6. Forms and polar spaces

In this section V is a vector space over a field k.

6.1. Sesquilinear forms. A *sesquilinear* form on V is a function

$$\beta : V \times V \to k$$

for which there exists $\sigma \in \mathrm{Aut}(k)$ such that

(1) $\beta(c_1x_1 + c_2x_2, y) = c_1\beta(x_1, y) + c_2\beta(x_2, y)$ for all $c_1, c_2 \in k$ and $x_1, x_2, y \in V$;
(2) $\beta(x, c_1y_1 + c_2y_2) = c_1^\sigma\beta(x, y_1) + c_2^\sigma\beta(x, y_2)$ for all c_1, c_2 in k and $x, y_1, y_2 \in V$.

In this case we say that β is *σ-sesquilinear*. If $\sigma = 1$, then k is a field and β is *bilinear*. We define

(1) The *left radical* of β is $\{x \in V \mid \beta(x, y) = 0, \forall y \in V\}$.
(2) The *right radical* of β is $\{y \in V \mid \beta(x, y) = 0, \forall x \in V\}$.

(E60*) *Prove that the left and right radicals are subspaces.*

(E61*) *Prove that if $\dim V < \infty$, then the left and right radicals have the same dimension. Give a counter-example to this assertion when $\dim V = \infty$.*

From here on we will assume that $n := \dim V < \infty$. We call β *non-degenerate* if its left and right radicals are trivial.

Recall that a *duality* of $\mathrm{PG}_{n-1}(k)$ is a weak automorphism that maps a subspace of dimension d to a subspace of dimension $n - d$. We can construct a duality from a non-degenerate sesquilinear form β as follows: for $y \in V$ define

$$\beta_y : V \to k,\ x \mapsto \beta(x, y).$$

Observe that the map $V \to V^*, y \mapsto \beta_y$ is a σ-semilinear bijection, and so induces an isomorphism $\mathrm{PG}(V) \to \mathrm{PG}(V^*)$. Now composing with the inverse of the 'annihilator map', $U \to U^\dagger$, which we have seen already, we obtain the duality

e: perp (9) $$\mathrm{PG}(V) \to \mathrm{PG}(V), U \mapsto U^\perp := \{x \in V \mid \beta(x, y) = 0 \text{ for all } y \in U\}.$$

(E62*) *Check that this is a duality*

t: sesq **Theorem 28.** *If $n \geq 3$, then any duality Δ of $\mathrm{PG}(V)$ has form $U \to U^\perp$ where $U^\perp$ is defined via (9) for some non-degenerate sesquilinear form β.*

Proof. Proposition 16 implies that $\Delta = st^{-1}$ where s is induced by a semilinear bijection $\phi : V \to V^*$ and $t : U \to U^\dagger$ is the annihilator map. Now set

$$\beta : V \times V \to k, (x, y) \mapsto x^{y\phi}$$

and the result follows. □

Let us fix β to be a σ-sesquilinear form on V. We say β is *reflexive* if $\beta(x, y) = 0$ implies $\beta(y, x) = 0$. For a reflexive form, the left and right radicals coincide and we shall just call this subspace the *radical* of β,

$$\mathrm{Rad}(\beta) := \{v \in V \mid \beta(v, w) = 0 \text{ for all } w \in V\}.$$

Recall that the form β is non-degenerate if and only if $\mathrm{Rad}(\beta) = \{0\}$.

Observe that $U \to (U^\perp)^\perp$ is a collineation of $\mathrm{PG}(V)$. A *polarity* is a duality with $U = (U^\perp)^\perp$ for all $U \leq V$.

Lemma 29. *Let β be non-degenerate. The duality (9) is a polarity if and only if β is reflexive.*

Proof. The form β is reflexive if and only if

$$x \in \langle y\rangle^\perp \Longrightarrow y \in \langle x\rangle^\perp.$$

Thus if β is reflexive, then $U \leq U^{\perp\perp}$ for all $U \leq V$. Now, since β is non-degenerate,

$$\dim(U^{\perp\perp}) = \dim(V) - \dim(U^\perp) = \dim(U),$$

and so $U = U^{\perp\perp}$ for all U.

For the converse, given a polarity $\perp$, if $y \in \langle x\rangle^\perp$, then $x \in \langle x\rangle^{\perp\perp} \leq \langle y\rangle^\perp$ and we are done. □

We say that β is

(1) *σ-Hermitian*, where $\sigma \in \mathrm{Aut}(k)$, if $\beta(y,x) = \beta(x,y)^\sigma$ for all $x,y \in V$;
(2) *symmetric*, if $\beta(y,x) = \beta(x,y)$ for all $x,y \in V$;
(3) *alternating*, if $\beta(x,x) = 0$ for all $x \in V$;
(4) *skew-symmetric*, if $\beta(x,y) = -\beta(y,x)$ for all $x,y \in V$.

Note: if we say 'β is σ-Hermitian', we will implicitly assume that $\sigma \neq 1$, otherwise we would say that 'β is symmetric'. We record a number of easy observations in the next lemma.

qui easy

Lemma 30. (1) *If β is σ-Hermitian, then $\sigma^2 = 1$ and $\beta(x,x) \in \mathrm{Fix}(\sigma)$ for all $x \in V$;*
(2) *If β is alternating, symmetric or skew-symmetric, then β is bilinear;*
(3) *If $\mathrm{char}(k) = 2$ and β is alternating, then β is symmetric;*
(4) *If $\mathrm{char}(k) \neq 2$, then β is alternating if and only if β is skew-symmetric.*
(5) *If β is σ-Hermitian, symmetric, alternating or skew-symmetric, then β is reflexive.*

Proof. (1) is easy. For (3) and (4) assume that β is alternating and observe that, for $x,y \in V$,

$$0 = \beta(x+y,x+y) = \beta(x,x) + \beta(x,y) + \beta(y,x) + \beta(y,y) = \beta(x,y) + \beta(y,x).$$

and the statements follow. For (2) and (5) the result is obvious unless β is alternating. But in that case, (3) and (4) imply that β is either symmetric or skew-symmetric, and the result follows. □

Theorem 32, proved below, is the partial converse to (5).

6.2. **Matrices and the classification of forms.** Let us fix a basis $\mathcal{B}$ for V and let β be a σ-sesquilinear form. Let $e_1, \dots, e_n$ be the elementary matrices in V and define A to be the matrix such that $A_{ij} = \beta_{e_i,e_j}$. Then one can check directly that, for $x,y \in V$, we have

$$\beta(x,y) = x \cdot A \cdot (y^T)^\sigma.$$

We call A *the matrix for β with respect to $\mathcal{B}$* and denote it $(\beta)_{\mathcal{B}}$. Note that here we are treating x and y as row vectors; what is more, writing y_i for the i-th entry of the row vector y, we write $(y^T)^\sigma$ to mean the column vector whose i-th entry is y_i^σ.

The following proposition connects properties of β to properties of A.

matrix

Proposition 31. *Let β be a σ-sesquilinear form and A the matrix for β with respect to some basis.*

(1) *β is non-degenerate $\Longleftrightarrow$ $\mathrm{rank}(A) = n$;*
(2) *β is σ-Hermitian $\Longleftrightarrow$ $\sigma^2 = 1 \neq \sigma$ and $A = (A^T)^\sigma$;*
(3) *β is symmetric $\Longleftrightarrow$ $\sigma = 1$ and $A = A^T$; for $i = 1, \dots, n$;*
(4) *β is skew-symmetric $\Longleftrightarrow$ $\sigma = 1$ and $A = -A^T$;*

Proof. **(E63)** *Prove this. There is a similar condition for β alternating; what is it?*

□

We are now ready to classify reflexive σ-sesquilinear forms. In the course of the proof we will encounter a matrix characterization of such a form.

fy forms

Theorem 32. *Let $\beta : V \times V \to k$ be a reflexive σ-sesquilinear form. If* $\dim(V/\mathrm{Rad}(\beta)) \geq 3$*, then β is of one of the following types:*

(1) *alternating;*
(2) *symmetric;*
(3) *a scalar multiple of a σ-Hermitian form with $\sigma^2 = 1 \neq \sigma$.*

The proof that follows comes directly from Cameron's *Classical Groups*: http://www.maths.qmul.ac.uk/~pjc/class_gps/

Proof. **1. Claim**: It is sufficient to prove the theorem for the case when β is non-degenerate. **Proof of claim**: Suppose that $\beta : V \times V \to k$ is degenerate. Write R for the radical $\mathrm{Rad}(\beta)$. Then define the form

$$\beta_0 : V/R \times V/R \to k, (x+R, y+R) \mapsto \beta(x,y).$$

It is easy to check that β_0 is a well-defined, non-degenerate, reflexive σ-sesquilinear form. If we assume that the theorem is true for non-degenerate forms, then β_0 is one of the three listed types. Now, since $\beta(x,y) = \beta_0(x+R, y+R)$, β is also one of the three listed types and we are done.

Thus we assume from here on that β is non-degenerate.

2. Assume that β is bilinear. Then observe that, for all $u, v, w \in V$, we have

e: key

$$\begin{aligned} & \beta(u,v)\beta(u,w) - \beta(u,w)\beta(u,v) = 0 \\ \text{(bilinearity)} \quad & \Longrightarrow \beta(u, \beta(u,v)w - \beta(u,w)v) = 0 \\ \text{(reflexivity)} \quad & \Longrightarrow \beta(\beta(u,v)w - \beta(u,w)v, u) = 0 \\ \text{(bilinearity)} \quad & \Longrightarrow \beta(u,v)\beta(w,u) = \beta(v,u)\beta(u,w) \qquad (10) \end{aligned}$$

We call $u \in V$ *fine* if there exists v with $\beta(u,v) = \beta(v,u) \neq 0$.

2a. Assume all $u \in V$ are not fine. Putting $u = w$ in (10) we obtain that

$$\beta(u,u)(\beta(u,v) - \beta(v,u)) = 0.$$

Now, since u is not fine and β is non-degenerate, there exists v with $\beta(u,v) \neq \beta(v,u)$. Thus we conclude that $\beta(u,u) = 0$. Since the same is true for all $u \in V$, β is alternating.

2b. Assume that there exists fine $u \in V$. Let v be a vector such that $\beta(u,v) = \beta(v,u) \neq 0$. We want to show that in this case β is symmetric. Observe first that (10) implies that $\beta(u,w) = \beta(w,u)$ for all $w \in V$.

Now observe that, by definition, any vector x such that $\beta(u,x) \neq 0$ is fine and so $\beta(x,w) = \beta(w,x)$ for all $w \in V$. Now suppose that $x \neq u$ is a vector such that $\beta(u,x) = 0$. Then $\beta(u, x+v) \neq 0$ and so $x+v$ is fine and so, for all $w \in V$, we have

$$\begin{aligned} & \beta(x+v, w) = \beta(w, x+v) \\ \Longrightarrow & \beta(x,w) + \beta(v,w) = \beta(w,x) + \beta(w,v) \\ \Longrightarrow & \beta(x,w)\beta(w,x). \end{aligned}$$

The result follows.

3. Claim: Let σ be a non-identity automorphism of k of order 2. Then $\{\lambda \in k \mid \lambda\lambda^\sigma = 1\} = \{\epsilon/\epsilon^\sigma \mid \epsilon \in k\}$

(E64*) *Prove the claim.*

(E65) *Use the claim to complete the proof.*

□

6.3. **Trace-valued forms.** Let k be a field and $\sigma \in \mathrm{Aut}(k)$ with $o(\sigma) \in \{1, 2\}$. Define

$$\mathrm{Fix}(\sigma) := \{c \in k \mid \sigma(c) = c\}$$
$$\mathrm{Trace}(\sigma) := \{c + c\sigma \mid c \in k\}.$$

The following exercises list the key properties of these subsets.

(E66) $\mathrm{Fix}(\sigma)$ *and* $\mathrm{Trace}(\sigma)$ *are both subfields of* k

: trace

(E67) *Fix*$(\sigma) = \mathrm{Trace}(\sigma)$ *unless* $\mathrm{char}(k) = 2$ *and* $\sigma = 1$*, in which case* $\mathrm{Trace}(\sigma) = \{0\}$.

If β is a σ-sesquilinear form, then we call β *trace-valued* if $\beta(x, x) \in \mathrm{Trace}(\sigma)$ for all x. Recall that, by Lemma 30, $\beta(x, x) \in \mathrm{Fix}(\sigma)$. This, and (E67), immediately yield the following result.

Lemma 33. *A* σ*-sesquilinear form is not trace-valued if and only if* $\mathrm{char}(k) = 2$ *and* β *is symmetric and not alternating.*

In what follows we will study only trace-valued forms, and this will be enough for us to define and study all of the finite classical groups. One reason to avoid non-trace-valued forms is given by the following exercise. Recall that a field of characteristic 2 is called *perfect* if the map $x \mapsto x^2$ is an automorphism. In particular a finite field of characteristic 2 is perfect.

(E68) *Let* $\mathrm{char}(k) = 2$ *and suppose that* k *is perfect. Let* β *be symmetric and define*

$$U := \{x \in V \mid \beta(x, x) = 0\}.$$

Then U *is a subspace of dimension at least* $n - 1$.

When we come to study isometries we shall see that this exercise implies that the isometry group of a non-trace-valued form cannot act *irreducibly* on the underlying vector space.

6.4. **Quadratic forms.** A *quadratic form* on V is a function $Q : V \to k$ such that

- $Q(cx) = c^2 Q(x)$ for all $c \in k, x \in V$;
- The function

$$\beta_Q : V \times V \to k, (x, y) \mapsto= Q(x + y) - Q(x) - Q(y)$$

is a bilinear form.

The form β_Q is called the *polarization of* Q. Observe that β_Q is symmetric. If $\mathrm{char}(k) = 2$, then it is also alternating (and so, in particular, β_Q is always trace-valued).

A quadratic form can be thought of as a homogeneous polynomial of degree 2 with coefficients in k. The next exercise makes this clear, as well as connecting quadratic forms to matrices.

(E69*) *Fix a basis* $\mathcal{B} = \{x_1, \dots, x_n\}$ *for* V *and let* $Q : V \to k$ *be a quadratic form. There is a matrix* A *such that* $Q(x) = xAx^T$. *Moreover*

$$A_{ij} = \begin{cases} \beta_Q(x_i, x_j), & \text{if } i < j, \\ Q(x_i), & \text{if } i = j, \\ 0, & \text{otherwise.} \end{cases}$$

The significance of quadratic forms depends on the characteristic of the field.

Suppose that $\mathrm{char}(k)$ **is odd.** In this case the study of quadratic forms is equivalent to the study of symmetric bilinear forms. For, from every quadratic form Q, one obtains a symmetric bilinear form β_Q, and the next exercise shows that one can reverse this:

(E70) *If* $\mathrm{char}(k) \neq 2$*, then* $Q(x) = \frac{1}{2}\beta_Q(x, x)$.

In particular a vector x satisfies $Q(x) = 0$ if and only if $\beta_Q(x, x) = 0$.

Suppose that $\mathrm{char}(k) = 2$**.** Our restriction to the study of trace-valued forms means that, by studying alternating forms, we cover all symmetric forms in which we are interested. However we also choose to also study quadratic forms because we obtain some interesting extra structure, as follows.

We know that, from every quadratic form Q, one obtains a symmetric, alternating bilinear form β_Q. However, in the reverse direction, suppose that β is a symmetric, alternating bilinear form with associated matrix B with respect to some basis β. Now define the matrix A via

$$A_{ij} = \begin{cases} B_{ij}, & \text{if } i < j, \\ 0, & \text{if } i > j. \end{cases}$$

We have not defined the diagonal on the matrix A - we can set it to be anything that we choose. Now define $Q(x) = x^T Ax$.

(E71*) *Check that Q polarizes to β.*

Thus we find that many quadratic forms polarize to the same alternating form. In particular it is **not true** in general that a vector x satisfies $Q(x) = 0$ if and only if $\beta_Q(x, x) = 0$. We shall see that this fact results in the geometric behaviour of Q and β_Q being very different.

Let $Q : V \to k$ be a quadratic form. Recall the definition of the *radical* of β_Q,

$$\mathrm{Rad}(\beta_Q) := \{v \in V \mid \beta_Q(v, w) = 0 \text{ for all } w \in V\}.$$

We define the *singular radical* of a quadratic form to be

$$\{v \in \mathrm{Rad}(\beta_Q) \mid Q(v) = 0\}.$$

If the singular radical of Q is trivial, then we say that Q is *non-degenerate.*

(E72) *If* $\mathrm{char}(k) \neq 2$*, then β_Q is non-degenerate if and only if Q is non-degenerate.*

e: kkk

(E73*) *If* $\mathrm{char}(k) = 2$*, k is perfect, and $Q : V \to k$ is non-degenerate, then* $\dim(\mathrm{Rad}(\beta_Q)) \leq 1$*.*

6.5. **Formed spaces.** We write (V, β) (resp. (V, Q)) to mean a vector space equipped with a trace-valued non-degenerate reflexive σ-sesquilinear form β (resp. non-singular quadratic form Q). We call such a pair a *formed space.*

Then

- (V, β) is called *symplectic* if β is alternating;
- (V, β) is called *unitary* if β is σ-Hermitian;
- (V, β) is called *orthogonal* if β is symmetric and $\mathrm{char}(k) \neq 2$;
- (V, Q) is called *orthogonal*;

In fact we will not need to consider the third of these, since they are a subclass of the fourth. We will say a number of formed spaces are *of the same type* if they are all σ-Hermitian or all alternating or all symmetric.

Two formed spaces (V_1, Q_1) and (V_2, Q_2) are isomorphic if there exists an invertible linear map $A : V_1 \to V_2$ such that $Q_2 \circ A = Q_1$. A similar definition applies for forms β_1 and β_2. [6]

Let U be a vector subspace of a formed space (V, β), and write $\perp$ for the polarity defined by β. Then

- a vector $u \in V$ is *isotropic* if $\beta(u, u) = 0$;
- U is *totally isotropic* if $\beta(u, v) = 0$ for all $u, v \in U$ (equivalently, if $U \subseteq U^\perp$);
- U is *non-degenerate* if $\beta|_U$ is non-degenerate;

[6] If working with two symmetric spaces over a field of odd characteristic, one with a quadratic form, the other with a symmetric bilinear form, then there is an obvious notion of isomorphism which we will not write down here.

- U is a *hyperbolic line* if $U = \langle u, v\rangle$ and
$$\beta(u,u) = \beta(v,v) = 0, \ \beta(u,v) = 1.$$
The pair (u,v) is called a *hyperbolic pair*. (Notice that u and v must be linearly independent, so $\dim(U) = 2$.)

Let U be a vector subspace of a formed space (V,Q), and write $\perp$ for the polarity defined by the polarized form β_Q. Then the above definitions all apply with respect to the polarized form β_Q. In addition

- a vector $u \in V$ is *singular* if $Q(u) = 0$;
- U is *totally singular* if $Q(u) = 0$ for all $u \in U$.

We are working towards a classification of formed spaces in which we build them up from smaller spaces. We need to define what me mean by "building up." Let $(U_1,\beta_1),\dots,(U_\ell,\beta_\ell)$ be formed spaces of the same type. Define *the orthogonal direct sum* $U_1 \perp \cdots \perp U_\ell$ to be the vector space $V = U_1 \oplus \cdots \oplus U_\ell$ with associated form

$$\begin{aligned}\beta := \beta_1 \perp \cdots \perp \beta_\ell : (U_1 \perp \cdots \perp U_\ell) \times (U_1 \perp \cdots \perp U_\ell) &\to k \\ ((u_1,\dots,u_\ell),(v_1,\dots,v_\ell)) &\mapsto \sum_{i=1}^{\ell} \beta(u_i,v_i).\end{aligned}$$

Notice that, for each i, the space V has a subspace

$$V_i := 0 \perp \cdots 0 \perp U_i \perp 0 \cdots \perp 0$$

such that $\beta|_{V_i} = \beta_i$. We will often abuse notation and identify U_i and V_i, so that we can think of (V,β) as a direct sum of k of its subspaces.

An obvious analogous notion of orthgonal direct sum also exists for formed spaces involving a quadratic form.

(E74) *Any two hyperbolic lines of the same type are isomorphic (as formed spaces).*

(E75) *Suppose that U, U' (resp. W, W') are isomorphic formed spaces of the same type. Then $U \perp W$ and $U' \perp W'$ are isomorphic formed spaces.*

Two more definitions:

- A formed space (V,β) is called *anisotropic* if $\beta(x,x) \neq 0$ for all $x \in V\backslash\{0\}$.
- A formed space (V,Q) is called *anisotropic* if $Q(x) \neq 0$ for all $x \in V\backslash\{0\}$.

d spaces

Theorem 34. *A formed space (V,β) (resp. (V,Q)) is the orthogonal direct sum of a number r of hyperbolic lines and an anisotropic space U.*

Proof. Define a function $f : V \to k$ which maps a vector x to $\beta(x,x)$ (resp. $Q(x)$). If V is anisotropic, then V does not contain a hyperbolic line, so $r = 0$ and U must equal V. Suppose then, that $f(v) = 0$ for some $v \in V\backslash\{0\}$. In the sesquilinear case, non-degeneracy implies that there exists $w \in V$ such that $\beta(v,w) \neq 0$. In the quadratic case, we claim there exists $w \in V$ such that $\beta(v,w) \neq 0$ where β is the polarized form. The claim follows because if no such w existed, then v would be in the radical of β and hence in the singular radical of κ which contradicts the fact that κ is non-singular.

We can replace w by a scalar multiple so that $\beta(v,w) = 1$. Observe that $\beta(v, w - \lambda v) = 1$ for all $\lambda \in k$. If we can find a value of λ for which $f(w - \lambda v) = 0$, then $\langle v, w\rangle$ will be a hyperbolic line. Consider three cases:

(1) If the form is alternating, then any value of λ works.

(2) If the form is σ-Hermitian, then

$$\begin{aligned} f(w-\lambda v) &= f(w) - \lambda\beta(v,w) - \lambda^\sigma\beta(w,v) + \lambda\lambda^\sigma f(v) \\ &= f(w) - (\lambda + \lambda^\sigma); \end{aligned}$$

and, since β is trace-valued, there exists $\lambda \in k$ with $\lambda + \lambda^\sigma = f(w)$ and we are done.

(3) If the form is quadratic, then

$$\begin{aligned} f(w-\lambda v) &= f(w) - \lambda\beta(w,v) + \lambda^2 f(v) \\ &= f(w) - \lambda \end{aligned}$$

and we choose $\lambda = f(w)$.

Now let W_1 be the hyperbolic line $\langle v, w - \lambda v\rangle$, and let $V_1 = W_1^\perp$.

(E76*) *$V = V_1 \oplus W_1$ and the restriction of the form to V_1 is non-degenerate (resp. non-singular).*

We conclude, by induction, that a decomposition of the given kind exists. □

In the next section we will prove Witt's Lemma, a corollary of which states that the number r and the isomorphism class of the space U, defined in Theorem 34, are invariants of the formed space (V,κ). We call r the *polar rank*, or the *Witt index*, of V, and U the *germ* of V.

It is worth taking a moment to reflect on the power of Theorem 34. Let us just consider the case where the form κ is σ-sesquilinear (there is a similar analysis when we have a quadratic form). Theorem 34 asserts that there is a basis for V such that

$$\beta(x,y) = xA(y^T)^\sigma$$

where the matrix A has form

$$\begin{pmatrix} A_{HL} & & & \\ & \ddots & & \\ & & A_{HL} & \\ & & & A_{An} \end{pmatrix}$$

where A_{HL} is a 2×2 matrix associated with a hyperbolic line, and A_{An} is a square matrix associated with an anisotropic form. Indeed we can be more precise:

$$A_{HL} = \begin{cases} \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}, & \kappa \text{ is alternating;} \\ \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, & \text{otherwise.} \end{cases}$$

We shall spend some time in §7.2 studying the possibilities for A_{An}; in particular, we will see that it too has dimension at most 2.

7. Isometries and Witt's Lemma

For $i = 1,2$, let β_i be a σ-sesquilinear form on a vector space V_i over a field k. We define

- an *isometry* between β_1 and β_2 to be an invertible linear map $g : V_1 \to V_2$ such that

$$\beta_2(xg, yg) = \beta_1(x,y), \text{ for all } x, y \in V_1.$$

- a *similarity* between β_1 and β_2 to be an invertible linear map $g : V_1 \to V_2$ for which there exists $c \in k$ such that

$$\beta_2(xg, yg) = c\beta_1(x,y), \text{ for all } x, y \in V_1.$$

- a *semisimilarity* between β_1 and β_2 to be an invertible semilinear map $g : V_1 \to V_2$ for which there exists $c \in k$ such that
$$\beta_2(xg, yg) = c\beta_1(x, y), \text{ for all } x, y \in V_1.$$

For $i = 1, 2$, let Q_i be a quadratic form on a vector space V_i over a field k. We define

- an *isometry* between Q_1 and Q_2 to be an invertible linear map $g : V_1 \to V_2$ such that
$$Q_2(xg) = Q_1(x), \text{ for all } x \in V_1,$$
- a *similarity* between Q_1 and Q_2 to be an invertible linear map $g : V_1 \to V_2$ for which there exists $c \in k$ such that
$$Q_2(xg) = cQ_1(x), \text{ for all } x \in V_1,$$
- a *semisimilarity* between Q_1 and Q_2 to be an invertible semilinear map $g : V_1 \to V_2$ for which there exists $c \in k$ such that
$$Q_2(xg) = cQ_1(x), \text{ for all } x \in V_1,$$

Now write κ_i for $\beta_i/ \ Q_i$ as appropriate. If $(V_1, \kappa_1) = (V_2, \kappa_2)$, then we drop the subscripts and we refer to *an isometry of* (V, κ), and similarly with similarities and semisimilarities. Now we define several subgroups of $GL(V)$:

- $\text{Isom}(\kappa)$: the set of isometries of κ;
- $\text{Sim}(\kappa)$: the set of similarities of κ;
- $\text{SemiSim}(\kappa)$: the set of semisimilarities of κ.

Observe that
$$\text{Isom}(\kappa) \leq \text{Sim}(\kappa) \leq \text{SemiSim}(\kappa).$$

Before we move on, let us note the connection to matrices. Fix a basis for the vector space V and fix κ to be a σ-sesquilinear form given by
$$\kappa(x, y) = xA(y^T)^\sigma$$
where A is some matrix. Then
$$\text{Isom}(\kappa) = \{X \mid X^T A X^\sigma = A\}.$$
One can give similar formulations for similarities and semisimilarities, and for quadratic forms. [7]

7.1. **Witt's lemma.** We call (V, κ) a *(de)formed space* if it is a pair satisfying all the conditions to be a formed space with the possible exception of non-degeneracy. In this section we prove a crucial result concerning (de)formed spaces which allows us to extend isometries between subspaces to isometries of the full space.

> **(E77)** *Let β be a σ-Hermitian, or alternating form, with radical* $\text{Rad}(V)$. *Prove that the natural map $V \to V/\text{Rad}(V)$ is an isometry. What happens if we ask the same question with β replaced by a quadratic form Q?*

Theorem 35. (Witt's Lemma) *Let (V, β) be a (de)formed space, U a subspace of V and*
$$h : U \to Uh < V$$
an isometry. Then h extends to an isometry $g : V \to V$ if and only if
$$(U \cap Rad(V))h = Uh \cap Rad(V).$$
In particular, if the radical is trivial, then any h extends.

[7] We have rarely mentioned the complex numbers in this course. But, letting $k = \mathbb{C}$ and taking $A = I$ and $\sigma = 1$, you should observe that $\text{Isom}(\kappa)$ is then the set of orthogonal matrices over $\mathbb{C}$, a group you undoubtedly encountered at some point during undergraduate mathematics.

Proof. **1. "only if"** Suppose that g is an isometry $V \to V$ with $g|_U = h$. Then

$$(U \cap \mathrm{Rad}(V))h = (U \cap Rad(V))g = Ug \cap Rad(V) = Uh \cap Rad(V),$$

and we are done.

2. "if" Suppose that $(U \cap Rad(V))h = Uh \cap Rad(V)$.

> **(E78*)** *Let U_1 and U_2 be subspaces of a vector space V having the same dimension. Show that there is a subspace W of V which is a complement for both U_1 and U_2.*

2a. It is sufficient to assume that $\mathrm{Rad}(V) \leq U \cap Uh$. Suppose that U and Uh don't contain $\mathrm{Rad}(V)$. Observe that, by supposition, $\dim(U \cap \mathrm{Rad}(V)) = \dim(Uh \cap \mathrm{Rad}(V))$, and let W be a common complement to $U \cap \mathrm{Rad}(V)$ and $Uh \cap Rad(V)$ in $\mathrm{Rad}(V)$. Now extend h to $h \oplus 1 : U \oplus W \to Uh \oplus W$ and observe that it is an isometry.

2b. Assume that $\mathrm{Rad}(V) \leq U \cap Uh$. We proceed by induction on $\dim(U)/\mathrm{Rad}(V)$.

2c. Base case. If $U = \mathrm{Rad}(V) = Uh$, then choose a complement W to U in V and extend h by the identity on W. The base case is done.

2d. Inductive step. Assume that the result holds for V', U', h' whenever

$$\dim(U'/\mathrm{Rad}(V')) \leq \dim(U/\mathrm{Rad}(V)).$$

Let H be a hyperplane of U containing $\mathrm{Rad}(V)$. Then $h|_H$ extends to an isometry g' of V. It is enough to show that $h(g')^{-1}$ extends to an isometry; in other words we may assume that h is the identity on H.

If h is the identity on U, then we may take $g = 1$. Thus we assume that $h \neq 1$ and so $\ker(h-1) = H$ and the image of $h - 1$ is a one-dimensional subspace P of Uh. Since h is an isometry, if $x, y \in U$, then

$$\begin{aligned}\beta(xh, y(h-1)) &= \beta(xh, yh) - \beta(xh, y)\\ &= \beta(x, y) - \beta(xh, y)\\ &= \beta(x - xh, y).\end{aligned}$$

Observe that, if $y \in H$, then the left hand side equals zero. Since $x - xh = -x(h-1) \in P$, we conclude that $H \leq P^\perp$.

Suppose next that $P \not\leq U^\perp$. Then $P \not\leq (Uh)^\perp$ and so $U \cap P^\perp - H = Uh \cap P^\perp$. Thus if W is a complement to H in $P^\perp$, then we can extend h to $h \oplus 1 : U \oplus W \to Uh \oplus W$ and observe that it is an isometry. Now induction gives the result. Thus we assume that $P \leq U^\perp$ and, in particular, $U, Uh, P \leq P^\perp$.

Suppose next that U, Uh and $P^\perp$ do not all coincide. If $U \neq Uh$, then $U_i = \langle H, u_1\rangle$ for $i = 1, 2$. Let W_0 be a complement for $U + Uh$ in $P^\perp$, and $W = \langle W_0, u_1 + u_2\rangle$; then h can be extended by the identity on W to an isometry on $P^\perp$. If, on the other hand $U = Uh \neq P^\perp$, then let W be a complement to U in $P^\perp$ and, once again, h can be extended by the identity on W to an isometry on $P^\perp$. Now the result follows by induction. We conclude that $U = Uh = P^\perp$.

Write $P = \langle x\rangle$ where $x = uh - u$ for some $u \in U$. Observe that $\beta(x, x) = 0$ and, in the orthogonal case

$$Q(x) = Q(uh - u) = Q(uh) + Q(u) - \beta(uh, u) = 2Q(u) - \beta(u, u) = 0.$$

Thus x is isotropic (singular in the orthogonal case), and there is a hyperbolic plane $L = \langle x, y\rangle$. Observe that $y \notin P^\perp$, thus it is sufficient to extend h to $\langle U, y\rangle$.

Now $\langle x\rangle$ is a hyperplane in L, thus $L^\perp h$ is a hyperplane in $\langle xh\rangle^\perp$. Thus there exists $y' \in V \backslash U$ such that $\langle xh, y'\rangle^\perp = L^\perp h$. Now, $\langle xh, t'\rangle = \langle xh, y''\rangle$ for some $y'' \in V\backslash U$ such that (x, y') is a hyperbolic pair.

We define $h' : y \to y'$ and, since $h \oplus h'$ is an isometry, we are done.

(E79) *Check that $h \oplus h'$ is an isometry.*

□

Witt's lemma has several important corollaries, which we leave as exercises.

witt

(E80*) *Let (V, κ) be a formed space. Then the Witt index and the isomorphism class of a maximal anisotropic subspace are determined.*

witless

(E81*) *Let (V, κ) be a formed space. Any maximal totally isotropic/ totally singular subspaces in V have the same dimension. This dimension is equal to the Witt index.*

d spaces

7.2. **Anisotropic formed spaces.** Let (V, κ) be a formed space. Recall that (V, κ) comes in three flavours. Our aim in this subsection is to refine Theorem 32 in each case – the first we can do in total generality; for the other two we restrict ourselves to vector spaces over finite fields.

ernating

7.2.1. *Alternating forms.* Our first lemma is nothing more than an observation.

ing germ

Lemma 36. *The only anisotropic space carrying an alternating bilinear form is the zero space.*

A formed space (V, β) with β alternating and bilinear is called a **symplectic space**. Lemma 36 and Theorem 32 implies that there is only one symplectic space of polar rank r. It is the space

($\mathbf{Sp_{2r}}$) with basis $\{v_1, w_1, \dots, v_r, w_r\}$ where, for $i = 1, \dots, r$, (v_i, w_i) are mutually orthogonal hyperbolic pairs.

7.2.2. *σ-Hermitian forms over finite fields.* It is convenient to establish some notation in this setting. Suppose that $k = \mathbb{F}_{q^2}$ for some prime power q. Then k has a unique subfield, k_0, of order q; k_0 is the fixed field of the field automorphism

$$\sigma : k \to k, x \mapsto x^q.$$

We define two important functions

$$\begin{aligned} \mathrm{Tr} : & k \to k_0, c \mapsto c + c^\sigma \\ \mathrm{N} : & k \to k_0, c \mapsto c \cdot c^\sigma \end{aligned}$$

We call Tr the *trace* and N the *norm.* [8]

e: norm

(E82) *The norm and trace functions are surjective.*

ian germ

Lemma 37. *Suppose that (V, β) is a formed space of dimension n over a finite field k with β σ-Hermitian. Then*

1. *$k = \mathbb{F}_q^2$ for some q;*
2. *An anisotropic subspace of V satisfies*

$$\dim(U) = \begin{cases} 0, & \text{if } n \text{ is even;} \\ 1, & \text{if } n \text{ is odd.} \end{cases}$$

3. *The space U is unique up to isomorphism.*

Proof. We know that σ has order 2, hence $k = \mathbb{F}_q^2$ for some q and $\sigma(x) = x^q$. We have proved (1).

To prove (2) we must show that an anisotropic subspace U of V has dimension at most 1. Suppose U is anisotropic of dimension at least 2. Let v, w be orthogonal vectors in U (i.e. $\beta(v, w) = 0$) and, replacing by scalar multiples if necessary, we can assume that $\beta(v, v) = \beta(w, w) = 1$. Consider the function $f(v + cw)$ as c varies over k. (E82) implies that we can choose c such that

[8] These functions have more general definitions for any finite Galois field extension.

$cc^q = -1$ we see that $f(v + cw) = 0$, contradicting the fact that U is anisotropic. Now (2) follows from Theorem 32.

To prove (3) we suppose that $\dim(U) = 1$. If $v \in U$ and $\beta(v, v) = c \in \mathbb{F}_q$ then, since the norm is onto, there is a bijective linear map $A : k \to k$ such that $A\beta(v, v) = 1$. The result follows. □

A formed space (V, β) with β σ-Hermitian (and σ non-trivial) is called a **unitary space**. The lemma and Theorem 32 implies a natural division of unitary spaces, as follows. Note that, in all cases, for $i = 1, \dots, r$, (v_i, w_i) are mutually orthogonal hyperbolic pairs.

($\mathbf{U_{2r}}$) with basis $\{v_1, w_1, \dots, v_r, w_r\}$.

($\mathbf{u_{2r+1}}$) with basis $\{v_1, w_1, \dots, v_r, w_r, u\}$ where $\langle u\rangle$ is anisotropic and orthogonal to $\langle v_1, w_2, \dots, v_r, w_r\rangle$.

Observe in particular that a unitary formed space of dimension n must have polar rank $r = \lfloor \frac{n}{2} \rfloor$.

orthog

7.2.3. *Quadratic forms over finite fields.*

: pippy

(E83*) *Let $a, b \in k^*$. For all $c \in k$, there exist $x, y \in k$ with $ax^2 + by^2 = c$.*

tic germ

Lemma 38. *If (V, Q) is anisotropic over $\mathbb{F}_q$, then $\dim(V) \leq 2$. Furthermore (V, Q) is unique for each dimension except that if q is odd and $\dim(V) = 1$, then there are two such, one a non-square multiple of the other.*

Proof. Assume that $\dim(V) \geq 3$ so that, in particular, β_Q is associated with a polarity of $\mathrm{PG}(V)$. If $\mathrm{char}(k) = 2$, then let $u \in V\backslash\{0\}$ and let $v \in \langle u\rangle^\perp\backslash\langle u\rangle$ (note that such a v exists since $\dim(V) \geq 3$). Then $Q(xu+yv) = x^2Q(u)+y^2Q(v)$ and, since every element of k is a square, there exist $x, y \in k^*$ such that $Q(xu + yv) = 0$, a contradiction.

If $\mathrm{char}(k)$ is odd, then let $u \in V\backslash\{0\}$, $v \in \langle u\rangle^\perp$ and $w \in \langle u, v\rangle^\perp$. By assumption u, v and w are non-singular, and so (E83) implies that there exist $x, y \in k$ such that $x^2Q(u) + y^2Q(v) = -Q(w)$. Then $Q(xu + yv + w) = 0$ and we are done.

If $\dim(V) = 1$, then any quadratic form is equivalent to either x^2 or ζx^2 for ζ a non-square.

Assume, then, that $\dim(V) = 2 \neq \mathrm{char}(k)$. By completing the square, a quadratic form over V is equivalent to one of $x^2 + y^2$, $x^2 + \zeta y^2$ or $\zeta x^2 + \zeta y^2$ where ζ is a non-square.

If $q \equiv 1 \pmod 4$, then $-1 = \alpha^2$ for some $\alpha \in k$ and so $x^2 + y^2 = (x + \alpha y)(x - \alpha y)$ and so the first and third forms are not anisotropic.

If $q \equiv 3 \pmod 4$, then we can assume that $\zeta = -1$. Now the second form is $(x + y)(x - y)$ which is not anisotropic. Moreover the set of squares is not closed under addition (or it would be a subgroup of the additive group, but $\frac{1}{2}(q + 1)$ does not divide q); thus there exist two squares whose sum is a non-square. By rescaling we can find $\alpha, \beta \in k$ such that $\alpha^2 + \beta^2 = -1$. Then

$$-(x^2 + y^2) = (\alpha x + \beta y)^2 + (\alpha x - \beta y)$$

and so the first and third forms are equivalent.

(E84*) *Prove the result for $\dim(V) = 2 = \mathrm{char}(k)$.*

□

A formed space (V, Q) with Q quadratic is called an **orthogonal space**. The lemma and Theorem 32 implies a natural division of orthogonal spaces, as follows. Note that, in all cases, for $i = 1, \dots, r$, (v_i, w_i) are mutually orthogonal hyperbolic pairs, with $Q(v_i) = Q(w_i) = 0$.

($\mathbf{O^+_{2r}}$) with basis $\{v_1, w_1, \dots, v_r, w_r\}$.

($\mathbf{O_{2r+1}}$) with basis $\{v_1, w_1, \dots, v_r, w_r, u\}$ where $\langle u\rangle$ is anisotropic and orthogonal to $\langle v_1, w_2, \dots, v_r, w_r\rangle$. We can prescribe, moreover, that $Q(u) = 1$ or, if q is odd, $Q(u)$ is 1 or a non-square.

($\mathbf{O^-_{2r+2}}$) with basis $\{v_1, w_1, \dots, v_r, w_r, u, u'\}$ where $\langle u, u'\rangle$ is anisotropic and orthogonal to $\langle v_1, w_2, \dots, v_r, w_r\rangle$. We can prescribe, moreover, that $Q(u) = 1$, $Q(u') = a$ and $x^2 + x + a$ is irreducible in $\mathbb{F}_q[x]$.

(E85) *Prove the final assertion.*