14. 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 β_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 $GL(V)$:

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

Observe that
$$\mathrm{Isom}(\kappa) \le \mathrm{Sim}(\kappa) \le \mathrm{SemiSim}(\kappa).$$

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
$$\kappa(x, y) = x^T Ay$$
where A is some matrix. Then
$$\mathrm{Isom}(\kappa) = \{X \mid XA(X^\sigma)^T = A\}.$$
One can give similar formulations for similarities and semisimilarities, and for quadratic forms. [41]

14.1. 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.

> **(E14.1)** *Let β be a σ-Hermitian, or alternating form, with radical $\mathrm{Rad}(V)$. Prove that the natural map $V \to V/\mathrm{Rad}(V)$ is an isometry. What happens if we ask the same question with β replaced by a quadratic form Q?*

Theorem 14.1. (Witt's Lemma) *Let (V, κ) 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.

[41] 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 $\mathrm{Isom}(\kappa)$ is then the set of orthogonal matrices over $\mathbb{C}$, a group you undoubtedly encountered at some point during undergraduate mathematics.

Note that if we wanted to prove Witt's Lemma for the situation when $\kappa = \beta$, a σ-sesquilinear form, then the first step of the proof would be to appeal to (E14.1) and quotient V by $Rad(V)$. We could then proceed on the assumption that κ is non-degenerate, in which case, we need to prove that any isometry h extends.

However we want to prove this result when $\kappa = Q$ also, thus we need to be a little more careful. For instance it is perfectly possible for a non-degenerate quadratic form to have non-trivial radical, thus considering the quotient in this situation is not sufficient.

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 $(U \cap Rad(V))h = Uh \cap Rad(V)$.

(E14.2*) *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 $\mathrm{Rad}(V) \leq U \cap Uh$. Write $m := \dim(V)$ and proceed by induction on $\dim(U)/\mathrm{Rad}(V) = m - \dim(Rad(V))$.

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 V. Now write β for κ if κ is sesquilinear, and write β for the polarized form of κ, when κ is quadratic. For X a subspace of V, define[42]

$$X^\perp := \{x \in V \mid \beta(x, y) = 0 \text{ for all } y \in U\}.$$

(E14.3) $\dim(X^\perp) \geq n - \dim(X)$ *with equality if and only if $\beta|_X$ is non-degenerate.*

We wish to study the subspace $P^\perp$. If $P \leq Rad(V)$, then $P^\perp = V$. Now let W be a a complement to both U and Uh in V. Then the function

$$h \oplus 1 : U \oplus W \to Uh \oplus W$$

is an isometry that extends h to V and the result is proved. Assume, instead, that $P \not\leq Rad(V)$, then $P^\perp$ is a subspace of V of dimension $n - 1$. Furthermore, since h is an isometry, if $x, y \in U$, then

$$\beta(xh, y(h-1)) = \beta(xh, yh) - \beta(xh, y) = \beta(x, y) - \beta(xh, y) = \beta(x - xh, y).$$

This identity implies two things:

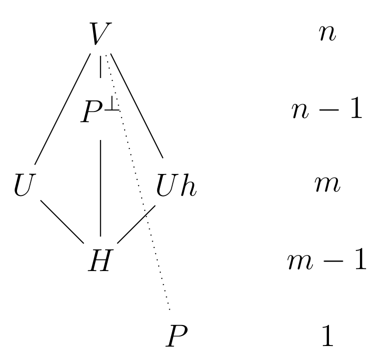
(1) By considering what happens as x and y vary over U we obtain that

$$U \subseteq P^\perp \Longleftrightarrow Uh \subseteq P^\perp.$$

(2) By letting x vary over H, and y vary over U we obtain that

$$\beta(xh, y(h-1)) = \beta(x - xh, y) = \beta(0, y) = 0$$

and, thus, $H \subseteq P^\perp$.



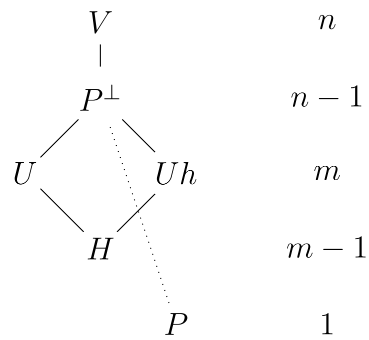
The diagram at the right summarises the situation (lines indicate inclusion; dimensions are written alongside).

[42] This is the same definition as before, but previously we assumed that β was non-degenerate, and we do not do that now.

Suppose next that $U \not\leq P^\perp$. Then (2) implies that $Uh \not\leq P^\perp$. Now let W be a complement to H in $P^\perp$ and observe that W is, then, a complement to U in V. Now the function

$$h \oplus 1 : U \oplus W \to Uh \oplus W$$

is an isometry that extends h to V and the result is proved. Thus, in what follows we assume that $U \leq P^\perp$. By (2) this implies that $Uh \leq P^\perp$ and, since $P \leq Uh - U$ we conclude that $P \leq P^\perp$. Again the diagram summarises the situation.



Suppose next that U, Uh and $P^\perp$ do not all coincide. There are two cases to consider:

- Suppose that $U \neq Uh$. Then $U = \langle H, u_1\rangle$ and $Uh = \langle H, U_2\rangle$ for some vectors $u_1, u_2 \in B$. Let W_0 be a complement for $U + Uh$ in $P^\perp$, and observe that $W = \langle W_0, u_1 + u_2\rangle$ is a complement for both U and U^h in $P^\perp$. Then the function
$$h \oplus 1 : U \oplus W \to U^h \oplus W$$
extends h to an isometry on $P^\perp$.
- Suppose, instead, that $U = Uh \neq P^\perp$ and let W be a complement to U in $P^\perp$. Then, once again, the function
$$h \oplus 1 : U \oplus W \to U^h \oplus W$$
extends h to an isometry on $P^\perp$.

Thus, in any case, we may assume 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). Since $x \notin Rad(V)$, x lies in a non-degenerate subspace of dimension $n - \mathrm{Rad}(V)$ (any complement of $Rad(V)$ that contains x will do). Now Theorem 13.7 implies that there is a hyperbolic line $L = \langle x, y\rangle$. Observe that $y \notin P^\perp$, thus our job is to extend h to $\langle U, y\rangle$.

> **(E14.4)** *Suppose that (V, Q) is a hyperbolic line containing two elements x, y such that (x, y) is a hyperbolic pair and $Q(x) = 0$. Then there exists an element z such that (x, z) is a hyperbolic pair and $Q(x) = Q(z) = 0$.*

Observe that neither x nor y are in $Rad(V)$ and (E14.4) implies that we may assume that $Q(y) = 0$. Then $\langle x\rangle^\perp$ has dimension $n - 1$ and, since $\langle x\rangle$ is a hyperplane in L, $L^\perp$ is a hyperplane in $\langle x\rangle^\perp = P^\perp$, while $L^\perp h$ is a hyperplane in $\langle xh\rangle^\perp$ (and so has dimension $n - 2$).

It is easy to check that $(L^\perp h)^\perp$ contains a non-degenerate subspace L' of dimension 2 that contains x. Then, since x is isotropic, Theorem 13.7 implies that L' is a hyperbolic line and (E14.3) implies that $(L')^\perp = L^\perp h$. Now choose $y' \in L'$ such that (x, y') is a hyperbolic pair and observe that $y' \notin U$. Furthermore, by (E14.4) we may choose y' so that $Q(y') = 0$.

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

> **(E14.5)** *Check that $h \oplus h'$ is an isometry.*

$\square$

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

> **(E14.6*)** *Let (V, κ) be a formed space. Then the Witt index and the isomorphism class of a maximal anisotropic subspace are determined.*

> **(E14.7*)** *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.*

14.2. **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 13.5 in each case – the first we can do in total generality; for the other two we restrict ourselves to vector spaces over finite fields.

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

Lemma 14.2. *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 14.2 and Theorem 13.5 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.

14.2.2. *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.* [43]

(E14.8) *The norm and trace functions are surjective.*

Lemma 14.3. *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. (E14.8) implies that we can choose c such that $cc^q = -1$ we see that $f(v+cw) = 0$, contradicting the fact that U is anisotropic. Now (2) follows from Theorem 13.5.

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. $\square$

A formed space (V, β) with β σ-Hermitian (and σ non-trivial) is called a **unitary space**. The lemma and Theorem 13.5 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 $r = \lfloor \frac{n}{2} \rfloor$.

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

14.2.3. *Quadratic forms over finite fields.*

(E14.9*) *Let $a, b \in k^*$. For all $c \in k$, there exist $x, y \in k$ with $ax^2 + by^2 = c$.*

Lemma 14.4. *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 $Q(xu + yv) = x^2 Q(u) + y^2 Q(v)$ 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 (E14.9) implies that there exist $x, y \in k$ such that $x^2 Q(u) + y^2 Q(v) = -Q(w)$. 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.

(E14.10*) *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 13.5 implies a natural division of orthogonal spaces, as follows. Note that, in all cases, for $i = 1, \ldots, r$, (v_i, w_i) are mutually orthogonal hyperbolic pairs, with $Q(v_i) = Q(w_i) = 0$.

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

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

(E14.11) *Prove the final assertion.*