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 matric (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 this 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 determines 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 identity 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 $\hat{B}(v_i)(v_j) = B(v_i, v_j)$ follows

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

□

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 $B(x_1 + x_2, y_1 + y_2) = B_1(x_1, y_1) + B_2(x_2, y_2)$ 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 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 of 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 defined 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.