

14.8 Witt's Extension and Cancellation Theorems

The previous section left one question open. A nondegenerate space splits as hyperbolic planes plus an anisotropic remainder, and the number of planes is pinned down by the Witt index — but the remainder is a subspace chosen along the way, and different choices give different subspaces. What should be true is that they all carry the same form. Proving it needs a theorem with a much wider reach: any isometry between two subspaces of a nondegenerate space is the restriction of an isometry of the whole space. That theorem is the longest proof of the chapter, and the cancellation statement that finishes Section 7 falls out of it in four lines.

Throughout, F is a field with $\text{char } F \neq 2$ (Definition 0.7.2), all spaces are finite-dimensional over F , and all forms are **symmetric** bilinear forms (Definition 14.3.1). Orthogonal complements $U^\perp$, orthogonal direct sums $U \perp W$, and isotropic and hyperbolic vocabulary are as in Section 7.

14.8.1 Isometries of forms

Chapter 11 called a linear map an isometry when it preserved the inner product (Definition 11.7.1). The same word works here, with the form in place of the inner product and with no positivity anywhere.

An isometry is a change of variables that the form does not notice.

Definition 14.8.1. Isometry of Bilinear Spaces

Let β be a bilinear form on V and β' one on V' . An **isometry** from (V, β) to (V', β') is a linear **bijection** $\sigma: V \rightarrow V'$ with

$$\beta'(\sigma(u), \sigma(v)) = \beta(u, v) \quad \text{for all } u, v \in V.$$

The two spaces are **isometric**, written $(V, \beta) \cong (V', \beta')$ or just $V \cong V'$, if such a σ exists. An isometry of (V, β) with itself is an **isometry of V** .

When $U \subseteq V$ and $U' \subseteq V'$ are subspaces, “an isometry $U \rightarrow U'$ ” always means an isometry for the **restricted** forms $\beta|_{U \times U}$ and $\beta'|_{U' \times U'}$.

Two clauses need pointing at. The map must be a **bijection**, so that the inverse is again an isometry; and the identity must hold for **all** pairs, though by bilinearity it is enough to check it on a pair of bases. The symbol $\cong$ is the one used for isomorphism throughout the book, and no confusion arises: an isometry is an isomorphism that also respects the form, and within this chapter $\cong$ between spaces carrying forms always means isometric.

Three readings make the notion concrete.

- **Isometry is congruence in disguise.** If $\mathcal{B}$ is a basis of V and $\mathcal{B}'$ one of V' , then σ is an isometry exactly when the Gram matrices satisfy $[\beta]_{\mathcal{B}}^{\mathcal{B}} = \mathbf{P}^\top [\beta']_{\mathcal{B}'}^{\mathcal{B}'} \mathbf{P}$ with $\mathbf{P} = [\sigma]_{\mathcal{B}}^{\mathcal{B}'}$. So $(V, \beta) \cong (V', \beta')$ if and only if their Gram matrices are congruent (Definition 14.2.1). Every classification theorem of this chapter is therefore a classification up to isometry.
- **Over $\mathbb{R}$.** Two real spaces with nondegenerate symmetric forms are isometric exactly when they have the same signature, by Corollary 14.5.2. So, writing $\mathbb{R}^{p,q}$ for $\mathbb{R}^{p+q}$ carrying the

form of signature (p, q) , we have $\mathbb{R}^{2,1} \not\cong \mathbb{R}^{1,2}$ even though both are three-dimensional and both nondegenerate.

- **The degenerate case.** An isometry carries $\text{rad}(\beta)$ onto $\text{rad}(\beta')$, because $\beta'(\sigma u, \sigma v) = \beta(u, v)$ and σ is surjective. In particular isometric spaces have radicals of equal dimension.

The isometries of a fixed (V, β) form a group under composition; Section 10 names the classical examples. For now only two kinds are needed, and the second is built from the first.

14.8.2 Reflections

Chapter 11 §08 built Householder reflections out of an inner product, to clear a column. The same formula works for any symmetric form, provided the vector we reflect in is anisotropic, and it is the only explicit isometry this section needs.

Definition 14.8.2. Reflection in an Anisotropic Vector

Let β be a symmetric bilinear form on V and let $w \in V$ be anisotropic, that is $q(w) \neq 0$. The **reflection in w** is the map

$$\tau_w: V \rightarrow V, \quad \tau_w(v) = v - \frac{2\beta(v, w)}{q(w)} w.$$

The formula is Definition 11.8.1 with $\langle v, w \rangle$ replaced by $\beta(v, w)$ and $\|w\|^2$ by $q(w)$; the division is legitimate precisely because w is anisotropic.

Proposition 14.8.1. Reflections Are Involutive Isometries

Let β be a symmetric bilinear form on V and $w \in V$ anisotropic. Then τ_w is linear, and:

- (a) $\tau_w(w) = -w$, and $\tau_w(v) = v$ for every v with $\beta(v, w) = 0$;
- (b) $\tau_w \circ \tau_w = \text{id}_V$; in particular τ_w is bijective;
- (c) $\beta(\tau_w u, \tau_w v) = \beta(u, v)$ for all $u, v \in V$.

Hence τ_w is an isometry of V .

Proof. Linearity holds because $v \mapsto \beta(v, w)$ is linear and $q(w)$ is a fixed nonzero scalar. Write $c(v) = 2\beta(v, w)/q(w)$.

- (a) $c(w) = 2q(w)/q(w) = 2$, so $\tau_w(w) = w - 2w = -w$. If $\beta(v, w) = 0$ then $c(v) = 0$ and $\tau_w(v) = v$.
- (b) By (a) and linearity, $\beta(\tau_w v, w) = \beta(v, w) - c(v)q(w) = -\beta(v, w)$, so $c(\tau_w v) = -c(v)$ and

$$\tau_w(\tau_w v) = (v - c(v)w) + c(v)w = v.$$

- (c) Expanding by bilinearity and using symmetry,

$$\begin{aligned} \beta(\tau_w u, \tau_w v) &= \beta(u, v) - c(v)\beta(u, w) - c(u)\beta(w, v) \\ &\quad + c(u)c(v)q(w). \end{aligned}$$

Now $c(u)c(v)q(w) = 4\beta(u, w)\beta(v, w)/q(w)$, while the two middle terms together contribute $-4\beta(u, w)\beta(v, w)/q(w)$. They cancel, leaving $\beta(u, v)$. Together with (b) this

makes τ_w a bijective linear map preserving β , that is an isometry. ■

The use of reflections is that they move one anisotropic vector to any other of the same value — the one explicit construction the long proof below will need.

Lemma 14.8.2. Moving One Anisotropic Vector to Another

Let $\text{char } F \neq 2$, let β be a symmetric bilinear form on V , and let $u, u' \in V$ satisfy

$$q(u) = q(u') \neq 0.$$

Then there is an isometry ρ of V with $\rho(u) = u'$, and ρ may be taken to be a reflection or a product of two reflections.

Idea. The reflection in $u - u'$ is the natural candidate, and it works whenever $u - u'$ is anisotropic. It need not be — but $u + u'$ then is, because the two values $q(u - u')$ and $q(u + u')$ add up to $4q(u) \neq 0$ and so cannot both vanish. Reflecting in $u + u'$ overshoots to $-u'$, and one more reflection, in u' itself, brings it back.

Proof. Expanding both by bilinearity and adding,

$$q(u - u') + q(u + u') = 2q(u) + 2q(u') = 4q(u) \neq 0,$$

where the last step uses $q(u) = q(u') \neq 0$. So at least one of $q(u - u')$ and $q(u + u')$ is nonzero.

Case 1: $q(u - u') \neq 0$. Put $w = u - u'$. Then

$$q(w) = q(u) - 2\beta(u, u') + q(u') = 2(q(u) - \beta(u, u')),$$

while $\beta(u, w) = q(u) - \beta(u, u')$. Hence $2\beta(u, w)/q(w) = 1$, and

$$\tau_w(u) = u - w = u'.$$

Take $\rho = \tau_w$.

Case 2: $q(u - u') = 0$. Then $q(u + u') = 4q(u) \neq 0$; put $w = u + u'$. The same computation with $-u'$ in place of u' gives $q(w) = 2(q(u) + \beta(u, u'))$ and $\beta(u, w) = q(u) + \beta(u, u')$, so again $2\beta(u, w)/q(w) = 1$ and

$$\tau_w(u) = u - w = -u'.$$

Since $q(u') \neq 0$, the reflection $\tau_{u'}$ is defined, and $\tau_{u'}(-u') = u'$ by [Proposition 14.8.1 \(a\)](#). Take $\rho = \tau_{u'} \circ \tau_w$, a composition of two isometries and hence an isometry. This proves the lemma. ■

Quick check. In $\mathbb{R}^3$ with $q(\mathbf{x}) = x_1^2 + x_2^2 - x_3^2$, find a reflection carrying $\mathbf{e}_1$ to $\mathbf{e}_2$.

Solution. Both have $q = 1 \neq 0$, so [Lemma 14.8.2](#) applies. Case 1 works: $\mathbf{w} = \mathbf{e}_1 - \mathbf{e}_2$ has $q(\mathbf{w}) = 1 + 1 = 2 \neq 0$, so

$$\tau_{\mathbf{w}}(\mathbf{v}) = \mathbf{v} - \beta(\mathbf{v}, \mathbf{w}) \mathbf{w},$$

since $2/q(\mathbf{w}) = 1$. Then $\beta(\mathbf{e}_1, \mathbf{w}) = 1$ and $\tau_{\mathbf{w}}(\mathbf{e}_1) = \mathbf{e}_1 - (\mathbf{e}_1 - \mathbf{e}_2) = \mathbf{e}_2$, as required. The reflection fixes $\mathbf{e}_1 + \mathbf{e}_2$ and $\mathbf{e}_3$, which are the vectors orthogonal to $\mathbf{w}$.

14.8.3 Witt's extension theorem

Here is the chapter's long theorem. Read the statement carefully: the two subspaces live in the **same** space V , and the form on V is required to be nondegenerate, but nothing at all is assumed about the restrictions to U and U' — they may be degenerate, they may be zero.

Theorem 14.8.3. Witt's Extension Theorem

Let F be a field with $\text{char } F \neq 2$, let V be a finite-dimensional vector space over F , and let β be a **nondegenerate** symmetric bilinear form on V . Let $U, U' \subseteq V$ be subspaces and let

$$\sigma: U \rightarrow U'$$

be an isometry for the restricted forms. Then there is an isometry φ of V with $\varphi|_U = \sigma$.

Idea. Induction, but on what? Two different moves are available, and each improves a different number.

① If $\beta|_U$ is **nondegenerate**, then U contains an anisotropic vector u_1 . A reflection moves $\sigma(u_1)$ back to u_1 , so we may assume σ fixes u_1 ; then everything of U orthogonal to u_1 stays inside the hyperplane $u_1^\perp$, which is again nondegenerate and **one dimension smaller**. Recurse there and glue.

② If $\beta|_U$ is **degenerate**, pick a nonzero z in its radical. Nondegeneracy of β on V produces a partner w making (z, w) a hyperbolic pair orthogonal to the rest of U , and σ extends to $U \oplus Fw$ by sending w to the matching partner on the other side. The subspace has grown, but its **radical has shrunk by one**.

So the induction runs on the pair $(\dim V, \dim \text{rad}(\beta|_U))$ read lexicographically: ① lowers the first entry, ② keeps it and lowers the second. Step 0 disposes of $U = \{0\}$.

Proof. We prove the statement for every triple (V, U, σ) satisfying the hypotheses, by induction on the pair

$$(\dim V, \dim \text{rad}(\beta|_{U \times U}))$$

ordered lexicographically: one pair precedes another if its first entry is smaller, or the first entries agree and the second is smaller. This order on pairs of nonnegative integers has no infinite descending chain, so the induction is legitimate. Write $R = \text{rad}(\beta|_{U \times U}) = U \cap U^{\perp_\beta}$.

Step 0: $U = \{0\}$. Then $U' = \{0\}$ and $\varphi = \text{id}_V$ works.

Step 1: $U \neq \{0\}$ and $R = \{0\}$. Since $\beta|_U$ is nondegenerate and $U \neq \{0\}$, the form $\beta|_U$ is not the zero form. By Lemma 14.4.1, applied to $\beta|_U$ on U and using $\text{char } F \neq 2$, there is

$u_1 \in U$ with $q(u_1) \neq 0$.

Claim. We may assume $\sigma(u_1) = u_1$.

Proof. Put $u'_1 = \sigma(u_1)$. Then $q(u'_1) = \beta(\sigma u_1, \sigma u_1) = q(u_1) \neq 0$, so [Lemma 14.8.2](#) gives an isometry ρ of V with $\rho(u_1) = u'_1$. The composite $\tau = \rho^{-1} \circ \sigma$ is an isometry from U onto $\rho^{-1}(U')$ with $\tau(u_1) = u_1$, and if φ_0 is an isometry of V extending τ , then $\rho \circ \varphi_0$ is an isometry of V extending σ . So it suffices to treat τ . ■

Assume then that $\sigma(u_1) = u_1$. The map $u \mapsto \beta(u_1, u)$ is a linear functional on U taking the nonzero value $q(u_1)$ at u_1 , so its kernel

$$U_1 = \{u \in U : \beta(u_1, u) = 0\}$$

has $\dim U_1 = \dim U - 1$ by Rank-Nullity (Theorem 2.3.1), and $U = \text{span}(u_1) \oplus U_1$, since $au_1 \in U_1$ forces $aq(u_1) = 0$ and hence $a = 0$.

Because $q(u_1) \neq 0$, the form restricted to $\text{span}(u_1)$ is nondegenerate, so Proposition 14.7.3 gives

$$V = \text{span}(u_1) \perp W, \quad W = \text{span}(u_1)^{\perp_\beta},$$

with $\beta|_W$ nondegenerate and $\dim W = \dim V - 1$. Now $U_1 \subseteq W$ by definition, and $\sigma(U_1) \subseteq W$ as well: for $u \in U_1$,

$$\beta(u_1, \sigma u) = \beta(\sigma u_1, \sigma u) = \beta(u_1, u) = 0.$$

So $\sigma|_{U_1} : U_1 \rightarrow \sigma(U_1)$ is an isometry between two subspaces of W , and $(W, \beta|_W)$ satisfies the hypotheses of the theorem with $\dim W < \dim V$. By the induction hypothesis there is an isometry θ of W with $\theta|_{U_1} = \sigma|_{U_1}$.

Define $\varphi : V \rightarrow V$ by

$$\varphi(au_1 + x) = au_1 + \theta(x) \quad (a \in F, x \in W),$$

which is well defined and linear because $V = \text{span}(u_1) \oplus W$, and bijective because θ is. It is an isometry: using the orthogonality of $\text{span}(u_1)$ and W on both sides,

$$\begin{aligned} \beta(\varphi(au_1 + x), \varphi(bu_1 + y)) &= abq(u_1) + \beta(\theta x, \theta y) \\ &= abq(u_1) + \beta(x, y) \\ &= \beta(au_1 + x, bu_1 + y). \end{aligned}$$

Finally φ extends σ : a vector $u \in U$ is $au_1 + x$ with $x \in U_1 \subseteq W$, and

$$\varphi(u) = au_1 + \theta(x) = a\sigma(u_1) + \sigma(x) = \sigma(u).$$

Step 2: $R \neq \{0\}$. Choose $z \in R$ with $z \neq 0$ and a complement U_0 of $\text{span}(z)$ in U , so that $U = \text{span}(z) \oplus U_0$ (Theorem 1.7.6). Since σ is an isometry of U onto U' , it carries R onto $\text{rad}(\beta|_{U'})$; write $z' = \sigma(z)$ and $U'_0 = \sigma(U_0)$, so that $U' = \text{span}(z') \oplus U'_0$ and z' lies in the radical of $\beta|_{U'}$. Note $q(z) = 0$, because z pairs to zero with everything in U , in particular with itself; likewise $q(z') = 0$.

Claim. There is $w \in V$ with $q(w) = 0$, $\beta(z, w) = 1$, and $\beta(u_0, w) = 0$ for every $u_0 \in U_0$.

Proof. Consider the linear map $S: V \rightarrow U^*$ sending v to the restriction of $\beta(\cdot, v)$ to U . Its kernel is $U^\perp_\beta$, which has dimension $\dim V - \dim U$ by Lemma 14.7.1, since β is nondegenerate. By Rank–Nullity (Theorem 2.3.1), $\text{rank } S = \dim U = \dim U^*$, so S is surjective. Let $\psi_z \in U^*$ be the functional with $\psi_z(z) = 1$ and $\psi_z(U_0) = 0$, which exists because $U = \text{span}(z) \oplus U_0$. Pick $w_0 \in V$ with $S(w_0) = \psi_z$, that is $\beta(z, w_0) = 1$ and $\beta(u_0, w_0) = 0$ for $u_0 \in U_0$.

Put $w = w_0 - \frac{1}{2}q(w_0)z$, which uses $\text{char } F \neq 2$. Since $q(z) = 0$ and $\beta(u, z) = 0$ for every $u \in U$,

$$\beta(z, w) = 1 - \frac{1}{2}q(w_0)q(z) = 1, \quad \beta(u_0, w) = 0,$$

and

$$q(w) = q(w_0) - q(w_0)\beta(w_0, z) + \frac{1}{4}q(w_0)^2q(z) = 0,$$

using $\beta(w_0, z) = \beta(z, w_0) = 1$.

■

Apply the claim on both sides: it gives w for (z, U_0) and, by the same argument with z' and U'_0 , a vector w' with $q(w') = 0$, $\beta(z', w') = 1$, and $\beta(U'_0, w') = 0$.

The vector w is not in U , since $\beta(z, w) = 1$ while $\beta(z, u) = 0$ for every $u \in U$; likewise $w' \notin U'$. So

$$\tilde{U} = U \oplus Fw, \quad \tilde{U}' = U' \oplus Fw'$$

are subspaces of V of dimension $\dim U + 1$. Define $\tilde{\sigma}(u + cw) = \sigma(u) + cw'$, a linear bijection $\tilde{U} \rightarrow \tilde{U}'$. It is an isometry: for $u = az + u_0 \in U$ we have

$$\beta(u, w) = a\beta(z, w) + \beta(u_0, w) = a,$$

and $\sigma(u) = az' + \sigma(u_0)$ with $\sigma(u_0) \in U'_0$, so $\beta(\sigma u, w') = a$ as well. Hence, expanding by bilinearity and using $q(w) = q(w') = 0$,

$$\begin{aligned} \beta(\tilde{\sigma}(u + cw), \tilde{\sigma}(y + dw)) &= \beta(\sigma u, \sigma y) + d\beta(\sigma u, w') + c\beta(\sigma y, w') \\ &= \beta(u, y) + d\beta(u, w) + c\beta(y, w) \\ &= \beta(u + cw, y + dw). \end{aligned}$$

Claim. $\text{rad}(\beta|_{\tilde{U}}) = R \cap U_0$, and its dimension is $\dim R - 1$.

Proof. Let $x = az + u_0 + cw$ lie in $\text{rad}(\beta|_{\tilde{U}})$, with $a, c \in F$ and $u_0 \in U_0$. Pairing x with w gives $a\beta(z, w) + \beta(u_0, w) + cq(w) = a$, so $a = 0$. Pairing x with z gives $\beta(u_0, z) + c\beta(w, z) = c$, since $z \in R$ kills u_0 ; so $c = 0$. Hence $x = u_0 \in U_0$, and x pairs to zero with all of $U \subseteq \tilde{U}$, so $x \in R \cap U_0$. Conversely a vector of $R \cap U_0$ pairs to zero with U and with w , hence with $\tilde{U}$.

For the dimension: every $r \in R \subseteq U$ is $az + u_0$, and $u_0 = r - az \in R$ because $z \in R$; so $R = \text{span}(z) \oplus (R \cap U_0)$ and $\dim(R \cap U_0) = \dim R - 1$.

■

The pair attached to the triple $(V, \tilde{U}, \tilde{\sigma})$ is therefore $(\dim V, \dim R - 1)$, which precedes $(\dim V, \dim R)$ in the lexicographic order. By the induction hypothesis there is an isometry φ of V with $\varphi|_{\tilde{U}} = \tilde{\sigma}$. Since $U \subseteq \tilde{U}$ and $\tilde{\sigma}|_U = \sigma$, this φ extends σ .

Steps 0, 1, and 2 cover every case, so the induction is complete and the theorem is proved.

■

Three places earned their hypotheses. Nondegeneracy of β on V was used twice, once through Proposition 14.7.3 in Step 1 and once through the surjectivity of S in Step 2. Characteristic $\neq 2$ was used twice as well, in Lemma 14.4.1 and in the correction $w = w_0 - \frac{1}{2}q(w_0)z$, which is the same correction that built a hyperbolic pair in Lemma 14.7.4. And symmetry is everywhere: without it, “the” radical and “the” orthogonal complement would each split into a left and a right version.

14.8.4 Cancellation

The corollary is what the theorem is usually used for, and it is where a careless statement goes wrong. Witt cancellation removes a summand from an **orthogonal** decomposition of two spaces that are **already known to be isometric**, and what it produces is an isometry of the complements.

Corollary 14.8.4. Witt's Cancellation Theorem

Let $\text{char } F \neq 2$.

- (a) Let β be a nondegenerate symmetric form on V , and let $U, U' \subseteq V$ be isometric subspaces. Then $U^{\perp_\beta} \cong U'^{\perp_\beta}$.
- (b) Let (V, β) and (V', β') be finite-dimensional spaces with nondegenerate symmetric forms, and suppose

$$V = U \perp W, \quad V' = U' \perp W'.$$

If $V \cong V'$ and $U \cong U'$, then $W \cong W'$.

Idea. For (a), extend the isometry $U \rightarrow U'$ to the whole of V and watch where the complement goes: an isometry of V carrying U onto U' has no choice but to carry $U^\perp$ onto $U'^\perp$. For (b), transport everything into the single space V along an isometry $V \rightarrow V'$, and apply (a).

Proof.

- (a) Let $\sigma: U \rightarrow U'$ be an isometry. By Theorem 14.8.3 there is an isometry φ of V with $\varphi|_U = \sigma$; in particular $\varphi(U) = U'$. If $x \in U^{\perp_\beta}$ and $u' \in U'$, write $u' = \varphi(u)$ with $u \in U$; then

$$\beta(u', \varphi x) = \beta(\varphi u, \varphi x) = \beta(u, x) = 0,$$

so $\varphi(U^{\perp_\beta}) \subseteq U'^{\perp_{\beta'}}$. Both subspaces have dimension $\dim V - \dim U$ by Lemma 14.7.1, using $\dim U = \dim U'$, and φ is injective, so the inclusion is an equality. Restricting φ gives an isometry $U^{\perp_\beta} \rightarrow U'^{\perp_{\beta'}}$.

- (b) First, $W = U^{\perp_\beta}$: the orthogonality in $V = U \perp W$ gives $W \subseteq U^{\perp_\beta}$, and both have dimension $\dim V - \dim U$, so they are equal (Theorem 1.6.8). Likewise $W' = U'^{\perp_{\beta'}}$.

Let $\psi: V \rightarrow V'$ be an isometry. Then $\psi^{-1}(U')$ is a subspace of V isometric to U' , hence isometric to U . Moreover $\psi^{-1}(U'^{\perp_{\beta'}}) = (\psi^{-1}(U'))^{\perp_\beta}$, because ψ preserves the forms and is surjective. Applying (a) inside V to the isometric subspaces U and $\psi^{-1}(U')$,

$$W = U^{\perp_\beta} \cong (\psi^{-1}(U'))^{\perp_\beta} = \psi^{-1}(W') \cong W',$$

the last isometry being the restriction of ψ . This proves the corollary. ■

Warning. Cancellation needs the whole spaces to be isometric, and the sums to be orthogonal. Neither hypothesis can be dropped.

Drop the first: inside $\mathbb{R}^2$ with $q = x_1^2 + x_2^2$ and inside $\mathbb{R}^2$ with $q' = x_1^2 - x_2^2$, the lines $\text{span}(\mathbf{e}_1)$ are isometric, each carrying the form $\langle 1 \rangle$. Their complements are $\text{span}(\mathbf{e}_2)$ with $q = x_2^2$ and $\text{span}(\mathbf{e}_2)$ with $q' = -x_2^2$, which are **not** isometric: one is positive definite, the other negative definite. Isometric subspaces of **different** ambient spaces say nothing about complements.

Drop the second: in $\mathbb{R}^2$ with $q = x_1^2 - x_2^2$, both

$$V = \text{span}(\mathbf{e}_1) \oplus \text{span}(\mathbf{e}_1 + \mathbf{e}_2) \quad \text{and} \quad V = \text{span}(\mathbf{e}_1) \oplus \text{span}(\mathbf{e}_2)$$

are direct sums with the same first summand. The second summands carry $q(\mathbf{e}_1 + \mathbf{e}_2) = 0$ and $q(\mathbf{e}_2) = -1$, so they are not isometric. The first decomposition is not orthogonal, since $\beta(\mathbf{e}_1, \mathbf{e}_1 + \mathbf{e}_2) = 1 \neq 0$, and that is exactly what breaks.

14.8.5 The Witt decomposition is unique

We can now close the question Section 7 left open.

Corollary 14.8.5. The Anisotropic Part Is Determined

Let $\text{char } F \neq 2$, let β be a nondegenerate symmetric form on a finite-dimensional V , and let

$$V = H_1 \perp \cdots \perp H_m \perp V_0 = H'_1 \perp \cdots \perp H'_{m'} \perp V'_0$$

be two decompositions as in Theorem 14.7.5. Then $m = m' = \text{ind}(\beta)$ and $V_0 \cong V'_0$.

Proof. That $m = m' = \text{ind}(\beta)$ is Proposition 14.7.6. Put $U = H_1 \perp \cdots \perp H_m$ and $U' = H'_1 \perp \cdots \perp H'_{m'}$. Choosing a hyperbolic basis of each plane gives bases of U and of U' in which both Gram matrices are the same block diagonal matrix, namely m copies of $\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$ down the diagonal. The linear bijection $U \rightarrow U'$ matching these bases in order is therefore an isometry.

Both V_0 and V'_0 are complements: $V_0 \subseteq U^{\perp_\beta}$ by orthogonality, and the dimensions agree, so $V_0 = U^{\perp_\beta}$ (Theorem 1.6.8), and likewise $V'_0 = U'^{\perp_\beta}$. By Corollary 14.8.4 (a), $V_0 \cong V'_0$. This proves the corollary. ■

So a nondegenerate symmetric form is completely described by two pieces of data: an integer, the Witt index, and an anisotropic form, determined up to isometry. Classifying all forms over a field F therefore reduces to classifying the **anisotropic** ones, which is where the arithmetic of F enters and where the subject stops being linear algebra. Over $\mathbb{R}$ the anisotropic forms are the definite ones, so the data (ind, V_0) is just the signature again. Over $\mathbb{C}$ the anisotropic forms

have dimension 0 or 1, so the index and the parity of n are everything. Over $\mathbb{Q}$ the classification is a theorem of number theory and is not in this book.

14.8.6 Exercises

14.8.6.1 A. Check your understanding

Exercise. A1

- State Witt's extension theorem, with all its hypotheses.
- Define the reflection τ_w and say which vectors it fixes.
- Determine whether the following statement is correct, and justify your answer: if $U \subseteq V$ and $U' \subseteq V'$ are isometric subspaces of nondegenerate spaces, then $U^\perp$ and $U'^\perp$ are isometric.
- Where is $\text{char } F \neq 2$ used in the proof of [Theorem 14.8.3](#)?
- Two real nondegenerate forms of dimension 6 both have Witt index 2. Must they be isometric?

Solution.

- Let $\text{char } F \neq 2$, let β be a nondegenerate symmetric bilinear form on a finite-dimensional V over F , let $U, U' \subseteq V$ be subspaces and $\sigma: U \rightarrow U'$ an isometry for the restricted forms. Then σ extends to an isometry of V .
- $\tau_w(v) = v - (2\beta(v, w)/q(w))w$, defined for anisotropic w . It fixes every v with $\beta(v, w) = 0$ and sends w to $-w$.
- Incorrect. The warning after [Corollary 14.8.4](#) gives the witness: the line $\text{span}(\mathbf{e}_1)$ inside $(\mathbb{R}^2, x_1^2 + x_2^2)$ and inside $(\mathbb{R}^2, x_1^2 - x_2^2)$ are isometric, with complements of opposite definiteness. Cancellation requires the ambient spaces to be isometric too.
- Twice. In Step 1, through Lemma 14.4.1, which produces an anisotropic vector in a nonzero subspace where the form is not zero. In Step 2, through the correction $w = w_0 - \frac{1}{2}q(w_0)z$, which divides by 2.
- No. By [Corollary 14.8.5](#) each is two hyperbolic planes orthogonal to an anisotropic part of dimension $6 - 4 = 2$, and over $\mathbb{R}$ an anisotropic form is definite, so that part has signature $(2, 0)$ or $(0, 2)$. The two possibilities give signatures $(4, 2)$ and $(2, 4)$ for the whole space, which are different, so the forms need not be isometric. What [Corollary 14.8.5](#) says is that the anisotropic part is determined by the form, not that the index determines the form.

14.8.6.2 B. Practice

Exercise. B1: Extend an isometry by hand

Let $V = \mathbb{R}^3$ with $q(\mathbf{x}) = x_1^2 + x_2^2 - x_3^2$, let $U = \text{span}(\mathbf{e}_1)$, $U' = \text{span}(\mathbf{e}_2)$, and let $\sigma(\mathbf{e}_1) = \mathbf{e}_2$.

- Verify that σ is an isometry of U onto U' .
- Extend σ to an isometry of V , and write down its matrix in the standard basis.
- Determine $U^{\perp_\beta}$ and $U'^{\perp_\beta}$ and exhibit the isometry between them produced by your extension.

Solution.

- (a) $\beta(a\mathbf{e}_1, b\mathbf{e}_1) = ab$ and $\beta(\sigma(a\mathbf{e}_1), \sigma(b\mathbf{e}_1)) = \beta(a\mathbf{e}_2, b\mathbf{e}_2) = ab$, and σ is a linear bijection $U \rightarrow U'$.
- (b) Use the Quick check: $\mathbf{w} = \mathbf{e}_1 - \mathbf{e}_2$ has $q(\mathbf{w}) = 2$, and $\tau_{\mathbf{w}}(\mathbf{v}) = \mathbf{v} - \beta(\mathbf{v}, \mathbf{w})\mathbf{w}$ sends $\mathbf{e}_1$ to $\mathbf{e}_2$. In coordinates $\beta(\mathbf{v}, \mathbf{w}) = v_1 - v_2$, so

$$\tau_{\mathbf{w}}(\mathbf{v}) = (v_2, v_1, v_3), \quad \mathbf{P} = \begin{pmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \end{pmatrix}.$$

This swaps the first two coordinates and indeed satisfies $\mathbf{P}^\top \text{diag}(1, 1, -1)\mathbf{P} = \text{diag}(1, 1, -1)$.

- (c) $U^{\perp\beta} = \{\mathbf{v} : v_1 = 0\} = \text{span}(\mathbf{e}_2, \mathbf{e}_3)$ and $U'^{\perp\beta} = \text{span}(\mathbf{e}_1, \mathbf{e}_3)$. The extension maps $\mathbf{e}_2 \mapsto \mathbf{e}_1$ and $\mathbf{e}_3 \mapsto \mathbf{e}_3$, an isometry between them; both carry the form $\text{diag}(1, -1)$, as [Corollary 14.8.4](#) (a) predicts.

Exercise. B2: Cancel a hyperbolic plane

Let H denote a hyperbolic plane over $\mathbb{R}$, and let A and B be nondegenerate real spaces with forms, with $\dim A = \dim B = 3$. Suppose $H \perp A \cong H \perp B$.

- (a) Prove that $A \cong B$.
- (b) If A has signature $(2, 1)$, what is the signature of B ?
- (c) Does $A \perp B \cong A \perp B$ with $A \cong A$ allow us to conclude $B \cong B$? Say which part of [Corollary 14.8.4](#) is being used and why the statement is not vacuous.

Solution.

- (a) Put $V = H \perp A$ and $V' = H \perp B$, both nondegenerate. The two copies of H are isometric, and $V \cong V'$ by hypothesis, so [Corollary 14.8.4](#) (b) gives $A \cong B$.
- (b) By (a), $B \cong A$, so B has signature $(2, 1)$ as well; isometric real spaces have equal signatures by [Corollary 14.5.2](#).
- (c) It uses (b) of [Corollary 14.8.4](#) with $U = U' = A$ and $W = W' = B$; the conclusion $B \cong B$ is true but empty. The content of (b) appears only when the two decompositions are genuinely different, as in (a) above, where the hypothesis $V \cong V'$ is an assumption about the **whole** spaces and not about A and B .

Exercise. B3: Reflections in an indefinite space

In $\mathbb{R}^2$ with $q(\mathbf{x}) = x_1^2 - x_2^2$:

- (a) Compute the matrix of $\tau_{\mathbf{e}_1}$ and of $\tau_{\mathbf{e}_2}$ in the standard basis, and check each satisfies $\mathbf{P}^\top \mathbf{A} \mathbf{P} = \mathbf{A}$ with $\mathbf{A} = \text{diag}(1, -1)$.
- (b) Explain why $\tau_{\mathbf{v}}$ is undefined for $\mathbf{v} = (1, 1)$, and say what fails.
- (c) Find an isometry carrying $(1, 0)$ to $(-1, 0)$ and one carrying $(2, \sqrt{3})$ to $(-2, \sqrt{3})$. (Check

the values of q first.)

Solution.

- (a) $q(\mathbf{e}_1) = 1$ and $\beta(\mathbf{v}, \mathbf{e}_1) = v_1$, so $\tau_{\mathbf{e}_1}(\mathbf{v}) = \mathbf{v} - 2v_1\mathbf{e}_1 = (-v_1, v_2)$, with matrix $\text{diag}(-1, 1)$. Similarly $q(\mathbf{e}_2) = -1$ and $\beta(\mathbf{v}, \mathbf{e}_2) = -v_2$, so the coefficient is $2(-v_2)/(-1) = 2v_2$ and $\tau_{\mathbf{e}_2}(\mathbf{v}) = \mathbf{v} - 2v_2\mathbf{e}_2 = (v_1, -v_2)$, with matrix $\text{diag}(1, -1)$. Both matrices $\mathbf{P}$ are diagonal with entries ± 1 , so $\mathbf{P}^\top \mathbf{A} \mathbf{P} = \mathbf{P} \mathbf{A} \mathbf{P} = \mathbf{A}$, as each sign is squared.
- (b) $q(1, 1) = 1 - 1 = 0$, so $(1, 1)$ is isotropic and the denominator $q(\mathbf{w})$ in Definition 14.8.2 is zero. The formula divides by 0; there is no reflection in an isotropic vector.
- (c) Both $(1, 0)$ and $(-1, 0)$ have $q = 1 \neq 0$. Here $\mathbf{u} - \mathbf{u}' = (2, 0)$ with $q = 4 \neq 0$, so Case 1 of Lemma 14.8.2 applies: $\tau_{(2,0)} = \tau_{\mathbf{e}_1}$ works, and indeed $\tau_{\mathbf{e}_1}(1, 0) = (-1, 0)$. For the second pair, $q(2, \sqrt{3}) = 4 - 3 = 1 = q(-2, \sqrt{3})$. Now $\mathbf{u} - \mathbf{u}' = (4, 0)$, with $q = 16 \neq 0$, so $\tau_{\mathbf{e}_1}$ again works: it negates the first coordinate and fixes the second.

14.8.6.3 C. Going deeper

Exercise. C1: Inertia from cancellation

Work over $\mathbb{R}$ and let V be an n -dimensional space with a nondegenerate symmetric form.

- (a) Prove that if $\mathbb{R}^{p,q}$ denotes $\mathbb{R}^{p+q}$ with the form $x_1^2 + \cdots + x_p^2 - x_{p+1}^2 - \cdots - x_{p+q}^2$, then $\mathbb{R}^{p,q} \cong \mathbb{R}^{p',q'}$ forces $p = p'$ and $q = q'$, using only Corollary 14.8.4 and Proposition 14.7.7.
- (b) Explain in one sentence how this compares with the proof of Theorem 14.5.1 in Section 5.

Solution.

- (a) Suppose $\mathbb{R}^{p,q} \cong \mathbb{R}^{p',q'}$. Equal dimension gives $p + q = p' + q' = n$. By Proposition 14.7.7 (a) the Witt index is an isometry invariant, so $\min(p, q) = \min(p', q') = k$. By Corollary 14.8.5 each space is k hyperbolic planes orthogonal to an anisotropic part, and those anisotropic parts are isometric. The anisotropic part of $\mathbb{R}^{p,q}$ is positive definite of dimension $p - q$ when $p \geq q$ and negative definite of dimension $q - p$ when $q > p$. A positive definite form is never isometric to a negative definite one of the same dimension, since $q > 0$ on one and $q < 0$ on the other away from 0 — unless both dimensions are 0. So the two anisotropic parts have the same dimension and the same sign, giving $p - q = p' - q'$. With $p + q = p' + q'$ this forces $p = p'$ and $q = q'$.
- (b) Section 5 proved this directly, by producing a positive subspace and a nonpositive subspace whose dimensions are too large to intersect trivially; the route here instead invokes the whole Witt machinery, so it is longer but shows that inertia is the real instance of a statement that holds over every field of characteristic $\neq 2$.

Exercise. C2: The isometry group acts transitively

Let β be a nondegenerate symmetric form on V , with $\text{char } F \neq 2$, and let G be the group of isometries of V .

- (a) Prove that if $q(u) = q(u') \neq 0$ then some $\varphi \in G$ has $\varphi(u) = u'$.
- (b) Prove that if u and u' are both isotropic and nonzero, then some $\varphi \in G$ has $\varphi(u) = u'$.
Hint: an isotropic line is a one-dimensional subspace on which the form is zero.
- (c) Deduce that G acts transitively on each “level set” $\{v \neq 0 : q(v) = c\}$ for $c \neq 0$, and on the set of nonzero isotropic vectors.

Solution.

- (a) This is [Lemma 14.8.2](#), which already produces such an isometry as a product of at most two reflections. Alternatively, $\text{span}(u) \rightarrow \text{span}(u')$, $u \mapsto u'$, is an isometry of one-dimensional subspaces because $q(u) = q(u')$, so [Theorem 14.8.3](#) extends it.
- (b) The map $\sigma: \text{span}(u) \rightarrow \text{span}(u')$ with $\sigma(au) = au'$ is a linear bijection, and

$$\beta(\sigma(au), \sigma(bu)) = abq(u') = 0 = abq(u) = \beta(au, bu),$$

so it is an isometry of the restricted forms — both of which are zero. By [Theorem 14.8.3](#) it extends to $\varphi \in G$. Note the restricted forms here are **degenerate**, which is exactly the case Step 2 of the proof was built for.

- (c) Immediate from (a) and (b): any two members of such a set are carried to one another by some $\varphi \in G$. In particular, over $\mathbb{R}^{1,3}$ the isometry group moves any nonzero null vector to any other, which is the statement that the light cone has no distinguished direction.

Exercise. C3: What extension does not say

- (a) Give an example of a nondegenerate (V, β) and subspaces U, U' of the **same dimension** that are not isometric, and say why [Theorem 14.8.3](#) does not apply.
- (b) Let β be nondegenerate on V and let $U \subseteq V$ be totally isotropic with $\dim U = \text{ind}(\beta)$. Prove that any two such U are carried onto one another by an isometry of V .
- (c) Deduce that all maximal totally isotropic subspaces of a nondegenerate space have the same dimension, and compare with Proposition 14.7.2.

Solution.

- (a) Take $V = \mathbb{R}^2$ with $q = x_1^2 - x_2^2$, $U = \text{span}(\mathbf{e}_1)$, and $U' = \text{span}(\mathbf{e}_2)$. Both are lines, but q is positive on $U \setminus \{0\}$ and negative on $U' \setminus \{0\}$, so no linear bijection can preserve the form. [Theorem 14.8.3](#) has nothing to extend: its hypothesis is that an isometry $U \rightarrow U'$ is **given**, and here none exists.
- (b) Let U and U' be totally isotropic of the same dimension k . Any linear bijection $\sigma: U \rightarrow U'$ is an isometry, since both restricted forms are identically zero, so $\beta(\sigma u, \sigma v) = 0 = \beta(u, v)$ for all $u, v \in U$. By [Theorem 14.8.3](#), σ extends to an isometry φ of V , and $\varphi(U) = U'$.
- (c) Let U be maximal among totally isotropic subspaces, and let U_1 be one of the largest dimension $m = \text{ind}(\beta)$. If $\dim U < m$, choose any k -dimensional subspace $U_2 \subseteq U_1$ with $k = \dim U$; it is totally isotropic, so by (b) there is an isometry φ of V with $\varphi(U) = U_2$. Then $\varphi^{-1}(U_1)$ is totally isotropic of dimension $m > k$ and contains $\varphi^{-1}(U_2) = U$, contradicting maximality. So $\dim U = m$ for every maximal U . Proposition 14.7.2 says

only $m \leq n/2$; the present statement is sharper, since it says that no totally isotropic subspace can be maximal below the top dimension.