Cartan-Dieudonné theorem

Jan Vysoký

April 2, 2020

Theorem 0.1 (**Cartan-Dieudonné**). *Let (V, g) be a n-dimensional real vector space equipped with symmetric bilinear form g. Then every orthogonal endomorphism $A \in \mathrm{O}(V, g)$ can be written as a composition of k reflections, where $k \leq n$ and $\det(A) = (-1)^k$.*

The proof is done in several stages. Let $A \in \mathrm{O}(V, g)$. Let $\hat{A} := A - 1_V$ and let $L(A) := \ker(\hat{A})$. This is in fact precisely the $+1$ eigenspace of A.

Lemma 0.2. *$L(A)$ is an orthogonal complement to $\mathrm{im}(\hat{A})$, that is $L(A) = \mathrm{im}(\hat{A})^{\perp}$.*

Proof. Let $v \in L(A)$, and let $w \in V$. Then

$$g(v, \hat{A}(w)) = g(v, A(w) - w) = g(v, A(w)) - g(v, w) = g(A(v), A(w)) - g(v, w) = 0. \tag{1}$$

We have used the fact that $A(v) = v$ and $A \in \mathrm{O}(V, g)$. Hence $v \in \mathrm{im}(\hat{A})^{\perp}$. Conversely, suppose $v \in \mathrm{im}(\hat{A})^{\perp}$. Then for any $w \in V$, one has

$$g(A(v) - v, A(w)) = g(A(v), A(w)) - g(v, A(w)) = g(v, w) - g(v, A(w)) = -g(v, \hat{A}(w)) = 0. \tag{2}$$

As g is non-degenerate and A invertible, this implies $A(v) - v = 0$, hence $v \in L(A)$. ■

Corollary 0.3. *The above observation has the following consequences:*

(i) $L(A)^{\perp} = \mathrm{im}(\hat{A})$;

(ii) $\mathrm{im}(\hat{A})$ *is an isotropic subspace, iff* $\hat{A}^2 = 0$.

Proof. The first of the two statements follows immediately from the previous lemma. For the second one, $\mathrm{im}(\hat{A})$ is isotropic, iff $\mathrm{im}(\hat{A}) \subseteq \mathrm{im}(\hat{A})^{\perp} = \ker(\hat{A})$. This is equivalent to $\hat{A}^2 = 0$. ■

Lemma 0.4. *For any vector $w \in V$, $\hat{A}(w)$ is isotropic, iff $g(w, \hat{A}(w)) = 0$.*

Proof. This is a straightforward verification using the definition of $\hat{A}$ and the fact that $A \in \mathrm{O}(V, g)$. In fact, one can prove the identity valid for all $w \in V$:

$$g(\hat{A}(w), \hat{A}(w)) = -2g(\hat{A}(w), w). \tag{3}$$

It clearly implies the statement of the lemma. ■

The proof itself now relies on the following technical lemma:

Lemma 0.5. *Suppose $\hat{A}^2 \neq 0$. Then* *(i)* *There exists an anisotropic non-zero vector $w \in V$, such that $z = \hat{A}(w)$ is also anisotropic, or it is zero, $z = 0$.*

(ii) *If $z \neq 0$, and $A_1 = R_z \circ A$, then $w \in L(A_1)$. R_z denotes the reflection along the hyperplane orthogonal to z, that is for all $v \in V$, one has*

$$R_z(v) = v - \frac{2g(v,z)}{g(z,z)} z. \tag{4}$$

Before we actually prove it, let us argue why it is any useful in the proof.

Proof of Theorem 0.1. The proof is done by induction on $n = \dim(V)$. For $n = 1$, the statement is trivial. Hence assume $n > 1$ and suppose the theorem holds for any vector space (V', g') with $\dim(V') < n$. Suppose $A \in \mathrm{O}(V, g)$ *cannot be written* as a composition of at most n reflections. We claim that then necessary $\hat{A}^2 = 0$. Indeed, if $\hat{A}^2 \neq 0$, there exists a non-zero $w \in V$ given to us by Lemma 0.5, and two things can happen:

(1) The element $z = \hat{A}(w)$ is zero. Hence $A(w) = w$. As w is anisotropic, we have a decomposition $V = \mathbb{R}\{w\} \oplus \mathbb{R}\{w\}^{\perp}$. Let $V' = \mathbb{R}\{w\}^{\perp}$, let g' be the restriction of g onto V'. By construction g' is non-degenerate and it is easy to see that $A(V') \subseteq V'$. It follows that the restriction of A onto W' can be by induction hypothesis written as a composition of at most $n-1$ reflections in V'. Those can be extended by identity on $\mathbb{R}\{w\}$, such that A is a composition of at most $n-1$ reflections in V. This is a contraction.

(2) The element $z = \hat{A}(w)$ is anisotropic and thus also non-zero. By *(ii)* of Lemma 0.5, we have $A_1 = R_z \circ A$ with $w \in L(A_1)$. But this means that $A_1(w) = w$, and by part (1), A_1 is a composition of at most $n-1$ reflections in V. Hence $A = R_z \circ A_1$ is a product of at most n reflections. This is a contradiction.

This analysis shows that A which is not a product of at most n reflections has to satisfy $\hat{A}^2 = 0$, that is $\mathrm{im}(\hat{A}) \subseteq \ker(\hat{A})$. On the other hand $\ker(\hat{A}) \equiv L(\sigma)$ must be isotropic. Otherwise there would be anisotropic w such that $A(w) = w$ and we can prove by repeating the arguments of (1) above, that A is a product of at most $n-1$ reflections. Hence

$$\ker(\hat{A}) \subseteq \ker(\hat{A})^{\perp} = \mathrm{im}(\hat{A}). \tag{5}$$

The both subspaces thus must be equal, $\ker(\hat{A}) = \mathrm{im}(\hat{A})$. This implies $n = 2\dim(L(A))$, as the orthogonal complement always has a complementary dimension. In particular, the dimension n must be even. Moreover, A acts by identity on the subspace $L(V)$. It also induces a linear endomorphism A' of the quotient space $V/L(V)$. But as $A(v) = v + (A(v) - v)$, it follows that A' is the identity on $V/L(V)$. There is always a non-canonical isomorphism of the vector space V with $L(V) \oplus V/L(V)$. It follows that with respect to this isomorphism, A has the block form

$$A = \begin{pmatrix} 1 & A^{\circ} \\ 0 & 1, \end{pmatrix}, \tag{6}$$

where $A^{\circ} : V/L(V) \to L(V)$ is some linear map. This implies that $\det(A) = 1$, and thus necessarily $A \in \mathrm{SO}(V, g)$. Now, suppose R is any reflection of V. Then $R \circ A \notin \mathrm{SO}(V, g)$ and it thus cannot be used as a counterexample! Thus $R \circ A$ must be a product of at most n reflections and consequently, A is a product of at most $n+1$ reflections. It cannot be a composition of exactly $n+1$ reflections, as then $\det(A) = (-1)^{n+1} = -1$ as n was proved to be even. Then A would have to be a product of at most n reflections, which is the final contradiction. ∎

We have now justified the existence of the lemma. To prove it, we will need one general result for symmetric bilinear forms:

Lemma 0.6. *Let y be a non-zero isotropic vector in V, where $\dim(V) > 1$. Then there exists a 2-dimensional subspace $H \subseteq V$ containing y, such that g restricted to H is non-degenerate. Any such H is called the* ***hyperbolic plane****.*

Proof. The space $U = \mathbb{R}\{y\} \subseteq V$ is one-dimensional. There must be a non-zero $z \in V$, such that $g(y, z) \neq 0$. Equivalently, $U^{\perp} \neq V$, which is clear, otherwise $U = V^{\perp} = \{0\}$. It follows that the vectors y and z are linearly independent and $H = \mathbb{R}\{y, z\}$ is a 2-dimensional subspace of V. Moreover, the matrix of $g|_H$ in the basis (y, z) is

$$g|_H = \begin{pmatrix} 0 & g(y,z) \\ g(y,z) & g(z,z) \end{pmatrix}, \tag{7}$$

which is non-singular as $g(y, z) \neq 0$. This finishes the proof. ■

Proof of Lemma 0.5. Suppose (i) of the statement is false. Hence suppose that for every anisotropic non-zero vectors $w \neq 0$, the vector $\hat{A}(w)$ is non-zero and isotropic. By Lemma 0.4, we have $g(w, \hat{A}(w)) = 0$. We claim that w and $\hat{A}(w)$ are linearly independent. Indeed, suppose

$$\lambda w + \lambda' \hat{A}(w) = 0. \tag{8}$$

Hence $0 = \lambda g(w, w) + \lambda' g(w, \hat{A}(w)) = \lambda g(w, w)$. As $g(w, w) \neq 0$, this implies $\lambda = 0$. Moreover, as $\hat{A}(w) \neq 0$, we find $\lambda' = 0$. It follows that the subspace $S = \mathbb{R}\{w, \hat{A}(w)\}$ is 2-dimensional. The restriction of g onto S is degenerate as $\hat{A}(w)$ generates its kernel. In particular, S has to be a proper subspace of V and thus $\dim(V) \geq 3$. We claim that

$$g(\hat{A}(y), y) = 0, \text{ for all } y \in V. \tag{9}$$

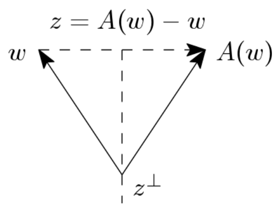
For $y = 0$, the statement is trivial. We have already argued that it holds for any non-zero anisotrpic y. Hence suppose y is non-zero and isotropic. By Lemma 0.6, there is a hyperplane H containing y. One can thus write $V = H \oplus H^{\perp}$ and as $\dim(V) \geq 3$, there is a non-zero anisotropic vector $w \in H^{\perp}$. In particular, $g(y, w) = 0$. Let $u = y + \epsilon w$, where $\epsilon \in \mathbb{R} - \{0\}$. Then

$$g(u, u) = g(y + \epsilon w, y + \epsilon w) = \epsilon^2 g(w, w) \neq 0. \tag{10}$$

It follows that u is non-zero (y and w are linearly independent) and anisotropic. Consequently, by our original assumption $\hat{A}(u)$ is non-zero and isotropic. Equivalently $g(\hat{A}(u), u) = 0$. Hence

$$0 = g(\hat{A}(y + \epsilon w), y + \epsilon w) = g(\hat{A}(y), y) + \epsilon(g(\hat{A}(w), y) + g(\hat{A}(y), w)) + \epsilon^2 g(\hat{A}(w), w). \tag{11}$$

Note that the last term also vanishes. As $\epsilon \in \mathbb{R} - \{0\}$ is arbitrary, this implies $g(\hat{A}(y), y) = 0$. This proves that (9) holds for any $y \in V$. By Lemma 0.4, this proves that $\text{im}(\hat{A}) \subseteq V$ is an isotropic subspace. By Corollary 0.3, this implies $\hat{A}^2 = 0$. This contradicts the assumption of the lemma we are trying to prove. Hence (i) of Lemma 0.5 must hold. It remains to prove (ii). Suppose $z = \hat{A}(w)$ is a non-zero anisotropic vector. We have to prove that $R_z(A(w)) = w$. This is a straightforward verification, or there is a nice geometrical touch to it:



As $A \in \mathrm{O}(V, g)$, w and $A(w)$ form the vertices of an isosceles triangle. Then $z = A(w) - w$ is vector connecting those two vertices. Then R_z is the reflection along the hyperplane $z^{\perp}$ orthogonal to it. It then obviously maps $A(w)$ to w and vice versa. ■