

QUADRATIC FORMS OVER FIELDS I: FOUNDATIONS

PETE L. CLARK

CONTENTS

1. Four equivalent definitions of a quadratic form	1
2. Action of $M_n(K)$ on n -ary quadratic forms	3
3. The category of quadratic spaces	6
4. Orthogonality in quadratic spaces	9
5. Diagonalizability of Quadratic Forms	10
6. Isotropic and hyperbolic spaces	12
7. Witt's theorems: statements and consequences	15
8. Orthogonal groups, reflections and the proof of Witt Cancellation	17
9. The Witt Ring	19
9.1. The Grothendieck-Witt Ring	20
10. Additional Exercises	22
References	23

Quadratic forms were first studied over \mathbb{Z} , by all of the great number theorists from Fermat to Dirichlet. Although much more generality is now available (and useful, and interesting), it is probably the case that even to this day integral quadratic forms receive the most attention. However, at the end of the 19th century it was realized that the theory of quadratic forms with \mathbb{Q} -coefficients is significantly simpler – indeed, in a sense it was completely solved by Minkowski and Hasse – but still of great use in understanding the integral case. In a 1937 paper [Wit], Witt showed that many formal aspects of the theory of quadratic forms over \mathbb{Q} carry over unchanged to the case of quadratic forms over an arbitrary field K of characteristic different from 2, and he discovered in this very general context a key result, the **Witt Cancellation Theorem** and used this to define a commutative ring $W(K)$ whose elements are equivalence classes of (certain) quadratic forms over K . This was the beginning of a new subject, the **algebraic theory of quadratic forms**.

In these notes we give a detailed treatment of the foundations of this theory, starting from scratch and ending with Witt Cancellation and the Witt ring.

Let K denote a field of characteristic different from 2 but otherwise arbitrary.

1. FOUR EQUIVALENT DEFINITIONS OF A QUADRATIC FORM

There are several equivalent but slightly different ways of thinking about quadratic forms over K . The standard “official” definition is that a quadratic form is a

polynomial $q(t) = q(t_1, \dots, t_n) \in K[t_1, \dots, t_n]$, in several variables, with coefficients in K , and such that each monomial term has total degree 2: that is,

$$q(t) = \sum_{1 \leq i < j \leq n} a_{ij} t_i t_j,$$

with $a_{ij} \in K$.

But apart from viewing a polynomial purely formally – i.e., as an element of the polynomial ring $K[x]$ – we may of course also view it as a function. In particular, every quadratic form $q(x)$ determines a function

$$f_q : K^n \rightarrow K, \quad x = (x_1, \dots, x_n) \mapsto \sum_{1 \leq i < j \leq n} a_{ij} x_i x_j.$$

The function f_q has the following properties:

- (i) For all $\alpha \in K$, $f(\alpha x) = \alpha^2 f(x)$, i.e., it is homogeneous of degree 2.
 - (ii) Put $B_f(x, y) := \frac{1}{2}(f_q(x+y) - f_q(x) - f_q(y))$.¹
- Then we have, for all $x, y, z \in K^n$ and $\alpha \in K$, that

$$B_f(x, y) = B_f(y, x)$$

and

$$B_f(\alpha x + y, z) = \alpha B_f(x, z) + B_f(y, z).$$

In other words, $B_f : K^n \times K^n \rightarrow K$ is a **symmetric bilinear form**.

Moreover, we have

$$B_f(x, x) = \frac{1}{2}(f_q(2x) - 2f_q(x)) = \frac{1}{2}(4f_q(x) - 2f_q(x)) = f_q(x).$$

Thus each of f_q and B_f determines the other. Now consider *any* function $f : K^n \rightarrow K$ which satisfies (i) and (ii), a **homogeneous quadratic function**. Let e_1, \dots, e_n be the standard basis of K^n and for any $1 \leq i, j \leq n$, put $b_{ij} = B_f(e_i, e_j)$. Let B be the $n \times n$ symmetric matrix with entries b_{ij} . Then B_f can be expressed in terms of B . We make the convention of identifying $x \in K^n$ with the $n \times 1$ matrix (or “column vector”) whose $(i, 1)$ entry is x_i . Then, for all $x, y \in K^n$, we have

$$y^T B x = B_f(x, y).$$

Indeed, the left hand side is also a bilinear form on K^n , so it suffices to check equality on pairs (e_i, e_j) of basis vectors, and this is the very definition of the matrix B . Thus each of B_f and B determines the other.

Moreover, taking $x = y$, we have

$$x^T B x = f(x).$$

If on the left-hand side we replace $x \in K^n$ by the indeterminates $t = (t_1, \dots, t_n)$, we get the polynomial

$$\sum_{i=1}^n b_{ii} t_i^2 + \sum_{1 \leq i < j \leq n} b_{ij} + b_{ji} t_i t_j = \sum_{i=1}^n b_{ii} t_i^2 + \sum_{1 \leq i < j \leq n} 2b_{ij} t_i t_j.$$

¹Note that $\frac{1}{2}$ exists in K since the characteristic of K is different from 2!

It follows that any homogeneous quadratic function is the f_q of a quadratic form $q = \sum_{i,j} a_{ij}t_it_j$, with

$$a_{ii} = b_{ii}, \quad a_{ij} = 2b_{ij} \forall i < j.$$

We have established the following result.

Theorem 1. *For $n \in \mathbb{Z}^+$, there are canonical bijections between the following sets:*

- (i) *The set of homogeneous quadratic polynomials $q(t) = q(t_1, \dots, t_n)$.*
- (ii) *The set of homogeneous quadratic functions on K^n .*
- (iii) *The set of symmetric bilinear forms on K^n .*
- (iv) *The set of symmetric $n \times n$ matrices on K^n .*

Example: When $n = 2$, one speaks of binary quadratic forms. Explicitly:

$$\begin{aligned} q(t_1, t_2) &= at_1^2 + bt_1t_2 + ct_2^2. \\ f_q(x_1, x_2) &= ax_1^2 + bx_1x_2 + cx_2^2 = [x_1x_2] \begin{bmatrix} a & \frac{b}{2} \\ \frac{b}{2} & c \end{bmatrix} \begin{bmatrix} x_1 \\ x_2 \end{bmatrix}. \\ B_f(x_1, x_2, y_1, y_2) &= ax_1y_1 + \frac{b}{2}x_1y_2 + \frac{b}{2}x_2y_1 + cx_2y_2. \end{aligned}$$

Two remarks are in order.

First, now that we know Theorem 1, it looks quite pedantic to distinguish between the polynomial $q(t_1, t_2)$ and the function $f_q(x_1, x_2)$, and we shall not do so from now on, rather writing a quadratic form as $q(x) = q(x_1, \dots, x_n)$.

Second, we note with mild distaste the presence of 2's in the denominator of the off-diagonal entries of the matrix. Arguably the formulas would be a little cleaner if we labelled our arbitrary binary quadratic form

$$q(x_1, x_2) = ax_1^2 + 2bx_1x_2 + cx_2^2;$$

this normalization is especially common in the classical literature (and similarly for quadratic forms in n variables). But again, since 2 is a unit in K , it is purely a cosmetic matter.²

The set of all n -ary quadratic forms over K has the structure of a K -vector space of dimension $\frac{n(n+1)}{2}$. We denote this space by Q_n .

2. ACTION OF $M_n(K)$ ON n -ARY QUADRATIC FORMS

Let $M_n(R)$ be the ring of $n \times n$ matrices with entries in K . Given any $M = (m_{ij}) \in M_n(K)$ and any n -ary quadratic form $q(x) = q(x_1, \dots, x_n)$, we define another n -ary quadratic form

$$(M \bullet q)(x) := q(Mx) = q(m_{11}x_1 + \dots + m_{1n}x_n, \dots, m_{n1}x_1 + \dots + m_{nn}x_n).$$

Thus we are simply making a linear change of variables. In terms of symmetric matrices, we have

$$(M \bullet q)(x) = x^T B_{M \bullet q} x = (Mx)^T B_q Mx = x^T M^T B_q Mx,$$

²This is to be contrasted with the case of quadratic forms over \mathbb{Z} , in which there is a technical distinction to be made between a quadratic form with integral coefficients a_{ij} and one with integral matrix coefficients b_{ij} . And things are much different when $2 = 0$ in K .

so that

$$(1) \quad B_{M \bullet q} = M^T B_q M.$$

This relation among matrices is classically known as **congruence**, and is generally distinct from the more familiar conjugacy relation $B \mapsto M^{-1}BM$ when M is invertible.³ This is an action in the sense that $I_n \bullet q = q$ and for all $M_1, M_2 \in M_n(K)$, we have

$$M_1 \bullet (M_2 \bullet q) = M_1 M_2 \bullet q$$

for all n -ary quadratic forms q . In other words, it is an action of the multiplicative monoid $(M_n(K), \cdot)$. Restricting to $GL_n(K)$, we get a group action.

We say that two quadratic forms q and q' are **equivalent** if there exists $M \in GL_n(K)$ such that $M \bullet q = q'$. This is evidently an equivalence relation in which the equivalence classes are precisely the $GL_n(K)$ -orbits. More generally, any subgroup $G \subset GL_n(K)$ certainly acts as well, and we can define two quadratic forms to be **G-equivalent** if they lie in the same G -orbit.

Example: We may consider $GL_n(\mathbb{Z})$ -equivalence of quadratic forms over \mathbb{Q} or \mathbb{R} .

Example: In general, we claim that the two binary forms $q_1(x, y) = xy$ and $q_2(x, y) = x^2 - y^2$ are $(GL_2(K))$ -equivalent. Indeed:

$$\begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix} \begin{bmatrix} 0 & \frac{1}{2} \\ \frac{1}{2} & 0 \end{bmatrix} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}.$$

Example: Viewing q_1 and q_2 as binary forms over \mathbb{Q} , they are *not* $GL_2(\mathbb{Z})$ -equivalent. If so, the sets $q_1(\mathbb{Z}^2)$ and $q_2(\mathbb{Z}^2)$ would be the same. But evidently $q_1(\mathbb{Z}^2) = \mathbb{Z}$, whereas a simple mod 4 argument shows that $2 \notin q_2(\mathbb{Z}^2)$.

Now suppose $M \in GL_n(K)$, and take determinants in (1) above. We get:

$$(2) \quad \det(B_{M \bullet q}) = \det(M)^2 \det(B_q).$$

So equivalent symmetric matrices need not have the same determinant.

Exercise: Find all fields K (of characteristic not equal to 2) for which any two equivalent quadratic fields have the same determinant.

However, we ought not give up so easily. On the one hand, having *zero determinant* is an equivalence invariant. We say that a quadratic form q is **degenerate** if $\det(B) = 0$. Thus degeneracy depends only on the equivalence class. Most quadratic forms arising in nature are nondegenerate. Moreover, we will shortly see a result which allows us to, in a canonical way, strip away the degenerate part of any quadratic form, leaving a nondegenerate form, so we may as well concentrate our attention on nondegenerate forms.

Suppose that q is nondegenerate, so $\det(B) \in K^\times$. Then (2) shows that the class

³The two coincide iff M is an orthogonal matrix, a remark which is helpful in relating the Spectral Theorem in linear algebra to the diagonalizability of quadratic forms. More on this shortly.

of $\det(B)$ in the quotient group $K^\times/K^{\times 2}$ is an equivalence invariant. The elements of the group $K^\times/K^{\times 2}$ are called **square classes** of K and play a quite prominent role in the algebraic theory of quadratic forms. By definition, for any quadratic form q , the **discriminant** $d(q)$ is the coset of $\det(B)$ in $K^\times/K^{\times 2}$.

So we have at the moment two invariants of a quadratic form: its dimension n , and its discriminant $d(q)$. Sometimes this is already enough to classify quadratic forms up to equivalence.

Definition: A field K is **quadratically closed** if every nonzero element of K is a square: $K^\times = K^{\times 2}$. Equivalently, K does not admit any quadratic field extension. So, for instance, the field \mathbb{C} of complex numbers is quadratically closed, as is any algebraically closed field or any separably closed field.

It turns out to be the case that over a quadratically closed field, any two nondegenerate quadratic forms of the same dimension are equivalent. In particular, any nondegenerate n -ary quadratic form over \mathbb{C} is $GL_n(\mathbb{C})$ -equivalent to $x_1^2 + \dots + x_n^2$.

Is the case for nondegenerate quadratic forms over \mathbb{R} ? Certainly not! For instance, consider the following forms:

$$\begin{aligned} q_1(x, y) &= x^2 + y^2. \\ q_2(x, y) &= x^2 - y^2. \\ q_3(x, y) &= -x^2 - y^2. \end{aligned}$$

I claim that no two of these forms are equivalent. Indeed, their corresponding quadratic functions have different images:

$$q_1(\mathbb{R}^2) = [0, \infty), \quad q_2(\mathbb{R}^2) = \mathbb{R}, \quad q_3(\mathbb{R}^2) = (-\infty, 0].$$

To explain carefully why this distinguishes the equivalence classes of forms, we introduce another fundamental definition: if $\alpha \in K^\times$, we say that a quadratic form q **represents** α iff α is in the image of the associated function, i.e., iff there exists $x \in K^n$ such that $q(x) = \alpha$. But now suppose that q represents α and let $M \in GL_n(R)$. Choose $x \in K^n$ such that $q(x) = \alpha$. Then

$$(M \cdot q)(M^{-1}x) = q(MM^{-1}x) = q(x) = \alpha.$$

That is:

Proposition 2. *Equivalent quadratic forms represent exactly the same set of scalars.*

Following T.-Y. Lam, we define

$$D(q) = q(K^n) \setminus \{0\}$$

to be the set of all nonzero values of K represented by q . Unlike the dimension or the determinant, $D(q)$ is a “second order” invariant, i.e., rather than being a single number or field element, it is a set of field elements.

On the other hand, $D(q) = D(q')$ need not imply that $q \cong q'$. Indeed, over \mathbb{R} the two forms

$$(3) \quad q_1 = x_1^2 - x_2^2 + x_3^2 + x_4^2, \quad q_2 = x_1^2 - x_2^2 - x_3^2 - x_4^2$$

have the same dimension, the same discriminant, and both represent all real numbers. The analyst's proof of this is to observe that they clearly represent arbitrarily large positive and arbitrarily small negative values and apply the Intermediate Value theorem. The algebraist's proof is that $q_1(x_1, x_2, 0, 0) = q_2(x_1, x_2, 0, 0) = x_1^2 - x_2^2$, which by Example X.X above is equivalent to $H(x, y) = xy$, which visibly represents all elements of K^\times . But in fact they are not equivalent, as was first established by the 19th century mathematician J.J. Sylvester. We will be able to establish this, and indeed to describe all isomorphism classes of quadratic forms over \mathbb{R} , once we have developed the basic theory of isotropic and hyperbolic subspaces.

Let q be an n -ary quadratic form over K . Then, with respect to the $GL_n(K)$ -action on the space of all n -ary quadratic forms, consider the **isotropy subgroup**

$$O_q = \{M \in GL_n(K) \mid M \bullet q = q\}.$$

Exercise: Let B be the symmetric matrix of the n -ary quadratic form q .

- Show that $O_q = \{M \in GL_n(K) \mid M^T B M = B\}$.
- Show that if $q \sim q'$, then O_q is conjugate (in $GL_n(K)$) to $O_{q'}$. In particular, the isomorphism class of O_q is an equivalence invariant of q .
- Suppose $q = x_1^2 + \dots + x_n^2$. Show that O_q is the standard orthogonal group $O(n)$.
- For those who know the definition of linear algebraic groups, confirm that O_q has the natural structure of a linear algebraic group. If q is nondegenerate, what is the dimension of O_q ?
- If K is a topological field, then O_q is a K -analytic Lie group. In case $K = \mathbb{R}$, show that O_q is compact iff q is either positive or negative definite.
- Let q_1 and q_2 be the real quadratic forms of (3). Are their isotropy subgroups isomorphic?

Similarities: Let $\mathbb{G}_m(K) = K^\times$ be the multiplicative group of K . Since \mathbb{G}_m is the center of $GL_n(K)$ – i.e., the scalar matrices – the above action of $GL_n(K)$ on Q_n restricts to an action of \mathbb{G}_m . However, there is *another* action of \mathbb{G}_m on Q_n which is relevant to the study of quadratic forms: namely $\alpha \cdot q = \alpha q$, i.e., we scale all of the coefficients of q by $\alpha \in \mathbb{G}_m$. If $q' = \alpha \cdot q$, we say that q and q' are **similar**.

The two actions are related as follows:

$$\alpha \bullet q = \alpha^2 \cdot q.$$

Since the \bullet action of $GL_n(K)$ preserves equivalence of quadratic forms (by definition), it follows that there is an induced action of $K^\times / K^{\times 2}$ on the set of equivalence classes.

Exercise: Let q be an n -ary quadratic form. Let $D(q) = \{\alpha \in \mathbb{G}_m \mid \alpha \cdot q \sim q\}$.

- Show that $D(q)$ is a subgroup of \mathbb{G}_m .
- Compute $D(q)$ for the form $x_1^2 + \dots + x_n^2$ over \mathbb{R} .
- Compute $D(q)$ for the hyperbolic plane $\mathbb{H} = x^2 - y^2$ over any field K .

3. THE CATEGORY OF QUADRATIC SPACES

In the previous section we saw some advantages of the symmetric matrix approach to quadratic forms: it gave a very concrete and transparent perspective on the actions of $GL_n(K)$ and \mathbb{G}_m on Q_n . In this section we turn to the coordinate-free approach to quadratic forms, that of a finite-dimensional K -vector space V endowed with a symmetric bilinear form $B : V \times V \rightarrow K$. To be precise, we call such a pair (V, B) a **quadratic space**.⁴

We pause to recall the meaning of nondegeneracy in the context of bilinear forms. Namely, let V be any K -vector space and $B : V \times V \rightarrow K$ be any bilinear form. Then B induces a linear map L_B from V to its dual space $V^\vee = \text{Hom}(V, K)$, namely $v \mapsto B(v, \cdot)$. We say that B is **nondegenerate** if L_B is an isomorphism. In this purely algebraic context, this is only possible if V is finite-dimensional – if V is an infinite-dimensional K -vector space, then $\dim V^\vee > \dim V$, so they are not isomorphic by any map, let alone by L_B – in which case, since $\dim V = \dim V^\vee$, it is equivalent to L_B being injective. In other words, to test for the nondegeneracy of a bilinear form B , it suffices to show that if $v \in V$ is every vector such that $B(v, w) = 0$ for all $w \in W$, then necessarily $v = 0$.

In the case of quadratic forms we have now given two definitions of nondegeneracy: one in terms of any associated symmetric matrix, and the other in terms of the associated symmetric bilinear form. So we had better check that they agree:

Proposition 3. *The two notions of nondegeneracy coincide for quadratic forms: that is, a symmetric bilinear form B on a finite-dimensional vector space is nondegenerate iff its defining symmetric matrix (with respect to any basis of V) has nonzero determinant.*

Proof. Choose a basis e_1, \dots, e_n for V and define a matrix B with (i, j) entry $b_{ij} = B(e_i, e_j)$. Then we have

$$B(v, w) = w^T Bv.$$

If the matrix B is singular, then there exists a nonzero $v \in V$ such that $Bv = 0$, and then the above equation implies $B(v, w) = 0$ for all $w \in W$. Conversely, if B is nonsingular, then for any nonzero $v \in V$, Bv is not the zero vector, so there exists at least one i , $1 \leq i \leq n$ for which the i th component of Bv is nonzero. Then $B(v, e_i) \neq 0$. \square

A **map** of quadratic spaces $(V, B_V) \rightarrow (W, B_W)$ is a K -linear map $L : V \rightarrow W$ which “respects the bilinear form structure”: precisely:

$$\forall v_1, v_2 \in V, B_W(L(v_1), L(v_2)) = B_V(v_1, v_2).$$

An **isometric embedding** is a morphism of quadratic spaces whose underlying linear map is injective.

Proposition 4. *Let $f : (V, B_V) \rightarrow (W, B_W)$ be a map of quadratic spaces. If B_V is nondegenerate, then f is an isometric embedding.*

⁴Probably it would be even more pedantically correct to call it a “symmetric bilinear space”, but this is not the standard terminology. As we have seen, the data of B and the associated quadratic function q are interchangeable in our present context.

Proof. Let $v \in V$ be such that $f(v) = 0$. Then, for all $v' \in V$, we have

$$0 = B_W(0, f(v')) = B_W(f(v), f(v')) = B_V(v, v').$$

Thus by the definition of nondegeneracy we must have $v = 0$. \square

Exercise: Let $\iota : (V, B_V) \rightarrow (W, B_W)$ be an isometric embedding of quadratic spaces. Show that the following are equivalent:

(i) There exists an isometric embedding $\iota' : (W, B_W) \rightarrow (V, B_V)$ such that $\iota' \circ \iota = 1_V$, $\iota \circ \iota' = 1_{W'}$.

(ii) ι is surjective.

An isometric embedding satisfying these conditions will be called an **isometry**.

The **category of quadratic spaces** over K has as its objects the quadratic spaces (V, B_V) and morphisms isometric embeddings between quadratic spaces.

If (V, B_V) is a quadratic space and $W \subset V$ is a K -subspace, let B_W be the restriction of B_V to W .

Exercise: Show that $(W, B_W) \hookrightarrow (V, B_V)$ is an isometric embedding.

Does the category of quadratic spaces have an initial object? Yes, a zero-dimensional vector space $V = \{0\}$ with the unique (zero) map $V \times V \rightarrow K$. Note that this bilinear form is nondegenerate according to the definition. (Presumably the determinant of a “ 0×0 ” matrix is 1, but we do not insist upon this.) This may seem like a pointless convention, but it is not: it will be needed later to give the identity element of the Witt group of K .

Exercise: Show that the category of quadratic spaces over K has no final object.

The category of quadratic spaces admits finite direct sums. In other words, given two quadratic spaces V and W , there exists a quadratic space $V \oplus W$ together with isometries $V \rightarrow V \oplus W$, $W \rightarrow V \oplus W$, such that every pair of isometries $V \rightarrow Z$, $W \rightarrow Z$ factors uniquely through $V \oplus W$. Indeed, the underlying vector space on $V \oplus W$ is the usual vector space direct sum, and the bilinear form is

$$B_{V \oplus W}((v_1, w_1), (v_2, w_2)) := B_V(v_1, v_2) + B_W(w_1, w_2).$$

Fixing bases e_1, \dots, e_m of V and e'_1, \dots, e'_n of W , if the symmetric matrices for the B_V and B_W are B_1 and B_2 , respectively, then the matrix for $B_{V \oplus W}$ is the block matrix

$$\begin{bmatrix} B_1 & 0 \\ 0 & B_2 \end{bmatrix}.$$

It is common to refer to the categorical direct sum of quadratic spaces as the **orthogonal direct sum**. However, in our work, whenever we write down an external direct sum, we will always mean this “orthogonal” direct sum.

One can also define a tensor product of quadratic spaces (V, B_V) and (W, B_W) . Again the underlying vector space is the usual tensor product $V \otimes W$, and the bilinear form is given on basis elements as

$$B_{V \otimes W}(v_1 \otimes w_1, v_2 \otimes w_2) := B_V(v_1, v_2) \cdot B_W(w_1, w_2),$$

and extended by bilinearity. The associated symmetric matrix is the **Kronecker product**. In particular, if with respect to some bases $(e_i), (e'_j)$ of V and W we have diagonal matrices $B_1 = \Delta(a_1, \dots, a_m), B_2 = \Delta(b_1, \dots, b_n)$, then the matrix of $B_{V \otimes W}$ is the diagonal $mn \times mn$ matrix $\Delta(a_i b_j)$.

4. ORTHOGONALITY IN QUADRATIC SPACES

Let (V, B) be a quadratic space, and let W_1, W_2 be subspaces. We say W_1 and W_2 are **orthogonal subspaces** if for all $v_1 \in W_1$, we have $v_2 \in W_2, B(v_1, v_2) = 0$. The notation for this is $W_1 \perp W_2$.

Exercise: Let $(V_1, B_1), (V_2, B_2)$ be quadratic spaces. Identifying V_i with its isometric image in $V_1 \oplus V_2$, show that $V_1 \perp V_2$. State and prove a converse result.

Let (V, B) be a quadratic space, and $W \subset V$ a subspace. We define the **orthogonal complement**

$$W^\perp = \{v \in V \mid \forall w \in W, B(v, w) = 0\}.$$

In other words, W^\perp is the maximal subspace of V which is orthogonal to W .

Exercise: Show that $W \mapsto W^\perp$ gives a self-dual Galois connection.

Example: If $K = \mathbb{R}$, a quadratic space (V, B) is an **inner product space** if B is positive definite: $B(v, v) \geq 0$ for all $v \in V$ and $B(v, v) = 0 \implies v = 0$. In this special case the notions of orthogonal direct sum, orthogonal complement (and orthogonal basis!) are familiar from linear algebra.

However, in general a quadratic space may have nonzero vectors v for which $B(v, v) = 0$, and this lends the theory a different flavor.

Definition: Let (V, B) be a nondegenerate quadratic space. A vector $v \in V$ is said to be **isotropic** if $q(v) = B(v, v) = 0$ and **anisotropic** otherwise. V itself is said to be **isotropic** if there exists a nonzero isotropic vector and otherwise **anisotropic**. Thus an inner product space is (in particular) an anisotropic real quadratic space.

Definition: The **radical of V** is $\text{rad}(V) = V^\perp$.

Exercise: Show that a quadratic space (V, B) is nondegenerate iff $\text{rad}(V) = 0$.

Exercise: Show that $\text{rad}(V \oplus W) = \text{rad}(V) \oplus \text{rad}(W)$.

Proposition 5. (*Radical Splitting*) Let (V, B) be any quadratic space. Then there exists a nondegenerate subspace W such that

$$V = \text{rad}(V) \oplus W$$

is an internal orthogonal direct sum decomposition.

Proof. Since by definition $\text{rad}(V)$ is orthogonal to all of V , any complementary subspace W to $\text{rad}(V)$ in the sense of usual linear algebra will give rise to an orthogonal direct sum decomposition $V = \text{rad}(V) \oplus W$. It follows from the preceding exercise that W is nondegenerate. \square

Remark: The complementary subspace W is in general far from being unique.

Remark: It is of interest to have an algorithmic version of this result. This will follow immediately from the algorithmic description of the diagonalization procedure given following Theorem 9.

Proposition 6. *Let (V, B) be a quadratic space, and $W \subset_K V$ a nondegenerate subspace. Then $V = W \oplus W^\perp$.*

Proof. By Exercise X.X, since W is nondegenerate, $\text{rad}(W) = W \cap W^\perp = 0$, so it makes sense to speak of the subspace $W \oplus W^\perp$ of V . Now let $z \in V$, and consider the associated linear form $Z \in \text{Hom}(W, K)$ given by $Z(v) := B(z, v)$. Since W is nondegenerate, there exists $w \in W$ such that for all $v \in W$,

$$Z(v) = B(z, v) = B(w, v).$$

Thus $w' = z - w \in W^\perp$ and $z = w + w'$. □

Proposition 7. *Let (V, B) be a nondegenerate quadratic space. Then for every subspace $W \subset V$ we have $(W^\perp)^\perp = W$.*

Proof. That $W \subset (W^\perp)^\perp$ is a tautology: indeed every vector w in W is perpendicular to every vector v that is perpendicular to every vector in W ! (Note that this does not use the nondegeneracy.)

Next, consider the linear map $L : V \rightarrow W^\vee$ given by $v \mapsto (w \mapsto B(v, w))$. Evidently $\text{Ker}(L) = W^\perp$. Moreover, this map factors as the composite $V \rightarrow V^\vee \rightarrow W^\vee$, where the first map is surjective by nondegeneracy and the second map is evidently surjective (any linear form on a subspace extends to a linear form on the whole space). Therefore L is surjective, so we get

$$\dim V = \dim W^\perp + \dim W^\vee = \dim W^\perp + \dim W.$$

Applying the same result with W^\perp in place of W , we get

$$\dim V = \dim(W^\perp)^\perp + \dim W^\perp,$$

and thus $\dim W = (\dim W^\perp)^\perp$. An inclusion between two vector spaces of the same finite dimension is necessarily an isomorphism, so the result follows. □

Corollary 8. *For a nondegenerate quadratic space (V, B) and $W \subset_K V$, TFAE:*

- (i) $W \cap W^\perp = 0$.
- (ii) W is nondegenerate.
- (iii) W^\perp is nondegenerate.

Exercise X.X: Prove Corollary 8.

5. DIAGONALIZABILITY OF QUADRATIC FORMS

Let $q \in Q_n$ be an n -ary quadratic form. We say that q is **diagonal** if either of the following equivalent conditions are satisfied:

- (D1) Its defining quadratic polynomial is of the form $\sum_i a_i x_i^2$.
- (D2) Its defining symmetric matrix is diagonal.

Exercise: Show that a diagonal form is nondegenerate iff $a_i \neq 0$ for all i .

Exercise: a) Let $\sigma \in S_n$ be a permutation, and let M_σ be the matrix obtained by applying the permutation σ to the columns of the $n \times n$ identity matrix. Show that if $D = \Delta(a_1, \dots, a_n)$ is any diagonal matrix, then $M_\sigma^T D M_\sigma = \Delta(a_{\sigma(1)}, \dots, a_{\sigma(n)})$. In particular, reordering the diagonal entries of a diagonal quadratic form does not change its equivalence class.

b) For $\alpha \in K^\times$, find an explicit matrix M such that

$$M^T \Delta(a_1, \dots, a_n) M = \Delta(\alpha^2 a_1, \dots, \alpha^2 a_n).$$

c) Show that any two nondegenerate diagonal quadratic forms over a quadratically closed field are equivalent.

d) Use the spectral theorem from linear algebra to show that any real quadratic form is equivalent to a diagonal form. Deduce that any nondegenerate real quadratic form is equivalent to $\Delta(1, \dots, 1, -1, \dots, -1)$ where there are $0 \leq r$ instances of 1 and $0 \leq s$ instances of -1 , with $r + s = n$.

In general, let us say that a quadratic form $q \in Q_n(K)$ is **diagonalizable** if it is $GL_n(K)$ -equivalent to a diagonal quadratic form. (By convention, we decree the trivial quadratic form to be diagonalizable.) We can now state and prove one of the most basic results of the theory.

Theorem 9. *Every quadratic form over K is diagonalizable.*

Before giving the proof, let us state the result in two equivalent forms, both using the language of quadratic spaces. A diagonalizable quadratic space (V, B) is one for which there exist one-dimensional subspaces W_1, \dots, W_n such that

$$V = W_1 \oplus \dots \oplus W_n.$$

Equivalently, there exists an **orthogonal basis** (e_1, \dots, e_n) for V , i.e., one for which $B(e_i, e_j) = 0$ for all $i \neq j$.

Proof. We go by induction on the dimension of V , the case $n = 0$ being trivial. Suppose the result is true for all quadratic spaces over K of dimension less than n , and let (V, B) be an n -dimensional quadratic space. If B is identically zero, the result is obvious, so let us assume not. If the associated quadratic form $q(x) = B(x, x)$ were identically zero, then by the polarization identity, so would B be. Thus we may assume that there exists $v_1 \in V$ with $q(v_1) \neq 0$. Then $W_1 = \langle v_1 \rangle$ is nondegenerate, and by Proposition 6 we have $V = W_1 \oplus W_1^\perp$. We are finished by induction! \square

This theorem and proof can be restated in the language of symmetric matrices. Namely, let B be an $n \times n$ symmetric matrix with coefficients in K . Then by performing a sequence of simultaneous row-and-column operations on B – equivalently, multiplying on the right by an elementary matrix E and on the left by its transpose – we can bring B to diagonal form.

Here is an algorithm description: if $B = 0$, we're done. Otherwise, there exists a nonzero entry b_{ij} . By taking E to be the elementary matrix corresponding to the transposition (ij) , we get a nonzero entry $\alpha = b'_{j1}$. If $j = 1$, great. If not, then by adding the j th row to the first row – and hence also the j th column to the first column – we get a matrix B'' with $b''_{11} = 2\alpha$ (which is nonzero since K does not have characteristic 2!). Then, since every element of K is a multiple of 2α , by usual row (+ column) reduction we can get an congruent matrix B''' with $b'''_{1j} = 0$ for all

$j > 1$. In the above proof, this corresponds to finding an anisotropic vector and splitting off its orthogonal complement. Now we proceed by induction.

Remark: As alluded to above, Theorem 9 is direct generalization of Proposition 5 (Radical Splitting), and the algorithmic description given above in particular gives an effective procedure that Proposition.

Remark X.X: We note for future use the following consequence of the proof: let V be a nondegenerate quadratic space, and let $\alpha \in K^\times$ be such that there exists $v \in V$ with $q(v) = \alpha$. Then V is isometric to a quadratic space $\langle \alpha, \alpha_2, \dots, \alpha_n \rangle$.

Exercise: Show that the usual Gram-Schmidt process from linear algebra works to convert any basis to an orthogonal basis, provided we have $q(x) \neq 0$ for all $x \neq 0$.

In view of Theorem 9 it will be useful to introduce some streamlined notation for diagonal quadratic forms. For any $\alpha \in K$, we let $\langle \alpha \rangle$ denote the one-dimensional quadratic space equipped with a basis vector e with $q(e) = \alpha$. For $\alpha_1, \dots, \alpha_n$, we write $\langle a_1, \dots, a_n \rangle$ for $\bigoplus_{i=1}^n \langle a_i \rangle$, or in other words, for the quadratic form corresponding to the matrix $\Delta(a_1, \dots, a_n)$.

Exercise: Convert this proof into an algorithm for diagonalizing quadratic forms. (Hint: explain how to diagonalize a corresponding symmetric matrix using simultaneous row and column operations.)

Remark: The result of Theorem 9 does not hold for fields of characteristic 2. For instance, the binary quadratic form $q(x, y) = x^2 + xy + y^2$ over \mathbb{F}_2 is not $GL_2(\mathbb{F}_2)$ -equivalent to a diagonal form. One way to see this is to observe that q is anisotropic over \mathbb{F}_2 , whereas any diagonal binary form is isotropic: certainly $ax^2 + by^2$ is isotropic if $ab = 0$; and otherwise $ax^2 + by^2 = (x + y)^2$ and an isotropic vector is $(x, y) = (1, 1)$.

6. ISOTROPIC AND HYPERBOLIC SPACES

Recall that a quadratic space V is **isotropic** if it is nondegenerate and there exists a nonzero vector v such that $q(v) = 0$.

The basic example of an isotropic space is the hyperbolic plane, given by $H(x, y) = xy$, or in equivalent diagonal form as $H(x, y) = \frac{1}{2}x^2 - \frac{1}{2}y^2$. A quadratic space is **hyperbolic** if it is isometric to a direct sum of hyperbolic planes.

A subspace W of a quadratic space (V, B) is said to be **totally isotropic** if $B|_W \equiv 0$. We have some misgivings about this terminology: if $0 \neq W \subset V$ is a totally isotropic subspace, then viewed as a quadratic space in its own right, W is *not* isotropic since it is degenerate. But the terminology is standard so we will not attempt to change it.

We come now to what is perhaps the first surprising result in the structure theory of nondegenerate quadratic forms. It says that, in some sense, the hyperbolic plane is the *only* example of an isotropic quadratic space. More precisely:

Theorem 10. *Let (V, B) be an isotropic quadratic space. Then there is an isometric embedding of the hyperbolic plane into (V, B) .*

Proof. Since B is nondegenerate, there exists $w \in V$ with $B(u_1, w) \neq 0$. By suitably rescaling w , we may assume that $B(u_1, w) = 1$. We claim that there exists a unique $\alpha \in K$ such that $q(\alpha u_1 + w) = 0$. Indeed,

$$q(\alpha u_1 + w) = \alpha^2 q(u_1) + 2\alpha B(u_1, w) + q(w) = 2\alpha + q(w),$$

so we may take $\alpha = \frac{-q(w)}{2}$. Putting $u_2 = \alpha u_1 + w$, we have $q(u_1) = q(u_2) = 0$ and

$$B(u_1, u_2) = B(u_1, \alpha u_1 + w) = \alpha q(u_1) + B(u_1, w) = 1,$$

so that the quadratic form q restricted to the span of u_1 and u_2 is, with respect to the basis u_1, u_2 , the hyperbolic plane: $q(xu_1 + yu_2) = xy$. \square

Here is a generalization.

Theorem 11. *Let (V, B) be a nondegenerate quadratic space and $U \subset V$ a totally isotropic subspace with basis u_1, \dots, u_m . Then there exists a totally isotropic subspace U' , disjoint from U , with basis u'_1, \dots, u'_m such that $B(u_i, u'_j) = \delta(i, j)$. In particular $\langle U, U' \rangle \cong \bigoplus_{i=1}^m \mathbb{H}$.*

Proof. We proceed by induction on m , the case $m = 1$ being Theorem 10. Since B is nondegenerate, there exists $w \in V$ with $B(u_1, w) \neq 0$. By suitably rescaling w , we may assume that $B(u_1, w) = 1$. We claim that there exists a unique $\alpha \in K$ such that $q(\alpha u_1 + w) = 0$. Indeed,

$$q(\alpha u_1 + w) = \alpha^2 q(u_1) + 2\alpha B(u_1, w) + q(w) = 2\alpha + q(w),$$

so we may take $\alpha = \frac{-q(w)}{2}$. Putting $u_2 = \alpha u_1 + w$, we have $q(u_1) = q(u_2) = 0$ and

$$B(u_1, u_2) = B(u_1, \alpha u_1 + w) = \alpha q(u_1) + B(u_1, w) = 1,$$

so that the quadratic form q restricted to the span of u_1 and u_2 is, with respect to the basis u_1, u_2 , the hyperbolic plane: $q(xu_1 + yu_2) = xy$.

Now assume the result is true for all totally isotropic subspaces of dimension smaller than m . Let $W = \langle u_2, \dots, u_m \rangle$. If we had $W^\perp \subseteq \langle u_1 \rangle^\perp$, then taking ‘perps’ and applying Proposition 7 we would get $\langle u_1 \rangle \subset W$, a contradiction. So there exists $v \in W^\perp$ such that $B(u_1, v) \neq 0$. As above, the subspace H_1 spanned by u_1 and v is a hyperbolic plane and hence contains a vector u'_1 such that $B(u'_1, u'_1) = 0$, $B(u_1, u'_1) = 1$. By construction we have $H_1 \subset W^\perp$; taking perps gives $W \subset H_1^\perp$. Since H_1^\perp is again a nondegenerate quadratic space, we may apply the induction hypothesis to W to find a disjoint totally isotropic subspace $W' = \langle u'_2, \dots, u'_n \rangle$ with each $\langle u_i, u_i \rangle$ a hyperbolic plane. \square

The following is an immediate consequence.

Corollary 12. *Let W be a totally isotropic subspace of a nondegenerate quadratic space V . Then $\dim W \leq \frac{1}{2} \dim V$.*

It will be convenient to have a name for the subspace U' shown to exist under the hypotheses of Theorem 11, but there does not seem to be any standard terminology. So, to coin a phrase, we will call U' an **isotropic supplement** of U .

We define a quadratic form q to be **universal** if it represents every element of K^\times . Evidently the hyperbolic plane $\mathbb{H} = xy$ is universal: take $x = \alpha$, $y = 1$.

Corollary 13. *Any isotropic quadratic space is universal.*

Proof. This follows immediately from Theorem 10. \square

Exercise X.X: Give an example of a universal quadratic form which is not anisotropic.

Corollary 14. *For any $\alpha \in K^\times$, the rescaling $\alpha \cdot \mathbb{H}$ is isomorphic to \mathbb{H} .*

Proof. $\alpha \cdot \mathbb{H}$ is a two-dimensional isotropic quadratic space. Apply Theorem 10. \square

Corollary 15. *Any quadratic space V admits an internal orthogonal direct sum decomposition*

$$V \cong \text{rad}(V) \oplus \bigoplus_{i=1}^n \mathbb{H} \oplus V',$$

where $n \in \mathbb{N}$ and V' is anisotropic.

Proof. By Proposition 5 we may assume V is nondegenerate. If V is anisotropic, we are done ($n = 0$). If V is isotropic, then by Theorem 10 there is a hyperbolic subspace $\mathbb{H} \subset V$. Since \mathbb{H} is nondegenerate, by Proposition 6 $V = \mathbb{H} \oplus \mathbb{H}^\perp$, with \mathbb{H}^\perp nondegenerate of smaller dimension. We are finished by induction. \square

Remark: This is half (the easier half) of the **Witt Decomposition Theorem**. The other, deeper, half is a uniqueness result: the number n and the isometry class of V' are independent of the choice of direct sum decomposition.

Theorem 16. (*First Representation Theorem*) *Let q be a regular quadratic form, and let $\alpha \in K^\times$. TFAE:*

- (i) q represents α .
- (ii) $q \oplus \langle -\alpha \rangle$ is isotropic.

Proof. If q represents α , then by Remark X.X, q is equivalent to a form $\langle \alpha, \alpha_2, \dots, \alpha_n \rangle$. Then $q \oplus \langle -\alpha \rangle$ contains (an isometric copy of) $\langle \alpha, -\alpha \rangle = \alpha \cdot \mathbb{H} \cong \mathbb{H}$ so is isotropic. Conversely, we may assume $q = \langle \alpha_1, \dots, \alpha_n \rangle$, and our assumption is that there exist x_0, \dots, x_n , not all 0, such that

$$-\alpha x_0^2 + \alpha_1 x_1^2 + \dots + \alpha_n x_n^2 = 0.$$

There are two cases. If $x_0 \neq 0$, then $\alpha_1(x_1/x_0)^2 + \dots + \alpha_n(x_n/x_0)^2 = \alpha$, so q represents α . If $x_0 = 0$, then $x = (x_1, \dots, x_n)$ is a nonzero isotropic vector for q , so q is isotropic and thus represents every element of K^\times , including α . \square

This has the following easy consequence, the proof of which is left to the reader.

Corollary 17. *For a field K and $n \in \mathbb{Z}^+$, TFAE:*

- (i) *Every nondegenerate n -ary quadratic form over K is universal.*
- (ii) *Every nondegenerate $(n + 1)$ -ary quadratic form over K is isotropic.*

Lemma 18. *Let $m, n \in \mathbb{Z}^+$ and let $f(x_1, \dots, x_m)$ and $g(y_1, \dots, y_n)$ be nondegenerate quadratic forms. Suppose that the form $f \oplus (-1) \cdot g = f(x_1, \dots, x_m) - g(y_1, \dots, y_n)$ is isotropic. Then there exists $\alpha \in K^\times$ which is simultaneously represented by both f and g .*

Proof. Since $f \oplus -g$ is isotropic, there are $x \in K^m$, $y \in K^n$, not both zero, such that $f(x) = g(y)$. If this common value is nonzero, we may take this to be α . Otherwise $f(x) = g(y) = 0$ and at least one of f and g is isotropic: say it is f . Then f contains \mathbb{H} and therefore represents every element of K^\times , so in particular represents $g(e_1) \neq 0$, where e_1, \dots, e_n is an orthogonal basis for K^n . \square

7. WITT'S THEOREMS: STATEMENTS AND CONSEQUENCES

In this section we state the fundamental result of Witt on which the entire algebraic theory of quadratic forms is based. It turns out that there are two equivalent statements of Witt's result: as an **extension theorem** and as a **cancellation theorem**. We now state these two theorems, demonstrate their equivalence, and derive some important consequences. The proof of the Witt Cancellation Theorem is deferred to the next section.

Theorem 19. (*Witt Cancellation Theorem*) *Let U_1, U_2, V_1, V_2 be quadratic spaces, with V_1 and V_2 isometric. If $U_1 \oplus V_1 \cong U_2 \oplus V_2$, then $U_1 \cong U_2$.*

Theorem 20. (*Witt Extension Theorem*) *Let X_1 and X_2 be isometric quadratic spaces. Suppose we are given orthogonal direct sum decompositions $X_1 = U_1 \oplus V_1$, $X_2 = U_2 \oplus V_2$ and an isometry $f : V_1 \rightarrow V_2$. Then there exists an isometry $F : X_1 \rightarrow X_2$ such that $F|_{V_1} = f$ and $F(U_1) = U_2$.*

Let us demonstrate the equivalence of Theorems 20 and 19. Assume Theorem 20, and let U_1, U_2, V_1, V_2 be as in Theorem 19. Put $X_1 = U_1 \oplus V_1$, $X_2 = U_2 \oplus V_2$, and let $f : V_1 \rightarrow V_2$ be an isometry. By Theorem 20, U_1 and U_2 are isometric.

Conversely, assume Theorem 19, and let $X_1, X_2, U_1, U_2, V_1, V_2$ be as in Theorem 20. Then Witt Cancellation implies that $U_1 \cong U_2$, say by an isometry $f_U : U_1 \rightarrow U_2$. Then $F = f_U \oplus f : X_1 \rightarrow X_2$ satisfies the conclusion of Theorem 20.

Remark: The statement of Theorem 20 is taken from [Cop, Prop. VII.18]. The advantage has just been seen: its equivalence with the Witt Cancellation Theorem (in the most general possible form) is virtually immediate. Each of the following results, which contain further assumptions on nondegeneracy, is sometimes referred to in the literature as ‘‘Witt’s Isometry Extension Theorem’’.

Corollary 21. *Let X be a quadratic space and $V_1, V_2 \subset X$ be nondegenerate subspaces. Then any isometry $f : V_1 \rightarrow V_2$ extends to an isometry F of X .*

Proof. Put $U_1 = V_1^\perp$, $U_2 = V_2^\perp$. Because of the assumed nondegeneracy of V_1 and V_2 , we have $X = U_1 \oplus V_1 = U_2 \oplus V_2$. Theorem 20 now applies with $X = X_1 = X_2$ to give an isometry F of X extending f . \square

Remark: The conclusion of Corollary 21 may appear weaker than that of Theorem 20, but this is not so. Since V_1 and V_2 are nondegenerate, any extended isometry F must map U_1 to U_2 : since $f(V_1) = V_2$, $f(U_1) = f(V_1^\perp) = f(V_1)^\perp = V_2^\perp = U_2$.

Corollary 22. *Let X be a nondegenerate quadratic space and $Y_1 \subset X$ any subspace. Then any isometric embedding $f : Y_1 \rightarrow X$ extends to an isometry F of X .*

Proof. Put $Y_2 = f(Y_1)$. Note that if Y_1 is nondegenerate, then so is Y_2 and we may apply Corollary 21. Our strategy of proof is to reduce to this case. Using Proposition 5 we may write $Y_1 = U_1 \oplus W_1$ with U_1 totally isotropic and W_1 nondegenerate. Evidently $U_1 \subset W_1^\perp$; since X and W_1 are nondegenerate, by Corollary 8 W_1^\perp is nondegenerate as well. We may therefore apply Theorem 11 to find an isotropic supplement U'_1 to U_1 inside W_1^\perp . Let $V_1 = \langle U_1, U'_1 \rangle \oplus W_1$. Then V_1 is nondegenerate and the natural inclusion $Y_1 \hookrightarrow V_1$ is, of course, an isometric embedding. We may apply the same reasoning to $Y_2 \cong U_2 \oplus W_2$ to get an isotropic supplement U'_2 to U_2 inside W_2^\perp and $Y_2 \hookrightarrow V_2 = \langle U_2, U'_2 \rangle \oplus W_2$. Since $U_i = \text{rad}(Y_i)$ and Y_1 and Y_2

are isometric, $U_1 \cong U_2$, and then $\langle U_1, U_1' \rangle$ and $\langle U_2, U_2' \rangle$ are hyperbolic spaces of the same dimension, hence isometric. By Witt Cancellation, $W_1 \cong W_2$. It follows that V_1 and V_2 are isometric, and we finish by applying Corollary 21. \square

This has the following interesting consequence.

Theorem 23. *Let V be a nondegenerate quadratic space. Then, for any $0 \leq d \leq \frac{1}{2} \dim V$, the group of isometries of V acts transitively on the set of all totally isotropic subspaces of dimension d .*

The following exercise shows that some nondegeneracy assumption is needed in order to be sure that isometries can be extended.

Exercise: Let X be the quadratic space $\langle 1, -1, 0 \rangle$. Let $V_1 = \langle e_1 + e_2 \rangle$ and $V_2 = \langle e_3 \rangle$.
 a) Show that there exists an isometry $f : V_1 \rightarrow V_2$.
 b) Show that f does not extend to an isometry of X .

Corollary 21 is equivalent to a weak version of Witt Cancellation in which we make the additional hypothesis that V_1 (hence also V_2) is nondegenerate. The one application of being able to cancel also degenerate subspaces is the following result.

Theorem 24. (*Witt Decomposition Theorem*) *Let (V, B) be a quadratic space. Then there exists an orthogonal direct sum decomposition*

$$V \cong \text{rad}(V) \oplus \bigoplus_{i=1}^I \mathbb{H} \oplus V',$$

where V' is an anisotropic quadratic space. Moreover the number $I = I(V)$ and the isometry class of V' are independent of the choice of decomposition.

Proof. The existence of such a decomposition has already been shown: Corollary 15. The uniqueness follows immediately from the Witt Cancellation Theorem and the fact that any isotropic quadratic form contains an isometrically embedded copy of the hyperbolic plane (Theorem 10). \square

Remark: Theorem 24 is a good excuse for restricting attention to nondegenerate quadratic forms. Indeed, unless indication is expressly given to the contrary, **we will henceforth consider only nondegenerate quadratic forms.**

Thus, assuming that V is nondegenerate, the natural number $I(V)$ is called the **Witt index** of V . By Exercise X.X, it can be characterized as the dimension of any maximal totally isotropic subspace of V .

Theorem 25. (*Sylvester's Law of Nullity*)

Let $n \in \mathbb{Z}^+$ and $r, s \in \mathbb{N}$ with $r + s = n$. Define

$$q_{r,s} = [r]\langle 1 \rangle \oplus [s]\langle -1 \rangle,$$

i.e., the nondegenerate diagonal form with r 1's and s -1 's along the diagonal. Then any n -ary quadratic form is isomorphic to exactly one quadratic form $q_{r,s}$.

Exercise: Use the Witt Decomposition Theorem to prove Theorem 25.

8. ORTHOGONAL GROUPS, REFLECTIONS AND THE PROOF OF WITT
CANCELLATION

Orthogonal group of a quadratic space: let V be a quadratic space. Then the **orthogonal group** $O(V)$ is, by definition, the group of all isometries from V to V , i.e., the group of linear automorphisms M of V such that for all $v, w \in V$, $B(v, w) = B(Mv, Mw)$. Identifying V with K^n (i.e., choosing a basis) and B with the symmetric matrix $(B(e_i, e_j))$, the definition becomes

$$\begin{aligned} O(V) &= \{M \in \text{GL}_n(K) \mid \forall v, w \in K^n, v^T B w = v^T M^T B M w\} \\ &= \{M \in \text{GL}_n(K) \mid M \bullet q = q\} \end{aligned}$$

where q is the associated quadratic form. In other words, $O(V)$ is none other than the **isotropy group** O_q of q for the $\text{GL}_n(K)$ -action on n -ary quadratic forms.

Remark: It is tempting to try to provide a conceptual explanation for the somewhat curious coincidence of isotropy groups and automorphism groups. But this would involve a digression on the groupoid associated to a G -set, a bit of abstract nonsense which we will spare the reader...for now.

Although we introduced isotropy groups in §1.2 and remarked that the isotropy group of the form $[n]\langle 1 \rangle$ is the standard orthogonal group $O(n)$, we did not provide much information about orthogonal groups over an arbitrary field. Essentially all we know so far is that equivalent forms have conjugate (in particular isomorphic) orthogonal groups. Here is one further observation, familiar from linear algebra.

By definition, for all $M \in O(V)$ we have $M^T B M = B$; taking determinants gives $\det(M)^2 \det B = \det B$. If (V, B) is nondegenerate, then $\det B \neq 0$, and we conclude that $\det M = \pm 1$. This brings us to:

Proposition 26. *Let V be a nondegenerate quadratic space. We have a short exact sequence of groups*

$$1 \rightarrow O^+(V) \rightarrow O(V) \xrightarrow{\det} \{\pm 1\} \rightarrow 1.$$

Proof. In other words, $O^+(V)$ is by definition the subgroup of matrices in $O(V)$ of determinant 1. It remains to see that there are also elements in $O(V)$ with determinant -1 . However, we may assume that V is given by a diagonal matrix, and then $M = \Delta(1, \dots, 1, -1)$ is such an element. \square

Exercise: Show that if V is degenerate, $O(V)$ contains matrices with determinant other than ± 1 .

Definition: We write $O^-(V)$ for the elements of $O(V)$ of determinant -1 . Of course this is not a subgroup, but rather the unique nontrivial coset of $O^+(V)$.

We now introduce a fundamental construction which will turn out to generalize the seemingly trivial observation that if q is diagonal, $\Delta(1, \dots, 1, -1)$ is an explicit element in $O^-(V)$. Indeed, let (V, B, q) be any quadratic space, and let $v \in V$ be an anisotropic vector. We define an element $\tau_v \in O^-(V)$ as follows:

$$\tau_v : x \mapsto x - \frac{2B(x, v)}{q(v)}v.$$

Note that in the special case in which $V = \mathbb{R}^n$ and B is positive definite, τ_v is reflection through the hyperplane orthogonal to v . In the general case we call τ_v a **hyperplane reflection**. We justify this as follows:

Step 1: τ_v is a linear endomorphism of V . (An easy verification.)

Step 2: Put $W = \langle v \rangle^\perp$, so that $V = W \oplus \langle v \rangle$. Let e_1, \dots, e_{n-1} be an orthogonal basis for W , so that (e_1, \dots, e_{n-1}, v) is an orthogonal basis for V . Then, with respect to this basis, the matrix representation of τ_v is indeed $\Delta(1, \dots, 1, -1)$. It follows that τ_v is an isometry, $\tau_v^2 = 1_V$ and $\det(\tau_v) = -1$.

Exercise: Let $\sigma \in O(V)$ and $v \in V$ an anisotropic vector. Show that $\sigma\tau_v\sigma^{-1} = \tau_{\sigma v}$.

Proposition 27. *Let (V, B, q) be any quadratic space. Suppose that $x, y \in V$ are anisotropic vectors with $q(x) = q(y)$. Then there exists $\tau \in O(V)$ such that $\tau(x) = y$.*

Proof. We compute

$$q(x+y) + q(x-y) = B(x+y, x+y) + B(x-y, x-y) = 2q(x) + 2q(-y) = 4q(x) \neq 0.$$

Therefore $q(x+y)$ and $q(x-y)$ are not both zero. Let us first suppose that $q(x-y) \neq 0$. Then

$$q(x-y) = B(x, x) + B(y, y) - 2B(x, y) = 2B(x, x) - 2B(x, y) = 2B(x, x-y),$$

so that

$$\tau_{x-y} x = x - \frac{2B(x, x-y)}{q(x-y)}(x-y) = y,$$

hence τ_{x-y} is an isometry carrying x to y . Otherwise we have $0 \neq q(x+y) = q(x - (-y))$, and the above argument shows that $\tau_{x+y}x = \tau_{x-(-y)}x = -y$ and thus $-(\tau_{x+y}x) = y$. \square

We can now give the proof of the Witt Cancellation Theorem. First a slight simplification: if U_1, U_2, V_1, V_2 are quadratic spaces such that $V_1 \cong V_2$ and $U_1 \oplus V_1 \cong U_2 \oplus V_2$, then we have $U_2 \oplus V_2 \cong U_2 \oplus V_1$, hence $U_1 \oplus V_1 \cong U_2 \oplus V_1$. So we may assume: $V_1 = V_2 = V$, $U_1 \oplus V \cong U_2 \oplus V$. We wish to conclude that $U_1 \cong U_2$.

Step 1: V is totally isotropic, say of dimension r and U_1 is nondegenerate, say of dimension s . Choose bases, and let B_1 (resp. B_2) be the symmetric matrix associated to U_1 (resp. U_2), so that we are assuming the existence of $M \in GL_{r+s}(K)$ such that

$$M^T \begin{bmatrix} 0_r & 0_{r,s} \\ 0_{s,r} & B_2 \end{bmatrix} M = \begin{bmatrix} 0_r & 0_{r,s} \\ 0_{s,r} & B_1 \end{bmatrix}.$$

But writing M as a block matrix $\begin{bmatrix} A & B \\ C & D \end{bmatrix}$, we find that the $s \times s$ submatrix in the lower right hand corner of the left hand side is $D^T M_2 D$. Thus $M_1 = D^T M_2 D$. Since M_1 is nonsingular, so is D , and we conclude that $U_1 \cong U_2$.

Step 2: V is totally isotropic. Choose orthogonal bases for U_1 and U_2 , and suppose WLOG that the matrix for U_1 has exactly r zeros along the diagonal, whereas the matrix for U_2 has at least r zeros. Then we can replace V by $V \oplus [r](0)$ and assume

that U_1 is nondegenerate, reducing to Case 1.

Step 3: $\dim V = 1$, say $V = \langle a \rangle$. If $a = 0$ we are done by Case 2, so we may assume $a \neq 0$. Explicitly, choose a basis x, e_2, \dots, e_n for $W_1 = \langle a \rangle \oplus U_1$ with $q(x) = a$ and a basis (x', e'_2, \dots, e'_n) for $W_2 = \langle a \rangle \oplus U_2$ with $q(x') = a$, and let $F : W_1 \rightarrow W_2$ be an isometry. Put $y = F^{-1}(x')$ and $U'_1 = F^{-1}(U_2)$, so that

$$W_1 = \langle x \rangle \oplus U_1 = \langle y \rangle \oplus U'_1.$$

By Proposition 27, there exists $\tau \in O(W_1)$ such that $\tau(x) = y$. Because $\langle x \rangle$ and $\langle y \rangle$ are nondegenerate, we have $U_1 = \langle x \rangle^\perp$ and $U'_1 = \langle y \rangle^\perp$, so that (as in Remark X.X above) we necessarily have $\tau(U_1) = U'_1$. Thus $U_1 \cong U'_1 \cong U_2$.

Step 4: General case: Write $V = \langle a_1, \dots, a_n \rangle$. By Step 3 we can cancel $\langle a_1 \rangle$, and then $\langle a_2 \rangle$, and so forth: i.e., an obvious inductive argument finishes the proof.

9. THE WITT RING

We have not yet touched the key part of the Witt Decomposition Theorem: namely, that given an arbitrary quadratic space V , it strips away the degenerate and hyperbolic parts of V and leaves an anisotropic form V' which is uniquely determined up to equivalence. In the literature, one sometimes sees V' referred to as the “anisotropic kernel” of V . However,, because I see no evident relation between this process and the kernel of a morphism, I prefer the more suggestive terminology **anisotropic core**.

Let us also introduce the following notation: let $[q]$ be an equivalence class of quadratic forms over K . Let $w[q]$ denote the anisotropic core, an equivalence class of anisotropic quadratic forms. We note that the operations \oplus (orthogonal direct sum) and \otimes (tensor product) are well-defined on equivalence classes of quadratic forms. The Witt Decomposition Theorem immediately yields the identity

$$(4) \quad w[q_1 \oplus q_2] = w[w[q_1] \oplus w[q_2]].$$

Let $W(K)$ be the set of isomorphism classes of anisotropic quadratic forms over K . Then (4) shows that \oplus induces a binary operation on $W(K)$: for anisotropic q_1, q_2 ,

$$[q_1] + [q_2] := w[q_1 \oplus q_2].$$

One checks immediately that this endows $W(K)$ with the structure of a commutative monoid, in which the additive identity is the class of the zero-dimensional quadratic form (which we have, fortunately, decreed to be anisotropic).

This operation is strongly reminiscent of the the operation Brauer defined on the set of all isomorphism classes of K -central finite dimensional division algebras over a field: by Wedderburn’s theorem, $D_1 \otimes D_2$ is isomorphic to $M_n(D_3)$, for a division algebra D_3 , uniquely determined up to isomorphism, and Brauer defined $[D_1] + [D_2] = [D_3]$. Indeed, just as repeatedly extracting the “core division algebra” makes this law into a group, in which the inverse of $[D_1]$ is given by the class of the opposite algebra $[D_1^{\text{opp}}]$, it turns out that repeated extraction of anisotropic cores makes $W(K)$ into a group. Explicitly, the inverse of $[q] = [\langle a_1, \dots, a_n \rangle]$ in $W(K)$ is given by $[-1 \cdot q] = [\langle -a_1, \dots, -a_n \rangle]$. Indeed,

$$[q] + [-1 \cdot q] = w[\langle a_1, \dots, a_n, -a_1, \dots, -a_n \rangle] = \sum_{i=1}^n w[\langle a_i, -a_i \rangle] = \sum_{i=1}^n w[\mathbb{H}] = 0.$$

Exercise: Define another binary operation on $W(K)$ as

$$[q_1] \cdot [q_2] := w[q_1 \otimes q_2].$$

Show that $(W(K), +, \cdot)$ is a commutative ring, the **Witt ring** of K .

In §X.X you are asked to compute the Witt rings for some simple fields K .

9.1. The Grothendieck-Witt Ring. The description of the Witt ring $W(K)$ given in the previous section is meant to be in the spirit of Witt's 1937 paper. More recently it has been found useful to describe $W(K)$ as a quotient of another commutative ring, the **Grothendieck-Witt ring** $\widehat{W}(K)$. We give a description of this approach here.

We begin with an observation which was essentially made in the previous section: the set $EQ(K)$ of equivalence classes of nondegenerate quadratic forms over K has the natural structure of a commutative semiring under \oplus and \otimes . Moreover it carries a natural \mathbb{N} -grading (given by the dimension) and therefore the only element in $EQ(K)$ with an additive inverse is the additive identity 0 (the class of the zero-dimensional quadratic form). It was one of A. Grothendieck's many abstract but useful insights that every monoid wants to be a group. More precisely, given a monoid $(M, +)$ which is not a group, there is a group $G(M)$ and a monoid homomorphism $M \rightarrow G(M)$ which is **universal** for monoid homomorphisms into a group. The best known case is the construction of $(\mathbb{Z}, +)$ as the group completion of the monoid $(\mathbb{N}, +)$.

If we assume that M is commutative, the general construction is essentially more complicated in exactly one respect. Namely, we define $G(M)$ to be the quotient of $M \oplus M$ modulo the equivalence relation $(a, b) \sim (c, d)$ iff there exists $m \in M$ with $m + a + d = m + b + c$. What is perhaps unexpected is the introduction of the "stabilizing" element $m \in M$. We ask the reader to check that without this, \sim need not be an equivalence relation! As is, the relation \sim is not only an equivalence relation but is compatible with the addition law on the monoid $M \oplus M$: that is, if $(a_1, b_1) \sim (a_2, b_2)$ and $(c_1, d_1) \sim (c_2, d_2)$, then

$$(a_1, b_1) + (c_1, d_1) = (a_1 + c_1, b_1 + d_1) \sim (a_2 + c_2, b_2 + d_2) = (a_2, b_2) + (c_2, d_2).$$

It follows that the set $G(M) := (M \times M) / \sim$ has a unique binary operation $+$ which makes it into a commutative monoid such that the natural map $M \times M \rightarrow G(M)$, $(a, b) \mapsto [a, b]$, is a homomorphism of monoids. In fact the monoid $(G(M), +)$ is a commutative group, since for any $(a, b) \in M \times M$,

$$[a, b] + [b, a] = [a + b, a + b] = [0, 0] = 0.$$

Exercise: Let $(M, +)$ be any commutative monoid.

- Let $G : M \rightarrow G(M)$ by $x \mapsto [x, 0]$. Show that G is a homomorphism of monoids.
- Show that $G : M \rightarrow G(M)$ is universal for monoid homomorphisms into a group.

Exercise: Let M be the monoid $(\mathbb{N} \cup \{\infty\}, +)$, where $\infty + m = m + \infty = \infty$ for all $m \in M$. Show that $G(M)$ is the trivial group.

Exercise X.X is an extreme example of "loss of information" in the passage from M

to $G(M)$. We may also ask when the homomorphism G is injective. By definition of the relation \sim , $[x, 0] = G(x) = G(y) = [y, 0]$ holds iff there exists $m \in M$ such that $x + m = y + m$. A commutative monoid $(M, +)$ is said to be **cancellative** if for all $x, y, m \in M$, $x + m = y + m \implies x = y$. Thus we have shown:

Proposition 28. *For a commutative monoid M , TFAE:*

- (i) M injects into its group completion.
- (ii) M is cancellative.

Now we return to the case of the commutative monoid $EQ(K)$ of equivalence classes of nondegenerate quadratic forms. It follows immediately from the Witt Cancellation theorem that $EQ(K)$ is a cancellative monoid, and thus $EQ(K)$ injects into its Grothendieck group, which is by definition $\widehat{W}(K)$. Concretely put, the elements of $\widehat{W}(K)$ are formal differences $[q_1] - [q_2]$ of isomorphism classes of quadratic forms. There is a monoid homomorphism

$$\dim : EQ(K) \rightarrow \mathbb{Z}$$

given by $[q] \mapsto \dim q$. By the universal property of the group completion, \dim factors through a group homomorphism

$$\dim : \widehat{W}(K) \rightarrow \mathbb{Z}.$$

(In less fancy language, we simply put $\dim([q_1] - [q_2]) = \dim[q_1] - \dim[q_2]$.)

Next recall that we also have a product operation, \otimes , which makes $EQ(K)$ into a commutative semiring. It is easy to check that the group completion of a commutative semiring $(R, +, \cdot)$ can be naturally endowed with the structure of a commutative ring, the multiplication operation on $G(R)$ being defined as $[a, b] \cdot [c, d] := [ac + bd, ad + bc]$. Thus $\widehat{W}(K)$ has the structure of a commutative ring, the **Grothendieck-Witt ring** of K .

Exercise: Let \hat{I} be the kernel of the homomorphism $\dim : \widehat{W}(K) \rightarrow \mathbb{Z}$. Show that \dim is in fact a ring homomorphism, and thus \hat{I} is an ideal of $\widehat{W}(K)$.

To get from the Grothendieck-Witt ring back to the Witt ring, we would like to quotient out by all hyperbolic spaces. It is not *a priori* clear whether this is compatible with the ring structure, but fortunately things work out very nicely.

Proposition 29. *The subgroup of $\widehat{W}(K)$ generated by the class $[\mathbb{H}]$ of the hyperbolic plane is an ideal of $\widehat{W}(K)$.*

Proof. Since any element of $\widehat{W}(K)$ is a formal difference of equivalence classes of nondegenerate quadratic forms, it suffices to show that for any nondegenerate quadratic form q , $[q] \cdot [\mathbb{H}] \in \mathbb{Z}[\mathbb{H}]$. And indeed, if $[q] = [a_1, \dots, a_n]$ is a nondegenerate quadratic form, then

$$[\mathbb{H}] \cdot [q] = [\mathbb{H} \otimes q] = [\langle 1, -1 \rangle \otimes \langle a_1, \dots, a_n \rangle] = \left[\bigoplus_{i=1}^n \langle a_i, -a_i \rangle \right] = \left[\bigoplus_{i=1}^n \mathbb{H} \right] = n[\mathbb{H}].$$

□

Theorem 30. *There is a canonical isomorphism $\widehat{W}(K)/\langle [\mathbb{H}] \rangle = W(K)$.*

Proof. Indeed taking the anisotropic core gives a surjective homomorphism from the semiring $EQ(K)$ to the Witt ring $W(K)$. By the universal property of group completion, it factors through a ring homomorphism $\Phi : \widehat{W}(K) \rightarrow W(K)$. Evidently $[\mathbb{H}] \in \text{Ker } \Phi$. Conversely, let $[q_1] - [q_2]$ be an element of the kernel of Φ . For $i = 1, 2$, by Witt Decomposition we may write $[q_i] = I_i[\mathbb{H}] + [q'_i]$ with $I_i \in \mathbb{N}$ and q'_i anisotropic. Then $\Phi([q_1]) = \Phi([q_2])$ implies $[q'_1] = [q'_2]$, so that $[q_1] - [q_2] \cong (I_1 - I_2)[\mathbb{H}] \in \langle [\mathbb{H}] \rangle$. \square

Exercise: Put $I = \Phi(\widehat{I})$, so that I is an ideal of the Witt ring, the **fundamental ideal**. Show that the dimension homomorphism factors through a surjective ring homomorphism $\text{dim} : W(K) \rightarrow \mathbb{Z}/2\mathbb{Z}$, with kernel I .

10. ADDITIONAL EXERCISES

Exercise: Recall that an integral domain R is a **valuation ring** if for any two elements $x, y \in R$, either $x \mid y$ or $y \mid x$. It is known that a Noetherian valuation ring is either a field or a discrete valuation ring. Let R be a valuation ring in which 2 is a unit – e.g. \mathbb{Z}_p for odd p or $k((t))$ for $\text{char}(k) \neq 2$ – and let $n \in \mathbb{Z}^+$. Show that every $n \times n$ symmetric matrix is congruent to a diagonal matrix. (Hint: adapt the algorithmic description of diagonalization following Theorem 9.)

Exercise: Over which of the following fields does there exist a nondegenerate universal anisotropic quadratic form?

- a) $K = \mathbb{C}$. b) $K = \mathbb{R}$. c) $K = \mathbb{F}_q$, q odd. d) $K = \mathbb{Q}_p$. e) $K = \mathbb{Q}$.

Exercise: Let q_1 and q_2 be binary quadratic forms over K . Show that $q_1 \cong q_2$ iff $\det(q_1) = \det(q_2)$ and q_1 and q_2 both represent at least one $\alpha \in K^\times$.

Exercise X.X: a) Let V_1 and V_2 be quadratic spaces. Show that every totally isotropic subspace W of $V_1 \oplus V_2$ is of the form $W \cap V_1 \oplus W \cap V_2$, with $W \cap V_i$ a totally isotropic subspace of V_i .

b) Same as part a) but with “totally isotropic subspace” replaced everywhere by “maximal totally isotropic subspace”.

c) Show that any two maximal totally isotropic subspaces of a quadratic space have the same dimension, namely $\dim(\text{rad } V) + I(V)$.

Exercise: Let K be a quadratically closed field. Show that $W(K) \cong \mathbb{Z}/2\mathbb{Z}$.

Exercise: Show that $W(\mathbb{R}) \cong \mathbb{Z}$.

Exercise: Let $K = \mathbb{F}_q$ be a finite field of odd order q .

- a) Show that every (nondegenerate) binary quadratic form over \mathbb{F}_q is universal.
 b) Deduce that every quadratic form in at least three variables over \mathbb{F}_q is isotropic.⁵
 c) Show there is exactly one class of anisotropic binary quadratic form over \mathbb{F}_q .
 d) Deduce that $\#W(K) = 4$.
 e) Show that the additive group of $W(K)$ is cyclic iff $-1 \notin K^{\times 2}$.

⁵Alternately, this is a special case of the **Chevalley-Warning theorem**.

Exercise: Let p be an odd prime. Show that as commutative groups,

$$W(\mathbb{Q}_p) \cong W(\mathbb{F}_p) \oplus W(\mathbb{F}_p).$$

Exercise ([Cas, Lemma 2.5.6]): Show that the additive group $(\widehat{W}(K), +)$ of the Grothendieck-Witt ring of K is isomorphic to the quotient of the free commutative group on the set of generators $\{[a] \mid a \in K^\times\}$ by the relations:

$$\begin{aligned} [ab^2] &= [a], \forall a, b \in K^\times, \\ [a] + [b] &= [a + b] + [ab(a + b)], \forall a, b \in K^\times \mid a + b \in K^\times. \end{aligned}$$

Exercise ([Cas, Cor. to Lemma 2.5.6]): Show that the additive group $(W(K), +)$ of the Witt ring of K is isomorphic to the quotient of the free commutative group on the set of generators $\{[a] \mid a \in K^\times\}$ by the relations of the previous Exercise together with $[1] + [-1] = 0$.

Exercise: Let $a, b \in K^\times$. Show that $\langle a, b, ab \rangle$ is isotropic iff $\langle 1, a, b, ab \rangle$ is isotropic.

Exercise: Suppose that for a given field K , we have an algorithm to tell us whether a quadratic form is isotropic and, if so, to find a nonzero isotropic vector. Construct from this an algorithm to decide whether two quadratic forms are equivalent. (Hint: Use Lemma 18 and repeated Witt Cancellation.)

REFERENCES

- [Cas] J.W.S. Cassels, *Rational quadratic forms*. London Mathematical Society Monographs, 13. Academic Press, Inc. [Harcourt Brace Jovanovich, Publishers], London-New York, 1978.
- [Cop] W.A. Coppel, *Number theory. An introduction to mathematics. Part B*. Revised printing of the 2002 edition. Springer, New York, 2006.
- [Lam] T.Y. Lam, *Introduction to quadratic forms over fields*. Graduate Studies in Mathematics, 67. American Mathematical Society, Providence, RI, 2005.
- [Wit] E. Witt, *Theorie der quadratischen Formen in beliebigen Körpern*. J. Reine Angew. Math. 176 (1937), 31-44.