Arithmetic of Quadratic Forms

1 Foundation

Throughout this section, F always denotes a field of characteristic different from 2.

1.1 Quadratic Forms and Quadratic Spaces

An (n-ary) *quadratic form* over F is a polynomial f in n variables $x_1, \ldots, x_n$ over F that is homogeneous of degree 2. In general, f takes the form

$$f(x_1, \ldots, x_n) = \sum_{i,j=1}^{n} b_{ij} x_i x_j, \quad b_{ij} \in F.$$

To render the coefficients symmetric, it is customary to rewrite f as

$$f(x_1, \ldots, x_n) = \sum_{i,j=1}^{n} a_{ij} x_i x_j,$$

where $a_{ij} = (b_{ij} + b_{ji})/2$. In this way, f determines a symmetric matrix (a_{ij}), which we shall denote by A_f. In terms of matrix multiplication, we have

$$f(\mathbf{x}) = \mathbf{x}^t A_f \, \mathbf{x}$$

where $\mathbf{x} = (x_1, \ldots, x_n)^t$.

Let a be an element in F. We say that a is represented by f if the equation

$$(*) \qquad f(\mathbf{x}) = a$$

has a solution in F^n. The *representation problem* of quadratic forms is to determine, in an effective manner, the set of elements of F that are represented by a particular quadratic form over F. We shall discuss the case when F is a field of arithmetic interest, for instance, the field of complex numbers $\mathbb{C}$, the field of real numbers $\mathbb{R}$, a finite field $\mathbb{F}$, and the field of rational numbers $\mathbb{Q}$. The representation problem for quadratic forms over any one of these fields has a very satisfactory solution. At the end, we shall discuss the solubility of equation $(*)$ over a subring R of F, that is, the problem of finding solution of $(*)$ in R^n. The most interesting and difficult case is when R is the ring of integers $\mathbb{Z}$ for which there is still a lot of questions left unanswered.

Let f and g be two n-ary quadratic forms. We say that f and g are *equivalent*, written $f \cong g$, if there exists an invertible matrix $C \in \mathrm{GL}_n(F)$ such that $f(\mathbf{x}) = g(C\mathbf{x})$. This is the same as saying that there is an invertible homogeneous linear substitution of the variables $x_1, \ldots, x_n$ which takes the form g to the form f. Since

$$g(C\mathbf{x}) = (C\mathbf{x})^t A_g \, (C\mathbf{x}) = \mathbf{x}^t (C^t A_g C) \mathbf{x},$$

the condition $f(\mathbf{x}) = g(C\mathbf{x})$ is equivalent to the matrix equality

$$A_f = C^t A_g C.$$

Thus equivalence of forms amounts to congruence of the associated symmetric matrices. As expected, equivalence of forms is indeed an equivalence relation. It is clear that equivalent forms represent the same set of elements of F.

Example 1.1 Let $g(x, y)$ be the binary form xy. If we make the substitution $x \mapsto x+y, y \mapsto x-y$, then g changes to

$$g(x+y, x-y) = (x+y)(x-y) = x^2 - y^2 = f(x, y).$$

The matrix C in this case is $\left(\begin{smallmatrix} 1 & 1 \\ 1 & -1 \end{smallmatrix}\right)$. This can be verified by

$$A_f = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \begin{pmatrix} 0 & 1/2 \\ 1/2 & 0 \end{pmatrix} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} = C^t A_g C.$$

Any quadratic form f gives rise to a map $Q_f : F^n \longrightarrow F$ defined by $Q_f(\mathbf{x}) = \mathbf{x}^t A_f \mathbf{x}$. We shall refer to Q_f as the *quadratic map* defined by f. The notion of equivalence of quadratic forms, $f \cong g$, amounts to the existence of a linear automorphism C of F^n (that is, an invertible matrix in $\mathrm{GL}_n(F)$) such that $Q_f(\mathbf{x}) = Q_g(C\mathbf{x})$ for all $\mathbf{x} \in F^n$. Note that the quadratic map Q_f determines the quadratic form f uniquely. For, suppose that $Q_f = Q_g$ as maps from F^n to F. Let $\mathbf{e}_1, \ldots, \mathbf{e}_n$ be the standard basis for F^n. Then for any i, we have

$$(A_f)_{ii} = Q_f(\mathbf{e}_i) = Q_g(\mathbf{e}_i) = (A_g)_{ii}.$$

For $i \neq j$, we have

$$Q_f(\mathbf{e}_i + \mathbf{e}_j) = Q_f(\mathbf{e}_i) + Q_f(\mathbf{e}_j) + 2(A_f)_{ij},$$

and a similar equation for $Q_g(\mathbf{e}_i + \mathbf{e}_j)$. Therefore, $(A_f)_{ij} = (A_g)_{ij}$; thus $A_f = A_g$ and $f = g$.

The quadratic map Q_f satisfies the following properties:

(1) For any $a \in F$ and $\mathbf{x} \in F^n$, $Q_f(a\mathbf{x}) = a^2 Q_f(\mathbf{x})$.

(2) The function $B_f(\mathbf{x}, \mathbf{y}) = \frac{1}{2}[Q_f(\mathbf{x}+\mathbf{y}) - Q_f(\mathbf{x}) - Q_f(\mathbf{y})]$ is a symmetric bilinear form on F^n. That is, B_f is a function from $F^n \times F^n$ to F satisfying

   (i) $B_f(\mathbf{x}, \mathbf{y}) = B_f(\mathbf{y}, \mathbf{x})$ for all $\mathbf{x}, \mathbf{y} \in F^n$, and

   (ii) $B_f(a\mathbf{x} + b\mathbf{y}, \mathbf{z}) = aB_f(\mathbf{x}, \mathbf{z}) + bB_f(\mathbf{y}, \mathbf{z})$ for all $a, b \in F$ and $\mathbf{x}, \mathbf{y}, \mathbf{z} \in F^n$.

Note that the quadratic map Q_f can be recaptured by the symmetric bilinear form B_f, since

$$Q_f(\mathbf{x}) = B_f(\mathbf{x}, \mathbf{x}), \qquad \forall \mathbf{x} \in F^n.$$

This motivates the following geometric approach to the notion of a quadratic form. Let V be an n-dimensional vector space over F equipped with a symmetric bilinear form B :

$V \times V \longrightarrow F$. The pair (V, B) is called a *quadratic space*, and associate with it is a quadratic map $Q = Q_B : V \longrightarrow F$ given by $Q(v) = B(v, v)$ for all $v \in V$. As in (1) and (2) above, we have $Q(av) = a^2 Q(v)$ for all $a \in F$ and $v \in V$, and $2B(u, v) = Q(u + v) - Q(u) - Q(v)$ for all $u, v \in V$. Therefore, Q and B determine each other and hence it is legitimate to write (V, Q) to represent the quadratic space (V, B).

Now, suppose that $v_1, \ldots, v_n$ is a basis for V. Then the quadratic space (V, B) gives rise to a quadratic form

$$f(x_1, \ldots, x_n) = \sum_{i,j} B(v_i, v_j) x_i x_j,$$

with

$$A_f = (B(v_i, v_j)).$$

If we identify V with F^n via the basis $v_1, \ldots, v_n$ that is, we identify each vector $v = x_1 v_1 + \ldots x_n v_n$ with the column $\mathbf{x} = (x_1, \ldots, x_n)^t$, then $Q = Q_B$ is precisely the quadratic map Q_f associated with the form f. An element $a \in F$ is represented by the form f if and only if a is represented by V, that is, there exists a vector $v \in V$ such that $Q(v) = a$.

Now, let us choose another basis $u_1, \ldots, u_n$ for V, and let g be the resulting quadratic form. Suppose that $u_i = \sum_k c_{ki} v_k$, then

$$\begin{aligned}
(A_g)_{ij} &= B(u_i, u_j) \\
&= B(\sum_k c_{ki} v_k, \sum_\ell c_{\ell j} v_\ell) \\
&= \sum_{k,\ell} c_{ki} B(v_k, v_\ell) c_{\ell j} \\
&= (C^t A_f C)_{ij}
\end{aligned}$$

where $C = (c_{k\ell})$. Thus the quadratic space (V, B) determines uniquely an equivalence class of quadratic forms, which we shall denote by $[f_B]$.

If (V, B) and (V', B') are two quadratic spaces, we say that they are *isometric*, written $(V, B) \cong (V', B')$, if there exists an isomorphism $\sigma : V \longrightarrow V'$ such that

$$B'(\sigma(u), \sigma(v)) = B(u, v), \qquad \forall u, v \in V.$$

Such σ is called an *isometry* from V to V'. The set of all isometries from V to V itself form a group $O(V)$ under the composition of functions. It is clear that

$$(V, B) \cong (V', B') \Longleftrightarrow [f_B] = [f_{B'}].$$

Thus there is a one-to-one correspondence between the equivalence classes of n-ary quadratic forms and the isometry classes of n-dimensional quadratic spaces. In this set of lecture notes, we shall adopt the geometric language of quadratic spaces.

Let (V, B) be an n-dimensional quadratic space, and $v_1, \ldots, v_n$ be a basis for V. Let A be the symmetric matrix $(B(v_i, v_j))$. We call A a matrix for V and write

$$V \cong A.$$

So, $V \cong A \cong C^t AC$ for any $C \in \mathrm{GL}_n(F)$. We call V *nondegenerate* if $\det(A)$ is nonzero. Otherwise, V is degenerate. For a nondegenerate space V, its discriminant of V, denoted $d(V)$, is defined to be the square class $\det(A)F^{\times 2}$ in $F^\times/F^{\times 2}$. For convention, the zero space is considered to be nondegenerate and its discriminant is defined to be $F^{\times 2}$.

If W is a subspace of V, the map $B_W : W \times W \longrightarrow F$ defined by $B_W(x, y) = B(x, y)$ for all $x, y \in W$ is a symmetric bilinear form on W. Thus (W, B_W) is also a quadratic space. We say that W is a nondegenerate subspace of V if (W, B_W) is nondegenerate as a quadratic space.

Let (V, B) be a quadratic space. Let V^* be the vector space of all homomorphisms from V to F. It is called the dual space of V. The function $\hat{B} : V \longrightarrow V^*$ defined by

$$\hat{B}(x)(y) = B(x, y)$$

is clearly linear.

Suppose that $\mathfrak{E} = \{v_1, \ldots, v_n\}$ is a basis for V. For each i, define $v_i^* \in V^*$ by

$$v_i^*(v_j) = \delta_{ij} = \begin{cases} 1 & \text{if } i = j, \\ 0 & \text{otherwise.} \end{cases}$$

Then $\mathfrak{E}^* = \{v_1^*, \ldots, v_n^*\}$ is a basis for V^*.

Lemma 1.2 *The matrix of $\hat{B}$ with respect to the bases $\mathfrak{E}$ and $\mathfrak{E}^*$ is the symmetric matrix for V associated with $\mathfrak{E}$.*

Proof. From $\hat{B}(e_i)(e_j) = B(e_i, e_j)$ follows

$$\hat{B}(e_i) = \sum_{j=1}^{n} B(e_i, e_j) e_j^*.$$

□

Corollary 1.3 *A quadratic space (V, B) is nondegenerate if and only if the map $\hat{B} : V \longrightarrow V^*$ is an isomorphism.*

1.2 Orthogonal Decomposition

Let (V, B) be a quadratic space. Two vectors $x, y \in V$ are *orthogonal* if $B(x, y) = 0$. Two subsets X and Y of V are said to be orthogonal if $B(x, y) = 0$ for all $x \in X$, $y \in Y$. With each subset X of V, the *orthogonal complement of X in V* is the set

$$X^\perp = \{v \in V : B(v, x) = 0 \text{ for all } x \in X\}.$$

The orthogonal complement of V itself is called the *radical* of V, denoted by $\mathrm{rad}(V)$ (but not by $V^\perp$).

Lemma 1.4 *Let X, Y be subsets of V. Then*

(a) $X^\perp$ *is a subspace of* V.

(b) If $X \subseteq Y$, *then* $X^\perp \supseteq Y^\perp$.

(c) $X \subseteq X^{\perp\perp}$

(d) V *is nondegenerate if and only if* $rad(V) = 0$.

Proof. Parts (a), (b) and (c) are direct consequences of the definition of orthogonal complements. For (d), note that the kernel of the map $\hat{B}$ is precisely $\mathrm{rad}(V)$. Therefore, $\dim(V) = \dim(\mathrm{rad}(V)) + \dim(\mathrm{Im}(\hat{B}))$. By Corollary 1.3, V is nondegenerate if and only if $\hat{B}$ is an isomorphism. Thus V is nondegenerate if and only if $\dim(\mathrm{rad}(V)) = 0$, that is, $\mathrm{rad}(V) = 0$.□

Definition 1.5 Let (V_1, B_1) and (V_2, B_2) be two quadratic spaces. The *orthogonal sum* $V_1 \perp V_2$ is the quadratic space $V_1 \oplus V_2$ with the symmetric bilinear form B defined by $B(x_1 + x_2, y_1 + y_2) = B_1(x_1, y_1) + B(x_2, y_2)$ for all $x_1, y_1 \in V_1$ and $x_2, y_2 \in V_2$.

So if $V = V_1 \perp V_2$ as above, then $(V_i, B_i) \cong (V_i, B|_{V_i})$ for $i = 1, 2$, and V_1 and V_2 are orthogonal in V.

Theorem 1.6 *Let* (V, B) *be a quadratic space. Suppose that* $V = rad(V) \oplus W$ *for some subspace* W. *Then*

(a) $V = rad(V) \perp W$.

(b) W *is nondegenerate.*

(c) $(W, B|_W)$ *is determined up to isometry by* V.

Proof. Part (a) is clear. For part (b), suppose that $x \in W$ is orthogonal to all vectors in W. Then x is orthogonal to all vectors in $\mathrm{rad}(V) \perp W = V$. Therefore, $x \in \mathrm{rad}(V) \cap W$ and hence $x = 0$.

For part (c), suppose that $V = \mathrm{rad}(V) \oplus W_1$. Then each $x \in W$ can be written uniquely as

$$x = y + \alpha(x), \quad y \in \mathrm{rad}(V), \alpha(x) \in W_1.$$

One can check that the map $\alpha : W \longrightarrow W_1$ defined by $x \longmapsto \alpha(x)$ is a vector space homomorphism. It is clear that α is injective and hence surjective since $\dim(W) = \dim(W_1)$. If $x = y + \alpha(x)$ and $x' = y' + \alpha(x')$, then

$$B(x, x') = B(y + \alpha(x), y' + \alpha(x')) = B(\alpha(x), \alpha(x')).$$

Hence α is an isometry.□

The isometry class of $(W, B|_W)$ obtained in the above theorem is called the nondegenerate component of (V, B). The classification of general quadratic spaces reduces to the classification of their nondegenerate components.

Lemma 1.7 *Let V, W, V', W' be quadratic spaces.*

(a) $V \perp V' \cong V' \perp V$.

(b) If $V \cong W$ *and* $V' \cong W'$, *then* $V \perp V' \cong W \perp W'$.

(c) If A *is a matrix for* V *and* A' *is a matrix for* V', *then*

$$V \perp V' \cong \begin{pmatrix} A & 0 \\ 0 & A' \end{pmatrix}.$$

(d) $V \perp V'$ *is nondegenerate if and only if both* V *and* V' *are nondegenerate. In this case,* $d(V \perp V') = d(V)d(V')$.

Proof. Everything is obvious.□

Proposition 1.8 *If* W *is a nondegenerate subspace of a quadratic space* (V, B) , *then* $V = W \perp W^{\perp}$.

Proof. It suffices to show that $V = W \oplus W^{\perp}$. Since W is nondegenerate, $0 = \ker(\widehat{B_W}) = W \cap W^{\perp}$. If $x \in V$ and $h = \hat{B}(x)|_W$, then because W is nondegenerate there exists $y \in W$ with $h = \widehat{B_W}(y)$. Hence for all $z \in W$,

$$B(x, z) = \hat{B}(x)(z) = h(z) = \widehat{B_W}(y)(z) = B(y, z)$$

and we can write $x = y + (x - y)$ where $y \in W$ and $(x - y) \in W^{\perp}$ by the above equation. Thereby $V = W + W^{\perp}$ is proven.□

The above proposition implies that $\dim(W) + \dim(W^{\perp}) = \dim(V)$ whenever W is a nondegenerate subspace of V. Below we show that the same additive property of the dimension holds for *every* subspace provided V itself is nondegenerate.

Proposition 1.9 *Let* (V, B) *be a nondegenerate quadratic space, and* W *be a subspace of* V. *Then*

(i) $\dim(W) + \dim(W^{\perp}) = \dim(V)$.

(ii) $(W^{\perp})^{\perp} = W$.

Proof. Part (ii) is a direct consequence of part (i) because $W \subseteq (W^{\perp})^{\perp}$. The map $\hat{B} : V \longrightarrow V^*$ is an isomorphism. Since W is a subspace of V, the canonical projection $V^* \longrightarrow W^*$ is surjective. The kernel of the composition $V \longrightarrow V^* \longrightarrow W^*$ is $W^{\perp}$. Therefore, $\dim(V) = \dim(W^{\perp}) + \dim(W^*) = \dim(W^{\perp}) + \dim(W)$. □

1.3 Witt's Theorems

Let (V, B) be a quadratic space. A nonzero vector $v \in V$ is called *isotropic* if $Q(v) = 0$. Otherwise, v is called *anisotropic*.

Theorem 1.10 *Every quadratic space has an orthogonal basis.*

Proof. Let (V, B) be a quadratic space. Since $\mathrm{rad}(V)$ is an orthogonal summand of V, we may assume that V is nondegenerate. Suppose that $Q(x) = 0$ for all $x \in V$. Then for any $u, v \in V$,

$$B(u, v) = \frac{1}{2}[Q(u + v) - Q(u) - Q(v)] = 0,$$

which implies that $\mathrm{rad}(V) = V$ which is impossible.

Now, pick an anisotropic vector $x \in V$. Then Fx is a nondegenerate subspace, and hence we have a decomposition $V = Fx \perp V'$ for some subspace V'. The subspace V' is also nondegenerate. An induction argument on the dimension of V will complete the proof.□

Corollary 1.11 *Every invertible symmetric matrix in $GL_n(F)$ is congruent to a diagonal matrix.*

We use the notation $\langle a_1, \ldots, a_n \rangle$ to denote a diagonal matrix with $a_1, \ldots, a_n$ as the diagonal entries. Then $V \cong \langle a_1, \ldots, a_n \rangle$ if V has an orthogonal basis $v_1, \ldots, v_n$ such that $Q(v_i) = a_i$ for all i.

Let v be an anisotropic vector in a quadratic space (V, B). Define a map $\tau_v : V \longrightarrow V$ by

$$\tau_v(x) = x - \frac{2B(v, x)}{Q(v)}v.$$

It is easy to verify that τ_v is linear. It is called the *symmetry* with respect to v (or a *reflection* with respect to the hyperplane $v^\perp$).

Lemma 1.12 *For each anisotropic vector $v \in V$, τ_v is an isometry of V and $\det(\tau_v) = -1$.*

Proof. The first assertion can be checked directly. Since $Q(v)$ is nonzero, the subspace Fv is nondegenerate and hence $V = Fv \perp V'$ for some subspace V'. Let $v_2, \ldots, v_n$ be a basis for V'. Then $v, v_2, \ldots, v_n$ is a basis for V. The matrix of τ_v with respect to this basis is the diagonal matrix $\langle -1, 1, \ldots, \rangle$. Therefore, $\det(\tau_v) = -1$.□

Lemma 1.13 *Let (V, B) be a quadratic space. If x and y are anisotropic vectors of V with $Q(x) = Q(y)$, then there is an isometry σ of V such that $\sigma(x) = y$.*

Proof. Let $u = (x + y)/2$ and $v = (x - y)/2$. Then $B(u, v) = 0$ and $Q(x) = Q(u) + Q(v)$. Either $Q(u)$ or $Q(v)$ is nonzero. In the first case, $-\tau_u(x) = y$ and in the second case $\tau_v(x) = y$.□

Lemma 1.14 *Let (V, B) and (V', B') be two quadratic spaces. If $\sigma : V \longrightarrow V'$ is an isometry and W is a subspace of V, then $\sigma(W^\perp) = \sigma(W)^\perp$.*

Proof. Let $x \in W^\perp$. For any $w \in W$,

$$B'(\sigma(x), \sigma(w)) = B(x, w) = 0.$$

Therefore, $\sigma(W^\perp) \subseteq \sigma(W)^\perp$. The reverse inclusion can be proved similarly.□

Theorem 1.15 (Witt's Cancellation Theorem) *If V, V_1, V_2 are nondegenerate quadratic spaces such that*

$$V_1 \perp V \cong V_2 \perp V,$$

then $V_1 \cong V_2$.

Proof. Since V is the orthogonal sum of 1-dimensional subspaces, it suffices to consider the case where $\dim(V) = 1$; thus $V = Fx$. It follows from the hypothesis and Lemma 1.13 that there exists an isometry

$$\Sigma : V_1 \perp Fx \longrightarrow V_2 \perp Fx$$

such that $\Sigma(x) = x$. By Lemma 1.14, $\Sigma(V_1) = V_2$.□

Corollary 1.16 (Witt's Extension Theorem) *Let V and V' be isometric nondegenerate quadratic spaces. Suppose that W and W' are nondegenerate subspaces of V and V', respectively, and that $\sigma : W \longrightarrow W'$ is an isometry. Then there exists an isometry $\Sigma : V \longrightarrow V'$ which extends σ, that is, $\Sigma|_W = \sigma$.*

Proof. Let $\tau : V' \longrightarrow V$ be an isometry. Then by Proposition 1.8,

$$W \perp W^\perp = V = \tau(W') \perp \tau(W')^\perp.$$

Since $W \cong \tau(W')$, it follows from Theorem 1.15 that there exists an isometry σ' from $W^\perp$ to $\tau(W')^\perp$. Then $\Sigma = \sigma \perp (\tau^{-1}\sigma')$ is the required isometry.□

1.4 Witt Index

Definition 1.17 A quadratic space V is said to be *isotropic* if it contains an isotropic vector. Otherwise, it is *anisotropic*. The space V is said to be *totally isotropic* if every nonzero vector in V is isotropic.

Theorem 1.18 *Let (V, B) be a 2-dimensional nondegenerate quadratic space. The following conditions are equivalent:*

(a) V is isotropic.

(b) $V \cong \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$.

(c) $V \cong \langle 1, -1\rangle \cong \langle \alpha, -\alpha\rangle$ *for any* $\alpha \in F^\times$.

(d) For any $\alpha \in F^\times$ *and any* $\gamma \in F$, $V \cong \begin{pmatrix} 0 & \alpha \\ \alpha & \gamma \end{pmatrix}$.

(e) $-d(V) = F^{\times 2}$.

Proof. Suppose that V is isotropic. Then V has an isotropic vector x, and $V = Fx \oplus Fy$ for some $y \in V$. Let $\alpha = B(x, y)$ and $\gamma = Q(y)$. Since V is nondegenerate, $\alpha \in F^\times$. If we let $e = \frac{1}{\alpha}x$ and $f = -\frac{\gamma}{2\alpha}x + y$, then the symmetric matrix associated to $\{e, f\}$ is $\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$. This proves (a) $\Longrightarrow$ (b).

Suppose (b) holds and the basis which yields the matrix is $\{x, y\}$. For any $\alpha \in F^\times$, $Q(\frac{1}{2}x + \alpha y) = \alpha$. So, the subspace spanned by $u = \frac{1}{2}x + \alpha y$ is nondegenerate and hence $V = Fu \perp Fv$ for some $v \in V$. Comparing the discriminants of both sides shows that v can be chosen so that $Q(v) = -\alpha$. This proves (b) $\Longrightarrow$ (c).

If (c) holds, then V has an isotropic vector, say x, which can be extended to a basis $\{x, y\}$ of V. Note that $B(x, y)$ must be nonzero because V is nondegenerate. Now, let

$$e = \frac{\alpha}{B(x, y)}x, \quad f = \frac{\gamma - Q(y)}{2B(x, y)}x + y.$$

Then $\{e, f\}$ is a basis for M whose associated symmetric matrix is the one stated in (d).

The implication (d) $\Longrightarrow$ (e) is trivial. We now show that (e) $\Longrightarrow$ (a). If $\{x, y\}$ is an orthogonal basis for V and $\langle \alpha_1, \alpha_2\rangle$ is the associated symmetric matrix, then $\alpha_1\alpha_2 = -\gamma^2$ for some $\gamma \in F^\times$. One easily checks that the vector $x + \gamma\beta_2^{-1}y$ is isotropic.□

The preceding theorem implies that there is only one isometry class of nondegenerate isotropic 2-dimensional quadratic space. Any one of such space is called a *hyperbolic plane* and is denoted by $\mathbb{H}$.

Definition 1.19 A quadratic space V is said to be universal if V represents all elements in F.

Corollary 1.20 *Let* (V, B) *be a nondegenerate isotropic quadratic space. Then* $V \cong \mathbb{H} \perp W$ *for some subspace* W. *In particular, every nondegenerate isotropic quadratic space is universal.*

Proof. The second assertion is a consequence of Theorem 1.18. Let x be an isotropic vector in V. Since V is nondegenerate, there exists $y \in V$ such that $B(x, y) = 1$. The subspace $Fx \oplus Fy$ is isometric to $\mathbb{H}$.□

By the preceding corollary, every nondegenerate quadratic space V has an orthogonal decomposition of the form

$$V \cong \mathbb{H} \perp \cdots \perp \mathbb{H} \perp V_0 = \mathbb{H}^m \perp V_0$$

where V_0 is nondegenerate and anisotropic. The number m is well-defined, that is, it is independent of the way we obtain the above orthogonal decomposition. For, suppose that

$$V \cong \mathbb{H}^k \perp V_1$$

where V_1 is nondegenerate and anisotropic. If $k > m$, by Witt's Cancellation Theorem it follows that

$$\mathbb{H}^{k-m} \perp V_1 \cong V_0,$$

which contradicts that V_0 is anisotropic. Therefore, $k = m$, and $V_0 \cong V_1$ by Witt's Cancellation Theorem once again. In summary, we have

Corollary 1.21 (Witt's Decomposition) *Every nondegenerate quadratic space V has an orthogonal decomposition*

$$V = \mathbb{H}^m \perp V_0,$$

where V_0 is nondegenerate and anisotropic. The integer m and the isometry class of V_0 are uniquely determined by the isometry class of V.

The number m, which is the number of copies of $\mathbb{H}$ in the above decomposition, is called the *Witt Index* of V and is usually denoted by $\mathrm{Ind}(V)$.

Definition 1.22 A quadratic space is called *hyperbolic* if it is an orthogonal sum of copies of $\mathbb{H}$.

Proposition 1.23 *Let (V, B) be a nondegenerate quadratic space, and W be a totally isotropic subspace of dimension k. Then W is contained in a hyperbolic subspace of V of Witt index k.*

Proof. Let $\{e_1, \ldots, e_k\}$ be a basis for W. Since V is nondegenerate, there exists $f_1 \in V$ such that $B(e_1, f_1) = 1$ and $B(f_1, e_i) = 0$ for $i = 2, \ldots, k$. The subspace $H_1 = Fe_1 \oplus Ff_1$ is isometric to $\mathbb{H}$; hence $V = H_1 \perp V_1$ for some nondegenerate subspace V_1. Moreover, $e_2, \ldots, e_k$ are vectors in V_1 which span a totally isotropic subspace. An induction on the dimension of W will complete the proof of the proposition.□

Corollary 1.24 *The dimension of a maximal totally isotropic subspace of a nondegenerate quadratic space V is equal to the Witt index of V.*

At last, the following lemma is useful when deciding which element in F is represented by V.

Lemma 1.25 *Let a be a nonzero element in F. If V is nondegenerate, then a is represented by V if and only if $V \perp \langle -a \rangle$ is isotropic.*

Proof. Let Fe be a 1-dimensional quadratic space over F with $Q(e) = -a$. Suppose that a is represented by V. Then there exists $x \neq 0$ in V such that $Q(x) = a$. Therefore, $Q(x + e) = 0$ which implies that $V \perp \langle -a \rangle$ is isotropic.

Conversely, suppose that $V \perp Fe$ is isotropic. If V is isotropic, then we are done. Otherwise, there exist $x \in V \setminus \{0\}$ and $t \in F^\times$ such that $Q(x + te) = 0$. Then $Q(t^{-1}x) = -Q(e) = a$. □

1.5 Quadratic spaces over $\mathbb{C}$

The field of complex numbers $\mathbb{C}$ is algebraically closed. Therefore, every nonzero complex number is a square. If a is a nonzero complex number, then $\langle a\rangle \cong \langle 1\rangle \cong \langle -1\rangle$ over $\mathbb{C}$.

Let (V, B) be an n-dimensional nondegenerate quadratic space over $\mathbb{C}$. Let r be the greatest integer smaller than or equal to $n/2$. There are $2r$ pairwise orthogonal vectors $x_1, \ldots, x_r, y_1, \ldots, y_r$ of V such that

$$Q(x_i) = 1, Q(y_j) = -1, \quad 1 \leq i, j \leq r.$$

By Theorem 1.18, the binary subspaces $\mathbb{C}x_i + \mathbb{C}y_i$ are all isometric to $\mathbb{H}$. This implies that V has an orthogonal decomposition isometric to $\mathbb{H}^r \perp V_0$, where $V_0 \cong \langle 1\rangle$ or 0. There are several implications of this observation:

(i) All nondegenerate quadratic spaces over $\mathbb{C}$ of dimension ≥ 2 are isotropic.

(ii) Every nondegenerate quadratic space V has maximal Witt index, that is, $\mathrm{Ind}(V)$ is always $\lfloor n/2 \rfloor$.

(iii) The dimension of V determines the isometry class of V.

1.6 Quadratic Spaces over $\mathbb{R}$

The quotient group $\mathbb{R}^\times/\mathbb{R}^{\times 2}$ has two elements which are represented by 1 and -1, respectively. Therefore, if V is a nondegenerate quadratic space, V can be decomposed as

$$V \cong \langle 1\rangle^p \perp \langle -1\rangle^q.$$

The integer p is called the *positive index* of V and is denoted by $\mathrm{Ind}^+(V)$. Similarly, $q = \mathrm{Ind}^-(V)$ is the *negative index* of V. The difference $\mathrm{Ind}^+(V) - \mathrm{Ind}^-(V)$ is called the *signature* of V. It is a consequence of the Witt's Cancellation Theorem that both $\mathrm{Ind}^+(V)$ and $\mathrm{Ind}^-(V)$, and hence the signature, depend only on the isometry class of V.

Theorem 1.26 (Sylvester's Law of Inertia) *Let V and W be two nondegenerate quadratic spaces over $\mathbb{R}$. Then $V \cong W$ if and only if $Ind^+(W) = Ind^+(V)$ and $Ind^-(W) = Ind^-(V)$.*

A quadratic space (V, Q) over $\mathbb{R}$ is said to be *positive definite* if $Q(x) > 0$ for all $x \neq 0$. A *negative definite* quadratic space over $\mathbb{R}$ is defined analogously. A nondegenerate quadratic space over $\mathbb{R}$ is called *indefinite* if it is neither positive definite nor negative definite. In particular, an nondegenerate indefinite quadratic space over $\mathbb{R}$ must be isotropic and universal.

1.7 Quadratic Spaces over Finite Fields

Let $\mathbb{F}$ be a finite field of q elements. We always assume that q is odd. The number of square classes in $\mathbb{F}^\times$ is 2. Let Δ be a fixed nonsquare element in $\mathbb{F}^\times$.

Proposition 1.27 *For $n \geq 2$, every nondegenerate n-dimensional quadratic space over $\mathbb{F}$ is universal.*

Proof. It suffices to prove the proposition for a binary quadratic space (V, B) over $\mathbb{F}$. We may assume that $V \cong \langle \delta, \epsilon \rangle$ where $\delta, \epsilon \in \{1, \Delta\}$. If $V \cong \langle 1, \Delta \rangle$, then we are done. If $V \cong \langle \Delta, \Delta \rangle$, the set $Q(V)$ is equal to $\Delta \cdot Q(\langle 1, 1 \rangle)$. Therefore, we may assume that $V \cong \langle 1, 1 \rangle$. Our goal is to show that V represents Δ. If -1 is a square, then $\langle 1, 1 \rangle \cong \langle 1, -1 \rangle \cong \mathbb{H}$ which is universal. Therefore, We may further assume that -1 is a nonsquare.

The sets $\mathbb{F}^{\times 2}$ and $1 + \mathbb{F}^{\times 2}$ have the same number of elements. They are not equal since 1 is not inside $1 + \mathbb{F}^{\times 2}$. Therefore, there exists $\alpha \in \mathbb{F}^\times$ such that $1 + \alpha^2$ is not in $\mathbb{F}^{\times 2}$. This element $1 + \alpha^2$ cannot be zero because -1 is not a square. Hence V represents a nonsquare.□

Corollary 1.28 *Let V be a nondegenerate quadratic space over $\mathbb{F}$. Then*

$$V \cong \langle 1 \rangle \perp \cdots \perp \langle 1 \rangle \perp \langle d(V) \rangle.$$

Proof. We have a decomposition $V \cong \langle 1 \rangle \perp V_0$ whenever V is universal.□

Corollary 1.29 *Every nondegenerate quadratic space of dimension ≥ 3 over $\mathbb{F}$ is isotropic.*

Proof. Let (V, B) be a quadratic space of dimension ≥ 3 over $\mathbb{F}$. We may assume that $\dim(V) = 3$; hence V has a decomposition $V \cong \langle 1, 1, d(V) \rangle$. Since $\langle 1, d(V) \rangle$ is universal, it represents -1. As a result, V contains a binary subspace which is isometric to $\langle 1, -1 \rangle \cong \mathbb{H}$. Thus V is isotropic.□

Theorem 1.30 *Let V and W be nondegenerate quadratic spaces over $\mathbb{F}$. Then $V \cong W$ if and only if $d(V) = d(W)$ and $\dim(V) = \dim(W)$.*

Proof. If $V \cong W$, then of course $d(V)$ is equal to $d(W)$ and $\dim(V) = \dim(W)$. The converse is a consequence of Corollary 1.28.□

2 The p-adic Numbers

2.1 Valuations

Let F be a field whose characteristic is different from 2. A valuation on F is a function $|\ |$ of F into $\mathbb{R}$ which satisfies:

V1 $|a| > 0$ if $a \neq 0$, $|0| = 0$;

V2 $|ab| = |a||b|$;

V3 $|a + b| \leq |a| + |b|$,

for all $a, b \in F$. A function which satisfies V1, V2 and

V3' $|a + b| \leq \max\{|a|, |b|\}$

will satisfy V3 and therefore is a valuation. Axiom V3 is called the *triangle inequality* and V3' is called the *ultra triangle inequality*. A valuation is called *nonarchimedean* if it satisfies V3'; otherwise it is called *archimedean*.

There is always a valuation on F, namely the trivial valuation obtained by putting $|a| = 1$ for all $a \in F^\times$. Since this valuation has no significant interest, therefore we assume that every valuation in the subsequent discussion is nontrivial.

Given a valuation $|\ |$ on F, the distance function $d(a, b) = |a - b|$ makes F into a metric space. By a completion of F with respect to d (or $|\ |$) we mean a field $\hat{F}$ together with a valuation which satisfies

(i) $\hat{F}$ is complete with respect to the given valuation;

(ii) F is a subfield of $\hat{F}$ and the given valuation on $\hat{F}$ extends $|\ |$;

(iii) F is dense in $\hat{F}$.

Theorem 2.1 *A completion of F with respect to a valuation exists*

Proof. We know from topology that as a metric space F has a completion, that is, there is a metric space $\hat{F}$ which is complete and contains F as a dense subset. Moreover, the metric on $\hat{F}$ induces the metric d on F. Without causing any confusion, we denote the metric on $\hat{F}$ also by d. We have to define addition and multiplication on $\hat{F}$ to make it become a field. Let α and β be two elements in $\hat{F}$. They are the limits of two Cauchy sequences $\{a_n\}$ and $\{b_n\}$ in F, respectively. It is obvious to see that both $\{a_n + b_n\}$ and $\{a_n b_n\}$ are Cauchy and hence they converge to some elements in $\hat{F}$. Define

$$\alpha + \beta = \lim_n (a_n + b_n), \qquad \alpha\beta = \lim_n (a_n b_n).$$

One can check that these definition are independent of the choices of $\{a_n\}$ and $\{b_n\}$. Take the original 0 and 1 of F as the 0 and 1 of $\hat{F}$. These all together make $\hat{F}$ into a field.

Finally define $\|\alpha\| = d(\alpha, 0)$ for all $\alpha \in \hat{F}$. It is clear that $\|\ \|$ extends the original valuation on F. Suppose that α is the limit of a Cauchy sequence $\{a_n\}$ of F. By the triangle inequality,

$$-d(a_n, \alpha) \leq d(a_n, 0) - d(\alpha, 0) \leq d(a_n, \alpha).$$

Since $|a_n| - \|\alpha\| = d(a_n, 0) + d(\alpha, 0)$, therefore

$$\lim_n |a_n| = \|\alpha\|.$$

Hence, if $b_n \longrightarrow \beta$, then

$$\|\alpha\beta\| = \lim_n |a_n b_n| = \lim_n |a_n| \lim_n |b_n| = \|\alpha\|\|\beta\|.$$

Similarly $\|\alpha+\beta\| \leq \|\alpha\|+\|\beta\|$. Therefore, $\| \ \|$ is a valuation on $\hat{F}$, and the metric associated with $\| \ \|$ is d because

$$\|\alpha - \beta\| = \lim_n |a_n - b_n| = \lim_n d(a_n, b_n) = d(\alpha, \beta).$$

□

Remark 2.2 Note that $\| \ \|$ is nonarchimedean if $| \ |$ is nonarchimedean.

From now on, by abuse of notation, the valuation on $\hat{F}$ that extends $| \ |$ on F is also denoted by $| \ |$.

2.2 Nonarchimedean Valuations

Let $| \ |$ be a nonarchimedean valuation on a field F. By Remark 2.2, the extension of $| \ |$ to $\hat{F}$ is also nonarchimedean. Here are some consequences of the ultra triangle inequality V3':

(1) (Principle of Domination) Let $\alpha_1, \ldots, \alpha_n \in \hat{F}$. If $|\alpha_i| < |\alpha_1|$ for all i, then

$$|\alpha_1 + \cdots + \alpha_n| = |\alpha_1|.$$

(2) Let $\{\alpha_n\}$ be a sequence of elements of $\hat{F}$. If $\sum \alpha_n$ converges, then of course $\alpha_n \longrightarrow 0$. Conversely, suppose that $\alpha_n \longrightarrow 0$. Then for all $M \geq N$,

$$|\alpha_N + \cdots + \alpha_M| \leq \max\{|\alpha_j| : N \leq j \leq M\}.$$

Therefore, the partial sums of $\sum \alpha_n$ form a Cauchy sequence. Thus $\sum \alpha_n$ converges to some element in $\hat{F}$.

(3) Let $\alpha \in \hat{F}^\times$. There exists a sequence $\{a_n\}$ of elements in F which converges to α. Therefore, for all sufficiently large n, $|a_n - \alpha| < |\alpha|$. This shows that $|a_n| = |\alpha|$ for all sufficiently large n. This in particular shows that the two sets $|F|$ and $|\hat{F}|$ are the same.

(4) Let $\mathfrak{o}$ be the subset of F containing all elements of F with valuation ≤ 1. The principle of domination implies that $\mathfrak{o}$ is a subring of F. Let $\hat{\mathfrak{o}}$ be the closure of $\mathfrak{o}$ in $\hat{F}$. It follows from (3) $\hat{\mathfrak{o}}$ is a subring of $\hat{F}$. It is called the *valuation ring* of $\hat{F}$. Since $\hat{F}$ is complete and $\hat{\mathfrak{o}}$ is closed, $\hat{\mathfrak{o}}$ itself is a complete metric space.

(5) Let $\alpha \in \hat{\mathfrak{o}}$ such that $|\alpha| = 1$. Then $\alpha \neq 0$ and $|\alpha^{-1}| = 1$ also. This means that α^{-1} is in $\hat{\mathfrak{o}}$ and hence α is a unit of $\hat{\mathfrak{o}}$. This shows that $\hat{\mathfrak{o}}$ has only one maximal ideal

$$\mathfrak{p} = \{x \in \hat{\mathfrak{o}} : |x| < 1\}.$$

Note that the group of units of $\hat{\mathfrak{o}}$ is precisely the set $\hat{\mathfrak{o}} \setminus \mathfrak{p}$.

The valuation $|\ |$ is called a *discrete* valuation if the image the composition

$$\hat{F}^\times \longrightarrow \mathbb{R}^+ \xrightarrow{\log} \mathbb{R}$$

is an infinite cyclic subgroup of $\mathbb{R}$. Let $\pi \in \hat{\mathfrak{o}}$ be a pull back of a generator of this cyclic group. Such an element is called a *prime element* of $\hat{F}$. The ideal $\mathfrak{p}$ is generated by π and $\hat{\mathfrak{o}}$ is a principal ideal domain. Every element in $\hat{F}^\times$ is of the form $\pi^n u$ for some $n \in \mathbb{Z}$ and a unit u of $\hat{\mathfrak{o}}$. Let $\mathcal{C}$ be a complete set of representatives of cosets of $\mathfrak{p}$ in $\hat{\mathfrak{o}}$. We always pick 0 to represent $\mathfrak{p}$.

Proposition 2.3 *Suppose that $|\ |$ is a discrete valuation on F. Let $\mathcal{C}$ be a complete set of representatives of $\mathfrak{p}$ in $\hat{\mathfrak{o}}$ as described above. Then every element $\alpha \in \hat{F}$ can be expressed uniquely by a Laurent series*

$$\sum_{j \geq n} c_j \pi^j$$

where $c_j \in \mathcal{C}$ for all j, $|\alpha| = |\pi|^n$ and $c_n \neq 0$.

Proof. We may assume that $\alpha \neq 0$. Suppose that $\alpha = \pi^n u$ for some unit u of $\hat{\mathfrak{o}}$. Choose $c_n \in \mathcal{C}$ such that $u \equiv c_n \bmod \mathfrak{p}$. Then $c_n \neq 0$ and

$$\alpha = c_n \pi^n + \alpha_1$$

with $|\alpha_1| \leq |\pi|^{n+1}$. Next apply this procedure to α_1 to obtain an α_2, then to α_2, and so on. From this procedure we obtain a sequence $c_n, c_{n+1}, \ldots$ of elements of $\mathcal{C}$ such that for each $m \geq n$, there exists $\beta_{m+1} \in \mathfrak{p}^{m+1}$ and

$$\alpha = c_n \pi^n + c_{n+1} \pi^{n+1} + \cdots + c_{n+m} \pi^{n+m} + \beta_{m+1}.$$

The partial sum

$$c_n \pi^n + \cdots + c_{n+m} \pi^{n+m}$$

clearly converges to α.

Suppose that there are two Laurent series

$$\sum_{j \geq n} c_j \pi^j = \sum_{j \geq n} d_j \pi^j$$

with $c_j, d_j \in \mathcal{C}$ for all j but $c_i \neq d_i$ for some $i \geq j$. Let i be the smallest index with this property. Then $c_i - d_i \notin \mathfrak{p}$ which means that $c_i - d_i$ is a unit of $\hat{\mathfrak{o}}$. Then

$$0 = \left| \sum_{j \geq n} c_j \pi^j - \sum_{j \geq n} d_j \pi^j \right| = |\pi|^i,$$

which is impossible.□

2.3 Valuations on $\mathbb{Q}$

Our primary objects of investigation here are the valuations of $\mathbb{Q}$. The usual absolute value is an archimedean valuation on $\mathbb{Q}$. We denote it by $|\ |_\infty$. The completion of $\mathbb{Q}$ with respect to $|\ |_\infty$ is the field of real numbers $\mathbb{R}$.

Beside $|\ |_\infty$, $\mathbb{Q}$ has other valuations. Let p be a prime number. Any $\alpha \in \mathbb{Q}^\times$ can be written as

$$\alpha = p^i \frac{a}{b}$$

where a and b are integers prime to p. Put

$$|\alpha|_p = \frac{1}{p^i}.$$

It is easy to show that this defines a discrete nonarchimedean valuation on $\mathbb{Q}$. The completion of $\mathbb{Q}$ with respect to $|\ |_p$ is the field of p-adic numbers $\mathbb{Q}_p$. Its valuation ring is the ring of p-adic integers $\mathbb{Z}_p$. The topology on $\mathbb{Q}$ or $\mathbb{Q}_p$ induced by $|\ |_p$ is called the p-adic topology. In the p-adic topology, every $p^n\mathbb{Z}_p$ is both open and closed.

Lemma 2.4 *The maximal ideal of $\mathbb{Z}_p$ is generated by p.*

Let α be a p-adic integer. Since $\mathbb{Z}_p$ is the closure of $\mathbb{Z}$ under the p-adic topology, therefore there exists $a \in \mathbb{Z}$ such that $\alpha \equiv a \mod p\mathbb{Z}_p$. Hence we can choose $\mathcal{C} = \{0, 1, \ldots, p-1\}$ to be a complete set of representatives of $\mathbb{Z}_p/p\mathbb{Z}_p$. In this way, every p-adic number can be represented uniquely as a Laurent series in p

$$\sum_{j=n}^{\infty} c_j p^j$$

with $c_j \in \mathcal{C}$.

Corollary 2.5 *$\mathbb{Z}_p/p\mathbb{Z}_p$ is a finite field of p elements.*

Proof. Let $\alpha \in \mathbb{Z}_p$. Then α can be represented by a Taylor series in p

$$\alpha = \sum_{j=0}^{\infty} c_j p^j$$

with $c_j \in \mathcal{C}$. The function $\alpha \mapsto c_0 \mod p$ is clearly a surjective ring homomorphism from $\mathbb{Z}_p$ onto $\mathbb{Z}/p\mathbb{Z}$ with kernel $p\mathbb{Z}_p$.□

Corollary 2.6 *$\mathbb{Z}_p$ is a compact topological space.*

Proof. Let $\{\mathcal{O}_\lambda : \lambda \in \Lambda\}$ be an opening covering of $\mathbb{Z}_p$. Suppose that it has no finite subcovering. Note that

$$\mathbb{Z}_p = \bigcup_{i=1}^{p-1} (i + p\mathbb{Z}_p).$$

Therefore, there exists $c_0 \in \mathcal{C} = \{0, 1, \ldots, p-1\}$ such that $c_0 + p\mathbb{Z}_p$ is not covered by finitely many of the $\mathcal{O}_\lambda$. Similarly, there exists $c_1 \in \mathcal{C}$ such that $c_0 + c_1 p + p^2\mathbb{Z}_p$ is not finitely covered. By continuing this process, we can construct a sequence $c_0, c_1 \ldots$ of elements of $\mathcal{C}$ such that for each $j \geq 0$,

$$c_0 + c_1 p + \cdots + c_j p^j + p^{j+1}\mathbb{Z}_p$$

is not finitely covered. Let

$$\alpha = \sum_{j=0}^{\infty} c_j p^j.$$

Then $\alpha \in \mathbb{Z}_p$, and α must be in $\mathcal{O}_{\lambda_0}$ for some $\lambda_0 \in \Lambda$. Since $\mathcal{O}_{\lambda_0}$ is open, there exists $m \geq 1$ such that $\alpha + p^m\mathbb{Z}_p \subseteq \mathcal{O}_{\lambda_0}$. But then

$$c_0 + c_1 p + \cdots + c_{m-1} p^{m-1} + p^m\mathbb{Z}_p \subseteq \mathcal{O}_{\lambda_0}$$

which is a contradiction.□

Definition 2.7 Two valuations $|\ |$ and $\|\ \|$ on a field F are said to be *equivalent* if there exists a nonzero real number k such that $|\ |^k = \|\ \|$.

Equivalent valuations on a field F define the same topology on F. It is not hard to see that the absolute value $|\ |_\infty$ and the p-adic valuations $|\ |_p$ are inequivalent valuations on $\mathbb{Q}$.

Theorem 2.8 (Ostrowski) Every nontrivial valuation of $\mathbb{Q}$ is equivalent to $|\ |_\infty$ or $|\ |_p$ for some prime p.

Before giving the proof of Ostrowski's theorem, we need a lemma to characterize the nonarchimedean valuations on $\mathbb{Q}$.

Lemma 2.9 *A valuation $\|\ \|$ on $\mathbb{Q}$ is nonarchimedean if and only if it is bounded on $\mathbb{Z}$.*

Proof. Suppose that $\|\ \|$ is nonarchimedean. Then for any positive integer n,

$$\|n\| = \|1 + \cdots + 1\| \leq \|1\| = 1.$$

Therefore, $\|\ \|$ is bounded on $\mathbb{Z}$.

Conversely, suppose that $\|m\| < K$ for all $m \in \mathbb{Z}$. Then for any positive integer k and any rational numbers x, y,

$$\|x + y\|^k \leq K(|x\|^k + \|x\|^{k-1}\|y\| + \cdots + \|y\|^k) \leq K(k+1)\max\{\|x\|, \|y\|\}^k.$$

Taking the k-th root on both sides and letting $k \longrightarrow \infty$, we see that $\|\ \|$ is nonarchimedean.□

Proof of Ostrowski's theorem. Let $\|\ \|$ be a nonarchimedean valuation on $\mathbb{Q}$. Then $\|n\| \leq 1$ for all $n \in \mathbb{Z}$. So, there must be a prime number p such that $\|p\| < 1$ because, if not, the Fundamental Theorem of Arithmetic would imply $\|x\| = 1$ for all $x \in \mathbb{Q}^\times$.

The set $\mathfrak{a} = \{a \in \mathbb{Z} : \|a\| < 1\}$ is an ideal of $\mathbb{Z}$ satisfying $p\mathbb{Z} \subseteq \mathfrak{a} \neq \mathbb{Z}$. Thus $p\mathbb{Z} = \mathfrak{a}$. If $a \in \mathbb{Z}$ and $a = p^m b$ with $\gcd(p, b) = 1$, then $\|b\| = 1$ and hence

$$\|a\| = \|p\|^m = |a|_p^s$$

where $s = -\log \|p\| / \log p$. Consequently $\| \ \|$ is equivalent to $| \ |_p$.

Now, suppose that $\| \ \|$ is archimedean. Let $m > 1$ and $n > 1$ be two natural numbers. Then

$$m = a_0 + a_1 n + \cdots + a_r n^r$$

where $a_i \in \{0, 1, \ldots, n-1\}$ and $n^r \leq m$. Observe that $r \leq \log m / \log n$ and $\|a_i\| \leq a_i \|1\| \leq n$. So, $\|m\| < n(1 + \|n\| + \cdots + \|n\|^r)$. If $\|n\| < 1$, then $\|m\| < n/(1 - \|n\|)$ and this is true for all $m \in \mathbb{Z}$. This contradicts that $\| \ \|$ is archimedean. Therefore, $\|n\| \geq 1$ and we obtain the inequality

$$\|m\| \leq \sum_{i=1}^{n} \|a_i\| \cdot \|n\|^r \leq \left(1 + \frac{\log m}{\log n}\right) n \cdot \|n\|^{\log m / \log n}.$$

Substituting here m^k for m, taking k-th roots on both sides, and letting k tend to ∞, one finally obtains

$$\|m\| \leq \|n\|^{\log m / \log n}, \text{ or } \|m\|^{1/\log m} \leq \|n\|^{1/\log n}.$$

Interchanging the roles of m and n gives

$$\|m\|^{1/\log m} = \|n\|^{1/\log n}.$$

Putting $c = \|n\|^{1/\log n}$ and pick s so that $c = e^s$. Then for any positive rational number x,

$$\|x\| = e^{s \log x} = |x|^s.$$

Therefore $\| \ \|$ is equivalent to $| \ |_\infty$.□

Proposition 2.10 (Product Formula) *For any $a \in \mathbb{Q}^\times$, we have*

$$|a|_\infty \prod_p |a|_p = 1.$$

Proof. The proof is obvious. Note that $|a|_p = 1$ for almost all p.□

2.4 Square Classes of $\mathbb{Q}_p$

Let p be a prime number. It is clear that every square class of $\mathbb{Q}_p^\times$ must contain either a unit or a prime element, but not both.

Lemma 2.11 (Local Square Theorem)*Let $\alpha \in \mathbb{Q}_p^\times$ and suppose that*

$$|\alpha - \epsilon^2|_p \leq |4p|_p$$

for some unit ϵ in $\mathbb{Z}_p$. Then α is a square in $\mathbb{Z}_p^\times$.

Proof. The hypothesis implies that α is in $\mathbb{Z}_p^\times$. Write ϵ as ϵ_0 and suppose that for any non-negative integer $k \leq n$, there is $\epsilon_k \in \mathbb{Z}_p^\times$ such that

$$\alpha \equiv \epsilon_k^2 \mod 4p^{k+1}.$$

Let $b \in \mathbb{Z}$ such that

$$\frac{\alpha - \epsilon_n^2}{4p^{n+1}} \equiv b\epsilon_n \mod p.$$

Putting $\epsilon_{n+1} = \epsilon_n + 2bp^{n+1}$ gives

$$\alpha - \epsilon_{n+1}^2 = 4p^{n+1}\left(\frac{\alpha - \epsilon_n^2}{4p^{n+1}} - b\epsilon_n\right) - 4b^2p^{2(n+1)}.$$

The choice of b implies $\alpha \equiv \epsilon_{n+1}^2 \mod 4p^{n+2}$. Thus we have proved the existence of a sequence $\{\epsilon_n\}$ in $\mathbb{Z}_p^\times$ such that $\alpha \equiv \epsilon_n^2 \mod 4p^{n+1}$ and $\epsilon_{n+1} \equiv \epsilon_n \mod p^{n+1}$ for every $n \geq 0$.

Now, for any $m > n$,

$$\begin{aligned} |\epsilon_m - \epsilon_n|_p &= |(\epsilon_m - \epsilon_{m-1}) + \cdots + (\epsilon_{n+1} - \epsilon_n)|_p \\ &\leq p^{-(n+1)} \end{aligned}$$

Therefore $\{\epsilon_n\}$ is a Cauchy sequence and it must converge to some x in $\mathbb{Z}_p$. As $\alpha \equiv \epsilon_{n+1}^2 \mod 4p^{n+2}$ for all n, we see that $\alpha = x^2$.□

Corollary 2.12 *For any $\alpha \in \mathbb{Q}_p^\times$, the set $\alpha\mathbb{Q}_p^{\times 2}$ is an open subset of $\mathbb{Q}_p^\times$.*

Proof. Let $\alpha y^2 \in \alpha\mathbb{Q}_p^{\times 2}$. For any $x \in \mathbb{Q}_p^\times$ such that $|x - \alpha y^2|_p \leq |4p\alpha y^2|_p$, we have

$$\left|\frac{x}{\alpha y^2} - 1\right|_p \leq |4p|_p.$$

Therefore $x(\alpha y^2)^{-1}$ is a square and hence $x \in \alpha\mathbb{Q}_p^{\times 2}$.□

Corollary 2.13 *$\mathbb{Q}_2^\times/\mathbb{Q}_2^{\times 2}$ is of order 8 and generated by $2, -1$ and 5. For $p \neq 2$, let Δ be a non-square unit in $\mathbb{Z}_p$. Then $\mathbb{Q}_p^\times/\mathbb{Q}_p^{\times 2}$ is of order 4 and generated by p and Δ.*

Proof. The assertion for $p \neq 2$ is clear since $(\mathbb{Z}/p\mathbb{Z})^\times$ has only 2 square classes represented by 1 and Δ respectively. Suppose $\alpha = x^2$ in $\mathbb{Z}_2^\times$. Let $x = \sum_{j=0}^\infty c_j 2^j$ with $c_j \in \{0, 1\}$ and $c_0 = 1$. Then

$$\begin{aligned} \alpha &= (c_0 + 2c_1)^2 + 2(c_0 + 2c_1)\sum_{j=2}^\infty c_j 2^j + \left(\sum_{j=2}^\infty c_j 2^j\right)^2 \\ &\equiv (c_0 + 2c_1)^2 \mod 8 \\ &\equiv 1 \mod 8. \end{aligned}$$

Therefore, $\alpha \in \mathbb{Z}_2^{\times 2}$ if and only if $\alpha \equiv 1 \bmod 8$. Thus the square classes represented by the units are generated by -1 and 5.□

In the following proposition, $\delta \in \{\Delta, p\Delta, p\}$ if $p > 2$, and $\delta \in \{-1, 3, 5, 2, -2, 6, 10\}$ if $p = 2$.

Proposition 2.14 *(a) If $p > 2$, then $x^2 - \delta y^2 \in \mathbb{Z}_p$ if and only if x and y are in $\mathbb{Z}_p$.*
(b) If $p = 2$ and $\delta \neq 5$, then $x^2 - \delta y^2 \in \mathbb{Z}_2$ if and only if $x, y \in \mathbb{Z}_2$.
(c) If $p = 2$ and $\delta = 5$, then $x^2 - 5y^2 \in \mathbb{Z}_2$ if and only if $x = s/2, y = t/2$, $s, t \in \mathbb{Z}_2$ and $s - t \in 2\mathbb{Z}_2$.

Proof. (a) We assume that $x^2 - \delta y^2 \in \mathbb{Z}_p$. The statement is clear if either x or y is zero. Thus we further assume that $xy \neq 0$. Consider the case when $\delta = \Delta$ first. Suppose $|x|_p \geq |y|_p$. Since the space $\langle 1, -\Delta \rangle$ is anisotropic over $\mathbb{Z}_p/p\mathbb{Z}_p \cong \mathbb{Z}/p\mathbb{Z}$, therefore $1 - (y/x)^2\Delta$ is always a unit in $\mathbb{Z}_p$. In other words, $|x|_p \leq 1$ and hence $|y|_p \leq 1$ also. Similar argument applies to the case when $|x|_p \leq |y|_p$. Now suppose $\delta = p\epsilon$ with $\epsilon = 1$ or Δ. If $|x|_p \geq |y|_p$, then

$$|x^2 - y^2 p\epsilon|_p = |x|_p^2 \left|1 - (\frac{y}{x})^2 p\epsilon\right|_p = |x|_p^2.$$

Thus both x and y are in $\mathbb{Z}_p$. If, on the other hand, $|y|_p \geq |x|_p$, then we consider

$$x^2 - y^2 p\epsilon = y^2 \left(\left(\frac{x}{y}\right)^2 - p\epsilon \right)$$

and deduce that $|(x/y)^2 - p\epsilon|_p$ is either 1 or $|p|_p$. Therefore, y is in $\mathbb{Z}_p$ and hence so is x.

For (b), we assume that $x^2 - y^2\delta \in \mathbb{Z}_2$ and $xy \neq 0$. If $2 \mid \delta$, then the above argument for $p > 2$ can apply here. Suppose $\delta = -1$. If $y/x \in \mathbb{Z}_2$, then $(y/x)^2 \equiv 0 \bmod 4$ or $1 \bmod 8$. So, $1 + (y/x)^2$ is a unit or it is congruent to 2 mod 8. The former implies that $|x|_2^2 \leq 1$ and thus $x \in \mathbb{Z}_2$. This implies $y \in \mathbb{Z}_2$ as well. If $1 + (y/x)^2 \equiv 2 \bmod 8$, then $2x^2 \in \mathbb{Z}_2$ which implies $x \in \mathbb{Z}_2$. Thus $y \in \mathbb{Z}_2$ also. Same argument works when $x/y \in \mathbb{Z}_2$. The case $\delta = 3$ can be done in a similar manner.

For (c), it is clear that if $x = s/2$ and $y = t/2$ with $s, t \in \mathbb{Z}_2^{\times}$, then $x^2 - 5y^2 \in \mathbb{Z}_2$ and $xy \neq 0$. Conversely, suppose $x^2 - 5y^2 \in \mathbb{Z}_2$. If $y/x \in \mathbb{Z}_2$, then $1 - 5(y/x)^2$ is either a unit or $\equiv 4 \bmod 8$. The first option implies that $x \in \mathbb{Z}_2$ and hence $y \in \mathbb{Z}_2$ as well. The second happens only if y/x is a unit and $x = s/2$ with $s \in \mathbb{Z}_2$. So, $y = t/2$ with $t \in \mathbb{Z}_2$. Note that $s - t \in 2\mathbb{Z}_2$ whenever $|s|_2 = |t|_2$. The argument is similar when $x/y \in \mathbb{Z}_2$.□

2.5 Quadratic Reciprocity

Let p be an odd prime and $\mathbb{F}_p$ be a finite field of p elements. For any $x \in \mathbb{F}_p^{\times}$, define

$$\left(\frac{x}{p}\right) := \begin{cases} 1 & \text{if } x \text{ is a square,} \\ -1 & \text{otherwise.} \end{cases}$$

It is called the Legendre symbol mod p. Its definition is often extended to integers that are relatively prime to p. It is clear that the Legendre symbol is multiplicative in x.

Lemma 2.15 *For any $a \in \mathbb{F}_p^\times$,*

$$a^{\frac{p-1}{2}} = \left(\frac{a}{p}\right) \quad in\ \mathbb{F}_p.$$

Proof. Let ξ be a generator of $\mathbb{F}_p^\times$. For any integer n, the order of $\xi^{\frac{(p-1)n}{2}}$ is 1 if n is even and 2 otherwise. Therefore $\xi^{\frac{(p-1)n}{2}}$ is 1 if n is even and -1 otherwise. The lemma follows from the fact that a can be written as ξ^n for some n and a is a square if and only if n is even.□

Lemma 2.16 *For any odd prime p,*

$$\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}}, \quad \left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}.$$

Proof. The first equality is clear. For the second one, let ξ be a primitive 8-th root of unity in the algebraic closure of $\mathbb{F}_p$. Then $\xi^4 = -1$ and $\xi^2 + \xi^{-2} = 0$. Therefore, if $y = \xi + \xi^{-1}$, then $y^2 = 2$. Hence 2 is a square in $\mathbb{F}_p$ if and only if $y \in \mathbb{F}_p$, or equivalently, $y^p = y$. The last condition is satisfied if and only if $\xi^{p+1}(\xi^{p-1} - 1) = \xi^{p-1} - 1$, which is the same as $\xi^{p-1} = 1$ or $\xi^{p+1} = 1$. Therefore, 2 is a square in $\mathbb{F}_p$ if and only if $p \equiv \pm 1 \bmod 8$. □

Theorem 2.17 (Quadratic Reciprocity Law) *Let $q \neq p$ be two odd primes. Then*

$$\left(\frac{q}{p}\right)\left(\frac{p}{q}\right) = (-1)^{\frac{p-1}{2}\frac{q-1}{2}}.$$

Proof. For simplicity, we put $\chi(a) = \left(\frac{a}{p}\right)$ for any $a \in \mathbb{F}_p^\times$ and $\chi(0) = 0$. Since half of the elements in $\mathbb{F}_p^\times$ are squares and the other half consists of non-squares, $\sum_{b\in\mathbb{F}_p} \chi(b) = 0$. Let x be a primitive p-th root of unity in the algebraic closure of $\mathbb{F}_q$. So it makes sense to talk about x^a for any $a \in \mathbb{F}_p \cong \mathbb{Z}/p\mathbb{Z}$. Put

$$g := \sum_{a\in\mathbb{F}_p} \chi(a)x^a.$$

Then

$$g^2 = \sum_{a,b\in\mathbb{F}_p} \chi(ab)x^{a+b} = \sum_{c\in\mathbb{F}_p} x^c \sum_{a\in\mathbb{F}_p} \chi(a(c-a)).$$

If $c \neq 0$, then we have

$$\begin{aligned}
\sum_{a\in\mathbb{F}_p} \chi(a(c-a)) &= \chi(-1)\sum_{a\in\mathbb{F}_p^\times} \chi(a^2-ac) \\
&= \chi(-1)\sum_{a\in\mathbb{F}_p^\times} \chi(1-a^{-1}c) \\
&= \chi(-1)\sum_{a\in\mathbb{F}_p^\times} \chi(1-a) \\
&= \chi(-1)\sum_{b\in\mathbb{F}_p} \chi(b) - \chi(-1) \\
&= -\chi(-1).
\end{aligned}$$

Thus

$$g^2 = -\chi(-1)\sum_{c\neq 0} x^c + \sum_{a\in\mathbb{F}_p} \chi(-a^2) = \chi(-1) + (p-1)\chi(-1) = p\chi(-1).$$

On the other hand, if we raise g to the q-th power, we get

$$g^q = \sum_{a\in\mathbb{F}_p} \chi(a)x^{qa} = \chi(q)\sum_{a\in\mathbb{F}_p} \chi(qa)x^{qa} = \chi(q)g$$

and so $g^{q-1} = \chi(q)$. Therefore, in $\mathbb{F}_q$,

$$\chi(-1)^{\frac{q-1}{2}} p^{\frac{q-1}{2}} = \left(\frac{q}{p}\right).$$

The left hand side is equal to $(-1)^{\frac{q-1}{2}\frac{p-1}{2}} \left(\frac{p}{q}\right)$ in $\mathbb{F}_q$. Therefore

$$(-1)^{\frac{p-1}{2}\frac{q-1}{2}} = \left(\frac{q}{p}\right)\left(\frac{p}{q}\right) \text{ in } \mathbb{F}_q.$$

This can be seen as an equality in $\mathbb{Z}$ because both sides are ± 1.$\square$

2.6 Hilbert Symbols and Hilbert Reciprocity

In this subsection, let F be either $\mathbb{R}$ or $\mathbb{Q}_p$ for some prime p. Let a, b be two nonzero elements in F. The Hilbert symbol $(a,b)_F$ is defined as

$$(a,b)_F = \begin{cases} 1 & \text{if } \langle a,b,-1\rangle \text{ is isotropic over } F, \\ -1 & \text{otherwise.} \end{cases}$$

For simplicity, we will use (a,b) unless confusion arises. It is clear from the definition that the Hilbert symbol is a symmetric function defined on $F^\times/F^{\times 2} \times F^\times/F^{\times 2}$. Moreover, $(a,b) = 1$ whenever a or b is a square.

Lemma 2.18 *For any $a, b, c \in F^\times$,*

(a) $(a,b) = (b,a)$, $(a,b^2) = 1$.

(b) $(a,-a) = (a,1-a) = 1$ *if* $a \neq 1$.

(c) $(a,a) = (a,-1)$.

(d) $(a,bc) = (a,b)(a,c)$.

Proof. Part (a) and (b) are obvious. For part (c), since $a \neq 0$, $\langle a, a, -1\rangle$ is isotropic if and only if $\langle -1, -1, a\rangle$ is isotropic.

For part (d), we may assume that a is not a square. The case $F = \mathbb{R}$ can be verified directly: $(-1,d) = 1$ if and only if $d > 0$.

When $F = \mathbb{Q}_p$, let

$$N_a = \{x^2 - ay^2 \neq 0 : x, y \in F\}.$$

Note that N_a is in fact a subgroup of $F^\times$. Observe that $(d,a) = 1$ if and only if $d \in N_a$. Therefore, part (d) is valid if either b or c is in N_a. It remains to show that $bc \in N_a$ if $b, c \notin N_a$. It suffices to show that $[F^\times : N_a] \leq 2$.

Suppose $p > 2$. Then we may assume that $a \in \{\Delta, p, p\Delta\}$, where Δ is a nonsquare unit in $\mathbb{Z}_p^\times$. If $a = p$ or $p\Delta$, then $-a \in N_a$, which implies $[N_a : F^{\times 2}] \geq 2$ and thus $[F^\times : N_a] \leq 2$. If $a = \Delta$, the space $\langle \Delta, -1, -1\rangle$ is isotropic over $\mathbb{Z}_p/p\mathbb{Z}_p$ but $\langle \Delta, -1\rangle$ is anisotropic. Therefore, there exist $z \in \mathbb{Z}_p^\times$ and $x, y \in \mathbb{Z}_p$ such that $(\Delta x^2 - y^2) - z^2 \equiv 0 \mod p$. By Lemma 2.11, $\Delta x^2 - y^2$ itself must be a square and hence $\Delta x^2 - y^2 = t^2$ for some $t \in \mathbb{Z}_p$. Therefore, $\Delta t^2 \in N_a$ and $[N_a : F^{\times 2}] \geq 2$.

If $p = 2$, we have to show that $[N_a : F^{\times 2}] \geq 4$. It suffices to produce 3 different square classes in N_a. We may assume that a is coming from $\{3, 5, -1, 2, 6, 10, -2\}$. If a is divisible by 2, the numbers $1, -a, 1-a$ fall into different square classes in N_a. When a is not divisible by 2, then $1, 1-a, 1-4a$ will do the job.□.

Note that even when a is a square, the assertion that $(d,a) = 1$ if and only if $d \in N_a$ is still true.

For $a \in \mathbb{Q}_p^\times$, we can write $a = p^m u$ with $m \in \mathbb{Z}$ and $u \in \mathbb{Z}_p^\times$. The integer m is called the order of a, denoted $\mathrm{ord}_p(a)$.

Lemma 2.19 *Let Δ be a nonsquare unit in $\mathbb{Z}_p$ if $p > 2$ and $\Delta = 5$ if $p = 2$. Then,*

$$(\Delta, a)_{\mathbb{Q}_p} = \begin{cases} 1 & \text{if } ord_p(a) \text{ is even,} \\ -1 & \text{otherwise.} \end{cases}$$

Proof. Obviously, we may assume that $\mathrm{ord}_p(a)$ is 0 or 1. We first treat the case when $p > 2$. Since the binary space $\langle 1, -\Delta\rangle$ is anisotropic over $\mathbb{Z}_p/p\mathbb{Z}_p$, therefore if $x^2 - \Delta y^2 \equiv 0 \mod p$, both x and y are $\equiv 0 \mod p$ and hence $\mathrm{ord}_p(x^2 - \Delta y^2) \geq 2$. In this case, $a \notin N_\Delta$ and so $(a, \Delta)_{\mathbb{Q}_p} = -1$. On the other hand, suppose $\mathrm{ord}_p(a) = 0$. Since the space $\langle 1, -\Delta\rangle$

is universal over $\mathbb{Z}_p/p\mathbb{Z}_p$, there exist $x, y \in \mathbb{Z}_p^\times$ such that $x^2 - \Delta y^2 \equiv a \mod p$. By the Local Square Theorem, there exist $z \in \mathbb{Z}_p^\times$ such that $x^2 - \Delta y^2 = az^2$, which implies that $(a, \Delta)_{\mathbb{Q}_p} = 1$.

Let us consider the case $p = 2$. Suppose $\mathrm{ord}_2(x^2 - 5y^2) = 1$. If $x, y \in \mathbb{Z}_2$, then both of them must be units in $\mathbb{Z}_2$. So $x^2 - 5y^2 \equiv 4 \mod 8$ which is a contradiction. This implies that $x = s/2$ and $y = t/2$ for some units s, t and $s^2 - 5t^2 \equiv 0 \mod 8$. But this is impossible because $s^2 - 5t^2 \equiv 4 \mod 8$ for any units x, y. Therefore, $2 \notin N_5$ and so $(5, 2)_{\mathbb{Q}_2} = -1$.

If $a \in \mathbb{Z}_2^\times$, we can always find $x, y \in \mathbb{Z}_2$ such that $x^2 - 5y^2 \equiv a \mod 8$. By the Local Square Theorem again, we see that $a \in N_5$ and so $(5, a)_{\mathbb{Q}_2} = 1$. □

Corollary 2.20 *If $p > 2$ and $\epsilon, \delta \in \mathbb{Z}_p^\times$, then $(\epsilon, \delta)_{\mathbb{Q}_p} = 1$.*

Corollary 2.21 *If $p > 2$ and $\epsilon \in \mathbb{Z}_p^\times$, then*

$$(\epsilon, p)_{\mathbb{Q}_p} = \begin{cases} 1 & \text{if } \epsilon \text{ is a square,} \\ -1 & \text{otherwise.} \end{cases}$$

Consequently, $(\epsilon, p)_{\mathbb{Q}_p}$ is the Legendre symbol $\left(\frac{\bar{\epsilon}}{p}\right)$, where $\bar{\epsilon}$ is the class of ϵ mod $p\mathbb{Z}_p$.

Theorem 2.22 (Hilbert Reciprocity Law) *For any $a, b \in \mathbb{Q}^\times$, we have*

$$(a, b)_{\mathbb{R}} \prod_p (a, b)_{\mathbb{Q}_p} = 1.$$

Proof. Put

$$F_a(x) := (a, x)_{\mathbb{R}} \prod_p (a, x)_{\mathbb{Q}_p}.$$

Since $(a, x)_{\mathbb{Q}_p} = 1$ for almost all p, therefore $F_a(x)$ is well defined. Moreover, $F_a(xy) = F_a(x)F_a(y)$, $F_a(x) = F_x(a)$ and $F_a(a) = F_a(-1)$. So it suffices to show that $F_{-1}(-1)$, $F_{-1}(2)$, $F_{-1}(p)$, $F_2(p)$, and $F_p(q)$ are all equal to 1, where p, q are odd prime numbers.

Note that $(a, b)_{\mathbb{R}} = -1$ if and only if both a and b are negative. If a is a unit in $\mathbb{Z}_2$, then $x^2 + y^2 = a$ is solvable in $\mathbb{Q}_2$ if and only if $a \equiv 1 \mod 4$. Therefore, $(-1, -1)_{\mathbb{Q}_2} = -1$ and $(-1, p)_{\mathbb{Q}_2} = (-1)^{\frac{p-1}{2}}$. The equation $x^2 - 2y^2 = p$ is solvable in $\mathbb{Q}_2$ if and only if $p \equiv \pm 1 \mod 8$. Therefore $(p, 2)_{\mathbb{Q}_2} = (-1)^{\frac{p^2-1}{8}}$ and in particular $(-1, 2)_{\mathbb{Q}_2} = 1$. Together with Lemma 2.16 and Corollary 2.20, these show that

$$F_{-1}(-1) = F_{-1}(2) = F_{-1}(p) = F_2(p) = 1.$$

For $F_p(q) = 1$, we have to show that $(p, q)_{\mathbb{Q}_2} = 1$ if and only if p or q is congruent to 1 mod 4. We first assume that either p or q is congruent to 1 mod 4. Without loss of generality, suppose $p \equiv 1 \mod 4$. We may further assume that p is either 1 or 5. Clearly, $(1, q)_{\mathbb{Q}_2} = 1$ for all q and Lemma 2.19 shows that $(5, q)_{\mathbb{Q}_2} = 1$ as well.

Now suppose that $(p,q)_{\mathbb{Q}_2} = 1$. So there exist $x, y \in \mathbb{Q}_2$ such that $x^2 - py^2 = q$. Assume that p and q are $\equiv 3 \mod 4$. Then x and y are in $\mathbb{Z}_2$. Modulo 4, we have

$$3 \equiv q \equiv x^2 - py^2 \equiv 1 \mod 4$$

which is a contradiction. Thus either p or q is $\equiv 1 \mod 4$.□

For our convenience, we extract the following from the proof above.

Corollary 2.23 *If a and b are odd integers, then*

$$\begin{cases} (a,b)_{\mathbb{Q}_2} = & (-1)^{\frac{(a-1)}{2}\frac{(b-1)}{2}}, \\ (a,2)_{\mathbb{Q}_2} = & (-1)^{\frac{a^2-1}{8}}. \end{cases}$$

Our last remark is that if $a \in \mathbb{Q}_p^\times$ which is not a square, then $(\ ,a) : \mathbb{Q}_p^\times \to \{\pm 1\}$ is a surjective group homomorphism with kernel N_a.

3 Quadratic Spaces over $\mathbb{Q}_p$

3.1 Hasse Invariants

Within this subsection, F is either $\mathbb{R}$ or $\mathbb{Q}_p$ for some prime p. Let (V,B) be a nondegenerate quadratic space over F. Take an orthogonal basis for V and suppose

$$V \cong \langle \alpha_1, \cdots, \alpha_n \rangle$$

in this basis. We define the *Hasse invariant* of V, written as $S_F(V)$ or simply $S(V)$ if F is clear from the context, to be

$$\prod_{1 \le i \le j \le n} (\alpha_i, \alpha_j),$$

where all the Hilbert symbols are over F.

Theorem 3.1 *$S(V)$ is independent of the choice of the orthogonal basis.*

Proof. If $n = 1$ and $V \cong \langle \alpha \rangle$, then $(\alpha, \alpha) = (\alpha, -1) = (d(V), -1)$ which depends only on V.

Suppose $n = 2$. A direct computation shows that

$$\prod_{i \le j} (\alpha_i, \alpha_j) = (d(V), -1)(\alpha_1, \alpha_2).$$

Now, $(\alpha_1, \alpha_2) = 1$ if and only if $\langle \alpha_1, \alpha_2, -1 \rangle \cong V \perp \langle -1 \rangle$ is isotropic. This is certainly dependent on V, not on the basis chosen.

When $n \geq 3$, we need a couple of definitions. Let $\{v_i\}$ and $\{u_i\}$ be two orthogonal bases for V. We write $\{v_i\} \sim \{u_i\}$ if $Fv_i = Fu_j$ for some i, j. We say that $\{v_i\}$ and $\{u_i\}$ are *linked* if there exist orthogonal bases $\{z_i^j\}$ of V such that

$$\{v_i\} = \{z_i^1\} \sim \{z_i^2\} \sim \cdots \sim \{z_i^m\} = \{u_i\}.$$

Claim: *If* $\dim(V) \geq 3$*, then every pair of orthogonal bases for* V *are linked.*

Let us show how the theorem follows from the claim. Using the claim, we may assume that

$$V \cong \langle \alpha_1, \ldots, \alpha_n \rangle \cong \langle \beta_1, \ldots, \beta_n \rangle$$

and $\alpha_h = \beta_k$ for some h, k. It suffices to show that $S(V)$ is unchanged in the following two situations:

(i) $\alpha_k = \beta_1$ for some $k \neq 1$, and $\alpha_i = \beta_i$ for all $i \neq 1, k$. Note that we could then assume that $\alpha_1 = \beta_k$ since $\alpha_1 \cdots \alpha_n$ and $\beta_1 \cdots \beta_n$ are in the same square class.

(ii) $\alpha_1 = \beta_1$.

For a fixed h,

$$\begin{aligned} \prod_{i \leq j} (\alpha_i, \alpha_j) &= \prod_{h \leq j} (\alpha_h, \alpha_j) \prod_{i < h} (\alpha_i, \alpha_h) \prod_{i \leq j; i,j \neq h} (\alpha_i, \alpha_j) \\ &= (\alpha_h, d(V)) \prod_{i \leq j; i,j \neq h} (\alpha_i, \alpha_j). \end{aligned}$$

In case (i), we have

$$\begin{aligned} \prod_{i \leq j} (\alpha_i, \alpha_j) &= (\alpha_1, d(V)) \prod_{1 < i \leq j} (\alpha_i, \alpha_j) \\ &= (\alpha_1, d(V))(\alpha_k, \alpha_1 d(V)) \prod_{i \leq j; i,j \neq 1,k} (\alpha_i, \alpha_j) \\ &= (\alpha_1 \alpha_k, d(V))(\alpha_k, \alpha_1) \prod_{i \leq j; i,j \neq 1,k} (\alpha_i, \alpha_j) \\ &= (\beta_1 \beta_k, d(V))(\beta_k, \beta_1) \prod_{i \leq j; i,j \neq 1,k} (\beta_i, \beta_j) \\ &= \prod_{i \leq j} (\beta_i, \beta_j) \end{aligned}$$

In case (ii), if $\alpha_1 = \beta_1$, then

$$\prod_{i \leq j} (\alpha_i, \alpha_j) = (\alpha_1, d(V)) \prod_{1 < i \leq j} (\alpha_i, \alpha_j) = (\alpha_1, d(V)) S(\langle \alpha_2, \ldots, \alpha_n \rangle).$$

Witt's Cancellation Theorem implies that $\langle \alpha_2, \ldots, \alpha_n \rangle$ is isometric to $\langle \beta_2, \ldots, \beta_n \rangle$. Therefore, case (ii) can be completed by an induction on $\dim(V)$.

Proof of the claim Write $v_1 = a_1 u_1 + \cdots + a_m u_m$, where $a_i \in F$ and $a_m \neq 0$, and define $\nu(\{u_i\}) = m$. Observe that $m = 1$ means that $\{v_i\}$ and $\{u_i\}$ are linked. Therefore, all we need to show is that if $m > 1$, then there exists another orthogonal basis $\{u_i'\}$ such that $\{u_i'\} \sim \{u_i\}$ and $\nu(\{u_i'\}) < m$.

Suppose $a_j = 0$ for some $j < m$. Define $\{u_i'\}$ as follows:

$$u_i' = \begin{cases} u_i & \text{if } i < j, \\ u_{i+1} & \text{if } j \leq i < n, \\ u_j & \text{if } i = n. \end{cases}$$

Then $\{u_i'\}$ and $\{u_i\}$ are linked and $\nu(\{u_i'\}) = m - 1$. Thus we may assume that $a_j \neq 0$ for all $j < m$. If $m \geq 3$, then we may suppose $Q(a_1 u_1 + a_2 u_2) = a_1^2 Q(u_1) + a_2^2 Q(u_2) \neq 0$ since one of

$$Q(a_1 u_1 + a_2 u_2), \quad Q(a_2 u_2 + a_3 u_3), \quad Q(a_1 u_1 + a_3 u_3)$$

is not equal to 0 (if they were all zero, then $Q(u_1) = Q(u_2) = Q(u_3) = 0$ which is impossible). Then we can extend $\{a_1 u_1 + a_2 u_2, u_3, \ldots, u_m\}$ to an orthogonal basis for V that is linked to $\{u_i\}$, and the value of ν for this basis is $m - 1$.

Suppose $m = 2$. Then $\{a_1 u_1 + a_2 u_2, a_2 Q(u_2) u_1 - a_1 Q(u_1) u_2, u_3 \ldots, \}$ is an orthogonal basis whose value of ν is equal to 1, and hence it is linked to $\{v_i\}$. But it is obvious that this basis is also linked to $\{u_i\}$. $\square$.

Suppose that

$$V \cong \langle \alpha_1, \ldots, \alpha_n \rangle.$$

Lemma 2.18 implies that

$$S(V) = \prod_{1 \leq i \leq n} (\alpha_i, \alpha_1 \cdots \alpha_i).$$

For a nontrivial decomposition $V = U \perp W$, we obtain

$$S(V) = S(U) S(W) (d(U), d(W)).$$

For any $\alpha \in F^\times$, we let V^α be the space (V, Q^α) where $Q^\alpha(x) = \alpha Q(x)$ for all $x \in V$. We call V^α the scaling of V by α. The discriminant of V^α is $\alpha^n d(V)$. Also,

$$S(V^\alpha) = (\alpha, (-1)^{n(n+1)/2} d(V)^{n+1}) S(V).$$

3.2 Classification

In this subsection, let p be a prime. The Hilbert symbol over $\mathbb{Q}_p$ is denoted by $(\ ,\ )$. If V is a nondegenerate quadratic space over $\mathbb{Q}_p$, then the Hasse invariant of V is denoted by $S(V)$.

Proposition 3.2 *A nondegenerate ternary space V over $\mathbb{Q}_p$ is isotropic if and only if $S(V) = (-1, -1)$.*

Proof. After a suitable scaling, we may assume that $V \cong \langle a, b, -1\rangle$. Therefore V is isotropic if and only if $(a, b) = 1$. However, $S(V)$ is equal to $(a, b)(-1, -1)$. As a result, V is isotropic if and only if $S(V) = (-1, -1)$.□.

Corollary 3.3 *Let a, b, c be units in $\mathbb{Z}_p^\times$ with $p > 2$. Then $\langle a, b, c\rangle$ is isotropic.*

Proof. The Hasse invariant of $\langle a, b, c\rangle$ is equal to $1 = (-1, -1)$.□

The above corollary is false if $p = 2$. For example, the ternary space $\langle 1, 1, 1\rangle$ is anisotropic over $\mathbb{Q}_2$.

Proposition 3.4 *A nondegenerate quaternary space V over $\mathbb{Q}_p$ is isotropic if and only if one of the following holds:*

(a) $d(V) = 1$ and $S(V) = (-1, -1)$;

(b) $d(V) \neq 1$.

Proof. If V is isotropic, then $V \cong \mathbb{H} \perp W$. Suppose $d(V) = 1$. Then $d(W) = -1$ and thus W is also a hyperbolic plane. A computation shows that $S(V) = (-1, -1)$ in this case.

For the converse, we have to show that for an anisotropic quaternary space V, both $d(V) = 1$ and $S(V) = -(-1, -1)$ hold. Suppose $V \cong \langle a, b, c, d\rangle$. Then both $\langle 1, ab, ac, ad\rangle$ and $\langle 1, cd, ad, bd\rangle$ are anisotropic. Suppose that $(x, -ab) = 1$ for some $x \in \mathbb{Q}_p^\times$. Then $\langle x, -ab, -1\rangle$ is isotropic or x is represented by the space $\langle ab, 1\rangle$. Hence x is not represented by $\langle -ac, -ad\rangle$ and so $\langle x, ac, ad\rangle$ is anisotropic. By Proposition 3.2, we see that

$$(x, xcd)(ac, cd)(ad, ad) = -(-1, -1).$$

The ternary space $\langle 1, ac, ad\rangle$ is also anisotropic. Using Proposition 3.2 again we have $(ac, cd)(ad, ad) = -(-1, -1)$ and hence $(x, -cd) = 1$. We thus show:

$$\begin{cases} (x, -ab) = 1 & \Longrightarrow \quad (x, -cd) = 1, \\ (x, -cd) = 1 & \Longrightarrow \quad (x, -ab) = 1. \end{cases}$$

Hence $(x, -ab) = (x, -cd)$ for all $x \in \mathbb{Q}_p^\times$. This implies that $d(V) = abcd$ must be a square. Another consequence is that $S(V^\alpha) = S(V)$ for all $\alpha \in \mathbb{Q}_p^\times$. Therefore

$$\begin{aligned} S(V) &= S(\langle 1, ab, ac, ad\rangle) \\ &= S(\langle ab, ac, ad\rangle) \\ &= -(-1, -1) \end{aligned}$$

since $\langle ab, ac, ad\rangle$ is anisotropic.□

Theorem 3.5 *If the dimension of a quadratic space V over $\mathbb{Q}_p$ is at least 5, then V is isotropic.*

Proof. We may assume that the dimension of V is 5 and that V is nondegenerate. Suppose $V \cong \langle a, b, c, d, e\rangle$, and yet V is anisotropic. Proposition 3.4 implies that the product of any four different elements chosen from $\{a, b, c, d, e\}$ is a square. This implies that $V \cong \langle a, a, a, a, a\rangle$ which is a scaling of $\langle 1, 1, 1, 1, 1\rangle$. So we may assume that $V \cong \langle 1, 1, 1, 1, 1\rangle$. If $p > 2$, then V contains an isotropic subspace isometric to $\langle 1, 1, 1\rangle$. If $p = 2$, then

$$1^2 + 1^2 + 1^2 + 2^2 + \sqrt{-7}^2 = 0.$$

Therefore, V is isotropic. □

Corollary 3.6 *Every nondegenerate quaternary space over $\mathbb{Q}_p$ is universal.*

If two nondegenerate quadratic spaces over $\mathbb{Q}_p$ are isometric, then their dimensions, discriminants, and Hasse invariants are the same. The main theorem in this subsection is that these three invariants determine the isometry class of a quadratic space over $\mathbb{Q}_p$.

Theorem 3.7 *Let V and W be two nondegenerate quadratic spaces over $\mathbb{Q}_p$. Then $V \cong W$ if and only if $\dim(V) = \dim(W)$, $d(V) = d(W)$, and $S(V) = S(W)$.*

Proof. Let the dimension of V be n. If $n = 1$, then the theorem is trivial. If $n = 2$, we may assume that $d(V) = d(W) \neq -1$; otherwise both V and W are isometric to the hyperbolic plane and hence $V \cong W$. Let U be the quaternary space $W \perp V^{-1}$. Then $d(U) = 1$ and $S(U) = (-1, -1)$ by a routine calculation. Therefore, U is isotropic by Proposition 3.4. Since both V and W are anisotropic, we can find nonzero vectors $v \in V$, $w \in W$ such that $Q(v) = Q(w) = a$. Thus

$$V \cong \langle a, ad(V)\rangle \cong W.$$

Suppose now that $n \geq 3$. Let U be the space $W \perp V^{-1}$ whose dimension is at least 6. Therefore, it is isotropic which implies that there is an $a \in \mathbb{Q}_\nu^\times$ which is represented by both V and W. Hence

$$V = \langle a\rangle \perp V_1, \qquad W = \langle a\rangle \perp W_1.$$

Direct computations show that $d(V_1) = d(W_1)$ and $S(V_1) = S(W_1)$. So, an induction argument (on the dimension) would show that V_1 and W_1 are isometric. Therefore, V and W are isometric.□

Corollary 3.8 *If V is an anisotropic quaternary space over $\mathbb{Q}_p$, then*

$$V \cong \langle 1, -\Delta, p, -\Delta p\rangle.$$

Proof. From Proposition 3.4, we have $d(V) = 1$ and $S(V) = -(-1, -1)$. These two conditions are satisfied by $\langle 1, -\Delta, p, -\Delta p\rangle$. Theorem 3.7 implies that such a space must be unique up to isometry.□

4 Quadratic Spaces over $\mathbb{Q}$

4.1 Strong Hasse Principle

Let Ω be the set of all prime numbers and the formal symbol ∞. We call an element in Ω a place of $\mathbb{Q}$; a prime number is called a finite place and ∞ is the infinite place. Let V be a quadratic space. For each $\nu \in \Omega$, let V_ν be the vector space $\mathbb{Q}_\nu \otimes_{\mathbb{Q}} V$ over $\mathbb{Q}_\nu$, where we put $\mathbb{Q}_\infty = \mathbb{R}$. We call V_ν the local completion of V at ν. We identify V as a subset of V_ν via the embedding $v \mapsto 1 \otimes v$.

Let $v_1, \ldots, v_n$ be a basis for V. Define a quadratic map Q_ν on V_ν by

$$Q_\nu(\sum_{i=1}^{n} x_i v_i) := \sum_{i,j=1}^{n} x_i x_j B(v_i, v_j), \qquad x_i \in \mathbb{Q}_\nu \text{ for all } i,$$

where B is the bilinear form on V. It is clear that (V_ν, Q_ν) becomes a quadratic space over $\mathbb{Q}_\nu$. Since Q and Q_ν are essentially the same, we will drop the subscript and use the same Q to denote the quadratic form on V_ν. Note that if A is a symmetric matrix for V, then A is also a symmetric matrix for V_ν. We say that V is isotropic at ν if V_ν is isotropic. The Hasse invariant of V_ν over $\mathbb{Q}_\nu$ will be written as $S_\nu(V)$. In particular, if $V \cong \langle a_1, \ldots, a_n \rangle$, then

$$S_\nu(V) = \prod_{1 \le i \le j \le n} (a_i, a_j)_{\mathbb{Q}_\nu}.$$

Lemma 4.1 *Let V be a nondegenerate quadratic space over $\mathbb{Q}$. Then*

$$\prod_{v \in \Omega} S_\nu(V) = 1.$$

Proof. This follows from the Hilbert Reciprocity Law.□

Theorem 4.2 (Strong Hasse Principle) *A nondegenerate quadratic space V over $\mathbb{Q}$ is isotropic if and only V_ν is isotropic for every $\nu \in \Omega$.*

Proof. The only if part is clear. We prove the converse by an induction on n, the dimension of V. There is nothing to verify when $n = 1$ since all one dimensional nondegenerate space are anisotropic.

Suppose that $n = 2$ and that $V \cong \langle a, b \rangle$. Since V_ν is isotropic, $-ab$ is a square in $\mathbb{Q}_\nu$ for every $\nu \in \Omega$. Hence $-ab$ is a square in $\mathbb{Q}$ and V is isotropic.

When $n = 3$, we scale V so that V represents 1. Hence we can suppose

$$V \cong \langle 1, -a, -b \rangle.$$

Moreover, by multiplying a and b by squares, we may assume that a and b are integers. We handle the problem by induction on $|a| + |b|$. Here $|\ |$ is the usual absolute value on $\mathbb{Q}$. If

$|a| + |b| = 2$, then $|a| = |b| = 1$. Since V_∞ is isotropic, therefore either a or b is positive. As a result, $V \cong \langle 1, 1, -1\rangle$ or $\langle 1, -1, -1\rangle$ and V is isotropic.

Suppose $|a| + |b| > 2$ and $|a| \leq |b|$. Then we must have $|b| \geq 2$. Moreover, by dividing squares if necessary, we may assume that both a and b are squarefree integers. If $a = 1$, then V is obviously isotropic. So we can assume that $a \neq 1$. We claim that the congruence $x^2 \equiv a \bmod b$ is solvable with $x \in \mathbb{Z}$. Up to $\pm$, b is a product of distinct primes. Therefore it suffices to prove the claim for every prime divisor p of b. We just need to look at those p which do not divide a. Moreover, we may solve the congruence over $\mathbb{Z}_p$ instead of $\mathbb{Z}$. Since V_p is isotropic, there exist $x, y, z \in \mathbb{Z}_p$, not all zero, such that $x^2 - ay^2 - bz^2 = 0$. We may assume that one of them is a unit in $\mathbb{Z}_p$. Since $b \not\equiv 0 \bmod p^2$, y must be in $\mathbb{Z}_p^\times$. Then $a \equiv (xy^{-1})^2 \bmod p$ and $xy^{-1} \in \mathbb{Z}_p$.

Now, there exists an integer c such that $c^2 = a + bd$ for some integer d. We can further assume that $|c| \leq |b|/2$. Note that $d \neq 0$ because a is not a square. Then

$$|d| = \frac{|c^2 - a|}{|b|} \leq \frac{|b|}{4} + 1 < |b|$$

by virtue of $|b| \geq 2$. Note that $bd = c^2 - a\,1^2$ which is a norm of the extension $\mathbb{Q}(\sqrt{a})/\mathbb{Q}$. Therefore, bd is also a norm of $F(\sqrt{a})/F$ whenever F is a field extension of $\mathbb{Q}$. This means that b is a norm of $F(\sqrt{a})/F$ if and only if d is.

By the assumption, $\langle 1, -a, -b\rangle$ is isotropic over $\mathbb{Q}_\nu$ and it is equivalent to saying that b is a norm of $\mathbb{Q}_\nu(\sqrt{a})/\mathbb{Q}_\nu$, and hence d is a norm of $\mathbb{Q}_\nu(\sqrt{a})/\mathbb{Q}_\nu$. Apply the induction hypothesis to $\langle 1, -a, -d\rangle$, we find that d is a norm of $\mathbb{Q}(\sqrt{a})/\mathbb{Q}$ and hence b is also a norm of $\mathbb{Q}(\sqrt{a})/\mathbb{Q}$. This means that V is isotropic.

When $n \geq 4$, put

$$V = U \perp W$$

where $U = \langle a_1, a_2\rangle$ and $W = \langle a_3, \ldots, a_n\rangle$. All the a_i can be assumed to be integers. For every $\nu \in \Omega$, V_ν is isotropic. Therefore, there exists $b_\nu \in \mathbb{Q}_\nu^\times$ such that

$$(*) \quad b_\nu \in Q(U_\nu) \cap -Q(W_\nu).$$

Scaling V by -1 if necessary, we can assume that $b_\infty > 0$. Write

$$b_p = c_p p^{e(p)}, \quad c_p \in \mathbb{Z}_p^\times$$

at every finite place p. We need to invoke an analytic result in number theory:

Theorem 4.3 (Dirichlet's Theorem on Primes in an Arithmetic Progression) *Let $m > 0$ and a be relatively prime integers. Then there exist infinite many primes $p \equiv a \bmod m$.*

Let d be the product $2a_1 \cdots a_n$ and let

$$c = \prod_{p|d} p^{e(p)}.$$

For every $p \mid d$, $c_p(cp^{-e(p)})^{-1}$ is in $\mathbb{Z}_p^\times$. Therefore, there is a sufficiently large prime q such that

$$q \equiv c_p(cp^{-e(p)})^{-1} \mod p^3,$$

for all $p \mid d$. If we set $b = qc > 0$, then $b/b_p \equiv 1 \mod p^3$ for $p \mid d$. This implies that $b/b_p \in \mathbb{Z}_p^{\times 2}$ for all $p \mid d$. By $(*)$,

$$(**) \quad b \in Q(U_\nu) \cap -Q(W_\nu)$$

for all $\nu \mid d$ and for $\nu = \infty$. If p is a prime which does not divide qd, then b and all the a_i are in $\mathbb{Z}_p^\times$. Therefore, both $U \perp \langle -b \rangle$ and $W \perp \langle b \rangle$ are isotropic at that p. So $(**)$ holds at all $p \neq q$. We claim that $(**)$ also holds at q. The ternary space $U \perp \langle -b \rangle$ is isotropic at all $p \neq q$. Hence $S_p(U \perp \langle -b \rangle) = (-1,-1)_{\mathbb{Q}_p}$ at all $p \neq q$. It follows from Lemma 4.1 that

$$S_q(U \perp \langle -b \rangle) = \prod_{v \neq q} (-1,-1)_{\mathbb{Q}_\nu} = (-1,-1)_{\mathbb{Q}_q}.$$

Thus $U \perp \langle -b \rangle$ is isotropic at q also. When $n = 4$, $W \perp \langle b \rangle$ is isotropic at q by the same reason. When $n > 4$, then W is already isotropic at q because the dimension of W is at least 3 and each a_i is in $\mathbb{Z}_q^\times$ (note that q is odd by choice). Hence $W \perp \langle b \rangle$ is isotropic at q.

Since the Strong Hasse Principle is proved for ternary spaces, therefore $U \perp \langle -b \rangle$ is isotropic. By induction hypothesis, $W \perp \langle b \rangle$ is also isotropic. Therefore, $b \in Q(U) \cap -Q(W)$ and thus $V = U \perp W$ is isotropic.□

4.2 Weak Hasse Principle

Let a be any number in $\mathbb{Q}$. Since V represents a if and only if $V \perp \langle -a \rangle$ is isotropic, therefore we have

Proposition 4.4 *A nondegenerate quadratic space V over $\mathbb{Q}$ represents $a \in \mathbb{Q}$ if and only if V_ν represents a for every $\nu \in \Omega$.*

Suppose that U is another nondegenerate quadratic space over $\mathbb{Q}$. A necessary condition for $U \cong V$ is that $U_\nu \cong V_\nu$ for every $\nu \in \Omega$. The converse also holds and we are going to prove it by induction on the dimension of U. The case where $\dim(U) = 1$ can be deduced from the last proposition. Suppose now that $\dim(U) > 1$. Let a be an nonzero element in $Q(U)$. Then $a \in Q(U_\nu) = Q(V_\nu)$ for all $\nu \in \Omega$; hence a is represented by V. So we have a decomposition

$$U = \langle a \rangle \perp U', \quad V = \langle a \rangle \perp V'.$$

It follows easily from Witt's Theorem that $U'_\nu \cong V'_\nu$ for all $\nu \in \Omega$, and $V' \cong U'$ by the induction assumption. Thus we have shown the following:

Theorem 4.5 (Weak Hasse Principle) *Let U and V be nondegenerate quadratic spaces over $\mathbb{Q}$. Then U and V are isometric if and only if U_ν and V_ν are isometric for all places ν of $\mathbb{Q}$.*

We have shown that the arithmetic of a quadratic space over $\mathbb{Q}$ (or its equivalent, a quadratic form over $\mathbb{Q}$) is completely determined by the local behavior of the space at every place of $\mathbb{Q}$. Using the earlier results proven for quadratic spaces over $\mathbb{Q}_p$ and $\mathbb{R}$, we obtain the following complete set of isometry class invariants for a nondegenerate quadratic space V over $\mathbb{Q}$:

(i) the dimension $\dim(V)$,

(ii) the discriminant $d(V)$,

(iii) the Hasse invariants $S_p(V)$ at all primes p,

(iv) the positive index $\mathrm{Ind}^+(V_\infty)$.

If $V \cong \langle a_1, \ldots, a_n \rangle$ with $a_1, \ldots, a_n \in \mathbb{Q}^\times$, then there exists a finite set of places S, which contains ∞ and 2, such that each a_i is a unit in $\mathbb{Z}_p$ for any $p \notin S$. Therefore, $S_p(V) = 1$ for each $p \notin S$. So in practice one has to check the Hasse invariants for only finitely many places. This also shows that V_ν is isotropic for almost all ν if $\dim(V) \geq 3$.

There is a version of Theorem 4.5, which is often referred as the Hasse Principle, which concerns general representations of quadratic spaces. Let W and V be nondegenerate quadratic spaces over a field F. We say that W is represented by V if there is an linear map $\sigma : W \to V$ such that $Q(\sigma(w)) = Q(w)$ for all $w \in W$. If $\dim(W) = 1$ and w is a basis vector for W with $Q(w) = a$, then W is represented by V if and only if a is represented by V.

Theorem 4.6 (Hasse Principle) *Let W and V be nondegenerate quadratic spaces over $\mathbb{Q}$. Then W is represented by V if and only if W_ν is represented by V_ν for all $\nu \in \Omega$.*

Proof. We proceed by an induction on $\dim(W)$. If $\dim(W) = 1$, this is just Proposition 4.4. Suppose that $\dim(W) \geq 2$. Let a be a nonzero rational number represented by W. Then a is represented by V_ν for all $\nu \in \Omega$. Therefore, a is represented by V. Hence

$$W = \langle a \rangle \perp W', \quad V = \langle a \rangle \perp V'.$$

By Witt's Cancellation Theorem, W'_ν is represented by V'_ν for all $\nu \in \Omega$. By the induction assumption, W' is represented by V' and we are done.□

5 Quadratic Forms over PID

In this section, R denotes a principal ideal domain (PID) and F is the field of fractions of R. We keep the general assumption that the characteristic of F is not 2. In the subsequent sections, R is usually taken to be $\mathbb{Z}$ or $\mathbb{Z}_p$ for some prime p. Unless stated otherwise, (V, Q) is a quadratic space over F.

5.1 Lattices on Quadratic Spaces

Definition 5.1 A subset L of V is called an R-lattice (or simply a lattice) in V if L is a finitely generated R-module. We say that L is a lattice *on* V if it is a lattice in V and $FL = V$.

Let L be a lattice on V. An element $a \in F$ is said to be represented by L if there exists a vector $v \in L$ such that $Q(v) = a$. To see the connection with number theory, let us fix a basis $\{v_1, \ldots, v_n\}$ for L. It is also a basis for V over F. Let $f(x_1, \ldots, x_n)$ be the quadratic form associated with this basis. Then a is represented by L if and only if the diophantine equation

$$f(x_1, \ldots, x_n) = a$$

has a solution $(x_1, \ldots, x_n) \in R^n$, not only in F^n. The fundamental question is still the *representation problem* which asks for an effective determination of $Q(L)$, the set of elements of F represented by L.

Two lattices M and L are *isometric*, written $M \cong L$, if there exists an isometry $\sigma : FM \longrightarrow FL$ such that $\sigma(M) = L$. It is clear that isometric lattices represent the same set of elements of F. Therefore, it is also important to determine, say by means of computable invariants, whether or not two given lattices are isometric. For any lattice L on V, the isometry group of L is the set

$$O(L) = \{\sigma \in O(V) : \sigma(L) = L\}.$$

Definition 5.2 Let L be a lattice on V. A sublattice N of L is called primitive if N is a direct summand of L.

So a sublattice N of a lattice L is primitive if and only if L/N is free. A vector $x \in L$ is said to be primitive in L if the rank one lattice Rx is a primitive sublattice of L.

Lemma 5.3 *Let L be a lattice on V and $x_1, \ldots, x_n$ be a basis for L. Suppose that e is a nonzero vector in L with $e = a_1x_1 + \cdots + a_nx_n$. Then e is primitive in L if and only if* $\gcd(a_1, \ldots, a_n) = 1$.

Proof. If $d := \gcd(a_1, \ldots, a_n)$ is not 1, then $d^{-1}e$ is a vector in L and so L/Re is not free. In other words, e is not primitive in L.

Conversely, suppose that e is not primitive in L. Then L/Re is not free. So there exists $x \in L$, but not in Re, and $n \neq 0$ such that $nx \in Re$. Note that n is not a unit in R. Therefore $nx = me$ for some $m \in R$ and we may assume that $\gcd(m, n) = 1$. Then

$$x = \frac{m}{n}(a_1x_1 + \cdots + a_nx_n)$$

which implies that n divides $\gcd(a_1, \ldots, a_n)$. In particular, $\gcd(a_1, \ldots, a_n) \neq 1$.□

Definition 5.4 A *fractional ideal* of F is a subset of F of the form $(a) = \{ar : r \in R\}$ for some $a \in F^\times$.

Lemma 5.5 *A subset I of F is a fractional ideal of F if and only if I is a nonzero R-module and $\lambda I \subseteq R$ for some nonzero $\lambda \in F$.*

Proof. It is clear that every fractional ideal is a nonzero R-module. If I is the fractional ideal (a), $a \in F^\times$, then $a^{-1}I = R$. Conversely, suppose that $I \subseteq F$ is a nonzero R-module, and that $\lambda I \subseteq R$ for some $\lambda \in F^\times$. Since λI is also a nonzero R-module and $\lambda I \subseteq R$, it is just an ideal of R. Therefore, $\lambda I = (\alpha)$ from some nonzero $\alpha \in R$. Then $I = (\lambda^{-1}\alpha)$.□

Let L be a lattice on V. For any $x \in V$, define the coefficient of x with respect to L to be the set

$$\mathfrak{a}_x = \{t \in F : tx \in L\}.$$

We claim that $\mathfrak{a}_x$ is a fractional ideal of F if $x \neq 0$. It is clear that $\mathfrak{a}_x$ is an R-module in F. Let $u_1, \ldots, u_n$ be a basis for L and write $x = a_1u_1 + \cdots + a_nu_n$ where $a_i \in F$ for all i. There exists a nonzero $r \in R$ such that $ra_i \in R$ for all i. Therefore, $r \in \mathfrak{a}_x$ which shows that $\mathfrak{a}_x$ is nonzero. For each i, write $a_i = \alpha_i\beta_i^{-1}$ where α_i and β_i are in R such that $\gcd(\alpha_i, \beta_i) = 1$. Let g be the gcd of the α_i and ℓ be the lcm of the β_i. Suppose that $t = \alpha\beta^{-1} \in \mathfrak{a}_x$ with $\alpha, \beta \in R$. So, $t\alpha_i\beta_i^{-1} \in R$ for all i. Therefore, we must have

$$\beta \mid \alpha_i \text{ and } \beta_i \mid \alpha \text{ for all } i$$

and hence $\beta \mid g$ and $\ell \mid \alpha$. If we set $\lambda = g\ell^{-1}$, then $\lambda t \in R$, that is, $\lambda\mathfrak{a}_x \subseteq R$.

Lemma 5.6 *Let L be a lattice on V and x be a nonzero vector in V. Then there exists $a \in F^\times$ such that ax is primitive in L.*

Proof. We know that $\mathfrak{a}_x = (a)$ for some $a \in F^\times$. In particular, $ax \in L$. Let $y \in L$ and suppose that there exists an nonzero $t \in R$ such that $ty \in Rax$. Then $ty = rax$ for some $r \in R$, and hence $t^{-1}rax \in L$. This means that $t^{-1}ra \in \mathfrak{a}_x$ and therefore $t^{-1}r \in R$. As a result, $y = t^{-1}rax \in Rax$ and so L/Rax is torsion free.□

We define the radical of a lattice L in V to be the sublattice

$$\operatorname{rad}(L) = \{x \in L : B(x, L) = 0\}.$$

We call L *nondegenerate* if $\operatorname{rad}(L) = 0$. It is easy to see that

$$F\operatorname{rad}(L) = \operatorname{rad}(FL)$$

and

$$\operatorname{rad}(L) = L \cap \operatorname{rad}(FL).$$

In particular, L is nondegenerate if and only if FL is nondegenerate.

Proposition 5.7 *Let L be a lattice in V. Then there exists a nondegenerate lattice K such that $L = K \perp rad(L)$.*

Proof. It is clear that if K exists then it must be nondegenerate. It remains to demonstrate the existence of K. It suffices to show that $\operatorname{rad}(L)$ is a primitive sublattice of L, equivalently,

$L/\mathrm{rad}(L)$ is a torsion free R-module. Suppose that there exists $v \in L$ and $r \in R$ such that $rv \in \mathrm{rad}(L)$. Then $B(rv, L) = 0$ which implies that $r = 0$ or $B(v, L) = 0$, that is, $v \in \mathrm{rad}(L)$.□

Remark 5.8 In the decomposition $L = K \perp \mathrm{rad}(L)$, the lattice K is not unique, but its isometry class is uniquely determine by that of L. As a consequence, if $L' = K' \perp \mathrm{rad}(L')$ is another lattice, then $L \cong L'$ if and only if $K \cong K'$ and $\mathrm{rank}(\mathrm{rad}(L)) = \mathrm{rank}(\mathrm{rad}(L'))$.

Let L be a nondegenerate lattice and $\{v_1, \ldots, v_k\}$ be a basis for L. If A is the symmetric matrix $(B(v_i, v_j))$, we shall write

$$L \cong A.$$

We call such an A a matrix for L. Since FL is a nondegenerate quadratic space, the determinant of the matrix A is nonzero. The discriminant of L, denoted $d(L)$, is the canonical image of $\det(A)$ in $F^\times/R^{\times 2}$. Note that $d(L)$ is well-defined because if A' is the symmetric matrix associated to another basis for L, then

$$A' = T^t A T$$

for some matrix $T \in \mathrm{GL}_k(R)$; thus $\det(A') = \det(A)\det(T)^2 \in \det(A)R^{\times 2}$. Quite often we also consider $d(L)$ as an element of $F^\times$. In this case, $d(L)$ is determined by L up to the multiplication of an element in $R^{\times 2}$.

Let M be a sublattice of L of the same rank. Let $[L/M]$ be the product of the invariant factors of the quotient R-module L/M. It is an ideal of R. By abusing the notation, we also use $[L/M]$ to denote one of its generators.

Proposition 5.9 *Let L be a nondegenerate lattice and M be a sublattice of L of the same rank. Then $d(M) = [L/M]^2 d(L)$.*

Proof. There exist a basis $\{e_1, \ldots, e_k\}$ for L and nonzero elements $a_1, \ldots, a_k$ of R such that $\{a_1 e_1, \ldots, a_k e_k\}$ is a basis for M. Then $[L/M] = a_1 \cdots a_k$, and

$$\begin{aligned} d(M) &= \det(B(a_i e_i, a_j e_j)) \\ &= (a_1 \cdots a_k)^2 \det(B(e_i, e_j)) \\ &= [L/M]^2 d(L) \end{aligned}$$

□

Remark 5.10 If $R = \mathbb{Z}$ or $\mathbb{Z}_p$, the group index $[L : M]$ is a generator of $[L/M]$. In either case, we have $d(M) = [L : M]^2 d(L)$.

Consider a nondegenerate lattice L. The *dual* of L is the set

$$L^\# = \{x \in FL : B(x, L) \subseteq R\}.$$

Let $\{v_1, \ldots, v_n\}$ be a basis for L. As FL is nondegenerate, there exists a basis $\{u_1, \ldots, u_n\}$ for FL such that

$$(B(v_i, u_j)) = I_n.$$

It is easy to see that $\{u_1, \ldots, u_n\}$ is a basis for $L^{\#}$; hence $L^{\#}$ is a lattice on the space FL and $(L^{\#})^{\#} = L$. Moreover, $L^{\#}$ is isomorphic to $\mathrm{Hom}(L, R)$ through the map $x \mapsto B(x, \ )$. Let T be the matrix defined by

$$(v_1, \ldots, v_n) = (u_1, \ldots, u_n)T.$$

Then $I_n = (B(u_i, u_j))T$ and $(B(v_i, v_j)) = T$. Therefore,

$$1 = d(L^{\#}) \det(T), \quad \det(T) = d(L).$$

Thus we have

$$d(L^{\#}) = d(L)^{-1}.$$

If L has a decomposition $L = J \perp K$, then

$$L^{\#} = J^{\#} \perp K^{\#}.$$

Finally, for any nonzero $a \in F$,

$$(aL)^{\#} = a^{-1}L^{\#}.$$

5.2 Modular Lattices

Consider a lattice L in V. The *scale* of L, denoted $\mathfrak{s}(L)$, is the R-module generated by the subset of $B(L, L)$ of F. If $\{e_1, \ldots, e_k\}$ is a basis for L, then

$$\mathfrak{s}(L) \subseteq \sum_{i,j} B(e_i, e_j)R$$

So, either $\mathfrak{s}(L)$ is either a fractional ideal or 0. We define the *norm* $\mathfrak{n}(L)$ to be the R-module generated by the subset $Q(L)$ of F. Since $Q(L) \subseteq B(L, L)$, it follows that $\mathfrak{n}(L)$ is also a fractional ideal or 0. Now, for all $x, y \in L$ we have

$$2B(x, y) = Q(x + y) - Q(x) - Q(y) \in \mathfrak{n}(L).$$

Hence

$$2\mathfrak{s}(L) \subseteq \mathfrak{n}(L) \subseteq \mathfrak{s}(L).$$

If $L = J \perp K$, then it is easily verified that

$$\mathfrak{s}(L) = \mathfrak{s}(J) + \mathfrak{s}(K), \quad \mathfrak{n}(L) = \mathfrak{n}(J) + \mathfrak{n}(K).$$

Let a be a nonzero element of F. Recall that V^a denotes the vector space V provided with a new quadratic map Q^a such that $Q^a(x) = aQ(x)$ for all $x \in V$. We shall use L^a to denote the lattice L when it is regarded as a lattice in V^a. It is easy to see that

$$\mathfrak{s}(L^a) = a\mathfrak{s}(L), \quad \mathfrak{n}(L^a) = a\mathfrak{n}(L), \quad d(L^a) = a^k d(L)$$

where $k = \mathrm{rank}(L)$.

Definition 5.11 A lattice L is called *unimodular* if $\mathfrak{s}(L) \subseteq R$ and $d(L)$ is a unit. It is called (a)*-modular* if $L^{a^{-1}}$ is unimodular.

Lemma 5.12 *Let L be a nondegenerate lattice in V. Then L is (a)-modular if and only if $aL^{\#} = L$. In particular, L is unimodular if and only if $L^{\#} = L$.*

Proof. First suppose that $aL^{\#} = L$. Then

$$B(L, L) = B(L, aL^{\#}) \subseteq (a),$$

and so $\mathfrak{s}(L) \subseteq (a)$. Therefore, $\mathfrak{s}(L^{a^{-1}}) \subseteq R$. Furthermore, if $\operatorname{rank}(L) = k$, then

$$d(L) = d(aL^{\#}) = a^{2k} d(L^{\#}) = a^{2k} d(L)^{-1}.$$

Therefore, $d(L^{a^{-1}}) = a^{-k} d(L)$ is a unit of R.

Now, assume that L is (a)-modular. Then $L^{a^{-1}}$ is unimodular. Therefore, $\mathfrak{s}(L^{a^{-1}}) \subseteq R$ and $d(L^{a^{-1}}) = a^{-k} d(L)$ is a unit. For any $v \in L$, we have

$$a^{-1} B(v, x) \subseteq R, \text{ for all } x \in L.$$

So $a^{-1}v \in L^{\#}$ or $v \in aL^{\#}$; hence $L \subseteq aL^{\#}$. Now,

$$d(aL^{\#}) = a^{2k} d(L^{\#}) = a^{2k} d(L)^{-1} = d(L)^2 d(L)^{-1} = d(L).$$

Thus $L = aL^{\#}$.□

Corollary 5.13 *Suppose that L is an (a)-modular lattice in V. Then*

$$L = \{x \in FL : B(x, L) \subseteq (a)\}.$$

Proof. This is clear because $x \in aL^{\#}$ if and only if $B(a^{-1}x, L) \subseteq R$, which is equivalent to $B(x, L) \subseteq (a)$.□

Proposition 5.14 *Let L be a nondegenerate lattice in V. If K is an (a)-modular sublattice of L with $\mathfrak{s}(L) = (a)$, then K is an orthogonal summand of L.*

Proof. Since K is (a)-modular, it is nondegenerate. Therefore, there is an orthogonal decomposition $FL = FK \perp W$ for some nondegenerate subspace W of FL. We claim that

$$L = K \perp (L \cap W).$$

It suffices to show that $L = K + (L \cap W)$. Let $x \in L$. Write $x = y + z$, where $y \in FK$ and $z \in W$. Then

$$B(y, K) = B(x, K) \subseteq B(L, K) \subseteq \mathfrak{s}(L) = (a).$$

But y is in FK; hence $y \in K$.□

6 Quadratic Forms over $\mathbb{Z}_p$

In this section, (V, Q) is always a quadratic space over $\mathbb{Q}_p$ for some prime p. Every lattice considered here is a $\mathbb{Z}_p$-lattice.

6.1 Classification in Terms of Jordan Decompositions

Lemma 6.1 *(a) If $p > 2$, every nondegenerate $\mathbb{Z}_p$-lattice has an orthogonal basis.*
(b) Every nondegenerate $\mathbb{Z}_2$-lattice is an orthogonal sum of modular sublattices of rank 1 or 2.

Proof. Let L be a nondegenerate lattice on V. If $\mathfrak{s}(L) = \mathfrak{n}(L)$, then there exists a vector $v \in L$ such that $(Q(v)) = \mathfrak{s}(L)$ and by Proposition 5.14 it follows that $\mathbb{Z}_p v$ is an orthogonal summand of L. This proves (a).

If $p = 2$ and $\mathfrak{n}(L) = 2\mathfrak{s}(L)$, then there exist $u, v \in L$ such that $Q(v), Q(u) \in 2\mathfrak{s}(L)$ and $(B(u, v)) = \mathfrak{s}(L)$. The binary submodule $\mathbb{Z}_2 u + \mathbb{Z}_2 v$ is $\mathfrak{s}(L)$-modular and therefore is an orthogonal summand of L. Thus repeating this argument, L is an orthogonal sum of modular sublattices of rank 1 or 2.□

Let L be a nondegenerate lattice on V. We can write

$$L = L_1 \perp \cdots \perp L_t,$$

where L_i is $\mathfrak{s}(L_i)$-modular and $\mathfrak{s}(L_1) \supsetneq \cdots \supsetneq \mathfrak{s}(L_t)$. Such an orthogonal decomposition is called a *Jordan decomposition* of L, and each L_i is a *Jordan component*. The first component L_1 is called the leading component of that Jordan decomposition. In general, a Jordan decomposition is not unique.

For any fractional ideal $\mathfrak{a}$ of $\mathbb{Q}_p$, let

$$L^{\mathfrak{a}} = \{x \in L : B(x, L) \subseteq \mathfrak{a}\}.$$

It is clear that $L^{\mathfrak{a}}$ is a lattice in V.

Lemma 6.2 *Suppose that M is a $\mathfrak{b}$-modular lattice and $\mathfrak{a} \neq \mathfrak{b}$. Then $\mathfrak{s}(M^{\mathfrak{a}}) \subsetneq \mathfrak{a}$.*

Proof. It suffices to prove the case when $\mathfrak{a} \subsetneq \mathfrak{b}$. By scaling the bilinear form, we may assume that M is unimodular. Consequently, $\mathfrak{a} \subsetneq \mathbb{Z}_p$. In particular, $\mathfrak{a} = (p^a)$ with $a \geq 1$. Let

$$M = M_1 \perp \cdots \perp M_\ell \perp M_{\ell+1} \perp \cdots \perp M_k$$

be an orthogonal decomposition of M such that $\operatorname{rank}(M_j)$ is 1 for all $j \leq \ell$ and 2 for all $j > \ell$. Note that $\ell < n$ happens only when $p = 2$. Let $x \in M^{\mathfrak{a}}$ and write $x = x_1 + \cdots + x_k$ where $x_j \in M_j$ for all j.

Suppose that $j \leq \ell$. Let z_j be a basis vector for M_j. Then $Q(z_j) \in \mathbb{Z}_p^\times$. From $B(x_j, z_j) \subseteq B(x, M_j) \subseteq B(x, M) \subseteq \mathfrak{a}$ we see that $x_j \in p^a M_j$.

If $p = 2$ and $j > \ell$, let $\{e_j, f_j\}$ be a basis for M_j such that $Q(e_j), Q(f_j) \in 2\mathbb{Z}_2$ and $B(e_j, f_j) = \gamma \in \mathbb{Z}_2^\times$. Write $x_j = \alpha e_j + \beta f_j$ where $\alpha, \beta \in \mathbb{Z}_2$. Then

$$\begin{aligned} B(x_j, e_j) &= \alpha Q(e_j) + \beta\gamma \in \mathfrak{a} \quad (1) \\ B(x_j, f_j) &= \beta Q(f_j) + \alpha\gamma \in \mathfrak{a} \quad (2) \end{aligned}$$

If $\alpha \notin \mathfrak{a}$, then from (2) $|\alpha|_2 = |\beta Q(f_i)|_2$. This implies that $|\alpha Q(e_j)|_2 = |\beta Q(f_j)Q(e_j)|_2 < |\beta|_2$, and by (1) we have $\beta \in \mathfrak{a}$. But then (2) says that α must be in $\mathfrak{a}$ which is a contradiction. Therefore, $\alpha \in \mathfrak{a}$ and from (1) it follows that β is also in $\mathfrak{a}$.

Finally, the above shows that $M^{\mathfrak{a}} \subseteq p^a M$. Therefore, $\mathfrak{s}(M^{\mathfrak{a}}) \subseteq p^{2a}\mathfrak{s}(M) \subsetneq \mathfrak{a}$.□

Lemma 6.3 *If $L = L_1 \perp \cdots \perp L_i \perp \cdots \perp L_t$ is a Jordan decomposition and $\mathfrak{s}(L_i) = \mathfrak{a}$, then L_i is the leading component of a Jordan decomposition of $L^{\mathfrak{a}}$.*

Proof. For any j, $L_j^{\mathfrak{a}}$ is a subset of $L^{\mathfrak{a}}$. If $x \in L^{\mathfrak{a}}$ and $x = x_1 + \cdots + x_t$ with $x_j \in L_j$ for all j, then

$$B(x_j, L_j) = B(x, L_j) \subseteq \mathfrak{a}.$$

Therefore, $x_j \in L_j^{\mathfrak{a}}$ and hence $L^{\mathfrak{a}} = L_1^{\mathfrak{a}} \perp \cdots \perp L_t^{\mathfrak{a}}$. Lemma 6.2 implies that $\mathfrak{s}(L_j^{\mathfrak{a}}) \subsetneq \mathfrak{a}$ for all $j \neq i$. Therefore, $L^{\mathfrak{a}} = L_i \perp M$ where $\mathfrak{s}(M) \subsetneq \mathfrak{s}(L_i)$. This proves the lemma.□

Theorem 6.4 *Suppose $p > 2$. If $L = L_1 \perp \cdots \perp L_t = K_1 \perp \cdots \perp K_s$ are two Jordan decompositions of L, then $t = s$ and $L_i \cong K_i$ for all i.*

Proof. Suppose $\mathfrak{s}(L_i) = \mathfrak{a}$. Then $L^{\mathfrak{a}}$ is not empty and hence there must be one and only one j such that $\mathfrak{s}(K_j) = \mathfrak{a}$. Similarly, for any K_i, there is a unique L_ℓ with $\mathfrak{s}(L_\ell) = \mathfrak{s}(K_i)$. Therefore, $t = s$ and $\mathfrak{s}(L_i) = \mathfrak{s}(K_i)$ for $1 \leq i \leq t$.

Since L_i and K_i are the leading components of two Jordan decompositions of the lattice $L^{\mathfrak{a}}$, we may assume that $i = 1$ and $\mathfrak{s}(L_1) = \mathfrak{s}(K_1) = \mathbb{Z}_p$ by scaling the quadratic form. The quotient L/pL becomes a quadratic space over the finite field $\mathbb{F} = \mathbb{Z}_p/p\mathbb{Z}_p$. While L_1 and K_1 induce nondegenerate subspaces of L/pL, both $L_2 \perp \cdots \perp L_t$ and $K_2 \perp \cdots \perp K_t$ become the radical of L/pL. Thus $L_1/pL_1 \cong K_1/pK_1$ as quadratic spaces over $\mathbb{F}$, and therefore $\operatorname{rank}(L_1) = \operatorname{rank}(K_1)$ and $d(L_1) = d(K_1)$ in $\mathbb{F}^\times/\mathbb{F}^{\times 2}$. Since $p > 2$, $d(L_1) = d(K_1)$ in $\mathbb{Z}_p^\times/\mathbb{Z}_p^{\times 2}$. Then theorem follows from Corollary 6.20.□

The above theorem does not hold when $p = 2$. For example, consider the $\mathbb{Z}_2$-lattice L with Jordan decomposition

$$L \cong \begin{pmatrix} 2 & 1 \\ 1 & 2 \end{pmatrix} \perp \langle -2 \rangle.$$

Suppose that $\{x, y, z\}$ is a basis which gives the symmetry matrix on the right. Then the vectors $x + z, y + z$ span a sublattices which is isometric to $\mathbb{H}$. Therefore, L has another Jordan decomposition

$$L \cong \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \perp \langle 6 \rangle.$$

Obviously, the leading components of the two Jordan decompositions are not isometric.

Theorem 6.5 *Let $L = L_1 \perp \cdots \perp L_t = K_1 \perp \cdots \perp K_s$ be two Jordan decompositions of a $\mathbb{Z}_2$-lattice L. Then*

(a) $t = s$;

(b) $\mathfrak{s}(L_i) = \mathfrak{s}(K_i)$, *rank*$(L_i) =$ *rank*(K_i) *for* $1 \le i \le t$;

(c) $\mathfrak{n}(L_i) = \mathfrak{n}(K_i)$ *for* $1 \le i \le t$;

(d) $\mathfrak{n}(L_1) = \mathfrak{n}(L)$ *and* $\mathfrak{s}(L_1) = \mathfrak{s}(L)$.

Suppose that $L = L_1 \perp \cdots \perp L_t$ is a Jordan decomposition of a $\mathbb{Z}_2$-lattice L. For $1 \le i \le t$, write $\mathfrak{s}_i = \mathfrak{s}(L_i)$ and $\mathfrak{n}_i = \mathfrak{n}(L_i)$, and set $\mathfrak{u}_i = \mathrm{ord}_2(\mathfrak{n}(L_i))$. The lattice L now has the following set of invariants:

$$t, \mathrm{rank}(L_i), \mathfrak{s}_i, \mathfrak{u}_i, \quad 1 \le i \le t.$$

They are called the Jordan invariants of L. For each i, let $L_{(i)} = L_1 \perp \cdots \perp L_i$.

Theorem 6.6 *Let L and K be lattices on a nondegenerate quadratic space over $\mathbb{Q}_2$. Suppose that L and K have the same Jordan invariants. Let t be the number of Jordan components in a Jordan decomposition of L. Then $L \cong K$ if and only if the following conditions hold for $1 \le i \le t-1$:*

(i) $d(L_{(i)})/d(K_{(i)}) \equiv 1$ *mod* $\mathfrak{n}_i\mathfrak{n}_{i+1}/\mathfrak{s}_i^2$,

(ii) $\mathbb{Q}_2K_{(i)} \perp \langle 2^{u_i}\rangle$ *has a subspace which is isometric to* $\mathbb{Q}_2L_{(i)}$ *when* $\mathfrak{n}_{i+1} \subseteq 4\mathfrak{n}_i$.

6.2 Maximal Lattices

Definition 6.7 Let a be a nonzero element in $\mathbb{Q}_p$. A lattice L on a nondegenerate space V over $\mathbb{Q}_p$ is called (a)-*maximal* if $\mathfrak{n}(L) \subseteq (a)$ and for any lattice M containing L properly, $\mathfrak{n}(M) \nsubseteq (a)$ holds.

Suppose that L is (a)-maximal but $\mathfrak{n}(L) \neq (a)$. If $\mathfrak{n}(L) \subseteq (p^2a)$, then $p^{-1}L$ properly contains L and $\mathfrak{n}(p^{-1}L) \subseteq (a)$. This contradicts the maximality of L. Therefore, for any (a)-maximal lattice L, $\mathfrak{n}(L)$ is either (a) or (pa).

Lemma 6.8 *Let L be a lattice on a nondegenerate quadratic space V of dimension n over $\mathbb{Q}_p$. If $\mathfrak{n}(L) \subseteq (a)$ and $((2a^{-1})^n d(L)) = \mathbb{Z}_p$ or $p\mathbb{Z}_p$, then L is (a)-maximal.*

Proof. Let M be a lattice on V which contains L and $\mathfrak{n}(M) \subseteq (a)$. Then

$$(d(M)) \subseteq \mathfrak{s}(M)^n \subseteq (2^{-1}\mathfrak{n}(M))^n \subseteq (a/2)^n.$$

However, $d(L) = [M : L]^2 d(M)$ which implies that

$$((2a^{-1})^n d(L)) = ([M : L]^2 (2a^{-1})^n d(M)) \subseteq [M : L]^2 \mathbb{Z}_p.$$

Therefore, $[M : L] = 1$ and hence $M = L$.□

Corollary 6.9 *If L is (a)-modular with $\mathfrak{n}(L) = (2a)$, then L is $(2a)$-maximal. In particular, if $p > 2$ then every (a)-modular lattice is (a)-maximal.*

Over $\mathbb{Z}_2$, there are unimodular lattices which are not $\mathbb{Z}_2$-maximal. For example, the $\mathbb{Z}_2$-lattice $N \cong \langle 1, 3\rangle$, with respect to a basis $\{e, f\}$, is unimodular. However it is not $\mathbb{Z}_2$-maximal because it is a sublattice of $M = \mathbb{Z}_2\frac{1}{2}(e+f) + \mathbb{Z}_2\frac{1}{2}(e-f)$ and $\mathfrak{n}(M) = \mathbb{Z}_2$.

Proposition 6.10 *Let V be an anisotropic quadratic space over $\mathbb{Q}_p$. A lattice L on V is (a)-maximal if and only if*

$$L = \{x \in V : Q(x) \in (a)\}.$$

In particular, there is one and only one (a)-maximal lattice on V.

Proof. We first claim that the set $M = \{x \in V : Q(x) \in (a)\}$ is a lattice. It is clear that M is closed under multiplication by $\mathbb{Z}_p$. Let $x, y \in M$. Assume that $2B(x, y) \notin (a)$. Let $t \geq 1$ be an integer such that $(2p^t B(x, y)) = (a)$. Then

$$Q(x)Q(y)B(x, y)^{-2} \in (4p^{2t})$$

and, since we also have $Q(x + y) = Q(x) + Q(y) + 2B(x, y)$, $1 - Q(x)Q(y)B(x, y)^{-2}$ is a square of some element $c \in \mathbb{Z}_p^\times$. This implies that

$$Q(x)Q(y) - B(x, y)^2 = -(cB(x, y))^2 \neq 0,$$

and, as a result, $\mathbb{Q}_p x \oplus \mathbb{Q}_p y$ is a hyperbolic plane which contradicts the assumption on V.

Next we show that M is finitely generated. Fix a lattice K on V with $\mathfrak{n}(K) \subseteq (a)$. Then K must be a subset of M. Let N be a finitely generated $\mathbb{Z}_p$-module such that $K \subseteq N \subseteq M$, and let $\{x_1, \ldots, x_n\}$ be a basis for N. Since $x_i \in M$ for all i, the diagonal entries and the off diagonal entries of the matrix $(B(x_i, x_j))$ are in (a) and $(\frac{a}{2})$ respectively. In particular, $\det(B(x_i, x_j)) \in (\frac{a}{2})^n$ and hence

$$\mathbb{Z}_p \supseteq ([N : K]^2) = (d(K)\, \det(B(x_i, x_j))^{-1}) \supseteq (d(K)) \left(\frac{a}{2}\right)^{-n}.$$

This implies that $[N : K]$ is bounded, and M must be finitely generated.

It is clear by now that M is an (a)-maximal lattice. If L is an (a)-maximal lattice on V, then $L \subseteq M$. But $\mathfrak{n}(M)$ is clearly contained in (a). Therefore, $L = M$. □

Lemma 6.11 *Let L be a lattice on the hyperbolic plane. The following three conditions are equivalent:*

(i) $L \cong \begin{pmatrix} 0 & c \\ c & 0 \end{pmatrix}$;

(ii) *L is (c)-modular and $\mathfrak{n}(L) \subseteq (2c)$;*

(iii) *L is $(2c)$-maximal.*

Proof. $(i) \Longrightarrow (ii)$ is obvious, and $(ii) \Longrightarrow (iii)$ follows from Corollary 6.9 by putting $a = 2c$. For $(iii) \Longrightarrow (i)$, let $\{x, y\}$ be a basis for L such that $Q(x) = 0$. Write $B(x, y) = a$ and $Q(y) = b$ for some $a, b \in \mathbb{Q}_p$. Then

$$a \in \mathfrak{s}(L) \subseteq 2^{-1}\mathfrak{n}(L) \subseteq (c), \text{ and } b \in \mathfrak{n}(L).$$

We claim that $(a) = (c)$. If not, then $a \in (cp)$ and for any $\alpha, \beta \in \mathbb{Z}_p$,

$$Q(\alpha p^{-1}x + \beta y) = 2\alpha\beta p^{-1}a + \beta^2 b \in (2c).$$

Therefore, the lattice $\mathbb{Z}_p p^{-1}x + \mathbb{Z}_p y$ contains L properly and its norm is contained in $(2c)$. This contradicts the maximality of L.

Now, write $c = a\epsilon$ for some $\epsilon \in \mathbb{Z}_p^\times$. Then $\{\epsilon x, -b(2a)^{-1}x + y\}$ is a basis for L whose associated symmetric matrix is $\begin{pmatrix} 0 & c \\ c & 0 \end{pmatrix}$.□

Theorem 6.12 *Let V be a nondegenerate isotropic quadratic space over $\mathbb{Q}_p$, and let L and K be (a)-maximal and (b)-maximal, respectively, lattices on V. Then there exists a splitting $V = U \perp W$ in which U is a hyperbolic plane and*

$$L = (L \cap U) \perp (L \cap W), \quad K = (K \cap U) \perp (K \cap W).$$

Proof. For any isotropic vector x of V, let $\mathfrak{a}_x$ be the coefficient of x with respect to L, that is,

$$\mathfrak{a}_x = \{t \in \mathbb{Q}_p : tx \in L\}.$$

It has been shown that $\mathfrak{a}_x$ is a fractional ideal. We let $\mathfrak{b}_x$ be the coefficient of x with respect to K. Now $\alpha K \subseteq L$ for some nonzero α in $\mathbb{Q}_p$. Therefore, $\mathfrak{r}_x := \mathfrak{b}_x/\mathfrak{a}_x$ is inside (α^{-1}); hence we can pick an isotropic vector x in V for which $\mathfrak{r}_x$ is maximal among all the coefficients of the isotropic vectors in V. For our convenience, we let ℓ and k be generators of $\mathfrak{a}_x$ and $\mathfrak{b}_x$ respectively. In particular, ℓx and kx are basis vectors of L and K respectively.

Note that

$$B(\ell x, L) \subseteq \mathfrak{s}(L) \subseteq 2^{-1}\mathfrak{n}(L) \subseteq (a/2).$$

We claim that $B(\ell x, L) = (a/2)$. If not, then $B(\ell x, L) \subseteq (pa/2)$. So, for any $v \in L$,

$$Q(v + p^{-1}\ell x) = Q(v) + 2p^{-1}B(v, \ell x) \subseteq (a).$$

This implies that the norm of the lattice $L + \mathbb{Z}_p p^{-1}\ell x$ is contained in (a). But $L \subsetneqq L + \mathbb{Z}_p p^{-1}\ell x$ and this contradicts the maximality of L.

Now, let $w \in L$ such that $B(\ell x, w) = a/2$. Put $y = w - a^{-1}Q(w)\ell x \in L$. Then

$$\mathbb{Z}_p \ell x + \mathbb{Z}_p y \cong \begin{pmatrix} 0 & a/2 \\ a/2 & 0 \end{pmatrix}.$$

So, $\mathbb{Z}_p\ell x + \mathbb{Z}_p y$ is an $(a/2)$-modular lattice on a hyperbolic plane. Since $\mathfrak{s}(L) \subseteq (a/2)$, $\mathbb{Z}_p\ell x + \mathbb{Z}_p y$ must be an orthogonal summand of L.

Let k' be a generator of $\mathfrak{b}_y$. Then $\mathbb{Z}_p kx + \mathbb{Z}_p k'y \subseteq K$ and so $kk'/\ell \in (b/a)$, that is,

$$\mathfrak{r}_x\mathfrak{r}_y \subseteq (b/a).$$

As is done in the last paragraph, there exists isotropic vector $z \in K$ such that $\mathbb{Z}_p z + \mathbb{Z}_p k'y$ splits K and $B(z, k'y) = b/2$. Let ℓ' be a generator of $\mathfrak{a}_z$. Then $\mathbb{Z}_p\ell' z + \mathbb{Z}_p y \subseteq L$ and so $\ell' b/k' \in (a)$, that is,

$$(b/a) \subseteq \mathfrak{r}_z\mathfrak{r}_y.$$

But $\mathfrak{r}_x$ is chosen to be maximal. Therefore,

$$\mathfrak{r}_x\mathfrak{r}_y = (b/a)$$

which implies that the scale of $\mathbb{Z}_p kx + \mathbb{Z}_p k'y$ is precisely $(b/2)$. Hence $\mathbb{Z}_p kx + \mathbb{Z}_p k'y$ splits K. Thus $U = \mathbb{Q}_p x + \mathbb{Q}_p y$ gives the desired splitting of V.□

Corollary 6.13 *Let L be an (a)-maximal lattice on a nondegenerate quadratic space V over $\mathbb{Q}_p$. Then*

$$L \cong \begin{pmatrix} 0 & a/2 \\ a/2 & 0 \end{pmatrix}^m \perp L_0$$

where m is the Witt index of V and L_0 is anisotropic. Moreover, the isometry class of L_0 is determined by that of V. As a result, all (a)-maximal lattices on V are isometric.

Proof. By Theorem 6.12, there is a splitting $V = U_1 \perp \cdots \perp U_m \perp V_0$, in which $U_1, \ldots, U_m$ are hyperbolic planes and V_0 is anisotropic, such that

$$L = (L \cap U_1) \perp \cdots \perp (L \cap U_m) \perp (L \cap V_0).$$

It is clear that each $L \cap U_i$ is isometric to $\left(\begin{smallmatrix} 0 & a/2 \\ a/2 & 0 \end{smallmatrix}\right)$. The isometry class of V_0 is uniquely determined by that of V and $L \cap V_0$ is the only (a)-maximal lattice on V_0. Thus the isometry class of $L \cap V_0$ is uniquely determined by that of V.□

Corollary 6.14 *Let L and K be (a)-maximal lattices on a nondegenerate quadratic space over $\mathbb{Q}_p$. Then $[L : L \cap K] = [K : L \cap K]$.*

Proof. By Theorem 6.12, there are hyperbolic pairs x_i, y_i, $1 \le i \le m$, and anisotropic lattice N such that

$$L = \left(\sum_{i=1}^m \mathbb{Z}_p x_i + \mathbb{Z}_p y_i\right) \perp N, \quad K = \left(\sum_{i=1}^m \mathbb{Z}_p a_i x_i + \mathbb{Z}_p a_i^{-1} y_i\right) \perp N,$$

where $a_1, \ldots, a_m$ are nonzero elements in $\mathbb{Z}_p$. Then $L \cap K = (\sum_{i=1}^m \mathbb{Z}_p a_i x_i + \mathbb{Z}_p y_i) \perp N$ and the corollary now follows immediately.□

Lemma 6.15 *Let N be a lattice in a nondegenerate quadratic space V over $\mathbb{Q}_p$. If $\mathfrak{n}(N) \subseteq (a)$, then there exists an (a)-maximal lattice on V which contains N.*

Proof. Let $\{v_1, \ldots, v_m\}$ be a basis for N. Extend it to a basis $\{v_1, \ldots, v_n\}$ for V $(m \leq n)$. Let

$$M = N \oplus \sum_{i=m+1}^{n} \mathbb{Z}_p p^t v_i$$

for some integer t. If t is large enough, then $\mathfrak{n}(M) \subseteq (a)$. Let L be a lattice on V which contains M and $\mathfrak{n}(L) \subseteq (a)$. Then $d(M) = [L : M]^2 d(L)$ and $d(L) \in \mathfrak{s}(L)^n \subseteq (2^{-1}a)^n$. Since $[L : M]$ is an integer, it must be bounded and hence there exists a lattice K which is maximal with respect to inclusion such that $K \supseteq M$ and $\mathfrak{n}(K) \subseteq (a)$. Such K must be an (a)-maximal lattice on V.□

Theorem 6.16 *Let L be an (a)-maximal lattice on a nondegenerate quadratic space V over $\mathbb{Q}_p$. For any $b \in \mathbb{Q}_p^\times$, b is represented by L if b is represented by V and $b \in (a)$.*

Proof. Let v be a vector in V such that $Q(v) = b$. Then the norm of the rank 1 lattice $\mathbb{Z}_p v$ is $(b) \subseteq (a)$. Using the previous lemma we find an (a)-maximal lattice K on V which contains $\mathbb{Z}_p v$. By Theorem 6.12, K is isometric to L and therefore there exists $w \in L$ with $Q(w) = b$.□

Corollary 6.17 *Let L be an (a)-maximal lattice on a nondegenerate quadratic space V of dimension ≥ 4 over $\mathbb{Q}_p$. Then L represents every element in (a).*

Proof. Since $\dim(V) \geq 4$, V is universal and hence it represents all elements in (a). By Theorem 6.16, L represents every element in (a).□

6.3 Modular Lattices over $\mathbb{Z}_p$, $p > 2$

In this subsection we shall present a solution to the classification problem of modular lattices over $\mathbb{Z}_p$ when $p > 2$. Together with Theorem 6.4 they provide a solution to the classification of arbitrary $\mathbb{Z}_p$-lattices when p is odd. By Corollary 6.9, all (a)-modular lattices are (a)-maximal. Therefore, if L is an (a)-modular lattice on a nondegenerate quadratic space over $\mathbb{Q}_p$, then

$$L \cong \begin{pmatrix} 0 & a \\ a & 0 \end{pmatrix}^m \perp L_0$$

where m is the Witt index of the ambient space and L_0 is anisotropic.

Corollary 6.18 *If $p > 2$ and L is an (a)-modular lattice of rank ≥ 3, then $\begin{pmatrix} 0 & a \\ a & 0 \end{pmatrix}$ is an orthogonal summand of L. In particular, L represents all elements in (a).*

Proof. Under the assumption on the rank of L, the ambient quadratic space is isotropic.□

Lemma 6.19 *If $p > 2$ and L is a unimodular lattice of rank 2, then L represents every unit of $\mathbb{Z}_p$.*

Proof. Let Δ be a nonsquare unit of $\mathbb{Z}_p$. By Lemma 6.1, L has an orthogonal basis; hence L is isometric to one of the following binary lattices:

$$\langle 1, 1\rangle, \quad \langle \Delta, \Delta\rangle, \quad \langle 1, \Delta\rangle.$$

It is clear that the last lattice represents all units in $\mathbb{Z}_p$. The first two are isometric because they are $\mathbb{Z}_p$-maximal lattices on isometric quadratic spaces over $\mathbb{Q}_p$; see Theorem 6.12. Therefore, it is enough to consider the case where $L \cong \langle 1, 1\rangle$. Then L is a $\mathbb{Z}_p$-maximal lattice on the space $\langle 1, 1\rangle$, and this space represents all units of $\mathbb{Z}_p$. By Theorem 6.16, L represents all units of $\mathbb{Z}_p$.□

Corollary 6.20 *If $p > 2$, the isometry class of an (a)-modular lattice L is determined by rank(L) and $d(L)$. In particular, if L is unimodular, then*

$$L \cong \langle 1\rangle \perp \cdots \perp \langle 1\rangle \perp \langle d(L)\rangle.$$

Proof. We may assume that L is unimodular. By Corollary 6.18 and Lemma 6.19, L represents 1 if $\operatorname{rank}(L) \geq 2$. Therefore, $L \cong \langle 1\rangle \perp L'$ for some unimodular lattice L'. An induction on the rank of L will complete the proof. □

6.4 Modular Lattices over $\mathbb{Z}_2$

If L is an (a)-modular $\mathbb{Z}_2$-lattice, then $\mathfrak{s}(L) = (a)$ and $\mathfrak{n}(L)$ is either (a) or $(2a)$. We say that L is *improper* if $\mathfrak{n}(L) = (2a)$; proper otherwise. If L is an improper $\mathbb{Z}_2$-modular lattice, then $\mathfrak{n}(L) = (2)$ and we call L *even* unimodular. On the hyperbolic plane $\mathbb{H}$, there is a unique unimodular lattice isometric to $\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$ which we also denote by $\mathbb{H}$.

Lemma 6.21 *Let L be a binary even unimodular $\mathbb{Z}_2$-lattice on a space V.*

(i) If L is isotropic, then $L \cong \mathbb{H}$, $d(L) = -1$, $S(V) = -1$ and $Q(L) = (2)$.

(ii) If L is anisotropic, then $L \cong \begin{pmatrix} 2 & 1 \\ 1 & 2 \end{pmatrix}$, $d(L) = 3$, $S(V) = 1$ and $Q(L) = \{x \in \mathbb{Z}_2 : ord_2(x) \equiv 1 \bmod 2\} \cup \{0\}$.

Proof. The lattice L is (2)-maximal by virtue of Corollary 6.9. The case where L is isotropic can be deduced from Lemma 6.11. Suppose that L is anisotropic. Let x be a basis vector of L. Since L is unimodular, there exists $y \in L = L^{\#}$ such that $B(x, y) = 1$. Then $\{x, y\}$ must be a basis for L and the corresponding symmetric matrix for L is

$$\begin{pmatrix} 2a & 1 \\ 1 & 2b \end{pmatrix}.$$

If a or b is divisible by 2, then $d(L) = 4ab - 1 \equiv -1 \bmod 8$. So L is isotropic which is a contradiction. As a result, both a and b are units and $d(L) = 3$. Moreover, $V \cong \langle 2a, 6a\rangle$ and a direct computation shows that $S(V) = 1$. By the classification of quadratic spaces over $\mathbb{Q}_2$, we see that

$$V \cong \begin{pmatrix} 2 & 1 \\ 1 & 2 \end{pmatrix},$$

which has a unique (2)-maximal lattice isometric to $\begin{pmatrix} 2 & 1 \\ 1 & 2 \end{pmatrix}$. Therefore, $L \cong \begin{pmatrix} 2 & 1 \\ 1 & 2 \end{pmatrix}$.

For any $x \in \mathbb{Q}_2^\times$, $x \in Q(L)$ if and only if $x \in Q(V)$ and $x \in (2)$ by Theorem 6.16. However, $x \in Q(V)$ if and only if $V \perp \langle -x\rangle$ is isotropic, which is equivalent to requiring that its Hasse invariant is equal to $(-1, -1) = -1$. A direct computation shows that the Hasse invariant of $V \perp \langle -x\rangle \cong \langle 2, 6, -x\rangle$ is $(5, -x) = (-1)^{\mathrm{ord}_2(x)}$. This completes the proof of the lemma.□

The last lemma says that there is only one isometry class of anisotropic binary even unimodular $\mathbb{Z}_2$-lattice. Any one of such lattices is denoted by $\mathbb{A}$.

Lemma 6.22 *Suppose that $L \cong \langle \epsilon_1, \epsilon_2, \epsilon_3\rangle$ where $\epsilon_i \in \mathbb{Z}_2^\times$ for all i. Then $L \cong \mathbb{P} \perp \langle \epsilon\rangle$ for some $\epsilon \in \mathbb{Z}_2^\times$ and an even unimodular lattice $\mathbb{P}$. Moreover $\mathbb{P} = \mathbb{H}$ if and only if L is isotropic.*

Proof. Let $\{v_1, v_2, v_3\}$ be an orthogonal basis for L in which $Q(v_i) = \epsilon_i$ for all i. Let $\mathbb{P}$ be the binary lattice spanned by $\{v_1 + v_2, v_2 + v_3\}$. Then

$$\mathbb{P} \cong \begin{pmatrix} \epsilon_1 + \epsilon_2 & \epsilon_2 \\ \epsilon_2 & \epsilon_2 + \epsilon_3 \end{pmatrix}.$$

Since the sum of any two units of $\mathbb{Z}_2$ is divisible by 2, $\mathbb{P}$ is a binary even unimodular lattice and hence $\mathbb{P} = \mathbb{H}$ or $\mathbb{A}$. Moreover, $L \cong \mathbb{P} \perp \langle \epsilon\rangle$ for some $\epsilon \in \mathbb{Z}_2^\times$. Lemma 6.21 implies that L is isotropic if and only if $\mathbb{P} = \mathbb{H}$.□

Theorem 6.23 *Let L be a unimodular $\mathbb{Z}_2$-lattice. If L is even, then $L \cong H$ or $H \perp \mathbb{A}$, where H is an orthogonal sum of some copies of $\mathbb{H}$. If $\mathfrak{n}(L) = \mathbb{Z}_2$, then L has an orthogonal basis.*

Proof. Suppose that L is even unimodular. Then L is (2)-maximal, and by Theorem 6.12 L is an orthogonal sum of binary even unimodular lattices. To complete the proof of this case, it suffices to show that

$$\mathbb{H} \perp \mathbb{H} \cong \mathbb{A} \perp \mathbb{A}.$$

Both lattices are (2)-maximal, and hence we only need to show that their ambient spaces are isometric. This can be done by comparing the Hasse invariants and the discriminants.

Suppose $\mathfrak{n}(L) = \mathbb{Z}_2$. Then $L \cong \langle \epsilon\rangle \perp L'$ for some $\epsilon \in \mathbb{Z}_2^\times$ and a unimodular lattice L'. Therefore it suffices to show that for any binary even unimodular lattice $\mathbb{P}$, $\langle \epsilon\rangle \perp \mathbb{P}$ has an orthogonal basis. This is done by Lemma 6.22.□

Corollary 6.24 *Let L be a unimodular $\mathbb{Z}_2$-lattice with rank ≥ 5. Then $\mathbb{H}$ is an orthogonal summand of L.*

Proof. If L is even unimodular, then Theorem 6.23 implies the assertion. So we may suppose that

$$L \cong \langle \epsilon_1, \ldots, \epsilon_n \rangle$$

where $\epsilon_i \in \mathbb{Z}_2^\times$ for all i. If $\langle \epsilon_1, \epsilon_2, \epsilon_3 \rangle$ is isotropic, then we are done by Lemma 6.22. Otherwise $\langle \epsilon_1, \epsilon_2, \epsilon_3 \rangle \cong \mathbb{A} \perp \langle \alpha \rangle$ for some $\alpha \in \mathbb{Z}_2^\times$. We may then assume that $\langle \alpha, \epsilon_4, \epsilon_5 \rangle \cong \mathbb{A} \perp \langle \beta \rangle$ for some $\beta \in \mathbb{Z}_2^\times$. But then $\mathbb{A} \perp \mathbb{A} \cong \mathbb{H} \perp \mathbb{H}$ is an orthogonal summand of L.□

7 Quadratic Forms over $\mathbb{Z}$

Unless stated otherwise, (V, Q) is always a quadratic space over $\mathbb{Q}$ and all lattices considered in this section are $\mathbb{Z}$-lattices. Since ± 1 are the only units in $\mathbb{Z}$, the discriminant of a nondegenerate lattice in V is well-defined as a rational number.

7.1 Preliminaries

A lattice L in V is called *integral* if $B(L, L) \subseteq \mathbb{Z}$. For an integral lattice L, $L^\#$ contains L and $d(L) = [L^\# : L]^2 d(L^\#)$. Since $d(L^\#) = d(L)^{-1}$, we have

$$[L^\# : L] = |d(L)|.$$

Lemma 7.1 *Let L be an integral lattice on a nondegenerate quadratic space V over $\mathbb{Q}$. There are only finitely many integral lattices on V which contain L.*

Proof. If M is an integral lattice on V which contains L, then $L \subseteq M \subseteq L^\#$. Since $L^\#/L$ is a finite abelian group, there are only finitely many such M.□

Lemma 7.2 *Let L be an integral lattice on a nondegenerate quadratic space V over $\mathbb{Q}$, and N be a nondegenerate sublattice of L. Then $d(N^\perp)$ divides $d(L)d(N)$.*

Proof. Since L is integral, therefore for any $x \in L$ the linear map $z \mapsto B(x, z)$ is a homomorphism from N to $\mathbb{Z}$. But N is nondegenerate; hence there exists a unique $y \in N^\#$ such that $B(x, z) = B(y, z)$ for all $z \in N$. Define a map $\phi : L \longrightarrow N^\#$ by $\phi(x) = y$. Since $\ker(\phi) = N^\perp$ and $\phi(x) = x$ for all $x \in N$, $\phi^{-1}(N) = N \perp N^\perp$ and this implies

$$[L : N \perp N^\perp] = [\phi(L) : N].$$

The right hand side of the above equation certainly divides $[N^\# : N] = |d(N)|$. But $d(N)\, d(N^\perp) = d(L)[L : N \perp N^\perp]^2$. Therefore, $d(N^\perp)$ divides $d(L)d(N)$.□

Theorem 7.3 (Hermite) *Let L be a lattice on a nondegenerate quadratic space V over $\mathbb{Q}$. Let $m(L) = \min\{|Q(x)| : x \in L \setminus \{0\}\}$. Then*

$$m(L) \leq \left(\frac{4}{3}\right)^{\frac{n-1}{2}} |d(L)|^{\frac{1}{n}}.$$

Proof. We may assume that L is anisotropic. The proof will be by induction on $n = \dim(V)$. When $n = 1$, the theorem is obviously true. Assume that the theorem holds for lattices on quadratic spaces of dimension $\leq n-1$. Let $e_1 \in L$ such that $|Q(e_1)| = m(L)$. Then e_1 must be primitive in L. If not, there would be an $x \in L$ and nonzero integer a such that $ax = e_1$. Then

$$|Q(x)| = a^{-2}|Q(e_1)| < |Q(e_1)|$$

which is impossible.

Now, extend $\{e_1\}$ to a basis $\{e_1, e_2, \ldots, e_n\}$ for L. Let $\Phi : V \longrightarrow V$ be the orthogonal projection of V onto $(\mathbb{Q}e_1)^{\perp}$. Then

$$\Phi(x) = x - \frac{B(x, e_1)}{Q(e_1)} e_1, \quad x \in V,$$

and $L' := \Phi(L) = \sum_{i=2}^{n} \mathbb{Z}\Phi(e_i)$. Let $f_1 = e_1$ and $f_i = \Phi(e_i)$ for $i \geq 2$. Then

$$|d(L)| = |\det(B(e_i, e_j))| = |\det(B(f_i, f_j))| = m(L)|d(L')|.$$

For any $x' \in L'$, there exist $t \in [-\frac{1}{2}, \frac{1}{2}]$ and $x \in L$ such that $x' = x + te_1$. Pick $x' \in L'$ so that $|Q(x')| = m(L')$. Then $Q(x) = Q(x') + t^2 Q(e_1)$ and hence $m(L) \leq |Q(x)| \leq m(L') + \frac{1}{4}m(L)$. That is,

$$\begin{aligned} \frac{3}{4}m(L) &\leq m(L') \\ &\leq \left(\frac{4}{3}\right)^{\frac{n-2}{2}} |d(L')|^{\frac{1}{n-1}}, \end{aligned}$$

where the last inequality is from the induction assumption. Using $|d(L)| = m(L)|d(L')|$ we obtain the desired inequality for $m(L)$.□

Theorem 7.4 *For any given positive integer n and nonzero rational number d, there are only finitely many non-isometric lattices of rank n and discriminant d.*

Proof. The theorem is obvious if $n = 1$. Let us assume that the theorem holds for all lattices of rank $\leq n-1$. Let L be a lattice of rank n and discriminant d. By scaling, we could assume that L is integral. Pick $e_1 \in L$ so that $|Q(e_1)| = m(L)$. Construct a sublattice N of L as follows:

- If $m(L) \neq 0$, put $N = \mathbb{Z}e_1$.
- Suppose that $m(L) = 0$. Since L is nondegenerate, the set $B(e_1, L)$ is a nonzero ideal of $\mathbb{Z}$ with a positive generator a. Then $a^2 \mid d$; so there are only finitely many choices for a. Let $e_2 \in L$ such that $B(e_1, e_2) = a$. Note that e_1 must be linearly independent from e_2. Since

$$Q(te_1 + e_2) = Q(e_2) + 2tB(e_1, e_2)$$

and

$$B(e_1, te_1 + e_2) = a,$$

we can choose e_2 so that $|Q(e_2)| \leq a$. We set $N = \mathbb{Z}e_1 + \mathbb{Z}e_2$.

In both cases, there are only finitely many possibilities for the isometry class of N. By Lemma 7.2, $d(N^\perp)$ divides $d(N) \cdot d$. By the induction assumption, there are only finitely many non-isometric lattices with rank and discriminant the same as those for $N^\perp$. Since L contains $N \perp N^\perp$, the theorem is now a consequence of Lemma 7.1.□

7.2 Genus and Class

Let L be a lattice on V. If p is a prime, the p-adic completion of L at p is the $\mathbb{Z}_p$-lattice $L_p = \mathbb{Z}_p \otimes L$. Let K be another lattice on V. By the Invariant Factor Theorem, there exist a basis $x_1, \ldots, x_n$ for L and nonzero rational numbers $r_1, \ldots, r_n$ such that $r_1x_1, \ldots, r_nx_n$ is a basis for K. Consequently, $L_p = K_p$ for almost all primes p. Since the only rational numbers that are p-adic units for every prime p are ± 1, therefore $L = K$ if and only if $L_p = K_p$ for all primes p.

Let $\sigma : V \to V$ be a linear map. For every prime p, σ can be extended uniquely to a linear map from V_p to V_p itself which we again denote by σ. It is not hard to check that $\sigma(L_p) = \sigma(L)_p$.

Suppose that M is a lattice in another quadratic space over $\mathbb{Q}$. A necessary condition for $M \cong L$ is that $M_p \cong L_p$ for all primes p and $\mathbb{R}M \cong V_\infty$. This necessary condition implies that $\mathbb{Q}_\nu M \cong V_\nu$ for all places ν of $\mathbb{Q}$. It follows from the Weak Hasse Principle that there exists an isometry $\mathbb{Q}M \longrightarrow V$ which sends M into V. Therefore, when studying the problem of deciding when two lattices are isometric, it is enough to consider lattices on the same quadratic space.

The *class* of L, written $\mathrm{cls}(L)$, is the set of all lattices M on V such that $M \cong L$. The *genus* of L, denoted by $\mathrm{gen}(L)$, is the set of all lattices M on V such that $M_p \cong L_p$ for all primes p. Note that $\mathbb{R}M \cong V_\infty$ is automatic since M is also on V. It is obvious that if $M \in \mathrm{gen}(L)$, then $d(M) = d(L)$ and $\mathrm{rank}(M) = \mathrm{rank}(L)$.

Theorem 7.5 *The genus of a lattice is partitioned into finitely many classes.*

Proof. This follows from Theorem 7.4.□

Definition 7.6 The number of classes in $\mathrm{gen}(L)$ is called the *class number* of L.

Example 7.7 A lattice L is said to be positive definite if $Q(x) \geq 0$ for all $x \in L$ and $Q(x) = 0$ if and only if $x = 0$. Now, suppose that L is a positive definite unimodular lattice of rank ≤ 5. Then Hermite's theorem implies that L must represent 1. Therefore, $L \cong \langle 1, \ldots, 1 \rangle$. In particular, the class number of L is 1. The same conclusion holds for positive definite unimodular lattices of rank ≤ 7, but the proof requires a much involved argument.

Theorem 7.8 *Let L be a lattice on a quadratic space V over $\mathbb{Q}$. For each prime p, let $M(p)$ be a $\mathbb{Z}_p$-lattice on V_p. Then there is a lattice M on V such that $M_p = M(p)$ for all p if and only if $L_p = M(p)$ for almost all p.*

Proof. We first assume that there exists M on V such that $M_p = M(p)$ for all p. Since we have seen that $M_p = L_p$ for almost all p, therefore $L_p = M(p)$ for almost all p.

Conversely, suppose that $L_p = M(p)$ for almost all p. It suffices to show that given a single prime q, there is a lattice K on V such that

$$K_p = \begin{cases} L_p & \text{if } p \neq q; \\ M(q) & \text{if } p = q. \end{cases}$$

The theorem will follow by successive applications of this special case.

We first prove the following contention: given a prime q, there is a basis $\{y_1, \ldots, y_n\}$ for V such that

$$M(q) = \mathbb{Z}_q y_1 + \cdots + \mathbb{Z}_q y_n.$$

To prove this we fix a basis $\{x_1, \ldots, x_n\}$ for V. By multiplying a suitable power of q to each x_i we may assume that all x_i are in $M(q)$. Suppose

$$M(q) = \mathbb{Z}_q z_1 + \cdots + \mathbb{Z}_q z_n.$$

Write each z_j as a linear combination of the x_i, say

$$z_j = \alpha_{1j} x_1 + \cdots + \alpha_{nj} x_n, \qquad \alpha_{ij} \in \mathbb{Q}_q.$$

Since $\mathbb{Q}$ is dense in $\mathbb{Q}_q$, we can find, for each i and j, a rational number $a_{ij} \in \mathbb{Q}$ such that $|a_{ij} - \alpha_{ij}|_q$ is as small as we wish. If the approximations are good enough we will obtain, by virtue of continuity of multiplication and addition in $\mathbb{Q}_q$,

$$|\det(a_{ij}) - \det(\alpha_{ij})|_q < |\det(\alpha_{ij})|_q.$$

Hence $|\det(a_{ij})|_q = |\det(\alpha_{ij})|_q$. Put $y_j = a_{1j} x_1 + \cdots + a_{nj} x_n$ for $1 \leq j \leq n$. Then

$$y_j - z_j \in \mathbb{Z}_q x_1 + \cdots + \mathbb{Z}_q x_n \subseteq M(q)$$

by our choice the a_{ij}, hence

$$\mathbb{Z}_q y_1 + \cdots + \mathbb{Z}_q y_n \subseteq M(q).$$

If we write $y_j = \sum_i \gamma_{ij} z_i$ with all $\gamma_{ij} \in \mathbb{Z}_q$ we have

$$(\gamma_{ij}) = (\alpha_{ij})^{-1} (a_{ij}),$$

hence $\det(\gamma_{ij})$ is a unit in $\mathbb{Z}_q$. As a result,

$$\mathbb{Z}_q y_1 + \cdots + \mathbb{Z}_q y_n = M(q).$$

Now, we can find a lattice J on V such that $J_q = M(q)$. By the Invariant Factor Theorem of finitely generated modules over PID, there exists a basis $e_1, \ldots, e_n$ for L and rational numbers $r_1, \ldots, r_n$ such that $r_1e_1, \ldots, r_ne_n$ is a basis for J. For any i, let t_i be the q-part of r_i. Then $K = \mathbb{Z}t_1e_1 + \cdots + \mathbb{Z}t_ne_n$ has the desired property.□

A rational number a is said to be represented by the genus of L if V_∞ represents a and L_p represents a for every p. This is a necessary condition for a to be represented by L.

Theorem 7.9 *If a is represented by the genus of L, then a is represented by some lattice in gen(L).*

Proof. We may assume that $a \neq 0$. From the Strong Hasse Principle it follows that a is represented by V. Let $v \in V$ such that $Q(v) = a$. Then for almost all p, $v \in L_p$. If $v \notin L_p$ for a prime p, then Witt's extension theorem implies that there exists an isometry σ_p of V_p such that $\sigma_p(v) \in L_p$. We define a lattice M on V by

$$M_p = \begin{cases} L_p & \text{if } v \in L_p; \\ \sigma_p^{-1}(L_p) & \text{otherwise.} \end{cases}$$

This is well-defined by Theorem 7.8. Then $M \in \mathrm{gen}(L)$ and $v \in M_p$ for all p; so $v \in M$.□

Corollary 7.10 *If L has class number 1, then L represents all rational numbers that are represented by its genus.*

Example 7.11 Consider the $\mathbb{Z}$-lattice $L = \langle 1, 11 \rangle$. The equation

$$3 = \left(\frac{8}{5}\right)^2 + 11\left(\frac{1}{5}\right)^2$$

shows that V_∞ represents 3. Since $5 \in \mathbb{Z}_p^\times$ for all $p \neq 5$, L_p represents 3 for those p; but $L_5 \cong \mathbb{H}$ also represents 3. Therefore 3 is represented by gen(L). But it is obvious that 3 is not represented by L. Incidentally this shows that there are at least two classes in gen(L). One can show that

$$M = \begin{pmatrix} 3 & 1 \\ 1 & 4 \end{pmatrix}$$

is a lattice in gen(L) which represents 3, and that $M \ncong L$.

7.3 Sum of Squares

For any integer $n \geq 1$, let I_n be the lattice corresponding to the sum of n squares, that is,

$$I_n = \langle 1, \ldots, 1 \rangle.$$

When $n \leq 7$, I_n has class number 1. Therefore, the set $Q(I_n)$ is precisely the set of positive integers that are represented by the genus of I_n.

Theorem 7.12 (Euler) *A positive integer m is a sum of two integer squares if and only if $ord_p(m)$ is even for all primes $p \equiv 3$ mod 4.*

Proof. Let p be a prime. We need to determine the set of p-adic integers that is represented by the lattice $\langle 1, 1\rangle$ over $\mathbb{Z}_p$.

(a) $p \equiv 1 \bmod 4$: In this case, -1 is a square in $\mathbb{Z}_p$. Therefore, $\langle 1, 1\rangle \cong \mathbb{H}$ over $\mathbb{Z}_p$ and hence $\langle 1, 1\rangle$ represents every p-adic integer.

(b) $p \equiv 3 \bmod 4$: Since -1 is a nonsquare in $\mathbb{Z}_p$, $\langle 1, 1\rangle$ is a $\mathbb{Z}_p$-maximal lattice on an anisotropic quadratic space over $\mathbb{Q}_p$. It follows from Theorem 6.16 that a nonzero $m \in \mathbb{Z}_p$ is represented by $\langle 1, 1\rangle$ if and only if the space $\langle 1, 1, -m\rangle$ is isotropic, and the latter is the same as saying that $\mathrm{ord}_p(m)$ is even.

(c) $p = 2$: A direct computation shows that a nonzero 2-adic integer m is represented by $\langle 1, 1\rangle$ if and only if $m = 2^\alpha b$, where $b \equiv 1 \bmod 4$.

The theorem is now a consequence of (a), (b) and (c) together.□

Theorem 7.13 (Legendre) *A positive integer m is a sum of three integer squares if and only if m is not of the form $m = 4^a(8b + 7)$, $a, b \in \mathbb{Z}$,*

Proof. Since $\langle 1, 1, 1\rangle$ is unimodular over $\mathbb{Z}_p$ for all odd primes p, by Corollary 6.18 it represents all elements of $\mathbb{Z}_p$. Therefore, it suffices to show that over $\mathbb{Z}_2$, $\langle 1, 1, 1\rangle$ represents all 2-adic integers not of them $4^a(8b + 7)$.

Over $\mathbb{Q}_2$, it is direct to show that the space $\langle 1, 1, 1, -m\rangle$ is anisotropic if and only if $m \in -\mathbb{Q}_2^{\times 2}$. Therefore, the lattice $\langle 1, 1, 1\rangle$ does not represent any integer of the form $4^a(8b + 7)$. But it is clear that $\langle 1, 1, 1\rangle$ represents 1, 3 and 5. Furthermore, since

$$\langle 1, 1, 1\rangle \cong \mathbb{A} \perp \langle 3\rangle$$

by Lemma 6.22, $\langle 1, 1, 1\rangle$ represents all 2-adic integers m with $\mathrm{ord}_2(m) \equiv 1 \bmod 2$; see Lemma 6.21. Consequently, $\langle 1, 1, 1\rangle$ represents all 2-adic integers of the form not of them $4^a(8b + 7)$.□

Theorem 7.14 (Lagrange) *Every positive integer is a sum of four integer squares.*

Proof. By Corollary 6.18 I_4 represents all elements of $\mathbb{Z}_p$ when $p > 2$. Over $\mathbb{Z}_2$, it can be checked directly that I_4 represents all 2-adic integers. Therefore, the genus of I_4 represents all positive integers.□

7.4 Spinor Norms

In this subsection, let (V, Q) be a nondegenerate quadratic space over an arbitrary field F whose characteristic is not 2. If W is a nondegenerate subspace of V, then $V = W \perp W^\perp$. Thus every isometry σ of W can be extended to an isometry of V by defining, $\sigma(x) = x$ for all $x \in W^\perp$. So we can identify $O(W)$ as a subgroup of $O(V)$.

Proposition 7.15 *Every isometry in $O(V)$ is a product of symmetries.*

Proof. The proof is by induction on $n = \dim(V)$. The case $n = 1$ is trivial, so we assume that $n > 1$. Take $\sigma \in O(V)$ and any $v \in V$ such that $Q(v) \neq 0$. Then

$$Q(v - \sigma(v)) + Q(v + \sigma(v)) = 4Q(v) \neq 0.$$

Hence either $Q(v - \sigma(v))$ or $Q(v + \sigma(v))$ is nonzero. In the first case we have

$$\tau_{v-\sigma(v)}(v) = \sigma(v),$$

while in the second case

$$\tau_{v+\sigma(v)}\tau_v(v) = \sigma(v).$$

So in either case there exists $\rho \in O(V)$ which is a product of one or two symmetries such that $\rho(v) = \sigma(v)$. Let W be the orthogonal complement of v. Then $\rho^{-1}\sigma$ is in $O(W)$ and induction hypothesis implies that $\rho^{-1}\sigma$ is a product of symmetries $\tau_{v_1} \cdots \tau_{v_k}$ in $O(W)$. Then

$$\sigma = \rho\tau_{v_1} \cdots \tau_{v_n}$$

which is a product of symmetries in $O(V)$.□

Remark 7.16 The proof of the above proposition can be modified to show that if $p > 2$ and L is a modular $\mathbb{Z}_p$-lattice, then $O(L)$ is also generated by symmetries. For, by scaling the quadratic form suitably we may assume that L is unimodular. Then L contains a vector v with $Q(v) \in \mathbb{Z}_p^\times$. Hence either $Q(v + \sigma(v))$ or $Q(v - \sigma(v))$ is in $\mathbb{Z}_p^\times$. The rest of the proof will go over in nearly verbatim fashion.

If $\sigma \in O(V)$ and $\sigma = \tau_{v_1} \cdots \tau_{v_k}$ for some anisotropic vectors $v_1, \ldots, v_k \in V$, we define the spinor norm of σ to be

$$\theta(\sigma) = Q(v_1) \cdots Q(v_k)F^{\times 2} \in F^\times/F^{\times 2}.$$

Theorem 7.17 *$\theta : O(V) \longrightarrow F^\times/F^{\times 2}$ is a well-defined group homomorphism.*

We are not going to be too rigid in our use of the θ notation, although it will always be clear from the context just what we have in mind. The equality $\theta(\sigma) = a$ with $a \in F^\times$ will often appear; this really means $\theta(\sigma)$ is the canonical image of a in $F^\times/F^{\times 2}$. Occasionally we regard $\theta(\sigma)$ as the full coset $aF^{\times 2}$ taken as a subset of $F^\times$. More generally, if X is a subset of $O(V)$, $\theta(X)$ is the image of X in $F^\times/F^{\times 2}$ under θ; but we shall also regard $\theta(X)$ as the union of the cosets

$$\theta(X) = \bigcup_{\sigma \in X} \theta(\sigma)F^{\times 2}.$$

Lemma 7.18 *If $\sigma \in O(V)$, then $\det(\sigma) = \pm 1$.*

Proof. Let $\mathfrak{B} = \{v_1, \ldots, v_n\}$ be a basis for V and A be the symmetric matrix $(B(v_i, v_j))$. For $1 \leq j \leq n$, write

$$\sigma(v_j) = \sum_{i=1}^{n} t_{ij} v_i.$$

Then the matrix $T = (t_{ij})$ is the matrix representation of σ with respect to the basis $\mathfrak{B}$. If we identify V with the column space F^n, then for any $x, y \in V$,

$$x^t A y = B(x, y) = B(\sigma(x), \sigma(y)) = x^t T^t A T y,$$

hence $A = T^t A T$. Therefore $\det(T) = \pm 1$.□

The *special orthogonal group* of V, denoted by $O^+(V)$, is the set

$$O^+(V) = \{\sigma \in O(V) : \det(\sigma) = 1\}.$$

The kernel of the homomorphism $\theta : O^+(V) \longrightarrow F^\times / F^{\times 2}$ is written as $O'(V)$. It is clear that $O'(V)$ is a normal subgroup of $O(V)$ (not only $O^+(V)$). Note that the groups $O'(V), O^+(V)$, and $O(V)$ are unchanged upon scaling the quadratic map on V by any nonzero element of F.

7.5 Spinor Genus

Suppose that V is a nondegenerate quadratic space over $\mathbb{Q}$. Let L be a lattice on V. The proper class of L is the set $\mathrm{cls}^+(L)$ of all lattices K on V such that $K = \sigma(L)$ for some $\sigma \in O^+(V)$. It is clear that

$$\mathrm{cls}^+(L) \subseteq \mathrm{cls}(L).$$

Each class in $\mathrm{gen}(L)$ breaks into at most two proper classes, and $\mathrm{cls}(L) = \mathrm{cls}^+(L)$ if and only if $O(L)$ contains an isometry of determinant -1.

We can define the proper genus of L to be the set $\mathrm{gen}^+(L)$ of all lattices K on V such that $K_p = \sigma_p(L_p)$ for some $\sigma_p \in O^+(V_p)$ at each p. However, this turns out to be an obsolete definition.

Lemma 7.19 *$gen^+(L) = gen(L)$.*

Proof. It suffices to show that at each p, $O(L_p)$ contains a symmetry. If L_p has an orthogonal basis, say $\{x_1, \ldots, x_n\}$, then it is easy to verify that τ_{x_i} is a symmetry in $O(L_p)$. Therefore we are left with the case when $p = 2$ and L_2 is an orthogonal sum of binary improper modular lattices. Upon scaling the quadratic form on L suitably, we may assume that $L_2 = J \perp K$ with $J \cong \mathbb{H}$ or $\mathbb{A}$. Take any vector $v \in J$ with $Q(v) = 2$. The symmetry τ_v is readily an element in $O(L_2)$.□

Lemma 7.20 *If $\dim(V) \geq 3$, then for any prime p, $\theta(O^+(V_p)) = \mathbb{Q}_p^\times$.*

Proof. If $\dim(V) \geq 4$, then V_p is universal. Hence there is a symmetry with any prescribed spinor norm and the proposition follows immediately.

Suppose that $\dim(V) = 3$. It is known that V_p represents $a \in \mathbb{Q}_p^\times$ if the discriminant of $V_p \perp \langle -a \rangle$ is not 1. So if $d(V_p)$ is a unit, V_p represents all prime elements of $\mathbb{Q}_p$ and at least one unit in $\mathbb{Z}_p$. Now every element of $\mathbb{Q}_p^\times$ is a product of exactly two such elements times a square in $\mathbb{Q}_p^\times$; hence $\theta(O^+(V_p)) = \mathbb{Q}_p^\times$. A similar argument applies when $d(V_p)$ is a prime element.□

A lattice K is in the proper spinor genus of L if there exist $\phi \in O^+(V)$ and $\sigma_p \in O'(V_p)$ at each prime p such that

$$\phi(K_p) = \sigma_p(L_p) \text{ for all } p.$$

The proper spinor genus of L is written as $\mathrm{spn}^+(L)$.

Theorem 7.21 *If a is represented by gen(L) and rank(L) ≥ 4, then a is represented by some lattice in spn$^+(L)$.*

Proof. We may assume that $a \neq 0$ and, by virtue of the Strong Hasse Principle, that V represents a. Let v be a vector in V such that $Q(v) = a$. Let S be the set of primes for which $v \notin L_p$. Note that S is a finite set. For $p \in S$, since L_p represents a, there exists an isometry $\sigma_p \in O(V_p)$ such that $\sigma_p(v) \in L_p$. Since $O(L_p)$ contains a symmetry, we may assume that σ is in $O^+(V_p)$. Let W be the orthogonal complement of v in V. By Lemma 7.20 there exists $\rho_p \in O^+(W_p)$ such that $\theta(\rho_p) = \theta(\sigma_p)$ for each $p \in S$. Define a lattice K on V by

$$K_p = \begin{cases} L_p & \text{if } p \notin S; \\ \rho_p \sigma_p^{-1}(L_p) & \text{if } p \in S. \end{cases}$$

Then $K \in \mathrm{spn}^+(L)$ and $v \in K$.□

8 Strong Approximation

8.1 Norms on orthogonal groups

In this subsection, let p be a prime and V be a nondegenerate quadratic space over $\mathbb{Q}_p$. We shall define a norm $\| \ \|_p$, or simply $\| \ \|$ if no confusion arises, on $O(V)$. Let $\{x_1, \ldots, x_n\}$ be a basis for V. The norm $\| \ \|$ which we are about to define is with respect to the basis $\{x_1, \ldots, x_n\}$ unless stated otherwise. Let M be the $\mathbb{Z}_p$-lattice spanned by this basis.

We first define the norm on V. For any $x \in V$, express it as

$$x = \alpha_1 x_1 + \cdots + \alpha_n x_n, \quad \alpha_i \in \mathbb{Q}_p,$$

and define the norm of x by

$$\|x\| = \max_i |\alpha_i|$$

where $|\ |$ is the p-adic valuation on $\mathbb{Q}_p$. It is not hard to see that $\| \ \|$ is a real-valued function which satisfies the following three properties:

(i) $\|x\| \geq 0$ for all $x \in V$ and $\|x\| = 0 \Leftrightarrow x = 0$;

(ii) $\|\alpha x\| = |\alpha|\|x\|$ for all $\alpha \in \mathbb{Q}_p$ and $x \in V$;

(iii) $\|x + y\| \leq \max\{\|x\|, \|y\|\}$, with equality sign holds when $\|x\| \neq \|y\|$.

Technically speaking, V becomes a normed vector space over $\mathbb{Q}_p$. We can make V into a metric space by defining the distance between two vectors x and y to be $\|x - y\|$. Addition and scalar multiplication will become continuous operations with respect to the topology induced by $\| \ \|$.

Let $\mathcal{L}$ be the vector space of linear operators on V. Consider a typical element $\sigma \in \mathcal{L}$. For each j, let

$$\sigma(x_j) = \sum_{i=1}^{n} \alpha_{ij} x_i.$$

Define the norm of σ to be

$$\|\sigma\| = \max_{i,j} |\alpha_{ij}| = \max_{j} \|\sigma(x_j)\|.$$

Then $\| \ \|$ makes $\mathcal{L}$ into a normed vector space over $\mathbb{Q}_p$. Therefore, $\mathcal{L}$ is a metric space and the distance between σ and τ is $\|\sigma - \tau\|$. The addition and scalar multiplication are continuous operations on $\mathcal{L}$. However, we also have multiplication in $\mathcal{L}$ to consider. We find that

$$\|\sigma(x)\| \leq \|\sigma\|\|x\|$$

for all $\sigma \in \mathcal{L}$ and $x \in V$. This shows that

$$\|\sigma\tau\| \leq \|\sigma\|\|\tau\|$$

for any σ and τ in $\mathcal{L}$. Therefore, multiplication is continuous on $\mathcal{L}$.

For any $\sigma \in O(V)$, we have $\det(\sigma) = \pm 1$. Therefore $\|\sigma\| \geq 1$. Then $\|\sigma\| = 1$ if and only if $\|\sigma\| \leq 1$, and this is equivalent to $\sigma(M) \subseteq M$. Hence $\sigma(M) = M$ since the discriminant of $\sigma(M)$ is the same as that of M. Therefore,

$$O(M) = \{\sigma \in O(V) : \|\sigma\| = 1\}.$$

Let $\{x'_1, \ldots, x'_n\}$ be another basis for V. Let $\| \ \|'$ denote the norm on V and $\mathcal{L}$ defined by this new basis. Suppose that

$$x'_j = \sum_{i=1}^{n} a_{ij} x_i \quad \text{and} \quad x_j = \sum_{i=1}^{n} b_{ij} x'_i.$$

Let $A = \max_{ij} |a_{ij}|$ and $B = \max_{ij} |b_{ij}|$. Then for any $x \in V$ and $\sigma \in \mathcal{L}$,

$$\frac{\|x\|}{A} \leq \|x\|' \leq B\|x\|$$

and

$$\frac{\|\sigma\|}{AB} \leq \|\sigma\|' \leq AB\|\sigma\|.$$

Therefore, $\| \ \|$ and $\| \ \|'$ induce equivalent topology on V and $\mathcal{L}$. Now let K be the $\mathbb{Z}_p$-lattice $\mathbb{Z}_p x_1' + \cdots + \mathbb{Z}_p x_n'$. If $\sigma \in O(V)$ is sufficiently close to 1 under the metric induced by $\| \ \|$, then $\|\sigma - 1\|' < 1$. Each such σ satisfies $\|\sigma\|' = 1$, hence $\sigma(K) = K$.

Now consider a third $\mathbb{Z}_p$-lattice N on V, and suppose that $N = \lambda(M)$ for some $\lambda \in O(V)$. We claim that $\sigma(M) = N$ for all $\sigma \in O(V)$ which are sufficiently close to λ. For, by choosing σ sufficiently close to λ we can make

$$\|\lambda^{-1}\sigma - 1\| \leq \|\lambda^{-1}\| \ \|\sigma - \lambda\|$$

arbitrary small. But all $\lambda^{-1}\sigma$ which are sufficiently close to 1 make $\lambda^{-1}\sigma(M) = M$. Hence all σ which are sufficiently close to λ make $\sigma(M) = \lambda(M) = N$.

8.2 Approximation for Isometries

Let V be a nondegenerate quadratic space over $\mathbb{Q}$. Fix a basis for V and use it to define the norms $\| \ \|_p$ on $O(V_p)$ for all primes p. The following Strong Approximation Theorem is due to Eichler.

Theorem 8.1 (Strong Approximation for $O'(V)$) *Let V be a nondegenerate quadratic space over $\mathbb{Q}$ with $\dim(V) \geq 3$. Suppose that V_ν is isotropic for some place ν (ν could be ∞ or a prime). Let S be a finite set of primes with $\nu \notin S$. For any $\epsilon > 0$ and any given family $\{\sigma_p \in O'(V_p) : p \in S\}$, there is an isometry $\sigma \in O'(V)$ such that*

(i) $\|\sigma - \sigma_p\|_p < \epsilon$ *for all* $p \in S$;

(ii) $\|\sigma\|_p = 1$ *for all* $p \notin S \cup \{\nu\}$.

A quadratic space (V, Q) over $\mathbb{Q}$ is called *indefinite* if V_∞ is an indefinite quadratic space over $\mathbb{R}$. This implies that Q takes on both positive and negative rational numbers. The follow theorem is a consequence of the Strong Approximation Theorem.

Theorem 8.2 *Let L be a lattice on a nondegenerate quadratic space V over $\mathbb{Q}$. If V is indefinite and $\dim(V) \geq 3$, then $cls^+(L) = spn^+(L)$.*

Proof. Let K be a lattice in $\mathrm{spn}^+(L)$. There exist isometries $\phi \in O^+(V)$ and $\sigma_p \in O'(V_p)$ at each p such that

$$\phi(K_p) = \sigma_p(L_p) \quad \text{for all primes } p.$$

Let T be the set $\{p : \phi(K_p) \neq L_p\}$, which is a finite set. Let S be the set of primes p for which $p \notin T$ and L_p is not the $\mathbb{Z}_p$-lattice spanned by the basis for V that defines $\| \ \|_p$. Note that S is also a finite set. By the Strong Approximation Theorem, there exists $\sigma \in O'(V)$ such that

(i) for all $p \notin T \cup S$, $\|\sigma\|_p = 1$;

(ii) for all $p \in T$, σ and σ_p are sufficiently close so that $\sigma(L_p) = \sigma_p(L_p)$;

(iii) for all $p \in S$, σ and 1_{V_p} are sufficient close so that $\sigma(L_p) = L_p$.

For any $p \notin T$, $\sigma(L_p) = L_p = \phi(K_p)$. For any $p \in T$, $\sigma(L_p) = \sigma_p(L_p) = \phi(K_p)$. As a result, $\sigma(L_p) = \phi(K_p)$ for all p and hence $K = \phi^{-1}\sigma(L)$. In particular, K is in $\mathrm{cls}^+(L)$.□

Corollary 8.3 *Let L be a lattice on an indefinite quadratic space of dimension ≥ 4 over $\mathbb{Q}$. If a is represented by gen(L), then a is represented by L.*

Proof. This follows from Theorems 7.21 and 8.2.□

Corollary 8.3 does not hold for ternary lattices. For example, let L be the $\mathbb{Z}$-lattice corresponding to the quadratic form $-9x^2 + 2xy + 7y^2 + 2z^2$. In terms of symmetric matrix

$$L \cong \begin{pmatrix} -9 & 1 & 0 \\ 1 & 7 & 0 \\ 0 & 0 & 2 \end{pmatrix}.$$

Since $d(L) = -2^7$, L_p is unimodular for all primes $p \geq 3$. In particular, L_p represents 1 for all $p \geq 3$. Over $\mathbb{Z}_2$, -9 is -1 times a square of a unit. Therefore, L_2 also represents 1. This means that gen(L) represents 1. We claim that L does not represent 1. The following elementary proof is due to D. Zagier.

Assume on the contrary that L represents 1, i.e. there exist integers x, y, z such that

$$-9x^2 + 2xy + 7y^2 + 2z^2 = 1.$$

We may rewrite this equation as

$$2z^2 - 1 = (x - y)^2 + 8(x - y)(x + y).$$

The left hand side is odd; hence $(x - y)$ and hence $x + y$ as well are odd. This shows that the right hand side is congruent to 1 mod 8, and thus z is odd and then $2z^2 - 1 \equiv 1 \bmod 16$. But $8(x - y)(x + y) \equiv 8 \bmod 16$. If follows that $(x - y)^2 \equiv 9 \bmod 16$ and hence

$$(x - y) \equiv \pm 3 \bmod 8.$$

In particular, $(x - y)$, and $2z^2 - 1$ as well, has a prime factor $p \equiv \pm 3 \bmod 8$. On the other hand, if such p divides $2z^2 - 1$, then 2 is a square mod p and it follows that $p \equiv \pm 1 \bmod 8$ which is a contradiction.

Here is another consequence of the Strong Approximation Theorem. Its proof is similar to that of Theorem 8.2

Theorem 8.4 *Let L be a $\mathbb{Z}$-lattice on a nondegenerate quadratic space V over $\mathbb{Q}$, and q be a prime for which V_q is isotropic. If $\dim(V) \geq 3$, then $\mathbb{Z}[1/q]L \cong \mathbb{Z}[1/q]M$ for any $M \in spn^+(L)$.*

Suppose that V is an indefinite quadratic space over $\mathbb{Q}$. Let L be a $\mathbb{Z}$-lattice on V and let M be a $\mathbb{Z}$-lattice in gen(L). Let T be a finite set of primes such that $L_p = M_p$

for all $p \notin T$. For each $p \in T$, let $\sigma_p \in O^+(V_p)$ such that $\sigma_p(M_p) = L_p$. If the Strong Approximation Theorem held for $O^+(V)$, then there would be an isometry $\sigma \in O^+(V)$ such that $\sigma(M_p) = \sigma_p(M_p)$ for all $p \in T$ and that $\sigma(M_p) = M_p$ for all $p \notin T$. Then $\sigma(M) = L$ and this means that $\mathrm{gen}(L)$ has only one class. But from the class number formula obtained in the next section we know that there exists indefinite $\mathbb{Z}$-lattice whose class number is not 1. Therefore, the Strong Approximation Theorem does not hold for $O^+(V)$. However, there is a weak approximation for $O^+(V)$.

Theorem 8.5 (Weak Approximation for $O^+(V)$) *Let V be a nondegenerate quadratic space over $\mathbb{Q}$ and let T be a finite set of primes on $\mathbb{Q}$. Suppose that σ_p is given in $O^+(V_p)$ at each $p \in T$. Then for every $\epsilon > 0$, there is a $\sigma \in O^+(V)$ such that*

$$\|\sigma - \sigma_p\|_p < \epsilon \text{ for all } p \in T.$$

Proof. For each $p \in T$, we may write

$$\sigma_p = \tau_{x_1(p)} \cdots \tau_{x_m(p)}$$

where every $x_{i(p)}$ is in V_p. Since m must be even and all symmetries have order 2, we may suppose that m is independent of $p \in T$. By Chinese Remainder Theorem, we can choose $x_i \in V$ such that x_i and $x_{i(p)}$ are sufficiently close in V_p for $p \in T$. Then τ_{x_i} and $\tau_{x_{i(p)}}$ are sufficiently close so that σ_p and $\sigma := \tau_{x_1} \cdots \tau_{x_m}$ are, for $p \in T$.□

Corollary 8.6 *Let L be a $\mathbb{Z}$-lattice on a nondegenerate quadratic space V over $\mathbb{Q}$, and let T be a finite set of primes. For every $\mathbb{Z}$-lattice M in gen(L), there exists $K \in cls^+(M)$ such that $K_p = L_p$ for all $p \in T$.*

Proof. For each $p \in T$, let $\sigma_p \in O^+(V_p)$ such that $\sigma_p(M_p) = L_p$. It follows from the Weak Approximation Theorem for $O^+(V)$ that there is a $\sigma \in O^+(V)$ satisfying $\sigma(M_p) = \sigma_p(M_p)$. Let $K = \sigma(M)$. Then $K_p = L_p$ for all $p \in T$.□

Finally, we can improve Theorem 8.3 to representations with approximation property.

Theorem 8.7 *Let L be a $\mathbb{Z}$-lattice on an indefinite quadratic space V over $\mathbb{Q}$ with $\dim(V) \geq 4$ and T be a finite set of primes. Let a be a nonzero rational number which is represented by gen(L), and suppose that for each $p \in T$ there is a $v_p \in L_p$ with $Q(v_p) = a$. Then for each $\epsilon > 0$, there exists $v \in L$ with $Q(v) = a$ and*

$$\|v - v_p\|_p < \epsilon \quad \forall\, p \in T,$$

where all $\| \ \|_p$ are defined by L

Proof. Since a is represented by $\mathrm{gen}(L)$, there exists $z \in V$ such that $Q(z) = a$. We enlarge T so that

(a) T contains all the prime divisors of $2d(L)$, and

(b) $z \in L_p$ for all $p \notin T$.

It suffices to prove the theorem for this enlarged T.

By Witt's theorem, there is an isometry $\rho_p \in O^+(V_p)$ at each $p \in T$ such that $\rho_p(z) = v_p$. Let W be the orthogonal complement of $\mathbb{Q}z$ in V. Since $\dim(W) \geq 3$, there exists $\tau_p \in O^+(W_p)$ at each $p \in T$ such that $\theta(\tau_p) = \theta(\rho_p)$. Let $\sigma_p = \rho_p\tau_p$. Then $\sigma_p \in O'(V_p)$ for all $p \in T$. By the Strong Approximation for $O'(V)$, there exists $\sigma \in O'(V)$ such that

$$\|\sigma - \sigma_p\|_p < \frac{\epsilon}{\|z\|_p} \quad \forall\, p \in T$$

and

$$\|\sigma\|_p = 1 \quad \forall\, p \notin T.$$

Let v be $\sigma(z)$. It is clear that $\|v - v_p\|_p < \epsilon$ for each $p \in T$. Since $v_p \in L_p$ and $\epsilon < 1$, $v \in L_p$ as well. For $p \notin T$, $\sigma \in O'(L_p)$ and $z \in L_p$. So $v = \sigma(z) \in L_p$. Consequently, $v \in L_p$ for all primes p; hence $v \in L$.□

9 Adelic Theory of Spinor Genus

In this section, let V be a nondegenerate quadratic space over $\mathbb{Q}$ and L be a $\mathbb{Z}$-lattice on V. We shall provide a formula for the number of proper spinor genera in $\mathrm{gen}(L)$. When V is indefinite, this formula gives the number of proper classes in $\mathrm{gen}(L)$. We also describe a procedure to decide if two given lattices in a given genus are inside the same proper spinor genus.

9.1 Adeles

Let Ω be the set of all places of $\mathbb{Q}$. Fix a basis $\mathfrak{B}$ of V and use it to define all the norms $\|\ \|_p$ on $O(V_p)$. If Σ is an element in the direct product $\prod_{\nu\in\Omega} O^+(V_\nu)$, then Σ_ν will denote its ν-component. The *adelization* of $O^+(V)$ is the set

$$O^+_{\mathbb{A}}(V) = \{\Sigma \in \prod_{\nu\in\Omega} O^+(V_\nu) : \|\Sigma_p\|_p = 1 \text{ for almost all primes } p\ \}.$$

Lemma 9.1 *$O^+_{\mathbb{A}}(V)$ is well-defined, that is, it is independent of the choice of the basis $\mathfrak{B}$.*

Proof. Let L be the lattice spanned by the vectors in $\mathfrak{B}$. Then for a prime p, $\|\Sigma_p\|_p = 1$ if and only if $\Sigma_p(L_p) = L_p$. Now, suppose that $\mathfrak{B}'$ is another basis for V. Let L' be the lattice spanned by the vectors in $\mathfrak{B}'$. Then for almost all p, $L_p = L'_p$. So, if Σ is in $O^+_{\mathbb{A}}(V)$, then

$$\Sigma_p(L'_p) = \Sigma_p(L_p) = L_p = L'_p$$

for almost all primes p.□

An element in $O^+_{\mathbb{A}}(V)$ is called an *adele* of $O^+(V)$. It is clear that $O^+_{\mathbb{A}}(V)$ is a subgroup of the direct product. The set of all elements $\Sigma \in O^+_{\mathbb{A}}(V)$ with the property

$$\Sigma_\nu \in O'(V_\nu) \text{ for all } \nu \in \Omega$$

is clearly a subgroup of $O^+_{\mathbb{A}}(V)$. We shall denote this subgroup by $O'_{\mathbb{A}}(V)$. It is evident that $O'_{\mathbb{A}}(V)$ contains the commutator subgroup of $O^+_{\mathbb{A}}(V)$.

Consider a typical element $\sigma \in O^+(V)$. Then σ can be regarded as an element in $O^+(V_\nu)$ for all $\nu \in \Omega$. Let T be the matrix representation of σ with respect to the basis $\mathfrak{B}$. Then the entries of T and $\det(T)$ are units in $\mathbb{Z}_p$ for almost all p. Therefore, $\|\sigma\|_p = 1$ for almost all primes p. Hence we can identify $O^+(V)$ as a subgroup of $O^+_{\mathbb{A}}(V)$ through the diagonal embedding.

For any $\Sigma \in O^+_{\mathbb{A}}(V)$ and any lattice L on V, define the lattice $\Sigma(L)$ by specifying its local completions as

$$\Sigma(L)_p = \Sigma_p(L_p) \text{ for all } p.$$

This definition is meaningful since $\Sigma_p(L_p) = L_p$ for almost all p. Therefore, we have an action of the group $O^+_{\mathbb{A}}(V)$ on the set of lattices on V.

Proposition 9.2 *We have $cls^+(L) = O^+(V)L$, $spn^+(L) = O^+(V)O'_{\mathbb{A}}(V)L$, and $gen(L) = O^+_{\mathbb{A}}(V)L$.*

Proof. We only demonstrate the equality $\mathrm{gen}(L) = O^+_{\mathbb{A}}(V)L$; the other two equalities can be proved in a similar way. It is clear that $\Sigma(L) \in \mathrm{gen}(L)$ for any $\Sigma \in O^+_{\mathbb{A}}(V)$. Suppose that $M \in \mathrm{gen}(L)$. Then for each prime p, there exists $\Sigma_p \in O^+(V_p)$ such that

$$\Sigma_p(L_p) = M_p.$$

Since $L_p = M_p$ for almost all p, therefore, $\|\Sigma_p\|_p = 1$ for almost all p. Let Σ_∞ be any isometry in $O^+(V_\infty)$ and put $\Sigma = (\Sigma_\nu)$. Then $M = \Sigma(L)$.□

The stabilizer of L in $O^+_{\mathbb{A}}(V)$ is the set

$$O^+_{\mathbb{A}}(L) = \{\Sigma \in O^+_{\mathbb{A}}(V) : \Sigma_\nu(L_p) = L_p \text{ for all primes } p\}.$$

9.2 Number of Spinor Genera

Lemma 9.3 *For any $\Sigma \in O^+_{\mathbb{A}}(V)$, we have $\Sigma(spn^+(L)) = spn^+(\Sigma(L))$.*

Proof. Let K be a lattice in $\Sigma(\mathrm{spn}^+(L))$. Then there exist $\phi \in O^+(V)$ and $\sigma_p \in O'(V_p)$ at each p such that

$$K_p = \Sigma_p \phi \sigma_p(L_p) \text{ for all } p.$$

Since $O'(V_p)$ contains the commutator subgroup of $O^+(V_p)$, there exists $\rho_p \in O'(V_p)$ such that

$$\Sigma_p \phi \sigma_p = \rho_p \phi \sigma_p \Sigma_p.$$

However, as $O'(V_p)$ is normal in $O^+(V_p)$, there exists $\tau_p \in O'(V_p)$ such that

$$\rho_p \phi \sigma_p \Sigma_p = \phi \tau_p \sigma_p \Sigma_p.$$

Therefore, $K \in \mathrm{spn}^+(\Sigma(L))$, and hence $\Sigma(\mathrm{spn}^+(L)) \subseteq \mathrm{spn}^+(\Sigma(L))$. The reverse inclusion can be proved in the same fashion.□

If Σ, Λ are elements in $O^+_{\mathbb{A}}(V)$, then the normality of $O'_{\mathbb{A}}(V)$ in $O^+_{\mathbb{A}}(V)$ implies that $\Sigma O'_{\mathbb{A}}(V) = O'_{\mathbb{A}}(V)\Sigma$, and the fact that $O'_{\mathbb{A}}(V)$ contains the commutator subgroup of $O^+_{\mathbb{A}}(V)$ implies that $\Sigma\Lambda O'_{\mathbb{A}}(V) = \Lambda\Sigma O'_{\mathbb{A}}(V)$, hence the set $O'_{\mathbb{A}}(V)\Sigma\Lambda$ is independent of the order of $O'_{\mathbb{A}}(V), \Sigma, \Lambda$. From this it follows that the set $O^+(V)O'_{\mathbb{A}}(V)O^+_{\mathbb{A}}(L)$ is independent of the order of $O^+(V), O'_{\mathbb{A}}(V), O^+_{\mathbb{A}}(L)$, and that this set is actually equal to the group generated by $O^+(V), O'_{\mathbb{A}}(V), O^+_{\mathbb{A}}(L)$, which is a normal subgroup in $O^+_{\mathbb{A}}(V)$.

Proposition 9.4 *The number of proper spinor genera in gen(L) is equal to the index*

$$[O^+_{\mathbb{A}}(V) : O^+(V)O'_{\mathbb{A}}(V)O^+_{\mathbb{A}}(L)].$$

Proof. It is clear that the group $O^+_{\mathbb{A}}(V)$ acts transitively on the set of proper spinor genera in $\mathrm{gen}(L)$ and $O^+(V)O'_{\mathbb{A}}(V)O^+_{\mathbb{A}}(L)$ is contained in the stabilizer of $\mathrm{spn}^+(L)$. Now, suppose that $\Sigma(\mathrm{spn}^+(L)) = \mathrm{spn}^+(\Sigma(L)) = \mathrm{spn}^+(L)$ for some $\Sigma \in O^+_{\mathbb{A}}(V)$. Then $\Sigma(L) \in \mathrm{spn}^+(L)$ and this means that there exist $\phi \in O^+(V)$ and $\sigma_p \in O'(V_p)$ at each p such that

$$\Sigma_p(L_p) = \phi\sigma_p(L_p) \text{ for all } p.$$

Therefore, $\Sigma \in O^+(V)O'_{\mathbb{A}}(V)O^+_{\mathbb{A}}(L)$.□

Corollary 9.5 *The number of proper spinor genera in a given genus is power of 2.*

Proof. At each place ν, the square of any element in $O^+(V_\nu)$ has trivial spinor norm. Therefore, the square of element in $O^+_{\mathbb{A}}(V)$ is in $O'_{\mathbb{A}}(V)$, and hence the exponent of the finite abelian group $O^+_{\mathbb{A}}(V)/O^+(V)O'_{\mathbb{A}}(V)O^+_{\mathbb{A}}(L)$ is 2.□

The set of ideles of $\mathbb{Q}$ is the set

$$J = \{x = (x_\nu) \in \prod_{\nu\in\Omega} \mathbb{Q}_\nu^\times : |x_p|_p = 1 \text{ for almost all } p\ \}.$$

It is clear that J is a group.

Lemma 9.6 *If $p > 2$ and L_p is a unimodular $\mathbb{Z}_p$-lattice of rank ≥ 2, then $\theta(O^+(L_p)) = \mathbb{Z}_p^\times \mathbb{Q}_p^{\times 2}$.*

Proof. By Lemma 6.19, L_p represents all units of $\mathbb{Z}_p$. Therefore, $\theta(O^+(L_p))$ contains $\mathbb{Z}_p^\times \mathbb{Q}_p^{\times 2}$. For the reverse inclusion, we first note that $O^+(L_p)$ is generated by symmetries (see Remark 7.16). Therefore it is enough to show that the spinor norm of any symmetry in $O^+(L_p)$ is a

unit. Take a typical symmetry $\tau_y \in O^+(L_p)$. We may assume that y is primitive in L_p and thus $p^{-1}y \notin L_p$. For any $x \in L_p$,

$$\tau_y(x) = x - \frac{2B(x,y)}{Q(y)}y.$$

Therefore $B(y, L_p) \subseteq Q(y)\mathbb{Z}_p$. But $B(y, L_p) = \mathbb{Z}_p$ because L_p is unimodular. Hence $\theta(\tau_y) = Q(y)\mathbb{Q}_p^{\times 2} \subseteq \mathbb{Z}_p^\times \mathbb{Q}_p^{\times 2}$.□

Corollary 9.7 *Let L be a lattice on V. If $\dim(V) \geq 2$, then for any $\Sigma \in O^+_{\mathbb{A}}(V)$, $\theta(\Sigma_p) \subseteq \mathbb{Z}_p^\times \mathbb{Q}_p^{\times 2}$ for almost all p.*

Proof. This is because L_p is unimodular for almost all p.□

Let Σ be an element in $O^+_{\mathbb{A}}(V)$. If $\mathrm{rank}(L) \geq 3$, then by Corollary 9.7 there exists an $x \in J$ such that $x_\nu \in \theta(\Sigma_\nu)$ for all $\nu \in \Omega$. If y is another element in J which is associated to Σ in this way, then $y \in xJ^2$. Let J_L be the subset of J defined by

$$J_L = \{x = (x_\nu) \in J : x_\nu \in \theta(O^+(L_\nu)) \text{ for all } \nu \in \Omega \}.$$

Then $J^2 \subseteq J_L$, and hence the image of x and y in $J/\mathbb{Q}^\times J_L$ are equal. We therefore have a well-defined homomorphism

$$\theta_{\mathbb{A}} : O^+_{\mathbb{A}}(V) \longrightarrow J/\mathbb{Q}^\times J_L.$$

Theorem 9.8 *If $\mathrm{rank}(L) \geq 3$, then the number of proper spinor genera in $\mathrm{gen}(L)$ is equal to the index $[J : \mathbb{Q}^\times J_L]$.*

Proof. It suffices to show that $\theta_{\mathbb{A}}$ is a surjective homomorphism with $O^+(V)O'_{\mathbb{A}}(V)O^+_{\mathbb{A}}(L)$ as its kernel. Since the definition of $O^+_{\mathbb{A}}(V)$ is independent of the choice of the basis $\mathfrak{B}$ of V, we may very well assume that $\mathfrak{B}$ is in fact a basis for L.

Take a typical element $x \in J$. By considering $-x$ instead if necessary, we may assume that $x_\infty \in \theta(\Sigma_\infty)$ for some $\Sigma_\infty \in O^+(V_\infty)$. For almost all p, x_p is a unit. Since L_p is unimodular for almost all p and $\theta(O^+(L_p))$ contains $\mathbb{Z}_p^\times$ at those p, we can find $\Sigma_p \in O^+(L_p)$ such that $x_p \in \theta(\Sigma_p)$ for almost all p. For the remaining finite number of primes q, there exist $\Sigma_q \in O^+(V_p)$ such that $x_q \in \theta(\Sigma_q)$ because $\dim(V_q) \geq 3$; see Theorem 7.20. Then $\Sigma = (\Sigma_\nu)$ is an element in $O^+_{\mathbb{A}}(V)$ and $\theta_{\mathbb{A}}(\Sigma) = x$.

It is clear that $O^+(V)O'_{\mathbb{A}}(V)O^+_{\mathbb{A}}(L)$ is a part of the kernel of $\theta_{\mathbb{A}}$. Now suppose that $\theta_{\mathbb{A}}(\Sigma) \in \mathbb{Q}^\times J_L$. Let us assume the following statement at this moment:

$$\theta(O^+(V)) = \begin{cases} \{a \in \mathbb{Q}^\times : a > 0\} & \text{if } V_\infty \text{ is anisotropic,} \\ \mathbb{Q}^\times & \text{otherwise.} \end{cases}$$

Then we can take $\sigma \in O^+(V)$ and $\Lambda \in O^+_{\mathbb{A}}(L)$ so that

$$\theta_{\mathbb{A}}(\Sigma\sigma\Lambda) \subseteq J^2.$$

As a result, $\Sigma\sigma\Lambda \in O'_{\mathbb{A}}(V)$ and hence the kernel of $\theta_{\mathbb{A}}$ is $O^+(V)O'_{\mathbb{A}}(V)O^+_{\mathbb{A}}(L)$.□

Proposition 9.9 *If* $\dim(V) \geq 3$*, then*

$$\theta(O^+(V)) = \begin{cases} \{a \in \mathbb{Q}^\times : a > 0\} & \text{if } V_\infty \text{ is anisotropic,} \\ \mathbb{Q}^\times & \text{otherwise.} \end{cases}$$

Proof. Let $a \in \mathbb{Q}^\times$ and suppose that $a > 0$ if V_∞ is anisotropic. If the latter situation arises, then by multiplying -1 to the quadratic form if necessary, we may assume that V_∞ is negative definite.

Let S be the set of primes for which V_p is anisotropic. Note that S is a finite set. If $p \in S$, we take $b_p \in \mathbb{Q}_p^\times$ such that both $b_p d(V)$ and $ab_p d(V)$ are not squares. Using the Chinese Remainder Theorem we can find $0 < b \in \mathbb{Q}^\times$ such that b and b_p are sufficiently close for all $p \in S$. If S is empty, then we set $b = 1$. Then both $V_v \perp \langle b \rangle$ and $V_v \perp \langle ab \rangle$ are isotropic for every place v of $\mathbb{Q}$. From the Strong Hasse principle it follows that both $-b$ and $-ab$ are represented by V. Let $x, y \in V$ such that $Q(x) = -b$ and $Q(y) = -ab$. Then $\theta(\tau_x \tau_y) = Q(x)Q(y) \in a\mathbb{Q}^{\times 2}$. Thus

$$\theta(O^+(V)) \supseteq \begin{cases} \{a \in \mathbb{Q}^\times : a > 0\} & \text{if } V_\infty \text{ is anisotropic,} \\ \mathbb{Q}^\times & \text{otherwise.} \end{cases}$$

The reverse inclusion is obvious.□

Corollary 9.10 *Let* L *be a nondegenerate* $\mathbb{Z}$*-lattice. If rank*$(L) \geq 3$ *and* $\theta(O^+(L_p)) \supseteq \mathbb{Z}_p^\times$ *for all primes* p*, then gen*$(L) = spn^+(L)$*.*

Proof. It suffices to show that the quotient group $J/\mathbb{Q}^\times J_L$ is trivial. Take a typical element $x \in J$. By multiplying -1 if necessary, we could assume that $x_\infty > 0$ and hence $x_\infty \in \theta(O^+(V_\infty))$. Let S be the set of primes p for which $x_p \notin \mathbb{Z}_p^\times \mathbb{Q}_p^{\times 2}$. Then there exists a rational number $a > 0$ such that $\mathrm{ord}_p(a) = 0$ for all $p \notin S$ and $ax_p \in \mathbb{Z}_p^\times$. As a result, $ax \in J_L$ and hence $x \in \mathbb{Q}^\times J_L$.□

Example 9.11 Let L be a nondegenerate unimodular $\mathbb{Z}$-lattice of rank ≥ 3. If $p > 2$, then $\theta(O^+(L_p)) = \mathbb{Z}_p^\times \mathbb{Q}_p^{\times 2}$ since L_p is unimodular. At $p = 2$, $\mathbb{P}$ is an orthogonal summand of L_2, where $\mathbb{P} = \mathbb{H}$ or $\mathbb{A}$, and $\theta(O^+(\mathbb{P})) \supseteq \mathbb{Z}_2^\times \mathbb{Q}_2^{\times 2}$. Therefore, $\mathrm{gen}(L) = \mathrm{spn}^+(L)$. If, in addition, L is indefinite, then $\mathrm{gen}(L) = cls^+(L)$ and the class number of L is 1.

9.3 Spinor Equivalence

Let L be a $\mathbb{Z}$-lattice on a nondegenerate space V, and K is another $\mathbb{Z}$-lattice in $\mathrm{gen}(L)$. How do we know if K is inside $\mathrm{spn}^+(L)$? By definition, $K = \Sigma L$ for some $\Sigma \in O_{\mathbb{A}}^+(V)$. Since the adelic spinor norm $\theta_{\mathbb{A}}$ induces an isomorphism

$$O_{\mathbb{A}}^+(V)/O(V)O'_{\mathbb{A}}(V)O_{\mathbb{A}}^+(L) \longrightarrow J/\mathbb{Q}^\times J_L,$$

therefore K is in $\mathrm{spn}^+(L)$ if and only if $\theta_{\mathbb{A}}(\Sigma) \in \mathbb{Q}^\times J_L$. The remaining question is: how do we construct Σ if L and K are given explicit enough?

It is clear that we can replace K by any lattice in $\mathrm{cls}^+(K)$. So by virtue of the Weak approximation Theorem we can assume that L and K only differ at the primes not dividing $2d(L)$, that is $L_p = K_p$ for all primes $p \mid 2d(L)$. Now take a prime p so that $L_p \neq K_p$. Then $p > 2$ and both L_p and K_p are unimodular $\mathbb{Z}_p$-lattices. Thus $[L_p : L_p \cap K_p] = [K_p : L_p \cap K_p]$ by Corollary 6.14. Consequently, $[L : L \cap K] = [K : L \cap K]$.

Lemma 9.12 *Suppose $L_p \neq K_p$. If σ_p is an isometry in $O^+(V_p)$ which sends L_p to K_p, then $\theta(\sigma_p) \in [L_p : L_p \cap K_p]\mathbb{Z}_p^\times \mathbb{Q}_p^{\times 2}$.*

Proof. For simplicity, let $e = \mathrm{ord}_p([L_p : L_p \cap K_p])$. Since $\theta(O^+(L_p)) = \mathbb{Z}_p^\times \mathbb{Q}_p^{\times 2}$, it suffices to exhibit an isometry in $O^+(V_p)$ of spinor norm p^e which sends L_p to K_p. By Theorem 6.12, we may assume that L_p and K_p are unimodular lattices on a hyperbolic plane with a hyperbolic pair x, y such that $L_p = \mathbb{Z}_p x + \mathbb{Z}_p y$ and $K_p = \mathbb{Z}_p p^e x + \mathbb{Z}_p p^{-e} y$. Then the isometry $\tau_{x-y}\tau_{x-p^{-e}y}$, which has spinor norm p^e, sends L_p to K_p.□

Definition 9.13 *The* intersecting idele *of L and K is the idele $j(L, K) \in J$ whose p-component is $p^{ord_p([L:L\cap K])}$.*

Theorem 9.14 *Let L and K be $\mathbb{Z}$-lattices in the same genus. If $[L : L \cap K]$ is relatively prime to $2d(L)$, then $K \in spn^+(L)$ if and only if $j(L, K) \in \mathbb{Q}^\times J_L$.*

Proof. If $\Sigma(L) = K$ where $\Sigma \in O^+_{\mathbb{A}}(V)$, then $\theta_{\mathbb{A}}(\Sigma) \in j(L, K)\mathbb{Q}^\times J_L$ by Lemma 9.12. Thus $K \in \mathrm{spn}^+(L)$ if and only if $j(L, K) \in \mathbb{Q}^\times J_L$.□

10 Representations of Spinor Genus

Throughout this section, L is a $\mathbb{Z}$-lattice on a nondegenerate space V of dimension ≥ 3. Suppose that a is a nonzero rational number which is represented by $\mathrm{gen}(L)$. Then a is represented by some lattice in $\mathrm{gen}(L)$. We say that a is represented by a proper spinor genus $\mathcal{S}$ in $\mathrm{gen}(L)$ if a is represented by some lattice in $\mathcal{S}$. The main question we would like to answer is: which proper spinor genera in $\mathrm{gen}(L)$ represent a?

Let $v \in V$ such that $Q(v) = a$ and let W be the orthogonal complement of the space spanned by v. For the questions with which we are concerned we may, without loss of generality, assume that $v \in L$.

10.1 Generators

An adele $\Sigma = (\Sigma_p) \in O^+_{\mathbb{A}}(V)$ is called a *generator* for L and v if $v \in \Sigma(L)$. Let $X_{\mathbb{A}}(L, v)$ be the set of generators for L and v. It is clear from the definition that

$$X_{\mathbb{A}}(L, v)O^+_{\mathbb{A}}(L) = O^+_{\mathbb{A}}(W)X_{\mathbb{A}}(L, v) = X_{\mathbb{A}}(L, v).$$

The importance of $X_{\mathbb{A}}(L, v)$ is illustrated in the following lemma.

Lemma 10.1 *Let $\Sigma \in O^+_{\mathbb{A}}(V)$. Then a is represented by $spn^+(\Sigma(L))$ if and only if $\Sigma \in O^+(V)O'_{\mathbb{A}}(V)X_{\mathbb{A}}(L,v)$.*

Proof. This is clear from the definitions.□

Note that in general $X_{\mathbb{A}}(L,v)$ may not be a group. However, we have

Theorem 10.2 *The set $O'_{\mathbb{A}}(V)X_{\mathbb{A}}(L,v)$ is a group.*

Proof. It suffices to prove that $\theta_{\mathbb{A}}(X_{\mathbb{A}}(L,v))$ is a group. Let p be a prime, and let $X(L_p,v)$ be the set of local generators, that is,

$$X(L_p,v) = \{\sigma \in O^+(V_p) : v \in \sigma(L_p)\}.$$

We need to show that $\theta(X(L_p,v))$ is a group. Since $X(L_p,v)O^+(L_p) = X(L_p,v)$, it is only necessary to consider the case when

$$[\mathbb{Q}_p^\times : \theta(O^+(L_p))] > 2.$$

This implies that L_p has only one dimensional Jordan components. When $p > 2$ this follows from the fact that the spinor norm of the isometry group of any binary unimodular $\mathbb{Z}_p$ lattices contains all p-adic units (Lemma 9.6). For $p = 2$, this follows from the explicit calculation of spinor norms of the isometry groups of modular $\mathbb{Z}_2$-lattices by Hsia.

So, we may write $L_p = \mathbb{Z}_p x_1 \perp \cdots \perp \mathbb{Z}_p x_n$ with $\mathrm{ord}_p(Q(x_1)) < \cdots < \mathrm{ord}_p(Q(x_n))$. We may assume that $\mathrm{ord}_p(Q(v)) = \mathrm{ord}_p(Q(x_1))$; otherwise one can replace L_p by $L'_p = \mathbb{Z}_p p x_1 \perp \cdots \perp \mathbb{Z}_p x_n$ because $X(L_p,v) = X(L'_p,v)$ and the argument can be repeated. Also, $x_1 = v$ can be assumed.

Let $\sigma \in X(L_p,v)$. Then $\sigma^{-1}(v) \in L_p$ and hence $\sigma^{-1}(v) = \alpha v + w$ where $\alpha \in \mathbb{Z}_p^\times$ and $w \in W$. One of $1-\alpha$ and $1+\alpha$ is not in $2p\mathbb{Z}_p$. Without loss of generality, we assume that $1-\alpha \notin 2p\mathbb{Z}_p$. A direct verification shows that $\tau_{\sigma^{-1}v-v}$ is in $O(L_p)$ and $\tau_{\sigma^{-1}v-v}(v) = \sigma^{-1}(v)$. Therefore,

$$\sigma \circ \tau_{\sigma^{-1}v-v} \circ \tau_{x_2}(v) = v$$

which implies that $\sigma \in O^+(W_p)O^+(L_p)$. However, it is clear from the definitions that $O^+(W_p)O^+(L_p) \subseteq X(L_p,v)$. Thus $X(L_p,v) = O^+(W_p)O^+(L_p)$ and $\theta(X(L_p,v))$ is a subgroup of J.□

We therefore have the following chain of containment of groups

$$O^+(V)O'_{\mathbb{A}}(V)O^+_{\mathbb{A}}(L) \subseteq O^+(V)O'_{\mathbb{A}}(V)O^+_{\mathbb{A}}(L)O^+_{\mathbb{A}}(W) \subseteq O^+(V)O'_{\mathbb{A}}(V)X_{\mathbb{A}}(L,v) \subseteq O^+_{\mathbb{A}}(V).$$

Lemma 10.3 *We have $O^+_{\mathbb{A}}(V)/O^+(V)O'_{\mathbb{A}}(V)O^+_{\mathbb{A}}(L)O^+_{\mathbb{A}}(W) \cong J/\mathbb{Q}^\times J_L\theta_{\mathbb{A}}(O^+_{\mathbb{A}}(W))$ and*

$$O^+_{\mathbb{A}}(V)/O^+(V)O'_{\mathbb{A}}(V)X_{\mathbb{A}}(L,v) \cong J/\mathbb{Q}^\times\theta_{\mathbb{A}}(X_{\mathbb{A}}(L,v)).$$

Proof. This follows from the application of the adelic spinor norm map $\theta_{\mathbb{A}}$.□

Finally, we show that everything discussed thus far is independent of the choice of v and L.

Lemma 10.4 *Suppose that $v' \in L'$ with $Q(v') = Q(v)$ and $L' \in gen(L)$. Then the groups generated by $X_{\mathbb{A}}(L, v)$ and $X_{\mathbb{A}}(L', v')$ are conjugate in $O^+_{\mathbb{A}}(V)$ so that the subgroup $O^+(V)O'_{\mathbb{A}}(V)X_{\mathbb{A}}(L, v)$ is independent of the choice of v and L.*

Proof. Let $G(L, v)$ be the group generated by $X_{\mathbb{A}}(L, v)$. Let $\Sigma \in O^+_{\mathbb{A}}(V)$ such that $L' = \Sigma(L)$. We first suppose that $v = v'$. Then $\Sigma \in X_{\mathbb{A}}(L, v)$ by definition. If $g \in X_{\mathbb{A}}(L', v)$, then $v \in g\Sigma(L)$; thus $g\Sigma \in X_{\mathbb{A}}(L, v)$ and hence $g \in G(L, v)$. This shows that $G(L', v) \subseteq G(L, v)$. By reversing the roles of L and L' we see that $G(L, v) = G(L', v)$.

In general, let $\phi \in O^+(V)$ such that $\phi(v) = v'$. Then

$$\phi G(L, v)\phi^{-1} = G(\phi(L), \phi(v)) = G(\phi(L), v') = G(L', v').$$

□

From now on we shall write $X_{\mathbb{A}}(L, a)$ for $X_{\mathbb{A}}(L, v)$.

10.2 Representations

We know from the previous subsection that the number of proper spinor genera in $\mathrm{gen}(L)$ representing a is given by the following indices

$$[O^+(V)O'_{\mathbb{A}}(V)X_{\mathbb{A}}(L, a) : O^+(V)O'_{\mathbb{A}}(V)O^+_{\mathbb{A}}(L)] = [\mathbb{Q}^\times\theta_{\mathbb{A}}(L, a) : \mathbb{Q}^\times J_L].$$

For simplicity, we have used $\theta_{\mathbb{A}}(L, a)$ to denote $\theta_{\mathbb{A}}(X_{\mathbb{A}}(L, a))$.

Suppose first that either $\dim(W) \geq 3$ or W is a hyperbolic plane. Then $\theta(O^+(W_p)) = \mathbb{Q}_p^\times$ for all primes p. Therefore $\mathbb{Q}^\times\theta_{\mathbb{A}}(O^+_{\mathbb{A}}(W)) = J$, so that a is represented by *every* proper spinor genus in $\mathrm{gen}(L)$. Note that this recaptures Theorem 7.21.

Consider next the case $\dim(W) = 2$ and W is anisotropic. Let $\delta = d(W)$ and $E = \mathbb{Q}(\sqrt{-\delta})$. Then E is a quadratic extension of $\mathbb{Q}$. Let Ω_E be the set of places of E (that is, the set of equivalence classes of valuations on E). Each place ν of $\mathbb{Q}$ has one or two extensions in Ω_E. Let J_E be the group of ideles of E defined by

$$J_E = \{(x_\omega) \in \prod_{\omega \in \Omega_E} E_\omega^\times : |x_\omega|_\omega = 1 \text{ for almost all } \omega\}.$$

Define the norm map $\mathbb{N}_{E/\mathbb{Q}} : J_E \to J$ by

$$\mathbb{N}_{E/\mathbb{Q}}((x_\omega)) = (\prod_{\omega|\nu} \mathbb{N}_{\omega/\nu}(x_\omega)),$$

where $\mathbb{N}_{\omega/\nu}$ is the norm of the extension $E_\omega/\mathbb{Q}_\nu$.

Remark 10.5 The definitions of J_E and the associated norm map $\mathbb{N}_{E/\mathbb{Q}}$ extend naturally to all finite extensions of $\mathbb{Q}$.

Lemma 10.6 *We have* $\theta_{\mathbb{A}}(O^+_{\mathbb{A}}(W)) = \mathbb{N}_{E/\mathbb{Q}}(J_E)$.

Proof. It suffices to show that $\theta(O^+(W_\nu)) = \prod_{\omega|\nu} \mathbb{N}_{\omega/\nu}(E_\omega^\times)$ for every place ν of $\mathbb{Q}$. This is obvious when ν splits since both groups are equal to $\mathbb{Q}_\nu^\times$.

Suppose that ν does not split in E. Then there is only one place ω of E lying above ν and E_ω is a quadratic extension of $\mathbb{Q}_v$. Take an anisotropic vector $x \in W$ and let $\alpha = Q(x)$. Then $W \cong \langle \alpha \rangle \perp \langle \alpha\delta \rangle$. Thus, after scaling by α, the quadratic space W_ν can be identified with E_ω and the quadratic map is simply the norm $\mathbb{N}_{\omega/\nu}$. Therefore, if t is given in $\mathbb{N}_{\omega/\nu}(E_\nu^\times)$, then there must be a vector $y \in W$ such that $\alpha Q(y) = t$ and so

$$t = \alpha \cdot \alpha^{-1} t = \theta(\tau_x \tau_y) \in \theta(O^+(W_\nu)).$$

Conversely, let $\sigma \in O^+(W_\nu)$. Then σ is a product of even number of symmetries of W_ν. It follows from the above discussion that $\theta(\sigma) \in \mathbb{N}_{\omega/\nu}(E_\omega^\times)$. $\square$

By class field theory, $[J : \mathbb{Q}^\times \mathbb{N}_{E/\mathbb{Q}}(J_E)] = [E : \mathbb{Q}] = 2$. We offer another proof here.

Lemma 10.7 *If* $E/\mathbb{Q}$ *is a quadratic extension, then* $[J : \mathbb{Q}^\times \mathbb{N}_{E/\mathbb{Q}}(J_E)] = 2$.

Proof. Define a function $R : J \to \{\pm 1\}$ by

$$R((x_\nu)) = \prod_\nu (x_\nu, -\delta)_\nu,$$

where $(\ ,\ )_\nu$ is the Hilbert symbol over $\mathbb{Q}_\nu$. It is well-defined since for almost all odd primes p, x_p and $-\delta$ are p-adic units and hence $(x_p, -\delta)_p = 1$. Since $-\delta \notin \mathbb{Q}^{\times 2}$, there is a place ν at which $-\delta \notin \mathbb{Q}_\nu^{\times 2}$. Hence there must be $x_\nu \in \mathbb{Q}_\nu^\times$ such that $(x_\nu, -\delta)_\nu = -1$. This shows that R is surjective. We shall show that $\ker R$ is precisely $\mathbb{Q}^\times \mathbb{N}_{E/\mathbb{Q}}(J_E)$.

Recall that $(x_\nu, -\delta)_\nu = 1$ if and only if x_ν is a norm of the field extension $\mathbb{Q}_p(\sqrt{-\delta})/\mathbb{Q}_p$. Thus $\mathbb{N}_{E/\mathbb{Q}}(J_E) \subseteq \ker R$. It follows from Hilbert Reciprocity Law that $\mathbb{Q}^\times \subseteq \ker R$. Hence $\mathbb{Q}^\times \mathbb{N}_{E/\mathbb{Q}}(J_E) \subseteq \ker R$. For the other inclusion, let $(x_\nu) \in \ker R$ and let $\nu_1, \ldots, \nu_m$ be the places for which $(x_\nu, -\delta)_\nu = -1$. Note that m is even and nonzero. Let S be a finite set of primes which contains the prime 2 and all the finite places among the ν_i, and such that for any $p \notin S$, x_p and δ are p-adic units. Put $e_p = \mathrm{ord}_p(x_p)$ and define

$$h = \prod_{p \in S} p^{e_p}.$$

We take a prime $q \notin S$ such that

$$q \equiv \eta h^{-1} x_p \bmod p^t, \qquad \text{for all } p \in S,$$

where t is a sufficiently large integer and $\eta = 1$ if all the places ν_i are finite; otherwise $\eta = -1$. We claim that $q\eta h^{-1}(x_\nu) \in \mathbb{N}_{E/\mathbb{Q}}(J_E)$, that is $(q\eta h^{-1} x_\nu, -\delta)_\nu = 1$ for all places ν. This will complete the proof.

If a prime p is not in S and $p \neq q$, then p is odd and $q\eta h^{-1} x_p$ and $-\delta$ are in $\mathbb{Z}_p^\times$, and thus $(q\eta h^{-1} x_p, -\delta)_p = 1$. If p is in S, then $q\eta h^{-1} x_p$ is a square in $\mathbb{Q}_p^\times$ (since t is

chosen large enough) and hence $(q\eta h^{-1}x_p, -\delta)_p = 1$ also. If all the places ν_i are finite, then $q\eta h^{-1} > 0$ and then $(q\eta h^{-1}x_\infty, -\delta)_\infty = (x_\infty, -\delta) = 1$. If $\nu_i = \infty$ for some i, then $\eta = -1$ and $(x_\infty, -\delta)_\infty = -1$. This means that $x_\infty < 0$. So, $(q\eta h^{-1}x_\infty, -\delta)_\infty = (-x_\infty, -\delta)_\infty = 1$. Finally at the prime q, since $q\eta h^{-1}(x_\nu) \in \ker R$, we have

$$(q\eta h^{-1}x_q, -\delta)_q = \prod_{\nu \neq q} (q\eta h^{-1}x_\nu, -\delta)_\nu = 1.$$

□

Since there are inclusions of groups

$$\mathbb{Q}^\times \mathbb{N}_{E/\mathbb{Q}}(J_E) \subseteq \mathbb{Q}^\times \theta_{\mathbb{A}}(L, a) \subseteq J,$$

therefore, $\mathbb{Q}^\times \theta_{\mathbb{A}}(L, a) \neq J$ if and only if $\mathbb{Q}^\times \theta_{\mathbb{A}}(L, a) = \mathbb{Q}^\times \mathbb{N}_{E/\mathbb{Q}}(J_E)$.

Lemma 10.8 *If $\mathbb{Q}^\times \theta_{\mathbb{A}}(L, a) = \mathbb{Q}^\times \mathbb{N}_{E/\mathbb{Q}}(J_E)$, then $\theta_{\mathbb{A}}(L, a) = \mathbb{N}_{E/\mathbb{Q}}(J_E)$.*

Proof. Assume the contrary that there exists $(x_\nu) \in \theta_{\mathbb{A}}(L, a)$ which is not in $\mathbb{N}_{E/\mathbb{Q}}(J_E)$. Then there must be a place ℓ for which $(x_\ell, -\delta)_\ell = -1$. Construct an idele $j = (j_\nu)$ such that $j_\nu = 1$ if $\nu \neq \ell$ and $j_\nu = x_\nu$. Then $j \in \theta_{\mathbb{A}}(L, a)$ and so we can write $j = \alpha n$ for some $\alpha \in \mathbb{Q}^\times$ and $n \in \mathbb{N}_{E/\mathbb{Q}}(J_E)$. For all $\nu \neq \ell$, since $j_\ell = 1$, we have $(\alpha, -\delta)_\nu = 1$. By Hilbert Reciprocity Law, $(\alpha, -\delta)_\ell = 1$ as well. Thus $(x_\nu, -\delta)_\nu = 1$ which is a contradiction.□

Therefore, $\mathbb{Q}^\times \theta_{\mathbb{A}}(L, a) \neq J$ if and only $\theta_{\mathbb{A}}(L, a) = \mathbb{N}_{E/\mathbb{Q}}(J_E)$. When this is the situation we shall call a a *spinor exception*. In this case, we have

$$[\mathbb{Q}^\times \theta_{\mathbb{A}}(L, a) : \mathbb{Q}^\times J_L] = \frac{[J : \mathbb{Q}^\times J_L]}{[J : \mathbb{Q}^\times \theta_{\mathbb{A}}(L, a)]} = \frac{[J : \mathbb{Q}^\times J_L]}{[J : \mathbb{Q}^\times \mathbb{N}_{E/\mathbb{Q}}(J_E)]} = \frac{1}{2}[J : \mathbb{Q}^\times J_L]$$

so that a is represented by exactly half of the proper spinor genera in $\mathrm{gen}(L)$. To summarize:

Theorem 10.9 *Suppose that a is represented by the genus of a ternary $\mathbb{Z}$-lattice L and $-ad(L) \notin \mathbb{Q}^{\times 2}$. Then a is a spinor exception if and only if $\theta_{\mathbb{A}}(L, a) = \mathbb{N}_{E/\mathbb{Q}}(J_E)$, where $E = \mathbb{Q}(\sqrt{-ad(L)})$. Moreover, $spn^+(\Sigma L)$ represents a if and only if $\theta_{\mathbb{A}}(\Sigma) \in \mathbb{Q}^\times \theta_{\mathbb{A}}(L, a)$.*

The groups $\theta_{\mathbb{A}}(L, a)$ are explicitly determined by Schulze-Pillot.

10.3 A Class Field Interpretation

Let F be a number field and $\mathcal{O}$ be the ring of integers in F. Let Ω_F be the set of places of F. The group of ideles of F is defined by

$$J_F = \{(x_\nu) \in \prod_{\nu \in \Omega_F} F_\nu^\times : x_\nu \in \mathcal{O}_\nu^\times \text{ for almost all } \nu\}.$$

Let Ω_F^f and Ω_F^∞ be the set of finite and infinite, respectively, places of F. We impose a topology on J_F as follows. Let

$$\mathcal{E} = \prod_{\nu \in \Omega_F^\infty} F_\nu^\times \prod_{\nu \in \Omega_F^f} \mathcal{O}_\nu^\times.$$

It is easy to see that $\mathcal{E}$ is a subgroup of J_F. Each factor of $\mathcal{E}$ has its metric topology induced by the associated valuation. Each $F_\nu^\times$ is locally compact while each $\mathcal{O}_\nu^\times$ is compact. We give $\mathcal{E}$ the product topology so that it becomes a locally compact topological group. Next we consider the following collection of subsets of J_F

$$\{j\mathcal{A} : j \in J_F \text{ and } \mathcal{A} \text{ is open in } \mathcal{E}\}.$$

We declare each subset in this collection open in J_F. It turns out that these open subsets form a basis of a topology on J_F which we call the *restricted product topology*.

An open subgroup H of J_F is called *principal* if $F^\times \subseteq H$ and $[J_F : H] < \infty$. For a finite abelian extension E/F, $F^\times \mathbb{N}_{E/F}(J_E)$ is a principal open subgroup of J_F. A main theorem in Class Field Theory says that

$$E \mapsto F^\times \mathbb{N}_{E/F}(J_E)$$

is a bijective inclusion-reversing correspondence between finite abelian extensions of F and principal open subgroups of J_F. Moreover, Artin Reciprocity Law, which is a generalization of Hilbert Reciprocity Law, gives an isomorphism

$$J_F/F^\times \mathbb{N}_{E/F}(J_E) \longrightarrow \mathrm{Gal}(E/F).$$

Let us go back to our discussion of spinor genera. In our case, the base field is $\mathbb{Q}$ (even though all the results discussed thus far about spinor genera can be generalized to any number field setting). The group $\mathbb{Q}^\times J_L$ is clearly a principal open subgroup of $J(= J_F)$. Associated to it by Class Field Theory is an abelian extension $\Sigma/\mathbb{Q}$. Since $J_L \supseteq J^2$, Σ/F is a multiquadratic extension. We call Σ the *spinor class field* of $\mathrm{gen}(L)$.

It is clear that we can rephrase all the results, especially Theorem 10.9, in terms of the spinor class fields. Here we offer a result that can be deduced easily from this class field setting but is not obvious from the previous discussion. The group $\mathbb{Q}^\times \theta_{\mathbb{A}}(L, a)$ is also a principal open subgroup of J and hence one can associate to it an abelian extension $\Sigma_{L/a}$ called a *relative spinor class field*. Since we have a chain of containments of groups

$$\mathbb{Q}^\times J_L \subseteq \mathbb{Q}^\times \theta_{\mathbb{A}}(L, a) \subseteq J,$$

we have a chain of fields

$$\mathbb{Q} \subseteq \Sigma_{L/a} \subseteq \Sigma.$$

If a is a spinor exception of $\mathrm{gen}(L)$, then $\theta_{\mathbb{A}}(L, a) = \mathbb{N}_{E/\mathbb{Q}}(J_E)$ where $E = \mathbb{Q}(\sqrt{-ad(L)})$. In particular, $\Sigma_{L/a}$ is in fact the quadratic extension $\mathbb{Q}(\sqrt{-ad(L)})$. Since Σ can have only finitely many quadratic subextensions of $\mathbb{Q}$, therefore we have

Proposition 10.10 *Let L be a ternary nondegenerate $\mathbb{Z}$-lattice. Then the spinor exceptions of gen(L) fall into finitely many square classes.*

11 Representations of Definite Quadratic Forms

In this section, we will prove the following theorem.

Theorem 11.1 (Tartakowsky, Kloosterman, Pall and Ross) *If L is a positive definite $\mathbb{Z}$-lattice of rank ≥ 5. Then there exists a constant $c(L)$ such that a is represented by L if a is represented by the genus of L and $a > c(L)$.*

The above theorem is false if the rank of L is 4. Consider the $\mathbb{Z}$-lattice $L = \langle 1, 1, 25, 25\rangle$. If $p \neq 5$, L_p is just the sum of 4 squares. Hence $Q(L_p) = \mathbb{Z}_p$ for $p \neq 5$. Since -1 is a square in $\mathbb{Z}_5$, L_5 is split by $\langle 1, 1\rangle \cong \mathbb{H}$; hence $Q(L_5) = \mathbb{Z}_5$. Consequently, the genus of L represents all positive integers. We claim that L does not represent all integers of the form $3 \cdot 2^r$. Let $\{v_1, v_2, v_3, v_4\}$ be an orthogonal basis for L whose associated symmetric matrix is $\langle 1, 1, 25, 25\rangle$. Suppose that there exists $v \in L$ such that $Q(v) = 3 \cdot 2^r$. If $v = \sum a_i v_i$, then

$$3 \cdot 2^r = a_1^2 + a_2^2 + 25a_3^2 + 25a_4^2.$$

If $r \leq 2$, then $a_3 = a_4 = 0$. But then the equation

$$3 \cdot 2^r = a_1^2 + a_2^2$$

is not soluble over $\mathbb{Z}$. If $r \geq 3$, then all the a_i must be even, and hence $3 \cdot 2^{r-2}$ is also represented by L. Eventually we arrive at the conclusion that L represents an integer of the form $3 \cdot 2^m$ with $m \leq 2$, which is impossible as shown earlier.

11.1 Some Local Results

In this subsection, L is a $\mathbb{Z}_p$-lattice on a nondegenerate quadratic space V over $\mathbb{Q}_p$. Recall that L is a maximal lattice if L is an (a)-maximal lattice for some $a \in \mathbb{Q}_p^\times$.

Proposition 11.2 *If L is a maximal lattice on V and $\dim(V) \geq 3$, then $\theta(O^+(L)) \supseteq \mathbb{Z}_p^\times$.*

Proof. By scaling the quadratic form on V, we may assume that L is (2)-maximal. If V is anisotropic, then L is the unique (2)-maximal lattice on V. This means that $O^+(L) = O^+(V)$. By Lemma 7.20, $\theta(O^+(L)) = \theta(O^+(V)) = \mathbb{Q}_p^\times$.

Suppose that V is isotropic. Then L is split by the hyperbolic plane $\mathbb{H}$; see Theorem 6.12. So, $\theta(O^+(L)) \supseteq \theta(O^+(\mathbb{H})) \supseteq \mathbb{Z}_p^\times$.□

Lemma 11.3 *Suppose that $p > 2$ and that L is a unimodular lattice. If x and y are primitive vectors of L with $Q(x) = Q(y)$, then there exists $\sigma \in O(L)$ such that $\sigma(x) = y$.*

Proof. Let $w = y - x$. Then $Q(w) = -2B(x, w)$. If $Q(w) \in \mathbb{Z}_p^\times$, then $\tau_w \in O(L)$ and $\tau_w(x) = y$. Therefore, we may assume that $Q(w) \in (p)$. Suppose that we can find an $u \in L$ such that

$$Q(u), B(u, x), B(u, y) \in \mathbb{Z}_p^\times. \qquad (*)$$

Let $v = y - \tau_u(x)$. Then $v \in L$ because $\tau_u \in O(L)$. Moreover,

$$Q(v) = Q(w) + 4B(u,x)B(u,y)Q(u)^{-1} \in \mathbb{Z}_p^\times.$$

So, $\tau_v \in O(L)$ and a direct computation shows that $\tau_v(y) = \tau_u(x)$. This implies $\tau_v\tau_u(x) = y$.

Now it remains to show the existence of v satisfying $(*)$. Let $\bar{L}$ be the quadratic space L/pL over the finite field $\mathbb{F} = \mathbb{Z}_p/p\mathbb{Z}_p$. Since L is unimodular, $\bar{L}$ is a nondegenerate space over $\mathbb{F}$. For any vector $t \in L$, let $\bar{t}$ be its canonical image in $\bar{L}$. By abusing the notation, we also use Q and B to denote the quadratic form and bilinear form, respectively, induced on $\bar{L}$. Condition $(*)$ is equivalent to

$$Q(\bar{L} \setminus (\bar{x}^\perp \cup \bar{y}^\perp)) \neq 0.$$

Since x is a primitive vector of L, there exists $z \in L$ such that $B(z,x) = 1$. Therefore, $\dim(\bar{x}^\perp) = \dim(\bar{L}) - 1$. Similarly, $\dim(\bar{y}^\perp) = \dim(\bar{L}) - 1$.

Suppose on the contrary that

$$Q(\bar{L} \setminus (\bar{x}^\perp \cup \bar{y}^\perp)) = 0.$$

Let $\bar{t} \in \bar{x}^\perp \cap \bar{y}^\perp$ and $\bar{s} \in \bar{L} \setminus (\bar{x}^\perp \cup \bar{y}^\perp)$. Then $a\bar{t} + \bar{s} \notin \bar{x}^\perp \cup \bar{y}^\perp$ for all $a \in \mathbb{F}$. Therefore,

$$Q(a\bar{t} + \bar{s}) = a^2Q(\bar{t}) + 2aB(\bar{t},\bar{s}) + Q(\bar{s}) = 0, \quad \text{for all } a \in \mathbb{F}.$$

Since $p > 2$, this implies that

$$Q(\bar{t}) = B(\bar{t},\bar{s}) = Q(\bar{s}) = 0 \quad \forall \bar{t} \in \bar{x}^\perp \cap \bar{y}^\perp \text{ and } \forall \bar{s} \in \bar{L} \setminus (\bar{x}^\perp \cup \bar{y}^\perp). \qquad (**)$$

Note that $\bar{w} \in \bar{x}^\perp \cap \bar{y}^\perp$ and the set $\bar{L} \setminus (\bar{x}^\perp \cup \bar{y}^\perp)$ spans the whole space $\bar{L}$. Therefore, $B(\bar{w},\bar{L}) = 0$ and then $\bar{x}^\perp = \bar{y}^\perp$. Together with $(**)$ we deduce that $Q(\bar{x}^\perp) = Q(\bar{L} \setminus \bar{x}^\perp) = 0$, and hence $Q(\bar{L}) = 0$ which is impossible.□

Theorem 11.4 *Suppose that $p > 2$ and that L is a unimodular lattice. If M and N are isometric primitive sublattices of L and $\tau : M \to N$ is an isometry, then there exists $\sigma \in O(L)$ such that $\sigma|_M = \tau$. In particular, $\sigma(M) = N$.*

Proof. We proceed by an induction on the rank of M. If the rank of M is 1, then the theorem is a consequence of Lemma 11.3. Suppose now that the rank of M is at least 2. If there exists $x \in M$ with $Q(x) \in \mathbb{Z}_p^\times$, then

$$M = \mathbb{Z}_p x \perp M', \quad L = \mathbb{Z}_p x \perp L',$$

where L' is unimodular. By Lemma 11.3, there exists an isometry of L which sends x to $\tau(x)$. So, we may assume that $x = \tau(x)$, and hence

$$N = \mathbb{Z}_p x \perp N'.$$

Both M' and N' are primitive sublattices of L'. Moreover, by Theorem 6.4, M' and N' are isometric. By the induction assumption, there exists an isometry $\phi \in O(L')$ such that $\phi|_{M'} = \tau|_{M'}$. Then $\sigma = 1 \perp \phi$ is an isometry of L and $\phi|_M = \tau$.

Now, suppose that $Q(M) \subseteq (p)$. Let $\{x_1, \ldots, x_n\}$ be an orthogonal basis for M. Since M is primitive in L, there exists $z \in L$ such that $B(z, x_1) = 1$ and $B(z, x_i) = 0$ for all $i \geq 2$. Then the binary lattice $H = \mathbb{Z}_p x_1 + \mathbb{Z}_p z$ is a hyperbolic plane. Therefore,

$$L = H \perp L_1,$$

where L_1 is unimodular. Note that the lattice $M_1 = \mathbb{Z}_p x_2 + \cdots + \mathbb{Z}_p x_n$ is a primitive sublattice of L_1. As is in the previous paragraph, we may assume that $x_1 = \tau(x_1)$. Then $N_1 := \mathbb{Z}_p \tau(x_2) + \cdots + \mathbb{Z}_p \tau(x_n)$ is also a primitive sublattice of L_1, and N_1 is isometric to M_1. By Lemma 11.3, there exists an isometric $\rho \in O(L_1)$ such that $\rho|_{M_1} = \tau|_{M_1}$. Then $\sigma = 1 \perp \rho$, which is an isometry of L, is the desired isometry.□

Remark 11.5 When $p = 2$, Theorem 11.4 holds if L is an even unimodular $\mathbb{Z}_2$-lattice.

11.2 Main Result

From now on, let L be a $\mathbb{Z}$-lattice on a positive definite quadratic space V over $\mathbb{Q}$. Let $Q(\mathrm{gen}(L))$ be the set of rational numbers represented by L. For any positive integer r, let

$$Q_r(\mathrm{gen}(L)) = \{n \in Q(\mathrm{gen}(L)) : \mathrm{ord}_p(n) \leq r \text{ for all } p \text{ for which } V_p \text{ is anisotropic } \}$$

and

$$Q_r(L) = Q(L) \cap Q_r(\mathrm{gen}(L)).$$

If $\dim(V) \geq 5$, then $Q(\mathrm{gen}(L)) = Q_r(\mathrm{gen}(L))$ for every r, since V_p is isotropic for every prime p. If $\dim(V) = 4$, the above definitions make sense because there are only finitely many p for which V_p is anisotropic. We will prove the following theorem which has Theorem 11.1 as a consequence.

Theorem 11.6 *Let L be a positive definite $\mathbb{Z}$-lattice of rank ≥ 4. Then $Q_r(gen(L)) \setminus Q_r(L)$ is finite.*

Lemma 11.7 *Let a be a positive rational number and M be a positive definite $\mathbb{Z}$-lattice of rank ≥ 3. Suppose that the genus of M contains only one spinor genus. Let q be a prime for which M_q is isotropic. Then there exists $s \in \mathbb{Z}$ such that*

(a) $Q(gen(q^s M)) \subseteq Q(M)$;

(b) $Q_r(gen(q^s M \perp \langle a \rangle)) \setminus Q(M \perp \langle a \rangle)$ is finite.

Proof. (a) By Theorem 8.4, $\mathbb{Z}[1/q]M \cong \mathbb{Z}[1/q]K$ for every $K \in \mathrm{spn}^+(M)$. Therefore, there exists $s \in \mathbb{Z}$ such that $q^s K \subseteq M$ and hence

$$Q(K) \subseteq \frac{1}{q^{2s}} Q(M).$$

This s can be chosen to be independent of K because there are only finitely many classes in $\mathrm{spn}^+(L)$. Let $n \in Q(\mathrm{gen}(q^s M))$. Then $q^{-2s}n$ is represented by some $K \in \mathrm{gen}(M) = \mathrm{spn}^+(M)$. So $n \in Q(M)$.
(b) For our convenience, let L' be the lattice $q^s M \perp \langle a \rangle$. Let S be the set containing all the prime divisors of $2d(L')$. Note that L'_ℓ is unimodular for all $\ell \notin S$. For each prime p, let

$$Q_r(L'_p) = \{t \in Q(L'_p) : \mathrm{ord}_p(t) \leq r \text{ if } L'_p \text{ is anisotropic}\}.$$

Let $p \in S$. Suppose that $t \in Q_r(L'_p)$ and $t = Q(v)$ for some $v \in q^s M_p$. If $t \neq 0$, then for a sufficiently large integer k, $t - ap^{2k} = t\epsilon^2$ for some $\epsilon \in \mathbb{Z}_p^\times$. So, $t = Q(\epsilon v) + ap^{2k}$. If $t = 0$ and v is an isotropic vector in $q^s M_p$, then there exist integer $m \geq 0$ and $w \in q^s M_p$ such that $Q(w) = -ap^{2m}$. So, $t = Q(w) + ap^{2m}$. If $t = 0$ but $q^s M_p$ is anisotropic, then L'_p must be isotropic. So, there exists $v' \in q^s M_p$ and nonzero $u \in \mathbb{Z}_p$ such that $t = Q(v') + au^2$.

In summary, for each $t \in Q_r(L'_p)$, there exists $u \in \mathbb{Z}_p$, $u \neq 0$, such that $t \in Q(q^s M_p) + au^2$. Since the set $Q_r(L'_p)$ is compact and $Q(q^s M_p)$ is open, there is a finite set I_p of nonzero p-adic integers such that

$$Q_r(L'_p) \subseteq \bigcup_{u_p \in I_p} (Q(q^s M_p) + au_p^2).$$

Therefore, the product

$$\prod_{p \in S} Q(L'_p)$$

is contained in the union of the sets

$$\prod_{p \in S} (Q(q^s M_p) + au_p^2)$$

where $u_p \in I_p$ for each $p \in S$. By the Chinese Remainder Theorem, we can find a finite set of nonzero integers J such that for each collection $\{u_p : p \in S\}$ there exists $u \in J$ with

$$\prod_{p \in S} (Q(q^s M_p) + au_p^2) = \prod_{p \in S} (Q(q^s M_p) + au^2).$$

Suppose that $t \in Q(\mathrm{gen}(L'))$ and that $t \geq au^2$ for all $u \in J$. Then for each $p \in S$, there exists $u \in J$ such that

$$t - au^2 \in Q(q^s M_p).$$

For each $\ell \notin S$, $t - au^2 \in \mathbb{Z}_\ell$ since L'_ℓ is unimodular and $u \in \mathbb{Z}_\ell$. But $q^s M_\ell$ is a unimodular lattice of rank ≥ 3 and ℓ is odd. Therefore, $Q(q^s M_\ell) = \mathbb{Z}_\ell$ and hence $t - au^2 \in Q(q^s M_\ell)$ for all $\ell \notin S$. Consequently, it follows from part (a) that

$$t - au^2 \in Q(\text{gen}(q^s M)) \subseteq Q(M).$$

As a result, $t \in Q(M \perp \langle a \rangle)$.$\square$

Proof of Theorem 11.6. Let L be a $\mathbb{Z}$-lattice on a positive definite quadratic space V of dimension at least 4 over $\mathbb{Q}$. Choose a prime $q \nmid 2d(L)$ such that the Witt index of V_q is at least 2. When $\dim(V) \geq 5$, q can be chosen to be any prime not dividing $2d(L)$. When $\dim(V) = 4$, Dirichlet's theorem implies that there are infinitely many primes ℓ which are congruent to 1 mod p^3 for all $p \mid 2d(L)$. By the Quadratic Reciprocity Law, $d(L)$ is a square mod ℓ. We then choose q to be one of these ℓ.

Let $p \in S$. For any $\alpha \in Q(L_p)$, $\alpha \in Q(\mathbb{Z}_p u)$ for some $u \in L_p$ with $|Q(u)|_p$ maximal. Since $Q(L_p)$ is compact and each $Q(\mathbb{Z}_p u)$ is open, there exists a finite subset I_p of L_p such that

$$Q(L_p) = \bigcup_{u_p \in I_p} Q(\mathbb{Z}_p u_p).$$

Let $\{u_p \in I_p : p \in S\}$ be given. Choose $t \in \mathbb{Q}$ with the following properties:

(1) $t \in \mathbb{Z}_p^{\times 2} Q(u_p)$ for all $p \in S$;

(2) the prime factors of the denominator of t are in S;

(3) if $p \notin S$, then t is either a prime or a unit in $\mathbb{Z}_p$.

We can construct such a t as follows. Let $Q(u_p) = p^{a_p}\epsilon_p$, where $\epsilon_p \in \mathbb{Z}_p^\times$. By the Chinese Remainder Theorem, there exists an integer k such that

$$k \prod_{\ell \in S \setminus p} \ell^{a_\ell} \equiv \epsilon_p \bmod p^3, \text{ for all } p \in S.$$

By Dirichlet's theorem there exists a prime $\tilde{p} \notin S$ such that

$$\tilde{p} \equiv k \bmod \prod_{\ell \in S} \ell^3$$

Then

$$\tilde{p} \prod_{\ell \in S} \ell^{a_\ell} \in p^{a_p} \epsilon_p \mathbb{Z}_p^{\times 2} = Q(u_p)\mathbb{Z}_p^{\times 2}.$$

We then set

$$t = \tilde{p} \prod_{\ell \in S} \ell^{a_\ell}$$

and we are done.

From (1), it is clear that $t \in Q(L_p)$ for all $p \in S$. For any $p \notin S$, p is odd and L_p is unimodular; hence $t \in Q(L_p)$. Consequently, $t \in Q(\mathrm{gen}(L))$. It follows form Theorem 7.21 that $t \in Q(\mathrm{spn}^+(L))$. In other words, there exists $K \in \mathrm{spn}^+(L)$ such that $t \in Q(K)$. Let ℓ be a prime not in S such that $\ell \nmid t$ and the Witt index of V_ℓ is at least 2. Then $\mathbb{Z}[1/\ell]K \cong \mathbb{Z}[1/\ell]L$ by Theorem 8.4, and hence there exists $v \in V$ such that $Q(v) = t$ and $v \in L_p$ for all $p \neq \ell$.

Choose an integer $e \geq 0$ such that $\ell^e v$ is a primitive vector in L. We shall construct a sublattice M of L of rank $\mathrm{rank}(L) - 1$. For the sake of convenience, let J be the rank one lattice spanned by $\ell^e v$. We construct M by specifying its localization M_p for each prime p. Let W be the orthogonal complement of $\mathbb{Q}J$ in V.

If $p \notin S$, $p \neq \ell$ and $p \nmid t$: since J_p is unimodular, it splits L_p. We let $M(p)$ be the orthogonal complement of J_p in L_p. Then $\theta(O^+(M(p))) \supseteq \mathbb{Z}_p^\times$ and $Q(q^s M(p) \perp L_p) = \mathbb{Z}_p$ because $q^s M(p)$ is unimodular of rank ≥ 3.

If $p \in S$: let $L'(p)$ be a maximal lattice which contains $L_p \cap W_p$. Then $p^a L'(p) \subseteq L_p \cap W_p$ for some $a \geq 0$. Let $M(p)$ be the $\mathbb{Z}_p$-lattice $p^a L'(p)$. Since $M(p)$ is maximal, $\theta(O^+(M(p))) \supseteq \mathbb{Z}_p^\times$ by Proposition 11.2. Also, $Q(q^s M(p) \perp J_p) \supseteq Q(J_p) = Q(\mathbb{Z}_p u_p)$.

If $p = \ell$: since the Witt index of V_ℓ is at least 2 and L_ℓ is unimodular, $L_\ell = H_1 \perp H_2 \perp K$, where H_1 and H_2 are hyperbolic planes and K is a unimodular $\mathbb{Z}_\ell$-lattice. Also, since $\ell^e v$ is primitive in L_ℓ, there exists $z \in L_\ell$ such that $B(z, \ell^e v) = 1$. Let G be the binary $\mathbb{Z}_\ell$ lattice spanned by z and $\ell^e v$. If $Q(\ell^e v)$ is not a unit, then G is a hyperbolic plane and hence $L_\ell = G \perp H$ with $H \cong H_2 \perp K$. In this case, we let $M(\ell) = I \perp H$ where I is the orthogonal complement of J_ℓ in G.

If $Q(\ell^e v)$ is a unit, then J_ℓ splits L_ℓ. Therefore, $L_\ell = J_\ell \perp E = H_1 \perp H_2 \perp K$, where E is a unimodular $\mathbb{Z}_\ell$-lattice. Let w be a primitive vector of H_1 such that $Q(w) = Q(\ell^e v)$. By Lemma 11.3, there exists an isometry $\phi \in O(L_\ell)$ such that $\phi(w) = \ell^e v$. Hence

$$E \cong H_2 \perp K \perp (\text{ orthogonal complement of } w \text{ in } H_1 \text{ }).$$

In this case, let $M(\ell)$ be E.

In any case, $\theta(O^+(M(\ell))) \supseteq \mathbb{Z}_p$ since $M(\ell)$ has a rank 2 unimodular component. Also, $Q(q^s M(\ell)) \supseteq Q(q^s M(\ell)) = \mathbb{Z}_\ell$.

If $p \notin S$ and $p \mid t$: by the construction of t, we see that $p^2 \nmid t$. Therefore, v is primitive in L_p. Let $z \in L_p$ such that $B(z, v) = 1$. Then the binary sublattice spanned by v and z, denoted H, is a hyperbolic plane. So, $L_p = H \perp G$ for some unimodular $\mathbb{Z}_p$-lattice G. Also, H has a vector w satisfying $B(w, v) = 0$ and $Q(w) = -Q(v) = -t$. Let $M(p)$ be $\mathbb{Z}_p w \perp G$. Then $\theta(O^+(M(p))) \supseteq \mathbb{Z}_p^\times$ and $Q(q^s M(p) \perp J_p) = \mathbb{Z}_p$.

Note that or almost all primes p, $M(p)$ is the orthogonal complement of J_p in L_p. By Theorem 7.8, there exists a $\mathbb{Z}$-lattice M on W such that $M_p = M(p)$ for all p. Since $\theta(O^+(M(p))) \supseteq \mathbb{Z}_p^\times$ for all p, the genus of M contains only one spinor genus. Note that all together we have constructed only finitely many t and M.

Let $\alpha \in Q_r(\mathrm{gen}(L))$. Then at each $p \in S$, $\alpha \in Q(\mathbb{Z}_p u_p)$ for some $u_p \in J_p$. For $p \notin S$, L_p is unimodular; hence $\alpha \in \mathbb{Z}_p$. Let t, J and M be as constructed as above. Then $\alpha \in Q_r(\mathrm{gen}(q^s M \perp J))$. By Lemma 11.6, all but finitely many α are in $Q(L)$.□

12 Classes and Genera of Representations

Throughout this section, R is either $\mathbb{Z}$ or $\mathbb{Z}_p$ for some prime p, and F is the field of fractions of R. An R-lattice L is said to be integral if $\mathfrak{s}(L) \subseteq R$.

12.1 Representations of Lattices

Definition 12.1 Let L and M be R-lattices. A representation of L by M is an injective R-homomorphism $\sigma : L \to M$ such that $Q(\phi(v)) = Q(v)$ for all $v \in L$.

This generalizes the representation of an element in R by a lattice. For, let $a \in R$, L be the rank 1 R-lattice $\langle a \rangle$, and M be an R-lattice. Then having a representation of L by M is equivalent to the existence of a vector $x \in M$ with $Q(x) = a$.

Definition 12.2 Two representations $\phi_i : L \to M_i$ $(i = 1, 2)$ of R-lattices are in the same class if there exists an isometry $\sigma : M_1 \to M_2$ such that $\phi_2 = \sigma\phi_1$.

Proposition 12.3 *Suppose that L and M are nondegenerate R-lattices. If $\phi : L \to M$ is a representation, then there exists an R-lattice M' such that $L \subseteq M'$ and ϕ is in the same class of the inclusion $L \hookrightarrow M'$.*

Proof. Let U be a quadratic space which is isometric to $\phi(FL)^\perp$, and let $\tau : U \to \phi(FL)^\perp$ be an isometry. Then $\phi \perp \tau$ is an isometry from $FL \perp U$ to FM. Let M' be $(\phi \perp \tau)^{-1}(M)$. Then $L \subseteq M'$ and ϕ is in the same class of the inclusion $L \hookrightarrow M'$. □

Lemma 12.4 *Suppose that L and M are unimodular $\mathbb{Z}_p$-lattices, $p > 2$. Then there is only at most one class of representations of L by M.*

Proof. Let $\phi_i : L \to M$, $i = 1, 2$, be two representations of L by M. Then $\phi_1(L)$ and $\phi_2(L)$ are two primitive sublattices of M. Let $\tau : \phi_1(L) \to \phi_2(L)$ be an isometry. By Theorem 11.4, there exists an isometry $\sigma \in O(M)$ such that $\sigma|_{\phi_1(L)} = \tau$. Then $\sigma\phi_1 = \phi_2$, hence ϕ_1 and ϕ_2 are in the same class.□

Lemma 12.5 *Suppose that L and M are nondegenerate R-lattices with $L \subseteq M$. Let N be the orthogonal complement of L in M. Then $d(N) \mid d(M)d(L)$. In fact, $N^\#/N$ is a homomorphic image of a subgroup of $M^\#/M \oplus L^\#/L$.*

Proof. This is just Lemma 7.2. Since M/N is torsion free, N is a primitive sublattice of M. So, the restriction map induces a surjective homomorphism

$$M^\#/(L \perp N) \to N^\#/N.$$

On the other hand, the map $M^\#/(L \perp N) \longrightarrow L^\#/L \oplus M^\#/M$ which sends x to $(P(x), x)$ where P is the orthogonal projection from FM onto FL, is injective.□

Theorem 12.6 *Suppose that L is a nondegenerate R-lattice. Given any positive integer n and element $d \in R \setminus \{0\}$, there are only finitely many classes of representations $\phi : L \to M$ with rank$(M) = n$ and $d(M) = d$.*

Proof. Let $\phi : L \to M$ be one of such representations. If N is the orthogonal complement of $\phi(L)$ in M, then

$$\phi(L) \perp N \subseteq M \subseteq M^{\#} \subseteq (\phi(L) \perp N)^{\#}.$$

By Lemma 12.5, $d(N)$ divides $d(M)d(L)$. Therefore, there are only finitely many isometry classes of N. Let $\{N_i\}$ be a complete set of representatives of these classes. For each i, there are only finitely many integral R-lattices M_{ij} with $\text{rank}(M_{ij}) = n$, $d(M_{ij}) = d$, and

$$L \perp N_i \subseteq M_{ij} \subseteq (L \perp N_i)^{\#}.$$

Since there are only finitely many N_i, the set $\{M_{ij}\}$ is finite. Let $\phi_{ij} : L \to M_{ij}$ be the representation induced by the inclusion $L \perp N_i \hookrightarrow M_{ij}$. We claim that every representation of L by some lattice M with $\text{rank}(M) = n$ and $d(M) = d$ is in the class of some ϕ_{ij}.

Let $\rho : L \to M$ be such a representation. Let N be the orthogonal complement of $\rho(L)$ in M. Then N must be isometric to N_i for some i. Let $\tau_i : N \to N_i$ be an isometry, and σ be the isometry $\phi^{-1} \perp \tau_i$ from $\phi(L) \perp N$ to $L \perp N_i$. Then $\sigma((\phi(L) \perp N)^{\#}) = (L \perp N_i)^{\#}$, and hence $\sigma(M) = M_{ij}$ for some j. It is immediate that $\sigma\rho = \phi_{ij}$.□

The above theorem is false if $d(L) = 0$. Consider a $\mathbb{Z}$-lattice $L = \mathbb{Z}x \cong \langle 0 \rangle$, and a hyperbolic plane M with a basis $\{e, f\}$ whose associated symmetric matrix is $\left(\begin{smallmatrix} 0 & 1 \\ 1 & 0 \end{smallmatrix}\right)$. Then $x \mapsto nf$, $n \in \mathbb{Z} \setminus \{0\}$, are all different representations. The orthogonal group of M is clearly finite because $\{\pm e, \pm f\}$ are the only primitive isotropic vectors in M and any isometry of L must send e (or f) to a primitive isotropic vector.

Lemma 12.7 *Let M_1 and M_2 be two R-lattices on a quadratic space over F. Then $[O(M_i) : O(M_1) \cap O(M_2)]$ is finite for $i = 1, 2$.*

Proof. There exist two nonzero elements a and b in F such that $bM_1 \subseteq M_2 \subseteq aM_1$. We have a natural homomorphism

$$O(M_1) \to \text{Aut}_{\mathbb{Z}}(aM_1/bM_1).$$

Let G be the kernel of this homomorphism. Then $[O(M_1) : G]$ is finite since aM_1/bM_1 is a finite group. The elements of G acts trivially on M_2/bM_1, hence $G \subseteq O(M_2)$. As a result, $G \subseteq O(M_1) \cap O(M_2)$ and thus $[O(M_1) : O(M_1) \cap O(M_2)]$, which is smaller than $[O(M_1) : G]$, is finite. Similarly, $[O(M_2) : O(M_1) \cap O(M_2)]$ is also finite.□

Theorem 12.8 *Let L be a nondegenerate $\mathbb{Z}$-lattice. If M is a positive definite $\mathbb{Z}$-lattice or $\mathbb{Q}M$ is the hyperbolic plane, then there are only finitely many representations of L by M.*

Proof. Since there are only finitely many classes of representations of L by M, it suffices to show that $O(M)$ is finite when M is positive definite or $\mathbb{Q}M$ is the hyperbolic plane.

Suppose that M is positive definite. Let $\{e_1, \ldots, e_n\}$ be an orthogonal basis for $\mathbb{Q}M$ with $Q(e_i) \leq Q(e_{i+1})$ for all i, and let $M' = \mathbb{Z}e_1 \perp \cdots \perp \mathbb{Z}e_n$. Then $|O(M')|$ is finite. By Lemma 12.7, $|O(M)|$ is finite.

If $\mathbb{Q}M$ is the hyperbolic plane, let M' be a lattice on $\mathbb{Q}M$ with symmetric matrix $\left(\begin{smallmatrix} 0 & 1 \\ 1 & 0 \end{smallmatrix}\right)$. Then $|O(M')|$, and hence $|O(M)|$ as well, is finite.□

Remark 12.9 It can be shown that if M is an indefinite $\mathbb{Z}$-lattice and $\mathbb{Q}M$ is not the hyperbolic plane, then $O(M)$ is an infinite group.

12.2 Genus of Representations

Definition 12.10 Two representations $\phi : L \to M$ and $\phi' : L \to M'$ of $\mathbb{Z}$-lattices are in the same genus if there are isometries $\sigma_p : M_p \to M'_p$ for all primes p such that $\phi' = \sigma_p \phi$ for all p.

For a prime p and a pair of $\mathbb{Z}$-lattices L and M, let $c(L_p, M_p)$ be the number of classes of representations of L_p by M_p. By Theorem 11.4, $c(L_p, M_p)$ is equal to 1 for almost all p.

Theorem 12.11 *Let L and M be nondegenerate $\mathbb{Z}$-lattices. The number of genera of representations of L by lattices in gen(M) is equal to $\prod_p c(L_p, M_p)$.*

Proof. Let $\mathcal{G}$ be the set of all genera of representations of L by lattices in $\mathrm{gen}(M)$. For each p, let $\mathcal{C}_p$ be the set of classes of representations of L_p by M_p. Let $\phi : L \to M'$ be a representation with $M' \in \mathrm{gen}(M)$. For each prime p, ϕ induces representations $\phi : L_p \to M'_p$. Let $\sigma_p : M'_p \to M_p$ be an isometry. Then $\sigma_p \phi : L_p \to M_p$ is a representation. Different choices of the isometry σ_p result in different representations of L_p by M_p that are in the same class. So we have a well-defined map

$$\Phi : \mathcal{G} \longrightarrow \prod_p \mathcal{C}_p.$$

Let $\phi : L \to K$ and $\tau : L \to N$ be two representations of L by lattices in $\mathrm{gen}(M)$. Suppose that for each p, the classes of representations of L_p by M_p induced by ϕ and τ are the same. Then for each p, there are isometries σ_p, ψ_p and ρ_p which make the following diagram commute

$$\begin{array}{ccccc} L_p & \xrightarrow{\phi} & K_p & \xrightarrow{\sigma_p} & M_p \\ & & & & \downarrow \psi_p \\ L_p & \xrightarrow{\tau} & N_p & \xrightarrow{\rho_p} & M_p \end{array}$$

Let $\eta_p = \rho_p^{-1} \psi_p \sigma_p$. Then $\tau = \eta_p \phi$. Therefore, ϕ and τ are in the same genus. This shows that Φ is injective.

Suppose that a representation $\phi_p : L_p \to M_p$ is given for each p. Let T be a finite set of primes satisfying

(a) $c(L_p, M_p) = 1$ for all $p \notin T$;

(b) $L_p \subseteq M_p$ for all $p \notin T$.

Let W and V be the $\mathbb{Q}$-spaces spanned by L and M, respectively. By the Hasse Principle, there is an isometry sending W into V. So we may assume that L is a $\mathbb{Z}$-lattice in V. For each p, it follows from Witt's extension theorem that there exists an isometry $\sigma_p \in O(V_p)$ such that $\sigma_p|_{L_p} = \phi_p$. Define a $\mathbb{Z}$-lattice M' on V by specifying its localization as follows:

$$M'_p = \begin{cases} M_p & \text{for all } p \notin T; \\ \sigma_p^{-1}(M_p) & \text{for all } p \in T. \end{cases}$$

Then at each $p \in T$,

$$L_p = \sigma_p^{-1}(\phi_p(L_p)) \subseteq M'_p.$$

Note that for each $p \notin T$, $L_p \subseteq M_p = M'_p$. Therefore, $L \subseteq M'$. Let $j : L \hookrightarrow M'$ be the inclusion. Then for each $p \notin T$, ϕ_p and j are in the same class because $c(L_p, M_p) = 1$. For each $p \in T$, $\sigma_p(\phi_p(x)) = x$ for all $x \in L_p$; thus $j = \sigma_p^{-1}\phi_p$ for each $p \in T$. Consequently, j and ϕ_p are in the same class for all p. This proves that Φ is surjective.$\square$