# Contents

# 0. Foreword

These are notes for a course (Spezialvorlesung) on quadratic forms held at Heidelberg University in the summer semester of 2025.

The main reference throughout these notes is the book *Quadratische Formen* (in German!) by Martin Kneser, in the second edition edited in collaboration with Winfried Scharlau, which I loosely followed.

I also drew material from the *Introduction to Quadratic Forms over Fields* by T.Y. Lam, from *Symmetric bilinear forms* by Milnor and Husemoller, from *Arithmetic of Quadratic Forms* by Y. Kitaoka, and from *Sphere packings, lattices and groups* by Conway, Sloane and other authors. Other references are indicated by footnotes.

# 1. Basics

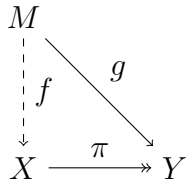
## 1.1. Bilinear forms

We begin not by studying quadratic forms but the closely related bilinear forms. This section is mostly meant to fix definitions and notation.

Let $R$ be an integral domain with 1. From now on, this is always assumed when we say $R$ is a ring. Our $R$-modules will almost always be finitely generated projective $R$-modules. Recall that a (finitely generated) $R$-module $M$ is **projective** if any of the following equivalent definitions is true:

(1) There is another $R$-module $N$ such that the direct sum $F = M \oplus N$ is (finitely generated and) free;

(2) For any surjective homomorphism $\pi : X \twoheadrightarrow Y$ of $R$-modules, any homomorphism $g : M \to Y$ can be pulled back to a homomorphism $f : M \to X$ for which $\pi \circ f = g$. In pictures, we have the commutative diagram




(3) For any system of generators $e_1, ..., e_n$, there are linear functionals $e_1^*, ..., e_n^* : M \to R$ such that each $x \in M$ can be written as the linear combination

$$x = \sum_{i=1}^{n} e_i^*(x) e_i.$$

(The $e_i^*$ might not be unique!) This setup is usually called a *dual basis* even though $e_1, ..., e_n$ is not necessarily a basis of $M$ at all.

(4) All localizations of $M$ are (finitely generated) free modules. (This is ultimately the reason for working with projective modules.)

**Definition 1.1.** A **bilinear form** on $M$ is a function

$$\beta : M \times M \longrightarrow R$$

that satisfies

$$\beta(ax_1 + bx_2, y_i) = a\beta(x_1, y_i) + b\beta(x_2, y_i);$$
$$\beta(x_i, ay_1 + by_2) = a\beta(x_i, y_1) + b\beta(x_i, y_2);$$

for any $x_1, x_2, y_1, y_2 \in M$ and $a, b \in R$.

As long as there is no risk of confusion, we will often use the notation

$$x \cdot y = \beta(x, y).$$

The space of bilinear forms on $M$ is itself an $R$-module with the natural notion of addition and multiplication by $R$. We denote it by $\mathrm{Bil}(M)$.

A bilinear form induces a homomorphism of $R$-modules

$$\begin{aligned} b &: M \longrightarrow M^* := \mathrm{Hom}_R(M, R), \\ b(x)(y) &:= \beta(x, y) \quad (x, y \in M). \end{aligned} \tag{1.1}$$

from $M$ into its dual. Conversely, any such homomorphism corresponds to a bilinear form $\beta$.

We call $\beta$ **non-degenerate** if $b$ is injective and **regular** if $b$ is bijective and $M$ is finitely generated projective. (These definitions are mainly used when $\beta$ is symmetric or skew-symmetric; see below.) These notions are equivalent over fields but not over general rings.

Given $\beta \in \mathrm{Bil}(M)$, define the bilinear form

$$\beta^*(x, y) := \beta(y, x).$$

**Definition 1.2.** (i) $\beta$ is **symmetric** if $\beta = \beta^*$.
(ii) $\beta$ is **skew-symmetric** if $\beta = -\beta^*$.
(iii) $\beta$ is **alternating** if $\beta(x, x) = 0$ for every $x \in M$.

An alternating bilinear form is skew-symmetric due to the calculation

$$0 = (x + y) \cdot (x + y) - x \cdot x - y \cdot y = y \cdot x + x \cdot y.$$

In the other direction, setting $x = y$ in $x \cdot y = -y \cdot x$ implies

$$2 \cdot \beta(x, x) = 0,$$

which **if** $\mathrm{char}(R) \neq 2$ (!) implies that $\beta$ is alternating. When $\mathrm{char}(R) = 2$, alternating is a stronger condition than skew-symmetric.

Usually our bilinear forms will be symmetric.

Now consider the case of the free module $M$, and let $\beta$ be a symmetric bilinear form. With respect to any basis $e_1, ..., e_n$, the form $\beta$ is represented by the matrix

$$B = (e_i \cdot e_j)_{i,j=1}^n$$

in the sense that if $x = \sum_i x_i e_i$ and $y = \sum_i y_i e_i \in M$ are identified with the column vectors $(x_i)_i$, $(y_i)_i \in R^n$, then

$$x \cdot y = x^T B y.$$

This shows that $\beta$ is nondegenerate if and only if $B$ is injective as a matrix map (equivalently, if $\det(B) \neq 0$) and that $\beta$ is regular if and only if $\det(B) \in R^\times$. Note however that different bases yield different matrix determinants. In a different basis

$$e'_j = \sum_{i=1}^n a_{ij} e_i$$

with the matrix $A = (a_{ij})_{i,j=1}^n \in \mathrm{GL}_n(R)$, the form $\beta$ is represented by the matrix

$$B' = A^T B A.$$

Therefore

$$\det(B') = \det(B) \cdot \det(A)^2 \in \det(B) \cdot (R^\times)^2.$$

So the following notion is well-defined:

**Definition 1.3.** Let $(M, \beta)$ be a free $R$-module of finite rank with symmetric bilinear form. The **discriminant** of $\beta$ is the coset

$$\mathrm{disc}(\beta) = \det(B) \cdot (R^\times)^2 \in R/(R^\times)^2$$

modulo squares of units, where $B$ is any representation matrix for $\beta$.

**Example 1.4.** Let $R = \mathbb{Z}$. Then $(\mathbb{Z}^\times)^2 = \{1\}$ and $\mathbb{Z}/(\mathbb{Z}^\times)^2 = \mathbb{Z}$, so the discriminant of a symmetric bilinear form is just an integer.
The **hyperbolic plane** $H$ is the $\mathbb{Z}$-module $\mathbb{Z}^2$ with bilinear form

$$\beta\Big( \begin{pmatrix} a \\ b \end{pmatrix}, \begin{pmatrix} c \\ d \end{pmatrix} \Big) = ad + bc.$$

Its discriminant is $-1$.

In order to connect symmetric bilinear forms and quadratic forms (which we will do later), we need the following definition.

**Definition 1.5.** A bilinear form $\beta$ is called **even** if there is a bilinear form $\gamma$ such that

$$\beta = \gamma + \gamma^*.$$

The bilinear form $\gamma$ is unique modulo adding skew-symmetric forms. ($\gamma$ is generally a bilinear form that is not symmetric!) This leads to an isomorphism of $R$-modules:

$$\mathrm{Bil}^{\mathrm{even}}(M) \cong \mathrm{Bil}(M)/\mathrm{Bil}^{\mathrm{skew}}(M), \quad \beta \mapsto [\gamma].$$

Whether a bilinear form $\beta$ is even can be read off of the values $\beta(x,x)$:

**Lemma 1.6.** *Let $(M,\beta)$ be a finitely generated projective $R$-module together with a symmetric bilinear form. The following are equivalent:*
*(i) $\beta$ is even;*
*(ii) $\beta(x,x) \in 2R$ for every $x \in M$.*

*Proof.* (i) $\Rightarrow$ (ii) $\beta = \gamma + \gamma^*$ implies

$$\beta(x,x) = 2 \cdot \gamma(x,x) \in 2R.$$

(ii) $\Rightarrow$ (i) $M$ appears as a direct summand in a free $R$-module: $F = M \oplus N$. The bilinear form $\beta$ can be trivially extended to all of $F$ by defining $\beta(x,y) = 0$ for $x \in F$ and $y \in N$, and if that extension is even then it follows immediately that $\beta$ itself is even. So we can assume without loss of generality that the module $M$ is free.

Suppose $e_1, ..., e_n$ is a basis of $M$ and define

$$\gamma(e_i, e_j) := \begin{cases} \beta(e_i,e_j): & i < j; \\ x_i: & i = j; \\ 0: & i > j; \end{cases}$$

where $x_i \in R$ is an arbitrary (but fixed) element such that $2x_i = \beta(e_i,e_i)$. Then $\gamma$ extends in a unique way to a bilinear form defined on all of $M$ and $\gamma + \gamma^* = \beta$ holds as one can check on any basis elements. □

Now we return to the general case. Let $M$ be a finitely generated projective $R$-module with a symmetric bilinear form $\beta$.

**Definition 1.7.** Two vectors $x, y \in M$ are **orthogonal** or perpindicular if $x \cdot y = 0$. In this case we write $x \perp y$.
Submodules $U, V \subseteq M$ are called **orthogonal**, written $U \perp V$, if $x \perp y$ for every $x \in U$ and $y \in V$.
The **orthogonal complement** of a submodule $U \subseteq M$ is

$$U^{\perp} = \{x \in M : \ x \cdot y = 0 \text{ for every } y \in U\}.$$

The **radical** of $\beta$ is the orthogonal complement of the entire module $M$:

$$\mathrm{rad}(\beta) = M^{\perp} = \{x \in M : \ x \cdot y = 0 \text{ for all } y \in M\} = \ker(b).$$

In particular, $\beta$ is nondegenerate if and only if its radical is zero.

Given two symmetric bilinear forms $(U, \beta_U)$ and $(V, \beta_V)$, the (external) orthogonal direct sum $U \perp V$ is $(U \oplus V, \beta)$, where for $(x_U, x_V), (y_U, y_V) \in U \oplus V$ we define

$$\beta((x_U, x_V), (y_U, y_V)) = \beta_U(x_U, y_U) + \beta_V(x_V, y_V).$$

The (external) orthogonal direct sum $\perp_{i=1}^{n} U_i$ of a family $(U_i, \beta_i)$ is defined similarly. However, we also write $M = U \perp V$ if $M$ is the (internal) direct sum of two submodules $U, V$ that are perpindicular to one another.

If $U \subseteq M$ is a submodule then we write $\beta|_U$ for the restricted bilinear form

$$\beta|_U : U \times U \longrightarrow R, \quad \beta|_U(x, y) := \beta(x, y).$$

(Note that submodules need not be projective in general. An integral domain for which all submodules of projectives remain projective is usually called a Dedekind ring. But direct summands in projectives are certainly always projective.)

**Definition 1.8.** Let $(M, \beta)$ be an $R$-module (finitely generated, projective) with a symmetric bilinear form.
(i) $x \in M$ is **isotropic** if $x \neq 0$ and $x \perp x$.
(ii) A submodule $U \subseteq M$ is **isotropic** if it contains an isotropic vector.
(iii) A submodule $U \subseteq M$ is **totally isotropic** if all of its elements (other than 0) are isotropic.

A degenerate module is always isotropic because any vector $x \in \mathrm{rad}(\beta)$ is orthogonal to itself. The converse is far from being true. For example, the hyperbolic plane (Example 1.4) is nondegenerate, even regular, but it contains the isotropic vectors $(a, 0)$ and $(0, b)$ for any $a, b \in \mathbb{Z}\backslash\{0\}$.

Let $b : M \to M^*$ be the module homomorphism $b(x)(y) = x \cdot y$. For a submodule $U \subseteq M$, define

$$b_U : M \longrightarrow U^*, \quad b_U(x)(y) := x \cdot y.$$

**Lemma 1.9.** *Let $U \subseteq M$ be a submodule. The following are equivalent:*
*(i) $M = U \perp U^{\perp}$;*
*(ii) $U$ is non-degenerate and $b_U(M) = b_U(U)$.*

*Proof.* (ii) is another way of saying that for every $x \in M$ there is a unique $y \in U$ such that $b_U(x) = b_U(y)$. The latter condition is equivalent to

$$x \cdot u = y \cdot u$$

for all $u \in U$, i.e. $x - y \in U^{\perp}$. □

**Corollary 1.10.** *Any regular submodule $U \subseteq M$ splits off as a direct summand: more precisely,*

$$M = U \perp U^{\perp}.$$

**Corollary 1.11.** *Let $(M, \beta)$ be an $R$-module (finitely generated, projective) with a symmetric bilinear form. For $u \in R^{\times}$, let $\langle u \rangle$ be $R$ itself as an $R$-module together with the symmetric bilinear form $\beta_u(x, y) = uxy$. Then $M$ has an orthogonal decomposition*

$$M = \langle u_1 \rangle \perp ... \perp \langle u_r \rangle \perp N,$$

*where $u_1, ..., u_r \in R^{\times}$ are units and $\beta(x, x) \notin R^{\times}$ for every $x \in N$.*

*Proof.* We use induction on the rank of $M$. If $M$ has rank 0 then $M = \{0\}$.

Suppose $\text{rank}(M) > 0$. If $\beta(x, x)$ is already a nonunit for every $x \in M$ then we have $N = M$. Otherwise, there exists $x_1 \in M$ with $\beta(x_1, x_1) = u_1 \in R^{\times}$. The submodule $\langle u_1 \rangle$ spanned by $R \cdot x_1$ is then regular and by Corollary 1.10 it splits off as a direct summand:

$$M = \langle u_1 \rangle \perp \langle u_1 \rangle^{\perp}.$$

Since $\langle u_1 \rangle^{\perp}$ has rank $\text{rank}(M) - 1$, it decomposes by the induction assumption. □

On the other hand, submodules $U \subseteq M$ can split off as direct summands without $M$ being of the form $U \perp U^{\perp}$. We borrow some terminology from Kneser:

**Definition 1.12.** (i) A submodule $U \subseteq M$ is called **primitive** if $M = U \oplus V$ for some other submodule $V$.
(ii) $U \subseteq M$ is called **sharply primitive** (scharf primitiv) if it is primitive and the map

$$b_U : M \longrightarrow U^*, \quad b_U(x)(y) = x \cdot y$$

is surjective.

We do not ask for a primitive submodule to split off as an *orthogonal* direct summand.

Note that a regular submodule is automatically sharply primitive, since in this case $b_U$ is already surjective from $U$ onto $U^*$.

We have the following important construction of regular modules:

**Definition 1.13.** Let $M$ be a finitely generated projective $R$-module. The **hyperbolic module** $H(M)$ is

$$H(M) := M \oplus M^*$$

equipped with the bilinear form $\beta$ defined by

$$\beta(x, \varphi) = \varphi(x), \quad x \in M,\ \varphi \in M^*$$

and by $\beta(x, y) = \beta(\varphi, \psi) = 0$ for $x, y \in M$ and $\varphi, \psi \in M^*$.

To see that $H(M)$ is regular, note that we can find another $R$-module $N$ such that $F = M \oplus N$ is finitely generated and free, and that

$$H(F) = H(M) \perp H(N).$$

The fact that $H(F)$ is regular is equivalent to the canonical map $F \to (F^*)^*$ being an isomorphism. As a direct summand in a regular module, $H(M)$ is also regular.

If we view $M$ as a totally isotropic module (i.e. endowed with the bilinear form which is identically zero), then $M \subseteq H(M)$ is a sharply primitive, but clearly not regular, submodule. The orthogonal complement of $M$ in $H(M)$ is exactly $M$ itself.

## 1.2. Quadratic forms

Let $R$ be an integral domain.

By definition, an $n$-ary quadratic form is just a polynomial that is homogeneous of degree two:

$$Q = \sum_{1 \le i \le j \le n} a_{ij} X_i X_j \in R[X_1, ..., X_n]. \tag{1.2}$$

For example,

$$Q(X, Y, Z) = X^2 + Y^2 + Z^2$$

is a ternary quadratic form.

It is often more natural to consider the function on $R^n$ induced by $Q$, namely

$$f_Q : R^n \longrightarrow R, \quad f_Q(x_1, ..., x_n) := \sum_{i \le j} a_{ij} x_i x_j.$$

This function can be thought of as attaching a "length" to vectors in $R^n$; for instance, if $R = \mathbb{R}$ and $Q$ is the ternary quadratic form above then $f_Q(x)$ is the square of the usual Euclidean length $\|x\|$. In general, the function $f_Q$ has the following properties:

**Lemma 1.14.** *(i) $f_Q(ax) = a^2 f_Q(x)$ for all $x \in R^n$ and $a \in R$;*
*(ii) The function*

$$\beta : R^n \times R^n \longrightarrow R, \quad \beta(x, y) := f_Q(x + y) - f_Q(x) - f_Q(y)$$

*is a symmetric bilinear form.*

The bilinear form $\beta$ is called the **polar** or **polarization** of $Q$.
Both properties are easy to check. If $e_1, ..., e_n$ is the natural basis of $R^n$ then the coefficients of 1.2 are recovered as $f_Q(e_i) = a_{ii}$ and $\beta(e_i, e_j) = a_{ij}$. Hence $f_Q$ uniquely determines the (polynomial) quadratic form $Q$ regardless of the ground field. We usually abuse notation and just write $Q = f_Q$.

Conditions (i),(ii) of Lemma 1.14 extend naturally to modules. For an $R$-module $M$, we define a **quadratic form** $Q : M \to R$ as a function satisfying

$$Q(ax) = a^2 Q(x), \quad x \in M,\ a \in R$$

for which $\beta(x, y) = Q(x + y) - Q(x) - Q(y)$ defines a bilinear form. (This is called the **polar** bilinear form attached to $Q$.)

**Definition 1.15.** (i) A **quadratic $R$-module** is a pair $(M, Q)$ where $M$ is a finitely generated projective $R$-module and $Q : M \to R$ is a function satisfying Lemma 1.14.
(ii) $(M, Q)$ is called a **quadratic space** if the polarization $\beta$ is nondegenerate.

Note that the form $\beta$ is always even, because

$$\beta(x, x) = Q(2x) - 2Q(x) = 2 \cdot Q(x) \in 2R.$$

Conversely, an even symmetric bilinear form $\beta$ uniquely determines a quadratic form *as long as the characteristic of $R$ is not two.* In this case we have $Q(x) = \frac{1}{2}\beta(x, x)$.
If $\mathrm{char}(R) = 2$ then this is no longer true:

**Example 1.16.** Let $R$ be a ring of characteristic 2. The binary quadratic form

$$H(X, Y) := XY$$

induces the bilinear form

$$\beta\Big( \begin{pmatrix} a \\ b \end{pmatrix}, \begin{pmatrix} c \\ d \end{pmatrix} \Big) = ad + bc.$$

The quadratic form

$$E(X, Y) := X^2 + XY + Y^2$$

induces the same bilinear form $\beta$.

This is because the bilinear form attached to the quadratic form $X^2$ is identically zero (by the "freshman's dream" identity $x^2 + y^2 = (x + y)^2$).

The simple observation above turns out to cause a great deal of difficulty.

However, since $\beta$ is even, by Lemma 1.6 there is a bilinear form $\gamma$, unique up to addition by skew-symmetric forms, such that $\beta = \gamma + \gamma^*$. The form $\gamma$ can be chosen such that $Q(x) = \gamma(x, x)$; under this condition, $\gamma$ is unique up to addition by *alternating forms*. Hence we have isomorphisms

$$\{\text{even symmetric bilinear forms}\} \cong \mathrm{Bil}(M)/\mathrm{Bil}^{\mathrm{skew}}(M);$$
$$\{\text{quadratic forms}\} \cong \mathrm{Bil}(M)/\mathrm{Bil}^{\mathrm{alt}}(M).$$

Finally, the *matrix* $B$ of a quadratic form $Q$ on $R^n$ is the matrix of its polar form with respect to the standard basis. Equivalently, this is the Hessian (or Gram) matrix of $Q$. In terms of the coefficients $a_{ij}$ of $Q$, the entries of $B$ are

$$B_{ij} = \begin{cases} 2a_{ii} : & i = j; \\ a_{ij} : & i < j; \\ a_{ji} : & j < i. \end{cases}$$

The matrix $B$ uniquely determines the polar form $\beta$; if $\mathrm{char}(R) \neq 2$, it also uniquely determines $Q$. The discriminant of $Q$ is defined as

$$\mathrm{disc}(Q) = \mathrm{disc}(\beta) = \det(B) \cdot (R^\times)^2.$$

**Example 1.17.** The quadratic form $Q = X^2 - XY + Y^2$ has matrix $B = \begin{pmatrix} 2 & -1 \\ -1 & 2 \end{pmatrix}$. As a quadratic form over $\mathbb{Z}$ its discriminant is 3.

To summarize the situation:

**Proposition 1.18.** *Let $M = R^n$. The following data are equivalent:*
*(i) A quadratic form $Q$ viewed as a homogeneous polynomial of degree two;*
*(ii) A quadratic form viewed as a function $Q : R^n \to R$ satisfying the constraints of Lemma 1.14;*
*(iii) The class $[\gamma]$ of a bilinear form modulo alternating forms with $\gamma(x, x) = Q(x)$.*

*If $\mathrm{char}(R) \neq 2$, these are also equivalent to any of the following:*
*(iv) An even symmetric bilinear form $\beta$, the polarization of $Q$;*
*(v) A symmetric matrix $B \in R^{n \times n}$ whose diagonal entries belong to $2R$;*
*(vi) The class $[\gamma]$ of a bilinear form modulo skew-symmetric forms with $\gamma(x, x) = Q(x)$.*

Usually we define properties or invariants of quadratic forms as the corresponding property or invariant of its polarization $\beta$, but there are a few exceptions (relevant in characteristic 2). For example, the radical of the quadratic form $Q : M \to R$ is

$$\mathrm{rad}(Q) = \{x \in M : \ Q(x) = 0 \text{ and } x \cdot y = 0 \text{ for every } y \in M\}$$

and it may be a proper submodule of $\mathrm{rad}(\beta)$. This is the case for the quadratic form $Q(X) = X^2$ over $\mathbb{F}_2$, where $\mathrm{rad}(Q) = \{0\}$ but $\mathrm{rad}(\beta) = \mathbb{F}_2$.

Hence a quadratic form $Q$ is called nondegenerate if its polarization $\beta$ is nondegenerate, and regular if $\beta$ is regular. These definitions have the disadvantage that they never apply to forms of odd rank in characteristic two. For free modules this is because if $n$ is odd and $B \in R^{n\times n}$ is a symmetric matrix whose diagonal entries belong to $2R$ then $\det(B) \in 2R$. Indeed, when we apply the Leibniz formula to

$$\det(B) = \det \begin{pmatrix} 2a_1 & b_{12} & \dots & b_{1n} \\ b_{12} & 2a_2 & \dots & b_{2n} \\ \dots & \dots & \dots & \dots \\ b_{1n} & b_{2n} & \dots & 2a_n \end{pmatrix}, \quad a_i = \frac{b_{ii}}{2},$$

most of the $n!$ summands occur twice (each term appearing along with its reflection across the diagonal), and because $n$ is odd, any monomial that stays unchanged upon reflecting across the diagonal must be a product that contains at least one factor $2a_i$ from the diagonal. This proves that we can write

$$\det \begin{pmatrix} 2a_1 & b_{12} & \dots & b_{1n} \\ b_{12} & 2a_2 & \dots & b_{2n} \\ \dots & \dots & \dots & \dots \\ b_{1n} & b_{2n} & \dots & 2a_n \end{pmatrix} = 2 \cdot P(Q),$$

where $P$ is a polynomial with integral coefficients in the variables $a_i, b_{ij}$ (which are coefficients of the quadratic form $Q$; hence $P$ depends only on $Q$ and the choice of a basis!) This polynomial makes sense over any ring and leads to the following definition:

**Definition 1.19.** A quadratic form $Q$ in $n$ variables ($n$ odd) is called **semiregular** if $P(Q) \in R^\times$ is a unit.

Changing bases multiplies $P(Q)$ by the square of a unit in $R$, so this notion is well-defined.

**Example 1.20.** The quadratic form $Q(X) = aX^2$ in one variable is semiregular if and only if $a \in R^\times$.

## 1.3. Isometries

Let $(M_1, Q_1)$ and $(M_2, Q_2)$ be quadratic modules over an integral domain $R$.

**Definition 1.21.** An **isometric embedding**

$$\varphi : (M_1, Q_1) \longrightarrow (M_2, Q_2)$$

is an injective $R$-linear map $\varphi : M_1 \to M_2$ that satisfies

$$Q_2\Big(\varphi(x)\Big) = Q_1(x) \quad \text{for every } x \in M_1.$$

$\varphi$ is called an **isometry** if it is bijective.

Sometimes the condition that $\varphi$ is injective is omitted from the definition of an isometry. (We do not do this.) If $(M_1, Q_1)$ is nondegenerate then any linear map $\varphi : M_1 \to M_2$ that satisfies $Q_2 \circ \varphi = Q_1$ is automatically injective anyway.

If $\varphi$ is an isometry then its inverse $\varphi^{-1}$ is also an isometry;. The composition of isometries also remains an isometry. Therefore the notion of isometric quadratic modules (i.e. quadratic modules that admit an isometry) is an equivalence relation; isometric quadratic forms are also called equivalent.

**Definition 1.22.** Let $M = (M, Q)$ be a quadratic space. The **orthogonal group**

$$\mathrm{O}(M) = \mathrm{O}(Q) = \mathrm{O}(M, Q)$$

is the group of self-isometries $\varphi : (M, Q) \to (M, Q)$.

If the characteristic of the base ring is not two, then $\mathrm{O}(M)$ can also be defined as the group of linear maps that preserve the bilinear form $\beta$:

$$\varphi \in \mathrm{O}(M) \;\Leftrightarrow\; \beta(\varphi x, \varphi y) = \beta(x, y) \text{ for all } x, y \in M.$$

Preserving $\beta$ is a strictly weaker condition in general. For example if $Q$ is the quadratic form $Q(X, Y) = X^2 + Y^2$ over $\mathbb{F}_2$ then the bilinear form is trivial, hence preserved by all of $\mathrm{GL}_2(\mathbb{F}_2)$, but $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \in \mathrm{GL}_2(\mathbb{F}_2)$ does not preserve $Q$.

The most important transformations in $\mathrm{O}(M)$ are reflections.

**Definition 1.23.** Let $(M, Q)$ be a quadratic space with an orthogonal decomposition

$$M = U \perp V.$$

The **reflection** in $M$ with respect to the splitting $(U, V)$ is the map

$$\sigma_{U,V} : U \perp V \longrightarrow U \perp V, \quad \sigma_{U,V}(u + v) = u - v.$$

$\sigma_{U,V}$ preserves the quadratic form and it is bijective (in fact it is its own inverse).

If $2 \in R^\times$ then any vector $r \in M$ whose length $Q(r) \in R^\times$ is invertible spans a regular submodule of $M$. By Corollary 1.10 it induces an orthogonal splitting

$$M = r^\perp \perp (R \cdot r).$$

The reflection associated to this decomposition is simply denoted $\sigma_r$. So $\sigma_r(r) = -r$ and $\sigma_r(x) = x$ for $x \in r^\perp$; the general formula is

$$\sigma_r(x) = x - \frac{x \cdot r}{Q(r)} r, \quad x \in M.$$

This formula makes sense even when 2 is not invertible and yields a transformation $\sigma_r \in \mathrm{O}(M)$, which we still call the **reflection** along $r$ (but not all authors do, and they are justified in this). Indeed, by the polarization formula,

$$Q(\sigma_r x) = Q(x) - \frac{(x \cdot r)}{Q(r)}(x \cdot r) + \frac{(x \cdot r)^2}{Q(r)^2} Q(r) = Q(x).$$

In characteristic two, the maps $\sigma_r$ behave differently, sometimes in ways that contradict geometric intuition: they are often instead called transvections. We will return to this later.

# 2. Quadratic forms over a local ring

Let $R$ be a local ring with the unique maximal ideal $\mathfrak{m}$ and residue field $k = R/\mathfrak{m}$. So $\mathfrak{m}$ consists of exactly the non-units in $R$. An important special case is when $R = k$ is already a field: the unique maximal ideal is $\mathfrak{m} = \{0\}$.

The basic structure theorems for quadratic spaces are due to Witt in the case $R = k$ is a field of characteristic other than two. The structure theory over fields of characteristic two is due to Arf. Ultimately Witt's theory was extended to local rings by Kneser.

By applying Nakayama's lemma one can show that a finitely generated projective module over a local ring is free. (In fact this is also true for projective modules that are not finitely generated, by a theorem of Kaplansky, but we do not need this.) So we can and often do work with bases.

**Remark 2.1.** Suppose $R$ is a local ring and $Q : M \to R$ is a quadratic form. From $M$ one can construct a $k$-vector space $\overline{M} = M/(\mathfrak{m} \cdot M)$, and $\{x_1, ..., x_n\}$ is an $R$-basis for $M$ if and only if $\{x_1 + \mathfrak{m} \cdot M, ..., x_n + \mathfrak{m} \cdot M\}$ is a $k$-basis for $\overline{M}$. (This again follows from Nakayama's lemma.) We write

$$\overline{x} = x + \mathfrak{m} \cdot M \in \overline{M}$$

for $x \in M$. The quadratic form $Q$ induces a quadratic form

$$\overline{Q} : \overline{M} \longrightarrow k, \quad \overline{Q}(\overline{x}) := Q(x) + \mathfrak{m}.$$

This is well-defined because if $x, y \in M$ and $a \in \mathfrak{m}$ then

$$Q(x + ay) = Q(x) + a(x \cdot y) + a^2 Q(y) \in Q(x) + \mathfrak{m}.$$

## 2.1. Diagonalization

For elements $a_1, ..., a_n \in R$, the **diagonal quadratic form** is

$$\langle a_1, ..., a_n \rangle := \langle a_1 \rangle \perp ... \perp \langle a_n \rangle = \sum_{i=1}^{n} a_i X_i^2.$$

**Definition 2.2.** A quadratic space $(M, Q)$ is **diagonalizable** if there is an isometry from $Q$ to a diagonal quadratic form.
Equivalently, $(M, Q)$ is diagonalizable if it admits an **orthogonal basis**, in other words a basis $e_1, ..., e_n$ where $\beta(e_i, e_j) = 0$ if $i \neq j$.

The diagonalization problem depends a lot on whether 2 has an inverse in $R$. If it does then we immediately have:

**Proposition 2.3.** *Suppose $2 \in R^\times$. Then every regular quadratic space is diagonalizable.*

*Proof.* Let $(M, Q)$ be a regular quadratic space. Recall that by Corollary 1.11, $M$ splits as an orthogonal direct sum

$$M = \langle u_1, ..., u_r \rangle \perp N,$$

where $u_i \in R^\times$ and where $N$ is a submodule satisfying

$$x \cdot x \notin R^\times \text{ for any } x \in N.$$

We will show $N = \{0\}$ which immediately implies the claim.

Suppose there were an $x \in N$, $x \neq 0$. Since $M$ (and therefore $N$) is regular, there exists $y \in N$ with $x \cdot y = 1$. (Where $x \cdot y$ refers to the polar bilinear form of $Q$.) Then

$$2 = 2(x \cdot y) = (x + y) \cdot (x + y) - x \cdot x - y \cdot y.$$

But $x, y, x + y \in N$ so neither $x \cdot x$ nor $y \cdot y$ nor $(x + y) \cdot (x + y)$ is a unit. Since $R$ is a local ring, its nonunits are closed under addition and therefore $2 \notin R^\times$. □

If 2 does not have an inverse in $R$ then there are regular quadratic forms that cannot be diagonalized.

**Example 2.4.** The hyperbolic plane, $R^2$ with quadratic form $H(X, Y) = XY$, cannot be diagonalized over any local ring in which $2 \notin R^\times$. One way to see this is that for a diagonalizable quadratic form $Q : M \to R$, (WLOG a diagonal quadratic form $Q = \langle a_1, ..., a_n \rangle$), the polar bilinear form $\beta$ satisfies $\beta(x, y) \in 2R$ for any $x, y \in M$. But the bilinear form attached to $H$ takes on every value of $R$ because, for any $a \in R$, we have $a = (1, 0) \cdot (0, a)$.

So regular quadratic forms can fail to be diagonalizable. However it turns out that, at least over local rings, they can be decomposed into blocks of size at most $2 \times 2$. This is sometimes called Jordan decomposition.

**Proposition 2.5.** *Let $R$ be a local ring and let $(M, Q)$ be a quadratic $R$-module. Then $M$ has an orthogonal direct sum decomposition*

$$M = \langle u_1, .., u_r \rangle \perp \bigperp_{i=1}^{s} E_i \perp F$$

*where $u_i \in R^\times$, where $E_i$ are regular indecomposable submodules of rank two, and where $F$ is a submodule that satisfies*

$$\beta(x, y) \in \mathfrak{m} \text{ for every } x, y \in F.$$

*Proof.* Start again with the decomposition

$$M = \langle u_1, ..., u_r \rangle \perp N$$

where $\beta(x, x) \in \mathfrak{m}$ for every $x \in N$. If $\beta(x, y) \in \mathfrak{m}$ for every $x, y \in N$ then we have $F = N$ and we are done. Otherwise there exist $x, y \in N$ for which $\beta(x, y) \in R^\times$. Then $E_1 := Rx \oplus Ry$ is a regular submodule of $N$ so we have an orthogonal splitting $N = E_1 \perp E_1^\perp$.
By inducting on the rank of $N$ we obtain the decomposition. □

**Corollary 2.6.** *Suppose $2 \notin R^\times$.*
*(i) Every regular quadratic space over $R$ decomposes in the form*

$$M = \bigperp_{i=1}^{s} E_i$$

*where* $\mathrm{rank}(E_i) = 2$.
*(ii) Every semiregular quadratic space over $R$ decomposes in the form*

$$M = \langle u \rangle \perp E$$

*where $E$ is regular and $u \in R^\times$.*

In particular if $M$ is regular then $\mathrm{rank}(M)$ is even.

*Proof.* (i) The summands $\langle u_1, ..., u_r \rangle$ and $F$ in Proposition 2.5 are not regular and therefore cannot appear.
(ii) Semiregular spaces have odd rank, so in the decomposition of Proposition 2.5 the quadratic form $Q = \langle u_1, ..., u_r \rangle \perp F$ must have odd rank. If $P$ is the half-discriminant then $P(Q) \in \mathfrak{m}$ unless $F = 0$, in which case

$$P(Q) = P(\langle u_1, ..., u_r \rangle) = 2^{r-1} \cdot u_1 u_2 ... u_r \cdot (R^\times)^2.$$

By assumption this is a unit if and only if $r = 1$. □

## 2.2. Witt's theorem

Diagonalization and related decompositions are a step towards the classification of quadratic forms. However, a big problem is that these decompositions are far from unique. The fundamental result we need is Witt's theorem (in any of its forms).

One form of Witt's theorem is about extending isometries. Briefly, if $M$ is a quadratic space, the theorem gives conditions for isometries $U \to V$ between submodules $U, V \subseteq M$ to extend to elements of $\mathrm{O}(M)$, defined on the entire space.

The extension is generally constructed as a composition of reflections. So in a situation where Witt's theorem in one of its forms applies, there is often a corollary stating that $\mathrm{O}(M)$ is generated by its reflections.

**Theorem 2.7** (Witt extension theorem)**.** *Let $M$ be a quadratic module over a local ring $R$. Let $U, V \subseteq M$ be sharply primitive submodules and $t : U \to V$ an isometry. Then there exists $\varphi \in \mathrm{O}(M)$ such that $\varphi|_U = t$.*

**Corollary 2.8.** *Let $(M, Q)$ be a quadratic module over a local ring $R$. Let $x, y \in M$ with $Q(x) = Q(y) \in R^\times$. Then there exists $\sigma \in \mathrm{O}(M)$ with $\sigma x = y$.*

This follows from the theorem because $Rx$ and $Ry$ are sharply primitive submodules. When $2 \in R^\times$ this corollary is easy to prove directly. In fact one can even take $\sigma$ to be a reflection along an appropriately chosen vector: Let $u = \frac{x-y}{2}$ and $v = \frac{x+y}{2}$, such that $u \cdot v = 0$. Then we have

$$Q(x) = Q(u + v) = Q(u) + Q(v).$$

Since $Q(x) \in R^\times$ and the nonunits in a local ring are closed under addition, we have either $Q(u) \in R^\times$ or $Q(v) \in R^\times$. Suppose $Q(v) \in R^\times$. Then the reflection $\sigma_v$ maps $u \mapsto u$ and $v \mapsto (-v)$ and therefore $\sigma_v x = y$. If instead $Q(u) \in R^\times$ then $-\sigma_u x = y$.

**Remark 2.9.** When 2 is a nonunit, the analog of the "Witt extension theorem" for symmetric bilinear forms is **false** even for fields! Consider $\mathbb{F}_2^3$ and take the bilinear form

$$\beta((x_1, x_2, x_3), (y_1, y_2, y_3)) = x_1y_1 + x_2y_2 + x_3y_3.$$

Let $x = (1, 0, 0)$ and $y = (1, 1, 1)$ and let $U = Rx$, $V = Ry$. Then $U$ and $V$ are sharply primitive and the map $t : U \to V$, $tx = y$ is an isometry, but the orthogonal complements

$$U^\perp = R(0, 1, 0) \oplus R(0, 0, 1), \quad V^\perp = R(1, 1, 0) \oplus R(0, 1, 1)$$

do not carry equivalent bilinear forms ($V^\perp$ is even and $U^\perp$ is not) so there cannot be an isometry of the total space $\varphi \in \mathrm{O}(M)$ mapping $U$ to $V$.

We will prove the following generalized version due to Kneser.

Recall that if $(M, Q)$ is a quadratic module and $U \subseteq M$ is a submodule then we define

$$b_U : M \longrightarrow U^*, \quad b_U(x)(y) = x \cdot y \ (x \in M,\ y \in U).$$

**Theorem 2.10** (Witt extension theorem)**.** *Let $(M, Q)$ be a quadratic module. Suppose $U, V \subseteq M$ are any submodules and there is a submodule $H$ such that*

$$b_U(H) = U^* \quad \textit{and} \quad b_V(H) = V^*.$$

*Suppose $t : U \to V$ is an isometry that satisfies $t(x) - x \in H$ for every $x \in U$. Then there is an isometry $\varphi \in \mathrm{O}(M)$ such that $\varphi|_U = t$; moreover, $\varphi$ can be chosen such that*

$$\varphi(x) - x \in H \textit{ for every } x \in M$$

*and $\varphi(x) = x$ for every $x \in H^\perp$.*

$H$ is meant to be the subspace through which we are allowed to take reflections, and this theorem is formulated to keep $H$ as small as possible. However we do need $H$ to contain a hyperbolic complement to both $U$ and $V$ simultaneously, which is the same as demanding $b_U(H) = U^*$ and $b_V(H) = V^*$.

If 2 were invertible, and $x_1, ..., x_r$ were an orthogonal basis of $U$, and each $h_i = \frac{t(x_i) - x_i}{2}$ satisfied $Q(h_i) \in R^\times$, then (as in the remark following Corollary 2.8 above) we could define $\varphi$ as the product of reflections along $h_i$. Unfortunately it won't be that easy.

Theorem 2.7 follows immediately from Theorem 2.10 by taking $H = M$.

*Proof.* Let $(\overline{M}, \overline{Q})$ be the quadratic module over $k$ given by reducing $Q$ mod $\mathfrak{m}$, as outlined in Remark 2.1.

We want to construct $\varphi$ as a product of reflections along vectors of $H$. This is not necessarily possible. In fact there might not be any vectors of invertible length (equivalently, any reflections) in $H$ at all. To guarantee that there are enough reflections we need the following assumption: either
(1) $\#k \geq 3$ and $\overline{Q}(\overline{H}) \neq \{0\}$; or
(2) $\#k = 2$ and $\overline{Q}(\overline{H}^\perp) \neq \{0\}$.
(In (2) note that $\overline{H}^\perp$ is the radical of the bilinear space, but not the quadratic form. In other words we are asking for $\overline{x} \in \overline{H}$ such that $\overline{x} \cdot \overline{y} = 0$ for all $\overline{y} \in \overline{H}$ but $\overline{Q}(\overline{x}) \neq 0$.) We may assume without loss of generality that (1) or (2) holds (depending on $k$) because: if not, then define

$$M' := M \perp E$$

where $E$ is a hyperbolic plane: $E = Re \oplus Rf$ with vectors satisfying $Q(e) = Q(f) = 0$ and $e \cdot f = 1$. Then take $U' := U \perp Re$ and $V' := V \perp Re$ and $H' := H \perp R(e + f)$.

Conditions (1) or (2) are satisfied because $\overline{Q}(\overline{e}+\overline{f}) \neq 0$ (and if $k = \mathbb{F}_2$ then $\overline{e}+\overline{f}$ belongs to the radical). Any isometry $t : U \to V$ with $t(x) = x \bmod H$ extends to an isometry

$$t' : U' \to V',\ t'(e) = e,$$

and if the Witt extension theorem holds for $M'$ then we obtain an extension $\varphi' \in \mathrm{O}(M')$ which satisfies $\varphi'(e) = e$ and also (since $e - f$ is orthogonal to $H'$) $\varphi'(e - f) = e - f$. Hence $\varphi'$ acts trivially on $E$ and has the form $\varphi' = \varphi \perp \mathrm{id}_E$ where $\varphi \in \mathrm{O}(M)$ is the extension we need.

So assume (1) or (2) holds. We will prove by total induction on $\mathrm{rank}(U) = \mathrm{rank}(V)$ that $\varphi$ can be constructed as a product of reflections:

**1. Base case.** First suppose $\mathrm{rank}(U) = \mathrm{rank}(V) = 1$, so $U = R \cdot x$ and $V = R \cdot y$ where $t(x) = y$. By assumption, we can write

$$h = y - x = t(x) - x \in H.$$

Since

$$Q(x) = Q(y) = Q(x + h) = Q(x) + Q(h) + (x \cdot h),$$

we have

$$x \cdot h = -Q(h)$$

and also

$$y \cdot h = (h + x) \cdot h = Q(h).$$

If $Q(h)$ is invertible, then the reflection $\sigma_h$ satisfies

$$\sigma_h(x) = x - \frac{x \cdot h}{Q(h)} h = x + h = y$$

and it acts trivially on $H^\perp$, so $\varphi = \sigma_h$ is the extension. The difficult case is $Q(h) \in \mathfrak{m}$. We will actually construct $\varphi$ as a product of two reflections $\sigma_d \sigma_e$ where $d, e \in H$ and $Q(d), Q(e) \in R^\times$. We use the ansatz

$$d = y - \sigma_e(x),$$

in other words

$$d = y - x + \frac{e \cdot x}{Q(e)} e = h + \frac{e \cdot x}{Q(e)} e.$$

Then the earlier computation (with $x$ replaced by $\sigma_e x$) shows that $\sigma_d \sigma_e x = y$.

Since

$$\begin{aligned} Q(d) &= Q(h) + \frac{(e \cdot x)(e \cdot h)}{Q(e)} + \frac{(e \cdot x)^2}{Q(e)} \\ &= Q(h) + \frac{(e \cdot x)(e \cdot y)}{Q(e)} \end{aligned}$$

and $Q(h)$ was assumed to be a nonunit, $Q(d) \in R^\times$ is equivalent to both $e \cdot x \in R^\times$ and $e \cdot y \in R^\times$. So it is enough to find a vector $e \in H$ with

$$Q(e) \in R^\times \text{ and } e \cdot x \in R^\times \text{ and } e \cdot y \in R^\times.$$

The equations $\overline{e} \cdot \overline{x} = 0$ and $\overline{e} \cdot \overline{y} = 0$ for $\overline{e} \in \overline{H}$ define hyperplanes $\overline{H}_1, \overline{H}_2$ in $\overline{H}$. (This is due to the assumption $b_U(H) = U^*$ and $b_V(H) = V^*$.) To produce $e$ we need to show that $\overline{Q}$ does not vanish identically on the complement of $\overline{H}_1 \cup \overline{H}_2$. Suppose this were not the case. Let $\overline{u} \in \overline{H}_1 \cap \overline{H}_2$ and $\overline{v} \notin \overline{H}_1 \cup \overline{H}_2$ be any vectors. Then for $\lambda \in k$, the vector $\lambda\overline{u} + \overline{v}$ also does not belong to $\overline{H}_1 \cup \overline{H}_2$ and therefore

$$0 = \overline{Q}(\lambda\overline{u} + \overline{v}) = \lambda^2\overline{Q}(\overline{u}) + \lambda(\overline{u} \cdot \overline{v}) + \overline{Q}(\overline{v}).$$

If $\#k \geq 3$ then the fact that this polynomial in $\lambda$ is identically zero implies

$$0 = \overline{Q}(\overline{u}) = \overline{u} \cdot \overline{v} = \overline{Q}(\overline{v}).$$

Taking $\overline{u} = \overline{h}$ (which is possible since $\overline{h} \cdot \overline{x} = -\overline{Q}(\overline{h}) = 0$ and $\overline{h} \cdot \overline{y} = \overline{Q}(\overline{h}) = 0$) we obtain $\overline{h} \cdot \overline{v} = 0$ for every $\overline{v} \notin \overline{H}_1 \cup \overline{H}_2$. Since $\overline{H} \backslash (\overline{H}_1 \cup \overline{H}_2)$ spans all of $\overline{H}$, we obtain $\overline{h} \cdot \overline{H} = 0$. But $\overline{h} = \overline{y} - \overline{x}$ and therefore $\overline{H}_1 = \overline{H}_2$, so we have

$$\overline{Q}(\overline{u}) = 0,\ \overline{Q}(\overline{v}) = 0 \text{ for all } \overline{u} \in \overline{H}_1,\ \overline{v} \in \overline{H} \backslash \overline{H}_1$$

hence $\overline{Q}(\overline{H}) = \{0\}$, in contradiction to assumption (1).

If $\#k = 2$ then we have $\overline{H}^\perp \cap \overline{H}_1 = \overline{H}^\perp \cap \overline{H}_2$, so every vector of $\overline{H}^\perp$ belongs to either $\overline{H}_1 \cap \overline{H}_2$ or $\overline{H} \backslash (\overline{H}_1 \cup \overline{H}_2)$. But for any $\overline{u} \in \overline{H}^\perp \cap \overline{H}_1 \cap \overline{H}_2$ and any $\overline{v} \in \overline{H}^\perp \backslash (\overline{H}_1 \cup \overline{H}_2)$ and any $\lambda \in k$, still under the assumption that $\overline{Q}$ vanishes identically on the complement of $\overline{H}_1 \cup \overline{H}_2$, we have

$$0 = \overline{Q}(\lambda\overline{u} + \overline{v}) = \lambda^2\overline{Q}(\overline{u}) + \overline{Q}(\overline{v}).$$

The fact that this polynomial vanishes identically forces

$$\overline{Q}(\overline{u}) = \overline{Q}(\overline{v}) = 0,$$

even in characteristic two, but then $\overline{Q}(\overline{H}^\perp) = \{0\}$ in contradiction to assumption (2).

In all cases, we obtain a vector $\overline{e} \in \overline{H}$ with $\overline{Q}(\overline{e}) \neq 0$ and $\overline{e} \cdot \overline{x} \neq 0$, $\overline{e} \cdot \overline{y} \neq 0$. Then for any preimage $e \in H$, with $d = y - \sigma_e(x)$, we obtain the Witt extension $\varphi = \sigma_d\sigma_e$.

**2. Induction step.** Suppose $r = \text{rank}(U) > 1$ and let $x_1, ..., x_r$ be an $R$-basis of $U$. Let $U' = \bigoplus_{i=2}^r Rx_i$. By the induction assumption, the restricted isometry $t|_{U'}$ extends to a product of reflections $\sigma \in \mathrm{O}(M)$. After replacing $t$ by $\sigma^{-1}t$, we may assume without loss of generality that $t(x_i) = x_i$ for all $i \neq 1$.

Since $b_U(H) = U^*$, there are vectors $h_1, ..., h_r \in H$ such that

$$x_i \cdot h_j = \delta_{i,j}.$$

Then

$$H = \Big( \bigoplus_{i=1}^{r} Rh_i \Big) \oplus (H \cap U^\perp).$$

Let $H_1$ be the submodule $H_1 = Rh_1 \oplus (H \cap U^\perp)$. Since

$$(t(x_1) - x_1) \cdot x_j = t(x_1) \cdot t(x_j) - x_1 \cdot x_j = 0$$

for every $j \geq 2$, we have $t(x_1) - x_1 \in H_1$. Now we want to apply the induction assumption to $U_1 = Rx_1$, $V_1 = Rt(x_1)$ and $H_1$ instead of $U, V, H$. For an appropriate choice of the basis, these satisfy the assumptions (1) or (2), because: let $\overline{h} \in \overline{H}$ or $\overline{h} \in \overline{H}^\perp$, according to whether $\#k \geq 3$ or $\#k = 2$, be a vector with $\overline{Q}(\overline{h}) \neq 0$. We choose $h_1$ not in $H \cap U^\perp$ such that $\overline{h}$ has a preimage $h \in H_1 = Rh_1 \oplus (H \cap U^\perp)$, and extend $H_1$ via an arbitrary basis $h_2, ..., h_r$ to a basis of $H$. Then let $x_1, ..., x_r \in U$ be the dual basis of $h_1, ..., h_r$.

By the induction hypothesis applied to $U_1, V_1$ and $H_1$, we get an isometry $\varphi_1 \in \mathrm{O}(M)$ with $\varphi(x_1) = t(x_1)$ and which leaves $H_1^\perp$ pointwise fixed. But $x_2, ..., x_r \in H_1^\perp$, so $\varphi(x_i) = x_i = t(x_i)$ for all $i \geq 2$ and therefore $\varphi$ extends $t$. This is the extension we wanted. □

## 2.3. Generators of orthogonal groups

Before going further, note that the proof of Witt's theorem in the formulation given by Kneser implies that orthogonal groups over local rings are almost always generated by reflections. This was hinted at earlier and it will be proved now.

First the statement for fields:

**Theorem 2.11.** *Let $(M, Q)$ be a regular or semiregular quadratic module over a field $K$. Then,* ***with exactly one exception****, $\mathrm{O}(M)$ is generated by reflections.*

*The exception is the space $H \perp H$ over $\mathbb{F}_2$.*

Here $H$ is the hyperbolic plane $H(X, Y) = XY$.

**Remark 2.12.** The orthogonal group of $H \perp H$ over $\mathbb{F}_2$ really cannot generated by reflections. $\mathrm{O}(H \perp H)$ is a finite group of size only 72 so one could simply go through

the reflections and check that they generate a strictly smaller group, but the isometry

$$H \perp H \cong E \perp E,$$

where $E(X,Y) = X^2 + XY + Y^2$ is the elliptic plane over $\mathbb{F}_2$, makes it clearer. Since $E$ is anisotropic, every vector in $E \perp E$ that does not lie in either copy of $E$ has norm 0. Hence every reflection of $E \perp E$ leaves the subspaces $E \perp \{0\}$ and $\{0\} \perp E$ invariant. However the map

$$E \perp E \longrightarrow E \perp E, \quad (x,y) \mapsto (y,x) \text{ for } x, y \in E$$

is an isometry that does not leave those subspaces invariant.

The theorem follows from the general result for local rings:

**Theorem 2.13.** *Let $(M,Q)$ be a regular quadratic module over a local ring $R$ with residue field $k = R/\mathfrak{m}$. If $k = \mathbb{F}_2$ then suppose* $\operatorname{rank}(M) \geq 6$. *Then* $\mathrm{O}(M)$ *is generated by reflections.*

Theorem 2.11 can be derived from this, because:
(i) The only regular modules of rank two over $\mathbb{F}_2$ are the hyperbolic and elliptic planes $H(X,Y) = XY$, $E(X,Y) = X^2 + XY + Y^2$, and since any regular module over $\mathbb{F}_2$ is an orthogonal direct sum of planes, the only such modules of rank four are $H \perp H$, $H \perp E$ and $E \perp E \cong H \perp H$. The fact that $\mathrm{O}(H)$ and $\mathrm{O}(H \perp E)$ are reflection groups can be checked by hand.
(ii) A semiregular module (over a field $k$ of characteristic two) has the form $M = kx \perp N$ where $Q(x)$ is a unit and $M$ is regular. For any isometry $\varphi \in \mathrm{O}(M)$, apply the Witt extension theorem to $t = \varphi|_N$ with $H = M$, (this is allowed because $H$ has nontrivial bilinear radical, since $\langle Q(x) \rangle$ does) to obtain a product of reflections $\sigma$ with $\sigma|_N = \varphi|_N$. Then $\sigma^{-1}\varphi$ maps $N$ into itself, so it maps $x \mapsto ax$ for some $a \in k^\times$. Since this is an isometry, we have $a^2 = 1$; but $k$ has characteristic two and therefore $a = 1$. Hence $\sigma^{-1}\varphi = \mathrm{id}$ and $\varphi = \sigma$ is already a product of reflections.

*Proof.* [Proof of Theorem 2.13] Let $\varphi \in \mathrm{O}(M)$. If $k \neq \mathbb{F}_2$, then the claim follows immediately from the proof of the Witt extension theorem: taking $U = V = H = M$, and observing that $\overline{Q}(\overline{H}) \neq \{0\}$, we obtain a product of reflections which "extends" and therefore coincides with $\varphi$.
In the case $k = \mathbb{F}_2$, we first choose any vector $x \in M$ with $Q(x) \notin \mathfrak{m}$. We can assume without loss of generality that $\varphi(x) = x$, because: Take $U = R \cdot x$ and $V = R \cdot y$ where $y = \varphi(x)$, and look for a submodule $H$ with the property

$$x \cdot H = y \cdot H = R, \quad y - x \in H$$

as well as $\overline{Q}(\overline{H}^\perp) \neq \{0\}$. This is possible if we take $H = h^\perp + \mathfrak{m} \cdot M$ where $h$ is any vector with

$$Q(h) \in R^\times,\ \overline{h} \in \overline{(y-x)^\perp},\ \overline{h} \neq \overline{x}, \overline{y}$$

since in this case $\overline{h} \in \overline{H^\perp}$. In other words it is enough if the hyperplane $\overline{(y-x)^\perp}$ contains at least three vectors $\overline{h}$ with $\overline{Q}(\overline{h}) \neq 0$. This is possible if $\operatorname{rank}(M) \geq 6$, since $\overline{x}$ and $\overline{y}$ belong to at most two regular planes that split off orthogonally from $\overline{Q}$, with the orthogonal complement being regular and having nontrivial intersection with $\overline{(y-x)^\perp}$. By Witt's theorem, there is a product of reflections $\sigma$ with $\sigma x = y$, and $\sigma^{-1}\varphi \in \mathrm{O}(M)$ maps $x$ to $x$.

So assume there exists $x \in M$ with $Q(x) \in R^\times$ and $\varphi(x) = x$. By Nakayama's lemma, $M$ splits as a direct sum (which is not necessarily orthogonal),

$$M = (R \cdot x) \oplus N.$$

By applying Witt's theorem to $U = N$ and $V = \varphi(N)$ and $H = x^\perp$, noting that $x \in \overline{H^\perp}$, we obtain a product of reflections $\sigma$ with $\sigma|_N = \varphi|_N$ and which leaves $H^\perp$ pointwise fixed. But $x \in H^\perp$ and therefore $\sigma x = x = \varphi x$, so $\sigma = \varphi$ everywhere. □

For fields of characteristic $\neq 2$, analyzing the proof gives us the following more precise result.

**Theorem 2.14** (Cartan–Dieudonné theorem)**.** *Let $K$ be a field,* $\operatorname{char}(K) \neq 2$*, and let $(M, Q)$ be a regular quadratic space of dimension $n$. Then every automorphism $\varphi \in \mathrm{O}(M)$ is a product of at most $n$ reflections.*

## 2.4. Witt decomposition

From Witt's theorem on extending isometries we quickly get the version of Witt's theorem that allows you to "cancel" regular quadratic subspaces.

**Theorem 2.15** (Witt cancellation theorem)**.** *Let $(M, Q_M)$ and $(N, Q_N)$ be quadratic modules over a local ring $R$ and let $F$ be a regular quadratic space over $R$. If $F \oplus M \cong F \oplus N$, then $M \cong N$.*

*Proof.* Let $\varphi : F \oplus M \to F \oplus N$ be an isometry. Then $\varphi|_F$ defines an isometric embedding of $F$ into $F \oplus N$, which by Witt's theorem extends to an automorphism $\psi \in \mathrm{O}(F \oplus N)$. The composition $\psi^{-1} \circ \varphi|_F$ acts as the identity on $F$ and therefore has the form

$$\psi^{-1} \circ \varphi|_F = \mathrm{id} \perp t,$$

where $t : M \to N$ is an isometry. □

Conversely, Witt's theorem in the form of extending isometries (for regular modules) follows easily from the Witt cancellation theorem. If $U, V \subseteq M$ are regular submodules

of a quadratic space and $t : U \to V$ is an isometry, then we have decompositions

$$M = U \perp U^\perp = V \perp V^\perp \cong U \perp V^\perp,$$

the rightmost isometry being $t^{-1} \perp \mathrm{id}$. By Witt cancellation, $U \perp U^\perp \cong U \perp V^\perp$ implies the existence of an isometry $t^\perp : U^\perp \to V^\perp$, and then $t + t^\perp \in \mathrm{O}(M)$ is an automorphism extending $t$.

So Witt's extension theorem and cancellation theorem are essentially equivalent.

**Remark 2.16.** This has been said already but it bears repeating. Over local rings where 2 is not a unit, (e.g. fields of characteristic two), Witt's theorem, also in the form of the cancellation theorem, does *not* hold for symmetric bilinear forms.

Witt's cancellation theorem leads to the following normal form for quadratic forms over local rings:

**Theorem 2.17** (Witt decomposition)**.** *Let $(M, Q)$ be a regular quadratic space over a local ring $R$. Then $M$ decomposes as*

$$M = H^r \perp N,$$

*where $H(X, Y) = XY$ is the hyperbolic plane, where $H^r = H \perp ... \perp H$ is $r$ orthogonal copies of $H$, and where $N$ is anisotropic. The* **Witt index** *$r$ is unique, and the* **core form** *$N$ is unique up to isometry.*

The existence of this decomposition is relatively easy to prove. The salient point is the uniqueness of the core form $N$ and the number of hyperbolic planes (i.e. the Witt index).

*Proof.* **Existence:** induction on $\mathrm{rank}(M)$. If $M$ is anisotropic then we are done. Otherwise let $x \in M$ with $Q(x) = 0$ and (by regularity) choose $y \in M$ with $x \cdot y = 1$. If $y$ does not already have $Q(y) = 0$ then replace it by $y - Q(y)x$, noting that

$$Q(y + ax) = Q(y) + a(x \cdot y) = 0 \text{ for } a = -Q(y).$$

Then $x, y$ span a hyperbolic plane $H$ which is regular and therefore splits off orthogonally: $M = H \perp M_1$ where $\mathrm{rank}(M_1) = \mathrm{rank}(M) - 2$. The claim follows by induction.

**Uniqueness:** Suppose we have two decompositions

$$M = H^{r_1} \perp N_1 = H^{r_2} \perp N_2,$$

where $N_1$ and $N_2$ are anisotropic. Without loss of generality assume $r_1 \geq r_2$. Since $H$ is regular, by repeatedly applying the Witt cancellation theorem, we obtain

$$H^{r_1 - r_2} \perp N_1 \cong N_2.$$

Since $H$ is isotropic and $N_2$ is not, we have $r_1 - r_2 = 0$ and therefore $N_1 \cong N_2$. □

The Witt index can also be described as the rank of any totally isotropic subspace $T$ of $M$ which is maximal in the sense that any totally isotropic subspace of $M$ containing $T$ must already be $T$ itself. Remember that a totally isotropic subspace means a *finitely-generated* and *projective* (hence in this case free) submodule on which the quadratic form vanishes identically, not merely the bilinear form. (In practice we only care about discrete valuation rings, i.e. local *principal ideal domains*, in which case submodules are automatically finitely-generated and free.)

More precisely we have the following:

**Proposition 2.18.** *Let $(M, Q)$ be a regular quadratic space over a local ring $R$.*
*(i) Let $T \subseteq M$ be a totally isotropic subspace. Then the hyperbolic space $H(T) \cong H^{\mathrm{rank}(T)}$ embeds isometrically into $M$.*
*(ii) For any two totally isotropic spaces $T_1, T_2 \subseteq M$ of equal rank, there exists $\varphi \in \mathrm{O}(M)$ such that $\varphi T_1 = T_2$.*
*(iii) All maximal totally isotropic subspaces $T$ have equal rank, equal to the Witt index of $M$.*

*Proof.* (i) Since $M$ is regular, every linear functional on $T$ is realized as the bilinear product with an element of $M$. So if $e_1, ..., e_r$ is any basis of $T$ then there exist $f_1, ..., f_r \in M$ such that $e_i \cdot f_j = \delta_{ij}$. The elements $f_j$ can further be assumed to satisfy $Q(f_j) = 0$; if not, then use the usual trick of replacing $f_j$ by $f_j - Q(f_j)e_j$. Then $e_1, ..., e_r, f_1, ..., f_r$ are linearly independent and span a subspace that is isometric to $H(T)$.
(ii) The hyperbolic spaces $H(T_1)$ and $H(T_2)$ are isometric and regular, and by Witt's theorem any isometry between them extends to all of $M$.
(iii) The maximal free totally isotropic subspaces have equal rank by (ii). If $M = H^r \perp N$ with $N$ anisotropic, and each copy of $H$ is written $Re_i \oplus Rf_i$ with vectors satisfying $Q(e_i) = Q(f_i) = 0$, $e_i \cdot f_i = 1$, then $\{e_1, ..., e_r\}$ spans a maximal, totally isotropic space of rank equal to the Witt index $r$, which proves (iii). □

For fields of characteristic other than two, we obtain the Witt decomposition without the assumption of regularity:

**Corollary 2.19.** *Let $(M, Q)$ be a quadratic space over a field $K$ with $\mathrm{char}(K) \neq 2$. Then $M$ decomposes as*

$$M = \mathrm{rad}(M) \perp N \perp H^r,$$

*where $H(X, Y) = XY$, where $N$ is anisotropic, and $\mathrm{rad}(M)$ is the radical, and the Witt index $r$ and core form $N$ are unique.*

*Proof.* $\mathrm{rad}(M)$ splits off as a direct summand:

$$M = \mathrm{rad}(M) \oplus M_1,$$

and the direct sum is orthogonal by definition of rad($M$). Then $M_1$ is regular and has a unique Witt decomposition. □

**Definition 2.20.** Regular quadratic spaces $M_1, M_2$ are **Witt equivalent** if there are hyperbolic spaces $H_1, H_2$ (=sums of copies of the hyperbolic plane) such that

$$M_1 \perp H_1 \cong M_2 \perp H_2.$$

In other words, $M_1, M_2$ are Witt equivalent if their core forms are isometric. Hyperbolic spaces are exactly the quadratic spaces that are Witt equivalent to 0.

## 2.5. The Witt ring

The uniqueness of the Witt decomposition naturally leads to a *group structure* on the set of Witt equivalence classes.

The sum of Witt equivalence classes is defined to be

$$[M] \oplus [N] := [M \perp N].$$

This is clearly well-defined, associative and commutative. Every Witt equivalence class has an inverse, because: let $(M, Q)$ be any regular space and consider the space

$$F := (M, Q) \perp (M, -Q),$$

where $-Q$ is the negative of the quadratic form $Q$. We will show that $F$ is hyperbolic: If $x_1, ..., x_n$ is any $R$-basis of $M$, then $e_1 = (x_1, x_1), ..., e_n = (x_n, x_n)$ is a system of vectors of $F$ which are all orthogonal and have norm zero: $Q(e_i) = e_i \cdot e_j = 0$. Hence $F$ has Witt index $n = \text{rank}(M) = \frac{1}{2}\text{rank}(F)$, which means it splits completely into hyperbolic planes.

Therefore, taking orthogonal direct sums defines a group structure on Witt equivalence classes.

**Definition 2.21.** The **Witt group** $W(R)$ of a local ring $R$ is the abelian group of Witt equivalence classes of regular quadratic spaces over $R$.

$W(R)$ carries the additional structure of a *commutative ring* with multiplication given by the tensor product. If $(M_1, Q_1)$ and $(M_2, Q_2)$ are regular quadratic spaces, then we define a quadratic form on $M_1 \otimes_R M_2$ on pure tensors by

$$Q_1 \otimes Q_2(x_1 \otimes x_2) = 2 \cdot Q_1(x_1) \cdot Q_2(x_2)$$

and its bilinear form by

$$\beta_{Q_1 \otimes Q_2}(x_1 \otimes x_2, y_1 \otimes y_2) = \beta_{Q_1}(x_1, y_1) \cdot \beta_{Q_2}(x_2, y_2).$$

Now $\beta_{Q_1 \otimes Q_2}$ extends to all of $M_1 \otimes_R M_2$ by bilinearity, and $Q_1 \otimes Q_2$ extends to $M_1 \otimes_R M_2$ by the polarization formula.
(If $R$ has charactistic two then this multiplication is identically zero. In this case it would seem to be more natural to define $Q_1 \otimes Q_2(x_1 \otimes x_2) = Q_1(x_1)Q_2(x_2)$, but then it is no longer clear how $Q_1 \otimes Q_2$ is defined on tensors that are not pure.) To prove that this defines a ring structure, one uses the rule

$$(M \oplus H) \otimes N \cong (M \otimes N) \oplus (H \otimes N),$$

together with the fact that $H \otimes N$ is a hyperbolic space, (where $H$ is the hyperbolic plane): if we write $H = Re \oplus Rf$, where $Q(e) = Q(f) = 0$ and $e \cdot f = 1$, then $(Re) \otimes N$ is a hyperbolic space of rank $\frac{1}{2}\text{rank}(H \otimes N)$.

In practice, to compute the tensor product of quadratic forms, we usually use the observation that for diagonal quadratic forms,

$$\langle a_1, ..., a_m \rangle \otimes \langle b_1, ...b_n \rangle = \langle a_i b_j : \ 1 \leq i \leq m, \ 1 \leq j \leq n \rangle.$$

We will now work out some examples of the Witt ring (or Witt group).

**Example 2.22.** Over $\mathbb{C}$ (or any algebraically closed field of characteristic $\neq 2$), the only anisotropic quadratic spaces are those of dimension one, and they are all equivalent. So the Witt ring is $W(\mathbb{C}) = \mathbb{Z}/2$.
(This remains true for algebraically closed fields $K$ of characteristic two, but those spaces are not regular so we have $W(K) = \{0\}$.)

**Example 2.23.** Over $\mathbb{R}$, a quadratic form is anisotropic if and only if it is definite (positive or negative). So an anisotropic form can be diagonalized to $\langle a_1, ..., a_n \rangle$, with $a_i$ either all positive or negative, hence is equivalent to either $\langle 1, ..., 1 \rangle$ or $\langle -1, ..., -1 \rangle$. This observation leads to an isomorphism (of rings!)

$$\text{sgn} : W(\mathbb{R}) \longrightarrow \mathbb{Z},$$

sending $Q$ to $n$ if its core form is positive definite of dimension $n$, and to $-n$ if its core form is negative definite of dimension $n$. Equivalently, if the matrix of $Q$ has $r$ positive and $s$ negative eigenvalues then $\text{sgn}(Q) = r - s$. The fact that this number is the same for equivalent quadratic forms over $\mathbb{R}$ is generally known as Sylvester's law of inertia.

**Example 2.24.** Over $\mathbb{F}_2$, all regular quadratic spaces are orthogonal direct sums of regular quadratic planes (this is true over any field of characteristic two) and over $\mathbb{F}_2$ the only regular planes are the hyperbolic plane

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

and elliptic plane

$$E(X, Y) = X^2 + XY + Y^2.$$

The form $E$ is anisotropic and $H$ is isotropic, so we definitely have $H \ncong E$. But $E \perp E$ is isotropric, and we cannot have $E \perp E \cong E \perp H$ as that would violate Witt cancellation . Hence $E \perp E$ has trivial core form and (by the uniqueness of the Witt decomposition) there must exist an isometry $E \perp E \cong H \perp H$.
In any case, we have $W(\mathbb{F}_2) \cong \mathbb{Z}/2$, where $E$ represents the nontrivial class.

**Example 2.25.** More generally, in this extended example we will work out the Witt rings of finite fields. The *Chevalley theorem* (or rather a special case of it) states that a polynomial $f$ of homogeneous degree $d$ in $n$ variables over $K$ has a nontrivial zero whenever $n > d$. In particular every quadratic form in at least three variables is isotropic. (Proof: let $q = \#K$. Expanding coefficients in the polynomial identity

$$X^q - X = \prod_{a \in K} (X - a) \in K[X]$$

implies that $\sum_{a \in K} a^n = 0$ for every $n < q - 1$. The number of zeros of $f$ is then

$$\sum_{a_1 \in K} ... \sum_{a_n \in K} \Big(1 - f(a_1, ..., a_n)^{q-1}\Big),$$

and writing out $1 - f^{q-1}$ as a sum of monomials shows that this sum is zero if $n > d$; in other words, the number of zeros of $f$ is a multiple of $\mathrm{char}(K)$. But $f$ has at least the zero $(a_1, ..., a_n) = (0, ..., 0)$, so it must have at least $\mathrm{char}(K) - 1$ other zeros.)

Hence an anisotropic space $Q$ has dimension at most two. If $\mathrm{char}(K) \neq 2$ then $Q$ can be diagonalized. Let $a \in K^\times/(K^\times)^2$ represent the (unique) nontrivial square class of $K$. Then any rank one regular form is equivalent to either $\langle 1 \rangle$ or $\langle a \rangle$, and both are anisotropic. Any rank two regular form is equivalent to one of $\langle 1, 1 \rangle$ or $\langle 1, a \rangle$ or $\langle a, a \rangle$.

The forms $\langle 1, 1 \rangle$ and $\langle a, a \rangle$ are anisotropic if and only if $-1$ is a nonsquare in $K$, or equivalently if $q = \#K \equiv 3 \pmod 4$. In this case we can take $a = -1$. Since $\langle 1, 1, 1 \rangle$ is isotropic, and $\langle 1, 1, 1 \rangle \cong H \oplus \langle 1 \rangle$ would violate Witt's theorem, we have $[\langle 1, 1, 1 \rangle] = [\langle -1 \rangle]$. But then

$$[\langle 1, 1, 1, 1 \rangle] = [\langle 1, -1 \rangle] = [0]$$

in $W(K)$, hence $[\langle -1, -1 \rangle] = [\langle 1, 1, 1, 1, 1, 1 \rangle] = [\langle -1, -1 \rangle]$, and we obtain $W(K) \cong \mathbb{Z}/4\mathbb{Z}$ (as rings) with $\langle 1 \rangle$ as a generator.

If on the other hand $q = \#K \equiv 1 (\mathrm{mod}\, 4)$, then the Witt group has elements $[0], [\langle 1 \rangle], [\langle a \rangle], [\langle 1, a \rangle]$, and since $[\langle 1 \rangle]$ and $[\langle a \rangle]$ both have order two, the ring structure can only be $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.

Finally, suppose $\mathrm{char}(K) = 2$. Then the only anisotropic regular spaces over $K$ are planes. A regular quadratic form in two variables is necessarily of the form $Q = aX^2 + bXY + cY^2$ where $b \in K^\times$, and if it is anisotropic then we must have $a, c \in K^\times$ as well. Since every element of $K$ is a square, we may assume up to equivalence that $Q = X^2 + XY + aY^2$ with $a \in K$. The equivalence class of $Q$ depends only on $a$ modulo the (additive) subgroup

$$\wp(K) := \{b^2 + b : \ b \in K\}$$

which has index two in $K$; this equivalence is realized by the substitution

$$(X, Y) \mapsto (X + bY, Y).$$

(This is related to Artin–Schreier theory. The coset $a + \wp(K)$ is a special case of the *Arf invariant*.) And since $\wp(K)$ contains $a = 0$, for which the form is isotropic, there is only one equivalence class of anisotropic forms. Hence the Witt group is

$$W(K) \cong \mathbb{Z}/2\mathbb{Z},$$

where the nontrivial Witt class is represented by any form $X^2 + XY + aY^2$ with $a$ not equal to $b^2 + b$ for $b \in K$. If $K = \mathbb{F}_2$ then we may take $a = 1$ as before.

# 3. Clifford algebra

## 3.1. Clifford algebra

Let $(M, Q)$ be a quadratic module over a ring $R$.

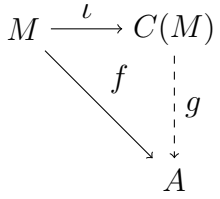
The *Clifford algebra* is a noncommutative algebra, containing the set $M$ and the ground ring $R$, in which the square of any element $x \in M$ is $Q(x)$. It is meant to be the most general such algebra in the sense that all relations can be derived from $x^2 = Q(x)$. The way to make this definition precise is through a universal property:

**Definition 3.1.** A **Clifford algebra** $C(M)$ is an associative $R$-algebra together with an $R$-module homomorphism

$$\iota : M \longrightarrow C(M)$$

that satisfies $\iota(x)^2 = Q(x)$ for $x \in M$, and for which if $A$ is any other associative algebra and $f : M \to A$ is any module homomorphism satisfying $f(x)^2 = Q(x)$, there is a unique algebra homomorphism $g : C(M) \to A$ with $f = g \circ \iota$.

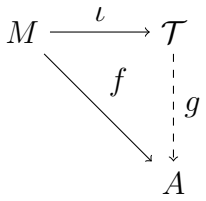
This is expressed by the commutative diagram




If a Clifford algebra for $(M, Q)$ exists, it is certainly unique up to unique isomorphism by the universal property. To construct a Clifford algebra, we begin with the tensor algebra of $M$:

$$\mathcal{T} := \bigoplus_{n=0}^{\infty} M^{\otimes n} = R \oplus M \oplus (M \otimes M) \oplus (M \otimes M \otimes M) \oplus ...$$

an associative algebra in which multiplication is given by the tensor product $\otimes$. The tensor algebra comes with an inclusion $M \to \mathcal{T}$ and satisfies a universal property: for any module homomorphism $f : M \to A$ into an associative $R$-algebra, there is a unique homomorphism of $R$-algebras $g : \mathcal{T} \to A$ such that $f = g \circ \iota$.




Let $\mathcal{I}$ be the two-sided ideal of $\mathcal{T}$ generated by all expressions of the form $x \otimes x - Q(x) \cdot 1_R$ for $x \in M$, and define the algebra

$$C := \mathcal{T}/\mathcal{I}.$$

Suppose $A$ is an associative algebra and $f : M \to A$ is a module homomorphism such that $f(x)^2 = Q(x)$ for all $x$. By the universal property of tensor algebras, there is a unique algebra homomorphism $g : \mathcal{T} \to A$ with $g(x) = f(x)$ for $x \in M$. The map $g$ sends $\mathcal{I}$ to 0 because

$$g(x \otimes x - Q(x) \cdot 1) = g(x)^2 - Q(x) = f(x)^2 - Q(x) = 0, \quad x \in M,$$

so it descends to a (unique) algebra homomorphism $\overline{g} : C \to A$ satisfying $\overline{g} \circ \iota = f$, where $\iota : M \to \mathcal{T} \to \mathcal{T}/\mathcal{I} = C$ is the natural map. This shows:

**Proposition 3.2.** *A Clifford algebra $C(M)$ for $(M, Q)$ exists and is unique up to unique isomorphism.*

**Remark 3.3.** Some basic properties of the Clifford algebra:

(i) Let $\beta(x, y) = Q(x + y) - Q(x) - Q(y)$ be the polar bilinear form of $Q$. By abuse of notation, write $x = \iota(x)$ for $x \in M$ (the justification for this will come later). Then the equation

$$x^2 = Q(x), \quad x \in M$$

implies

$$xy + yx = (x + y)^2 - x^2 - y^2 = Q(x + y) - Q(x) - Q(y) = \beta(x, y).$$

(ii) Let $(M, Q)$ be a quadratic $R$-module and let $C$ be its Clifford algebra, with homomorphism $\iota : M \to C$. Define the opposite algebra $C^{\mathrm{op}}$ to be the set $C$ with the reversed multiplication $x * y := yx$. Then the map $\iota^{\mathrm{op}} : M \to C^{\mathrm{op}}$, $x \mapsto \iota(x)$ also satisfies

$$\iota^{\mathrm{op}}(x)^2 = \iota(x)^2 = Q(x),$$

so by the universal property of Clifford algebras there is a canonical algebra homomorphism

$$J : C \longrightarrow C^{\mathrm{op}};$$

in other words, $C$ comes with a natural *anti*-automorphism

$$J : C \longrightarrow C, \quad J(xy) = J(y)J(x),$$

and it satisfies $J(\iota x) = \iota x$ for every $x \in M$.

(iii) The tensor algebra has a $\mathbb{Z}$-grading, where an element of $M^{\otimes n}$ is defined to have degree $n$. The generators of the ideal $\mathcal{I}$ do not have homogeneous degree, but their degrees are all even ($x \otimes x$ has degree two, $Q(x)$ has degree zero). So the construction above shows that $C(M)$ has a natural $\mathbb{Z}/2\mathbb{Z}$-grading:

$$C(M) = C_0(M) \oplus C_1(M),$$

where $C_0(M)$ consists of elements of even degree and $C_1(M)$ consists of elements of odd degree, and that this grading is compatible with the multiplication. In other words, $C(M)$ is a **superalgebra**.
In particular, $C_0(M)$ is itself an algebra: the **even Clifford algebra** of $(M, Q)$.

(iv) Let $f : (M_1, Q_1) \to (M_2, Q_2)$ be an isometric embedding. Composing $f$ with the map $\iota_2 : M_2 \to C(M_2)$ gives us a map $\iota_2 \circ f : M_1 \to C(M_2)$ satisfying

$$(\iota_2 f(x))^2 = Q_2(f(x)) = Q_1(x), \quad x \in M_1.$$

Hence $f$ induces an algebra homomorphism

$$C(f) : C(M_1) \longrightarrow C(M_2),$$

by the universal property of $C(M_1)$. This makes the Clifford algebra a functor.

(v) As a special case of (iv), any $\varphi \in \mathrm{O}(M)$ induces an automorphism $C(\varphi) : C \to C$ of the Clifford algebra.

**Example 3.4.** Let $M$ be a finitely generated projective $R$-module and let $Q \equiv 0$ be the trivial quadratic form on $M$. Then the Clifford algebra is the quotient $\mathcal{T}/\mathcal{I}$ by the two-sided ideal generated by all $x \otimes x$, $x \in M$. This special case of the Clifford algebra is usually known as the Grassmann algebra or exterior algebra $\wedge M$ of $M$, and multiplication in it is written $x \wedge y$.

We have not yet shown that the map from $M$ to $C(M)$ is injective, or even that the Clifford algebra $C(M)$ is nonzero (i.e. that the ideal $\mathcal{I}$ generated by expressions $x \otimes x - Q(x)$ is not the entire tensor algebra). This is not trivial. The situation is similar to (but easier than) the Poincaré–Birkhoff–Witt theorem that embeds Lie algebras in their universal enveloping algebra. We only prove the case where $M$ is free.

**Theorem 3.5.** *Suppose $(M, Q)$ is a free quadratic module with basis $e_1, ..., e_n$. Then $C(M)$ is free as an $R$-module, with basis*

$$e_{i_1} ... e_{i_r} = [e_{i_1} \otimes ... \otimes e_{i_r}], \quad 1 \le i_1 < ... < i_r \le n.$$

*In particular* $\operatorname{rank} C(M) = 2^n$.

In particular the *module* structure of $C(M)$ is essentially independent of $Q$! By comparing with the form $Q = 0$, we get an isomorphism of modules $C(M) \cong \wedge M$ with the Grassmann algebra.
It is not hard to see that these elements are a spanning set: The tensor algebra is spanned by pure tensors $e_{i_1} \otimes ... \otimes e_{i_r}$ without any restriction on the ordering of $i_1, ..., i_r$. Due to the relations $e_i e_j + e_j e_i = \beta(e_i, e_j)$ and $e_i e_i = Q(e_i)$, the Clifford algebra is spanned, modulo products of shorter length, by terms $e_{i_1} ... e_{i_r}$ with $i_1 < ... < i_r$. The essential point is that those products are linearly independent.

The main step of the proof is the following lemma (which is useful anyway):

**Lemma 3.6.** *Suppose $M = M_1 \perp M_2$. Then*

$$C(M) = C(M_1) \hat{\otimes} C(M_2),$$

*where $C(M_1)\hat{\otimes}C(M_2)$ is the algebra which has $C(M_1) \otimes C(M_2)$ (tensor of modules) as its underlying $R$-module, and where the multiplication is defined on pure tensors by*

$$(x_1 \otimes x_2)(y_1 \otimes y_2) = (-1)^{ij}(x_1 y_1) \otimes (x_2 y_2)$$

*if $x_2$ has degree $i$ and $y_1$ has degree $j$.*

N.B. This is the usual definition of tensor product of superalgebras.

*Proof.* This is proved by showing that $C(M_1)\hat{\otimes}C(M_2)$ satisfies the universal property of Clifford algebras. Let $\iota_i : M_i \to C(M_i)$ be the maps that come with $C(M_i)$, and define the linear map

$$\iota : M_1 \perp M_2 \longrightarrow C(M_1) \otimes C(M_2), \quad v_1 + v_2 \mapsto \iota_1(v_1) \otimes 1 + 1 \otimes \iota_2(v_2)$$

for $v_i \in M_i$. Let $f : M \to A$ be any module homomorphism into an associative algebra for which $f(x)^2 = Q(x)$ for all $x \in M$. From the restrictions of $f$ to $M_1$ and $M_2$ and the universal properties of $C(M_i)$, we obtain unique algebra homomorphisms

$$g_i : C(M_i) \longrightarrow A \quad \text{with } g_i(\iota x_i) = f(x_i), \quad x_i \in M_i.$$

These yield a unique *module* homomorphism

$$g : C(M_1) \otimes C(M_2) \longrightarrow A$$

with the property

$$g(x_1 \otimes x_2) = g_1(x_1) \cdot g_2(x_2), \quad x_1 \in C(M_1),\ x_2 \in C(M_2).$$

It is in fact an algebra homomorphism, because: note that in $A$, the identity $f(v)^2 = Q(v)$ implies

$$f(v)f(w) + f(w)f(v) = \beta(v, w), \quad v, w \in M.$$

If $v \in M_1$ and $w \in M_2$ then $\beta(v,w) = 0$ implies

$$f(v)f(w) = -f(w)f(v).$$

Then the fact that $g_1, g_2$ are algebra homomorphisms and $\iota_i(M_i)$ generates $C(M_i)$ gives us the general super-commutativity rule:

$$g_1(x)g_2(y) = (-1)^{ij} g_2(y)g_1(x), \quad x \in C_i(M_1),\ y \in C_j(M_2).$$

Hence

$$\begin{aligned} g((x_1 \otimes x_2)(y_1 \otimes y_2)) &= (-1)^{ij} g(x_1 y_1 \otimes x_2 y_2) \\ &= (-1)^{ij} g_1(x_1)g_1(y_1)g_2(x_2)g(y_2) \\ &= g_1(x_1)g_2(x_2)g_1(y_1)g_2(y_2) \\ &= g(x_1 \otimes x_2)g(y_1 \otimes y_2) \end{aligned}$$

for any $x_1, y_1 \in C(M_1)$ and $x_2, y_2 \in C(M_2)$ if $x_2$ has degree $i$ and $y_1$ has degree $j$.

By construction, the algebra homomorphism $g$ satisfies

$$g(\iota(v_1 + v_2)) = g_1(\iota_1 v_1) \otimes 1 + 1 \otimes g_2(\iota_2 v_2) = f(v_1) + f(v_2) = f(v_1 + v_2)$$

for any $v_1 \in M_1$, $v_2 \in M_2$. It is uniquely determined from the fact that

$$g(x_1 \otimes x_2) = \pm g((x_1 \otimes 1)(1 \otimes x_2)) = \pm g_1(x_1)g_2(x_2)$$

and the uniqueness of $g_1, g_2$. □

*Proof.* [Proof of Theorem 3.5] Via two reduction steps, we will eventually reduce to the case of fields of characteristic $\neq 2$, which is simpler.

(1) Suppose $R = K$ is a field of characteristic $\mathrm{char}(K) \neq 2$. Then $M$ can be diagonalized:

$$M = \coprod_{i=1}^{n} (Re_i)$$

and its Clifford algebra splits as a superalgebra tensor product:

$$C(M) = \hat{\bigotimes} C(Re_i).$$

For a one-dimensional quadratic module $R \cdot e$, the Clifford algebra has a single generator $e$ and a single relation $e^2 = Q(e)1$, so as a module

$$C(R \cdot e) = R \oplus Re.$$

Therefore, on the level of $R$-modules,

$$C(M) = (R \oplus Re_1) \otimes (R \oplus Re_2) \otimes ... \otimes (R \oplus Re_n)$$

which has the claimed basis.

(2) Reduction to fields. Suppose $R$ is an integral domain of characteristic $\mathrm{char}(R) \neq 2$ and let $K$ be its field of fractions. We can pass from $M$ to the $K$-quadratic module $M \otimes_R K$. The construction as a quotient of the tensor algebra yields

$$C(M \otimes_R K) = C(M) \otimes_R K.$$

By (1) the elements $e_{i_1}...e_{i_r}$, $i_1 < ... < i_r$ are linearly independent, viewed as elements of $C(M \otimes_R K) = C(M) \otimes_R K$. Hence they must also be linearly independent in $C(M)$.

(3) Reduction to $\mathrm{char}(R) \neq 2$. Let $R$ be an integral domain with $\mathrm{char}(R) = 2$, and write $R = S/\mathfrak{a}$ where $\mathrm{char}(S) = 0$ and $\mathfrak{a}$ is an appropriate ideal. (For example, one can use the group algebra $S = \mathbb{Z}[R]$ and take $\mathfrak{a}$ as the kernel of the map that sends each basis element $\mathfrak{e}_x$ to $x$, $x \in R$.) Let $M'$ be the free $S$-module with formal basis $e'_1, ..., e'_n$ and identify

$$M \cong M'/(\mathfrak{a} \cdot M'), \quad e_i \mapsto e'_i + \mathfrak{a} \cdot M',$$

and choose a quadratic form $Q'$ on $M'$ for which

$$Q'(e'_i) + \mathfrak{a} = Q(e_i).$$

By (2), the Clifford algebra $C(M')$ of $(M', Q')$ is free on the basis $e'_{i_1}...e'_{i_r}$, $i_1 < ... < i_r$. It follows that $C(M')/(\mathfrak{a} \cdot C(M'))$ is a free $R$-module on the basis $e'_{i_1}...e'_{i_r} + \mathfrak{a} \cdot C(M')$. Now the $R$-linear map

$$f : M \longrightarrow C(M')/(\mathfrak{a} \cdot C(M')), \quad e_i \mapsto e'_i + \mathfrak{a} \cdot C(M')$$

satisfies

$$\begin{aligned} f(x)^2 &= \Big( \sum_i x_i e'_i + \mathfrak{a} \cdot C(M') \Big)^2 \\ &= \sum_i x_i^2 Q'(e'_i) + \sum_{i,j} x_i x_j \beta'(e'_i, e'_j) + \mathfrak{a} \cdot C(M') \\ &= Q' \Big( \sum_i x_i e'_i \Big) + \mathfrak{a} \cdot C(M') \\ &= Q(x) \end{aligned}$$

for every $x = \sum_i x_i e_i \in M$. By the universal property of Clifford algebras, there is an algebra homomorphism

$$h : C(M) \longrightarrow C(M')/(\mathfrak{a} \cdot C(M'))$$

with $h(e_i) = e'_i + \mathfrak{a} \cdot C(M')$. Since the images of $h(e_{i_1}...e_{i_r})$ $(i_1 < ... < i_r)$ are linearly independent in $C(M')/(\mathfrak{a} \cdot C(M'))$, it follows that $e_{i_1}...e_{i_r}$ themselves are linearly independent in $C(M)$. $\square$

**Remark 3.7.** The module isomorphism $C(M) \cong \wedge M$ with the exterior algebra and the fact that $M$ injects into $C(M)$ hold even when $M$ is not free. We omit the proof[1].

## 3.2. The Clifford algebra of a plane

In this section we will study the Clifford algebra of a free rank two module in more detail. For a quadratic module $(M, Q)$, we identify $M$ with its image in the Clifford algebra $C(M)$.

**Example 3.8.** Let $(M, Q)$ be a free quadratic module of rank two with basis $e_1, e_2$. The even Clifford algebra $C_0$ is then spanned by 1 and $z = e_1 e_2$. The antiautomorphism $J$ of 3.3 maps $J(1) = 1$ and $J(z) = e_2 e_1$, and we have

$$z + Jz = \beta(e_1, e_2), \quad z(Jz) = Q(e_1) \cdot Q(e_2),$$

so if $X$ is a formal indeterminate then $(X - z)(X - Jz) = X^2 - bX + ac$ where

$$b = \beta(e_1, e_2),\ a = Q(e_1),\ c = Q(e_2),$$

i.e. where $Q = \begin{pmatrix} a & b \\ & c \end{pmatrix}$. Therefore the even Clifford algebra is

$$C_0 \cong R[X]/(X^2 - bX + ac).$$

Recall that if $C$ is an algebra (say the Clifford algebra $C(M)$) and $X \subseteq C$ is a subset then

$$C^X = \{y \in C :\ yx = xy \text{ for all } x \in X\}$$

denotes the centralizer of $X$.

The centralizer of the even algebra $C_0$ turns out to play an important role. Suppose $M$ is *regular* and free of rank two, and choose a basis $e, f \in M$ with $\beta(e, f) = b \neq 0$. Then $C_0$ is spanned by 1 and $ef$, and $C^{C_0}$ is just the centralizer of $ef$. That element satisfies

$$vef = fev \quad \text{for every } v \in M,$$

as one can check on the basis elements $v = e, f$; and since $fe = b - ef \neq ef$, it follows that $ef$ does not commute with any element of odd degree. So

$$C^{C_0} = C_0 = R \cdot 1 + R \cdot ef.$$

From this one obtains further that the center $C^C$ is just $R \cdot 1$.

**Example 3.9.** Let's look at two examples:
(i) Take $R = \mathbb{R}$, and let $Q$ be the quadratic form

$$Q(X, Y) = -X^2 - Y^2.$$

[1]See section II.2 of R. Baeza, *Quadratic forms over semilocal rings*, Lecture Notes in Mathematics **655**, Springer-Verlag 1978.

If $e_1, e_2$ is the standard basis of $\mathbb{R}^2$, and we denote $i = e_1$, $j = e_2$ and $k = e_1, e_2$, then the Clifford algebra is the vector space with basis $1, i, j, k$, and the multiplication satisfies

$$i^2 = Q(1,0) = -1, \quad j^2 = Q(0,1) = -1,$$
$$ijk = k^2 = e_1e_2e_1e_2 = -e_1e_1e_2e_2 = -(-1)(-1) = -1.$$

These are the defining equations for the quaternions $\mathbb{H}$.

(ii) Let $R = K$ be any field and $M = H$ the hyperbolic plane with standard basis $e, f$. The Clifford algebra has basis $1, e, f, ef$ with the multiplication

$$e^2 = f^2 = 0, \quad ef + fe = 1.$$

This is isomorphic to the algebra of $(2 \times 2)$-matrices over $R$ via the map

$$e \mapsto \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}, \quad f \mapsto \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix}.$$

Both are examples of *central simple algebras*, that is, finite-dimensional $K$-algebras whose center is exactly $R$ and which have no proper two-sided ideals other than 0. This is true for regular quadratic spaces in general:

**Lemma 3.10.** *Let $(M, Q)$ be a regular quadratic space over a field $K$ and that $M$ is free of rank two. Then the Clifford algebra $C = C(M)$ is a central simple algebra.*

*Proof.* Suppose $I \subseteq C$ is a two-sided ideal that contains a nonzero element $x = x_0 + x_1$, where $x_0 \in C_0$ and $x_1 \in C_1$, and suppose without loss of generality that $x_1 \neq 0$ (otherwise, multiply it by any $v \in M$ with $Q(v) \in R^\times$). Let $e, f \in M$ be a basis and write $a = Q(e)$, $b = \beta(e, f)$, $c = Q(f)$. Then one can compute

$$\begin{aligned}(ef - fe)(ef - fe) &= efef + fefe - 2 * ac \\ &= (b - fe)ef + (b - ef)fe - 2 * ac \\ &= b(ef + fe) - 4 * ac \\ &= b^2 - 4ac.\end{aligned}$$

Up to sign, this is the determinant of the Gram matrix $\begin{pmatrix} 2a & b \\ b & 2c \end{pmatrix}$ in the basis $e, f$ and in particular it is a unit. Since $I$ contains the element

$$xef - efx = x_1ef - efx_1 = x_1(ef - fe),$$

it also contains $x_1$ itself. But then if $y \in M$ is any element with $\beta(x_1, y) = 1$, we obtain

$$1 = \beta(x_1, y) = x_1y + yx_1 \in I$$

and therefore $I$ is the entire ring. □

A central simple algebra $C/K$ with $\dim_K C = 4$ is also called a **quaternion algebra**. So Clifford algebras of two-dimensional regular quadratic spaces are quaternion algebras. If $\mathrm{char}(K) \neq 2$ and $Q = aX^2 + bY^2$ is a diagonal quadratic form, then $C$ has basis $1$, $i := e_1$, $j := e_2$, $k := e_1e_2$ with multiplication

$$i^2 = a, \quad j^2 = b, \quad ij = -ji = k;$$

this algebra is denoted by the symbol $\left(\frac{a,b}{K}\right)$.

## 3.3. Discriminant algebra and center

We will now discuss the center and the centralizer of $C_0$ in a general Clifford algebra.

Let $R$ be a local ring or field, and let $(M, Q)$ be a quadratic $R$-module with Clifford algebra $C$. As usual we identify $M$ with its image in $C$.

**Definition 3.11.** The **discriminant algebra** $\Delta(M)$ of $(M, Q)$ is the centralizer of $C_0$ in $C$:

$$\Delta(M) = C^{C_0} = \{x \in C : \ xz = zx \text{ for all } z \in C_0\}.$$

$\Delta(M)$ is easiest to describe in the case $2 \in R^\times$. In this case, any regular quadratic space over $R$ can be orthogonally diagonalized:

$$M = \bigperp_{i=1}^{n} Re_i, \quad \beta(e_i, e_j) = 0 \text{ for } i \neq j.$$

The equation $\beta(e_i, e_j) = 0$ means that the Clifford product satisfies $e_ie_j = -e_je_i$. If $I = \{i_1, ..., i_r\}$ is a set of indices with $i_1 < ... < i_r$, and the Clifford product is denoted

$$e_I := e_{i_1}...e_{i_r},$$

then this computation shows that

$$e_je_I = (-1)^{|I|}e_Ie_j \text{ if } j \notin I.$$

On the other hand, since $e_j$ does commute with itself, we have

$$e_je_I = (-1)^{|I|-1}e_Ie_j \text{ if } j \in I.$$

This implies that for any two indices $i, j$,

$$e_ie_je_I = \begin{cases} e_Ie_ie_j : & \text{either } i, j \in I \text{ or } i, j \notin I; \\ -e_Ie_ie_j : & \text{either } i \in I, j \notin I \text{ or } i \notin I, j \in I. \end{cases}$$

In particular, the longest Clifford product

$$z := e_1e_2...e_n$$

commutes with all products $e_ie_j$, $1 \le i < j \le n$; conversely, every other Clifford product (besides the trivial 1) anticommutes with at least one pair $e_ie_j$. Since the $e_ie_j$ generate the even Clifford algebra $C_0$, we obtain:

**Proposition 3.12.** *Suppose $R$ is a field or local ring, $2 \in R^\times$, and let $e_1, ..., e_n$ be an orthogonal basis of a regular quadratic space $(M, Q)$. Then*

$$\Delta(M) = R \oplus Rz, \quad z = e_1e_2...e_n.$$

The algebra structure of $\Delta(M)$ is determined by

$$\begin{aligned} z^2 &= e_1...e_ne_1...e_n = (-1)^{r-1}e_1^2e_2...e_ne_2...e_n \\ &= ... = \Big(\prod_{i=1}^{r}(-1)^{i-1}\Big)Q(e_1)...Q(e_n) \\ &= (-1)^{r(r-1)/2}Q(e_1)...Q(e_n) \end{aligned}$$

where $r = \operatorname{rank}(M)$, so

$$\Delta(M) \cong R[X]/(X^2 - d)$$

where $d = (-1)^{r(r-1)/2} \cdot \operatorname{disc}(e_1, ..., e_n)$ is the signed discriminant in the basis $e_1, ..., e_n$. (Hence the name discriminant algebra.) Conversely, the isomorphism class of the $R$-algebra $\Delta(M)$ uniquely determines the discriminant as an element of $(R^\times)/(R^\times)^2$.

**Corollary 3.13.** *Suppose $R$ is a local ring, $2 \in R^\times$, and let $e_1, ..., e_n$ be an orthogonal basis of a regular quadratic space $M$. Let $z = e_1...e_n$.*
*(i) The center of $C$ is*

$$\begin{cases} R: & n \equiv 0\,(2); \\ R \oplus Rz: & n \equiv 1\,(2). \end{cases}$$

*(ii) The center of $C_0$ is*

$$\begin{cases} R \oplus Rz: & n \equiv 0\,(2); \\ R: & n \equiv 1\,(2). \end{cases}$$

*Proof.* (i) Since $e_ize_i^{-1} = (-1)^{n-1}z$, it follows that $z$ commutes with all $C$ if and only if $n$ is odd.
(ii) We have $C_0^{C_0} = C_0 \cap C^{C_0}$, and $z \in C_0$ if and only if $n$ is even. □

If $2 \notin R^\times$, then for regular quadratic spaces we only have a decomposition into planes $M = \perp_{i=1}^{n} E_i$, $\operatorname{rank}(E_i) = 2$. We have to reduce the computation of $\Delta(M)$ to the computation of $\Delta(E_i)$, which was essentially done in the previous section: if $e, f$ is a basis of $E_i$ and $a = Q(e)$, $b = \beta(e, f)$, $c = Q(f)$ then

$$\Delta(E_i) = R[X]/(X^2 - bX + ac).$$

**Lemma 3.14.** *Let $(M, Q)$ be a regular quadratic space. There is a unique automorphism $\alpha$ of $\Delta(M)$ with the property*

$$xz = \alpha(z)x, \quad x \in M,$$

*and it satisfies $\alpha^2 = \mathrm{id}$.*

For example, if $\mathrm{rank}(M) = 2$ then $\alpha$ is the natural *anti*automorphism $J$ of $C$, restricted to $\Delta(M)$.

*Proof.* Let $e \in M$ be any element with $e^2 = Q(e) = a \in R^\times$ (this exists since $M$ is regular). Then $\alpha$ is uniquely determined by

$$\alpha(z) = \alpha(z)e^2a^{-1} = ezea^{-1}, \quad z \in C^{C_0}.$$

This definition satisfies

$$\alpha(z)x = ezexa^{-1} = e(ex)za^{-1} = xz$$

for every $x \in M$, since $z$ commutes with $ex \in C_0$ by definition, and we have

$$\alpha(\alpha z) = e(eze)ea^{-2} = Q(e)zQ(e)a^{-2} = z.$$

It maps $\Delta(M)$ into itself, because

$$\alpha(z)xy = xzy = x\alpha(\alpha(z))y = xy\alpha(z)$$

for any $x, y \in M$ and because the products $xy$ generate $C_0$. It is an algebra homomorphism, since $\alpha(zw) = ezwea^{-1} = eze^2wea^{-2} = \alpha(z)\alpha(w)$ for $z, w \in C^{C_0}$. □

**Lemma 3.15.** *Let $M = M_1 \perp M_2$ be a regular quadratic space over $R$, $2 \notin R^\times$, where $M_1, M_2$ are regular, and let $\alpha_i$ be the automorphism of $\Delta(M_i)$ constructed in the previous lemma. Then*

$$\Delta(M) = \{z \in \Delta(M_1) \otimes \Delta(M_2) : \ (\alpha_1 \otimes -I)(z) = (-I \otimes \alpha_2)(z)\}.$$

*If*

$$\Delta(M_i) = R \oplus Rz_i \cong R[X]/(X^2 - X + c_i), \ i = 1, 2,$$

*then*

$$\Delta(M) = R \oplus Rz \cong R[X]/(X^2 - X + c), \quad c = c_1 + c_2 - 4c_1c_2,$$

*where $z = z_1 \otimes z_2 + \alpha_1(z_1) \otimes \alpha_2(z_2)$, and the involution $\alpha$ of $\Delta(M)$ maps*

$$\alpha(z) = z_1 \otimes \alpha_2(z_2) + \alpha_1(z_1) \otimes z_2.$$

Here we view $\Delta(M_1) \otimes \Delta(M_2)$ as a subalgebra of $C(M) = C(M_1)\hat{\otimes}C(M_2)$, and $-I$ is the automorphism of $C(M_i)$ induces by $-\mathrm{id}$; i.e. $-I$ acts as $(-1)^j$ on elements of degree $j$. Note that this value of $c$ satisfies

$$1 - 4c = (1 - 4c_1)(1 - 4c_2).$$

The proof is more or less a direct computation; see II.7.8 in Kneser for details.

From the decomposition $M = \perp_{i=1}^{n} E_i$, we obtain:

**Theorem 3.16.** *Let $M$ be a regular quadratic space over a local ring $R$, $2 \notin R^\times$ and write $M = \perp_{i=1}^{m} E_i$ with $\mathrm{rank}(E_i) = 2$. Suppose each $E_i$ has basis $e_{2i-1}, e_{2i}$ with $Q(e_{2i-1}) = a_i$, $\beta(e_{2i-1}, e_{2i}) = 1$, $Q(e_{2i}) = c_i$. Then*

$$\Delta(M) \cong R \oplus Rz = R[X]/(X^2 - X + c)$$

*where*

$$1 - 4c = \prod_{i=1}^{m}(1 - 4a_ic_i) = (-1)^m \cdot \mathrm{disc}(e_1, ..., e_{2m})$$

*is the signed discriminant in the basis $e_1, ..., e_{2m}$. The basis element $z$ can be chosen such that $z + \alpha(z) = 1$ and $z\alpha(z) = c$.*

## 3.4. The spin group

The spin group is a double cover of the special orthogonal group. In this section we will define both of those groups. (The definition of SO is somewhat subtle over a field of characteristic two.)

**Example 3.17.** For a concrete example of spin group, let $K = \mathbb{R}$ and consider the space $V = \mathbb{R}^{2\times 2}$ of matrices of size two. This becomes a quadratic space where the quadratic form is given by the determinant. Its orthogonal group contains left- and right-multiplication maps

$$L_A : X \mapsto AX, \quad R_A : X \mapsto XA$$

where $A \in \mathrm{SL}_2(\mathbb{R})$; and in fact these transformations generate the special orthogonal group: so we have a surjective map

$$\mathrm{SL}_2(\mathbb{R}) \times \mathrm{SL}_2(\mathbb{R}) \longrightarrow \mathrm{SO}(\det), \quad (A, B) \mapsto [X \mapsto AXB].$$

But this map has a kernel: $(-I, -I)$ acts trivially. Hence $\mathrm{SL}_2(\mathbb{R}) \times \mathrm{SL}_2(\mathbb{R})$ is a double cover of $\mathrm{SO}(\det) = \mathrm{SO}(2, 2; \mathbb{R})$.

To define general spin groups, we use the Clifford algebra.

Let $(M, Q)$ be a regular quadratic space over a field or local ring $R$, and view $M$ as a submodule of its Clifford algebra $C$. Fix an element $z$ such that

$$\Delta(M) = R \oplus Rz;$$

as we saw earlier, if $M = \perp_{i=1}^{n} Re_i$ is diagonalizable then we take

$$z = e_1 ... e_n$$

to be the longest Clifford product, and if $M = \perp_{i=1}^{n} E_i$, $E_i = Re_{2i-1} \oplus Re_{2i}$ with $\beta(e_{2i-1}, e_{2i}) = 1$ in the case that 2 is a nonunit, then we take $z$ such that $z + \alpha(z) = 1$ where

$$\alpha(z)x = xz \quad \text{for } z \in \Delta(M),\ x \in M.$$

An orthogonal transformation $\varphi \in \mathrm{O}(M)$ can be viewed as a homomorphism

$$\varphi : M \longrightarrow C$$

satisfying

$$\varphi(x)^2 = Q(\varphi x) = Q(x),$$

and it induces, by the universal property, an algebra automorphism $C(\varphi) : C \to C$. Conversely, if $u \in \mathrm{Aut}(C)$ is an automorphism of $C$ that maps $M$ into itself, then for $x \in M$ we have

$$Q(u(x)) = u(x)^2 = u(x^2) = u(Q(x)) = Q(x)$$

and therefore $u|_M \in \mathrm{O}(M)$. Hence we have an identification

$$\mathrm{O}(M) \cong \{u \in \mathrm{Aut}(C) :\ u(M) = M\}.$$

We will fix the following definition now and explain it later:

**Definition 3.18.** The **special orthogonal group** $\mathrm{SO}(M)$ is the stabilizer of $z$:

$$\mathrm{SO}(M) = \{\varphi \in \mathrm{O}(M) :\ \varphi(z) = z\}.$$

The motivation for this definition comes from reflections,

$$\sigma_x : y \mapsto y - \frac{\beta(x, y)}{Q(x)} x, \quad x \in M \text{ with } Q(x) \in R^\times.$$

Any $r \in M$ with $Q(r) \in R^\times$ is invertible in the Clifford algebra, with inverse $r^{-1} = r/Q(r)$, and it comes with an inner automorphism

$$i_r \in \mathrm{Aut}(C), \quad i_r(x) = rxr^{-1}.$$

The automorphism $i_r$ and the reflection $\sigma_r$ are related via

$$\begin{aligned} i_r(x) &= rxr^{-1} \\ &= -(xr - \beta(x, r))r/Q(r) \\ &= -x + \frac{\beta(x, r)}{Q(r)} r \qquad (3.1) \\ &= -\sigma_r(x), \quad x \in M; \qquad (3.2) \end{aligned}$$

that is, $i_r$ is exactly the automorphism of $C$ induced by $-\sigma_r$.

By definition, the involution $\alpha$ of Lemma 3.14 satisfies

$$xz = \alpha(z)x, \quad x \in M,$$

and we have $\alpha(z) = (-1)^{n-1}z$ if $2 \in R^\times$ and $n = \operatorname{rank}(M)$ and $\alpha(z) = 1 - z$ otherwise. So $\sigma_r$ acts on $z$ via

$$\sigma_r(z) = C(-1)i_r(z) = C(-1)\alpha(z) = \begin{cases} -z: & 2 \in R^\times; \\ 1-z: & 2 \notin R^\times. \end{cases}$$

This immediately implies:

**Proposition 3.19.** *Suppose* $\mathrm{O}(M)$ *is generated by reflections. Then* $\mathrm{SO}(M)$ *has index two in* $\mathrm{O}(M)$*, and it consists exactly of products of an even number of reflections.*

**Corollary 3.20.** *If* $R$ *is a local ring with* $\operatorname{char}(R) \neq 2$*, then*

$$\mathrm{SO}(M) = \{\varphi \in \mathrm{O}(M) : \det \varphi = 1\}.$$

If $R = K$ is a field of characteristic two, then any $\varphi \in \mathrm{O}(M)$ satisfies $\varphi z = z + D(\varphi)$ for some number $D(\varphi) \in \mathbb{Z}/2\mathbb{Z}$. This follows for all cases except $H \perp H$ over $\mathbb{F}_2$ by the above observation, since $\mathrm{O}(M)$ is then a reflection group. It remains true in the exceptional case as well (one can check this directly, or apply the Skolem–Noether theorem that automorphisms of central simple algebras are inner).
The number $D(\varphi)$ is called the **Dickson invariant** of $\varphi$; by this observation, it defines an isomorphism

$$D : \mathrm{O}(M)/\mathrm{SO}(M) \longrightarrow \mathbb{Z}/2\mathbb{Z}$$

and is therefore an "additive" analog of the determinant in characteristic two.

Generalizing beyond reflections, we have:

**Definition 3.21.** (i) The **Clifford group** $\Gamma$ is the subgroup of units $a \in C^\times$ for which the (twisted) inner automorphism

$$i_a : C \longrightarrow C, \quad y \mapsto \overline{a}ya^{-1}$$

maps $M$ into itself.
(ii) The **even Clifford group** is $\Gamma_0 := C_0 \cap \Gamma$.

Here we abbreviate $\overline{a} = C(-1)a$. So if $a = a_0 + a_1$ where $a_0$ is even and $a_1$ is odd, then $\overline{a} = a_0 - a_1$.

By definition, the map $a \mapsto i_a|_M$ defines a group homomorphism

$$\Gamma \to \mathrm{O}(M)$$

that restricts to a group homomorphism

$$\Gamma_0 \to \mathrm{SO}(M).$$

From now on, let $R = K$ be a field.

**Proposition 3.22.** *Let $(M, Q)$ be a regular quadratic space over a field $K$, $\mathrm{char}(K) \neq 2$. Then there are exact sequences*

$$1 \longrightarrow K^\times \longrightarrow \Gamma \longrightarrow \mathrm{O}(M) \longrightarrow 1$$

*and*

$$1 \longrightarrow K^\times \longrightarrow \Gamma_0 \longrightarrow \mathrm{SO}(M) \longrightarrow 1$$

*and therefore $\mathrm{O}(M) \cong \Gamma/K^\times$ and $\mathrm{SO}(M) \cong \Gamma_0/K^\times$.*

This also holds when $\mathrm{char}(K) = 2$ but we will not prove this.

*Proof.* The kernel of the map $a \mapsto i_a|_M$ consists of elements

$$a = a_0 + a_1 \in C^\times, \quad a_0 \in C_0,\ a_1 \in C_1$$

that satisfy

$$(a_0 - a_1)y = y(a_0 + a_1) \text{ for all } y \in M,$$

i.e. for which $a_0 y = y a_0$ and $a_1 y = -y a_1$. The equation $a_0 y = y a_0,\ y \in M$ implies that $a_0$ is central of even degree and therefore a scalar. Meanwhile $a_1 y = -y a_1$ implies that $a_1 xy = xy a_1$ for all $x, y \in M$, so $a_1$ belongs to $C^{C_0} = K \oplus Kz$.
Since $a_1$ is odd, it actually belongs to $Kz$; and if $a_1 \neq 0$, then necessarily $z$ is odd. But in this case $z \in C^C$ is central and the equation $a_1 y = -y a_1$ is a contradiction. So $a_1 = 0$ and $a = a_0 \in K^\times$.

The map to $\mathrm{O}(M)$ is surjective since $\mathrm{O}(M)$ is already generated by reflections $i_a|_M$, $a \in M \cap C^\times$. Hence we have the exact sequence

$$1 \longrightarrow K^\times \longrightarrow \Gamma \longrightarrow \mathrm{O}(M) \longrightarrow 1$$

and therefore the exact sequence

$$1 \longrightarrow K^\times \longrightarrow \Gamma_0 \longrightarrow \mathrm{SO}(M) \longrightarrow 1. \qquad \square$$

The Clifford group $\Gamma$ is too large. We will consider only the subgroup of elements of so-called unit norm:

**Lemma 3.23.** *Let $a \in \Gamma$. Then $N(a) := a\overline{(Ja)} \in K^\times$ is a scalar, called its* ***norm****.*

$J$ is, as always, the natural antiautomorphism of $C$ that reverses the order in Clifford products, and $\overline{a_0 + a_1} = a_0 - a_1$.
Bear in mind that $a \cdot J\overline{a}$ does not land in $K$ for arbitrary $a \in C$. The norm is only meaningful on $\Gamma$.

*Proof.* Applying the antiautomorphism $J$ to the equation

$$\iota_a(x) = \overline{a}xa^{-1} = y, \quad x, y \in M,$$

we get

$$J(a)^{-1}xJ(\overline{a}) = y$$

and therefore

$$\overline{a}(Ja)y(aJ\overline{a})^{-1} = \overline{a}xa^{-1} = y$$

for every $y \in M$. It follows that $a\overline{(Ja)}$ belongs to the kernel of the map $\Gamma \to \mathrm{O}(M)$, which we proved consists only of scalars. □

The norm satisfies $N(ab) = abJ(\overline{ab}) = abJ(\overline{b})J(\overline{a}) = N(a)N(b)$ for $a, b \in \Gamma$; i.e. it is a group homomorphism

$$N : \Gamma \longrightarrow R^\times.$$

So its kernel is also a group.

**Definition 3.24.** (i) The **spin group** is

$$\mathrm{Spin}(M) = \{a \in \Gamma_0 : \ N(a) = 1\}.$$

(ii) The **pin group** is

$$\mathrm{Pin}(M) = \{a \in \Gamma : \ N(a) = 1\}.$$

The exact sequence

$$1 \longrightarrow K^\times \longrightarrow \Gamma_0 \longrightarrow \mathrm{SO}(M) \longrightarrow 1$$

descends to an exact sequence

$$1 \longrightarrow \mu_2(K) \longrightarrow \mathrm{Spin}(M) \longrightarrow \mathrm{SO}(M).$$

The final map in the sequence is not generally surjective.

Since $N : \Gamma \to K^\times$ maps $K^\times$ into $(K^\times)^2$, it induces a homomorphism:

**Definition 3.25.** The **spinor norm** is the group homomorphism

$$N : \mathrm{O}(M) \longrightarrow K^\times/(K^\times)^2, \quad \sigma_x \mapsto N(x) \cdot (K^\times)^2.$$

For a reflection $\sigma_x$ with $x \in M$, $Q(x) \in K^\times$, the norm of $x$ is

$$N(x) = -xJ(x) = -x^2 = -Q(x).$$

So the spinor norm of $\sigma_x$ is simply the class of $-Q(x)$ modulo squares. (The minus sign is a slightly annoying convention that is used to make $N$ a homomorphism even for non-homogeneous elements of $\Gamma$.) So the exact sequence actually goes

$$1 \longrightarrow \mu_2(K) \longrightarrow \mathrm{Spin}(M) \longrightarrow \mathrm{SO}(M) \xrightarrow{N} \mathbb{Q}^\times/(\mathbb{Q}^\times)^2.$$

## 3.5. The Witt invariant

Let $K$ be a field.

Recall that for a regular quadratic space $(M, Q)$ of dimension two over $K$, we proved that the Clifford algebra $C(M)$ is a central simple algebra over $K$. In the case of a hyperbolic plane $H$, we observed that $C(H)$ is the algebra $K^{2\times 2}$ of $(2 \times 2)$-matrices.

The property of being a central simple algebra is preserved under tensor product. However, Clifford algebras only make super tensor products out of orthogonal direct sums:

$$C(M_1 \perp M_2) = C(M_1)\hat{\otimes}C(M_2),$$

with multiplication

$$(x_1 \otimes x_2)(y_1 \otimes y_2) = (-1)^{ij}(x_1y_1) \otimes (x_2y_2)$$

if $x_1, y_1 \in C(M_1),\ x_2, y_2 \in C(M_2),\ \deg(x_2) = i,\ \deg(y_1) = j.$

To fix this in the case $\dim(M_1)$ is even, recall that $\Delta(M_1) = K \oplus Kz_1$ with an element that satisfies $xz_1 = \alpha_1(z_1)x$ for any $x \in C(M_1)$ of odd degree. Hence $K$ is the center of $C(M_1)$, while if we define $z := \alpha_1(z_1) - z_1$ then $z$ and its scalar multiples are the only elements that satisfy $zx = (-1)^{\deg(x)}xz$ for every homogeneous $x \in C(M_1)$. It follows that the algebras $C(M_1) \otimes 1$ and

$$1 \otimes C_0(M_2) \oplus z \otimes C_1(M_2)$$

commute with one another; and since their dimensions match as well, we have an isomorphism

$$C(M_1 \perp M_2) \cong C(M_1) \otimes \Big(1 \otimes C_0(M_2) \oplus z \otimes C_1(M_2)\Big).$$

But $1 \otimes C_0(M_2) \oplus z \otimes C_1(M_2)$ is nothing other than the Clifford algebra of the quadratic module $\{z \otimes x : \ x \in M_2\}$, which is $M_2$ with its quadratic form rescaled by

$$Q(z) = z^2 = (\alpha_1(z_1) - z_1)^2 = d_1,$$

the signed discriminant of $M_1$. We record this observation in the following lemma:

**Lemma 3.26.** *Let $M = M_1 \perp M_2$ be a regular quadratic space with $r = \dim M_1$ even. Then*

$$C(M) \cong C(M_1) \otimes C(M_2(d_1)),$$

*where $M_2(d_1)$ is $M_1$ with its quadratic form multiplied by*

$$d_1 = (-1)^{r(r-1)/2}\mathrm{disc}(M_1),$$

*the signed discriminant of $M_1$.*

$d_1$ is only determined modulo $(K^\times)^2$ but any two choices of $d_1$ yield equivalent modules $M_2(d_1)$.

**Remark 3.27.** Lemma 3.26 and the fact that tensor products of CSAs are again CSA implies that the Clifford algebra of any even-dimensional regular quadratic space is a central simple algebra.

If $(M, Q)$ is an odd-dimensional semiregular quadratic space, the candidate for a CSA is the even subalgebra $C_0(M)$ as this is known to have exactly $K$ as its center. In fact, if we can write $M = N \perp Ke$ where $N$ is regular and $e \in M$ has $Q(e) \in K^\times$, then

$$C_0(M) = C_0(N) \otimes 1 \oplus C_1(N) \otimes e$$

is just $C(N(\delta))$ with $\delta = -Q(e)$. (Note that $(xe)^2 = -x^2e^2 = -Q(e)x^2$ for $x \in N$.)

To summarize: if $M$ is regular of even dimension, then $C(M)$ is a CSA, while if $M$ is semiregular of odd dimension then $C_0(M)$ is a CSA.

The Witt decomposition theorem for regular, or half-regular, quadratic spaces over $K$ yields

$$M \cong H^r \perp N$$

where $r = \mathrm{ind}(M)$ is the Witt index and $N$ is anisotropic. As we observed earlier, $C(H) = K^{2\times 2}$ is the matrix algebra. Since $H$ has signed discriminant 1, repeatedly applying Lemma 3.26 yields

$$C(M) = (K^{2\times 2})^{\otimes r} \otimes C(N) = K^{2r\otimes 2r} \otimes C(N);$$
$$C_0(M) = (K^{2\times 2})^{\otimes r} \otimes C_0(N) = K^{2r\otimes 2r} \otimes C_0(N).$$

That motivates the following definition:

**Definition 3.28.** (i) Two central simple algebras $A, B$ are **Brauer equivalent** if there are matrix algebra $K^{m\times m}$, $K^{n\times n}$ such that

$$A \otimes K^{m\times m} \cong B \otimes K^{n\times n}.$$

In other words, $A \sim B$ if the matrix algebras $A^{m\times m}$ and $B^{n\times n}$ are isomorphic.
(ii) The **Brauer group** $\mathrm{Br}(K)$ of $K$ is the group of central simple algebras over $K$ modulo Brauer equivalence, with group law given by the tensor product.
(iii) The **Witt invariant** of a regular or semiregular quadratic space $M$ is

$$c(M) = \begin{cases} [C(M)]: & \dim(M) \text{ even;} \\ [C_0(M)]: & \dim(M) \text{ odd;} \end{cases}$$

the equivalence class of $C(M)$ or $C_0(M)$ in the Brauer group.

Thus the Witt invariant of $M$ depends only on the Witt equivalence class $[M] \in W(K)$. Note however that the Witt invariant as a map $c : W(K) \to \mathrm{Br}(K)$ is *not* a homomorphism, due to the rescaling in Lemma 3.26.
By the Artin–Wedderburn theorem, the Brauer group $\mathrm{Br}(K)$ can be interpreted as the group of *division algebras* (or skew fields) over $K$: any CSA is uniquely of the form $D^{n\times n}$ where $D$ is a division algebra.

**Remark 3.29.** For finite fields $K$, one can show that $\mathrm{Br}(K) = 0$. (This follows immediately from Wedderburn's little theorem: a finite division algebra is already a field.)
Also, for any algebraically closed field $K$ we have $\mathrm{Br}(K) = 0$. In these cases the Witt invariant gives no information.

**Remark 3.30.** In general the Brauer group is too large: what we have really shown is that the Witt invariant of a semiregular quadratic form belongs to the subgroup of $\mathrm{Br}(K)$ generated by quaternion algebras. Call that group $\mathrm{Br}_Q(K)$.

If $\mathrm{char}(K) \neq 2$, recall that $(a, b)$ or $\left(\frac{a,b}{K}\right)$ denotes the quaternion algebra

$$K \oplus Ki \oplus Kj \oplus Kij$$

with multiplication rules

$$i^2 = a, \quad j^2 = b, \quad ij + ji = 0,$$

where $a, b \in K\backslash\{0\}$. By abuse of notation we also denote by $(a, b)$ its Brauer equivalence class. Then we have the following useful calculation rules: $(au^2, bv^2)$ for $u, v \in K^\times$, i.e. $(a, b)$ depends only on the square classes of $a, b$; and

$$(1, b) = (1, 1) = [K] =: 1 \text{ for all } bin K^\times;$$

$$(a, b) = (b, a);$$

and

$$(a,c)(b,c) = (ab,c), \quad (a,b)(a,c) = (a,bc).$$

As a corollary, we get

$$(a,b)(a,b) = (a^2,b) = (1,b) = 1 \in \mathrm{Br}(K),$$

so $\mathrm{Br}_Q(K)$ consists only of 2-torsion. (In fact the Merkurjev theorem states that $\mathrm{Br}_Q(K)$ is exactly the 2-torsion group of $\mathrm{Br}(K)$; we do not need this.)

**Example 3.31.** Let's work out the Clifford algebras of the quadratic forms

$$Q_k = X_1^2 + ... + X_k^2, \quad Q_{-k} = -X_1^2 - ... - X_k^2$$

over $\mathbb{R}$. Note first that

$$\begin{aligned} C(Q_0) &= \mathbb{R}; \\ C(Q_{-1}) &= \mathbb{R}[X]/(X^2+1) = \mathbb{C}; \\ C(Q_1) &= \mathbb{R}[X]/(X^2-1) \cong \mathbb{R} \oplus \mathbb{R}. \end{aligned}$$

We observed earlier that $C(Q_{-2}) = \mathbb{H}$ is the Hamilton quaternions.
The algebra $C(Q_2)$ is generated by basis vectors $e_1$, $e_2$ mod the relations

$$e_1^2 = e_2^2 = 1, \quad e_1e_2 + e_2e_1 = 0;$$

it can be identified with the matrix algebra $\mathbb{R}^{2\times 2}$, for example by mapping

$$e_1 = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}, \quad e_2 = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}.$$

By Lemma 3.26, we have the general rule

$$C(Q_k) = C(Q_2 \perp Q_{k-2}) \cong C(Q_2) \otimes C(Q_{2-k});$$

i.e. $C(Q_k)$ is the $2 \times 2$ matrix algebra over the algebra $C(Q_{2-k})$. Hence $C(Q_3) = \mathbb{C}^{2\times 2}$; and $C(Q_4) = \mathbb{H}^{2\times 2}$. Similarly, we have

$$C(Q_{-k}) = C(Q_{-2} \perp Q_{2-k}) \cong C(Q_{-2}) \otimes C(Q_{k-2}) = \mathbb{H} \otimes C(Q_{k-2}),$$

such that $C(Q_{-3}) = \mathbb{H} \otimes (\mathbb{R} \oplus \mathbb{R}) = \mathbb{H} \oplus \mathbb{H}$, and $C(Q_{-4}) = \mathbb{H} \otimes \mathbb{R}^{2\times 2} = \mathbb{H}^{2\times 2}$.

To go further, we use the identifications

$$\mathbb{C}^{2\times 2} = \mathbb{H} \otimes_{\mathbb{R}} \mathbb{C}, \quad \mathbb{R}^{4\times 4} = \mathbb{H} \otimes_{\mathbb{R}} \mathbb{H}$$

to write

$$\begin{aligned} C(Q_{-5}) &= \mathbb{H} \otimes \mathbb{C}^{2\times 2} = \mathbb{H} \otimes \mathbb{H} \otimes \mathbb{C} = \mathbb{C}^{4\times 4}; \\ C(Q_5) &= (\mathbb{H} \oplus \mathbb{H})^{2\times 2} = \mathbb{H}^{2\times 2} \oplus \mathbb{H}^{2\times 2}; \\ C(Q_{-6}) &= \mathbb{H} \otimes \mathbb{H} \otimes \mathbb{R}^{2\times 2} = \mathbb{R}^{8\times 8}; \\ C(Q_6) &= (\mathbb{H}^{2\times 2})^{2\times 2} = \mathbb{H}^{4\times 4}; \\ C(Q_{-7}) &= \mathbb{H} \otimes (\mathbb{H}^{2\times 2} \oplus \mathbb{H}^{2\times 2}) = \mathbb{R}^{8\times 8} \oplus \mathbb{R}^{8\times 8}; \\ C(Q_7) &= (\mathbb{C}^{4\times 4})^{2\times 2} = \mathbb{C}^{8\times 8}; \end{aligned}$$

and finally

$$C(Q_{-8}) = C(Q_8) = \mathbb{R}^{16\times 16}.$$

The latter equation implies that $C(Q_{k+8})$ is just the algebra of $(16 \times 16)$-matrices over the algebra $C(Q_k)$, and that $C(Q_{-k-8})$ is the algebra of $(16 \times 16)$-matrices over $C(Q_{-k})$. It follows that the Brauer classes of $C(Q_k)$ ($k$ even) and $C_0(Q_k)$ ($k$ odd) are periodic with period 8. (This is an incarnation of a very pervasive and important phenomenon called *Bott periodicity*.)
Since $C_0(Q_k) = C_0(Q_{-k}) = C(Q_{1-k})$ for $k > 0$ by Remark 3.27, we finally get the following table:

| $k$ | $C(Q_k)$ | $C_0(Q_k)$ | $c(Q_k)$ |
|---|---|---|---|
| $-8$ | $\mathbb{R}^{16\times 16}$ | $\mathbb{R}^{8\times 8} \oplus \mathbb{R}^{8\times 8}$ | $[\mathbb{R}]$ |
| $-7$ | $\mathbb{R}^{8\times 8} \oplus \mathbb{R}^{8\times 8}$ | $\mathbb{R}^{8\times 8}$ | $[\mathbb{R}]$ |
| $-6$ | $\mathbb{R}^{8\times 8}$ | $\mathbb{C}^{4\times 4}$ | $[\mathbb{R}]$ |
| $-5$ | $\mathbb{C}^{4\times 4}$ | $\mathbb{H}^{2\times 2}$ | $[\mathbb{H}]$ |
| $-4$ | $\mathbb{H}^{2\times 2}$ | $\mathbb{H} \oplus \mathbb{H}$ | $[\mathbb{H}]$ |
| $-3$ | $\mathbb{H} \oplus \mathbb{H}$ | $\mathbb{H}$ | $[\mathbb{H}]$ |
| $-2$ | $\mathbb{H}$ | $\mathbb{C}$ | $[\mathbb{H}]$ |
| $-1$ | $\mathbb{C}$ | $\mathbb{R}$ | $[\mathbb{R}]$ |
| 0 | $\mathbb{R}$ | $\mathbb{R}$ | $[\mathbb{R}]$ |
| 1 | $\mathbb{R} \oplus \mathbb{R}$ | $\mathbb{R}$ | $[\mathbb{R}]$ |
| 2 | $\mathbb{R}^{2\times 2}$ | $\mathbb{C}$ | $[\mathbb{R}]$ |
| 3 | $\mathbb{C}^{2\times 2}$ | $\mathbb{H}$ | $[\mathbb{H}]$ |
| 4 | $\mathbb{H}^{2\times 2}$ | $\mathbb{H} \oplus \mathbb{H}$ | $[\mathbb{H}]$ |
| 5 | $\mathbb{H}^{2\times 2} \oplus \mathbb{H}^{2\times 2}$ | $\mathbb{H}^{2\times 2}$ | $[\mathbb{H}]$ |
| 6 | $\mathbb{H}^{4\times 4}$ | $\mathbb{C}^{4\times 4}$ | $[\mathbb{H}]$ |
| 7 | $\mathbb{C}^{8\times 8}$ | $\mathbb{R}^{8\times 8}$ | $[\mathbb{R}]$ |
| 8 | $\mathbb{R}^{16\times 16}$ | $\mathbb{R}^{8\times 8} \oplus \mathbb{R}^{8\times 8}$ | $[\mathbb{R}]$ |

Figure 3.1: Clifford algebras, even Clifford algebras and Witt invariants of quadratic forms over $\mathbb{R}$.

Now any regular quadratic form $Q$ over $\mathbb{R}$ is Witt-equivalent to $Q_\sigma$, where

$$\sigma = \operatorname{sig}(Q) \in \mathbb{Z}$$

is the signature. So the Witt invariants of regular quadratic forms over $\mathbb{R}$ depend only on the signature modulo 8:

$$c(Q) = \begin{cases} [\mathbb{R}]: & \sigma \equiv 0, 1, 2, 7 \bmod 8; \\ [\mathbb{H}]: & \sigma \equiv 3, 4, 5, 6 \bmod 8. \end{cases}$$

**Remark 3.32.** Suppose $\operatorname{char}(K) \neq 2$, and $Q$ is a regular quadratic form that is diagonalized as

$$Q = \langle a_1, ..., a_n \rangle, \quad a_i \in K^\times.$$

Then we have the following expression for $c(Q)$ in terms of quaternion symbols:

$$c(\langle a_1, ..., a_n \rangle) = \Big( \prod_{i<j} (a_i, a_j) \Big) \cdot (-1, d)^r \cdot (-1, -1)^s, \quad d = \prod a_i,$$

where: if $n = 2m$ is even, then $r = m - 1$ and $s = m(m-1)/2$, and if $n = 2m + 1$ is odd then $r = m$ and $s = m(m+1)/2$. This can be proved by induction using the rule of Lemma 3.26. In the case of $K = \mathbb{R}$, we can take all $a_i = \pm 1$; the quaternion symbols are $(1, \pm 1) = (\pm 1, 1) = [\mathbb{R}]$ and $(-1, -1) = [\mathbb{H}]$; and the result can be compared with the previous example.

# 4. Quadratic forms over $p$-adic fields

## 4.1. The $p$-adic numbers

We review some properties of $p$-adic numbers, without any proofs. Let $p$ be a prime.

For $n \in \mathbb{Z}$, $n \neq 0$, define

$$\nu_p(n) = a \text{ if } n = p^a m \text{ where } p \nmid m.$$

The **$p$-adic valuation** is defined by

$$|n|_p := p^{-\nu_p(n)}, \quad n \in \mathbb{Z},\ n \neq 0,$$

and $|0|_p = 0$. It satisfies the ultrametric inequality

$$|m+n|_p \leq \max(|m|_p, |n|_p), \quad m, n \in \mathbb{Z}$$

as well as multiplicativity,

$$|mn|_p = |m|_p \cdot |n|_p,$$

and in particular it makes $\mathbb{Z}$ into a metric space. The ring of $p$-adic integers $\mathbb{Z}_p$ is the completion of $\mathbb{Z}$ with respect to $|\cdot|_p$.

Concretely, elements $a \in \mathbb{Z}_p$ can be represented as formal power series

$$a = \sum_{k=0}^{\infty} a_k p^k, \quad a_k \in \{0, ..., p-1\}.$$

The exponential valuation $\nu_p$ extends to the map

$$\nu_p : \mathbb{Z}_p \backslash \{0\} \longrightarrow \mathbb{N}_0, \quad \nu_p(a) = \min\{k :\ a_k \neq 0\}.$$

The ring $\mathbb{Z}_p$ has the following key properties:
(1) it is local and its maximal ideal has a single generator: $\mathfrak{m} = p\mathbb{Z}_p$;
(2) the residue field is finite: $\mathbb{Z}_p / p\mathbb{Z}_p \cong \mathbb{Z}/p\mathbb{Z}$.

Property (1) is the definition of a discrete valuation ring. The discrete valuation is exactly $|\cdot|_p$.
By (1), the units $\mathbb{Z}_p^\times$ are exactly the elements $a \in \mathbb{Z}_p$ with $\nu_p(a) = 0$.

The field of fractions of $\mathbb{Z}_p$ is the field of $p$-adic numbers, $\mathbb{Q}_p$. Equivalently, $\mathbb{Q}_p$ is the completion of $\mathbb{Q}$ with respect to $|\cdot|_p$ (defined by $|r/s|_p = |r|_p/|s|_p$ for $r, s \in \mathbb{Z}$ with $s \neq 0$). Nonzero elements of $\mathbb{Q}_p$ can be represented as formal Laurent series

$$a = \sum_{k=k_0}^{\infty} a_k p^k, \quad a_k \in \{0, ..., p-1\},\ k_0 \in \mathbb{Z},\ a_{k_0} \neq 0,$$

and the exponential valuation is $\nu_p(a) = k_0$.

If $p \neq 2$, then it follows from *Hensel's lemma* that any $p$-adic integer $a = \sum_{k=0}^{\infty} a_k p^k$ for which $a_0 \in \{1, ..., p-1\}$ is a square modulo $p$ actually has a square root in $\mathbb{Z}_p$. The procedure is completely constructive: first choose $b_0 \in \{1, ..., p-1\}$ such that $b_0^2 = a_0 \mod p$, then choose $b_1$ such that $(b_0 + pb_1)^2 = a_0 + pa_1 \mod p^2$, then choose $b_2$, etc. For example, the square roots of 7 in $\mathbb{Q}_3$ are

$$1 + 1 \cdot 3 + 1 \cdot 3^2 + 2 \cdot 3^3 + 0 \cdot 3^4 + 2 \cdot 3^5 + ...$$

and

$$2 + 1 \cdot 3 + 1 \cdot 3^2 + 2 \cdot 3^3 + 0 \cdot 3^4 + 2 \cdot 3^5 + ...$$

For $p = 2$ the procedure must begin with a number that is a square modulo 8 (i.e. 1); a dyadic unit

$$a = \sum_{k=0}^{\infty} a_k 2^k \in \mathbb{Z}_2^\times, \quad a_k \in \{0, 1\}, \quad a_0 = 1$$

is a square if and only if $a_1 = a_2 = 0$.

## 4.2. Quadratic forms over $\mathbb{Q}_p$, $p \neq 2$

In this section, $p$ is always an odd prime.

The exponential valuation $\nu_p$ defines an exact sequence

$$0 \longrightarrow \mathbb{Z}_p^\times \longrightarrow \mathbb{Q}_p^\times \longrightarrow \mathbb{Z} \longrightarrow 0.$$

By Hensel's lemma,

$$\mathbb{Z}_p^\times/(\mathbb{Z}_p^\times)^2 \cong \mathbb{F}_p^\times/(\mathbb{F}_p^\times)^2 \cong \mathbb{Z}/2\mathbb{Z},$$

so we obtain a (split) exact sequence

$$0 \longrightarrow \mathbb{Z}/2 \longrightarrow \mathbb{Q}_p^\times/(\mathbb{Q}_p^\times)^2 \longrightarrow \mathbb{Z}/2 \longrightarrow 0.$$

In other words:

**Lemma 4.1.** *The square classes in $\mathbb{Q}_p$ are*

$$\mathbb{Q}_p^\times/(\mathbb{Q}_p^\times)^2 = \{1, p, \alpha, p\alpha\},$$

*where $\alpha \in \mathbb{Z}$ is any fixed nonsquare modulo $p$.*

From now on (at least within this section) we fix such an element $\alpha$.

A regular quadratic form over $\mathbb{Q}_p$ can be diagonalized, and up to isometry its coefficients depend only on their square classes. So up to isometry we may write

$$Q = Q_1 \perp pQ_2 = \langle u_1, ..., u_m \rangle \perp \langle pv_1, ..., pv_n \rangle,$$

where $u_i, v_j \in \{1, \alpha\}$. The quadratic forms $Q_1, Q_2$ determine quadratic forms $\overline{Q}_1 = \langle \overline{u_1}, ..., \overline{u_m} \rangle$ and $\overline{Q}_2 = \langle \overline{v_1}, ..., \overline{v_n} \rangle$ defined over $\mathbb{F}_p$, where $\overline{u_i}, \overline{v_j}$ are the mod $p$ cosets of $u_i, v_j$.

**Theorem 4.2.** *Let $Q = Q_1 \perp pQ_2$ as above. The following are equivalent:*
*(i) $Q$ is anisotropic;*
*(ii) $Q$ is anisotropic as a quadratic form defined over $\mathbb{Z}_p$;*
*(iii) Both $\overline{Q}_1$ and $\overline{Q}_2$ are anisotropic forms over $\mathbb{F}_p$.*

*Proof.* (i) $\Leftrightarrow$ (ii) Any solution $v \in \mathbb{Z}_p$ of $Q(v) = 0$ is, a fortiori, a solution defined over $\mathbb{Q}_p$. Conversely any solution $v \in \mathbb{Q}_p$ of $Q(v) = 0$ can be improved to a solution defined over $\mathbb{Z}_p$ by clearing denominators.

(ii) $\Rightarrow$ (iii) Suppose either $\overline{Q}_1$ or $\overline{Q}_2$ is isotropic over $\mathbb{F}_p$. The solvability of $\overline{Q}_i(\overline{v}) = 0$ with $\overline{v} \neq 0$ can be interpreted as the existence of a certain nonzero square root in $\mathbb{F}_p$. By Hensel's lemma $\overline{v}$ lifts to a solution $v$ of $Q_i(v) = 0$ over $\mathbb{Z}_p$. Hence one of $Q_1$ or $Q_2$ is isotropic, so $Q = Q_1 \perp pQ_2$ is isotropic.

(iii) $\Rightarrow$ (ii) Suppose $\overline{Q}_1$ and $\overline{Q}_2$ are both anisotropic, and suppose $v$ is a solution, defined over $\mathbb{Z}_p$, of $Q(v) = 0$. Write $v = (v_1, v_2)$ with respect to the splitting $Q = Q_1 \perp pQ_2$. Then $Q_1(v_1) = -pQ_2(v_2)$ implies $\overline{Q}_1(\overline{v_1}) = 0 \in \mathbb{F}_p$, so by anisotropy $\overline{v_1} = 0$; in other words, $v_1 = pv_3$ with $v_3$ defined over $\mathbb{Z}_p$. But then

$$-pQ_2(v_2) = Q_1(pv_3) = p^2 Q_1(v_3)$$

implies $\overline{Q_2}(\overline{v_2}) = 0$, so by anisotropy $\overline{v_2} = 0$ and $v_2 = pv_4$ with $v_4$ defined over $\mathbb{Z}_p$. Repeating this argument shows that both $v_1, v_2$ are divisible by arbitrarily large powers of $p$ and therefore $v_1 = 0$, $v_2 = 0$. This proves that $Q$ is anisotropic. $\square$

**Corollary 4.3.** *(i) Every quadratic form over $\mathbb{Q}_p$ in at least five variables is isotropic.*
*(ii) Any anisotropic, regular quadratic form over $\mathbb{Q}_p$ in four variables is equivalent to the diagonal form*

$$U = \langle 1, -\alpha, p, -\alpha p \rangle.$$

*Proof.* (i) If $Q$ is not regular then it is certainly isotropic. If $Q$ is regular and we diagonalize and decompose $Q = Q_1 \perp pQ_2$ as above, then $Q$ is anisotropic if and only if both $\overline{Q_1}$ and $\overline{Q_2}$ are anisotropic. But Chevalley's theorem implies that an anisotropic form over $\mathbb{F}_p$ has rank at most two (Example 2.25).

(ii) Example 2.25 shows that there is a unique anisotropic form over $\mathbb{F}_p$ of rank two and it is $\langle 1, -\alpha \rangle$. □

**Corollary 4.4.** *Every regular quadratic form $Q$ over $\mathbb{Q}_p$ in at least four variables represents every number in $\mathbb{Q}_p$.*

That is: for every $a \in \mathbb{Q}_p$, the equation $Q(x) = a$ has a solution $x$.

*Proof.* If $Q$ is isotropic, then by Witt decomposition it splits a hyperbolic plane $H$, and $H$ already represents every number.

So assume that $Q$ is the anisotropic form in four variables. Then $Q \perp \langle -a \rangle$ has five variables and is therefore isotropic. Since $Q$ itself is anisotropic, any vector of norm zero for $Q \perp \langle -a \rangle$ can be rescaled to have the form $v = (x, 1)$ (with $x \in \mathbb{Q}_p^4$) and then $Q(x) = a$. □

**Corollary 4.5.** *(i) Every regular quadratic form $Q$ over $\mathbb{Z}_p$ in at least three variables splits a hyperbolic plane over $\mathbb{Z}_p$.*
*(ii) Every regular quadratic form $Q$ over $\mathbb{Z}_p$ in at least two variables represents every number $t \in \mathbb{Z}_p^\times$.*

As a special case of (ii) we find that $-1 \in \mathbb{Z}_p$ can always be written as a sum of two squares. Of course if $p \equiv 1 \pmod 4$ then $-1$ already has a square root in $\mathbb{Z}_p$ by Hensel's lemma.

*Proof.* (i) If $Q$ is a regular quadratic form over $\mathbb{Z}_p$, then it can be diagonalized to $\langle u_1, ..., u_m \rangle$ where $u_i \in \mathbb{Z}_p^\times$. In particular the decomposition $Q = Q_1 \perp pQ_2$ holds with $Q_1 = Q$ and $Q_2 = 0$. Since $\overline{Q}$ is isotropic due to having rank at least three, Theorem 4.2 shows that $Q$ is isotropic (over $\mathbb{Z}_p$), hence splits a hyperbolic plane. (ii) follows because the quadratic form $Q \perp \langle -t \rangle$ is isotropic. □

**Corollary 4.6.** *There is a unique quaternionic division algebra over $\mathbb{Q}_p$: it is represented by the quaternion symbol $(\alpha, p)$.*

*Proof.* Suppose $D = (a, b)$ is a quaternion algebra:

$$D = \mathbb{Q}_p \oplus \mathbb{Q}_p i \oplus \mathbb{Q}_p j \oplus \mathbb{Q}_p k$$

with $i^2 = a$, $j^2 = b$, $ij = -ji = k$ and $k^2 = -ab$. Then $D$ defines a division algebra if and only if the norm

$$N(x_1 1 + x_i i + x_j j + x_k k) = (x_1 + x_i i + x_j j + x_k k)(x_1 - x_i i - x_j j - x_k k) = x_1^2 - a x_i^2 - b x_j^2 + ab x_k^2$$

is an anisotropic quadratic form. Proposition 4.2 and the classification of anisotropic forms over $\mathbb{F}_p$ shows that either $a$ or $b$ must have odd valuation: without loss of generality, $b = pu$ with $u \in \mathbb{Z}_p^\times$. Then without loss of generality, we may assume $a$ has even valuation (otherwise, swap the roles of $i$ and $k$) and even that $a \in \mathbb{Z}_p^\times$. Then modulo squares, we must have $a = \alpha$. The two choices $b = p$ or $b = p\alpha$ yield equivalent quaternion algebras (up to swapping $j$ and $k$) so $D$ is uniquely determined. □

In the notation of Section 3.5, the subgroup of $\mathrm{Br}(\mathbb{Q}_p)$ generated by quaternion algebras is $\mathrm{Br}_Q(\mathbb{Q}_p) = \mathbb{Z}/2\mathbb{Z}$.
By the way, the full Brauer group of $\mathbb{Q}_p$ is described by local class field theory in a reasonably explicit way: there is a canonical isomorphism

$$\mathrm{inv}: \ \mathrm{Br}(\mathbb{Q}_p) \xrightarrow{\sim} \mathbb{Q}/\mathbb{Z},$$

under which the division algebra $D = (\alpha, p)$ is mapped to $\frac{1}{2}$. But we do not need this.

To make these computations less abstract we introduce the following notation:

**Definition 4.7.** (i) Let $a, b \in \mathbb{Q}_p^\times$. The **Hilbert symbol** is

$$(a,b)_p = \begin{cases} 1: & \langle a, b, -1\rangle \text{ is isotropic;} \\ -1: & \text{otherwise.} \end{cases}$$

(ii) Let $Q$ be a regular quadratic form over $\mathbb{Q}_p$ with diagonalization

$$Q = \langle a_1, ..., a_n\rangle.$$

The **Hasse invariant** of $Q$ is

$$s(Q) := \prod_{i<j} (a_i, a_j)_p.$$

If $(a,b)_p = 1$, then the norm form $\langle 1, -a, -b, ab\rangle$ on the quaternion algebra $(a,b)$ is certainly also isotropic. Conversely, if $(a,b)_p = -1$ then the quaternion algebra $(a,b)$ cannot split, ($\mathbb{Q}_p^{2\times 2}$ has no 3-dimensional anisotropic subspaces) so it must be the division algebra $D$. So the Hilbert symbol is essentially the Witt invariant of the quadratic form $aX^2 + bY^2$:

$$(a,b)_p = \begin{cases} 1: & c(\langle a, b\rangle) = 0; \\ -1: & c(\langle a, b\rangle) \neq 0. \end{cases}$$

Since the Witt invariant of a diagonal quadratic form is given by the formula

$$c(\langle a_1, ..., a_n\rangle) = \Big(\prod_{i<j} (a_i, a_j)\Big) \cdot (-1, d)^r \cdot (-1, -1)^s, \quad d = \prod a_i,$$

| | 1 | $\alpha$ | $p$ | $p\alpha$ |
|---|---|---|---|---|
| 1 | + | + | + | + |
| $\alpha$ | + | + | − | − |
| $p$ | + | − | $+\varepsilon$ | $-\varepsilon$ |
| $p\alpha$ | + | − | $-\varepsilon$ | $+\varepsilon$ |

Figure 4.1: The Hilbert symbol $(a,b)_p$ for an odd prime $p$. In the table, $\varepsilon = +1$ if $p \equiv 1 \bmod 4$ and $\varepsilon = -1$ if $p \equiv 3 \bmod 4$.

it follows that, once the discriminant is fixed, the Hasse invariant and the Witt invariant uniquely determine one another. In particular, the Hasse invariant really is an invariant of the quadratic form (it does not depend on how $Q$ was diagonalized).

Together with the discriminant, the Hasse (or Witt) invariant completely solves the equivalence problem:

**Theorem 4.8.** *Let $Q, Q'$ be regular quadratic forms over $\mathbb{Q}_p$. The following are equivalent:*
*(i) $Q$ and $Q'$ are isometric;*
*(ii) $Q, Q'$ have equal rank, discriminant and Hasse invariant.*

*Proof.* Clearly (i) implies (ii), so the point is to show that quadratic forms of equal rank, discriminant and Hasse invariant are isometric over $\mathbb{Q}_p$. The forms $Q$ and $Q'$ can be diagonalized and may be supposed to be in diagonal form:

$$Q = \langle a_1, ..., a_n \rangle, \quad Q' = \langle a'_1, ..., a'_n \rangle.$$

We split the proof into cases depending on the rank.

(i) Rank one: $Q(X) = a_1 X^2$ and $Q'(X) = a'_1 X^2$. The Hasse invariant is trivial and the equality of discriminants

$$2a_1 = 2a'_1 \in \mathbb{Q}_p^\times / (\mathbb{Q}_p^\times)^2$$

implies that $a_1$ and $a'_1$ are equal modulo squares, so $Q$ and $Q'$ are equivalent.

(ii) Rank two: $Q(X,Y) = a_1 X^2 + a_2 Y^2$ and $Q'(X,Y) = a'_1 X^2 + a'_2 Y^2$. Then the quaternion algebras $(a_1, a_2)$ and $(a'_1, a'_2)$ are isomorphic, so their norm forms

$$\langle 1, -a_1, -a_2, a_1 a_2 \rangle \cong \langle 1, -a'_1, -a'_2, a'_1 a'_2 \rangle.$$

are equivalent. On the other hand, $a_1 a_2$ and $a'_1 a'_2$ are the discriminants of $Q$ and $Q'$ as cosets modulo squares:

$$a_1 a_2 = a'_1 a'_2 \in \mathbb{Q}_p^\times / (\mathbb{Q}_p^\times)^2.$$

By applying Witt cancellation to remove $\langle 1, a_1a_2\rangle = \langle 1, a_1'a_2'\rangle$ from both sides, we obtain

$$\langle -a_1, -a_2\rangle \cong \langle -a_1', -a_2'\rangle$$

and therefore $Q \cong Q'$.

(iii) Rank three: Let $d = \det(Q) = \det(Q')$. By rescaling $Q$ and $Q'$ by $-d$, we can assume without loss of generality that both $Q$ and $Q'$ have discriminant $-1$ ($\times(\mathbb{Q}_p^\times)^2$), and can therefore be diagonalized to

$$Q = \langle a_1, a_2, -a_1a_2\rangle, \quad Q' = \langle a_1', a_2', -a_1'a_2'\rangle$$

with $a_i, a_i' \in \mathbb{Q}_p^\times$. The Witt invariants of $Q$ and $Q'$ are represented by their even Clifford algebras, and therefore by the quaternion symbols $(a_1, a_2)$ and $(a_1', a_2')$. Since these are equivalent, their norm forms

$$\langle 1, -a_1, -a_2, a_1a_2\rangle \cong \langle 1, -a_1', -a_2', a_1'a_2'\rangle$$

are equivalent. Using Witt cancellation to remove $\langle 1\rangle$ from both sides, we obtain $Q \cong Q'$.

(iv) Rank $\geq 4$: In this case $Q$ and $Q'$ both represent every number in $\mathbb{Q}_p$. In particular, they represent 1, say $Q(e) = Q'(e') = 1$. Then we can split

$$Q = (Ke) \perp N = \langle 1\rangle \perp N, \quad Q' = \langle 1\rangle \perp N'$$

where $N$ and $N'$ are quadratic forms, again of equal discriminant and Hasse invariant, and of lower rank. The fact that $N \cong N'$ (and therefore $Q \cong Q'$) follows by an induction argument. □

**Corollary 4.9.** *Up to equivalence, there are exactly 16 anisotropic quadratic forms over $\mathbb{Q}_p$.*

The anisotropic forms are listed below. From the table one can see that the Witt group $W(\mathbb{Q}_p)$ decomposes into two copies of the Witt group $W(\mathbb{F}_p)$ (which is $\mathbb{Z}/4$ if $p \equiv 3 \bmod 4$, and $(\mathbb{Z}/2)^2$ if $p \equiv 1 \bmod 4$).

**Corollary 4.10.** *There are unique group homomorphisms*

$$\psi_0, \psi_1 : W(\mathbb{Q}_p) \longrightarrow W(\mathbb{F}_p),$$

*called the* ***residue class form homomorphisms****, with the properties*

$$\psi_0(\langle u\rangle) = \langle \overline{u}\rangle, \quad \psi_0(\langle pu\rangle) = 0,$$

$$\psi_1(\langle u\rangle) = 0, \quad \psi_1(\langle pu\rangle) = \langle \overline{u}\rangle$$

*for every $u \in \mathbb{Z}_p^\times$.*

| $Q$ | $r(Q)$ | $d(Q)$ | $s(Q)$ |
|---|---|---|---|
| $0$ | $0$ | $1$ | $1$ |
| $\langle 1\rangle$ | $1$ | $1$ | $1$ |
| $\langle \alpha\rangle$ | $1$ | $\alpha$ | $1$ |
| $\langle p\rangle$ | $1$ | $p$ | $1$ |
| $\langle p\alpha\rangle$ | $1$ | $p\alpha$ | $1$ |
| $\langle 1,-\alpha\rangle$ | $2$ | $-\alpha$ | $1$ |
| $\langle p,-p\alpha\rangle$ | $2$ | $-\alpha$ | $-1$ |
| $\langle 1,p\rangle$ | $2$ | $p$ | $1$ |
| $\langle \alpha,p\alpha\rangle$ | $2$ | $p$ | $-1$ |
| $\langle 1,p\alpha\rangle$ | $2$ | $p\alpha$ | $1$ |
| $\langle p,\alpha\rangle$ | $2$ | $p\alpha$ | $-1$ |
| $\langle \alpha,p,-p\alpha\rangle$ | $3$ | $-1$ | $-1$ |
| $\langle 1,-p,p\alpha\rangle$ | $3$ | $-\alpha$ | $-1$ |
| $\langle 1,-\alpha,-p\alpha\rangle$ | $3$ | $p$ | $-\varepsilon$ |
| $\langle 1,-\alpha,-p\rangle$ | $3$ | $p\alpha$ | $-\varepsilon$ |
| $\langle 1,-\alpha,p,-p\alpha\rangle$ | $4$ | $1$ | $-1$ |

Figure 4.2: Representatives for the 16 isometry classes of anisotropic quadratic forms over $\mathbb{Q}_p$, $p \neq 2$, with their ranks, discriminants and Hasse invariants. As in the previous figure, $\varepsilon = 1$ if $p \equiv 1 \bmod 4$ and $\varepsilon = -1$ if $p \equiv 3 \bmod 4$.

## 4.3. Quadratic forms over $\mathbb{Q}_2$

The results for quadratic forms over $\mathbb{Q}_2$ turn out to be similar to those for $\mathbb{Q}_p$, $p \neq 2$, but the proofs have to be modified. Since $\mathbb{Q}_2$ is a field of characteristic zero, all quadratic forms over $\mathbb{Q}_2$ can be diagonalized. (For $\mathbb{Z}_2$ this will no longer be true!)

But the immediate problem is that there are 8 square classes instead of 4:

$$\mathbb{Z}_2^\times/(\mathbb{Z}_2^\times)^2 = \{1, 3, 5, 7\}$$

and

$$\mathbb{Q}_2^\times/(\mathbb{Q}_2^\times)^2 = \{1, 3, 5, 7, 2, 6, 10, 14\}.$$

Hence there are seven quadratic extensions of $\mathbb{Q}_2$. The extension $\mathbb{Q}_2(\sqrt{5})$ is distinguished because it is unramified: its discriminant (5) has valuation 0.

For each of the seven quadratic extensions $K/\mathbb{Q}_2$, the norm group $N(K^\times)$ is a subgroup of $\mathbb{Q}_2^\times$, containing $(\mathbb{Q}_2^\times)^2$ (any $a^2$, $a \in \mathbb{Q}_2^\times$ occurs as the norm of $a$ itself). Hence $N(K^\times)/(\mathbb{Q}_2^\times)^2$ is a subgroup of $\mathbb{Q}_2^\times/(\mathbb{Q}_2^\times)^2$. Kummer theory guarantees that that group is of size exactly four.

In the case of the unramified extension $K = \mathbb{Q}_2(\sqrt{5})$, the valuation of an element $x \in K^\times$ is always an integer and the valuation of its norm $x\sigma(x)$ must be even, so $N(K^\times)/(\mathbb{Q}_2^\times)^2 = \{1, 3, 5, 7\}$.
The norm groups (modulo squares) of the other extensions can be worked out directly, by computing the norms of sufficiently many elements of $K^\times$. In any case, the square classes represented by the norms are as follows:

$$\begin{aligned}
\mathbb{Q}_2(\sqrt{3}): &\quad 1, 5, 6, 14\\
\mathbb{Q}_2(\sqrt{5}): &\quad 1, 3, 5, 7\\
\mathbb{Q}_2(\sqrt{7}): &\quad 1, 2, 5, 10\\
\mathbb{Q}_2(\sqrt{2}): &\quad 1, 2, 7, 14\\
\mathbb{Q}_2(\sqrt{6}): &\quad 1, 3, 10, 14\\
\mathbb{Q}_2(\sqrt{10}): &\quad 1, 6, 7, 10\\
\mathbb{Q}_2(\sqrt{14}): &\quad 1, 2, 3, 6
\end{aligned}$$

The dyadic Hilbert symbol is defined by exactly the same rule as $(a, b)_p$, $p \neq 2$: for $a, b \in \mathbb{Q}_2^\times$,

$$(a, b)_2 := \begin{cases} 1: & \langle a, b, -1\rangle \text{ is isotropic over } \mathbb{Q}_2;\\ -1: & \text{otherwise.}\end{cases}$$

As before, $(a, b)_2$ depends only on the classes of $a, b$ modulo squares. For $\Delta \notin (\mathbb{Q}^\times)^2$ we have $(a, \Delta)_2 = +1$ if and only if $a$ is a norm from $\mathbb{Q}(\sqrt{\Delta})$. So we get the following table.

| | 1 | 3 | 5 | 7 | 2 | 6 | 10 | 14 |
|---|---|---|---|---|---|---|---|---|
| 1 | + | + | + | + | + | + | + | + |
| 3 | + | − | + | − | − | + | − | + |
| 5 | + | + | + | + | − | − | − | − |
| 7 | + | − | + | − | + | − | + | − |
| 2 | + | − | − | + | + | − | − | + |
| 6 | + | + | − | − | − | − | + | + |
| 10 | + | − | − | + | − | + | + | − |
| 14 | + | + | − | − | + | + | − | − |

Figure 4.3: The dyadic Hilbert symbol.

**Proposition 4.11.** *(i) Let $Q$ be an anisotropic quadratic form over $\mathbb{Q}_2$ in four variables. Then* $\operatorname{discr}(Q) = 1$.
*(ii) Let $Q$ be a regular ternary form over $\mathbb{Q}_2$. Then $Q$ represents every element of seven square classes.*
*(iii) Let $Q$ be a quadratic form over $\mathbb{Q}_2$ in at least five variables. Then $Q$ is isotropic.*
*(iv) Let $Q$ be a regular quadratic form over $\mathbb{Q}_2$ in four variables. Then $Q$ represents every number $t \in \mathbb{Q}_2$.*

*Proof.* (i) We can diagonalize $Q$ and write it in the form

$$Q = \langle a, -a\Delta_1, -b, b\Delta_2 \rangle$$

with some square classes $a, b, \Delta_1, \Delta_2$. Since the binary forms $\langle a, -a\Delta_1 \rangle$ and $\langle b, -b\Delta_2 \rangle$ are anisotropic, they are multiples of the norms on quadratic extensions $\mathbb{Q}_2(\sqrt{\Delta_1})$ and $\mathbb{Q}_2(\sqrt{\Delta_2})$. Since $Q$ is anisotropic, it follows that $\langle a, -a\Delta_1 \rangle$ and $\langle b, -b\Delta_2 \rangle$ never represent the same number $t$; equivalently, $(at, \Delta_1)_2 \neq (bt, \Delta_2)_2$ for every $t \in \mathbb{Q}_2^\times$. But that is only possible if $\Delta_1 = \Delta_2$ (as one can read off the table), which implies

$$\operatorname{disc}(Q) = \Delta_1\Delta_2 = 1 \cdot (\mathbb{Q}_2^\times)^2.$$

(ii) The ternary quadratic form $\langle a, b, c \rangle$ *fails* to represent $t \in \mathbb{Q}_2^\times$ exactly when $\langle a, b, c, -t \rangle$ is anisotropic. By (i) this implies $-abct \in 1 \cdot (\mathbb{Q}_2^\times)^2$ and therefore

$$t \in (-abc) \cdot (\mathbb{Q}_2^\times)^2.$$

(iii) Suppose $Q$ is anisotropic. After diagonalizing, we can write $Q$ as a sum

$$Q = T \perp (-B)$$

where $T$ is an anisotropic ternary quadratic form and $B$ is an anisotropic binary quadratic form. By (ii), $T$ represents every element of (at least) 7 square classes; and

$B$ represents every element of exactly 4 square classes. In particular they represent at least one square class in common, so $T \perp (-B)$ represents 0 nontrivially.

(iv) If $Q$ is isotropic then it splits a hyperbolic plane by Witt's theorem, and therefore represents every number. Otherwise, $Q \perp \langle -t \rangle$ is isotropic by (iii) and any isotropic vector after rescaling to $(x, 1)$ yields a solution $Q(x) = t$. □

We state the following theorem without proof.[1]

**Theorem 4.12.** *There is a unique quaternionic division algebra $D$ over $\mathbb{Q}_2$. It is represented by the quaternion symbol $(-1, -1)$: i.e.*

$$D = \mathbb{Q}_2 \oplus \mathbb{Q}_2 i \oplus \mathbb{Q}_2 j \oplus \mathbb{Q}_2 k, \quad i^2 = j^2 = k^2 = ijk = -1.$$

*For $a, b \in \mathbb{Q}_2^\times$, we have the following interpretation of the Hilbert symbol:*
*(i) The quaternion algebra $(a, b)$ splits if and only if $(a, b)_2 = +1$;*
*(ii) The quaternion algebra $(a, b)$ is the division algebra $D$ if and only if $(a, b)_2 = -1$.*

Moreover, $D \otimes \mathbb{Q}_2(\sqrt{d})$ splits for every nontrivial square class $d \neq 1 \in \mathbb{Q}_2^\times / (\mathbb{Q}_2^\times)^2$.

If a quadratic form is diagonalized as

$$Q = \langle a_1, ..., a_n \rangle$$

then its **Hasse invariant** is defined to be

$$s(Q) := \prod_{i<j} (a_i, a_j)_2.$$

By Theorem 4.12, the Hasse invariant and Witt invariant uniquely determine one another. In particular $s(Q)$ is independent of the diagonalization of $Q$.

The proof of Theorem 4.8 carries over to $p = 2$ exactly:

**Theorem 4.13.** *Let $Q, Q'$ be regular quadratic forms over $\mathbb{Q}_2$. The following are equivalent:*
*(i) $Q$ and $Q'$ are isometric;*
*(ii) $Q, Q'$ have equal rank, discriminant and Hasse invariant.*

Also, just as for $p \neq 2$, the anisotropic quadratic form in four variables is unique:

[1] More generally, a form of this theorem holds over every nonarchimedean local field. This was easy enough for $\mathbb{Q}_p$, $p \neq 2$, but even over $\mathbb{Q}_2$ the proof is hard. See Main Theorem 12.3.2 of J. Voight, *Quaternion algebras* for more details.

**Remark 4.14.** This implies, just as for $p \neq 2$, that all anisotropic quadratic forms over $\mathbb{Q}_2$ are equivalent; in particular, equivalent to the form

$$X_1^2 + X_2^2 + X_3^2 + X_4^2.$$

We showed earlier that any such form has $\operatorname{discr}(Q) = 1 \cdot (\mathbb{Q}^\times)^2$, and also that $Q$ represents 1. This implies that $Q$ can be diagonalized as

$$Q = \langle 1, -a, -b, ab \rangle, \quad a, b \in K^\times,$$

i.e. that $Q$ is the norm form on a quaternion algebra $(a, b)$, which in turn represents its Witt invariant $c(Q)$. But $Q$ is anisotropic and therefore $(a, b)$ is nontrivial.

Note that the Hasse invariant of $Q$ is actually $+1$! This is because $c(Q)$ and $s(Q)$ differ by factors involving $(-1, \operatorname{discr}(Q))$ and $(-1, -1)$.

With that in mind, we can compute the Witt group:

**Proposition 4.15.** *The Witt group of $\mathbb{Q}_2$ is*

$$W(\mathbb{Q}_2) \cong \mathbb{Z}/8\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}.$$

*So there are exactly 32 isometry classes of anisotropic quadratic forms over $\mathbb{Q}_2$.*

First consider the generator $\langle 1 \rangle$: Since $4\langle 1 \rangle = \langle 1, 1, 1, 1 \rangle$ is anisotropic, it is nonzero in $W(\mathbb{Q}_2)$. On the other hand, $\langle -1, -1, -1, -1 \rangle$ is anisotropic and therefore equivalent to $\langle 1, 1, 1, 1 \rangle$; so

$$8\langle 1 \rangle \cong 4\langle 1 \rangle \perp 4\langle -1 \rangle \cong H \perp H \perp H \perp H = 0 \in W(\mathbb{Q}_2).$$

So $\langle 1 \rangle$ generates a subgroup $\mathbb{Z}/8$.

The Witt group is generated by the eight classes $\langle a \rangle$, $a \in \mathbb{Q}_2^\times/(\mathbb{Q}_2^\times)^2$. We have

$$\langle 1, 1 \rangle \cong \langle 2, 2 \rangle \cong \langle 5, 5 \rangle \cong \langle 10, 10 \rangle$$

since all of these forms have the same determinant (1) and Hasse invariant $(+1)$. So

$$2\langle 2 \rangle = 2\langle 5 \rangle = 2\langle 10 \rangle = \langle 1, 1 \rangle$$

in $W(\mathbb{Q}_2)$, from which it follows that

$$2\langle 3 \rangle = 2\langle 7 \rangle = 2\langle 6 \rangle = 2\langle 14 \rangle = -2\langle 1, 1 \rangle = 6\langle 1, \rangle$$

in $W(\mathbb{Q}_2)$, and finally

$$\langle 3 \rangle = 7\langle 5 \rangle, \quad \langle 7 \rangle = 7\langle 1 \rangle, \quad 6 = 7\langle 10 \rangle, \quad \langle 14 \rangle = 7\langle 2 \rangle.$$

In particular, $W(\mathbb{Q}_2)$ is already generated by $\langle 1\rangle$ and the differences

$$x := [\langle 1\rangle] - [\langle 2\rangle] = [\langle 1, 14\rangle], \quad y := [\langle 1\rangle] - [\langle 5\rangle] = [\langle 1, 3\rangle], \quad z := [\langle 1\rangle] - [\langle 10\rangle] = [\langle 1, 6\rangle],$$

where $2x = 2y = 2z = 0$. Also,

$$x + y = [\langle 1, 1\rangle] - [\langle 2, 5\rangle], \quad y + z = [\langle 1, 1\rangle] - [\langle 5, 10\rangle], \quad x + z = [\langle 1, 1\rangle] - [\langle 2, 10\rangle]$$

do not belong to the subgroup of $W(\mathbb{Q}_2)$ generated by $\langle 1\rangle$, since the discriminants $2 \cdot 5,\ 5 \cdot 10,\ 2 \cdot 10$ do not belong to $\pm 1 \cdot (\mathbb{Q}^\times)^2$. However, the form $\langle 1, 2, 5, 10\rangle$ is the norm form of the split quaternion algebra $\left(\frac{-2,-5}{\mathbb{Q}_2}\right)$ and is therefore hyperbolic:

$$\langle 1, 2, 5, 10\rangle = H \perp H,$$

which implies that

$$x + y + z = [\langle 1, 1, 1, 1\rangle] - [\langle 1, 2, 5, 10\rangle] = [\langle 1, 1, 1, 1\rangle].$$

Altogether, $W(\mathbb{Q}_2)$ is generated by $\langle 1\rangle$ and $x, y$ modulo only the relations $8\langle 1\rangle = 2x = 2y = 0$.

The 32 anisotropic forms over $\mathbb{Q}_2$ (up to isometry) can be described as follows:
(1) The quadratic form of rank zero;
(2) 8 unary quadratic forms, with all 8 possible discriminants and Hasse invariant $+1$;
(3) 14 binary quadratic forms, with all discriminant classes $d \neq -1$ and either Hasse invariant $\pm 1$;
(4) 8 ternary quadratic forms, with all 8 possible discriminants $d$, and with Hasse invariant given by the dyadic Hilbert symbol $(-1, -d)_2$;
(5) The quaternary form $\langle 1, 1, 1, 1\rangle$ with discriminant $+1$ and Hasse invariant $+1$.

Representatives of the anisotropic binary forms can be found among the multiples of the seven field norms $N_{K/\mathbb{Q}_2}$, where $K/\mathbb{Q}_2$ is a quadratic extension. For ternary forms we have the diagonal forms $\pm\langle 1, 1, d\rangle$ where $d \in \{1, 2, 5, 10\}$.

**Definition 4.16.** The **oddity** is the homomorphism

$$t_2 : W(\mathbb{Q}_2) \longrightarrow \mathbb{Z}/8\mathbb{Z},$$

defined by $t_2(\langle 1\rangle) = 1$, $t_2(x) = 0$, $t_2(y) = 4$.

Here $x = \langle 1\rangle - \langle 2\rangle$, $y = \langle 1\rangle - \langle 5\rangle$ are the two additional generators of $W(\mathbb{Q}_2)$ as described above. Using the computations above, this leads to the strange formula

$$t_2(\langle u\rangle) = u,$$

$$t_2(\langle 2u\rangle) = \begin{cases} u : & u \equiv \pm 1 \pmod 8; \\ u + 4 : & u \equiv \pm 3 \pmod 8; \end{cases}$$

for $u \in \{1, 3, 5, 7\} \pmod 8$. More generally, if $Q = \langle a_1, ..., a_n\rangle$ has been diagonalized, then by definition $t_2(Q) = \sum_i t_2(a_i)$.

# 5. Quadratic forms over the rational numbers

The goal of this chapter is to understand the theory of quadratic forms over $\mathbb{Q}$.

Any quadratic form $Q/\mathbb{Q}$ can be viewed "locally" as a quadratic form over $\mathbb{R}$, and over every $p$-adic field $\mathbb{Q}_p$. Over these local fields, $Q$ is completely described by simple invariants: its signature in the case of $\mathbb{R}$, and its discriminant and Hasse invariant in the case of $\mathbb{Q}_p$. This collection of local data turns out to determine the global quadratic form $Q$ uniquely.

## 5.1. The Witt group of $\mathbb{Q}$

First we describe the (infinite) group $W(\mathbb{Q})$ of Witt equivalence classes.

Since $\mathbb{Q}$ is a field of characteristic $\neq 2$, all quadratic forms can be diagonalized. So $W(\mathbb{Q})$ is certainly generated by the forms $\langle a\rangle$, where $a \in \mathbb{Q}^\times/(\mathbb{Q}^\times)^2$.

For $k \in \mathbb{N}$, denote by $W^k$ the subgroup of $W(\mathbb{Q})$ generated by the quadratic forms $\langle \pm a\rangle$, $a \in \mathbb{N}$, for which all prime divisors of $a$ are $\leq k$. We will try to build up $W(\mathbb{Q})$ from the quotient groups $W^k/W^{k-1}$. These are trivial unless $k = p$ is a prime.

The elements of $W^1$ are diagonal forms $\langle \pm 1, ..., \pm 1\rangle$ modulo Witt equivalence. Here $\langle 1, -1\rangle \cong H$ is hyperbolic over $\mathbb{Q}$. On the other hand, the signature

$$\mathrm{sgn}(Q) = \#\{\text{positive diagonal terms}\} - \#\{\text{negative diagonal terms}\}$$

is an invariant of Witt classes over $\mathbb{R}$ (and therefore also over $\mathbb{Q}$), we obtain an isomorphism

$$\mathrm{sgn} : W^1 \xrightarrow{\sim} \mathbb{Z}.$$

For $p = 2$: $W^2/W^1$ is generated by the Witt classes of $\langle \pm 2\rangle$. There are equivalences

$$\pm(X^2 + Y^2) = \langle \pm 1, \pm 1\rangle \cong \langle \pm 2, \pm 2\rangle = \pm 2(x^2 + y^2)$$

given by the substitutions $X = (x + y)$, $Y = (x - y)$; and $\langle 2, -2\rangle$ is hyperbolic and therefore Witt equivalent to 0. So

$$W^2/W^1 = \{\langle 2\rangle\}.$$

Another way of looking at this is that the map

$$s_2 : W(\mathbb{Q}) \longrightarrow \mathbb{Z}/2\mathbb{Z}, \quad s_2([Q]) = \begin{cases} 0: & \nu_2(d(Q)) \equiv 0\,(2); \\ 1: & \nu_2(d(Q)) \equiv 1\,(2); \end{cases}$$

where $d(Q) \in \mathbb{Q}^\times/(\mathbb{Q}^\times)^2$ is the discriminant, is well-defined and induces an isomorphism

$$s_2 : W^2/W^1 \xrightarrow{\sim} \mathbb{Z}/2\mathbb{Z}.$$

Finally, let $p$ be an odd prime. Let $Q$ be a regular quadratic form. By diagonalizing, up to equivalence we can write $Q$ in the form

$$Q = \langle a_1, ..., a_m \rangle \perp \langle pb_1, ..., pb_n \rangle$$

where $a_1, ..., a_m, b_1, ..., b_n$ are squarefree integers not divisible by $p$. The main result is:

**Theorem 5.1.** *The map*

$$\langle a_1, ..., a_m \rangle \perp \langle pb_1, ..., pb_n \rangle \mapsto \langle \overline{b_1}, ..., \overline{b_n} \rangle$$

*determines a well-defined isomorphism*

$$s_p : W^p/W^{p-1} \xrightarrow{\sim} W(\mathbb{F}_p) = \begin{cases} \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}: & p \equiv 1\,(4); \\ \mathbb{Z}/4\mathbb{Z}: & p \equiv 3\,(4). \end{cases}$$

*Proof.* Extending scalars from $\mathbb{Q}$ to $\mathbb{Q}_p$ gives us a projection map

$$\pi : W(\mathbb{Q}) \longrightarrow W(\mathbb{Q}_p).$$

We observed earlier that the map

$$\langle a_1, ..., a_m \rangle \perp \langle pb_1, ..., pb_n \rangle \mapsto (\langle \overline{a}_1, ..., \overline{a}_m \rangle, \langle \overline{b}_1, ..., \overline{b}_n \rangle), \quad a_i, b_j \in \mathbb{Z}_p^\times$$

determines an isomorphism $W(\mathbb{Q}_p) \xrightarrow{\sim} W(\mathbb{F}_p) \oplus W(\mathbb{F}_p)$. Applying $\pi$ and taking the second component of that isomorphism is therefore a well-defined map

$$s_p : W(\mathbb{Q}) \longrightarrow W(\mathbb{F}_p).$$

Since any class in $W^{p-1}$ is represented by a diagonal form $\langle a_1, ..., a_m \rangle$ with $p \nmid a_i$, we have $s_p(W^{p-1}) = \{0\}$. So $s_p$ descends to a map

$$s_p : W^p/W^{p-1} \longrightarrow W(\mathbb{F}_p).$$

The fact that $s_p$ is surjective is clear. That it is injective (i.e. its kernel is $W^{p-1}$) is due to the following lemma: □

**Lemma 5.2.** *Suppose $a = a_1 \cdot ... \cdot a_r \in \mathbb{Z}$ with factors $|a_i| < p$. Let $b \in \{1, ..., p-1\}$ with $b \equiv a \mod p$. Then*

$$\langle pa \rangle \equiv \langle pb \rangle \mod W^{p-1}.$$

*Proof.* Induction on $r$, beginning with $r = 2$. (The case $r = 1$ follows from this by taking $a_2 = 1$.)
Suppose $a = a_1 a_2 = b + pc$. Then

$$|c| < \frac{(p-1)^2 + (p-1)}{p} < p.$$

We can write $\langle a, pc \rangle \cong \langle b, pabc \rangle$, because: $\langle a, pc \rangle$ represents $b = a - pc$, so it can be diagonalized in the form $\langle b, x \rangle$, and the value of $x$ is determined by $bx \equiv apc \mod (\mathbb{Q}^\times)^2$.
Rescaling both sides by $p$ yields

$$\langle pa, c \rangle = \langle pa, p^2 c \rangle = \langle pb, p^2 abc \rangle = \langle pb, abc \rangle,$$

i.e. $\langle pa \rangle \perp \langle c \rangle = \langle pb \rangle \perp \langle abc \rangle$. But both $\langle c \rangle$ and $\langle abc \rangle$ belong to $W^{p-1}$.

In general if $c \in \{1, ..., p-1\}$ with $a_1 \cdot ... \cdot a_{r-1} \equiv c \mod p$, then by the induction hypothesis we have

$$\langle p(a/a_r) \rangle \equiv \langle pc \rangle$$

mod $W^{p-1}$, and after recaling by $a_r$ (which preserves the subgroup $W^{p-1}$) we obtain

$$\langle pa \rangle \equiv \langle pca_r \rangle \equiv \langle pb \rangle \mod W^{p-1};$$

in the last step we again use the proof in rank $r = 2$. □

**Theorem 5.3.** *The map $s = (\mathrm{sgn}, s_p : p \text{ prime})$ defines an isomorphism of groups*

$$s : W(\mathbb{Q}) \xrightarrow{\sim} \mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z} \oplus \bigoplus_{p \neq 2} W(\mathbb{F}_p).$$

*Proof.* More precisely, one can use the above description of $W^p / W^{p-1}$ to show that

$$W^k \cong \mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z} \oplus \bigoplus_{2 < p \leq k} W(\mathbb{F}_p)$$

via the map $(\mathrm{sgn}, s_p : p \leq k)$. □

## 5.2. Hilbert reciprocity

Let $t$ denote the homomorphism

$$t : W(\mathbb{Q}) \xrightarrow{\pi} W(\mathbb{Q}_2) \xrightarrow{t_2} \mathbb{Z}/8\mathbb{Z},$$

where $\pi$ corresponds to extending scalars from $\mathbb{Q}$ to $\mathbb{Q}_2$, and $t_2$ is the oddity. ($t$ itself is also called the *oddity*.)

Let

$$s : W(\mathbb{Q}) \xrightarrow{\sim} \mathbb{Z} \oplus \mathbb{Z}/2 \oplus \bigoplus_{p \neq 2,\infty} W(\mathbb{F}_p)$$

be the isomorphism given by the local symbols, and define homomorphisms

$$t_\infty : \mathbb{Z} \longrightarrow \mathbb{Z}/8\mathbb{Z};$$

$$t_2 : \mathbb{Z}/2\mathbb{Z} \longrightarrow \mathbb{Z}/8\mathbb{Z};$$

$$t_p : W(\mathbb{F}_p) \longrightarrow \mathbb{Z}/8\mathbb{Z}$$

by

$$t_\infty(u_\infty) + t_2(u_2) + \sum_{p \neq 2,\infty} t_p(u_p) = ts^{-1}(u_\infty, u_2, u_p, \, p \,\text{prime}).$$

We will compute $t_\infty$ and $t_p$. Surprisingly, the result of this computation leads to a significant generalization of the law of quadratic reciprocity.

For $t_\infty$, the form $\langle 1 \rangle$ is mapped to zero under $s_p$ for every $p < \infty$, but its signature is $\operatorname{sgn}(\langle 1 \rangle) = 1$. Therefore we have

$$t_\infty(1) = t(\langle 1 \rangle) = 1 \bmod 8,$$

which shows that $t_\infty(n) = n \bmod 8$ for every $n \in \mathbb{Z}$.

To compute $t_2$, note that $\langle 1, -2 \rangle$ is mapped to zero under $s_p$ for every $p \neq 2$ (and has signature zero), but is nonzero under $s_2$. Since its oddity is trivial, we have

$$t_2(1) = t(\langle 1, -2 \rangle) = 0,$$

so $t_2$ is the zero map.

For an odd prime $p$, the form $\langle -1, p \rangle$ is mapped to 0 under $s_q$ for every $q \neq p$, and to $\langle \overline{1} \rangle \in W(\mathbb{F}_p)$ under $s_p$. The oddity is always $p - 1 \pmod 8$. So $t_p$ satisfies

$$t_p(\langle \overline{1} \rangle) = p - 1 \bmod 8.$$

Evaluating $t_p$ on the rest of $W(\mathbb{F}_p)$ is more difficult and is the content of the following lemma:

**Lemma 5.4.** *Let $\alpha$ be a quadratic nonresidue mod $p$ and let $Q = \langle \overline{1}, -\overline{\alpha} \rangle$ represent the nontrivial Witt class of even rank. Then $t_p(Q) = 4$.*

*Proof.* We use induction on $p$.
If $p \equiv 3 \bmod 4$ then $W(\mathbb{F}_p)$ is cyclic, generated by $\langle\overline{1}\rangle$, so $t_p$ is already completely determined. If $p \equiv 5 \bmod 8$, then consider the quadratic form $\langle -p, 2p\rangle$: it has signature 0 and satisfies

$$s_2(\langle -p, 2p\rangle) = 1, \quad s_p(\langle -p, 2p\rangle) = \langle -\overline{1}, \overline{2}\rangle,$$

and $s_q(\langle -p, 2p\rangle) = 0$ at all primes $q \neq 2, p$. The oddity is

$$t(\langle -p, 2p\rangle) = -p + (p+4) = 4 \,(\mathrm{mod}\, 8).$$

The fact that the image under $s_2$ is nonzero does not matter, since $t_2$ is identically zero. Therefore we have

$$t_p(\langle -\overline{1}, \overline{2}\rangle) = t(\langle -p, 2p\rangle) = 4.$$

(Incidentally, the form $\langle \overline{1}, -\overline{2}\rangle$ must be anisotropic because its image under $t_p$ is nonzero. This implies that $\overline{2}$ is not a square modulo $p$.)

The remaining case is $p \equiv 1 \bmod 8$: here is where we use induction. Let $q < \sqrt{p}$ be a prime with the property that $p$ is not a square modulo $q$. This exists, because: suppose not. Let $m$ be the odd number for which $m < \sqrt{p} < m+2$ and define

$$N := \frac{p-1}{4} \cdot \frac{p-9}{4} \cdot \ldots \cdot \frac{p-m^2}{4}.$$

Since $p - a^2 = (\sqrt{p} - a)(\sqrt{p} + a) < (m+2-a)(m+2+a)$, we have

$$\begin{aligned} N &< \frac{(m+2+1)(m+2-1)}{4} \cdot \frac{(m+2+3)(m+2-3)}{4} \cdot \ldots \cdot \frac{(m+2+m)(m+2-m)}{4} \\ &= \frac{2 \cdot 4 \cdot \ldots \cdot (2m+2)}{2^{m-1}} \\ &= (m+1)!. \end{aligned}$$

If $p$ is a square modulo $q$, say $p \equiv a^2 \pmod{q}$, then it is a square of exactly four residues modulo $4q^i$ for every $i \in \mathbb{N}$; and the solutions $a \in \{1, \ldots, m\}$ with $a^2 \equiv p \bmod q^i$ are precisely those for which $q^i$ divides the factor $(p - a^2)/4$. By counting the number of solutions, we obtain the valuation

$$\nu_q(N) = \sum_{i=1}^{\infty} \lfloor \frac{(m+1)}{q^i} \rfloor,$$

where $\lfloor - \rfloor$ is the floor function. But the right-hand side is $\nu_q((m+1)!)$. Since $N < (m+1)!$, there are primes $q$ for which the equality does not hold, i.e. for which $p$ is not a square mod $q$.

For this prime $q$, consider the rational quadratic form

$$Q = \langle 1, -p, -q, pq\rangle.$$

This has signature 0 and

$$s_p(Q) = \langle -\overline{1}, \overline{q}\rangle, \quad s_q(Q) = \langle -\overline{1}, \overline{p}\rangle, \quad s_\ell(Q) = 0 \ (\ell \neq p, q).$$

Its oddity is

$$\text{oddity}(Q) = 1 - p - q + pq \ (\text{mod}\, 8) = 0 \ (\text{mod}\, 8)$$

since $p \equiv 1\,(8)$. So

$$t_p(\langle -\overline{1}, \overline{q}\rangle) + t_q(\langle -\overline{1}, \overline{p}\rangle) = t(\langle 1, -p, -q, pq\rangle) = 0 \bmod 8.$$

Since $t_q(\langle -\overline{1}, \overline{p}\rangle) = 4 \bmod 8$ by induction, we also have

$$t_p(\langle -\overline{1}, \overline{q}\rangle) = 4 \bmod 8. \qquad \square$$

Altogether this proves the following:

**Proposition 5.5.** *The homomorphisms*

$$t_\infty : \mathbb{Z} \to \mathbb{Z}/8, \quad t_2 : \mathbb{Z}/2 \to \mathbb{Z}/8, \quad t_p : W(\mathbb{F}_p) \to \mathbb{Z}/8$$

*are given as follows:*
*(i)* $t_\infty(n) = n$ *mod* $8$*;*
*(ii)* $t_2 \equiv 0$*;*
*(iii) For an odd prime* $p$*,* $t_p(\langle\overline{1}\rangle) = p - 1$ *mod* $8$*, and* $t_p(\langle\overline{\alpha}\rangle) = p + 3$ *mod* $8$ *where* $\alpha$ *is any quadratic nonresidue mod* $p$*.*

Now let $a, b \in \mathbb{Q}^\times$, and let

$$Q = \langle 1, -a, -b, ab\rangle$$

be the norm on the quaternion algebra $(a, b)$. In $\mathbb{Q}_2$, if $(a, b)_2 = +1$ then $Q$ is hyperbolic and therefore has oddity zero; otherwise, $Q$ is anisotropic, hence equivalent to $\langle 1, 1, 1, 1\rangle$, hence has oddity 4.
For an odd prime $p$, if $(a, b)_p = 1$ then $Q$ is hyperbolic and satisfies $s_p(Q) = 0$. Otherwise, if $(a, b)_p = -1$ then $Q$ is equivalent to the form $\langle 1, -\alpha, p, -p\alpha\rangle$, such that $s_p(Q) = \langle\overline{1}, -\overline{\alpha}\rangle \in W(\mathbb{F}_p)$, and $t_p s_p(Q) = 4 \bmod 8$.

The signature of $Q$ modulo 8 is

$$\text{sgn}(Q) \bmod 8 = \begin{cases} 0: & a > 0 \text{ or } b > 0; \\ 4: & a < 0 \text{ and } b < 0. \end{cases}$$

We write $(a, b)_\infty := +1$ if $a > 0$ or $b > 0$, and $(a, b)_\infty := -1$ if $a < 0$ and $b < 0$.

The oddity equation

$$t_\infty(\mathrm{sgn}(Q)) + \sum_{p\,\mathrm{odd}} t_p s_p(Q) = t(Q) = \begin{cases} 0: & (a,b)_2 = +1; \\ 4: & (a,b)_2 = -1; \end{cases}$$

now becomes the **Hilbert reciprocity law**:

**Theorem 5.6** (Hilbert reciprocity)**.**

$$\prod_{p \le \infty} (a,b)_p = 1.$$

The infinite product is well-defined in the sense that $(a,b)_p = 1$ for almost all $p$. For example, this is the case for any prime $p \neq 2$ for which $\nu_p(a)$, $\nu_p(b)$ are both even.

**Remark 5.7.** Hilbert reciprocity generalizes the law of quadratic reciprocity. Recall that the reciprocity symbol is defined by

$$\left(\frac{a}{p}\right) = \begin{cases} 1: & a \text{ is a quadratic residue mod } p; \\ -1: & a \text{ is a quadratic nonresidue mod } p; \\ 0: & p|a. \end{cases}$$

If $p, q$ are odd primes, then using the tables for the Hilbert symbol we find

$$(p,q)_p = \left(\frac{q}{p}\right), \quad (p,q)_q = \left(\frac{p}{q}\right), \quad (p,q)_2 = \begin{cases} -1: & p \equiv q \equiv 3 \,(\mathrm{mod}\, 4); \\ 1: & \text{otherwise}; \end{cases}$$

and $(p,q)_\ell = +1$ for all $\ell \neq p, q, 2$. By Hilbert reciprocity we get

$$\left(\frac{q}{p}\right) \cdot \left(\frac{p}{q}\right) = (p,q)_2 = (-1)^{(p-1)(q-1)/4}.$$

The auxiliary laws follow similarly: for an odd prime $p$, we have

$$(2,p)_p = \left(\frac{2}{p}\right), \quad (2,p)_2 = \begin{cases} 1: & p \equiv \pm 1 \,(\mathrm{mod}\, 8); \\ -1: & p \equiv \pm 3 \,(\mathrm{mod}\, 8); \end{cases}$$

and $(2,p)_q = +1$ for all $q \neq 2, p$. Therefore

$$\left(\frac{2}{p}\right) = (2,p)_2 = (-1)^{(p^2-1)/8}.$$

Finally,

$$(-1,p)_p = \left(\frac{-1}{p}\right), \quad (-1,p)_2 = \begin{cases} 1: & p \equiv 1 \,(\mathrm{mod}\, 4); \\ -1: & p \equiv 3 \,(\mathrm{mod}\, 4); \end{cases}$$

and $(-1,p)_q = +1$ for all $q \neq 2, p$, so

$$\left(\frac{-1}{p}\right) = (-1,p)_2 = (-1)^{(p-1)/2}.$$

**Corollary 5.8** (Reciprocity for Witt invariants)**.** *Let $(V, Q)$ be a regular quadratic $\mathbb{Q}$-space. For $p$ a prime, let $V_p = V \otimes \mathbb{Q}_p$, and let $V_\infty = V \otimes \mathbb{R}$.*
*(i) The Hasse invariants satisfy*

$$\prod_{p \leq \infty} s(V_p) = +1.$$

*(ii) Write $c(V_p) = +1$ if the Witt invariant of $V_p$ is trivial and $c(V_p) = -1$ if the Witt invariant is nontrivial. Then*

$$\prod_{p \leq \infty} c(V_p) = +1.$$

## 5.3. The Hasse–Minkowski principle

The computation of the Witt group of $\mathbb{Q}$ immediately implies the following theorem (which is the "weak" Hasse–Minkowski principle; the "strong" Hasse–Minkowski principle will be discussed later).

Let $(V, \mathbb{Q})$ be a regular quadratic space. For any prime $p$, let $V_p := V \otimes_{\mathbb{Q}} \mathbb{Q}_p$ be the quadratic space given by extending scalars to $\mathbb{Q}_p$; similarly, define $V_\infty := V \otimes_{\mathbb{Q}} \mathbb{R}$ by extending scalars to $\mathbb{R}$.

**Theorem 5.9** (Weak Hasse–Minkowski principle)**.** *The following are equivalent:*
*(i) $V$ is hyperbolic;*
*(ii) $V_p$ is hyperbolic for every $p$ (including $\infty$).*

*Proof.* Certainly if $V = \perp H$ splits into hyperbolic planes over $\mathbb{Q}$, then it does so over $\mathbb{R}$ and every $\mathbb{Q}_p$.
The converse is true because (ii) means that the image of $V$ under the map

$$s : W(\mathbb{Q}) \xrightarrow{\sim} \mathbb{Z} \oplus \mathbb{Z}/2 \oplus \bigoplus_{p \neq 2} W(\mathbb{F}_p)$$

is zero, hence $[V] = 0 \in W(\mathbb{Q})$. □

**Corollary 5.10.** *Let $(V, Q_V)$ and $(W, Q_W)$ be regular quadratic spaces over $\mathbb{Q}$. The following are equivalent:*
*(i) $V \cong W$;*
*(ii) $V_p \cong W_p$ for every $p$ (including $\infty$).*

*Proof.* This is equivalent to the weak Hasse–Minkowski principle because $V \cong W$ if and only if $V \oplus W(-1)$ is hyperbolic. □

**Theorem 5.11** (Strong Hasse–Minkowski principle)**.** *Let $(V, Q)$ be a regular quadratic space over $\mathbb{Q}$. The following are equivalent:*
*(i) $V$ is isotropic;*
*(ii) $V_p$ is isotropic for every $p$ (including $\infty$).*

As the name suggests, the strong Hasse–Minkowski principle implies the weak principle: Suppose $V_p$ is hyperbolic for every $p$. (In particular, $\operatorname{rank}(V)$ is even.) By induction on $r = \operatorname{rank}(V_p)$ we will show that $V$ is hyperbolic. If $r = 2$ then $V$ being hyperbolic is equivalent to it being isotropic, by Witt's theorem. In general, the strong principle implies that $V$ is isotropic, and therefore $V = H \perp N$ for some other regular quadratic space $N$. But then $V_p = H \perp N_p$ is hyperbolic, so $N_p$ is hyperbolic for every $p$. By induction, $N$ and therefore $V$ is hyperbolic.

*Proof.* The nontrivial direction is (ii) $\Rightarrow$ (i). We prove it for small values of $r = \operatorname{rank}(V)$ by cases, and in general by induction.

The theorem is vacuous for $r = 1$ as a regular quadratic space of rank one is never isotropic.
For $r = 2$, being isotropic is equivalent to being hyperbolic and the theorem follows from the weak Hasse–Minkowski principle.
For $r = 3$, let $d = \operatorname{disc}(V)$ and consider the space

$$W = V \perp \langle d \rangle.$$

Then each $W_p$ is isotropic, hence splits in the form

$$W_p = H \perp Q_p$$

for some binary quadratic form $Q_p$. Since $\operatorname{disc}(W) = 1$ $(\cdot(\mathbb{Q}^\times)^2)$, it follows that each $Q_p$ has discriminant $-1$ and is therefore hyperbolic. So $W_p$ is hyperbolic for all $p$. By the weak Hasse–Minkowski principle, $W$ is hyperbolic, which forces $V$ to be isotropic, because:

$$H \perp H \perp \langle -d \rangle \cong W \perp \langle -d \rangle \cong V \perp \langle d, -d \rangle \cong V \perp H$$

implies $V \cong H \perp \langle -d \rangle$ by Witt cancellation.

Now suppose $r = 4$. Write each $V_p$ in the form $V_p = U_p \perp H$ where $U_p$ is two-dimensional. Fix a representative $d \in \mathbb{Z}$ of the discriminant $[d] = \operatorname{disc}(V) \in \mathbb{Q}^\times/(\mathbb{Q}^\times)^2$. Then each $U_p$ has discriminant $-d \cdot (\mathbb{Q}_p^\times)^2$, and can be diagonalized in the form

$$U_p = \langle a_p, -da_p \rangle, \quad \text{where } a_p \in \mathbb{Q}_p^\times.$$

Moreover, if $p < \infty$ and $p \nmid 2d$, then by Witt's decomposition theorem we can split

$$V_p = U_p \perp H$$

over $\mathbb{Z}_p$, where $U_p$ is $\mathbb{Z}_p$-regular, and hence assume $a_p \in \mathbb{Z}_p^\times$. (By abuse of notation, if $p = \infty$ then $\mathbb{Q}_p$ means $\mathbb{R}$.)

We will construct a quadratic $\mathbb{Q}$-space

$$W = \langle a, -da \rangle, \quad a \in \mathbb{Q}$$

with $W_p \cong U_p$ for every $p$. If $p \nmid 2d$ then $\langle a_p, -da_p \rangle$ is equivalent to $\langle 1, -d \rangle$ over $\mathbb{Q}_p$ whenever $(a_p, -da_p)_p = 1$: both sides have discriminant $-d$ and Hasse invariant $+1$. This is automatically the case if $\nu_p(a_p) = 0$.

We will find $a \in \mathbb{Z}$ such that $[a] = [a_p] \in \mathbb{Q}_p^\times / (\mathbb{Q}_p^\times)^2$ for the remaining places $p|2d$ (including $\infty$). This is a finite set of congruence conditions on $a$. By Dirichlet's theorem on primes in arithmetic progressions, there is actually a solution of the form

$$a = \pm q \cdot \prod_{p|2d} p^\alpha,$$

with $q \nmid 2d$ prime. So at every $p \leq \infty$, with the possible exception of $p = q$,

$$\langle a, -da \rangle \cong \langle a_p, -da_p \rangle = U_p.$$

But by reciprocity for Witt invariants, we also have

$$c(U_q) = c(V_q) = c(\langle a, -da \rangle_q)$$

at the missing place $p = q$, and therefore $\langle a, -da \rangle \cong U_q$ as well.

Finally, suppose $r \geq 5$. We will show that $V$ already contains an isotropic space of dimension four. Let $U \subseteq V$ be any three-dimensional space for which $U_\infty$ is indefinite, and diagonalize it in the form $U = \langle a, b, c \rangle$ with $a, b, c \in \mathbb{Z}$. Let $P$ be the finite set of primes dividing $abc$. If $p \notin P$ then the form $U_p$ is isotropic (since $a, b, c \in \mathbb{Z}_p^\times$). Suppose $p \in P$ for which $U_p$ is anisotropic. Since the full space $V_p$ is isotropic, we can find a norm-zero element $x_p + y_p$ where $x_p \in U_p$, $y_p \in U_p^\perp$ are both nonzero. If $U_p^\perp$ is anisotropic, then $Q(y_p)$ is automatically nonzero; otherwise, it represents a hyperbolic plane and therefore every number, so we can choose $x_p \in U_p$ nonzero and arbitrary and find $y_p \in U_p^\perp$ with $Q(y_p) = -Q(x_p) \neq 0$. In all cases, the four-dimensional space $U_p \perp \mathbb{Q}_p y_p$ is isotropic.

Now we choose $y \in \mathbb{Q}$ with the property that $Q(y) \in Q(y_p) \cdot (\mathbb{Q}_p^\times)^2$ for all $p \in P$. This can be done by approximating the coordinates of $y_p$ with respect to any basis of $V$ by rational numbers. Then $W := U \perp \mathbb{Q}y$ is a four-dimensional space for which

$$W_p = U_p \perp \mathbb{Q}_p y = U_p \perp \mathbb{Q}_p y_p$$

is isotropic for all $p \leq \infty$, so $W$ is already isotropic. $\square$

**Corollary 5.12.** *Let $Q$ be a rational quadratic form. Then $Q$ represents a number $t \in \mathbb{Q}$ if and only if $Q_p$ represents $t$ for every $t \leq \infty$.*

*Proof.* This is because $Q$ represents $t$ if and only if $Q \perp \langle -t \rangle$ is isotropic. □

**Corollary 5.13** (Mayer's theorem)**.** *Every indefinite quadratic form over $\mathbb{Q}$ in at least five variables is isotropic.*

*Proof.* Any such form $Q$ is isotropic over every $\mathbb{Q}_p$, ($p$ prime, i.e. $p < \infty$) since it involves at least five variables. It is also isotropic over $\mathbb{R}$ as it is indefinite. By the Hasse–Minkowski principle, $Q$ is already isotropic over $\mathbb{Q}$. □

**Example 5.14.** Every positive rational number can be represented as a sum of four rational squares.

*Proof.* Let $t \in \mathbb{Q}_{>0}$; then the quadratic form

$$Q(X_1, ..., X_4, X_5) = X_1^2 + X_2^2 + X_3^2 + X_4^2 - tX_5^2$$

is indefinite and involves five variables, and is therefore isotropic over $\mathbb{Q}$. Any vector $v = (v_1, ..., v_5) \in \mathbb{Q}^5$ with $Q(v) = 0$ and $v \neq 0$ necessarily has $v_5 \neq 0$, and therefore can be rescaled to have $v_5 = 1$. So

$$t = v_1^2 + v_2^2 + v_3^2 + v_4^2.$$

□

**Example 5.15.** A positive rational number $t$ can be written as a sum of three rational squares if and only if it is not of the form $t = 4^a \cdot n$ with $n \equiv 7 \bmod 8$.

*Proof.* The quadratic form $Q(X_1, ..., X_4) = X_1^2 + X_2^2 + X_3^2 - tX_4^2 = \langle 1, 1, 1, -t \rangle$ is isotropic over $\mathbb{R}$ because it is indefinite, and it is isotropic over every $\mathbb{Q}_p$, $p \neq 2$ because $\langle 1, 1, 1 \rangle$ is already isotropic.
By the Hasse–Minkowski principle, $Q$ is isotropic over $\mathbb{Q}$ if and only if it is isotropic in $\mathbb{Q}_2$, and that is the case if and only if $-t \in (\mathbb{Q}_2^\times)^2$, or equivalently

$$t \in 7 \cdot (\mathbb{Q}_2^\times)^2.$$

□

**Example 5.16.** A positive rational number $t$ can be written as a sum of two rational squares if and only if $\nu_p(t)$ is even for every prime $p \equiv 3 \bmod 4$.

*Proof.* The quadratic form $Q(X_1, X_2, X_3) = X_1^2 + X_2^2 - tX_3^2$ is isotropic over $\mathbb{R}$. Over $\mathbb{Q}_2$, it is anisotropic if and only if

$$-t \in \{1, 2, 5, 10\} \bmod (\mathbb{Q}_2^\times)^2,$$

i.e. if

$$t \in \{3, 6, 7, 14\} \bmod (\mathbb{Q}_2^\times)^2,$$

which is the case if and only if $t = 2^a \cdot n$ with $n \equiv 3 \bmod 4$.
At an odd prime $p$, the discriminant is $d(Q) = -t$ and the Hasse invariant is $s(Q) = 1$. These are the invariants of an anisotropic ternary form if and only if $p \equiv 3 \bmod 4$ and $\nu_p(t)$ is odd. □

## 5.4. The existence theorem

The Hasse–Minkowski local-global principle shows that the most interesting questions for quadratic forms over $\mathbb{Q}$ can be answered by passing to their localizations at $\mathbb{R} =: \mathbb{Q}_\infty$ and $\mathbb{Q}_p$. In this section, we will consider a kind of converse: when do quadratic forms over $\mathbb{R}$ and $\mathbb{Q}_p$ "glue" to a global quadratic form over $\mathbb{Q}$?

As before, by abuse of notation we write $\mathbb{Q}_p = \mathbb{R}$ for $p = \infty$.

**Theorem 5.17.** *Let $n \geq 2$ and let $d \in \mathbb{Q}^\times/(\mathbb{Q}^\times)^2$ be fixed. Suppose $Q_p$, $p \leq \infty$ are regular quadratic forms over $\mathbb{Q}_p$ in $n$ variables, with common discriminant*

$$d(Q_p) = d \cdot (\mathbb{Q}_p^\times)^2, \quad p \leq \infty$$

*for some $d \in \mathbb{Q}^\times$, and whose Hasse invariants satisfy*

$$\prod_{p \leq \infty} s(Q_p) = +1.$$

*(In particular, $s(Q_p)$ may be $-1$ for only finitely many $p$.) Then there exists a regular quadratic form $Q$, defined over $\mathbb{Q}$, which is equivalent to $Q_p$ at every $p \leq \infty$.*

The form $Q$ is then unique up to $\mathbb{Q}$-equivalence by the weak Hasse–Minkowski principle.

*Proof.* Let $P$ be a finite set of primes containing $\infty$, 2, and every prime $p$ for which $\nu_p(d) \equiv 1\,(2)$ or $s(Q_p) = -1$.

The proof uses induction on $n$. First suppose $n = 2$. For each $p \in P$, let $t_p \in \mathbb{Q}_p^\times$ be any number that is represented by $Q_p$. So we can diagonalize

$$Q_p = \langle t_p, dt_p \rangle.$$

For $p = \infty$ we may assume without loss of generality that $t_\infty = 1$ (otherwise, replace all $Q_p$ by their negatives).

By Dirichlet's theorem on primes in arithmetic progressions, there exists a prime $q \notin P$ with the property

$$q \in t_p \cdot (\mathbb{Q}_p^\times)^2, \quad p \in P.$$

(At $p = \infty$ this is a sign condition, while at $p < \infty$ this is a congruence condition modulo $p$.) Then define

$$Q := \langle q, dq \rangle.$$

By construction, $Q \cong Q_p$ at every prime $p \in P$. At any prime $p \notin P$, $p \neq q$, both $Q$ and $Q_p$ have trivial Hasse invariant and the same discriminant and are therefore

equivalent. Finally, Hilbert reciprocity and the condition $\prod_{p\le\infty} s(Q_p) = +1$ implies that $Q$ and $Q_q$ also have the same $q$-adic Hasse invariant, and are therefore equivalent over $\mathbb{Q}_q$.

Now suppose $n \ge 3$. As before, let $t_p \in \mathbb{Q}_p^\times$ be any numbers represented by $Q_p$, and let $q \notin P$ be a prime with

$$q \in t_p \cdot (\mathbb{Q}_p^\times)^2, \quad p \in P.$$

In particular, $Q_p$ represents $q$ for every $p \in P$. At any prime $p \notin P$, the form $Q_p$ is isotropic, and therefore also represents $q$. So we can write

$$Q_p = \langle q \rangle \perp f_p$$

with some quadratic forms $f_p$ in $(n-1)$ variables. We will show that the family $(f_p)_{p\le\infty}$ also satisfies the conditions of the theorem: every $f_p$ has discriminant $qd$ modulo $\mathbb{Q}_p^\times$, and the Hasse invariants satisfy

$$s(Q_p) = s(\langle q \rangle \perp f_p) = (q, d)_p \cdot s(f_p).$$

By Hilbert reciprocity, $\prod_{p\le\infty}(q, d)_p = 1$ and therefore

$$\prod_{p\le\infty} s(f_p) = \prod_{p\le\infty} s(Q_p) = 1.$$

By the induction assumption, there is a global quadratic form $f/\mathbb{Q}$ that is $\mathbb{Q}_p$-equivalent to every $f_p$. Then the quadratic form $Q = \langle q \rangle \perp f$ is $\mathbb{Q}_p$-equivalent to every $Q_p$. $\square$

# 6. Quadratic forms over the integers

## 6.1. Lattices

To study quadratic forms over $\mathbb{Z}$, it is often helpful to take a somewhat different point of view: we identify $\mathbb{Z}$-quadratic modules $(M, Q)$ with *lattices* in the space $M \otimes \mathbb{Q}$, or in the spaces $M \otimes \mathbb{R}$ or $M \otimes \mathbb{Q}_p$.

In this section we introduce some terminology for lattices (also over more general rings):

**Definition 6.1.** Let $R$ be an integral domain with field of fractions $K$. Let $V$ be a finite-dimensional $K$-vector space with a basis $f_1, ..., f_n$. An $R$**-lattice** in $V$ is an $R$-submodule $L \subseteq V$ with the following property: there exist elements $a, b \in K^\times$ such that

$$a \cdot \sum_{i=1}^{n} Rf_i \subseteq L \subseteq b \cdot \sum_{i=1}^{n} Rf_i.$$

Note that this definition is independent of the choice of basis $f_1, ..., f_n$: for any other basis $g_1, ..., g_n$, we obtain values of $a, b$ with

$$a \cdot \sum_{i=1}^{n} Rf_i \subseteq \sum_{i=1}^{n} Rg_i \subseteq b \cdot \sum_{i=1}^{n} Rf_i$$

by taking common denominators in the change-of-basis matrices from $\{f_1, ..., f_n\}$ to $\{g_1, ..., g_n\}$ and back.

In this generality we do not assume that $L$ is free. But over $\mathbb{Z}$ (or any principal ideal domain) $L$ is automatically free, and the condition

$$a \cdot \sum_{i=1}^{n} Rf_i \subseteq L \subseteq b \cdot \sum_{i=1}^{n} Rf_i$$

implies that $L$ is free of rank exactly $n$.

For the rest of this section, suppose $R$ is a principal ideal domain of characteristic zero. (Later we will specialize to $R = \mathbb{Z}$ or $R = \mathbb{Z}_p$, $p$ a prime.) Then the definition of lattices becomes much simpler:

**Definition 6.2.** Let $V$ be a finite-dimensional $K$-vector space. A **lattice** in $V$ is a set of the form

$$L = \sum_{i=1}^{n} Rf_i = \{a_1 f_1 + ... + a_n f_n : \ a_i \in R\},$$

where $f_1, ..., f_n$ is a $K$-basis of $V$.

By an *integral lattice* we mean a lattice $L$ in a regular symmetric bilinear space $(V, \langle -, - \rangle)/K$, written $x \cdot y = \langle x, y \rangle$, with the property that $x \cdot y \in R$ for every $x, y \in L$. The integral lattice is called *even* if $x \cdot x \in 2R$ for every $x \in L$, and *odd* otherwise. In the even case, we denote by

$$Q(x) = \frac{1}{2}(x \cdot x)$$

the $R$-valued quadratic form $Q : L \to R$.

Conversely, every nondegenerate quadratic space $(L, Q)$ over $R$ can be interpreted as an even lattice in the space

$$V := L \otimes K.$$

So the notions of even lattice and nondegenerate quadratic form are equivalent.

**Definition 6.3.** Let $L$ be a lattice in a regular symmetric bilinear space $(V, \langle -, - \rangle)/K$. The **dual lattice** is

$$L' := \{y \in V : \ x \cdot y \in R \text{ for all } x \in L\}.$$

If $e_1, ..., e_n$ is an $R$-basis of $L$ then, since $\langle -, - \rangle$ is regular, there are elements $f_1, ..., f_n \in V$ with the property

$$e_i \cdot f_j = \begin{cases} 1 : & i = j; \\ 0 : & i \neq j. \end{cases}$$

Then $L'$ has the $R$-basis $f_1, ..., f_n$. Dually, the basis $f_1, ..., f_n$ of $L'$ admits the corresponding $K$-basis $e_1, ..., e_n$ of $V$ with

$$f_i \cdot e_j = \begin{cases} 1 : & i = j; \\ 0 : & i \neq j; \end{cases}$$

which shows that the double dual $(L')'$ is exactly $L$ itself.

If $L$ is an integral lattice, (not necessarily even) we have $L \subseteq L'$. The lattice $L$ is **unimodular** if $L = L'$. Note that $L$ is unimodular if and only if $L$ is regular as a symmetric bilinear $R$-module, and $L$ is even unimodular if and only if it is regular as a quadratic $R$-module.

**Example 6.4.** Let $R = \mathbb{Z}$ and let $V = \mathbb{Q}^n$ with the standard (Euclidean) inner product

$$e_i \cdot e_j = \begin{cases} 1: & i = j; \\ 0: & i \neq j; \end{cases}$$

where $e_i = (0, ..., 1, ..., 0)$. Then $L = \mathbb{Z}^n$ is an odd unimodular lattice.

If $L \subseteq V$ is a lattice and $K \subseteq L$ is a subgroup, then $K$ is a lattice in $K \otimes \mathbb{R} \subseteq V$. Recall from Chapter 1 that $K \subseteq L$ is called *primitive* if $L = K \oplus N$ for some other $R$-module $N$ (as abstract modules, not as quadratic modules!). The module $K^*$ may be identified with the dual lattice $K'$.

**Lemma 6.5.** *Let $L \subseteq V$ be a lattice and $P \subseteq L$ a submodule. The following are equivalent:*
*(i) $P$ is primitive in $L$;*
*(ii) $L/P$ is torsion-free;*
*(iii) There is a vector subspace $W \subseteq V$ with $P = L \cap W$;*
*(iv) $P = (P^\perp)^\perp$, where $\perp$ means the orthogonal complement in $L$.*

*Proof.* (i) $\Rightarrow$ (ii) If $L = P \oplus N$ then $L/P \cong N$ is a submodule of the torsion-free $R$-module $L$, hence free.
(ii) $\Rightarrow$ (iii) By the elementary divisor theorem, for any subgroup $P \subseteq L$, there is a basis $e_1, ..., e_n$ of $L$ and natural numbers $d_1, ..., d_k \in \mathbb{N}$ such that $d_1 e_1, ..., d_k e_k$ is a basis of $K$. If $L/P$ is torsion-free then $d_1 = ... = d_k = 1$, hence $P = L \cap W$ where $W$ is the $K$-vector space spanned by $e_1, ..., e_k$.
(iii) $\Rightarrow$ (iv): If $P = L \cap W$ then $P^\perp = L \cap W^\perp$, hence

$$(P^\perp)^\perp = L \cap (W^\perp)^\perp = L \cap W = P.$$

(iv) $\Rightarrow$ (i): Any submodule of the form $X^\perp$, where $X \subseteq L$ is a set, is primitive: this is because $X^\perp$ is the intersection of $L$ with the orthogonal complement of $X$ in $V$. So $P = (P^\perp)^\perp$ is primitive. □

The *determinant* or *discriminant* $\det(L)$ of an integral lattice $L$ is the discriminant of the underlying quadratic form (viewed as a coset modulo $(R^\times)^2$).

**Proposition 6.6.** *Let $L$ be an integral lattice that is* regular *as a quadratic module over $R$. For any primitive submodule $P \subseteq L$,*

$$\det(P^\perp) = \det(E) \cdot \det(P) \ mod \ (R^\times)^2.$$

Note that $\det(E) \in R^\times$ is a unit. So $\det(P^\perp)$ equals $\det(P)$ up to a unit.

*Proof.* Since $P \subseteq E$ and $P^\perp \subseteq E$ are both primitive, they have complements:

$$E = P \oplus Q = P^\perp \oplus R,$$

where $Q, R \subseteq E$ are submodules. Now the $R$-module $E \perp P(-1)$ has determinant

$$\det(E \perp P(-1)) = \det(E) \cdot \det(P(-1)) = (-1)^{\mathrm{rank}(P)} \cdot \det(E) \cdot \det(P);$$

on the other hand, it contains the totally isotropic submodule $P' = \{(x, x) : \ x \in P\}$ and a direct sum decomposition

$$E \perp P(-1) = E \oplus P'.$$

With respect to the decomposition

$$E \perp P(-1) = E \oplus P' = R \oplus P^\perp \oplus P',$$

any Gram matrix decomposes in block form

$$S = \begin{pmatrix} * & * & C \\ * & B & 0 \\ C^T & 0 & 0 \end{pmatrix}$$

where $B$ is a Gram matrix for $P^\perp$ (such that $\det(C) = \det(P^\perp)$) and where $C$ is the matrix of inner products of a basis of $R$ with a basis of $P'$. The matrix $C$ is invertible, because $E$ is regular and $P'$ has trivial inner product with the other summands $P^\perp$ and $P'$ itself. So $\det(C)^2 \in (R^\times)^2$, and

$$\begin{aligned} (-1)^k \det(E)\det(P) &= \det(E \perp P(-1)) \\ &= \det(S) \\ &= (-1)^k \det(B) \cdot \det(C)^2 \\ &= (-1)^k \det(B) = (-1)^k \det(P^\perp) \mod (R^\times)^2, \end{aligned}$$

and $\det(E)\det(P) = \det(P^\perp) \bmod (R^\times)^2$. □

**Example 6.7.** Let $n \in \mathbb{N}$. The $A_n$ *root lattice*, denoted $A_n$, is the orthogonal complement of the all-ones vector $(1, ..., 1)$ in the odd unimodular lattice $\mathbb{Z}^{n+1}$. With respect to the $\mathbb{Z}$-basis $(1, -1, 0, ..., 0)$, $(0, 1, -1, 0, ..., 0)$, ..., $(0, ..., 0, 1, -1)$, it has the Gram matrix

$$\begin{pmatrix} 2 & -1 & 0 & \dots & 0 \\ -1 & 2 & -1 & \dots & 0 \\ 0 & -1 & 2 & \dots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \dots & 2 \end{pmatrix}.$$

Since $P = \mathbb{Z} \cdot (1, ..., 1)$ has determinant

$$\det(P) = (1, ..., 1) \cdot (1, ..., 1) = n + 1,$$

it follows that $A_n = P^\perp$ also has determinant

$$\det(A_n) = n + 1.$$

**Proposition 6.8.** *Let $L$ be an integral lattice over $\mathbb{Z}$, and let $M \subseteq L$ be a subgroup of finite index $[L : M]$. Then*

$$\det(L) = [L : M]^2 \cdot \det(M).$$

*Proof.* By the elementary divisor theorem, there is a basis $e_1, ..., e_n$ of $L$ and elements $d_1, ..., d_n \in R$, $d_1|d_2|...|d_n$ such that $d_1e_1, ..., d_ne_n$ is a basis of $M$. The Gram matrix of $M$ is just the Gram matrix of $L$ with the $i$th row and $i$th column multiplied by $d_i$, so

$$\det(M) = d_1^2 \cdot ... \cdot d_n^2 \cdot \det(L).$$

On the other hand, the quotient module is

$$L/M \cong \mathbb{Z}/d_1 \times ... \times \mathbb{Z}/d_n$$

and the index is $[L : M] = |d_1...d_n|$. □

**Example 6.9.** The *$D_n$ root lattice*, denoted $D_n$, is the subgroup of vectors $x = (x_1, ..., x_n) \in \mathbb{Z}^n$ with $\sum_i x_i \in 2\mathbb{Z}$. Since

$$x \cdot x = \sum_i x_i^2 \equiv \sum_i x_i \equiv 0 \,(\mathrm{mod}\, 2)$$

for any $x \in D_n$, this is an even integral lattice. Since $D_n$ has index two in $\mathbb{Z}^n$, it follows that $\det(D_n) = 4$.

## 6.2. Lattices over $\mathbb{Z}_p$

Fix a prime $p$.

In this section we will describe the structure of $\mathbb{Z}_p$-integral lattices (or quadratic forms). As usual, the theory differs significantly for the prime $p = 2$. Therefore we first suppose that *$p$ is odd*.

**Lemma 6.10.** *Let $p$ be an odd prime and let $L_1$ and $L_2$ be unimodular $\mathbb{Z}_p$-integral lattices. Then $L_1$ and $L_2$ are $\mathbb{Z}_p$-equivalent if and only if the reductions $\overline{L_1}$, $\overline{L_2}$ modulo $p$ are $\mathbb{F}_p$-equivalent.*

*Proof.* A $\mathbb{Z}_p$-equivalence from $L_1$ to $L_2$ reduces mod $p$ to an $\mathbb{F}_p$-equivalence from $\overline{L_1}$ to $\overline{L_2}$. Conversely, an $\mathbb{F}_p$-equivalence from $\overline{L_1}$ to $\overline{L_2}$ lifts by Hensel's lemma[1] to a $\mathbb{Z}_p$-equivalence from $L_1$ to $L_2$. □

**Theorem 6.11.** *Let $p$ be an odd prime and let $L$ be a $\mathbb{Z}_p$-integral lattice. Then $L$ has a* Jordan decomposition

$$L = \bigperp_{i=0}^{\infty} L_i(p^i),$$

*where each $L_i$ is a unimodular lattice. The constituents $L_i(p^i)$ are unique up to $\mathbb{Z}_p$-isometry.*

Here $L_i(p^i)$ means $L_i$ with its bilinear form multiplied by $p^i$. (This $p^i$ is called the *scale* of the constituent $L_i(p^i)$.) The dual lattice is therefore

$$L' = \bigperp_{i=0}^{\infty} L_i(p^{-i}).$$

*Proof.* The existence of such a decomposition can be shown by diagonalizing

$$L = \langle a_1, ..., a_n \rangle$$

and by taking $L_i(p^i)$ to be the sublattice $\langle a_j : \nu_p(a_j) = i \rangle$.
To show uniqueness we use induction on $\text{rank}(L)$. We may assume without loss of generality that $L$ represents numbers of $p$-adic valuation 0, (otherwise $L(p^{-1})$ is integral and represents numbers of lesser valuation).

If $\text{rank}(L) = 1$ then uniqueness is clear. Generally, suppose

$$L = \bigperp_{i=0}^{n} L_i(p^i) = \bigperp_{i=0}^{n} M_i(p^i)$$

are two Jordan decompositions. After reducing mod $p$ we have $\overline{L_i(p^i)} = 0$, $\overline{M_i(p^i)} = 0$ for all $i \geq 1$, (i.e. the quadratic forms are identically zero), hence $\overline{L_0} \cong \overline{M_0}$ by the Witt decomposition theorem over $\mathbb{F}_p$. Since both $L_0$ and $M_0$ are unimodular, we have $L_0 \cong M_0$. By the Witt cancellation theorem, we can remove $L_0$ and $M_0$ and obtain Jordan decompositions

$$\bigperp_{i=1}^{n} L_i(p^i) = \bigperp_{i=1}^{n} M_i(p^i).$$

By the induction hypothesis we have $L_i \cong M_i$ for all $i \geq 1$. □

By the computation of the Witt group $W(\mathbb{F}_p)$, each reduced form $\overline{L_i}$ is uniquely determined up to $\mathbb{F}_p$-equivalence by its rank and the square class of its discriminant. Hence the Jordan constituents $L_i(p^i)$ are uniquely determined by their scale $p^i$, their rank, and the square classes of their determinants.

**Definition 6.12.** Let $p$ be an odd prime and let $L$ be a $\mathbb{Z}_p$-integral lattice with Jordan decomposition

$$L = \bigperp_{i=0}^{\infty} L_i(p^i).$$

The **$p$-adic genus symbol** is the formal symbol

$$1^{\varepsilon_0 r_0} p^{\varepsilon_1 r_1} (p^2)^{\varepsilon_2 r_2} ...,$$

where $r_i = \text{rank}(L_i)$ and where

$$\varepsilon_i = \left(\frac{\det(L_i)}{p}\right) \in \{\pm 1\}.$$

So the $\mathbb{Z}_p$-integral lattice $L$ is determined up to isometry by its genus symbol.

**Example 6.13.** Consider the $A_2$ root lattice as the lattice spanned by basis vectors $x, y$ where

$$x \cdot x = y \cdot y = 2, \quad x \cdot y = -1.$$

We view $A_2$ as a lattice over $\mathbb{Z}_3$. The vector $x$ spans a regular submodule $\langle 2 \rangle$, so we can diagonalize $A_2 \cong \langle 2, ? \rangle$; and $\det(A_2) = 3$ so the diagonalization must be

$$A_2 \cong \langle 2, 3/2 \rangle \cong \langle 2, 6 \rangle$$

over $\mathbb{Z}_3$. Since 2 is a nonsquare, $A_2$ has 3-adic genus symbol $1^{-1}3^{-1}$.

By contrast, the 3-adic quadratic form $A_2(-1) \cong \langle -2, -6 \rangle$ has genus symbol $1^{+1}3^{+1}$.

The situation for integral lattices over $\mathbb{Z}_2$ is complicated. For one thing, lattices are not generally diagonalizable. Even without diagonalizing, we can emulate the Jordan decomposition for $p = 2$ but the constituents are still not generally unique. Also one has to distinguish between even and odd unimodular lattices, and even among unimodular lattices there is an invariant (the oddity).

**Proposition 6.14.** *Let $p = 2$. Then $L$ has a* Jordan decomposition

$$L = \bigperp_{i=0}^{\infty} L_i(2^i),$$

*where each $L_i$ is a unimodular lattice.*

*Proof.* Use induction on rank$(L)$. By rescaling by $2^{-n}$ if necessary, we can assume that $L$ represents numbers of 2-adic valuation 0.
By Proposition 2.5 there is a decomposition

$$L = L_0 \perp F,$$

where $L_0$ is unimodular (written there in the form

$$L_0 = \langle u_1, ..., u_r \rangle \perp \bigperp_{i=1}^{s} E_i,$$

where $u_i \in \mathbb{Z}_2^\times$ and $E_i$ is unimodular and indecomposable of rank two), and where $F$ satisfies $x \cdot y \in p\mathbb{Z}_p$ for every $x, y \in F$. But then $F(2^{-1})$ is an integral lattice of lower rank and therefore has a Jordan decomposition $\perp_{i=1}^{n} L_i(2^{i-1})$, so

$$L = L_0 \perp F = L_0 \perp \bigperp_{i=1}^{n} L_i(2^i). \qquad \square$$

Given a Jordan decomposition $L = \perp_{i=0}^{\infty} L_i(2^i)$ over $\mathbb{Z}_2$, we attach to each block $L_i(2^i)$ the following data:
(i) the *scale* $2^i$;
(ii) the *type*: I if $L_i$ is odd and II if $L_i$ is even;
(iii) the *rank* $r_i = \text{rank}(L_i)$;
(iv) the *sign*

$$\varepsilon_i = \begin{cases} +1: & \det(L_i) \equiv \pm 1 \,(\text{mod}\, 8); \\ -1: & \det(L_i) \equiv \pm 3 \,(\text{mod}\, 8); \end{cases}$$

(v) the *oddity* $t_i$ of $L_i$ (viewed as a quadratic form over $\mathbb{Q}_2$).

The **dyadic genus symbol** of a type I block $L_i(2^i)$ of scale $s$, rank $r$, sign $\pm$ and oddity $t$ is

$$[s^{\pm r}]_t.$$

The **dyadic genus symbol** of a type II block $L_i(2^i)$ of scale $s$, rank $r$ and sign $\pm$ is $[s^{\pm r}]_{\text{II}}$, or simply $s^{\pm r}$.

**Remark 6.15.** The reason that the notation for type II blocks is different is that if $L$ is 2-adically type II unimodular then its oddity is automatically 0. Since any such $L$ decomposes as $L = \perp_{i=1}^{s} E_i$ into type II unimodular planes, it is enough to prove this for each $E_i$; so assume rank$(L) = 2$. Then $L$ is represented by a Gram matrix $\begin{pmatrix} 2a & b \\ b & 2c \end{pmatrix}$ where $b \equiv 1 \bmod 2$, and after diagonalizing over $\mathbb{Q}_2$ we have

$$L \cong \langle 2a, \frac{4ac - b^2}{2a} \rangle \cong \langle 2a, 8a^2c - 2ab^2 \rangle$$

with oddity

$$t(L) = t(\langle 2a \rangle) + t(\langle -2ab^2 \rangle) = 0.$$

**Example 6.16.** Consider the $A_3$ root lattice over $\mathbb{Z}_2$ : choose basis vectors $x_1, x_2, x_3$ with respect to which $A_3$ has Gram matrix $\begin{pmatrix} 2 & -1 & 0 \\ -1 & 2 & -1 \\ 0 & -1 & 2 \end{pmatrix}$.

The vectors $x_1, x_2$ span a sublattice, isometric to $A_2$ with Gram matrix $\begin{pmatrix} 2 & -1 \\ -1 & 2 \end{pmatrix}$, which is 2-adically even unimodular and therefore splits off as an orthogonal direct summand. The remainder is determined by $\det(A_3) = 4$: since $\det(A_2) = 3$, the decomposition must be

$$A_3 \cong A_2 \perp \langle 4/3 \rangle \cong A_2 \perp \langle 3 \rangle(4).$$

The block $A_2$ of scale zero is type II unimodular with determinant 3 (nonsquare), and the block $\langle 3 \rangle$ with scale 4 is type I unimodular with determinant 3 (again nonsquare) and oddity 3. So the dyadic genus symbol is

$$1^{-2}[4^{-1}]_3.$$

**Example 6.17.** The $\mathbb{Z}_2$-lattice $H(2)$ with Gram matrix $\begin{pmatrix} 0 & 2 \\ 2 & 0 \end{pmatrix}$ consists of a single Jordan block, of scale 2, type II, rank 2 and sign + and therefore has genus symbol

$$2^2.$$

The $\mathbb{Z}_2$-lattice $\langle 2, -2 \rangle$ with Gram matrix $\begin{pmatrix} 2 & 0 \\ 0 & -2 \end{pmatrix}$ also consists of a single Jordan block, of the same scale (2), rank (2), sign (+) and oddity (0) as above; but the block is type I and therefore the genus symbol is

$$[2^2]_0.$$

A dyadic genus symbol then specifies an integral lattice uniquely up to $\mathbb{Z}_2$-isometry. **Warning:** unlike the case of odd primes, the genus symbol is not unique! The classification problem for quadratic forms over $\mathbb{Z}_2$ is more technical.[2]

## 6.3. The Hermite constant

Let $(V, \langle -, - \rangle)$ be a regular quadratic space over $\mathbb{Q}$. Since $(\mathbb{Z}^\times)^2 = \{1\}$, the determinant $\det(L)$ of a lattice $L \subseteq V$ is nothing but a rational number. In the case that $V$ is positive-definite one can interpret $\det(L)$ as the square of the *covolume* of $L$,

[2] An algorithm to decide whether two dyadic genus symbols are equivalent is given in Chapter 15 (*On the classification of integral quadratic forms*) of Conway and Sloane's *Sphere packings, lattices and groups*.

i.e. of the volume of a fundamental parallelotope for $V/L$. There is a geometric intuition that if $\det(L)$ is small then some of the points in $L$ must also be relatively small.

The following inequality makes that notion precise: there is indeed a relationship between $|\det(L)|$ and the size of the norms $(x \cdot x)$, $x \in L$. (This is independent of the signature!)

**Theorem 6.18.** *There is a constant $C_n$, depending only on $\dim(V)$, with the property that for any lattice $L \subseteq V$, the minimum*

$$m(L) := \min(|x \cdot x| : \ x \in L, \ x \neq 0)$$

*and the determinant satisfy the inequality*

$$m(L) \leq C_n \cdot |\det(L)|^{1/n}.$$

The best possible constant $C_n$ in this theorem is the *Hermite constant*. The exact values of $C_n$ are known only for $n \leq 8$ and $n = 24$.

The inequality we will prove is actually

$$m(L) \leq (4/3)^{(n-1)/2} \cdot |\det(L)|^{1/n}.$$

*Proof.* We may assume without loss of generality that $L$ is anisotropic (otherwise $m(L) = 0$). The proof uses induction on $n$. If $n = 1$ then trivially $m(L) = |\det(L)|$.

In general, choose a vector $e_1 \in L$ that realizes $m(L) = |e_1 \cdot e_1|$. Then $e_1$ is primitive (if not, then some $e_1/n$ with $n \geq 2$ would be a lattice vector of smaller norm) and can therefore be extended to a $\mathbb{Z}$-basis $e_1, e_2, ..., e_n$. Let $p$ be the orthogonal projection

$$p : V \longrightarrow V, \quad p(x) = x - \frac{x \cdot e_1}{e_1 \cdot e_1} e_1$$

onto the hyperplane $e_1^{\perp}$. Then

$$L' := p(L) = \mathbb{Z}p(e_2) \oplus ... \oplus \mathbb{Z}p(e_n)$$

can be viewed as an $(n-1)$-dimensional lattice in $e_1^{\perp}$. We have

$$|\det(L)| = |\det(\mathbb{Z}e_1 + ... + \mathbb{Z}e_n)| = |\det(\mathbb{Z}e_1 + \mathbb{Z}p(e_2) + ... + \mathbb{Z}p(e_n))| = m(L) \cdot |\det(L')|.$$

In addition, if $x \in L'$ is chosen such that $m(L') = |x \cdot x|$, and $y \in L$ is chosen such that $y = x + te_1$ with $-1/2 \leq t \leq 1/2$, then

$$y \cdot y = x \cdot x + t^2(e_1 \cdot e_1)$$

implies

$$m(L) \leq |y \cdot y| \leq |x \cdot x| + (1/4)|e_1 \cdot e_1| = m(L') + m(L)/4,$$

i.e.

$$m(L) \leq (4/3)m(L').$$

Using the induction assumption for $L'$ we obtain

$$\begin{aligned} m(L) &\leq (4/3)m(L') \\ &\leq (4/3) \cdot (4/3)^{(n-2)/2} |\det(L')|^{1/(n-1)} \\ &= (4/3)^{n/2} \cdot \Big( \frac{1}{m(L)} |\det(L)| \Big)^{1/(n-1)}, \end{aligned}$$

such that

$$m(L)^n \leq (4/3)^{n(n-1)/2} |\det(L)|$$

and finally

$$m(L) \leq (4/3)^{(n-1)/2} |\det(L)|^{1/n}. \qquad \square$$

This leads to a finiteness theorem for lattices of a fixed discriminant:

**Theorem 6.19.** *Let $n$ and $d$ be fixed. Then (up to isometry) there are only finitely many integral lattices $L$ with $\operatorname{rank}(L) = n$ and $|\det(L)| \leq d$.*

*Proof.* Induction on $n$; this is trivial if $n = 1$. Suppose $n > 1$ and let $L$ be a lattice with $\operatorname{rank}(L) = n$ and $|\det(L)| \leq d$.
If $m = m(L) \neq 0$, choose a minimizing vector $x \in L$ with $|x \cdot x| = m$ and define the submodule $M := \mathbb{Z}x$.
Otherwise, let $x \in L$ be primitive with $x \cdot x = 0$, choose a vector $y \in L$ such that

$$(x \cdot y)\mathbb{Z} = x \cdot L$$

as ideals of $\mathbb{Z}$, and define the submodule $M := \mathbb{Z}x \oplus \mathbb{Z}y$. By replacing $y$ by $y + \lambda x$ with $\lambda \in \mathbb{Z}$, such that

$$(y + \lambda x) \cdot (y + \lambda x) = (y \cdot y) + 2\lambda(x \cdot y),$$

we may assume that

$$|y \cdot y| \leq a := |x \cdot y|.$$

Note that $a^2$ divides $\det(L)$, as one can see by considering a Gram matrix for $L$ in a basis whose first vector is $x$.

In either case, there are finitely many possibilities for the submodule $M$. Define the submodule

$$N := L \cap M^{\perp};$$

then the orthogonal projection to $M \otimes \mathbb{Q}$ defines an injective map

$$L/(M \perp N) \longrightarrow M'/M$$

such that $M \perp N \subseteq L$ is a sublattice of index at most $|M'/M| = |\det(M)|$, and therefore

$$|\det(M)| \cdot |\det(N)| = |\det(M \perp N)| \leq |\det(M)|^2 \cdot |\det(L)|.$$

So the determinant of $N$ is bounded by $|\det(N)| \leq |\det(M)| \cdot |\det(L)|$. Since $N$ has lower rank than $L$, by the induction hypothesis there are finitely many possible lattices $N$.

Since

$$M \perp N \subseteq L \subseteq L' \subseteq M' \perp N'$$

it follows that there are only finitely many possiblities for $L$. □

## 6.4. Genera and equivalence classes

A rational quadratic form is determined uniquely by its localizations at $\mathbb{R}$ and at $\mathbb{Q}_p$, $p$ prime.

The analogous statement for *integral* quadratic forms is usually not true. Nevertheless, it defines a useful equivalence relation:

**Definition 6.20.** Let $V$ and $W$ be regular quadratic spaces over $\mathbb{Q}$. Two integral lattices $L \subseteq V$ and $M \subseteq W$ **belong to the same genus** if their localizations

$$L_p \cong M_p$$

are isometric at every place $p \leq \infty$.

For $p < \infty$, we write

$$L_p = L \otimes \mathbb{Z}_p \subseteq V \otimes \mathbb{Q}_p,$$

and at $p = \infty$ we mean $L_\infty = L \otimes \mathbb{R}$.

If $L$ and $M$ belong to the same genus, then the rational quadratic spaces $V = L \otimes \mathbb{Q}$ and $W = M \otimes \mathbb{Q}$ containing them are locally equivalent at every place $p \leq \infty$, hence isometric over $\mathbb{Q}$ by the Hasse–Minkowski principle.
So there is no loss of generality in assuming that $V = W$.

If $L, M \subseteq V$ are integrally equivalent, (i.e. equivalent as quadratic spaces over $\mathbb{Z}$), then they are certainly equivalent over $\mathbb{R}$ and over every $\mathbb{Z}_p$. So each genus splits into equivalence classes.

**Lemma 6.21.** *Integral lattices in the same genus have the same determinant.*

*Proof.* Suppose $L$ and $M$ belong to a common genus. Then $L_p \cong M_p$ at every prime $p$, hence

$$\det(L_p) = \det(M_p) \bmod (\mathbb{Z}_p^\times)^2.$$

So $\det(L)$ and $\det(M)$ contain the same power of $p$.
From $L_\infty \cong M_\infty$ we see that $\det(L)$ and $\det(M)$ have the same sign.
This shows that $\det(L) = \det(M)$ in $\mathbb{Z}$. □

**Example 6.22.** The even, unimodular $\mathbb{Z}$-lattices of any fixed signature $(p, q)$ form a single genus: they are locally equivalent
(i) over $\mathbb{R}$, because they have the same signature;
(ii) over $\mathbb{Z}_p$, $p$ odd, because they have the same genus symbol $1^{\pm(p+q)}$ with $\pm = \left(\frac{-1}{p}\right)^q$;
(iii) over $\mathbb{Z}_2$, because they have the same genus symbol $[1^{p+q}]_{\mathrm{II}}$.

Any such lattice $L \subseteq V$ has oddity 0 mod 8 by Remark 6.15. The oddity equation

$$t_\infty(\mathrm{sgn}(V)) + \sum_{p\,\mathrm{odd}} t_p s_p(V) = t(V) = 0$$

together with the fact that $V$ has local invariants $s_p(V) = 0$ implies

$$\mathrm{sgn}(L) = \mathrm{sgn}(V) \equiv 0 \,(\mathrm{mod}\, 8).$$

So unimodular even $\mathbb{Z}$-lattices can only exist in signature $(p, q)$ with $p - q \equiv 0$ mod 8.

Conversely, if $p \equiv q \,(\mathrm{mod}\, 8)$ then there do exist even unimodular $\mathbb{Z}$-lattices of signature $(p, q)$: Let $E_8$ be the $E_8$ *root lattice*

$$E_8 = D_8 \cup (D_8 + (1/2, ..., 1/2)),$$

where $D_8 \subseteq \mathbb{Z}^8$ is the (even) sublattice of vectors whose sum is even, and $D_8 + (1/2, ..., 1/2)$ is that lattice shifted by $(1/2, ..., 1/2)$. It is not hard to check that this is indeed an even lattice; since it properly contains $D_8$ and $\det(D_8) = 4$, we must have $\det(E_8) = 1$. Then even unimodular lattices of any signature $(p, q)$ with $p \equiv q \,(\mathrm{mod}\, 8)$ can be constructed as direct sums of $E_8, E_8(-1)$ and the hyperbolic plane $H$.

For a similar reason, the odd unimodular $\mathbb{Z}$-lattice of a fixed signature $(p, q)$ also form a single genus. (At $p = 2$ the oddity is determined by the signature mod 8.)

So in any signature $(p, q)$ there are at most two genera of unimodular lattices: there is always the genus $\mathrm{I}_{p,q}$ of odd unimodular lattices; and if $p \equiv q$ mod 8 then there is also the genus $\mathrm{II}_{p,q}$ of even unimodular lattices.

**Theorem 6.23** (Finiteness of the class number)**.** *A genus of integral lattices contains only finitely many equivalence classes.*

*Proof.* The theorem follows immediately from the fact that all lattices in a genus have the same determinant, and that there are finitely many integral lattices (up to integral equivalence) of any fixed determinant and rank by Theorem 6.19. □

**Remark 6.24.** "Finitely many" tends to grow very quickly as the rank of the lattices becomes larger. For example, the class number $h_n$ of the genus of even, unimodular, positive-definite lattices of rank $n$ is known only for $n = 8, 16, 24$:

$$h_8 = 1, \quad h_{16} = 2, \quad h_{24} = 24 \text{ (Niemeier)}.$$

For $n = 32$ the best lower bound is $h_{32} \geq 1,162,109,024$[3].

The following construction is a useful way to understand the different integral lattices that live in a fixed rational quadratic space:

**Proposition 6.25.** *Let $V$ be a regular quadratic space over $\mathbb{Q}$ and let $L \subseteq V$ be a fixed integral lattice. There is a bijection:*

$$\{\textit{integral lattices } M \subseteq V\}$$

$$\leftrightarrow \{\textit{sequences of } \mathbb{Z}_p\textit{-integral lattices } (M_p)_p \textit{ with } M_p = L_p \textit{ for almost all } p\},$$

*under which $M \subseteq V$ corresponds to $M_p = M \otimes \mathbb{Z}_p$. The inverse map sends $(M_p)_p$ to*

$$M := \bigcap_{p \textit{ prime}} (M_p \cap V).$$

*Proof.* Fix bases of $L$ and $M$; then the change-of-basis matrix sending $L$ to $M$ belongs to $\mathrm{GL}_n(\mathbb{Q})$, and is $p$-adically integral at all but finitely many primes $S$. Then $M_p = L_p$ for every $p \notin S$.
Conversely, suppose $(M_p)$ is such a sequence of $\mathbb{Z}_p$-integral lattices. Then

$$M := \bigcap_{p \,\text{prime}} (M_p \cap V)$$

is a $\mathbb{Z}$-integral lattice, because: Let $S$ be a finite set of primes for which $M_p = L_p$ for every $p \notin S$, and at any $p \in S$ choose exponents $a_p, b_p \in \mathbb{Z}$ with

$$p^{a_p}\mathbb{Z}_p \cdot L \subseteq M_p \subseteq p^{b_p}\mathbb{Z}_p \cdot L.$$

[3]Corollary 17 of O. King, *A mass formula for unimodular lattices with no roots*, Math. Comp. **72** (2003), 839–863.

Then we have

$$\begin{aligned}\Big(\prod_{p\in S} p^{a_p}\Big)\cdot L &= \bigcap_{p\,\text{prime}} (p^{a_p}\mathbb{Z}_p L \cap V)\\ &\subseteq \bigcap_{p\,\text{prime}} (M_p \cap V)\\ &\subseteq \bigcap_{p\,\text{prime}} (p^{b_p}\mathbb{Z}_p L \cap V) = \Big(\prod_{p\in S} p^{b_p}\Big)\cdot L,\end{aligned}$$

which shows that $M$ is a lattice. For any $x \in M$, we have

$$x \cdot x \in \bigcap_{p\,\text{prime}} (\mathbb{Z}_p \cap \mathbb{Q}) = \mathbb{Z},$$

so $M$ is integral.

These correspondences are inverse to one another, because: if $M$ is an integral lattice with basis $e_1, ..., e_n$, then $\mathbb{Z}_p M \cap V$ consists of rational linear combinations of $e_1, ..., e_n$ that do not have $p$ in the denominator, so

$$\bigcap_{p\,\text{prime}} (\mathbb{Z}_p M \cap V)$$

consists exactly of rational linear combinations of $e_1, ..., e_n$ in which all coordinates are integers; i.e. it is $M$. On the other hand, suppose $(M_p)$ is a sequence of $\mathbb{Z}_p$-integral lattices as in the theorem, and define

$$M := \bigcap_{p\,\text{prime}} (M_p \cap V).$$

Then we certainly have

$$\mathbb{Z}_q \otimes M \subseteq \mathbb{Z}_q \otimes M_q = M_q$$

at every prime $q$. This is an equality, because: let $e_1, ..., e_n$ be a $\mathbb{Z}$-basis of the lattice $M$. Then $e_1, ..., e_n$ is also a $\mathbb{Q}_q$-basis of $M_q$. Let $x \in M_q$ be any element, write

$$x = \sum_{i=1}^{n} a_i e_i, \quad a_i \in \mathbb{Q}_q,$$

and fix $n \in \mathbb{N}$ such that we can decompose

$$a_i = \frac{b_i}{q^n} + c_i, \quad \text{where } b_i \in \mathbb{Z},\ c_i \in \mathbb{Z}_q.$$

Then

$$\sum_{i=1}^{n} c_i e_i \in \mathbb{Z}_q \otimes M$$

and

$$\sum_{i=1}^{n} \frac{b_i}{q^n} e_i \in (M_q \cap V);$$

and trivially $\sum_{i=1}^{n} \frac{b_i}{q^n} e_i \in M_p \cap V$ for every $p \neq q$. So

$$\sum_{i=1}^{n} \frac{b_i}{q^n} e_i \in \bigcap_p (M_p \cap V) = M$$

and therefore

$$x = \Big( \sum_{i=1}^{n} c_i e_i \Big) + \Big( \sum_{i=1}^{n} \frac{b_i}{q^n} e_i \Big) \in \mathbb{Z}_q \otimes M. \qquad \square$$

**Theorem 6.26.** *Let $L$ be an integral lattice in a regular quadratic space $(V, Q)$. Let $t \in \mathbb{Q}$. The following are equivalent:*
*(i) $L_p$ represents $t$ for every $p \leq \infty$;*
*(ii) There is a lattice $M$ in the genus of $L$ that represents $t$.*

*Proof.* (ii) $\Rightarrow$ (i) holds because $L_p \cong M_p$ for all $p \leq \infty$ (by definition of genus), and because $M$ already represents $t$.
(i) $\Rightarrow$ (ii): By the Hasse–Minkowski theorem, $V = L \otimes \mathbb{Q}$ represents $t$; choose $x \in V$ with $Q(x) = t$. Let $S$ be the (finite) set of primes for which $x \notin L_p$, i.e. the set of primes that occur in the denominators of the coordinates of $x$. For each $p \in S$, choose a vector $x_p \in L_p$ with $Q(x_p) = t$. Then $x$ and $x_p$ span isometric sublattices in $V_p$. By the Witt extension theorem, there exists $u_p \in \mathrm{O}(V_p)$ such that

$$x = u_p x_p \text{ for all } p \in S.$$

Now we define the integral lattice

$$M := \bigcap_{p \notin S} (L_p \cap V) \cap \bigcap_{p \in S} (u_p L_p \cap V) \subseteq V,$$

which satisfies $M_p = L_p$ for $p \notin S$ (including $p = \infty$) and $M_p = u_p L_p \cong L_p$ for $p \in S$. So $M$ belongs to the genus of $L$. By construction, $x \in M$ represents $t$. $\square$

This is a "local-global principle" for genera of lattices that consist of only a single equivalence class.

**Example 6.27.** The genus of the (odd) unimodular lattice $\mathbb{Z}^n$ consists of a single class for $1 \leq n \leq 5$.
(In fact, this is true for $1 \leq n \leq 8$. For $n = 9$ we already have two non-isomorphic

classes $\langle 1, ..., 1\rangle$ and $\langle 1\rangle \perp E_8$ in the genus $\mathrm{I}_{9,0}$, and the situation deteriorates rapidly as $n$ grows.)
Proof: Any lattice $L$ in the genus of $\mathbb{Z}^n$ has $\det(L) = 1$. By Hermite's inequality its minimum is

$$m(L) = \min(x \cdot x : \ x \in L\backslash\{0\}) \leq (4/3)^{(n-1)/2},$$

which is $< 2$ for $n \leq 5$. In particular there exists $x \in L$ with $x \cdot x = 1$. This spans a regular submodule that can be split off:

$$L = \langle 1\rangle \perp \tilde{L},$$

where $\tilde{L}$ is also odd unimodular, hence belongs to the genus of $\mathbb{Z}^{n-1}$. The claim follows by induction.

**Example 6.28** (Sums of two squares)**.** A number $t \in \mathbb{N}$ can be written as a sum of two integral squares if and only if $\nu_p(t)$ is even for every prime $p \equiv 3\,(4)$.

*Proof.* Since $\langle 1, 1\rangle$ is alone in its genus, it is enough to check representability over the $p$-adic integers.
The form $\langle 1, 1\rangle$ is hyperbolic over $\mathbb{Z}_p$ at every prime $p \equiv 1\,(4)$, so it represents everything. Over $p \equiv 3\,(4)$ or $p = 2$, it represents $t$ over $\mathbb{Z}_p$ if and only if it represents $t$ over $\mathbb{Q}_p$. (For $p \equiv 3\,(4)$, this is because $x^2 + y^2 \equiv 0 \bmod p$ has only the trivial solution $x \equiv y \equiv 0 \bmod p$, since $-1$ is not a square. So $p$ cannot occur in the denominator of a solution $x^2 + y^2 = t$ with $t$ integral. At $p = 2$ this is similarly because 0 is not a sum of two odd squares modulo 8.) So:

$$\begin{aligned}
& t \text{ is a sum of two integer squares} \\
\Leftrightarrow\ & t \text{ is a sum of two squares in } \mathbb{Z}_p \text{ for every prime } p \\
\Leftrightarrow\ & t \text{ is a sum of two squares in } \mathbb{Q}_p \text{ for every prime } p \\
\Leftrightarrow\ & t \text{ is a sum of two rational squares} \\
\Leftrightarrow\ & \nu_p(t) \text{ is even for every prime } p \equiv 3\,(4).
\end{aligned}$$

□

**Example 6.29** (Sums of three squares)**.** A number $t \in \mathbb{N}$ can be written as a sum of three integral squares if and only if it is not of the form $t = 4^a n$ with $n \equiv 7 \bmod 8$.

*Proof.* Again $\langle 1, 1, 1\rangle$ is alone in its genus, so it is enough to check representability over $\mathbb{Z}_p$.
At every odd prime, $\langle 1, 1, 1\rangle$ splits a hyperbolic plane and therefore represents everything.
Over $p = 2$, it represents $t$ over $\mathbb{Z}_2$ if and only if it represents $t$ over $\mathbb{Q}_2$: if we can write

$$t = x^2 + y^2 + z^2, \quad x, y, z \in \mathbb{Q}_2$$

where $x, y, z$ are not all integers, then clearing denominators yields a representation $0 \equiv a^2 + b^2 + c^2$ modulo 4 where at least one of $a, b, c$ is odd, which is impossible. The condition of representing $t$ over $\mathbb{Q}_2$ was $t \neq 4^a n$ with $n \equiv 7 \bmod 8$. □

**Corollary 6.30** (Lagrange four-square theorem)**.** *Every $t \in \mathbb{N}$ can be written as a sum of four integral squares.*

*Proof.* Every integer that is not of the form $t = 4^a n$ with $n \equiv 7 \bmod 8$ is already a sum of three integral squares. If $t$ is of that form, then $t - 4^{a+1}$ is positive and *not* of that form, so it is represented as a sum $x^2 + y^2 + z^2$ of three integral squares. Then

$$t = x^2 + y^2 + z^2 + (2^{a+1})^2$$

is a representation of $t$ as a sum of four integral squares. □

## 6.5. Spinor genera

Integral lattices $L \subseteq V$ and $M \subseteq W$ belong to the same *class* if there is an isometry $u : V \to W$ of quadratic $\mathbb{Q}$-spaces for which $u(L) = M$. And $L$ and $M$ belong to the same genus if there are isometries $u_p : V_p \to W_p$ over every localization with the property $u_p(L_p) = M_p$.

Spinor genera of lattices fit somewhere between the notions of genus and equivalence class. In practice, the genus of a lattice almost always consists of a single spinor genus (more on this later).

**Definition 6.31.** $L$ and $M$ belong to the same **spinor genus** if there are isometries $u : V \to W$ and $v_p \in \mathrm{SO}(V_p)$, $p \leq \infty$ with the property:
(i) $uv_p(L_p) = M_p$ for every $p \leq \infty$;
(ii) $v_p$ has trivial spinor norm.

Similarly to the usual notion of genus, if $L \subseteq V$ is an integral lattice then all classes of lattices in the spinor genus of $L$ are represented by other lattices in $V$.

Recall that the ($p$-adic) spinor norm is a homomorphism

$$N : \mathrm{SO}(V_p) \longrightarrow \mathbb{Q}_p^\times / (\mathbb{Q}_p^\times)^2$$

with the property that, if $u \in \mathrm{SO}(V_p)$ is written as a product of reflections $\sigma_{x_1} ... \sigma_{x_n}$, then

$$N(u) = \prod_i Q(x_i) \cdot (\mathbb{Q}_p^\times)^2.$$

The most important property of the spinor genus is that, for indefinite lattices, it very often consists of a single equivalence class. This follows from *strong approximation* for the orthogonal and spin groups, which we cite without proof.[4]

[4]See Satz 24.1, 24.2, 24.6 of Kneser.

**Theorem 6.32** (Strong approximation for orthogonal groups)**.** *Let $L \subseteq V$ be an integral lattice in a regular quadratic space over $\mathbb{Q}$ with $\dim(V) \geq 3$. Let $T$ be a set consisting of $\{\infty\}$ and a finite number of primes, and let $\ell \in T$ be a place for which $V_\ell$ is isotropic. Let*

$$\mathrm{SO}'(V) := \{u \in \mathrm{SO}(V) : \ N(u) = 1\}$$

*be the spinor kernel and let $\mathrm{Spin}(V)$ be the spin group. Define the subgroups*

$$\begin{aligned} \mathrm{O}(L;T) &= \{u \in \mathrm{O}(V) : \ uL_p = L_p \text{ for every } p \notin T\}; \\ \mathrm{SO}'(L;T) &= \mathrm{O}(L;T) \cap \mathrm{SO}'(V); \\ \mathrm{Spin}(L;T) &= \{u \in \mathrm{Spin}(V) : \ u \in C_0(L_p) \text{ for every } p \notin T\}. \end{aligned}$$

*Then the images of the embeddings*

$$\mathrm{Spin}(L;T) \longrightarrow \prod_{p \in T\setminus\{\ell\}} \mathrm{Spin}(V_p)$$

*and*

$$\mathrm{SO}'(L;T) \longrightarrow \prod_{T\setminus\{\ell\}} \mathrm{SO}'(V_p)$$

*are dense.*

So: any family of finitely many transformations $u_p \in \mathrm{SO}'(V_p)$, $p \in T\setminus\{\ell\}$, all of trivial spinor norm, can simultaneously be approximated arbitrarily well by a single $u \in \mathrm{SO}'(V)$ which "almost" preserves $L$, and the same is true for the spin cover.

**Theorem 6.33.** *Let $L$ be an indefinite integral lattice of rank at least three. Then all lattices in the spinor genus of $L$ are equivalent over $\mathbb{Z}$.*

*Proof.* Let $V = L \otimes \mathbb{Q}$ and let $M \subseteq V$ be another lattice in the spinor genus of $L$. Let $u \in \mathrm{O}(V)$ be an isometry such that $uv_p(L_p) = M_p$ for all $p \leq \infty$ and $v_p$ has trivial spinor norm. By Proposition 6.25 we have $v_p = \mathrm{id}$ for all but finitely many primes; let $T$ be the set $\{\infty\}$ together with all primes $p$ with $v_p \neq \mathrm{id}$. Using strong approximation with the exceptional place $\ell = \infty$, construct $v \in \mathrm{SO}'(L;T)$ such that

$$v(L_p) = v_p(L_p) \text{ for every } p \in T\setminus\{\infty\}$$

and

$$v(L_p) = L_p \text{ for every } p \notin T.$$

Then $uvL_p = M_p$ for every $p < \infty$ and therefore $uv$ is an integral equivalence from $L$ to $M$. □

**Remark 6.34.** By the same argument, if $L \subseteq V$ is a **definite** integral lattice of rank at least three and $\ell$ is any prime with $\ell \nmid \det(L)$, then every class in the spinor genus of $L$ is represented by a lattice $M \subseteq V$ with $L_p = M_p$ for all $p$ **except** $p = \ell$. Unfortunately we really need an exceptional prime $\ell$: there are generally many equivalence classes in a spinor genus of definite lattices.

**Remark 6.35.** The condition that the rank is at least three is necessary - equivalence of indefinite binary quadratic forms behaves differently. This is related to the problem of computing class numbers of orders in real-quadratic fields. As an example, consider the genus of indefinite binary quadratic forms of discriminant $p = 229$ (a prime). These really form a single genus: they are all equivalent over $\mathbb{R}$ because they have the same signature $(1, 1)$; over $\mathbb{Q}_2$ because they are type II unimodular with the same determinant; and they have Hasse invariant $-1$ over $\mathbb{Q}_p$ by Hilbert reciprocity, hence $p$-adic genus symbol $1^{-1}p^{-1}$. They also happen to form a single spinor genus. However, there are three distinct $\mathbb{Z}$-equivalence classes of such quadratic forms, represented by

$$X^2 + 15XY - Y^2, \quad 3X^2 + 13XY - 5Y^2, \quad 5X^2 + 13XY - 3Y^2.$$

We will now show that a genus "usually" contains only a single spinor genus - more precisely, as long as the determinant does not contain primes to very high powers. The difficulty consists essentially in determining which numbers can be realized as spinor norms.

**Lemma 6.36.** *Let $(V, Q)$ be a regular quadratic space over $\mathbb{Q}$ with $\dim(V) \geq 3$. Let $a \in \mathbb{Q}^\times$, (and if $V$ is definite then suppose $a > 0$). Then there exists an isometry $u \in \mathrm{SO}(V)$ with spinor norm*

$$N(u) = a \cdot (\mathbb{Q}^\times)^2.$$

*Proof.* We have to show that $Q$ represents two numbers (or an even number of numbers) whose product is $a$.
If $\dim(V) \geq 4$, then $Q$ represents every rational number (if $V$ is indefinite) or it represents exactly the positive or negative rational numbers (if $V$ is positive or negative definite) as a consequence of the Hasse–Minkowski theorem. Then the result easily follows.

Suppose $\dim(V) = 3$ and let $d \in \mathbb{Q}^\times$ represent $\mathrm{disc}(V)$ modulo $(\mathbb{Q}^\times)^2$. Then there is a finite set $S$ of primes such that if $p \notin S$, then $Q$ represents every $p$-adic number. (More precisely, $V_p$ is isotropic whenever $\nu_p(d)$ is even, which is the case for all but finitely many primes.) If $Q$ does *not* represent a number $c \in \mathbb{Q}_p$ for some prime $p$ then $V_p \perp \langle -c \rangle$ is the four-dimensional anisotropic quadratic space over $\mathbb{Q}_p$ so it has discriminant 1, and therefore

$$c \in -d \cdot (\mathbb{Q}_p^\times)^2.$$

Now at every $p \in S$, choose a number $b_p \in \mathbb{Q}_p^\times$ for which

$$b_p \neq -d, -ad \bmod (\mathbb{Q}_p^\times)^2.$$

By construction there exist vectors $x_p \in V_p$ such that $Q(x_p) = b_p$. Choose a vector $x \in V$ that approximates the elements $x_p$ closely enough that

$$Q(x) \equiv Q(x_p) \bmod (\mathbb{Q}_p^\times)^2 \quad \text{for all } p \in S \cup \{\infty\},$$

(where as usual we write $\mathbb{Q}_\infty := \mathbb{R}$).

By construction, $a/Q(x) \neq -d \bmod (\mathbb{Q}_p^\times)^2$ for each exceptional prime $p \in S$, so $Q$ represents $a/Q(x)$ locally at all $p \in S$. Also, $a/Q(x)$ is represented at any $p \notin S$ anyway (including $\infty$, because if $V$ is definite then $a/Q(x)$ has the correct sign). By the Hasse–Minkowski theorem, there exists $y \in V$ such that $a/Q(x) = Q(y)$. Therefore

$$a = Q(x)Q(y) = N(\sigma_x \sigma_y)$$

is the spinor norm of $\sigma_x \sigma_y \in \mathrm{SO}(V)$.

□

**Theorem 6.37.** *Let $L \subseteq V$ be an integral lattice in a regular quadratic space over $\mathbb{Q}$ with $\dim(V) \geq 3$. Suppose that for every prime $p < \infty$ and every $a \in \mathbb{Z}_p^\times$ there exists $\gamma_p \in \mathrm{SO}(L_p)$ such that*

$$N(\gamma) = a \cdot (\mathbb{Q}_p^\times)^2.$$

*Then the genus of $L$ contains only one spinor genus.*

A number $a \in \mathbb{Z}_p^\times$ that can be realized as the spinor norm of $\gamma_p \in \mathrm{SO}(L_p)$ is also called a **$p$-adically automorphous number** for $L$.

*Proof.* Let $M \subseteq V$ be any lattice in the genus of $L$. For each $p < \infty$, write $M_p = u_p(L_p)$ with $u_p \in \mathrm{SO}(V_p)$, where $u_p = \mathrm{id}$ for all but finitely many primes $p \in S$. (There is no loss of generality in assuming $\det(u_p) = 1$, since every $p$-*adic* lattice $L_p$ admits automorphisms of determinant $-1$: if $L_p$ is rescaled such that the vectors of minimal length are units, then the reflection along any such vector will work.) For $p \in S$, write the spinor norm of $u_p$ as

$$N(u_p) = p^{\alpha_p} \cdot b_p \bmod (\mathbb{Q}_p^\times)^2$$

where $b_p \in \mathbb{Z}_p$. By the lemma, there exists $u \in \mathrm{SO}(V)$ with

$$N(u) = \prod_{p \in S} p^{\alpha_p} \bmod (\mathbb{Q}^\times)^2,$$

such that $N(u^{-1}u_p) = b_p \bmod (\mathbb{Q}_p^\times)^2$. By assumption, $b_p$ can be realized as the spinor

norm of $\gamma_p \in \mathrm{SO}(L_p)$. Then

$$M_p = uu^{-1}u_p\gamma_p \cdot L_p$$

where $u \in \mathrm{SO}(V)$ and $u^{-1}u_p\gamma_p$ has trivial spinor norm, so $M$ and $L$ belong to the same spinor genus. □

Suppose $p \neq 2$ and $L$ has been put in normal form as

$$L_p = \bigperp_{i \geq 0} L_i(p^i), \quad L_i \text{ unimodular.}$$

Then the condition

$$\mathbb{Z}_p^\times \cdot (\mathbb{Q}_p^\times)^2 \subseteq N(\mathrm{SO}(L_p))$$

is satisfied as long as any $L_i$ has rank at least two: in this case, $L_i$ represents every number over $\mathbb{Q}_p$ and therefore also over $\mathbb{Z}_p$, and we already have

$$\mathbb{Z}_p^\times \cdot (\mathbb{Q}_p^\times)^2 \subseteq N(\mathrm{SO}(L_i)) = N(\mathrm{SO}(L_i(p))).$$

This works similarly over $p = 2$ if $L$ contains a *regular two-dimensional summand* in its orthogonal decomposition over $\mathbb{Z}_2$. Suppose it does not, i.e. $L_2$ is diagonalizable, and write

$$L = \bigperp_i \langle 2^{\alpha_i} b_i \rangle, \quad \alpha_i \in \mathbb{N}_0,\ b_i \in \mathbb{Z}_2^\times.$$

If any three exponents $\alpha_i = \alpha_j = \alpha_k$ are equal for pairwise distinct $i, j, k$, so there are orthogonal $e_i, e_j, e_k \in L_2$ with

$$\langle e_i, e_i \rangle = 2^{\alpha_i} b_i, \quad \langle e_j, e_j \rangle = 2^{\alpha_j} b_j, \quad \langle e_k, e_k \rangle = 2^{\alpha_k} b_k,$$

then we can decompose

$$\mathbb{Z}_2 e_i \perp \mathbb{Z}_2 e_j \perp \mathbb{Z}_2 e_k = \mathbb{Z}_2(e_i + e_j + e_k) \perp N$$

with a regular two-dimensional summand $N$ and apply the earlier argument. Also, if any three exponents differ by at most one, say $\alpha_i = \alpha_j = \alpha_k - 1$ (the case $\alpha_i = \alpha_j = \alpha_k + 1$ is analogous), and choose orthogonal $e_i, e_j, e_k$ as before, then $\mathrm{O}(L_2)$ contains the reflections through the vectors

$$e_i, e_i + 2e_j, e_i + e_k$$

of norms

$$Q(e_i) = 2^{\alpha_i} b_i, \quad Q(e_i + 2e_j) = 2^{\alpha_i}(b_i + 4b_j), \quad Q(e_i + e_k) = 2^{\alpha_i}(b_i + 2b_k).$$

So the image of the spinor group contains elements of norm

$$N = Q(e_i + 2e_j)/Q(e_i) = 1 + 4(b_j/b_i) \equiv 5 \bmod 8$$

and

$$N = Q(e_i + e_k)/Q(e_i) = 1 + 2(b_k/b_i) \equiv 3 \bmod 4,$$

and therefore all of $\mathbb{Z}_2^\times \cdot (\mathbb{Q}_2^\times)^2$.

We summarize this below:

**Theorem 6.38.** *Let $L$ be an integral lattice with $\mathrm{rank}(L) \geq 3$. Suppose:*
*(i) Over any odd prime $p$, the normal form*

$$L_p = \bigperp_{i\geq 0} L_i(p^i), \quad L_i \text{ unimodular}$$

*contains at least one summand with $\mathrm{rank}(L_i) \geq 2$;*
*(ii) Over $p = 2$, **either** $L_2$ is not diagonalizable **or** $L_2$ is diagonalizable, and in*

$$L_2 = \bigperp_{i} \langle 2^{\alpha_i} b_i \rangle$$

*there are three exponents $\alpha_i, \alpha_j, \alpha_k$ that belong to a set of the form $\{n, n+1\}$.*
*Then the genus of $L$ consists of a single spinor genus.*

**Corollary 6.39.** *Suppose $L$ and $M$ are integral lattices that belong to the same genus. Then*

$$L \perp H \cong M \perp H$$

*are $\mathbb{Z}$-equivalent.*

The converse is also true: if $L \perp H \cong M \perp H$ over $\mathbb{Z}$, then $L_p \perp H \cong M_p \perp H$ at every $p \leq \infty$, and the Witt cancellation theorem over $\mathbb{Z}_p$ or $\mathbb{R}$ implies that $L_p \cong M_p$, hence $L$ and $M$ belong to the same genus.

*Proof.* Certainly $L \perp H$ and $M \perp H$ also belong to the same genus. That genus consists of a single spinor genus because $L \perp H$ splits a regular direct summand of rank two over $\mathbb{Z}$, (namely $H$), and therefore over every prime $p$. The spinor genus consists of a single $\mathbb{Z}$-equivalence class because $L \perp H$ is indefinite. □

**Corollary 6.40.** *Let $L$ be an even integral lattice with $n = \mathrm{rank}(L) \geq 3$. Suppose:*
*(i) $\det(L)$ is not divisible by $2^m$, where $m = \lfloor (n^2+1)/2 \rfloor$, and*
*(ii) $\det(L)$ is not divisible by $p^{n(n-1)/2}$ for any odd prime $p$.*
*Then the genus of $L$ consists of a single spinor genus.*

For odd integral lattices the condition (i) is weakened to $m = \lfloor (n^2+1)/2 \rfloor - n$, while condition (ii) stays the same.

*Proof.* Let $p$ be an odd prime and suppose the normal form of $L_p$ *fails* to contain a summand of rank $\geq 2$. Then $L_p$ must split in the form

$$L_p = \bigperp_{i\geq 0} \langle p^{\alpha_i} b_i \rangle, \quad b_i \in \mathbb{Z}_p^\times$$

where all $\alpha_i$ are pairwise distinct. So we have

$$\alpha_0 \geq 0,\ \alpha_1 \geq 1,\ \alpha_2 \geq 2, ...$$

and therefore

$$\nu_p(\det(L_p)) \geq 0 + 1 + 2 + ... + (n-1) = n(n-1)/2.$$

For $p = 2$, if $L_2$ is diagonalizable and fails to contain three exponents belonging to any set $\{n, n+1\}$, then after ordering the exponents we have

$$\alpha_{2n} \geq \alpha_{2n-1} \geq 2n - 1$$

and therefore

$$\nu_2(\det(L_2)) \geq 1 + 1 + 3 + 3 + 5 + 5 + ... = \lfloor (n^2+1)/2 \rfloor.$$

If $L$ is odd then we can only deduce

$$\nu_2(\det(L_2)) \geq 0 + 0 + 2 + 2 + 4 + 4 + ... = \lfloor (n^2+1)/2 \rfloor - n.$$

□

**Corollary 6.41.** *(i) Suppose $m, n \geq 1$. Then the genus $\mathrm{I}_{m,n}$ of odd indefinite lattices consists of a single equivalence class.*
*(ii) Suppose $m, n \geq 1$ and $m \equiv n \bmod 8$. Then the genus $\mathrm{II}_{m,n}$ of even indefinite lattices consists of a single equivalence class.*

*Proof.* Except for the cases $\mathrm{I}_{1,1}$, $\mathrm{II}_{1,1}$ of rank two, both claims follow from the above discussion: since $\mathrm{I}_{m,n}$ and $\mathrm{II}_{m,n}$ are unimodular, the bound on the discriminant is satisfied and each genus consists of a single spinor genus. Since these lattices are unimodular, the spinor genus consists of a single $\mathbb{Z}$-equivalence class.

The genera $\mathrm{I}_{1,1}$ and $\mathrm{II}_{1,1}$ can be treated directly. Any lattice in either genus is isotropic, and therefore represented by the Gram matrix $\begin{pmatrix} 0 & a \\ a & b \end{pmatrix}$ where $a, b \in \mathbb{Z}$; and by substituting $(e_1, e_2) \mapsto (\pm e_1, e_2 + \lambda e_1)$ with a suitably chosen $\lambda$, one can assume modulo $\mathbb{Z}$-equivalence that $0 \leq |b| \leq a$. Such a lattice is unimodular only if $a = 1$ and $b \in \{-1, 0, 1\}$. The case $b = 0$ is then the unique class in $\mathrm{II}_{1,1}$, while the cases $b = \pm 1$ are equivalent and represent the unique class in $\mathrm{I}_{1,1}$. □

**Corollary 6.42.** *All members of the genus of any lattice of the form $L \perp H(N)$, ($N \in \mathbb{N}$, $L$ an integral lattice) are equivalent over $\mathbb{Z}$.*

*Proof.* For $\operatorname{rank}(L) \geq 1$, this follows from Theorem 6.38 because the normal form decomposition of $L \perp H(N)$ at any prime contains a rank two rescaled unimodular direct summand. If $L = \{0\}$ one can show directly that $H(N)$ is alone in its genus. $\square$

**Example 6.43.** For an example[5] of quadratic forms in the same genus that belong to distinct spinor genera, consider the even lattice $L$ with quadratic form

$$Q(X, Y, Z) = X^2 + Y^2 + 16Z^2.$$

After reducing $Q$ mod 8 we find that $Q$ represents only numbers that are $0, 1, 2, 4, 5$ modulo 8, and no products of these numbers land in the cosets of 3 or 7 modulo $(\mathbb{Q}_2^\times)^2$. Therefore 3 and 7 are not 2-adically automorphous: the square classes of 3 and 7 are not realized as spinor norms of any $\gamma \in \mathrm{SO}(L_2)$.
If we define $M_p = L_p$ for $p \neq 2$ and $M_2 = uL_2$ for any $u \in \mathrm{SO}(L \otimes \mathbb{Q}_2)$ of spinor norm 3 (which exists as $Q$ does represent 3 over $\mathbb{Q}_2$) then we get a representative

$$M = \bigcap_{p\,\text{prime}} (M_p \cap V)$$

of the second spinor genus. To be explicit one can take the Gram matrix $\begin{pmatrix} 4 & 0 & 2 \\ 0 & 4 & 2 \\ 2 & 2 & 10 \end{pmatrix}$.

## 6.6. Indecomposable lattices

**Definition 6.44.** An integral lattice $L$ is **decomposable** if it can be written as an orthogonal direct sum of two proper sublattices:

$$L = M \perp N, \quad \operatorname{rank}(M),\ \operatorname{rank}(N) \geq 1.$$

$L$ is **indecomposable** if it is not decomposable.

Any integral lattice can be decomposed as

$$L = \bigperp_i L_i$$

where each $L_i$ is indecomposable. The natural question is: to what extent are the sublattices $L_i$ unique?

Call a vector $x \in L$ **indecomposable** if it *cannot* be written as a sum

$$x = y + z, \quad y, z \neq 0,\ y \cdot z = 0.$$

[5] from Will Jagy on mathoverflow: https://mathoverflow.net/questions/83989/spin-representation

We define an equivalence relation $\sim$ on the indecomposable vectors $x \in L$ as follows: say $x \sim y$ if there is a chain of indecomposable vectors $x = x_0, x_1, ..., x_{r-1}, x_r = y$ with the property

$$x_i \cdot x_{i+1} \neq 0.$$

**Lemma 6.45.** *Let $L$ be an integral lattice. Suppose $L$ can be generated by a set $x_1, ..., x_n$ of indecomposable vectors, all of which belong to the same $\sim$ equivalence class: $x_i \sim x_j$. Then $L$ is indecomposable.*

*Proof.* Suppose we can split $L = M \perp N$. Write

$$x_i = y_i + z_i, \quad y_i \in M,\ z_i \in N.$$

Since $y_i \cdot z_i = 0$ and each $x_i$ is indecomposable, one of $y_i$ and $z_i$ must be zero; so each $x_i$ belongs either to $M$ or to $N$. Without loss of generality, say $x_1 \in M$.
But if $x \sim y$ and $x$ belongs to $M$, then $y$ also belongs to $M$. So all $x_i$ belong to $M$. Since the $x_i$ generate $L$, it follows that $L = M$ and $N = \{0\}$. □

**Example 6.46.** Suppose $R$ is a simple root system of $ADE$ type, and $L$ is the $\mathbb{Z}$-span of the roots. (These are the $A_n$ root lattices, the $D_n$ root lattices with $n \geq 4$, and the exceptional lattices $E_6, E_7, E_8$.) The roots are indecomposable vectors of $L$ by virtue of having the smallest possible norm. Since the root system is simple, all roots belong to a single $\sim$-equivalence class. So $L$ is indecomposable.

**Theorem 6.47** (Lattice decomposition)**.** *(i) Let $L$ be a positive-definite integral lattice. Then $L$ can be written*

$$L = \bigperp_i L_i$$

*as an orthogonal direct sum of indecomposable lattices $L_i$, and the lattices $L_i$ are **unique** up to relabelling the indices $i$.*
*(ii) The indecomposable summands $L_i \leq L$ are exactly the spans of equivalence classes of indecomposable vectors of $L$.*

The uniqueness of this decomposition is *completely* false for indefinite lattices! Consider the examples in the prior section.

*Proof.* It is clear that a decomposition into indecomposable lattices exists; we need to show that it is unique.
Let $L = \bigperp_i L_i$ be such a decomposition and write $x \in L$ is written in the form $x = \sum_i x_i$ with $x_i \in L_i$. If any two components $x_i$ are nonzero, then $x$ is decomposable. Hence any indecomposable vector lies entirely in one of the components $L_i$; moreover, any

two indecomposable vectors $x, y \in L$ with $x \sim y$ belong to the same component. Let $M_i \subseteq L_i$ be the sublattice spanned by the indecomposable vectors; then $M_i$ is itself indecomposable. Moreover, we have

$$L = \bigperp_i M_i,$$

because any vector $x \in L$ can be written as a sum of indecomposable vectors. (If $x$ is not already indecomposable, then we can write $x = y + z$ with $y \cdot z = 0$ and $y, z \neq 0$, such that $0 < Q(y), Q(z) < 0$. Therefore, the process of repeatedly decomposing the summands $y$ and $z$ will terminate after finitely many steps. *Here is where we use the fact that $L$ is definite.*) It follows that $L_i = M_i$ for all $i$, which proves (ii) and also the uniqueness of (i). □

**Corollary 6.48** (Cancellation for definite lattices)**.** *Suppose $L, M, N$ are positive-definite integral lattices with*

$$L \perp M \cong L \perp N.$$

*Then $M \cong N$.*

*Proof.* This follows from the uniqueness of the decomposition into indecomposables of $M, N$ and $L \perp M, L \perp N$. □

## 6.7. Lattice neighbors

Kneser's method of *lattice neighbors* is a powerful method of computing the equivalence classes in a (spinor) genus of lattices.

Let $V$ be a fixed positive-definite rational quadratic space over $\mathbb{Q}$.

**Definition 6.49.** Let $p$ be a prime. Integral lattices $L, M \subseteq V$ are called **$p$-neighbors** if

$$[L : L \cap M] = [M : L \cap M] = p.$$

We write $L \sim_p M$ if $L$ and $M$ are $p$-neighbors. Note that $\sim_p$ is not generally an equivalence relation (it is usually not transitive).

If $L \sim_p M$ then since

$$\det(L) \cdot p^2 = \det(L \cap M) = \det(M) \cdot p^2,$$

it follows that lattices that are $p$-neighbors have the same determinant.

If $L$ and $M$ are $p$-neighbors then there is a rational change-of-basis matrix, whose denominator only contains powers of $p$, from $L$ to $M$. In particular $L_q$ and $M_q$ are **equal** for all $q \neq p$ (including $\infty$).

If $p \nmid \det(L)$ and $p \neq 2$, then we have $L_p \cong M_p$ because $L_p$ and $M_p$ are unimodular, with the same determinant, and by Hilbert reciprocity the same Hasse invariant; so $L$ and $M$ belong to the same genus. This also holds for $p = 2$ if we additionally assume that $L$ and $M$ have the same type; i.e. they are both even or both odd, as that information forces $L_2 \cong M_2$.
The condition $p \nmid \det(L)$ is usually assumed in practice.

Conversely, suppose $L$ and $M$ belong to the same **spinor** genus. Using strong approximation for the spinor kernel, with the exceptional place chosen to be $\ell = p$ (as in Remark 6.34), we find that $M$ is equivalent to a lattice with $M_q = L_q$ for all $q \neq p$. Then

$$[L : L \cap M] = [L_p : L_p \cap M_p]$$

is a power of $p$. Using the following description of $p$-neighbors, which is of its own interest, we will show that $L$ and $M$ are "connected" by a chain of $p$-neighbors as long as $p \nmid \det(L)$.

**Lemma 6.50.** *Let $p$ be a prime and let $L$ be an integral lattice that is maximal at $p$; that is, $L_p = L \otimes \mathbb{Z}_p$ is not properly contained in any $\mathbb{Z}_p$-integral lattice in $L \otimes \mathbb{Q}_p$. (This holds automatically if $p \nmid \det(L)$.)*
*(i) Let $x \in L \backslash (p \cdot L)$ be a vector with $x \cdot x \in p^2\mathbb{Z}$. Then*

$$L(x) := \mathbb{Z}\frac{x}{p} + L_x, \quad L_x := \{y \in L : \ x \cdot y \in p\mathbb{Z}\}$$

*is an integral lattice and a $p$-neighbor of $L$.*
*(ii) Every $p$-neighbor of $L$ is of the form $L(x)$.*
*(iii) If $p \neq 2$, then the $p$-neighbors of $L$ are in bijection with the isotropic lines in $L \otimes \mathbb{F}_p$.*

In the case $p = 2$ in (iii) one can show that if $L$ is even then its even 2-neighbors can still be identified with isotropic lines of $L \otimes \mathbb{F}_2$.

*Proof.* (i) By construction, $L(x)$ is integral: $\frac{x}{p} \cdot \frac{x}{p} \in \mathbb{Z}$, and $\frac{x}{p} \cdot y \in \mathbb{Z}$ for any $y \in L_x$. If $L_x$ were already all of $L$, then $L(x)$ would be a proper $p$-adic integral overlattice of $L$. This is impossible because $L$ is maximal at $p$. Therefore the map

$$L \longrightarrow \mathbb{Z}/p\mathbb{Z}, \quad y \mapsto x \cdot y \bmod p$$

is surjective, with kernel $L_x = L \cap L(x)$, hence

$$[L : L \cap L(x)] = [L(x) : L \cap L(x)] = p$$

and $L$ and $L(x)$ are $p$-neighbors.
(ii) Let $M$ be a $p$-neighbor of $L$ and choose an element $x \in pM$ with $x \notin pL$. Since $pM \subseteq L$, we have $x \in L \backslash pL$ and we can construct the $p$-neighbor $L(x)$ by (i). But $L \cap M \subseteq L_x$ because $x/p \in M$, so we have

$$L \cap M \subseteq L_x \subsetneq L.$$

Since the index $[L : L \cap M]$ is prime, it follows that $L \cap M = L_x$. From $x/p \in M$ and $L_x \subseteq M$ we obtain

$$L(x) \subseteq M,$$

with equality because both $L(x)$ and $M$ have the same determinant $\det(L)$.
(iii) Given a $p$-neighbor $L(x)$, such that $L_x = L \cap L(x)$, we recover the isotropic line $\mathbb{F}_p x \subseteq L \otimes \mathbb{F}_p$ as the orthogonal complement of $L_x \otimes \mathbb{F}_p$. Conversely, given any isotropic line $\mathbb{F}_p x$, we can always find a representative $x+py \in L \backslash (pL)$ with $(x+py)\cdot(x+py) \in p^2\mathbb{Z}$ using the above argument that the map $L \to \mathbb{Z}/p\mathbb{Z}, \quad y \mapsto x \cdot y \bmod p$ is surjective. Then the $p$-neighbor $L(x + py)$ is well-defined and depends only on the line $\mathbb{F}_p x$. □

**Theorem 6.51.** *Let $L \subseteq V$ be an integral lattice and $p$ a prime with $p \nmid \det(L)$. Let $M$ be any lattice in the spinor genus of $L$. Then there is a chain of $p$-neighbors*

$$L = L_1 \sim_p L_2 \sim_p \ldots \sim_p L_r = M$$

*that connects $L$ to $M$.*

*Proof.* Using strong approximation for the spinor kernel, we may assume without loss of generality that $L_q = M_q$ for every $q \neq p$. Write

$$[L : L \cap M] = [M : L \cap M] = p^s, \quad s \in \mathbb{N}_0.$$

Now use induction on $s$:
(i) If $s = 1$, then $M$ is already a $p$-neighbor of $L$.
(ii) In the general case, choose $x \in M$ such that $\overline{x} \in M/(L \cap M)$ has order $p$; that is, $x \notin L$ but $px \in L$. Then the element $y := px$ satisfies $y \notin pL$ and $y \cdot y \in p^2\mathbb{Z}$, so the $p$-neighbor $L(y)$ is well-defined. Since $z \cdot y = p(z \cdot x) \in p\mathbb{Z}$ for any $z \in L \cap M$, we have

$$L \cap M = L_y \cap M \subseteq L(y) \cap M,$$

where $L_y = \{z \in L : \ z \cdot y \in p\mathbb{Z}\}$. The inclusion is proper because $x \in L(y) \cap M$. So

$$[L(y) : L(y) \cap M] = [M : L(y) \cap M] < p^s,$$

and the fact that $L(y)$ is connected to $M$ via $p$-neighbors follows from the induction hypothesis. □

**Lemma 6.52.** *Let $L \subseteq V$ be an integral lattice and $p$ a prime with $p \nmid \det(L)$. Suppose $x \in L \backslash (p \cdot L)$ is a vector with $x \cdot x \in p^2\mathbb{Z}$, such that the $p$-neighbor $L(x)$ is well-defined.*
*(i) Let $y \in pL$ satisfy $x \cdot y \in p^2\mathbb{Z}$. Then the $p$-neighbors $L(x)$ and $L(x+y)$ coincide.*
*(ii) Let $\varphi \in \mathrm{O}(L)$. Then $\varphi$ defines an isometry*

$$\varphi : L(x) \xrightarrow{\sim} L(\varphi x).$$

(i) says that the $p$-neighbor $L(x)$ depends only on the coset of $x$ modulo $pL_x$.

*Proof.* (i) Denoting

$$L_x = \{z \in L : \ x \cdot z \in p\mathbb{Z}\},$$

we have $L_x = L_{x+y}$ and therefore

$$L(x+y) = L_{x+y} + \mathbb{Z}\frac{1}{p}(x+y) = L_x + \mathbb{Z}\frac{1}{p}x = L(x).$$

(ii) is easy. □

We will apply the neighbor method to positive-definite, unimodular lattices of small rank, using the prime $p = 2$. Denote by $I_n$ the lattice $\mathbb{Z}^n$ with the Euclidean inner product.

**Lemma 6.53.** *The 2-neighbors of $I_n$ are (up to isometry) exactly the lattices $D_m^+ \perp I_{n-m}$ where $m \leq n$, $m \equiv 0$ mod 4.*

Here $D_m^+$ is the unimodular lattice spanned by $D_m = \{\sum x_i e_i \in \mathbb{Z}^n : \ \sum x_i \equiv 0 \,(\mathrm{mod}\, 2)\}$ and $(1/2, ..., 1/2)$. Note that $D_4^+$ is isometric to $I_4$ via the map

$$(1/2, 1/2, 1/2, 1/2) \mapsto e_1, \quad (-1/2, -1/2, 1/2, 1/2) \mapsto e_2,$$

$$(-1/2, 1/2, -1/2, 1/2) \mapsto e_3, \quad (-1/2, 1/2, 1/2, -1/2) \mapsto e_4.$$

For $m > 4$, the lattice $D_m^+$ is indecomposable. So the lattices $D_m^+ \perp I_{n-m}$ where $m \neq 4$ are inequivalent.

*Proof.* Let $x = \sum_{i=1}^n x_i e_i \in \mathbb{Z}^n$ be a vector with $x \cdot x \in 4\mathbb{Z}$ but not all $x_i \in 2\mathbb{Z}$, such that the 2-neighbor $I_n(x)$ is well-defined.
If any $x_i \in 2\mathbb{Z}$, then by Lemma 6.52 we can replace $x$ by $x - x_i e_i$ without changing the neighbor. So we can assume that $x_i = 0$. Similarly, if $x_i$ is an odd integer, say $x_i = 4y_i \pm 1$, then we can replace $x$ by $x - 4y_i e_i$ without changing the neighbor to assume that $x_i = \pm 1$; up to a reflection (which does not change the isometry type of

the neighbor lattice) we can even assume that $x_i = 1$.
So up to permutation, $x = (1, ..., 1, 0, ..., 0)$ with $m$ ones and $n - m$ zeros. We have $m \equiv 0 \bmod 4$ because $x \cdot x \in 4\mathbb{Z}$. The 2-neighbor $I_n(x)$ is $D_m^+ \perp I_{n-m}$ essentially by definition. □

For $n \leq 7$, it immediately follows that $I_n$ is the unique (up to isometry) positive-definite unimodular lattice of rank $n$.

For $n = 8$, we see that the only 2-neighbors of $I_8$ are $E_8$ $(= D_8^+)$ and $I_8$ itself. To compute *all* unimodular lattices of rank 8, we have to compute the 2-neighbors of $E_8$ also.

Note that $E_8$ is an even integral lattice. It contains 240 roots (vectors $v$ with $v \cdot v = 2$): namely, the $112 = 4 \cdot \frac{8 \cdot 7}{2}$ roots $\pm e_i \pm e_j$ from $D_8$, and the $128 = 2^7$ roots $(\pm 1/2, ... \pm 1/2)$ that have an even number of + signs. The 120 pairs $\pm v$ of roots and their negatives all define distinct cosets in $E_8/2E_8$.

**Lemma 6.54.** *All 2-neighbors of $E_8$ are isometric to either $I_8$ or to $E_8$ itself.*

*Proof.* Let $x \in E_8$ be a vector with $x \cdot x \in 4\mathbb{Z}$ but $x \notin 2E_8$, such that the 2-neighbor $E_8(x)$ is well-defined. By Lemma 6.52 the 2-neighbor $E_8(x)$ depends only on the coset of $x$ in

$$E_8/2E_8 \cong E_8 \otimes \mathbb{F}_2 (\cong H \perp H \perp H \perp H).$$

The orthogonal group of $E_8/2E_8$ acts transitively on the classes of even norm and of odd norm by Witt's theorem on extension of isometries; it is generated by 120 reflections through the 120 classes of odd norm, which are represented exactly by the $\pm$ pairs of roots of $E_8$, each of which comes with a reflection defined over $\mathbb{Z}$. Hence the map

$$\mathrm{O}(E_8) \longrightarrow \mathrm{O}(E_8/2E_8)$$

is surjective, and $\mathrm{O}(E_8)$ also acts transitively on the cosets of $E_8/2E_8$ of even and odd norm.

Modulo $\mathrm{O}(E_8)$, we may therefore assume that $x \in (2, 0, ..., 0) + 2E_8$. Then

$$(E_8)_x = \{y \in E_8 : \ y \cdot x \in 2\mathbb{Z}\} = E_8 \cap \mathbb{Z}^8 = D_8,$$

and the neighbor $E_8(x)$ depends only on the class of $x + 2D_8$. Since $[E_8 : D_8] = 2$, there are exactly two possibilities for $x$: either $x \in 2D_8$ already, or

$$x \in (2, 0, ..., 0) + 2(1/2, ..., 1/2) + 2D_8.$$

In the first case, $E_8(x)$ contains the vector $x/2$ with $(x/2) \cdot (x/2) = 1$; then $x/2$ splits off orthogonally with the complement being unimodular of rank 7 and therefore isometric to $I_7$, hence $E_8(x) \cong I_8$. In the second case, we have $E_8(x) = D_8 + \mathbb{Z}\frac{x}{2} = E_8$. □

It follows that the only unimodular positive-definite lattices of rank 8 (up to isometry) are $I_8$ and $E_8$.

With similar arguments one can show that there are exactly two isometry classes of positive-definite unimodular lattices of ranks $n = 9, 10, 11$. Namely

$$I_n \quad \text{and} \quad L := I_{n-8} \perp E_8.$$

To prove this it will be enough to determine the 2-neighbors $L(x)$ of $L$. If $x$ belongs to the sublattice $I_{n-8}$ or $E_8$ then we have $L(x) = I_{n-8}(x) \perp E_8$ or $L(x) = I_{n-8} \perp E_8(x)$, respectively, so suppose $x = x_1 + x_2$ with $x_1 \in I_{n-8}$, $x_2 \in E_8$ and neither $x_1$ nor $x_2$ is identically zero mod 2. Since $x \cdot x \in 4\mathbb{Z}$, we have $x_1 \cdot x_1 \in 2\mathbb{Z}$, which already rules out the case $n = 9$. In the cases $n = 10$ and $n = 11$, exactly two of the components in $x_1$ must be odd, so (modulo $2L$ and modulo reflections) we have $x_1 = e_1 + e_2$. Now $x_2 \cdot x_2 \equiv 2 \bmod 4$. Since $\mathrm{O}(E_8)$ acts transitively on the even-norm cosets of $E_8/2E_8$, we may assume (modulo $2E_8$) that $x_2$ is also $e_1 + e_2$.
The coset of $x \in L/2L$ is now uniquely determined. By Lemma 6.52, there are at most two 2-neighbors, namely $L(x)$ and $L(y)$ where $y \equiv x \bmod 2L$ but $y \not\equiv x \bmod 2L_x$; one can take $y = (e_1 + e_2, e_1 - e_2)$. But these yield isometric 2-neighbors.
The 2-neighbor $L(x)$ contains the vector $x/2$ of norm 1, which therefore splits off orthogonally: $L(x) \cong I_1 \perp M$ with unimodular $M$. Using an induction argument on $n$ we obtain $M \cong I_{n-9} \perp E_8$ or $M \cong I_{n-1}$.

The unimodular lattices in a few higher ranks[6] have also been completely enumerated. For example, for $12 \le n \le 16$ we have the following class representatives:

$$\begin{aligned}
n = 12: &\quad I_{12},\ I_4 \perp E_8,\ D_{12}^+;\\
n = 13: &\quad I_{13},\ I_5 \perp E_8,\ I_1 \perp D_{12}^+;\\
n = 14: &\quad I_{14},\ I_6 \perp E_8,\ I_2 \perp D_{12}^+,\ (2E_7)^+;\\
n = 15: &\quad I_{15},\ I_7 \perp E_8,\ I_3 \perp D_{12}^+,\ I_1 \perp (2E_7)^+,\ A_{15}^+;\\
n = 16: &\quad I_{16},\ I_8 \perp E_8,\ I_4 \perp D_{12}^+,\ I_2 \perp (2E_7)^+,\ I_1 \perp A_{15}^+,\ 2E_8,\ D_{16}^+;
\end{aligned}$$

where $L^+$ means a maximal integral overlattice obtained from the root lattice $L$ by "gluing" to it certain cosets of $L'/L$ in a way that is similar to the construction of $D_n^+$. In principle, the 2-neighbor algorithm computes the unimodular lattices of any rank, but in practice the calculations become too difficult (and the number of classes grows extremely quickly).

For large rank, a lower bound for the number of lattices is given by the **Siegel–Minkowski–Smith mass formula** (which we do not have time to formulate, let alone prove; see Kneser's Chapter X for details). In the case of even unimodular lattices, the

[6]Up to rank 27. The lattices in rank 26 and 27 were very recently (as of 2025) classified by Chenevier. For odd lattices of rank 24, 25 the classification is due to Borcherds. The even rank 24 even unimodular lattices were identified in a famous paper of Niemeier.

statement of the theorem is:

$$\sum_{\mathrm{rank}(L)=8n} \frac{1}{\#\mathrm{O}(L)} = \frac{|B_{4n}|}{8n} \cdot \prod_{j=1}^{4n-1} \frac{|B_{2j}|}{4j},$$

where $B_n$ are the Bernoulli numbers, defined by the generating function

$$\sum_{n=0}^{\infty} \frac{B_n}{n!} x^n = \frac{x}{e^x - 1}.$$

Here $L$ runs through the inequivalent classes of even unimodular positive-definite lattices of rank $8n$.

For $n = 1$, we have already shown that $E_8$ is the unique even unimodular positive-definite lattice in rank 8, and the mass formula becomes

$$\frac{1}{\#\mathrm{O}(E_8)} = \frac{|B_4|}{8} \cdot \frac{|B_2|}{4} \cdot \frac{|B_4|}{8} \cdot \frac{|B_6|}{12} = \frac{1}{240} \cdot \frac{1}{12} \cdot \frac{1}{240} \cdot \frac{1}{252} = \frac{1}{696729600}.$$

The mass of rank 16 unimodular lattices is smaller than this, but after 16 it grows extremely quickly: in rank 32 the mass is already about $4 \cdot 10^7$, in rank 40 it is about $4.4 \cdot 10^{51}$ and in rank 48 it is already greater than $10^{121}$. The lower bound

$$\frac{1}{\#\mathrm{O}(L)} \leq \frac{1}{2},$$

which is less than sharp (it comes from observing that $\mathrm{O}(L)$ contains $\pm\mathrm{id}$) shows that the number of inequivalent lattices is at least twice the mass.

As for odd unimodular lattices $L$ in rank $8n$, note that $L$ has at most two even 2-neighbors up to isometry: if $L(x)$ is even, then $L_x = L \cap L(x)$ must be exactly the sublattice

$$L_0 = \{x \in L : \ x \cdot x \in 2\mathbb{Z}\}$$

of even-norm vectors in $L$, and is uniquely determined. $L_0$ has determinant four, so $L_0'/L_0$ splits into four cosets (say $L_0, L_1, L_2, L_3$), and for exactly one of these cosets we have $L = L_0 \cup L_1$ (say); then the other two $L_0 \cup L_2$, $L_0 \cup L_3$ are the even neighbors. They can be isometric to each other (this is true for $I_{8n}$, for example, where we observed that its only even 2-neighbor is $D_{8n}^+$) but in all cases they are each others' 2-neighbors. So the classes of odd unimodular lattices are roughly in correspondence with neighboring pairs of classes of even unimodular lattices – their number is much larger.