

Recovering a quadratic form from its orthogonal group

Pierre-Yves Gaillard¹

Theorem 1. *Let K be a field of characteristic different from 2, let V be a K -vector space of finite dimension $n \geq 2$, let q and r be two quadratic forms on V , let $O(q)$ and $O(r)$ be the respective orthogonal groups, and let $Q, R : V \times V \rightarrow K$ be the respective associated symmetric bilinear forms. Then we have*

$$O(q) = O(r) \iff Q^{-1}(0) = R^{-1}(0) \iff Kq = Kr.$$

The only non-trivial ingredient we will use is Witt's Extension Theorem. For completeness sake we give a proof of Witt's Extension Theorem at the end of the text. (I found this proof in Serre's book **A Course in Arithmetic**.) We will also use the following lemma:

Lemma 2. *Let K, V, q, Q and $O(q)$ be as in Theorem 1. Assume that q is degenerate. Then the radical $W = \text{rad}(q)$ of q is the smallest nonzero $O(q)$ -invariant subspace of V .*

Proof. Let U be a nonzero $O(q)$ -invariant subspace which does not contain W . It suffices to derive a contradiction. Let W' and V' be subspaces of V satisfying $U + W = U \oplus W'$, $V = U \oplus W' \oplus V'$. Note that $U \neq 0 \neq W'$. Let f' be a nonzero linear map from U to W' and define $f, g : V \rightarrow V$ by $f(u + w' + v') = f'(u)$ and $g = 1 + f$. We have $f^2 = 0$, and thus $1 - f = g^{-1}$. Moreover g is easily seen to be in $O(r) = O(q)$. For $u \in U$ such that $f'(u) \neq 0$ we have $gu = u + f'(u) \notin U$, contradiction. \square

To prove the theorem, we will show $O(q) = O(r) \implies Q^{-1}(0) = R^{-1}(0) \implies Kq = Kr \implies O(q) = O(r)$, the last implication being obvious.

- $O(q) = O(r) \implies Q^{-1}(0) = R^{-1}(0)$

We consider three (non-exclusive) cases, denoted A, B and C.

Case A: q and r are non-degenerate.

Lemma 3. *Suppose that $v, w \in V$ are linearly independent. Then $Q(v, w) = 0 \iff$ there is a g in $O(q)$ such that $gv = v, gw = -w$.*

Proof. \implies : Define $h \in \text{GL}(Kv + Kw)$ by $hv = v, hw = -w$. Then h is in $O(q|Kv + Kw)$, where $q|Kv + Kw$ is the restriction of q to $Kv + Kw$. By Witt's Extension Theorem, h extends to $g \in O(q)$.

\impliedby : We have $Q(v, w) = Q(gv, gw) = Q(-v, w) = -Q(v, w)$. \square

Lemma 4. *Suppose that $v \in V$ is nonzero. Then $q(v) \neq 0 \iff$ there is a g in $O(q)$ such that $g^2 = 1$ and the (-1) -eigenspace of g is Kv .*

Proof. \implies : Define $g \in \text{GL}(V)$ by $gv = -v$ and $gw = w$ if $Q(v, w) = 0$. Then g is in $O(q)$.

\impliedby : Let W be fixed subspace of g . Then we have $V = Kv \oplus W$. Moreover, $w \in W$ implies $Q(v, w) = Q(gv, gw) = Q(-v, w) = -Q(v, w)$, and thus $Q(v, w) = 0$. Since this holds for all w in W , and q is non-degenerate, we have $q(v) \neq 0$. \square

¹DOI 10.5281/zenodo.14513720. My texts at Zenodo. ORCID <https://orcid.org/0000-0002-7960-1698>.

Lemmas 3 and 4 imply the statement when q and r are non-degenerate.

Case B: q is non-degenerate. It suffices to show that r is non-degenerate too. Assume by contradiction that r is degenerate.

Case 1: $r = 0$. We have $O(q) = O(r) = GL(V)$. Then $O(q)$ acts transitively on the nonzero vectors, and on the pairs of linearly independent vectors. This implies $q(v) = q(w)$ for all $v \neq 0 \neq w$, hence $q(v) \neq 0$ for all $v \neq 0$, hence there are linearly independent v and w such that $Q(v, w) = 0$, hence $Q(v, w) = 0$ for all linearly independent v and w , hence $0 = Q(v, v + w) = Q(v, v) \neq 0$ for such v and w , contradiction.

Case 2: r is nonzero (but degenerate). The radical W of r satisfies $0 \subsetneq W \subsetneq V$. Set $G := O(q) = O(r)$. Then W is G -invariant and the only G -invariant subspaces of W are 0 and W . Thus, the intersection of W with the q -orthogonal U of W is equal to 0 or W .

Case 2.1: $U \cap W = 0$. We have $V = U \oplus W$, and U is G -invariant. This contradicts Lemma 2.

Case 2.2: $U \cap W = W$, i.e. $q|_W = 0$. Let $w \neq 0$ be in W . There is a $v \in V$ which is not q -orthogonal to w (in particular $v \notin W$). Setting $a := q(v)$, $b := Q(v, w) \neq 0$, we have $q(2bv - aw) = 0$, and Witt's Extension Theorem implies the existence of a g in G such that $gw = 2bv - aw \notin W$, contradiction.

Case C: q and r are degenerate.

By Lemma 2, the radical $\text{rad}(q)$ of q is the smallest nonzero $O(q)$ -invariant subspace of V , and similarly for r ; in particular $W := \text{rad}(r) = \text{rad}(q)$ and $\rho := \text{rank}(r) = \text{rank}(q)$. We leave the case $\rho \leq 1$ to the reader and assume $\rho \geq 2$. Let U be a linear complement to W in V , let q' and Q' be the respective restrictions of q to U and of Q to $U \times U$, and define r' and R' similarly. We get $O(q') = O(r')$, hence $Q'^{-1}(0) = R'^{-1}(0)$, and the equality $Q^{-1}(0) = R^{-1}(0)$ follows from Case A.

• $Q^{-1}(0) = R^{-1}(0) \implies Kq = Kr$. This implication will follow from:

Proposition 5. *Let L be a field of arbitrary characteristic, let V_1, \dots, V_n be L -vector spaces, let $f, g : V_1 \times \dots \times V_n \rightarrow L$ be n -linear maps such that $f^{-1}(0) \subset g^{-1}(0)$. Then there is a λ in L such that $g = \lambda f$.*

Lemma 6. *Let V be an L -vector space and f an endomorphism of V . Assume that, for all v in V , there is a $\lambda(v)$ in L such that $f(v) = \lambda(v)v$. Then there is a λ in L such that $f(v) = \lambda v$ for all v .*

The proof is left to the reader.

Lemma 7. *Let $f, g : V \rightarrow W$ two L -linear maps. Assume that, for all v in V , there is a $\lambda(v)$ in L such that $g(v) = \lambda(v)f(v)$. Then there is a λ in L such that $g(v) = \lambda f(v)$ for all v .*

Proof. We have $f^{-1}(0) \subset g^{-1}(0)$ and $g(V) \subset f(V)$. If $f', g' : V/f^{-1}(0) \rightarrow f(V)$ are the induced maps, then f' is bijective, and we prove the result by applying Lemma 6 to $g' \circ f'^{-1}$. \square

Proof of Proposition 5. We induct on $n \geq 1$, the case $n = 1$ being trivial. Let W be the space of $(n-1)$ -linear forms on $V_1 \times \dots \times V_{n-1}$, define $f' : V_n \rightarrow W$ by $f'(v_n)(v_1, \dots, v_{n-1}) := f(v_1, \dots, v_n)$, and define g' similarly. By the induction hypothesis, there is a $\lambda(v)$ in L such that $g'(v_n) = \lambda(v_n)f'(v_n)$ for all v_n , and we can and apply Lemma 7. \square

We end with a statement and a proof of Witt's Extension Theorem. We use the following terminology and notation. Let V be a finite dimensional vector space over a field K whose characteristic is not 2. Assume that V is endowed with a symmetric bilinear form, denoted simply by $(x, y) \mapsto xy$ (we even write x^2 for xx). We call such V a **quadratic module**. A map f between quadratic modules is **metric** if it is linear and satisfies $f(x)f(y) = xy$ for all x, y .

Theorem 8 (Witt's Extension Theorem). *Let V be a non-degenerate quadratic module, W a vector subspace of V , and $f : W \rightarrow V$ an injective metric map. Then f extends to a metric automorphism of V .*

Lemma 9. *In the above setting, assume that W is degenerate. Then f extends to a metric injection $f_1 : W_1 \rightarrow V$ with $W_1 \supsetneq W$.*

Proof. Let w_0 be a nonzero vector in $\text{rad}(W)$ and ℓ a linear form on W such that $\ell(w_0) = 1$. There is a v_0 in V such that $v_0 w = \ell(w)$ for all w in W . On replacing v_0 by $v_0 - (y^2/2)w_0$, we can assume $(v_0)^2 = 0$. Set $W_1 := W + Kw_0$. We have in particular $W_1 \supsetneq W$.

We do the same with $W' := f(W)$, $w'_0 := f(w_0)$, $\ell' := \ell \circ f^{-1}$ instead of W, w_0, ℓ , obtaining v'_0 in lieu of v_0 , we set $W'_1 := W' + Kw'_0$ and $f_1(v_0) := v'_0$, and we check that f_1 does the job. \square

Proof of Theorem 8. In view of the lemma, we can assume that W is non-degenerate. We argue by induction on $\dim W$.

Case 1: $\dim W = 1$. Let w_0 be a nonzero vector in W , and note $(w_0)^2 \neq 0$. Set $v_0 := f(w_0)$; in particular $(v_0)^2 = (w_0)^2 \neq 0$, which implies $(w_0 + \varepsilon v_0)^2 \neq 0$ for some $\varepsilon \in \{1, -1\}$. Setting $u := w_0 + \varepsilon v_0$, we get $V = Ku \oplus (Ku)^\perp$. Define the linear map $s : V \rightarrow V$ by $s(u) = -u$ and $s(v) = v$ if $v \perp u$. Note that $w_0 - \varepsilon v_0 \perp u$, and thus $s(w_0 - \varepsilon v_0) = w_0 - \varepsilon v_0$. Since $s(w_0 + \varepsilon v_0) = -w_0 - \varepsilon v_0$, we get $s(w_0) = -\varepsilon v_0 = -\varepsilon f(w_0)$, and we can set $g := -\varepsilon s$.

Case 2: $\dim W \geq 2$. Let $W = W_1 \oplus W_2$ be an orthogonal direct sum with $W_1 \neq 0 \neq W_2$. Write $f_i : W_i \rightarrow V$ for the restriction of f to W_i . By the induction hypothesis f_1 extends to a metric automorphism g_1 of V . The map $f' := g_1^{-1} \circ f : W \rightarrow V$ satisfies $f'(w_1) = g_1^{-1}(f(w_1)) = w_1$ for $w_1 \in W_1$, and thus $f'(W_2) \subset W_1^\perp$ (where W_1^\perp is the orthogonal of W_1 in V). Again by the induction hypothesis, f' extends to a metric automorphism g_2 of W_1^\perp . Define $g' : V \rightarrow V$ by $g'(w_1 + w_1^\perp) = w_1 + g_2(w_1^\perp)$ (obvious notation). Then g' is a metric automorphism of V . Finally set $g := g_1 \circ g'$ (again a metric automorphism of V). We get, for $w_i \in W_i$,

$$g(w_1) = g_1(g'(w_1)) = g_1(w_1) = f_1(w_1) = f(w_1),$$

$$g(w_2) = g_1(g'(w_2)) = g_1(g_2(w_2)) = g_1(f'(w_2)) = g_1(g_1^{-1}(f(w_2))) = f(w_2).$$

This shows that g is indeed a metric automorphism which extends f . \square