*.*

Let us define

$$\mathcal{O}(L_{\mathbb{A}}) = \{\{\sigma_p\} | \quad \sigma_p \in \mathcal{O}(L \otimes \mathbb{Q}_p) \text{ for all } p, \\ \sigma_p \in \mathcal{O}(L \otimes \mathbb{Z}_p) \text{ for almost all } p\}.$$

For $\{\sigma_p\} \in \mathcal{O}(L_{\mathbb{A}})$ we denote the $\mathbb{Z}$-lattice whose existence is guaranteed by Theorem 1.3(2) by $\{\sigma_p\}(L)$.

If $\{\sigma_p\} \in \mathcal{O}(L_{\mathbb{A}})$ and $\Lambda = \{\sigma_p\}(L)$, there are induced maps

$$\sigma_p : \quad \Lambda^{\#} \otimes \mathbb{Z}_p \to L^{\#} \otimes \mathbb{Z}_p$$

which combine to define a map $G_\Lambda \to G_L$, which we denote by

$$G_{\{\sigma_p\}} : G_{\{\sigma_p\}(L)} \to G_L.$$

Since each $\sigma_p : L \otimes \mathbb{Z}_p \to \Lambda \otimes \mathbb{Z}_p$ is an isometry, $G_{\{\sigma_p\}}$ is an isomorphism. Summarizing, we get:

COROLLARY 1.4. *Let* L *be an integral quadratic form.*

(1) *Every integral quadratic form with the same signature and discriminant-form as* L *is isometric to a lattice of the form* $\{\sigma_p\}(L)$ *for some* $\{\sigma_p\} \in \mathcal{O}(L_{\mathbb{A}})$*.*
(2) *For every* $\{\sigma_p\} \in \mathcal{O}(L_{\mathbb{A}})$*, the lattice* $\{\sigma_p\}(L)$ *has the same signature and discriminant form as* L*.*

2. A consequence of the strong approximation theorem

Let L be an integral quadratic form. Recall that the homomorphism $(\det, \text{spin})$ on $\mathcal{O}(L \otimes \mathbb{Q}_p)$ takes values in the group

$$\Gamma_p = \{\pm 1\} \times \mathbb{Q}_p^*/(\mathbb{Q}_p^*)^2.$$

We also recall that we defined

$\Gamma_{p,0} = \{(1,1), (1,u_p), (-1,1), (-1,u_p)\}$ for p odd, and some non-square $u_p \in \mathbb{U}_p$ and

$$\Gamma_{2,0} = \{(1,1), (1,3), (1,5), (1,7), (-1,1), (-1,3), (-1,5), (-1,7)\}$$

as subgroups of Γ_p.

Define

$$\Gamma_{\mathbb{A}} = \{((d_p, s_p)) \in \prod_p \Gamma_p \mid (d_p, s_p) \in \Gamma_{p,0} \text{ for almost all } p\}$$

and

$$\Gamma_{\mathbb{A},\not\sim} = \prod_p \Gamma_{p,0}.$$

LEMMA 2.1. *Let L be an integral quadratic form of rank at least 2. The homomorphisms*

$$(\det, \text{spin}) : \mathcal{O}(L \otimes \mathbb{Q}_p) \to \Gamma_p$$

combine to give a homomorphism

$$(\det, \text{spin}) : \mathcal{O}(L_{\mathbb{A}}) \to \Gamma_{\mathbb{A}}$$

and this homomorphism is surjective if $\text{rank}(L) \geq 3$.

PROOF. If $\{\sigma_p\} \in \mathcal{O}(L_{\mathbb{A}})$, then $\sigma_p \in \mathcal{O}(L \otimes \mathbb{Z}_p)$ for almost all p. Also, $L \otimes \mathbb{Z}$ is unimodular for almost all p. But by Corollary VII.12.11(2), if $L \otimes \mathbb{Z}_p$ is unimodular of rank at least two, then the image $\Sigma(L)$ of $(\det, \text{spin})$ equals $\Gamma_{p,0}$. Thus, $(\det \sigma_p, \text{spin}\, \sigma_p) \in \Gamma_{p,0}$ for almost all p, so that

$$(\det, \text{spin})(\mathcal{O}(L_{\mathbb{A}})) \subset \Gamma_{\mathbb{A}}.$$

For the surjectivity, it is enough to show that if $\text{rank}(L) \geq 3$, then for each p, $(\det, \text{spin}) : \mathcal{O}(L \otimes \mathbb{Q}_p) \to \Gamma_p$ is surjective. But this is the content of Proposition V.6.1(1). Q.E.D.

Recall that for a quadratic form L over an integral domain R with quotient field K, the kernel of $(\det, \text{spin}) : \mathcal{O}(L) \to \{\pm 1\} \times K^\times/(K^\times)^2$ is denoted by $\Theta(L)$.

We let $\Theta(L_{\mathbb{A}})$ denote the kernel of

$$(\det, \text{spin}) : \mathcal{O}(L_{\mathbb{A}}) \to \Gamma_{\mathbb{A}}$$

so that

$$\Theta(L_{\mathbb{A}}) = \{\{\sigma_p\} \mid \sigma_p \in \Theta(L \otimes \mathbb{Q}_p) \text{ for all } p, \\ \sigma_p \in \Theta(L \otimes \mathbb{Z}_p) \text{ for almost all } p\}.$$

The strong approximation theorem for the spin group (Theorem V.7.2) tells us that elements of $\Theta(L_{\mathbb{A}})$ are closely related to elements of $\Theta(L \otimes \mathbb{Q})$, if L is indefinite and $\text{rank}(L) \geq 3$. To make this more precise, if L is an integral quadratic form and $\sigma \in \mathcal{O}(L \otimes \mathbb{Q})$, then $\sigma(L) = \Lambda$ is another (isometric) $\mathbb{Z}$-lattice. Mimicking the construction in Section 1, we consider the induced map

$$\sigma : \Lambda^\# \to L^\#$$

which induces an isomorphism on discriminant-forms $G_\sigma : G_\Lambda \to G_L$.

THEOREM 2.2. *Let L be an indefinite integral quadratic form with* $\mathrm{rank}(L) \geq 3$. *For any $\{\sigma_p\} \in \Theta(L_{\mathbb{A}})$ there is a $\sigma \in \Theta(L \otimes \mathbb{Q})$ such that $\sigma(L) = \{\sigma_p\}(L)$ and $G_\sigma = G_{\{\sigma_p\}}$.*

PROOF. Let $\Lambda = \{\sigma_p\}(L)$, and for each p define

$$\mathcal{V}_p = \{\rho_p \in \Theta(L \otimes \mathbb{Q}_p) \mid \rho_p(L \otimes \mathbb{Z}_p) = \Lambda \otimes \mathbb{Z}_p, \\ \text{and for all } x \in (\Lambda \otimes \mathbb{Z}_p)^\#,\ \ \rho_p(x) - \sigma_p(x) \in L \otimes \mathbb{Z}_p\}$$

so that for all $\rho_p \in \mathcal{V}_p$, G_{ρ_p} and G_{σ_p} coincide as maps $G_{\Lambda \otimes \mathbb{Z}_p} \to G_{L \otimes \mathbb{Z}_p}$.

$\mathcal{V}_p$ is clearly a non-empty open subset of $\Theta(L \otimes \mathbb{Q}_p)$. Moreover, for almost all p, $L \otimes \mathbb{Z}_p = \Lambda \otimes \mathbb{Z}_p$ (by Theorem 1.3(1)), and $L \otimes \mathbb{Z}_p$ is unimodular. But in this case, the condition on $\mathcal{V}_p$ merely says that $\mathcal{V}_p = \Theta(L \otimes \mathbb{Z}_p)$.

Thus, by the strong approximation theorem for the spin group (Theorem V.7.2), there is a $\sigma \in \Theta(L \otimes \mathbb{Q})$ such that $\sigma \in \mathcal{V}_p$ for each p. But this means that $\sigma(L) = \Lambda$, and that G_σ and $G_{\{\sigma_p\}}$ coincide as maps $G_\Lambda \to G_L$. Q.E.D.

We wish to recast this theorem in terms of the groups we introduced in Chapter VII. For an integral quadratic form L, let

$$\Sigma^\#(L) = \prod_p \Sigma^\#(L \otimes \mathbb{Z}_p) \subset \Gamma_{\mathbb{A},0},$$

where we recall that

$$\Sigma^\#(L \otimes \mathbb{Z}_p) = \mathrm{Im}((\det, \mathrm{spin}) : \mathcal{O}^\#(L \otimes \mathbb{Z}_p) \to \Gamma_{p,0})$$

and

$$\mathcal{O}^\#(L \otimes \mathbb{Z}_p) = \mathrm{Ker}(\mathcal{O}(L \otimes \mathbb{Z}_p) \to \mathcal{O}(G_{L \otimes \mathbb{Z}_p})).$$

We also let

$$\Gamma_{\mathbb{Q}} = \{\pm 1\} \times \mathbb{Q}^\times / (\mathbb{Q}^\times)^2,$$

and regard $\Gamma_{\mathbb{Q}} \subset \Gamma_{\mathbb{A}}$ in a natural way.

THEOREM 2.3. *Let L be an indefinite integral quadratic form with* $\mathrm{rank}(L) \geq 3$, *and let $\{\sigma_p\} \in \mathcal{O}(L_{\mathbb{A}})$. Then the following are equivalent:*

1. *there is a $\sigma \in \mathcal{O}(L \otimes \mathbb{Q})$ such that $\sigma(L) = \{\sigma_p\}(L)$ and $G_\sigma = G_{\{\sigma_p\}}$*
2. *$\prod_p (\det \sigma_p, \mathrm{spin}\, \sigma_p) \in \Gamma_{\mathbb{Q}} \cdot \Sigma^\#(L) \subset \Gamma_{\mathbb{A}}$.*

PROOF. First suppose that σ exists. Then since $G_\sigma = G_{\{\sigma_p\}}$, we see that

$$(\sigma \otimes \mathbb{Q}_p)^{-1} \circ \sigma_p \in \mathcal{O}^\#(L \otimes \mathbb{Z}_p)$$

for each p. Thus,

$$(\det\sigma_p, \operatorname{spin}\sigma_p) \in (\det\sigma, \operatorname{spin}\sigma)\Sigma^{\#}(L\otimes\mathbb{Z}_p)$$

for each p, so that

$$\prod_p(\det\sigma_p, \operatorname{spin}\sigma_p) \in (\det\sigma, \operatorname{spin}\sigma)\prod_p\Sigma^{\#}(L\otimes\mathbb{Z}_p)$$
$$\subseteq \Gamma_{\mathbb{Q}}\Sigma^{\#}(L).$$

Conversely, suppose that (2) holds. Then there exists a $(d,s)\in\Gamma_{\mathbb{Q}}$ and for each p a $\rho_p\in\mathcal{O}^{\#}(L\otimes\mathbb{Z}_p)$ such that

$$(\det\sigma_p, \operatorname{spin}\sigma_p) = (d,s)\cdot(\det\rho_p, \operatorname{spin}\rho_p)$$

for each p. Moreover, by Proposition V.6.1(2), there is a $\psi\in\mathcal{O}(L\otimes\mathbb{Q})$ such that $(\det\psi, \operatorname{spin}\psi) = (d,s)$.

Let $\phi_p = \psi^{-1}\circ\sigma_p\circ\rho_p^{-1}$, so that $(\det\phi_p, \operatorname{spin}\phi_p) = (1,1)$, i.e., that $\{\phi_p\}\in\Theta(L_{\mathbb{A}})$. By Theorem 2.2, there is a $\phi\in\Theta(L\otimes\mathbb{Q})$ such that $\phi(L) = \{\phi_p\}(L)$ and $G_\phi = G_{\{\phi_p\}}$.

Let $\sigma = \psi\circ\phi$. Then for each p,

$$\sigma(L\otimes\mathbb{Z}_p) = \psi\circ\phi_p(L\otimes\mathbb{Z}_p) = \sigma_p\circ\rho_p^{-1}(L\otimes\mathbb{Z}_p) = \sigma_p(L\otimes\mathbb{Z}_p)$$

since $\rho_p\in\mathcal{O}(L\otimes\mathbb{Z}_p)$, while

$$G_{\sigma\otimes\mathbb{Z}_p} = G_{(\psi\otimes\mathbb{Z}_p)\circ\psi_p} = G_{\sigma_p\circ\rho_p^{-1}} = G_{\rho_p}^{-1}\circ G_{\sigma_p} = G_{\sigma_p}$$

since G_{ρ_p} is the identity (because $\rho_p\in\mathcal{O}^{\#}(L\otimes\mathbb{Z}_p)$). Q.E.D.

3. Uniqueness of even $\mathbb{Z}$-lattices

Let L be an integral quadratic form with $\operatorname{rank} L\geq 2$, and let

$$\Sigma(L) = \prod_p\Sigma(L\otimes\mathbb{Z}_p)$$

where $\Sigma(L\otimes\mathbb{Z}_p) = \operatorname{Im}((\det,\operatorname{spin}) : \mathcal{O}(L\otimes\mathbb{Z}_p)\to\Gamma_p)$. Since $L\otimes\mathbb{Z}_p$ is unimodular for almost all p, and $\Sigma(L\otimes\mathbb{Z}_p)\subset\Gamma_{p,0}$ whenever $L\otimes\mathbb{Z}_p$ is unimodular (Corollary VII.12.11(2)), we see that $\Sigma(L)\subset\Gamma_{\mathbb{A}}$.

THEOREM 3.1. *Let L be an indefinite integral quadratic form with* $\operatorname{rank}(L)\geq 3$. *Let $\Lambda_1,\Lambda_2\subset L\otimes\mathbb{Q}$ be $\mathbb{Z}$-lattices with $\Lambda_1 = \{\sigma_p\}(L)$ and $\Lambda_2 = \{\rho_p\}(L)$ for appropriate $\{\sigma_p\},\{\rho_p\}\in\mathcal{O}(L_{\mathbb{A}})$. Then Λ_1 is isometric to Λ_2 if and only if*

$$\prod_p(\det\sigma_p, \operatorname{spin}\sigma_p) \equiv \prod_p(\det\rho_p, \operatorname{spin}\rho_p) \mod \Gamma_{\mathbb{Q}}\cdot\Sigma(L).$$

PROOF. If $\psi : \Lambda_1 \to \Lambda_2$ is an isometry, then $\psi \in \mathcal{O}(L \otimes \mathbb{Q})$ and

$$\phi_p = \sigma_p^{-1} \circ (\psi \otimes \mathbb{Z}_p)^{-1} \circ \rho_p \in \mathcal{O}(L \otimes \mathbb{Z}_p)$$

for every p. Thus,

$$\begin{aligned} \prod_p (\det \sigma_p, \operatorname{spin} \sigma_p)^{-1} (\det \rho_p, \operatorname{spin} \rho_p) &= (\det \psi, \operatorname{spin} \psi) \prod_p (\det \phi_p, \operatorname{spin} \phi_p) \\ &\in \Gamma_{\mathbb{Q}} \cdot \Sigma(L). \end{aligned}$$

Conversely, if

$$\prod_p (\det \sigma_p, \operatorname{spin} \sigma_p)^{-1} (\det \rho_p, \operatorname{spin} \rho_p) \in \Gamma_{\mathbb{Q}} \cdot \Sigma(L)$$

then there exist $(d, s) \in \Gamma_{\mathbb{Q}}$ and $\phi_p \in \mathcal{O}(L \otimes \mathbb{Z}_p)$ for all p such that

$$(\det \sigma_p, \operatorname{spin} \sigma_p)^{-1} (\det \rho_p, \operatorname{spin} \rho_p) = (d, s)(\det \phi_p, \operatorname{spin} \phi_p)$$

for all p. Let

$$\psi_p = \rho_p \circ \phi_p^{-1} \circ \sigma_p^{-1}.$$

Then $\psi_p(\Lambda_1 \otimes \mathbb{Z}_p) = \Lambda_2 \otimes \mathbb{Z}_p$, and

$$\prod_p (\det \psi_p, \operatorname{spin} \psi_p) = (d, s) \in \Gamma_{\mathbb{Q}} \subset \Gamma_{\mathbb{Q}} \cdot \Sigma^{\#}(\Lambda_1).$$

By Theorem 2.3, there is a $\psi \in \mathcal{O}(\Lambda_1 \otimes \mathbb{Q}) = \mathcal{O}(L \otimes \mathbb{Q})$ such that $\psi(\Lambda_1) = \Lambda_2$. Q.E.D.

For an integral quadratic form L, let

$$\begin{aligned} g(L) = \ \{ &\text{ isometry classes of integral quadratic forms } \Lambda \text{ such that} \\ &G_L \cong G_\Lambda \text{ and } \operatorname{sign}(L) = \operatorname{sign}(\Lambda)\}. \end{aligned}$$

COROLLARY 3.2. *Let L be an indefinite integral quadratic form with* $\operatorname{rank}(L) \geq 3$. *Then the set $g(L)$ is in one-to-one correspondence with* $\Gamma_{\mathbb{A}}/\Gamma_{\mathbb{Q}} \cdot \Sigma(L)$.

PROOF. This follows from Corollary 1.4, the surjectivity of the homomorphism $(\det, \operatorname{spin}) : \mathcal{O}(L_{\mathbb{A}}) \to \Gamma_{\mathbb{A}}$ (Lemma 2.1), and Theorem 3.1. Q.E.D.

COROLLARY 3.3. *Let L be an indefinite integral quadratic form with* $\operatorname{rank}(L) \geq 3$. *Then L is uniquely determined up to isometry by its signature and discriminant-form if and only if*

$$\Gamma_{\mathbb{Q}} \cdot \Sigma(L) = \Gamma_{\mathbb{A}}.$$

4. Milnor's theorem and stable classes

We will derive some corollaries of the uniqueness criterion stated in Corollary 3.3.

LEMMA 4.1. $\Gamma_{\mathbb{A}} = \Gamma_{\mathbb{Q}} \cdot \Gamma_{\mathbb{A},\not\sim}$.

PROOF. Let $\prod_p (d_p, s_p) \in \Gamma_{\mathbb{A}}$, so that $(d_p, s_p) \in \Gamma_p$ for every p and $(d_p, s_p) \in \Gamma_{p,0}$ for almost all p. Let S be the set of primes p such that $(d_p, s_p) \notin \Gamma_{p,0}$; this is the set of primes such that s_p is not a represented by a unit, i.e., the set of primes such that s_p is divisible by p. Let $s = \prod_{p \in S} p$.

Then $(d_p, ss_p) \in \Gamma_{p,0}$ for all p, so that

$$\prod_p (d_p, s_p) = (1, 1/s) \prod_p (d_p, ss_p) \in \Gamma_{\mathbb{Q}} \cdot \Gamma_{\mathbb{A},\not\sim}.$$

Q.E.D.

COROLLARY 4.2. *Let L be an indefinite integral quadratic form with* $\operatorname{rank}(L) \geq 3$ *and* $\operatorname{rank}(L) \geq \ell(q_L) + 2$. *Then L is uniquely determined up to isometry by its signature and discriminant form.*

PROOF. By Corollary VII.12.11(1), $\Sigma^{\#}(L) = \Gamma_{\mathbb{A},\not\sim}$. Thus,

$$\Gamma_{\mathbb{A}} \supset \Gamma_{\mathbb{Q}} \cdot \Sigma(L) \supset \Gamma_{\mathbb{Q}} \cdot \Sigma^{\#}(L) = \Gamma_{\mathbb{Q}} \cdot \Gamma_{\mathbb{A},\not\sim} = \Gamma_{\mathbb{A}}$$

which forces $\Gamma_{\mathbb{A}} = \Gamma_{\mathbb{Q}} \cdot \Sigma(L)$; now the statement follows from Corollary 3.3. Q.E.D.

THEOREM 4.3. *Let L be an indefinite unimodular integral quadratic form. Then there exist a, b such that*

$$L \cong U^a \oplus E_8^b \quad \text{or} \quad L \cong U^a \oplus E_8(-1)^b$$

where U is the lattice whose form has matrix $\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$, *$E_8$ is the lattice whose form has matrix*

$$\begin{pmatrix}
2 & 0 & 0 & -1 & & & & \\
0 & 2 & -1 & 0 & & & & \\
0 & -1 & 2 & -1 & & & & \\
-1 & 0 & -1 & 2 & -1 & & & \\
 & & & -1 & 2 & -1 & & \\
 & & & & -1 & 2 & -1 & \\
 & & & & & -1 & 2 & -1 \\
 & & & & & & -1 & 2
\end{pmatrix}$$

and $E_8(-1)$ is the lattice whose form has the matrix above with all signs changed.

REMARK 4.4. The proof we give here is much too deep; a more elementary proof can be found in [**Serre 73**, Chapter V, Section 2.2, Theorem 5].

PROOF. We leave the case $\operatorname{rank}(L) = 2$ to the reader, and assume $\operatorname{rank}(L) \geq 3$. Let $\operatorname{sign}(L) = (s_+, s_-)$; since L is unimodular, $q_L = 0$ and we have $s_+ - s_- \equiv 0 \mod 8$ by Milgram's Theorem III.5.1. If $s_+ \geq s_-$, let $a = s_-$, and $b = \frac{1}{8}(s_+ - s_-)$. Since $\operatorname{sign}(U) = (1,1)$ and $\operatorname{sign}(E_8) = (8,0)$, we see that

$$U^a \oplus E_8^b$$

has signature (s_+, s_-). But now $\operatorname{rank}(L) \geq \ell(q_L) + 2 = 2$, so that by Corollary 4.2 there is at most one unimodular integral quadratic form with signature (s_+, s_-). Hence, $L \cong U^a \oplus E_8^b$.

The case $s_+ < s_-$ is similar. Q.E.D.

Let us say that two integral quadratic forms L_1 and L_2 are stably equivalent if there exist unimodular integral quadratic forms Λ_1 and Λ_2 with

$$L_1 \oplus \Lambda_1 \cong L_2 \oplus \Lambda_2.$$

THEOREM 4.5. *Two integral quadratic forms L_1 and L_2 are stably equivalent if and only if $q_{L_1} \cong q_{L_2}$.*

REMARK 4.6. Once again our proof is too deep; a more elementary proof is in [**Wall 72**].

PROOF. If L_1 and L_2 are stably equivalent, then

$$q_{L_1} = q_{L_1} \oplus q_{\Lambda_1} \cong q_{L_2} \oplus q_{\Lambda_2} = q_{L_2}.$$

Conversely, if $q_{L_1} \cong q_{L_2}$, let $\operatorname{sign}(L_1) = (s_+, s_-)$ and $\operatorname{sign}(L_2) = (t_+, t_-)$; we may suppose that $s_+ \geq t_+$. By Milgram's Theorem III.5.1 we have $s_+ - s_- \equiv t_+ - t_- \mod 8$. Consider the lattices

$$L_1 \oplus U \quad \text{and} \quad L_2 \oplus U^{s_+ - t_+ + 1} \oplus E_8(-1)^{\frac{1}{8}(s_- - t_- - s_+ + t_+)}$$

if $s_- \geq t_- + s_+ - t_+$;

$$L_1 \oplus U \oplus E_8(-1)^{\frac{1}{8}(s_+ - t_+ - s_- + t_-)} \quad \text{and} \quad L_2 \oplus U^{s_+ - t_+ + 1}$$

if $s_- < t_- + s_+ - t_+$.

In the first case, both have signature $(s_+ + 1, s_- + 1)$; they have isomorphic discriminant-forms and

$$\operatorname{rank}(L_1 \oplus U) = \operatorname{rank}(L_1) + 2 \geq \ell(q_{L_1}) + 2$$

so that by Corollary 4.2, they must be isometric. In particular, L_1 and L_2 are stably equivalent.

The second case is similar. Q.E.D.

5. Surjectivity of the map between orthogonal groups

We turn now to the study of the natural map $\mathcal{O}(L) \to \mathcal{O}(G_L)$ for an integral quadratic form L.

THEOREM 5.1. *Let L be an indefinite integral quadratic form with* $\operatorname{rank}(L) \geq 3$. *Then there is an exact sequence*

$$\mathcal{O}(L) \to \mathcal{O}(G_L) \to \Sigma(L)/(\Gamma_{\mathbb{Q}} \cap \Sigma(L)) \cdot \Sigma^{\#}(L) \to 0.$$

PROOF. By Corollaries IV.2.14 and IV.5.9, for each p the map

$$\mathcal{O}(L \otimes \mathbb{Z}_p) \to \mathcal{O}(G_{L \otimes \mathbb{Z}_p})$$

is surjective. Thus, there is a commutative diagram with exact rows and columns

$$\begin{array}{ccccccccc} 1 & \to & \mathcal{O}^{\#}(L \otimes \mathbb{Z}_p) & \to & \mathcal{O}(L \otimes \mathbb{Z}_p) & \to & \mathcal{O}(G_{L \otimes \mathbb{Z}_p}) & \to & 1 \\ & & \downarrow & & \downarrow & & & & \\ 0 & \to & \Sigma^{\#}(L \otimes \mathbb{Z}_p) & \to & \Sigma(L \otimes \mathbb{Z}_p) & & & & \\ & & \downarrow & & \downarrow & & & & \\ & & 0 & & 0 & & & & \end{array}$$

which induces a surjective map $\mu_p : \mathcal{O}(G_{L \otimes \mathbb{Z}_p}) \to \Sigma(L \otimes \mathbb{Z}_p)/\Sigma^{\#}(L \otimes \mathbb{Z}_p)$ for each p. These combine to give a surjective map

$$\mu : \mathcal{O}(G_L) \to \Sigma(L)/\Sigma^{\#}(L).$$

Given an element $\gamma \in \mathcal{O}(G_L)$, for each p there exists $\sigma_p \in \mathcal{O}(L \otimes \mathbb{Z}_p)$ such that σ_p and γ induce the same transformation in $\mathcal{O}(G_{L \otimes \mathbb{Z}_p})$, by the surjectivity of $\mathcal{O}(L \otimes \mathbb{Z}_p) \to \mathcal{O}(G_{L \otimes \mathbb{Z}_p})$. We consider the collection $\{\sigma_p\}$ to be in $\mathcal{O}(L_{\mathbb{A}})$; then by construction $G_{\{\sigma_p\}} = \gamma \in \mathcal{O}(G_L)$. Moreover, for any such $\{\sigma_p\}$, we have $\mu(\gamma) = \prod_p (\det \sigma_p, \operatorname{spin} \sigma_p) \mod \Sigma^{\#}(L)$.

By Theorem 2.3, $G_{\{\sigma_p\}}$ is in the image of $\mathcal{O}(L) \to \mathcal{O}(G_L)$ if and only if $\prod_p (\det \sigma_p, \operatorname{spin} \sigma_p) \in \Gamma_{\mathbb{Q}} \cdot \Sigma^{\#}(L)$; this is equivalent to having

$$\mu(\gamma) \in (\Gamma_{\mathbb{Q}} \cdot \Sigma^{\#}(L)) \cap \Sigma(L) \mod \Sigma^{\#}(L).$$

Since

$$(\Gamma_{\mathbb{Q}} \cdot \Sigma^{\#}(L)) \cap \Sigma(L) = (\Gamma_{\mathbb{Q}} \cap \Sigma(L)) \cdot \Sigma^{\#}(L),$$

we see that the image of $\mathcal{O}(L) \to \mathcal{O}(G_L)$ coincides with the kernel of the composite map

$$\mathcal{O}(G_L) \xrightarrow{\mu} \Sigma(L)/\Sigma^{\#}(L) \to \Sigma(L)/(\Gamma_{\mathbb{Q}} \cap \Sigma(L)) \cdot \Sigma^{\#}(L).$$

Q.E.D.

COROLLARY 5.2. *Let L be an indefinite integral quadratic form with* $\operatorname{rank}(L) \geq 3$. *Then the natural map $\mathcal{O}(L) \to \mathcal{O}(G_L)$ is surjective if and only if*

$$(\Gamma_{\mathbb{Q}} \cap \Sigma(L)) \cdot \Sigma^{\#}(L) = \Sigma(L).$$

6. Computations in terms of the discriminant-form

We wish to indicate how the results of Chapter VII enable one to compute the finite groups introduced in Corollary 3.2 and Theorem 5.1 in terms of the discriminant-form. The computation requires consulting the tables in Section 12 of Chapter VII, and then computing a finite number of Legendre symbols.

Let S be the (finite) set of square-free integers dividing $2\operatorname{disc}(L)$, and let

$$\Gamma_S = \{(d, s) \in \Gamma_{\mathbb{Q}} \mid s \in S\}.$$

Let T be the (infinite) set of square-free integers relatively prime to $2\operatorname{disc}(L)$, and let

$$\Gamma_T = \{(d, s) \in \Gamma_{\mathbb{Q}} \mid s \in T\}.$$

Clearly, $\Gamma_{\mathbb{Q}} = \Gamma_S \cdot \Gamma_T$ and $\Gamma_S \cap \Gamma_T = \{\pm 1, \pm 1\}$.

PROPOSITION 6.1. *Let L be an indefinite integral quadratic form with* $\operatorname{rank}(L) \geq 3$.

(1) *The genus group of L is isomorphic to the cokernel of*

$$\Gamma_S \to \left(\prod_{p \mid 2\operatorname{disc}(L)} \Gamma_p / \cdot \Sigma(L \otimes \mathbb{Z}_p) \right) / \{(\pm 1, \pm 1)\}_S.$$

where $\{(\pm 1, \pm 1)\}_S$ is the projection of $\{(\pm 1, \pm 1)\} \subset \Gamma_{\mathbb{Q}}$ to $\prod_{p \mid 2\operatorname{disc}(L)} \Gamma_p$.

(2) *The cokernel of $\mathcal{O}(L) \to \mathcal{O}(G_L)$ is isomorphic to the cokernel of*

$$\Gamma_S \cap \Sigma(L) \to \Sigma(L)/\Sigma^{\#}(L).$$

Note that in both cases, the map generally fails to be injective, so that one must compute the image (or the kernel) as well as the two finite groups involved.

PROOF. The genus group coincides with $\Gamma_{\mathbb{A}}/\Gamma_{\mathbb{Q}} \cdot \Sigma(L)$ by Corollary 3.2. We have the exact sequence

$$0 \to \Gamma_{\mathbb{Q}} \cdot \Sigma(L)/\Gamma_T \cdot \Sigma(L) \to \Gamma_{\mathbb{A}}/\Gamma_T \cdot \Sigma(L) \to \Gamma_{\mathbb{A}}/\Gamma_{\mathbb{Q}} \cdot \Sigma(L) \to 0,$$

and since $\Gamma_{\mathbb{Q}} = \Gamma_S \cdot \Gamma_T$ we have

$$\Gamma_{\mathbb{Q}} \cdot \Sigma(L)/\Gamma_T \cdot \Sigma(L) = \Gamma_S \cdot \Gamma_T \cdot \Sigma(L)/\Gamma_T \cdot \Sigma(L) \cong \Gamma_S/\Gamma_S \cap \Gamma_T \cdot \Sigma(L).$$

Therefore the genus group $g(L)$ is isomorphic to the cokernel of the natural map

$$\Gamma_S \to \Gamma_{\mathbb{A}}/\Gamma_T \cdot \Sigma(L)$$

and to prove (1) we must identify the quotient $\Gamma_{\mathbb{A}}/\Gamma_T \cdot \Sigma(L)$

Fix an element $\gamma = ((d_p, s_p)) \in \Gamma_{\mathbb{A}}$, so that $(d_p, s_p) \in \Gamma_p$ for every p and is in $\Gamma_{p,0}$ for almost all p. Let X denote the (finite) set of primes which do not divide $2\,\mathrm{disc}(L)$ such that $(d_p, s_p) \notin \Gamma_{p,0}$. This means that for each $p \in X$, the spin value s_p has a p factor. Let n be the product of the primes of X. Then $(1, n) \in \Gamma_T$ and $(1, n) \cdot (d_p, s_p) \in \Gamma_{p,0}$ for every p.

For the primes p which do not divide $2\,\mathrm{disc}(L)$, $L \otimes \mathbb{Z}_p$ is unimodular, and so by Corollary VII.12.11(2), $\Sigma(L \otimes \mathbb{Z}_p) = \Gamma_{p,0}$. Therefore the element

$$\gamma' = \prod_{p \nmid 2\,\mathrm{disc}(L)} (d_p, n s_p) \in \Sigma(L).$$

Consider the element

$$\gamma'' = \prod_{p | 2\,\mathrm{disc}(L)} (d_p, s_p/n) \in \prod_{p | 2\,\mathrm{disc}(L)} \Gamma_p.$$

Then $\gamma = (1, n) \cdot \gamma' \cdot \gamma''$, and shows that

$$\gamma \in [\prod_{p | 2\,\mathrm{disc}(L)} \Gamma_p] \cdot \Gamma_T \cdot \Sigma(L).$$

Since γ was arbitrary in $\Gamma_{\mathbb{A}}$ this proves that

$$\Gamma_{\mathbb{A}} = [\prod_{p | 2\,\mathrm{disc}(L)} \Gamma_p] \cdot \Gamma_T \cdot \Sigma(L)$$

and therefore the inclusion

$$\prod_{p | 2\,\mathrm{disc}(L)} \Gamma_p \subset \Gamma_{\mathbb{A}}$$

induces an onto homomorphism

$$\phi : \prod_{p | 2\,\mathrm{disc}(L)} \Gamma_p \to \Gamma_{\mathbb{A}}/\Gamma_T \cdot \Sigma(L).$$

The kernel of ϕ is $[\prod_{p | 2\,\mathrm{disc}(L)} \Gamma_p] \cap [\Gamma_T \cdot \Sigma(L)]$; suppose that

$$\prod_{p | 2\,\mathrm{disc}(L)} (d_p, s_p) = (d, n) \cdot \prod_p (d'_p, s'_p)$$

is in this kernel, with $(d, n) \in \Gamma_T$ and $(d'_p, s'_p) \in \Sigma(L \otimes \mathbb{Z}_p)$ for each p. If n is divisible by a prime q which does not divide $2\,\mathrm{disc}(L)$, then (since $\Sigma(L \otimes \mathbb{Z}_q) = \Gamma_{q,0}$ in this case) we have a contradiction: in the q

part of the above equation, the left side is 1 and the right side is not. Therefore since $n \in T$ we must have $n = \pm 1$, so that the kernel of ϕ is

$$[\prod_{p|2\,\mathrm{disc}(L)} \Gamma_p] \cap [\Gamma_T \cdot \Sigma(L)] = [\prod_{p|2\,\mathrm{disc}(L)} \Gamma_p] \cap [\{(\pm 1, \pm 1)\} \cdot \Sigma(L)].$$

Recall that $\{(\pm 1, \pm 1)\}_S$ denotes the projection of the subgroup $\{(\pm 1, \pm 1)\}$ into $\prod_{p|2\,\mathrm{disc}(L)} \Gamma_p$. We claim that the above intersection is equal to

(6.2)
$$[\prod_{p|2\,\mathrm{disc}(L)} \Gamma_p] \cap [\{(\pm 1, \pm 1)\} \cdot \Sigma(L)] = \{(\pm 1, \pm 1)\}_S \cdot \prod_{p|2\,\mathrm{disc}(L)} \Sigma(L \otimes \mathbb{Z}_p).$$

Clearly the right-hand side is contained in $\prod_{p|2\,\mathrm{disc}(L)} \Gamma_p$; to show it is contained in $\{(\pm 1, \pm 1)\} \cdot \Sigma(L)$, fix an element $(d', s') \in \{(\pm 1, \pm 1)\}_S$ and elements $(d_p, s_p) \in \Sigma(L \otimes \mathbb{Z}_p)$ for each p dividing $2\,\mathrm{disc}(L)$. Lift (d', s') to $(d, s) \in \{(\pm 1, \pm 1)\}$, and for each p not dividing $2\,\mathrm{disc}(L)$, set $d_p = d$ and $s_p = s$. Then these are not divisible by p, so that for these p, we have $(d_p, s_p) \in \Sigma(L \otimes \mathbb{Z}_p)$ since $\Sigma(L \otimes \mathbb{Z}_p) = \Gamma_{p,0}$ in this case. Now the product $(d, s) \prod_p (d_p, s_p) \in \{(\pm 1, \pm 1)\} \cdot \Sigma(L)$, and is equal to the original product $(d', s') \prod_{p|2\,\mathrm{disc}(L)} (d_p, s_p)$ since for the other primes the (d, s) factor cancels the (d_p, s_p) term. This proves that the right-hand side of (6.2) is contained in the left-hand side.

That the left-hand side is contained in the right is clear. This identifies the kernel of the map ϕ and proves that

$$\Gamma_{\mathbb{A}} / \Gamma_T \cdot \Sigma(L) \cong \left(\prod_{p|2\,\mathrm{disc}(L)} \Gamma_p / \cdot \Sigma(L \otimes \mathbb{Z}_p) \right) / \{(\pm 1, \pm 1)\}_S$$

which finishes the proof of (1).

To see (2), since $\Sigma(L \otimes \mathbb{Z}_p) = \Gamma_{p,0}$ when $p \not| \, 2\,\mathrm{disc}(L)$ we have $\Gamma_{\mathbb{Q}} \cap \Sigma(L) \subset \Gamma_S$ so that

$$\Gamma_{\mathbb{Q}} \cap \Sigma(L) = \Gamma_S \cap \Sigma(L).$$

Now there is a natural exact sequence

$$0 \to \Gamma_{\mathbb{Q}} \cap \Sigma(L) / \Gamma_{\mathbb{Q}} \cap \Sigma^{\#}(L) \to \Sigma(L) / \Sigma^{\#}(L) \to \Sigma(L) / (\Gamma_{\mathbb{Q}} \cap \Sigma(L)) \cdot \Sigma^{\#}(L) \to 0$$

which gives rise to an exact sequence

$$\Gamma_S \cap \Sigma(L) \to \Sigma(L) / \Sigma^{\#}(L) \to \Sigma(L) / (\Gamma_{\mathbb{Q}} \cap \Sigma(L)) \cdot \Sigma^{\#}(L) \to 0.$$

Since the cokernel of $\mathcal{O}(L) \to \mathcal{O}(G_L)$ is $\Sigma(L) / (\Gamma_{\mathbb{Q}} \cap \Sigma(L)) \cdot \Sigma^{\#}(L)$ by Theorem 5.1, the proposition is proved. Q.E.D.

Now Section 12 of Chapter VII enables us to compute $\Sigma(L \otimes \mathbb{Q}_p)$ and $\Sigma(L \otimes \mathbb{Z}_p)/\Sigma^{\#}(L \otimes \mathbb{Z}_p)$ immediately given the discriminant-form; the Proposition above enables us to find both the genus group and the cokernel of $\mathcal{O}(L) \to \mathcal{O}(G_L)$ with a finite amount of computation.

7. A criterion for uniqueness and surjectivity

In this section, we find a group which is an extension of the cokernel of $\mathcal{O}(L) \to \mathcal{O}(G_L)$ by the genus group. This group has the advantage of being more readily computable than either of its constituents; it can be essentially read off of the tables in Section 12 of Chapter V. Moreover, in many applications, one only needs to know the product of the orders of the cokernel of $\mathcal{O}(L) \to \mathcal{O}(G_L)$ and the genus group; this is easily found by computing the group below.

By Lemma 4.1, the natural map $\Gamma_{\mathbb{A},0} \to \Gamma_{\mathbb{A}}/\Gamma_{\mathbb{Q}}$ is surjective; we let Γ_0 denote the kernel of this map, which coincides with $\Gamma_{\mathbb{A},0} \cap \Gamma_{\mathbb{Q}}$. It is easy to see that

$$\Gamma_0 = \{(1,1),(1,-1),(-1,1),(-1,-1)\} \subset \Gamma_{\mathbb{Q}},$$

so that this agrees with the notation of Chapter VII Section 12. In that section, we defined

$$\Sigma_0^{\#}(L \otimes \mathbb{Z}_p) = \phi_p^{-1}(\Sigma^{\#}(L \otimes \mathbb{Z}_p))$$

where $\phi_p : \Gamma_0 \to \Gamma_{p,0}$ is the natural map; we now define, for an integral quadratic form L,

$$\Sigma_0^{\#}(L) = \Sigma^{\#}(L) \cap \Gamma_0 = \cap_p \Sigma_0^{\#}(L \otimes \mathbb{Z}_p).$$

Lemma 7.1. *Let L be an integral quadratic form. Then there is an exact sequence*

$$0 \to \Sigma(L)/(\Gamma_{\mathbb{Q}} \cap \Sigma(L)) \cdot \Sigma^{\#}(L) \to (\Gamma_{\mathbb{A},0}/\Sigma^{\#}(L))/(\Gamma_0/\Sigma_0^{\#}(L)) \to \Gamma_{\mathbb{A}}/\Gamma_{\mathbb{Q}} \cdot \Sigma(L) \to 0$$

Proof. The exact sequence

$$0 \to \Gamma_0 \to \Gamma_{\mathbb{A},0} \to \Gamma_{\mathbb{A}}/\Gamma_{\mathbb{Q}} \to 0$$

induces an exact sequence

$$0 \to \Gamma_0/\Sigma_0^{\#}(L) \to \Gamma_{\mathbb{A},0}/\Sigma^{\#}(L) \to \Gamma_{\mathbb{A}}/\Gamma_{\mathbb{Q}} \cdot \Sigma^{\#}(L) \to 0$$

by the definition of $\Sigma_0^{\#}(L) = \Sigma^{\#}(L) \cap \Gamma_0$. Thus, the middle term of the exact sequence in the statement is isomorphic to

$$\Gamma_{\mathbb{A}}/\Gamma_{\mathbb{Q}} \cdot \Sigma^{\#}(L).$$

But now, since $\Sigma(L) \cap (\Gamma_{\mathbb{Q}} \cdot \Sigma^{\#}(L)) = (\Gamma_{\mathbb{Q}} \cap \Sigma(L)) \cdot \Sigma^{\#}(L)$, there is a canonical exact sequence

$$0 \to \Sigma(L)/(\Gamma_{\mathbb{Q}} \cap \Sigma(L)) \cdot \Sigma^{\#}(L) \to \Gamma_{\mathbb{A}}/\Gamma_{\mathbb{Q}} \cdot \Sigma^{\#}(L) \to \Gamma_{\mathbb{A}}/\Gamma_{\mathbb{Q}} \cdot \Sigma(L) \to 0.$$

Q.E.D.

THEOREM 7.2. *Let L be an indefinite integral quadratic form with* $\operatorname{rank}(L) \geq 3$. *Then there is an exact sequence*

$$0 \to \mathit{coker}\,(\mathcal{O}(L) \to \mathcal{O}(G_L)) \to (\Gamma_{\mathbb{A},0}/\Sigma^{\#}(L))/(\Gamma_0/\Sigma_0^{\#}(L)) \to g(L) \to 0$$

where $g(L)$ is the genus group of L.

The proof is immediate from Corollary 3.2, Theorem 5.1 and Lemma 7.1. From Corollaries 3.3 and 5.2, using Lemma 7.1 we also get:

COROLLARY 7.3. *Let L be an indefinite integral quadratic form with* $\operatorname{rank}(L) \geq 3$. *Then the following are equivalent:*

(1) *L is uniquely determined by its signature and discriminant-form*
and $\mathcal{O}(L) \to \mathcal{O}(G_L)$ is surjective.
(2) $\Gamma_0/\Sigma_0^{\#}(L) \cong \Gamma_{\mathbb{A},0}/\Sigma^{\#}(L)$.

Computing the group

$$(\Gamma_{\mathbb{A},0}/\Sigma^{\#}(L))/(\Gamma_0/\Sigma_0^{\#}(L))$$

is even easier than computing its constituents, the cokernel of $\mathcal{O}(L) \to \mathcal{O}(G_L)$ and the genus group $g(L)$. For

$$\Gamma_{\mathbb{A},0}/\Sigma^{\#}(L) = \prod_{p|\operatorname{disc}(L)} \Gamma_{p,0}/\Sigma^{\#}(L \otimes \mathbb{Z}_p)$$

and

$$\Gamma_0/\Sigma_0^{\#}(L) = \Gamma_0/\cap_{p|\operatorname{disc}(L)} \Sigma_0^{\#}(L \otimes \mathbb{Z}_p)$$

(since $\Sigma^{\#}(L \otimes \mathbb{Z}_p) = \Gamma_{p,0}$ and hence $\Sigma_0^{\#}(L \otimes \mathbb{Z}_p) = \Gamma_0$ whenever $L \otimes \mathbb{Z}_p$ is unimodular, by Corollary VII.12.11(2)). Since one can read the groups $\Sigma^{\#}(L \otimes \mathbb{Z}_p)$ and $\Sigma_0^{\#}(L \otimes \mathbb{Z}_p)$ from the tables in Section 12 of Chapter VII, the computation is immediate.

Due to its importance in applications, we want to make this computation explicit in one particular case; namely, we wish to translate Corollary 7.3 into information about the discriminant form, and so get a criterion for uniqueness and surjectivity solely in terms of the discriminant-form.

DEFINITION 7.4. Let L be an integral quadratic form.

(1) L is $\underline{p\text{-regular}}$ if $\Sigma^{\#}(L \otimes \mathbb{Z}_p) = \Gamma_{p,0}$.
(2) L is $\underline{p\text{-semiregular of type } (a,b)}$ where $(a,b) \in \{(1,-1),(-1,1),(-1,-1)\}$ if $[\Gamma_{p,0} : \Sigma^{\#}(L \otimes \mathbb{Z}_p)] = 2$ and $\Sigma_0^{\#}(L \otimes \mathbb{Z}_p) = \{(1,1),(a,b)\}$.
(3) L is $\underline{p\text{-pseudoregular}}$ if $[\Gamma_{p,0} : \Sigma^{\#}(L \otimes \mathbb{Z}_p)] = 4$ and $\Sigma_0^{\#}(L \otimes \mathbb{Z}_p) = \{(1,1)\}$.

(4) We say that L is p-nonregular if it is neither p-regular, p-semiregular, nor p-pseudoregular.

THEOREM 7.5. *Let L be an indefinite integral quadratic form with* $\operatorname{rank}(L) \geq 3$. *Then L is uniquely determined by its signature and discriminant-form and $\mathcal{O}(L) \to \mathcal{O}(G_L)$ is surjective if and only if one of the following holds:*

(1) *L is p-regular for all p.*
(2) *There is one prime p such that L is p-semiregular; for all primes $q \neq p$, L is q-regular.*
(3) *There are two primes p_1, p_2 such that L is p_1-semiregular of type (a_1, b_1) and L is p_2-semiregular of type (a_2, b_2) with $(a_1, b_1) \neq (a_2, b_2)$; for all primes $q \neq p_1, p_2$, L is q-regular.*
(4) *There is one prime p such that L is p-pseudoregular; for all primes $q \neq p$, L is q-regular.*

PROOF. By Corollary 7.3, we must find the conditions under which

$$(*) \qquad \Gamma_0/\Sigma_0^{\#}(L) \cong \prod_{p|\operatorname{disc}(L)} \Gamma_{p,0}/\Sigma^{\#}(L \otimes \mathbb{Z}_p).$$

Note that the left-hand side maps injectively to the right-hand side, and since Γ_0 is a group of order 4, the left-hand side has order at most 4.

First we note that it is easy to see that any one of the conditions (1)-(4) are sufficient. If (1) holds, then $\Sigma^{\#}(L \otimes \mathbb{Z}_p) = \Gamma_{p,0}$ for all p, so that the right-hand side of (*) has order one, forcing an equality. If (2) holds, then both sides of (*) have order two, and if either (3) or (4) hold then both sides of (*) have order four.

To see that one of the conditions is necessary, we assume that (*) holds, and suppose first that the right-hand side of (*) has order 1. Then $\Sigma_0^{\#}(L) = \Gamma_0$ for all p, so that L is p-regular for all p, and we have (1).

If the right hand side of (*) has order 2, then there is exactly one prime p such that $[\Gamma_{p,0} : \Sigma^{\#}(L \otimes \mathbb{Z}_p)] = 2$. Since for all $q \neq p$ we have $\Sigma_0^{\#}(L \otimes \mathbb{Z}_q) = \Gamma_0$, we see that $\Sigma_0^{\#}(L) = \Sigma_0^{\#}(L \otimes \mathbb{Z}_p)$. Thus, equality holding in (*) implies that $|\Sigma_0^{\#}(L \otimes \mathbb{Z}_p)| = 2$, that is, L is p-semiregular and we have case (2).

If the right hand side of (*) has order 4 and (*) holds, we must have $\Sigma_0^{\#}(L) = \{(1,1)\}$. Either there are primes p_1, p_2 with $[\Gamma_{p_i,0} : \Sigma^{\#}(L \otimes \mathbb{Z}_{p_i})] = 2$ for each i, or there is a prime p with $[\Gamma_{p,0} : \Sigma^{\#}(L \otimes \mathbb{Z}_p)] = 4$; all other primes q are such that $\Sigma^{\#}(L \otimes \mathbb{Z}_q) = \Gamma_{q,0}$, and hence for these q we have $\Sigma_0^{\#}(L \otimes \mathbb{Z}_q) = \Gamma_0$. Note that by Theorems VII.12.1-VII.12.4, we have that $\Sigma_0^{\#}(L \otimes \mathbb{Z}_{p_i})$ has order at least 2 for each i.

Hence in the first case with the two primes, in order that $\Sigma_0^{\#}(L) = \{(1,1)\}$ we must have that these groups $\Sigma_0^{\#}(L \otimes \mathbb{Z}_{p_i})$ have order exactly 2 with the two groups being distinct; this is (3). In the second case, $\Sigma_0^{\#}(L) = \Sigma_0^{\#}(L \otimes \mathbb{Z}_p)$ so we must have $\Sigma_0^{\#}(L \otimes \mathbb{Z}_p) = \{(1,1)\}$, i.e., L is p-pseudoregular and we have case (4). Q.E.D.

In order to make Theorem 7.5 effective, we need explicit descriptions of the p-regular, p-semiregular and p-pseudoregular forms. We give these descriptions below; as they follow directly from Theorems VII.12.1-VII.12.4 we omit the proofs.

LEMMA 7.6. *Let L be an integral quadratic form, let p be an odd prime, and let $\delta = \operatorname{disc}(L)/\operatorname{disc}(q_{L\otimes\mathbb{Z}_p})$.*

(1) *L is p-regular if and only if $\operatorname{rk}(L) \geq \ell(q_{L\otimes\mathbb{Z}_p}) + 2$.*
(2) *L is p-semiregular if and only if $\operatorname{rk}(L) \geq \ell(q_{L\otimes\mathbb{Z}_p}) + 1$ and either*
   (a) *$p \equiv 3 \mod 4$, or*
   (b) *$p \equiv 1 \mod 4$ and $\chi(\delta) \neq (-1)^{\frac{p^2-1}{8}}$ where $\chi(v) = (\frac{v}{p}) = \pm 1$ is the Legendre symbol mod p.*

   In case (a), the type is $(-1, (-1)^{\frac{p^2-1}{8}}\chi(\delta))$, while in case (b), the type is $(1,-1)$.
(3) *L is p-pseudoregular if and only if $\operatorname{rk}(L) = \ell(q_{L\otimes\mathbb{Z}_p})$ and $p \equiv 3 \mod 4$.*
(4) *L is p-nonregular if and only if $p \equiv 1 \mod 4$ and either*
   (a) *$\operatorname{rk}(L) = \ell(q_{L\otimes\mathbb{Z}_p})$; or*
   (b) *$\operatorname{rk}(L) = \ell(q_{L\otimes\mathbb{Z}_p}) + 1$ and $\chi(\delta) = (-1)^{\frac{p^2-1}{8}}$.*

LEMMA 7.7. *Let L be an integral quadratic form, and write $q_{L\otimes\mathbb{Z}_2}$ in partial normal form as*

$$q_{L\otimes\mathbb{Z}_2} = q_1 \oplus q_2 \oplus q_3 \oplus q_4 \oplus q''$$

where

$$q_i = u_i^{N(i)} \oplus v_i^{e(i)} \oplus w(i)$$

for each $i = 1, 2, 3$ and scale $(q'') \geq 4$. Then:

(1) *If $\operatorname{rank}(L) > \ell(q_{L\otimes\mathbb{Z}_2})$ then L is 2-regular.*
(2) *If $\operatorname{rank}(L) = \ell(q_{L\otimes\mathbb{Z}_2})$ and $N(1) + e(1) > 0$ then*
   (a) *if $\ell(w(1)) > 0$ then L is 2-regular;*
   (b) *if $\ell(w(1)) = 0$ then L is 2-semiregular of type $(1,-1)$.*
(3) *If $\operatorname{rank}(L) = \ell(q_{L\otimes\mathbb{Z}_2})$, $N(1) + e(1) = 0$, and $\ell(w(1)) = 2$ then if we write $q_1 = w_{2,1}^{\varepsilon} \oplus w_{2,1}^{\phi}$, we have:*
   (a) *if $\varepsilon\phi = 3 \mod 4$ then L is 2-regular;*

(b) *if* $\varepsilon\phi = 1 \mod 4$ *and* $\ell(w(2)) > 0$ *then* L *is* 2*-regular;*
(c) *if* $\varepsilon\phi = 1 \mod 4$ *and* $\ell(w(2)) = 0$ *then* L *is* 2*-semiregular, of type* $(-1,1)$ *if* $\varepsilon = \phi = 1 \mod 4$ *and of type* $(-1,-1)$ *if* $\varepsilon = \phi = 3 \mod 4$.

(4) *If* $\operatorname{rank}(L) = \ell(q_{L\otimes\mathbb{Z}_2})$, $N(1) + e(1) = 0$, *and* $\ell(w(1)) = 1$ *then if we write* $q_1 = w_{2,1}^{\varepsilon}$ *and define* $\delta = \chi(\operatorname{disc}(L))/\operatorname{disc}_8(q_2 \oplus q_3 \oplus q'')$, *then the* 2*-regularity of* L *is determined by the following table:*

$N(2)+e(2)$ $+\ell(w(3))$	$w(2)$	$\delta \mod 8$	2*-regularity*
>0	$\neq 0$		*regular*
>0	0	1,5	*semi-, type* $(-1,1)$
>0	0	3,7	*semi-, type* $(-1,-1)$
0	*length* 2		*regular*
0	$w_{2,2}^{\phi}$, $\varepsilon\phi = 3 \mod 4$	1,7	*non-*
0	$w_{2,2}^{\phi}$, $\varepsilon\phi = 3 \mod 4$	3,5	*semi-, type* $(1,-1)$
0	$w_{2,2}^{\phi}$, $\varepsilon\phi = 1 \mod 4$	1,3	*semi-, type* $(-1,1)$
0	$w_{2,2}^{\phi}$, $\varepsilon\phi = 1 \mod 4$	5,7	*semi-, type* $(-1,-1)$
0	0	1,7	*non-*
0	0	3,5	*pseudo-*

(5) $\operatorname{rank}(L) = \ell(q_{L\otimes\mathbb{Z}_2})$, $q_1 = 0$, *and* $N(2) + e(2) > 0$ *then* L *is* 2*-pseudoregular;*
(6) $\operatorname{rank}(L) = \ell(q_{L\otimes\mathbb{Z}_2})$, $q_1 = 0$, $N(2) + e(2) = 0$, *and* $\ell(w(2)) = 2$ *then* L *is* 2*-pseudoregular;*
(7) $\operatorname{rank}(L) = \ell(q_{L\otimes\mathbb{Z}_2})$, $q_1 = 0$, $N(2) + e(2) = 0$, *and* $\ell(w(2)) \leq 1$ *then* L *is* 2*-nonregular.*

COROLLARY 7.8. *Let* L *be an indefinite integral quadratic form such that* $r = \operatorname{rank}(L) \geq 3$. *Write*

$$G_L = \mathbb{Z}/d_1\mathbb{Z} \oplus \cdots \oplus \mathbb{Z}/d_r\mathbb{Z}$$

with $d_i \geq 1$ *and* $d_i | d_{i+1}$. *Suppose that one of the following holds:*

(1) *For some prime* $p \equiv 3 \mod 4$, $d_2 = p^k$ *(with* $k \geq 0$*).*
(2) *For some prime* $p \equiv 3 \mod 4$, $d_1 = 2, d_2 = 2p^k$ *(with* $k \geq 0$*), and* $d_3 \equiv 2 \mod 4$.
(3) $d_1 = d_2 = 2$.
(4) $d_1 = 2$, $d_2 = 4$, *and* $d_3 \equiv 4 \mod 8$.
(5) $d_1 = d_2 = 4$.

Then L *is uniquely determined by its signature and discriminant-form, and the map* $\mathcal{O}(L) \to \mathcal{O}(G_L)$ *is surjective.*

PROOF. We check that the hypotheses of Theorem 7.5 holds in each case. Write $q_{L\otimes\mathbb{Z}_2}$ in partial normal form, as in Lemma 7.7.

In case (1), for all primes $\ell \neq p$, we have $\mathrm{rk}(L) - \mathrm{rk}(q_{L\otimes\mathbb{Z}_\ell}) \geq 2$ so that L is ℓ-regular by Lemma 7.6(1). If $k = 0$, then L is also p-regular, and we have hypothesis (1) of Theorem 7.5. Since $d_1 \div d_2$, also $d_1 = p^m$ for some $m \leq k$. If $m = 0$ and $k \geq 1$, then since $p \equiv 3 \mod 4$ and $\mathrm{rk}(L) = \mathrm{rk}(q_{L\otimes\mathbb{Z}_p}) + 1$, we have that L is p-semiregular by Lemma 7.6(2)(a); therefore hypothesis (2) of Theorem 7.5 holds. If $m \geq 1$ then $\mathrm{rk}(L) = \mathrm{rk}(q_{L\otimes\mathbb{Z}_p})$ so that L is p-pseudoregular by Lemma 7.6(3), and we have hypothesis (4) of Theorem 7.5.

In case (2), L is ℓ-regular for all $\ell \neq 2, p$. In addition, $\mathrm{rk}(L) - \ell(q_{L\otimes\mathbb{Z}_p}) \geq 1$ and $p \equiv 3 \mod 4$ so that L is either p-regular (if $k = 0$), or p-semiregular of type $(-1, \pm 1)$, by Lemma 7.6(2). Also note that since $d_1 = 2$, $\mathrm{rk}(L) = \ell(q_{L\otimes\mathbb{Z}_2})$. Finally, since $d_3 = equiv2 \mod 4$, we have $\ell(u_1^{N(1)} \oplus v_1^{e(1)} \oplus w(1)) \geq 3$; this forces $N(1) + e(1) > 0$, so that L is either 2-regular, or 2-semiregular of type $(1, -1)$ by Lemma 7.7(2). Thus, hypothesis (1), (2) or (3) of Theorem 7.5 applies.

In cases (3), (4) and (5), L is ℓ-regular for all $\ell \neq 2$. Moreover $\mathrm{rk}(L) = \ell(q_{L\otimes\mathbb{Z}_2})$ in these cases. We may assume in case (3) that $4|d_3$ (otherwise case (2) applies). It is then easy to see that the following are the only possibilities for the invariants of $q_{L\otimes\mathbb{Z}_2}$:

Case	$N(1)+e(1)$	$\ell(w(1))$	$\ell(w(2))$	$N(2)+e(2)$
(3)	1			
	0	2		
(4)	0	1	2	
			≤ 1	> 0
(5)	0	0	2	
			≤ 1	> 0

We see that in case (3), Lemma 7.7(2)-(3) applies and we may conclude that L is 2-regular or 2-semiregular. In case (4), Lemma 7.7(4) applies, in particular we have the hypotheses of one of the first four rows of the table there; again we see that L is either 2-regular or 2-semiregular. Finally in case (5) we use Lemma 7.7(5)-(6) to conclude that L is 2-pseudoregular.

Therefore in any of the cases (3), (4), or (5) we conclude that L is ℓ-regular for all $\ell \neq 2$, and is either 2-regular, 2-semiregular, or 2-pseudoregular, so that part (1), (2) or (4) of Theorem 7.5 applies. Q.E.D.

8. Bibliographical Note for Chapter VIII

The use of the strong approximation theorem to compute the genus group goes back to [**Eichler 52**] and [**Kneser 56**]. Theorem 3.1 and Corollary 3.2 are essentially due to them, although they did not have sufficient techniques to compute $\Gamma_{\mathbb{A}}/\Gamma_{\mathbb{Q}} \cdot \Sigma(L)$ in all cases; these were provided by Earnest and Hsia [**E-H 75**].

The use of the same techniques to study the map $\mathcal{O}(L) \to \mathcal{O}(G_L)$ was begun in [**Nikulin 80a**] and refined in [**Nikulin 80b**]. Theorem 5.1 is essentially contained in these papers, although again, the group $\Sigma(L)/(\Gamma_{\mathbb{Q}} \cap \Sigma(L)) \cdot \Sigma^{\#}(L)$ could not be computed in all cases at that time. Nikulin in [**Nikulin 80b**] gave sufficient conditions for the simultaneous uniqueness of L and surjectivity of $\mathcal{O}(L) \to \mathcal{O}(G_L)$ which, although more restrictive than those in Theorem 7.5, do imply Corollary 7.8. The discussion of computational techniques in Section 6 is modelled on [**Cassels 78**, Section 3 of Chapter 11].

Milnor's Theorem (4.3) was first proved in [**Milnor 58**]. The characterization of stable equivalence classes (Theorem 4.5) was first proved by Durfee [**Durfee 71**] along the lines of the proof given here. A more elementary proof was given in [**Wall 72**], and a simplification of Wall's proof, due to Kneser, is presented in [**Durfee 77**].

List of Notation

Notation	Section	Description
$(L, \langle -, - \rangle)$	I.1	F-valued symmetric bilinear form over R
Ad	I.1	the adjoint map from L to $\mathrm{Hom}_R(L, F)$
$\mathrm{Ker}\langle\ ,\ \rangle$	I.1	the kernel of Ad
$\bar{L}$	I.1	$L/\mathrm{Ker}\langle\ ,\ \rangle$
(L, Q)	I.2	F-valued quadratic form over R
Ad_Q	I.2	the adjoint map to the associated bilinear form
$\mathrm{Ker}(Q)$	I.2	the kernel of the associated bilinear form
$\mathrm{Rad}_q(L, Q)$	I.2	the q-radical of Q, $= \{x \in \mathrm{Ker}(L, Q) \mid Q(x) = 0\}$
$\bar{\bar{L}}$	I.2	$L/\mathrm{Rad}_q(L)$
$\mathbb{Z}$	I.2	the integers
$\mathbb{Z}_p$	I.2	the p-adic integers
$R^\times$	I.3	the group of units of a ring R
$\mathrm{disc}(Q)$	I.3	the discriminant of a quadratic R-module
$\mathcal{D}(R)$	I.3	$R^\times/(R^\times)^2$
$\mathbb{Q})$	I.3	the rationals
$\mathbb{R})$	I.3	the reals
$\mathbb{C})$	I.3	the complexes
$\mathbb{Q}_p$	I.3	the p-adic rationals
$\mathbb{Z}/n$	I.3	the ring of integers modulo n
$\mathbb{U}_{\text{ı}}$	I.3	the units $\mathbb{Z}_p^\times$ of $\mathbb{Z}_p$
χ	I.3	isomorphisms from $\mathcal{D}(R)$ to standard groups
$\left(\frac{u}{p}\right)$	I.3	the Legendre symbol
$G^\#$	I.4	the dual of a torsion R-module G: $\mathrm{Hom}_R(G, K/R)$
P.I.D.	I.4	principal ideal domain
$\mathbb{Q}^{(p)}$	I.4	rationals with denominator a power of p
$L_1 \oplus L_2$	I.5	direct sum of quadratic forms
$X^\perp$	I.5	perpendicular module
$\cong$	I.6	isomorphism
$\sim_S$	I.6	stable isomorphism
$\langle a \rangle_R$	I.7	quadratic R-module of rank 1
$\mathbf{1}_R$	I.7	R with squaring as the quadratic form
$\langle a \rangle$	I.7	$\langle a \rangle_{\mathbb{Z}}$

$W_{p,k}^{\varepsilon}$	I.7	rank one form over $\mathbb{Z}_p$
U_R	I.7	the hyperbolic plane over R
A_N	I.7	integral rank N form defined by path graph
$D_N, N \geq 4$	I.7	integral rank N form defined by D_N Dynkin diagram
$E_N, N \geq 6$	I.7	integral rank N form defined by E_N Dynkin diagram
T_{pqr}	I.7	integral form defined by graph with single cubic vertex
$\widetilde{A}_N$	I.7	rank $N+1$ form defined by cycle graph
$\widetilde{D}_N, N \geq 4$	I.7	rank $N+1$ form defined by extended D_N Dynkin Diagram
$\widetilde{E}_N, N = 6, 7, 8$	I.7	rank $N+1$ form defined by extended E_N Dynkin diagram
U_k	I.7	indecomposable rank 2 form over $\mathbb{Z}_2$
V_k	I.7	indecomposable rank 2 form over $\mathbb{Z}_2$
$\bar{z}_{\ell}^{a}$	I.7	bilinear form on $\mathbb{Z}/\ell$
$\bar{w}_{p,k}^{\varepsilon}$	I.7	bilinear form on $\mathbb{Z}/p^k$
z_{ℓ}^{a}	I.7	quadratic form on $\mathbb{Z}/\ell$
$w_{p,k}^{\varepsilon}$	I.7	quadratic form on $\mathbb{Z}/p^k$
u_k	I.7	quadratic form on $\mathbb{Z}/2^k \times \mathbb{Z}/2^k$
v_k	I.7	quadratic form on $\mathbb{Z}/2^k \times \mathbb{Z}/2^k$
$\bar{u}_k$	I.7	bilinear form on $\mathbb{Z}/2^k \times \mathbb{Z}/2^k$
$\bar{v}_k$	I.7	bilinear form on $\mathbb{Z}/2^k \times \mathbb{Z}/2^k$
$-L$	I.7	negative of quadratic form L
(s_+, s_-)	I.7	signature of a real quadratic vector space
$A(r)$	I.7	expansion of the form A by the element r
(L_S, Q_S)	I.8	change of rings to S
L_p	I.8	change of rings to $\mathbb{Z}_p$
$\mathcal{O}(L, Q)$	I.9	the orthogonal group of (L, Q)
det	I.9	the determinant of an isometry
$\{+, -\}$	I.9	2-element value group for determinants of isometries
$\mathcal{O}^+(L)$	I.9	the kernel of det
τ_x	I.9	reflection
spin	I.10	the spinor norm
$\mathcal{O}_{++}(V)$	I.10	the kernel of $(\det, \text{spin})$
$\mathcal{O}_{+-}(V)$	I.10	the kernel of det
$\mathcal{O}_{-+}(V)$	I.10	the kernel of spin
$\mathcal{O}_{--}(V)$	I.10	the kernel of $\det \cdot \text{spin}$)
$\mathcal{O}_{\alpha\beta}(L)$	I.10	$\mathcal{O}(L) \cap \mathcal{O}_{\alpha\beta}(L \otimes_{\mathbb{Z}} \mathbb{R})$
GR^+	I.11	$\{r_+$-dimensional oriented subspace $W \subset V \,\vert\, Q\vert_W$ is positive defin
GR^-	I.11	$\{r_+$-dimensional oriented subspace $W \subset V \,\vert\, Q\vert_W$ is positive defin
$\ell(G)$	II.1	length of a f.g. module over a P.I.D.
Δ	II.1	the order of G, the product of the invariants
G_p	II.1	$\{x \in G \,\vert\, p^k x = 0$ for some $k \geq 0\}$
G^*	II.1	the dual module $\mathrm{Hom}_R(G, K/R)$

$G_{p,k}$	II.2	$\{x \in G \mid p^k x = 0\}$
$\rho_{p,k}(G)$	II.2	$G_{p,k}/(G_{p,k-1} + pG_{p,k+1})$
$\langle -,- \rangle_k$	II.2	bilinear form on $\rho_k(G)$
$\mathrm{disc}(G, \langle -,- \rangle)$	II.3	the discriminant of a torsion bilinear form
$\mathrm{disc}(G, q)$	II.4	the discriminant of a torsion quadratic form
G'	II.5	$G/G_{2,1}$
$\tau(G, \langle -,- \rangle)$	II.5	torsion quadratic form on G' for special G
$\mathrm{disc}_8(G, \langle -,- \rangle)$	II.6	the mod 8 discriminant of better extraspecial G
$\mathrm{disc}_8(G', q')$	II.6	the mod 8 discriminant of good special quadratic form
$L^\#$	II.7	dual lattice to L
L^*	II.7	R-dual $\mathrm{Hom}_R(L, R)$ to a lattice L
G_L	II.7	the discriminant-form module $L^\#/L$
q_L	II.7	torsion quadratic form on G_L
$\langle -,- \rangle_{G_L}$	II.7	bilinear form on G_L
$\mathcal{O}^\#(L)$	II.8	the kernel of $\mathcal{O}(L) \to \mathcal{O}(G_L)$
H_A	II.8	$\{C \in \mathcal{M}_{N\times N}(R) \mid C + C^\top + C^\top AC = 0\}$
γ_G	III.1	the Gauss sum invariant from $\mathrm{Hom}_{\mathbb{Z}}(\mathbb{Q}/\mathbb{Z}, \mathbb{Q}/\mathbb{Z})$ to $\mathbb{C}$
φ_N	III.1	multiplication by N on $\mathbb{Q}/\mathbb{Z}$
$\gamma_G(N)$	III.1	$\gamma_G(\varphi_N)$
$S(a, \ell)$	III.2	the Gauss sum
γ_L	III.4	Gauss invariant of integral form on L $(= \gamma_{G_L})$
$\rho(\ell)$	IV.1	$\sum_{j\le\ell} j \cdot r_j + \sum_{j>\ell} \ell \cdot r_j$
$\sigma_\ell(G)$	IV.1	the ℓ^{th} signature invariant of G
$\mathcal{Q}$	IV.1	isom. classes of nondeg. quadratic $\mathbb{Z}_{\text{ı}}$-modules
$\mathcal{T}^{\surd}$	IV.1	isom. classes of nondegenerate torsion quadratic forms over $\mathbb{Z}_{\text{ı}}$
$\mathcal{G}^{\surd}$	IV.1	isom. classes of good special nondegenerate torsion quadratic for
$\mathcal{I}_p^{\surd}$	IV.1	isom. classes of inner product $\mathbb{Z}_{\text{ı}}$-modules
$d : \mathcal{Q}_p \to \mathcal{T}_p$	IV.2	discriminant-form map
$G(k)$	IV.4	homogenous part of scale 2^k in a partial normal form
$w(k)$	IV.4	$w^\varepsilon_{2,k}$ part of $G(k)$
$x(k)$	IV.4	v_k and $w(k)$ part of $G(k)$
$d_2 : \mathcal{Q}_2 \to \mathcal{G}_2$	IV.5	expanded discriminant-form map
$(a, b)_p$	V.2	Hilbert Norm Residue Symbol
$c_p(V, Q)$	V.2	Hasse invariant
$\Theta(L)$	V.7	the kernel of $(\det, \mathrm{spin})$
$\mathcal{Q}$	VI.1	isom. classes of integral quadratic forms
$\mathcal{T}$	VI.1	isom. classes of torsion quadratic forms over $\mathbb{Z}$
$\mathcal{O}^{\mathrm{ref}}(L)$	VII.2	subgroup of $\mathcal{O}(L)$ generated by reflections
$\mathcal{O}^{\#,\mathrm{ref}}(L)$	VII.2	subgroup of $\mathcal{O}^\#(L)$ generated by reflections
$\mathrm{scale}(L)$	VII.2	scale of an inner product $\mathbb{Z}_p$-module

E_y^x	VII.3	generalized Eichler isometry
$\Sigma(L)$	VII.4	image of $(\det, \mathrm{spin})$ on $\mathcal{O}(L)$
$\Sigma^{\#}(L)$	VII.4	image of $(\det, \mathrm{spin})$ on $\mathcal{O}^{\#}(L)$
$\Gamma_{p,k}$	VII.4	subgroups of $\{\pm 1\} \times \mathbb{Q}_p^\times/(\mathbb{Q}_p^\times)^2$
${}^kE_y^x$	VII.7	rescaled Eichler isometry
$\Sigma^+(L)$	VII.8	$\{(d,s) \in \Sigma(L) \mid d = 1\}$
$\Sigma^{++}(L)$	VII.8	$\{(d,s) \in \Sigma(L) \mid d = 1, s \in \mathbb{U}_p\}$
$\Sigma^{\#,+}(L)$	VII.10	$\{(d,s) \in \Sigma^{\#}(L) \mid d = 1\}$
Γ_p	VII.12	$\{\pm 1\} \times \mathbb{Q}_p^\times/(\mathbb{Q}_p^\times)^2$
Γ_p^+	VII.12	$\{(d,s) \in \Gamma_p \mid d = 1\}$
Γ_p^{++}	VII.12	$\{(d,s) \in \Gamma_p^+ \mid s \in \mathbb{U}_p\}$
Γ_0	VII.12	$\{\pm 1\} \times \{\pm 1\}$
φ_p	VII.12	natural map from Γ_0 to $\Gamma_{p,0}$
$\Sigma_0^{\#}(L)$	VII.12	$\varphi_p^{-1}(\Sigma^{\#}(L))$
$\mathcal{O}(L_{\mathbb{A}})$	VIII.1	adelic construction for orthogonal groups
$\{\sigma_p\}(L)$	VIII.1	integral quadratic form defined by $\{\sigma_p\} \in \mathcal{O}(L_{\mathbb{A}})$
$G_{\{\sigma_p\}}$	VIII.1	isomorphism $G_{\{\sigma_p\}(L)} \to G_L$
$\Gamma_{\mathbb{A}}$	VIII.2	adelic construction for Γ_p groups
$\Gamma_{\mathbb{A},0}$	VIII.2	subgroup of $\Gamma_{\mathbb{A}}$
$\Theta(L_{\mathbb{A}})$	VIII.2	kernel of $(\det, \mathit{spin}) : \mathcal{O}(L_{\mathbb{A}}) \to \Gamma_{\mathbb{A}}$
$\Sigma^{\#}(L)$	VIII.2	$\prod_p \Sigma^{\#}(L \otimes \mathbb{Z}_p)$
$\Gamma_{\mathbb{Q}}$	VIII.2	$\{\pm 1\} \times \mathbb{Q}^\times/(\mathbb{Q}^\times)^2$
$\Sigma(L)$	VIII.3	$\prod_p \Sigma(L \otimes \mathbb{Z}_p)$
$g(L)$	VIII.3	genus group of the integral quadratic form L
Γ_S	VIII.6	$\{(d,s) \in \Gamma_{\mathbb{Q}} \mid s \text{ divides } 2\,\mathrm{disc}(L)\}$
Γ_T	VIII.6	$\{(d,s) \in \Gamma_{\mathbb{Q}} \mid (s, 2\,\mathrm{disc}(L)) = 1\}$
$\Sigma_0^{\#}(L)$	VIII.7	$\Sigma^{\#}(L) \cap \Gamma_0$

Bibliography

[B-S 66] Z. I. Borevich and I. R. Shafarevich. *Number Theory.* Academic Press, New York, San Francisco, and London (1966).

[Cassels 78] J.W.S. Cassels. *Rational Quadratic Forms.* London Mathematical Society Monographs No. 13, Academic Press London, New York, and San Francisco (1978).

[Durfee 71] A. H. Durfee: *Diffeomorphism classes of isolated hypersurface singularities.* Ph.D. Thesis, Cornell University (1971).

[Durfee 77] A.H. Durfee: "Bilinear and quadratic forms on torsion modules". *Advances in Math.***25** (1977), 133–164.

[E-H 75] A. G. Earnest and J. S. Hsia: Spinor norms of local integral rotations, II. *Pacific J. Math.* **61** (1975), 71–86.

[Eichler 52] M. Eichler: *Quadratische Formen und orthogonale Gruppen.* Springer-Verlag, Berlin Heidelberg, New York (1952).

[Kneser 56] M. Kneser: "Klassenzahlen indefiniter quadratischer Formen in drei order mehr Veränderlichen". *Arch. Math.* **7** (1956), 323–332.

[Lam 73] T.Y. Lam. *The Algebraic Theory of Quadratic Forms.* W. A. Benjamin, Inc., Reading, Massachusetts (1973).

[Milnor 58] J. Milnor: "On simply connected 4-manifolds". *Symposium Internacional de Topologia Algebraica*, La Universidad Nacional Autónoma de México y la UNESCO (1958), 122–128.

[Nikulin 80a] V.V. Nikulin. "Finite Automorphism Groups of Kähler K3 Surfaces". *Trans. Moscow Math. Soc.*, **38** Issue 2 (1980), 71-135.

[Nikulin 80b] V. V. Nikulin: "Integral Symmetric Bilinear Forms and some of their Applications". Math. USSR Izvestija, Vol. 14, No. 1 (1980), 103-167.

[O'Meara 63] O. T. O'Meara: *Introduction to Quadratic Forms.* Die Grundlehren der Mathematischen Wissenschaften in Einzeldarstellungen, Vol. 117, Springer-Verlag 1963.

[O-P65] O. T. O'Meara and B. Pollak: "Generation of local integral orthogonal groups". *Math. Zeit.* **87** (1965), 385–400.

[Serre 73] J.-P. Serre. *A Course in Arithmetic.* Graduate Texts in Mathematics No. 7, Springer-Verlag 1978.

[Wall 63] C. T. C. Wall: "Quadratic forms on finite groups, and related topics". *Topology* **2** (1963), 281–298.

[Wall 72] C. T. C. Wall: "Quadratic Forms on Finite Groups II", *Bull. London Math. Soc.*, Vol. 4 (1972), 156-160.

[Zassenhaus62] H. Zassenhaus: "On the spinor norm". *Arch. Math.* **13** (1962), 434–451.