QUADRATIC FORMS CHAPTER I: WITT'S THEORY

PETE L. CLARK

Contents

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.

By the late 19th century it was realized that it is easier to solve equations with coefficients in a field than in an integral domain R which is not a field (like $\mathbb{Z}$!) and that a firm understanding of the set of solutions in the fraction field of R is prerequisite to understanding the set of solutions in R itself. In this regard, a general theory of quadratic forms with $\mathbb{Q}$-coefficients was developed by H. Minkowski in the 1880s and extended and completed by H. Hasse in his 1921 dissertation.

The early 20th century saw the flowering of abstract algebra both as an important research area and as a common language and habitat for large areas of preexisting mathematics. The abstract definition of a field was first given by E. Steinitz in a landmark 1910 paper [Ste]. The study of quadratic forms over abstract fields was given a push by the work of E. Artin and O. Schreier in the 1920's, culminating in

Artin's 1927 solution of Hilbert's 17th problem: every positive semidefinite rational function with $\mathbb{R}$-coefficients is a sum of squares of rational functions.

It is natural to regard these developments as preludes and assert that the algebraic theory of quadratic forms properly begins with a seminal 1937 paper of E. Witt. The paper [Wit] contains the following advances:

• A recognition that many formal aspects of the Hasse-Minkowski theory carry over largely unchanged to the case of quadratic fields over an arbitrary field K of characteristic different from 2;

• The **Witt Cancellation Theorem**, which may be viewed as the "fundamental theorem" in this area of mathematics;

• The construction of a commutative ring $W(K)$ whose elements are equivalence classes of certain quadratic forms over K.

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

Let K denote a field of characteristic different fom 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 $q(t) = q(t_1, \ldots, t_n) \in K[t_1, \ldots, t_n]$, in several variables, with coefficients in K, and such that each monomial term has total degree 2: that is,

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

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

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

The function f_q has the following properties:

(i) For all $\alpha \in K$, $f_q(\alpha x) = \alpha^2 f_q(x)$, i.e., it is homogeneous of degree 2.
(ii) Put $B_f(x, y) := \frac{1}{2}(f_q(x + y) - f_q(x) - f_q(y))$.

(Note that $\frac{1}{2}$ exists in K since the characteristic of K is different from 2!)
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, $B_f : K^n \times K^n \to K$ 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 $f : K^n \to K$ which satisfies (i) and (ii), a **homogeneous quadratic function**. Let $e_1, \ldots, e_n$ 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

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

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

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

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

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

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

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

We have established the following result.

Theorem 1.1. *For $n \in \mathbb{Z}^+$, there are canonical bijections between the following sets:*
(i) The set of homogeneous quadratic polynomials $q(t) = q(t_1, \ldots, t_n)$.
(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:

$$q(t_1, t_2) = at_1^2 + bt_1 t_2 + ct_2^2.$$

$$f_q(x_1, x_2) = ax_1^2 + bx_1 x_2 + cx_2^2 = [x_1 x_2] \begin{bmatrix} a & \frac{b}{2} \\ \frac{b}{2} & c \end{bmatrix} \begin{bmatrix} x_1 \\ x_2 \end{bmatrix}.$$

$$B_f(x_1, x_2, y_1, y_2) = ax_1 y_1 + \frac{b}{2} x_1 y_2 + \frac{b}{2} x_2 y_1 + cx_2 y_2.$$

Two remarks are in order.

First, now that we know Theorem 1.1, it looks quite pedantic to distinguish between the polynomial $q(t)$ and the function $x \mapsto f_q(x)$, and we shall not do so from now on, rather writing a quadratic form as $q(x) = q(x_1, \ldots, x_n)$.

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

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

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.[1]

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 $q(x) = q(x_1, \ldots, x_n)$, we define another n-ary quadratic form

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

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

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

so that

$$B_{M \bullet q} = M B_q M^T. \tag{1}$$

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.[2] 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

[1] This 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.

[2] The 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.

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:

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

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 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 $x_1^2 + \ldots + x_n^2$.

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

$$q_1(x,y) = x^2 + y^2.$$
$$q_2(x,y) = x^2 - y^2.$$
$$q_3(x,y) = -x^2 - y^2.$$

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

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

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 2.1. *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

$$q_1 = x_1^2 - x_2^2 + x_3^2 + x_4^2,\ q_2 = x_1^2 - x_2^2 - x_3^2 - x_4^2 \tag{3}$$

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.
a) Show that $O_q = \{M \in GL_n(K) \mid M^T B M = B\}$.
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.
c) Suppose $q = x_1^2 + \ldots + x_n^2$. Show that O_q is the standard orthogonal group $O(n)$.
d) 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?
e) 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.
f) 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 $D(q) = \{\alpha \in \mathbb{G}_m \mid \alpha \cdot q \sim q\}$.
a) Show that $D(q)$ is a subgroup of $\mathbb{G}_m$.
b) Compute $D(q)$ for the form $x_1^2 + \ldots + x_n^2$ over $\mathbb{R}$.
c) 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 $B : V \times V \to K$. To be precise, we call such a pair (V, B) a **quadratic space**.[3]

We pause to recall the meaning of nondegeneracy in the context of bilinear forms. Namely, let V be any K-vector space and $B : V \times V \to K$ be any bilinear form. Then B induces a linear map L_B from V to its dual space $V^\vee = \mathrm{Hom}(V, K)$, namely $v \mapsto B(v, \ )$. 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

[3]Probably 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.

$B(v,w) = 0$ 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 3.1. *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 $e_1, \ldots, e_n$ for V and define a matrix B with (i,j) entry $b_{ij} = B(e_i, e_j)$. Then we have

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

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 ith component of Bv is nonzero. Then $B(v, e_i) \neq 0$. □

A **map** of quadratic spaces $(V, B_V) \to (W, B_W)$ is a K-linear map $L : V \to W$ 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 3.2. *Let $f : (V, B_v) \to (W, B_W)$ be a map of quadratic spaces. If B_V is nondegenerate, then f is an isometric embedding.*

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 $v = 0$. □

Exercise: Let $\iota : (V, B_V) \to (W, B_W)$ be an isometric embedding of quadratic spaces. Show that the following are equivalent:
(i) There exists an isometric embedding $\iota' : (W, B_W) \to (V, B_V)$ such that $\iota' \circ \iota = 1_V$, $\iota \circ \iota' = 1_{V'}$.
(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 $V \times V \to K$. 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 $V \to V \oplus W$, $W \to V \oplus W$, such that every pair of isometries $V \to Z$, $W \to Z$ 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 $e_1, \ldots, e_m$ of V and $e'_1, \ldots, e'_n$ 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 $B_1 = \Delta(a_1, \ldots, a_m)$, $B_2 = \Delta(b_1, \ldots, b_n)$, 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 **anistropic**. Thus an inner product space is (in particular) an anisotropic real quadratic space.

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

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

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

Proposition 4.1. *(Radical Splitting) Let (V, B) be any quadratic space. Then there exists a nondegenerate subspace W such that*

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

is an internal orthogonal direct sum decomposition.

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

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 Theoerem 5.1.

Proposition 4.2. *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, $\mathrm{rad}(W) = W \cap W^{\perp} = 0$, 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 $Z \in \mathrm{Hom}(W, K)$ 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 4.3. *Let (V, B) be a nondegenerate quadratic space and $W \subset V$ an arbitrary subspace. Then we have:*

$$\dim W + \dim W^{\perp} = \dim V. \tag{4}$$

$$(W^\perp)^\perp = W. \tag{5}$$

Proof. a) Consider the linear map $L : V \to W^\vee$ given by $v \mapsto (w \mapsto B(v,w))$. Evidently $\mathrm{Ker}(L) = W^\perp$. Moreover, this map factors as the composite $V \to V^\vee \to W^\vee$, 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

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

b) The inclusion $W \subset (W^\perp)^\perp$ is a tautology which does not require the nondegeneracy of V: indeed every vector in W is orthogonal to every vector which is orthogonal to every vector in W! On the other hand, by part a) we have $\dim W^\perp + \dim (W^\perp)^\perp = \dim V$, so $\dim W = \dim (W^\perp)^\perp$. Since W is finite-dimensional, we conclude $W = (W^\perp)^\perp$. □

Corollary 4.4. *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 4.4.

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 $D = \Delta(a_1, \ldots, a_n)$ is any diagonal matrix, then $M_\sigma^T D M = \Delta(a_{\sigma(1)}, \ldots, a_{\sigma(n)})$. 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

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

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 $\Delta(1, \ldots, 1, -1, \ldots, -1)$ 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 an 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 5.1. *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 $W_1, \ldots, W_n$ such that

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

Equivalently, there exists an **orthogonal basis** $(e_1, \ldots, e_n)$ 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 asociated 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 4.2 we have $V = W_1 \oplus W_1^{\perp}$. We are finished by induction! □

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 $(1i)$, we get a nonzero entry $\alpha = b'_{j1}$. If $j = 1$, great. If not, then by adding the jth row to the first row – and hence also the jth 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 5.1 is direct generalization of Proposition 4.1 (Radical Splitting), and the algorithmic description given above in particular gives an effective procedure that Proposition.

Corollary 5.2. *Let V be a nondegenerate quadratic space.*
a) For any anisotropic vector v, there exists an orthogonal basis $(v, e_2, \ldots, e_n)$.
b) If $\alpha \in K^{\times}$ is represented by q, then $(V, q) \cong \alpha x_1^2 + \alpha_2 x_2^2 + \ldots + \alpha_n x_n^2$.

Proof. Part a) is immediate from the proof of Theorem 5.1, and part b) follows immediately from part a). □

Corollary 5.3. *Let q be a nondegenerate binary form of discriminant d which represents $\alpha \in K^{\times}$. Then $q \cong \langle \alpha, \alpha d \rangle$. In particular, two nondegenerate binary forms are isometric iff they have the same discriminant and both represent any one element of $K^{\times}$.*

Proof. By Corollary 5.2, $q \cong \alpha x_1^2 + \alpha_2 x_2^2$. The discriminant of q is on the one hand $d \pmod{K}^{\times 2}$ and on the other hand $\alpha\alpha_2 \pmod{K}^{\times 2}$ so there exists $a \in K^{\times}$ such

that $\alpha\alpha_2 = da^{-2}$. So

$$q \cong \alpha x_1^2 + \left(\frac{d}{\alpha a^2}\right) x_2^2 = \alpha x_1^2 + \alpha d \left(\frac{x_2}{\alpha a}\right)^2 \cong \alpha x_1^2 + \alpha d x_2^2.$$

□

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 5.1 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 $\alpha_1, \ldots, \alpha_n$, we write $\langle a_1, \ldots, a_n \rangle$ for $\bigoplus_{i=1}^n \langle a_i \rangle$, or in other words, for the quadratic form corresponding to the matrix $\Delta(a_1, \ldots, a_n)$.

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 5.1 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 **totally isotropic** if $B|_W \equiv 0$.[4]

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 6.1. *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

[4]We have some misgivings here: 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, because isotropic subspaces are required to be nondegenerate. Nevertheless this is the standard terminology and we will not attempt to change it.

$\alpha \in K$ 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 hyerbolic plane: $q(xu_1 + yu_2) = xy$. □

Here is a generalization.

Theorem 6.2. *Let (V, B) be a nondegenerate quadratic space and $U \subset V$ a totally isotropic subspace with basis $u_1, \ldots, u_m$. Then there exists a totally isotropic subspace U', disjoint from U, with basis $u_1', \ldots, u_m'$ 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 6.1. 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 hyerbolic plane: $q(xu_1 + yu_2) = xy$.

Now assume the result is true for all totally isotropic subspaces of dimension smaller than m. Let $W = \langle u_2, \ldots, u_m \rangle$. If we had $W^\perp \subseteq \langle u_1 \rangle^\perp$, then taking "perps" and applying Proposition 4.3 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 $W' = \langle u_2', \ldots, u_n' \rangle$ with each $\langle u_i, u_i \rangle$ a hyperbolic plane. □

The following is an immediate consequence.

Corollary 6.3. *Let W be a maximal totally isotropic subspace of a nondegenerate quadratic space V. Then $\dim W \leq \frac{1}{2} \dim V$. Equality holds iff V is hyperbolic.*

It will convenient to have a name for the subspace U' shown to exist under the hypotheses of Theorem 6.2, 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 6.4. *Any isotropic quadratic space is universal.*

Proof. This follows immediately from Theorem 6.1. □

Exercise X.X: Give an example of an anisotropic universal quadratic form.

Corollary 6.5. *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 6.1. □

Corollary 6.6. *Any quadratic space V admits an internal orthogonal direct sum decomposition*

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

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

Proof. By Proposition 4.1 we may assume V is nondegenerate. If V is anisotropic, we are done ($n = 0$). If V is isotropic, then by Theorem 6.1 there is a hyperbolic subspace $\mathbb{H} \subset V$. Since $\mathbb{H}$ is nondegenerate, by Proposition 4.2 $V = \mathbb{H} \oplus \mathbb{H}^\perp$, with $\mathbb{H}^\perp$ nondegenerate of smaller dimension. We are finished by induction. □

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 6.7. *(First Representation Theorem) Let q be a nondegenerate 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 $\langle \alpha, \alpha_2, \ldots, \alpha_n \rangle$. 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 $q = \langle \alpha_1, \ldots, \alpha_n \rangle$, and our assumption is that there exist $x_0, \ldots, x_n$, not all 0, such that

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

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

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

Corollary 6.8. *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 6.9. *(Isotropy Criterion) Let $m, n \in \mathbb{Z}^+$, let $f(x_1, \ldots, x_m)$ and $g(y_1, \ldots, y_n)$ be nondegenerate quadratic forms, and put $h = f - g$. TFAE:*
(i) There is $\alpha \in K^\times$ which is represented by both f and g.
(ii) The quadratic form h is isotropic.

Proof. (i) $\implies$ (ii): Suppose there are $x \in K^m$, $y \in K^n$ such that $f(x) = g(y) = \alpha$. Then $h(x, y) = \alpha - \alpha = 0$ and since $f(x) = \alpha \neq 0$, some coordinate of x is nonzero. (ii) $\implies$ (i): Let $(x, y) \in K^{m+n} \setminus \{(0, \ldots, 0)\}$ be such that $h(x, y) = f(x) - g(y) = 0$. Let α be the common value of $f(x)$ and $f(y)$. If $\alpha \neq 0$, we're done. Otherwise 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 $e_1, \ldots, e_n$ is an orthogonal basis for K^n. □

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 7.1. *(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 7.2. *(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 $f : V_1 \to V_2$. Then there exists an isometry $F : X_1 \to X_2$ such that $F|_{V_1} = f$ and $F(U_1) = U_2$.*

Let us demonstrate the equivalence of Theorems 7.2 and 7.1. Assume Theorem 7.2, and let U_1, U_2, V_1, V_2 be as in Theorem 7.1. Put $X_1 = U_1 \oplus V_1$, $X_2 = U_2 \oplus V_2$, and let $f : V_1 \to V_2$ be an isometry. By Theorem 7.2, U_1 and U_2 are isometric.

Conversely, assume Theorem 7.1, and let $X_1, X_2, U_1, U_2, V_1, V_2$ be as in Theorem 7.2. Then Witt Cancellation implies that $U_1 \cong U_2$, say by an isometry $f_U : U_1 \to U_2$. Then $F = f_U \oplus f : X_1 \to X_2$ satisfies the conclusion of Theorem 7.2.

Remark: The statement of Theorem 7.2 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 7.3. *Let X be a quadratic space and $V_1, V_2 \subset X$ be nondegenerate subspaces. Then any isometry $f : V_1 \to V_2$ 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 7.2 now applies with $X = X_1 = X_2$ to give an isometry F of X extending f. □

Remark: The conclusion of Corollary 7.3 may appear weaker than that of Theorem 7.2, 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 7.4. *Let X be a nondegenerate quadratic space and $Y_1 \subset X$ any subspace. Then any isometric embedding $f : Y_1 \to X$ is an 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 7.3. Our strategy of proof is to reduce to this case. Using Proposition 4.1 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 4.4 $W_1^{\perp}$ is nondegenerate as well. We may therefore apply Theorem 6.2 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 $U_i = \mathrm{rad}(Y_i)$ 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 7.3. □

This has the following interesting consequence.

Theorem 7.5. *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.*

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 $f : V_1 \to V_2$.
b) Show that f *does not* extend to an isometry of X.

Corollary 7.3 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 7.6. *(Witt Decomposition Theorem) Let (V, B) be a quadratic space. Then there exists an orthogonal direct sum decomposition*

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

where V' is an anistropic 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 6.6. 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 6.1). □

Remark: Theorem 7.6 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 7.7. *(Sylvester's Law of Inertia)*
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 over $\mathbb{R}$ is isomorphic to exactly one form $q_{r,s}$.

Exercise: Use the Witt Decomposition Theorem to prove Theorem 7.7.

7.1. **The Chain Equivalence Theorem.**

In this section we present yet another fundamental theorem due E. Witt, albeit one of a more technical nature. This theorem will be needed at a key juncture later on in the notes, namely in order to show that the Hasse-Witt invariant is well-defined. The reader should feel free to defer reading about the proof, and even the statement, of the result until then.

Let $q_1 = \langle a_1, \ldots, a_n \rangle$, $q_2 = \langle b_1, \ldots, b_n \rangle$ be two diagonal n-ary quadratic forms over K. We say that q_1 and q_2 are **simply equivalent** if there exist not necessarily distinct indices i and j such that $\langle a_i, a_j \rangle \cong \langle b_i, b_j \rangle$ and for all $k \neq i, j$, $a_k = b_k$.

The following exercises are very easy and are just here to keep the reader awake.

Exercise X.X: If q and q' are simply equivalent, then they are isometric.

Exercise X.X: If $n \leq 2$, then two n-ary quadratic forms q and q' are simply equivalent iff they are isometric.

Exercise: If q and q' are chain equivalent, then so are $q \oplus q''$ and $q' \oplus q''$.

Despite the name, simple equivalence is *not* an equivalence relation: it is (obviously) reflexive and symmetric, but it is not transitive. For instance, let $a \in K \setminus \{0, \pm 1\}$ and $n \geq 3$, then the forms $q = \langle 1, \ldots, 1 \rangle$ and $q' = \langle a^2, \ldots, a^2 \rangle$ are not simply equivalent, since at least three of their diagonal coefficients differ. However, if we put $q_1 = \langle a^2, a^2, 1 \ldots, 1 \rangle$ $q_2 = \langle a^2, a^2, a^2, a^2, 1, \ldots 1 \rangle$ and so forth, changing at each step two more of the coefficients of q to a^2: if n is odd, then at the (final) $\frac{n+1}{2}$th step, we change the nth coefficient only. Then q is simply equivalent to q_1 which is simply equivalent to $q_2 \ldots$ which is simply equivalent to q_n which is simply equivalent to q'.

Let us temporarily denote the relation of simple equivalence by $\sim$. Since it is not transitive, it is natural to consider its transitive closure, say $\approx$. As for any transitive closure, we have $q \approx q'$ iff there exists a finite sequence $q_0, \ldots, q_{n+1}$ with $q_0 = q$, $q_{n+1} = q'$ and $q_i \sim q_{i+1}$ for all i. The reader may also verify that the transitive closure of any reflexive, symmetric relation remains reflexive and symmetric and is thus an equivalence relation. In this case, we say that two quadratic forms q and q' are **chain equivalent** if $q \approx q'$.

Note that in our above example of two chain equivalent but not simply equivalent quadratic forms, q and q' are in fact isometric. Indeed this must be true in general since the relation of simple equivalence is contained in that of the equivalence relation of isometry, so therefore the equivalence relation generated by simple equivalence must be contained in the equivalence relation of isometry. (Or just stop and think about it for a second: perhaps this explanation is more heavy-handed than necessary.) So a natural question[5] is how does chain equivalence compare to isometry. Is it possible for two isometric quadratic forms not to be chain equivalent?

Theorem 7.8. *(Witt's Chain Equivalence Theorem) For two n-ary quadratic forms $q = \langle \alpha_1, \ldots, \alpha_n \rangle$, $q' = \langle \beta_1, \ldots, \beta_n \rangle$, TFAE:*

[5]Well, as natural as the relation of simple equivalence, anyway.

(i) $q \approx q'$ (q and q' are chain equivalent).
(ii) $q \cong q'$ (q and q' are isometric).

Proof. The implication (i) $\implies$ (ii) has been established above. It remains to show that (ii) $\implies$ (i).
Step 0: Using Proposition 4.1 (Radical Splitting), we easily reduce to the case in which q and q' are nondegenerate, i.e., $\alpha_i, \beta_j \in K^\times$ for all i, j. (Moreover this will be the case of interest to us in the sequel.)
Step 1: Because the symmetric group S_n is generated by transpositions, it follows that for any permutation σ of $\{1, \ldots, n\}$ and any $\alpha_1, \ldots, \alpha_n \in K^\times$, the (isometric!) quadratic forms $\langle \alpha_1, \ldots, \alpha_n \rangle$ and $\langle \alpha_{\sigma(1)}, \ldots, \alpha_{\sigma(n)} \rangle$ are chain equivalent.
Step 2: We prove that any two isometric nondegenerate n-ary quadratic forms q and q' are chain equivalent, by induction on n. The cases $n = 1, 2$ have already been discussed, so assume $n \geq 3$. Any form which is chain equivalent to q is isometric to q' and hence represents β_1. Among all n-ary forms $\langle \gamma_1, \ldots, \gamma_n \rangle$ which are chain equivalent to q, choose one such that

$$\beta_1 = \gamma_1 a_1^2 + \ldots + \gamma_\ell a_\ell^2 \tag{6}$$

with minimal ℓ. We *claim* that $\ell = 1$. Suppose for the moment that this is the case. Then α is chain equivalent to a form $\langle \beta_1 a_1^{-2}, \gamma_2, \ldots, \gamma_n \rangle$ and hence to a form $q_1 = \langle \beta_1, \gamma_2, \ldots, \gamma_n \rangle$. Then, by Witt Cancellation, the form $\langle \gamma_2, \ldots, \gamma_n \rangle$ is isometric to $\langle \beta_2, \ldots, \beta_n \rangle$, and by induction these latter two forms are chain equivalent. By Exercise X.X, the forms q_1 and q' are chain equivalent, hence q and q' are chain equivalent.
Step 4: We verify our claim that $\ell = 1$. Seeking a contradiction we suppose that $\ell \geq 2$. Then no subsum in (6) can be equal to zero. In particular $d := \gamma_1 a_1^2 + \gamma_2 a_2^2 \neq 0$, hence by Corollary 5.3 we have $\langle \gamma_1, \gamma_2 \rangle \cong \langle d, \gamma_1 \gamma_2 d \rangle$. Using this and Step 1,

$$q \approx \langle \gamma_1, \ldots, \gamma_n \rangle \approx \langle d, \gamma_1 \gamma_2 d, \gamma_3, \ldots, \gamma_n \rangle \cong \langle d, \gamma_3, \ldots, \gamma_n, \gamma_1 \gamma_2 d \rangle.$$

But $\beta_1 = d + \gamma_3 a_3^2 + \ldots + \gamma_\ell a_\ell^2$, contradicting the minimality of ℓ. □

8. Orthogonal Groups

8.1. **The 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

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

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 $\mathrm{GL}_n(K)$-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 8.1. *Let V be a nondegenerate quadratic space. We have a short exact sequence of groups*

$$1 \to O^+(V) \to O(V) \stackrel{\det}{\to} \{\pm 1\} \to 1.$$

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 $M = \Delta(1, \ldots, 1, -1)$ is such an element. □

Exercise 8.1: 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 $O^+(V)$.

8.2. **Reflection through an anisotropic vector.**

We now introduce a fundamental construction which will turn out to generalize the seemingly trivial observation that if q is diagonal, $\Delta(1, \ldots, 1, -1)$ 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 $e_1, \ldots, e_{n-1}$ be an orthogonal basis for W, so that $(e_1, \ldots, e_{n-1}, v)$ is an orthogonal basis for V. Then, with respect to this basis, the matrix representation of τ_v is indeed $\Delta(1, \ldots, 1, -1)$. It follows that τ_v is an isometry, $\tau_v^2 = 1_V$ and $\det(\tau_v) = -1$.

Proposition 8.2. *Let (V, B, q) be any quadratic space. Suppose that $x, y \in V$ are anisotropic vectors with $q(x) = q(y)$. Then there is $M \in O(V)$ such that $Mx = y$. Moreover, we can choose M to be either a reflection or a product of two reflections.*

Proof. Case 1: Suppose $q(x) \neq \langle x, y \rangle$. Then $x - y$ is anisotropic: indeed

$$\langle x - y, x - y \rangle = q(x) - 2\langle x, y \rangle + q(y) = 2(q(x) - \langle x, y \rangle) \neq 0.$$

Then

$$\tau_{x-y}x = x - \frac{2\langle x, x-y\rangle}{\langle x-y, x-y\rangle}(x-y) = x - \frac{2(q(x)-\langle x,y\rangle)}{\langle x-y, x-y\rangle}(x-y) = y.$$

Case 2: Suppose $q(x) = \langle x, y\rangle$. Then, since $\operatorname{char} K \neq 2$, $\langle -x, y\rangle \neq q(x)$. Using Case 1 with $-x$ in place of x we get

$$\tau_{-x-y}\tau_x x = \tau_{-x-y} - x = y.$$

□

Exercise 8.2: a) Let $M \in O(V)$, and let $v \in V$ be an anisotropic vector. Show:

$$M\tau_v M^{-1} = \tau_{Mv}.$$

b) Let $v \in V$ be an anisotropic vector. Deduce that the conjugacy class of τ_v in $O(V)$ is $\{\tau_w \mid q(w) = q(v)\}$.

8.3. **Proof of Witt Cancellation.**

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 $V \oplus [r]\langle 0\rangle$ 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 $x, e_2, \ldots, e_n$ for $W_1 = \langle a\rangle \oplus U_1$ with $q(x) = a$ and a basis $(x', e_2' \ldots, e_n')$ for $W_2 = \langle a\rangle \oplus U_2$ with $q(x') = a$, and let $F : W_1 \to W_2$ 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 8.2, 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 $\tau(U_1) = U_1'$. Thus $U_1 \cong U_1' \cong U_2$.

Step 4: General case: Write $V = \langle a_1, \ldots, a_n\rangle$. 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.

8.4. **The Cartan-Dieudonné Theorem.**

In this section we state and prove one of the fundamental results of "geometric algebra," a theorem of E. Cartan and J. Dieudonné. Because this result is not used in the remainder of these notes and the proof is somewhat intricate, we encourage the beginning reader to read the statement and then skip to the next section.

We need one preliminary result.

Lemma 8.3. *Let V be a hyperbolic quadratic space, and let $\sigma \in O(V)$ be an isometry which acts as the identity on a maximal totally isotropic subspace of V. Then $\sigma \in O^+(V)$.*

Proof. Let M be a maximal isotropic subspace on which σ acts as the identity. Put $r = \dim M$, so $2r = \dim V$. Let N be an isotropic supplement to M (c.f. Theorem 6.2). For $x \in M$, $y \in N$ we have $\sigma x = x$ and

$$\langle x, \sigma y - y\rangle = \langle x, \sigma y\rangle - \langle x, y\rangle = \langle x, \sigma y\rangle - \langle x, \sigma y = 0.$$

Thus $\sigma y - y \in M^\perp = M$. Let $x_1, \ldots, x_r$ be a basis for M and $y_1, \ldots, y_r$ be a basis for N. It is then easy to see that the determinant of σ with respect to the basis $x_1, \ldots, x_r, y_1, \ldots, y_r$ is equal to 1. □

Theorem 8.4. *(Cartan-Dieudonné) Let V be a nondegenerate quadratic space of dimension n. Then every element of the orthogonal group $O(V)$ may be expressed as a product of n reflections.*

Proof. We follow [OM00, pp. 102-103].
Step 1: Suppose that there exists $\sigma \in O(V)$ satisfying the following condition: for every anisotropic vector x, the vector $\sigma x - x$ is nonzero and isotropic. Then $n \geq 4$, n is even and $\sigma \in O^+(V)$.
Certainly we cannot have $n = 1$, for then $O(V) = \{\pm 1\}$ and it is clear that neither 1 nor -1 satisfies the hypotheses. If $n = 2$, then let x be an anisotropic vector. Since $\sigma x - x$ is isotropic and nonzero, σx must be linearly independent from x. We then compute that the determinant of the quadratic form with respect to the basis $x, \sigma x$ is equal to 0, contradicting nondegeneracy. So we may assume $n \geq 3$.

By assumption we have $q(\sigma x - x) = 0$ for all anisotropic $x \in V$. We claim that in fact this holds for all $x \in V$. To see this, let $y \in V$ be a nonzero isotropic vector. There exists a hyperbolic plane containing y and splitting V, hence a vector z with $q(z) \neq 0$ and $\langle y, z\rangle = 0$. Then for all $\epsilon \in K^\times$ we have $q(y + \epsilon z) \neq 0$, hence by assumption

$$q(\sigma(y + \epsilon z) - (y + \epsilon z)) = 0,\ q(\sigma z) - z) = 0.$$

It follows that for all $\epsilon \in K^\times$ we have

$$q(\sigma y - y) + 2\epsilon\langle \sigma y - y, \sigma z - z\rangle = 0. \tag{7}$$

If in equation (7) we substitute $\epsilon = 1$ and then $\epsilon = -1$ and add, we get $q(\sigma y - y) = 0$, as claimed. In other words, if we put $W := (\sigma - 1)V$, then $q|_W \equiv 0$. Now for any $x \in V$ and $y \in W^\perp$ we have

$$\begin{aligned}\langle x, \sigma y - y\rangle &= \langle \sigma x, \sigma y - y\rangle - \langle \sigma x - x, \sigma y - y\rangle \\ &= \langle \sigma x, \sigma y - y\rangle = \langle \sigma x, \sigma y\rangle - \langle \sigma x, y\rangle \\ &= \langle x, y\rangle - \langle \sigma x, y\rangle = -\langle \sigma x - x, y\rangle = 0.\end{aligned}$$

Thus $\sigma y - y$ is perpendicular to all of V; by nondegeneragy, we conclude $\sigma y = y$. Our hypothesis now implies that $q|_{W^\perp} = 0$. Thus

$$W \subset W^\perp \subset W^{\perp\perp} = W,$$

so $W = W^\perp$. Therefore $\dim V = \dim W + \dim W^\perp = 2 \dim W$ is even, hence at least 4. Moreover V is hyperbolic and W is a maximal totally isotropic subspace on which σ acts as 1. By Lemma 8.3, we have $\sigma \in O^+(V)$, completing Step 1.
Step 2: We now prove the theorem, by induction on n. The case $n = 1$ is trivial, so we assume $n > 1$.
Case 1: Suppose there exists an anisotropic vector $x \in V$ such that $\sigma x = x$. Then $H = (Kx)^\perp$ is a hyperplane which is left invariant by σ. (Indeed, let $h \in H$. Then $\langle \sigma h, x\rangle = \langle h, \sigma^{-1}x\rangle = \langle h, \alpha x\rangle = 0$. So $\sigma h \subset (Kx)^\perp = H$.) By induction, $\sigma|_H$ is a product of at most $n-1$ reflections τ_{x_i} in anisotropic vectors $x_i \in H$. We may naturally view each τ_{x_i} as a reflection on all of V and the same product of reflections agrees with σ on H. Moreover, it also agrees with σ on Kx, since σ and all of the reflections are equal to the identity on Kx. Thus σ is itself equal to the product of the at most $n-1$ reflections τ_i.

Case 2: Next suppose that there is an anisotropic vector x such that $\sigma x - x$ is anisotropic. Note that

$$2\langle \sigma x, \sigma x - x\rangle = 2\left(\langle x, x\rangle - \langle \sigma x, x\rangle\right) = \langle \sigma x - x, \sigma x - x\rangle.$$

From this it follows that

$$(\tau_{\sigma x - x}\sigma)(x) = \sigma x - \frac{2\langle \sigma x, \sigma x - x\rangle}{\langle \sigma x - x, \sigma x - x\rangle}(\sigma x - x) = \sigma x - (\sigma x - x) = x,$$

i.e., $\tau_{\sigma x - x}\sigma$ leaves x fixed. By the previous case, it follows that $\tau_{\sigma x - x}\sigma$ is a product of at most $n-1$ reflections, hence σ is a product of at most n reflections.

The remaining case is that for every anisotropic vector $x \in V$, we have that $\sigma x - x$ is isotropic and nonzero. Now we apply Step 1 to conclude that n is even and $\sigma \in O^+(V)$. Let τ be any reflection. Then $\sigma' := \tau\sigma \in O^-(V)$, so that by Step 1 and the first two cases of Step 2, σ' must be a product of at most n reflections. Therefore σ is itself a product of at most $n+1$ reflections. But since n is even, if σ were a product of exactly $n+1$ reflections we would have $\sigma \in O^-(V)$, contradiction. Therefore σ is a product of at most n reflections, qed. □

Remark: Much of the time in the algebraic and arithmetic study of quadratic forms, the case of $K = \mathbb{R}$ is essentially trivial. Here we find an exception to this rule: Theorem 8.4 is already an important and useful result when applied to a positive definite quadratic form on $\mathbb{R}^n$.

Corollary 8.5. *Let $\sigma \in O(V)$ be a product of r reflections. Then the dimension of the space $W = \{v \in V \mid \sigma v = v\}$ of σ-fixed vectors is at least $n - r$.*

Exercise 8.3: Prove Corollary 8.5. (Hint: each of the r reflections determines a hyperplane H_i; show that $\bigcap_i H_i \subset W$.

Exercise 8.4: Exhibit an element of $O(V)$ which is not a product of fewer than n reflections.

Corollary 8.6. *Suppose that $\sigma \in O(V)$ may be expressed as a product of n reflections. Then it may be expressed as a product of n reflections with the first reflection arbitrarily chosen.*

Proof. Let $\sigma = \tau_1 \cdots \tau_n$ and let τ be any reflection. Applying Cartan-Dieudonné to $\tau\sigma$, there exists $r \leq n$ such that

$$\tau\sigma = \tau_1' \cdots \tau_r',$$

and thus

$$\sigma = \tau\tau_1' \cdots \tau_r'.$$

We have $\det(\sigma) = (-1)^n = (-1)^{r+1}$, so $r+1$ is at most $n+1$ and has the same parity as n, and thus $r+1 \leq n$. □

8.5. **Further Results on the Structure of Orthogonal Groups.**

Let V be a nondegenerate quadratic space over a field K: as usual, we assume that $\operatorname{char} K \neq 2$. Also, to avoid trivialities we assume that $V \neq 0$. Our main goal in this section is to determine the centers of the groups $O(V)$ and $O^+(V)$. In general this requires some fairly intricate calculations and casewise analysis, so we begin with two special cases in which a more straightforward approach succeeds.

Exercise 8.5: Let $q = x_1^2 + \ldots + x_n^2$, and let V be the associated quadratic space. For $1 \leq i \leq n$, let e_i be the ith standard basis vector of K^n.
a) For $1 \leq i \leq n$, let $\tau_i = \tau_{e_i}$. Show that $\tau_i = \operatorname{diag}(1, \ldots, -1, \ldots, 1)$.
b) Show by direct calculation that if $M \in \operatorname{GL} V$ is such that $M\tau_i = \tau_i M$ for all $1 \leq i \leq n$, then M is diagonal.
c) Show that if $M \in O(V)$ is diagonal, then each of its diagonal entries is $\{\pm 1\}$.
d) Show that every permutation matrix lies in $O(V)$.
e) Deduce that $ZO(V) = \{\pm 1\}$.

Exercise 8.6: Consider the hyperbolic plane $\mathbb{H}$ as a quadratic space V over K.
a) Show that

$$O^+(V) = \left\{ \begin{pmatrix} a & 0 \\ 0 & \frac{1}{a} \end{pmatrix} \mid a \in K^\times \right\},$$

which is isomorphic as a group to $K^\times$.
b) Show that

$$O^-(V) = \left\{ \begin{pmatrix} 0 & b \\ \frac{1}{b} & 0 \end{pmatrix} \mid b \in K^\times \right\}.$$

c) Suppose $\#K > 3$. Show: $ZO(V) = \{\pm 1\}$. Deduce $ZO(V) \cap O^+(V) \subsetneq ZO^+(V)$.
d) Suppose $K \cong \mathbb{F}_3$. Show: $O^+(V) = \{\pm 1\}$ and $O(V) = ZO(V) = \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.

Exercise 8.7: Use Exercise 8.6a) to give another proof of the fact that $O^+(V)$ is commutative when $\dim V = 2$. (Hint: $O^+(V) \subset O^+(V_{/\overline{K}})$.)

It is often the cases that the center of a "nice subgroup" $G \subset \operatorname{GL} V$ is the set of scalar matrices in G. Let's first nail down two basic cases.

Proposition 8.7. *Let K be an arbitrary field – for once we* do not *assume that* $\operatorname{char} K = 2$ *– and let $n \in \mathbb{Z}^+$.*
a) The center of $\operatorname{GL}_n(K)$ *consists of all scalar matrices* $\{\operatorname{diag}(\alpha, \ldots, \alpha) \mid \alpha \in K^\times\}$.
b) The center of $\operatorname{SL}_n(K)$ *consists of all scalar matrices* $\{\operatorname{diag}(\alpha, \ldots, \alpha) \mid \alpha^n = 1\}$.

Proof. a) Let Z be the center of $\mathrm{GL}_n(K)$. It is clear that every scalar matrix lies in Z. To prove the converse, let $M = (m_{ij}) \in \mathbb{Z}$, let $1 \leq i \neq j \leq n$, and let E_{ij} be the matrix obtained from the identity matrix by changing the (i,j)-entry from 0 to 1: thus $E_{ij} \in \mathrm{GL}_n(K)$. Since $M \in Z$ we have $E_{ij}M = ME_{ij}$; one checks that this holds iff $m_{ij} + m_{jj} = m_{ij} + m_{ii}$ and $m_{ii} = m_{ii} + m_{ji}$, i.e., iff $m_{ji} = 0$ and $m_{ii} = m_{jj}$. Since this holds for all $i \neq j$, M is a scalar matrix.
b) Let Z be the center of $\mathrm{SL}_n(K)$, and let $M \in Z$. Since for all $1 \leq i \neq j \leq n$, $E_{ij} \in \mathrm{SL}_n(K)$, the computation of part a) shows that M is scalar. Since $\det \mathrm{diag}(\alpha, \ldots, \alpha) = \alpha^n$, $\mathrm{diag}(\alpha, \ldots, \alpha)$ lies in $\mathrm{SL}_n(K)$ iff $\alpha^n = 1$. □

Lemma 8.8. *Let V be a two-dimensional nondegenerate quadratic space. Let $\tau_1 \in O(V) \setminus O^+(V)$, and let $M_1, M_2 \in O^+(V)$. Then:*
a) τ_1 is a reflection, and there are reflections τ_2, τ_3 such that $M_1 = \tau_1\tau_2$, $M_2 = \tau_1\tau_3$.
b) $\tau_1 M_1 \tau_1^{-1} = M_1^{-1}$.
c) $O^+(V)$ is commutative.
d) If $M_1^2 = 1$, then $M_1 = \pm 1$.
e) The following are equivalent:
(i) $O^+(V) = \{\pm 1\}$.
(ii) $O^+(V)$ is a 2-torsion group.
(iii) $O(V)$ is commutative.
(iv) $ZO(V) \supsetneq \{\pm 1\}$.

Proof. a) This follows from Corollary 8.5 (to the Cartan-Dieudonné Theorem).
b) Keeping in mind that $\tau_i = \tau_i^{-1}$ for all i, we have

$$\tau_1 M_1 \tau_1^{-1} = \tau_1\tau_1\tau_2\tau_1^{-1} = \tau_2^{-1}\tau_1^{-1} = (\tau_1\tau_2)^{-1} = M_1^{-1}.$$

c) As above, we have

$$M_2^{-1}M_1M_2 = (\tau_1\tau_3)^{-1}(\tau_1\tau_2)(\tau_1\tau_3) = \tau_3\tau_1\tau_1\tau_2\tau_1\tau_3 = \tau_3(\tau_2\tau_1)\tau_3 = \tau_1\tau_2 = M_1.$$

d) For any $M \in \mathrm{GL}(V)$ such that $M^2 = 1$, M satisfies the polynomial $t^2 - 1 = (t+1)(t-1)$, so its minimal polynomial has distinct linear factors and thus M is diagonalizable with diagonal entries ± 1. The condition $\det M = 1$ rules out the possibility that both $+1$ and -1 are eigenvalues.
e) (i) $\implies$ (ii) is immediate.
(ii) $\implies$ (iii): By part c), $O^+(V)$ is commutative. By part b), if every element of $O^+(V)$ has order 2, then every elmeent of $O(V) \setminus O^+(V)$ commutes with every element of $O^+(V)$.
(iii) $\implies$ (iv): Since $O^+(V) \supset \{\pm 1\}$ and $[O(V) : O^+(V)] = 2$, $\#O(V) \geq 4$. Thus if $O(V)$ is commutative, $O(V) = ZO(V) \supsetneq \{\pm 1\}$.
(iv) $\implies$ (i): We show the contrapositive: suppose $M \in O^+(V) \setminus \{\pm 1\}$. By part d), $M^2 \neq 1$, and then by part b), $\tau \in O(V) \setminus O^+(V)$, $\tau M \tau^{-1} = M^{-1}$, so τ does not commute with M. It follows that $ZO(V) = \{\pm 1\}$.

□

Lemma 8.9. *Let V be a nondegenerate quadratic space of dimension $n \geq 3$. Then:*

$$ZO^+(V) = ZO(V) \cap O^+(V).$$

Proof. It is clear that $ZO(V) \cap O^+(V) \subset ZO^+(V)$. For the converse, let $M \in ZO^+(V)$: we must show that $M \in ZO(V)$. Let x be an anisotropic vector, and let $e_1, \ldots, e_n$ be an orthogonal basis with $e_1 = x$. Let W_1 be the K-span of e_n, e_1, and

let W_2 be the K-span of e_1, e_2. Since $n \geq 3$, $W_1 \cap W_2 = Ke_1$. Put $\tau_i = \tau_{e_i}$.

We claim $MW_i \subset W_i$ for $i = 1, 2$. Indeed,

$$-Me_1 = M(\tau_1\tau_2 e_1) = \tau_1\tau_2 Me_1 = \tau_1(Me_1 - 2\frac{\langle Me_1, e_2\rangle}{\langle e_2, e_2\rangle}e_2)$$

$$= Me_1 - 2\frac{\langle Me_1, e_1\rangle}{\langle e_1, e_1\rangle}e_1 - 2\frac{\langle Me_1, e_2\rangle}{\langle e_2, e_2\rangle}e_2,$$

and thus

$$Me_1 = \frac{\langle Me_1, e_1\rangle}{\langle e_1, e_1\rangle}e_1 - \frac{\langle Me_1, e_2\rangle}{\langle e_2, e_2\rangle}e_2.$$

Similar calculations show $Me_2 \in W_2$ and – using e_n, e_1 in place of e_1, e_2 – we get $MW_i \subset W_i$. It follows that $MW_1 \cap W_2 \subset W_1 \cap W_2$, so $Mx = ax$ for some $a \in K$.

Since this holds for all anisotropic x, in particular it holds for each e_i – say $Me_i = a_i e_i$ – i.e., M is diagonal with respect to the basis $e_1, \ldots, e_n$. The reflections τ_i are also diagonal with respect to this basis, so $M\tau_i = \tau_i M$ for all $1 \leq i \leq n$. It follows that for every anisotropic vector x and every $c_1, \ldots, c_n \in K$,

$$M\tau_x(c_1e_1 + \ldots + c_ne_n) = -\sum_{i=1}^n M\tau_x\tau_i c_i e_i = -\sum_{i=1}^n \tau_x\tau_i M c_i e_i$$

$$= -\tau_x(\sum_{i=1}^n \tau_i a_i c_i e_i) = \tau_x \sum_{i=1}^n a_i c_i e_i = \tau_x M(c_1e_1 + \ldots + c_ne_n),$$

and thus $M\tau_x = \tau_x M$. By the Cartan-Dieudonné Theorem, $M \in ZO(V)$. □

Exercise 8.8: Let $K = \mathbb{F}_3$.
a) Show that there are up to isomorphism two nondegenerate binary quadratic forms over K: the hyperbolic plane $\mathbb{H}$ and $q = x_1^2 + x_2^2$.
b) Let V be the quadratic space associated to q. Show:
(i) $O(V) \cong D_4$, the dihedral group on 4 elements.
(ii) $O^+(V) \cong C_4$, the cyclic group of order 4.
(iii) $ZO(V) = \{\pm 1\}$, $ZO^+(V) \cong C_4$, and $ZO(V) \cap O^+(V) \subsetneq ZO^+(V)$.

Exercise 8.9: Let $\Delta \in K^\times$ be such that $-\Delta \notin K^{\times 2}$, so that the quadratic form $q = x^2 + \Delta y^2$ is anisotropic. Let $T_\Delta = \{(x, y) \in K^2 \mid x^2 + \Delta y^2 = 1\}$.
a) Let $L = K(\sqrt{-\Delta})$. Consider the injection $\iota : T_\Delta \hookrightarrow L^\times$ given by $(x, y) \mapsto x + \sqrt{-\Delta}y$. Show that $\iota(T)$ is a subgroup of $L^\times$. Show in fact that it is the kernel of the **norm map**

$$N_{L/K} : L^\times \to K^\times,\ x + \sqrt{-\Delta}y \mapsto (x + \sqrt{-\Delta}y)(x - \sqrt{-\Delta}y).$$

b) Let V be the quadratic space associated to q. Show that

$$O^+(V) = \left\{ \begin{bmatrix} x & y \\ -y\Delta & x \end{bmatrix} \mid x^2 + \Delta y^2 = 1 \right\}.$$

c) Show that as groups, $O^+(V) \cong T_\Delta$.

Theorem 8.10. *Let (V, q) be a nondegenerate quadratic space.*
a) We have $ZO(V) = \{\pm 1\}$ except in the single case $K \cong \mathbb{F}_3$ and $V \cong \mathbb{H}$, in which case $O(V) = ZO(V) \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.

b) Suppose $n = 2$ and $V \cong \mathbb{H}$. Then $O^+(V) \cong K^\times$.
c) Suppose $n = 2$ and V is anisotropic. Let $L = K(\sqrt{-\operatorname{disc} q})$. Then

$$O^+(V) \cong \operatorname{Ker}(N : L^\times \to K^\times).$$

d) Suppose $n \geq 3$. Then:
(i) If n is even, $ZO^+(V) = \{\pm 1\}$.
(ii) If n is odd, $ZO^+(V) = \{1\}$.

Proof. Of course when $n = 1$, $O(V) = \{\pm 1\}$, so the result of part a) holds. Henceforth we may assume $n \geq 2$.
a) First observe that $\{\pm 1\} \subset ZO(V)$. Now let $M \in ZO(V)$.
Step 1: We claim that M commutes with τ_x for all anisotropic x. Explicitly, for all such x and for all $y \in V$,

$$My - 2\frac{\langle y, x\rangle}{\langle x, x\rangle}Mx = (M \circ \tau_x)(y) = (\tau_x \circ M)(y) = My - 2\frac{\langle My, x\rangle}{\langle x, x\rangle}x$$

and thus

$$\langle y, x\rangle Mx = \langle My, x\rangle x.$$

Since $x \neq 0$, by nondegeneracy there is $y \in V$ with $\langle x, y\rangle \neq 0$, we deduce $Mx = a_x x$ for some $a_x \in K$, and then that

$$a_x^2\langle x, x\rangle = \langle a_x x, a_x x\rangle = \langle Mx, Mx\rangle = \langle x, x\rangle \neq 0,$$

so $a_x = \pm 1$. Now let $e_1, \ldots, e_n$ be an orthogonal basis for V, so $Me_i = a_i e_i$ for all i with $a_i \in \{\pm 1\}$ for all i. We claim that all the a_i's are equal. If $\#K > 3$, for all $1 \leq i, j \leq k$, there is $b_{ij} \in K^\times$ such that

$$\langle e_i, e_i\rangle + b_{ij}^2\langle e_j, e_j\rangle \neq 0,$$

and then

$$a_i e_i + b_{ij}a_j e_j = M(e_i + b_{ij}e_j) = c_{ij}(e_i + b_{ij}e_j)$$

for some $c_{ij} \in \{\pm 1\}$. It follows that $a_i = a_j$ and thus $M = \alpha$ is a scalar matrix. Then since for all $v, w \in V$, $\langle v, w\rangle = \langle Mv, Mw\rangle = \alpha^2\langle v, w\rangle$, so $\alpha \in \{\pm 1\}$.
Step 2: Now suppose $K \cong \mathbb{F}_3$. Then q is isometric to either

$$q_1 = x_1^2 + \ldots + x_n^2$$

or to

$$q_2 = x_1^2 + \ldots + x_{n-1}^2 - x_n^2.$$

The $n = 2$ case is handled by Exercise 8.8, so we may assume $n \geq 3$. Further, in Exercise 8.5 we showed that $ZO(V, q_1) = \{\pm 1\}$, so we may suppose that $V = (V, q_2)$. The argument of the previous step still shows that $Me_i = a_i e_i$ with $a_i \in \{\pm 1\}$. In particular M is diagonal with respect to the basis $e_1, \ldots, e_n$. If $\sigma : \{1, \ldots, n\} \to \{1, \ldots, n\}$ is a permutation fixing n, then the corresponding permutation matrix P_σ lies in $O(V)$. As in Exercise 8.5, this shows $a_i = a_j$ for all $1 \leq i, j \leq n-1$. Replacing M by $-M$ if necessary, we may assume $a_1 = \ldots = a_{n-1} = 1$, and it suffices to rule out the possibility $a_n = 1$, i.e., $M = \tau_{e_n}$. But $q(e_n) = q(e_1 + e_2) = -1$. Since e_n and $e_1 + e_2$ are linearly independent, $\tau_{e_1+e_2} \neq \tau_{e_n}$, but by Exercise 8.2b), $\tau_{e_1+e_2}$ and τ_{e_n} are conjugate in $O(V)$, contradicting the assumption that $\tau_{e_n} \in ZO(V)$.
b) This was done in Exercise 8.6.
c) The case of $q_\Delta = x^2 + \Delta y^2$ was treated in Exercise 8.9. A general anisotropic binary quadratic form q of discriminant Δ is of the form αq_Δ for some $\alpha \in K^\times$, and $O^+(\alpha q_\Delta) = O^+(q_\Delta)$.

d) Since $n \geq 3$, Lemma 8.9 applies. This, part a), and the fact that the determinant of the scalar matrix -1 is 1 if n is even and -1 if n is odd gives the result. □

Lemma 8.11. *Let V be a nondegenerate quadratic space. The sequence*

$$1 \to O^+(V) \to O(V) \to \{\pm 1\} \to 1$$

is split: there is an order 2 subgroup C of $O(V)$ such that $C \cap O^+(V) = \{1\}$. Thus

$$O(V) = O^+(V) \rtimes C.$$

Proof. Indeed, for any anisotropic vector $x \in V$, we may take $C = \{1, \tau_x\}$. □

Theorem 8.12. *Suppose $\#K > 3$, and let V be a nondegenerate quadratic space of dimension $n \geq 2$.*
a) There is a non-normal subgroup C such that $O(V) = O^+(V) \rtimes C$.
b) If n is odd, there is a normal subgroup C such that $O(V) = O^+(V) \rtimes C$ (and thus $O(V) = O^+(V) \times C$).
c) If n is even, there is no normal subgroup C such that $O(V) = O^+(V) \rtimes C$ (and thus $O(V) \neq O^+(V) \times C$).

Proof. Observe that an order 2 subgroup C of any group G is normal iff it is central, i.e., iff $C \subset Z(G)$. By Proposition 8.10a), $ZO(V) = \{\pm 1\}$. a) Take $C = \{1, \tau_x\}$ for an anisotropic vector x as in the proof of Lemma 8.11. By considering eigenvalues we see that $\tau_x \neq \pm 1$ and thus $\tau_x \notin ZO(V)$.
b) The scalar matrix -1 has determinant $(-1)^n$. Thus $-1 \notin O^+(V)$ iff n is odd. So when n is odd we may take $C = \{\pm 1\}$.
c) On the other hand, when n is even, $ZO(V) = \{\pm 1\} \subset O^+(V)$, so there is no order 2 central element $c \in O(V) \setminus O^+(V)$. □

Remark: Thanks to Max Kieff for bringing Theorem 8.12 to my attention. In fact we met by chance in a cafe in Athens, GA, and upon learning that I was a mathematician he asked me how to prove that $O(n) = O^+(n) \times C$ iff n is odd (for the standard quadratic form $x_1^2 + \ldots + x_n^2$ over $\mathbb{R}$). Unfortunately my first answer was part a) of Theorem 8.12, i.e., the construction of a non-normal complement C in every case. Soon enough I realized that my answer was not satisfactory, and these considerations led to the present section of these notes. (Eventually I suggested the rest of the theorem. The proof that $ZO(n) = \{\pm 1\}$ is easier for the form $x_1^2 + \ldots + x_n^2$ over $\mathbb{R}$ than in the general case, whence Exercise 8.5.)

The following exercise gives a more basic example that a normal subgroup N of a group G may have both normal and non-normal complements.

Exercise 8.10: Let A be any non-commutative group, let $G = A \times A$, and let $N = \{(a, 1) \mid a \in A\}$. Then N is a normal subgroup of G, and $G/N \cong A$.
a) Let $H_1 = \{(1, a) \mid a \in A\}$. Show that $G = N \rtimes H_1$ and H_1 is normal in G (so indeed $G = N \times H_1$).
b) Let $H_2 = \{(a, a) \mid a \in A\}$. Show that $G = N \rtimes H_2$ and H_2 is not normal in G.

Exercise 8.11: Let $K \cong \mathbb{F}_q$ be a finite field of cardinality q, let $n \in \mathbb{Z}^+$, and let V, W be two nondegenerate n-dimensional quadratic spaces over K.
a) Suppose n is odd. Show that $O(V_1) \cong O(V_2)$.
b) Suppose n is even. Show that the following are equivalent:

(i) $V \cong W$.
(ii) Either V and W are both hyperbolic or neither one is hyperbolic.
(iii) $O(V) \cong O(W)$.

Exercise 8.12: Let $K \cong \mathbb{F}_q$ be a finite field of cardinality q, and let V be an n-dimensional non-degenerate quadratic space over K.
a) Suppse that $n = 2k+1$ is odd. Show:

$$\#O(V) = 2q^k \prod_{i=0}^{k-1} \left(q^{2k} - q^{2i}\right).$$

b) Suppose $n = 2k$ is even and $-1 \in K^{\times 2}$. Show:

$$\#O(V) = 2(q^k - 1) \prod_{i=1}^{n-1} \left(q^{2k} - q^{2i}\right).$$

c) Suppose $n = 2k$ is even and $-1 \notin K^{\times 2}$. Show:

$$\#O(V) = 2(q^k + (-1)^{k+1}) \prod_{i=1}^{k-1} \left(q^{2k} - q^{2i}\right).$$

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 sees V' referred to as the "aniostropic kernel" of V. However, 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 $\oplus$ (orthgonal direct sum) and $\otimes$ (tensor product) are well-defined on equivalence classes of quadratic forms. The Witt Decomposition Theorem immediately yields the identity

$$w[q_1 \oplus q_2] = w[w[q_1] \oplus w[q_2]]. \tag{8}$$

Let $W(K)$ be the set of isomorphism classes of anisotropic quadratic forms over K. Then (8) 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 $[D_1^{\mathrm{opp}}]$, it turns out that repeated extraction of anisotropic cores

makes $W(K)$ into a group. Explicitly, the inverse of $[q] = [\langle a_1, \ldots, a_n \rangle]$ in $W(K)$ is given by $[-1 \cdot q] = [\langle -a_1, \ldots, -a_n \rangle]$. Indeed,

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

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 $M(K)$ 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 $M(K)$ 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 $M \to G(M)$ 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 comutative, the general construction is essentially more complicated in only 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 $M \times M \to G(M)$, $(a, b) \mapsto [a, b]$, 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.
a) Let $G : M \to G(M)$ by $x \mapsto [x, 0]$. Show that G is a homomorphism of monoids.
b) Show that $G : M \to G(M)$ 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 9.1. *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 $M(K)$ is a cancellative monoid, and thus $M(K)$ 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

$$\dim : M(K) \to \mathbb{Z}$$

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

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

(In less fancy language, we simply put $\dim([q_1] - [q_2]) = \dim[q_1] - \dim[q_2]$.)[6]

Proposition 9.2. *As an abelian group, $\hat{I}$ is generated by expressions of the form $\langle a \rangle - \langle 1 \rangle$ for $a \in K^\times$.*

Proof. An element x of $\hat{I}$ is of the form $q_1 - q_2$, where $q_1 = \langle a_1, \ldots, a_n \rangle$, $q_2 = \langle b_1, \ldots, b_n \rangle$. Thus

$$x = \sum_{i=1}^{n} \langle a_i \rangle - \sum_{i=1}^{n} \langle b_i \rangle = \sum_{i=1}^{n} \left(\langle a_i \rangle - \langle 1 \rangle \right) - \sum_{i=1}^{n} \left(\langle b_i \rangle - \langle 1 \rangle \right).$$

□

Corollary 9.3. *As an abelian group, I is generated by equivalence classes of quadratic forms $\langle 1, -a \rangle$ for $a \in K^\times$.*

Proof. Indeed $\langle 1, -a \rangle = \langle 1 \rangle + \langle -a \rangle \equiv \langle 1 \rangle + \langle -a \rangle - \langle a, -a \rangle = \langle 1 \rangle - \langle a \rangle$, so this follows from Proposition 9.2. □

Recall that we also have a product operation, $\otimes$, which makes $M(K)$ 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 $[a, b] \cdot [c - d] :=$

[6] In *more* fancy language, the dimension map is naturally a homomorphism of monoids $M(K) \to (\mathbb{N}, +)$. By the functoriality of the Grothendieck group construction, this induces a homomorphism of additive groups $M(K) \to \mathbb{Z}$.

$[ac + bd, ad + bc]$. 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 $\dim : \widehat{W}(K) \to \mathbb{Z}$. 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 9.4. *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 $[q] = [\langle a_1, \ldots, a_n \rangle]$ is a nondegnerate quadratic form, then

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

□

Theorem 9.5. *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 $M(K)$ to the Witt ring $W(K)$. By the universal property of group completion, it factors through a ring homomorphism $\Phi : \widehat{W}(K) \to W(K)$. Evidently $[\mathbb{H}] \in \operatorname{Ker} \Phi$. 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 $[q_1] - [q_2] \cong (I_1 - I_2)[\mathbb{H}] \in \langle [\mathbb{H}] \rangle$. □

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 $\dim : W(K) \to \mathbb{Z}/2\mathbb{Z}$, 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 $\operatorname{char}(k) \neq 2$ – 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 5.1.)

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 ([Lam73, Thm. 3.2]): For a two dimensional quadratic space (V, q), the following are equivalent:
(i) V is regular and isotropic.
(ii) V is regular with discriminant -1.
(iii) V is isometric to the hyperbolic plane $\mathbb{H} = \langle 1, -1 \rangle$.

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 $\dim(\operatorname{rad} V) + I(V)$.

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.[7]
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 $-1 \notin K^{\times 2}$.

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:

$$[ab^2] = [a], \forall a, b \in K^\times,$$
$$[a] + [b] = [a + b] + [ab(a + b)], \forall a, b \in K^\times \mid a + b \in K^\times.$$

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 comutative 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

[7] Alternately, this is a special case of the **Chevalley-Warning theorem**.

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 6.9 and repeated Witt Cancellation.)

References

[A] E. Artin, *Geometric Algebra*. Interscience Publishers, Inc., New York-London, 1957.

[Cas] J.W.S. Cassels, *Rational quadratic forms*. London Mathematical Society Monographs, 13. Academic Press, Inc., 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.

[Lam73] T.-Y. Lam, *Algebraic Theory of Quadratic Forms*, 1973.

[Lam] T.Y. Lam, *Introduction to quadratic forms over fields*. Graduate Studies in Mathematics, 67. American Mathematical Society, Providence, RI, 2005.

[OM00] T.O. O'Meara, *Introduction to quadratic forms*. Reprint of the 1973 edition. Classics in Mathematics. Springer-Verlag, Berlin, 2000.

[Ste] E. Steinitz, *Algebraische Theorie der Körper*. J. Reine Angew. Math. 137 (1910), 167-309.

[Wit] E. Witt, *Theorie der quadratischen Formen in beliebigen Körpern*. J. Reine Angew. Math. 176 (1937), 31-44.