# Chapter 7

# The Cartan–Dieudonné Theorem

## 7.1 Orthogonal Reflections

Orthogonal symmetries are a very important example of isometries. First let us review the definition of a (linear) *projection*.

Given a vector space $E$, let $F$ and $G$ be subspaces of $E$ that form a direct sum $E = F \oplus G$.

Since every $u \in E$ can be written uniquely as $u = v + w$, where $v \in F$ and $w \in G$, we can define the two *projections* $p_F \colon E \to F$ and $p_G \colon E \to G$, such that

$$p_F(u) = v \quad \text{and} \quad p_G(u) = w.$$

It is immediately verified that $p_G$ and $p_F$ are linear maps, and that $p_F^2 = p_F$, $p_G^2 = p_G$, $p_F \circ p_G = p_G \circ p_F = 0$, and $p_F + p_G = \mathrm{id}$.

**Definition 7.1.1** Given a vector space $E$, for any two subspaces $F$ and $G$ that form a direct sum $E = F \oplus G$, the *symmetry with respect to $F$ and parallel to $G$, or reflection about $F$* is the linear map $s\colon E \to E$, defined such that

$$s(u) = 2p_F(u) - u,$$

for every $u \in E$.

Because $p_F + p_G = \mathrm{id}$, note that we also have

$$s(u) = p_F(u) - p_G(u)$$

and

$$s(u) = u - 2p_G(u),$$

$s^2 = \mathrm{id}$, $s$ is the identity on $F$, and $s = -\mathrm{id}$ on $G$.

We now assume that $E$ is a Euclidean space of finite dimension.

**Definition 7.1.2** Let $E$ be a Euclidean space of finite dimension $n$. For any two subspaces $F$ and $G$, if $F$ and $G$ form a direct sum $E = F \oplus G$ and $F$ and $G$ are orthogonal, i.e. $F = G^{\perp}$, the *orthogonal symmetry with respect to $F$ and parallel to $G$, or orthogonal reflection about $F$* is the linear map $s\colon E \to E$, defined such that

$$s(u) = 2p_F(u) - u,$$

for every $u \in E$.

When $F$ is a hyperplane, we call $s$ an *hyperplane symmetry with respect to $F$ or reflection about $F$*, and when $G$ is a plane, we call $s$ a *flip about $F$*.

It is easy to show that $s$ is an isometry.

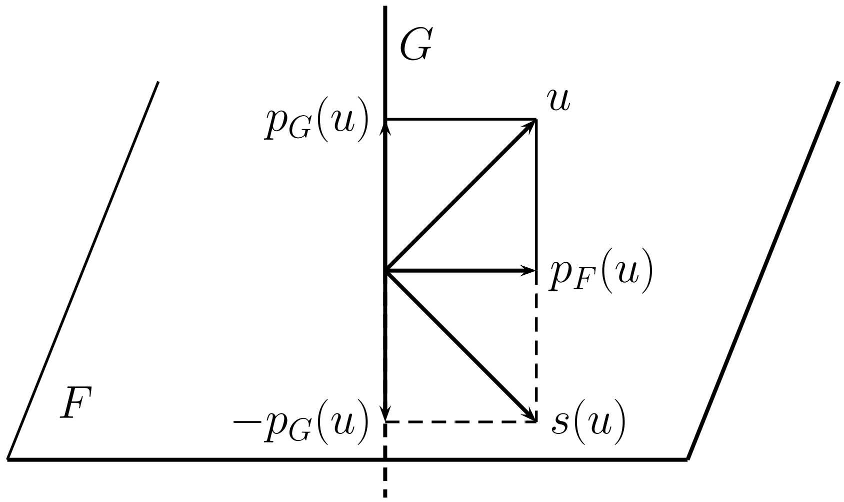


Figure 7.1: A reflection about a hyperplane $F$

Using lemma 5.2.7, it is possible to find an orthonormal basis $(e_1, \ldots, e_n)$ of $E$ consisting of an orthonormal basis of $F$ and an orthonormal basis of $G$.

Assume that $F$ has dimension $p$, so that $G$ has dimension $n - p$.

With respect to the orthonormal basis $(e_1, \ldots, e_n)$, the symmetry $s$ has a matrix of the form

$$\begin{pmatrix} I_p & 0 \\ 0 & -I_{n-p} \end{pmatrix}$$

Thus, $\det(s) = (-1)^{n-p}$, and $s$ is a rotation iff $n - p$ is even.

In particular, when $F$ is a hyperplane $H$, we have $p = n - 1$, and $n - p = 1$, so that $s$ is an improper orthogonal transformation.

When $F = \{0\}$, we have $s = -\mathrm{id}$, which is called the *symmetry with respect to the origin*. The symmetry with respect to the origin is a rotation iff $n$ is even, and an improper orthogonal transformation iff $n$ is odd.

When $n$ is odd, we observe that every improper orthogonal transformation is the composition of a rotation with the symmetry with respect to the origin.

When $G$ is a plane, $p = n - 2$, and $\det(s) = (-1)^2 = 1$, so that a flip about $F$ is a rotation.

In particular, when $n = 3$, $F$ is a line, and a flip about the line $F$ is indeed a rotation of measure $\pi$.

When $F = H$ is a hyperplane, we can give an explicit formula for $s(u)$ in terms of any nonnull vector $w$ orthogonal to $H$.

We get

$$s(u) = u - 2\,\frac{(u \cdot w)}{\|w\|^2}\,w.$$

Such reflections are represented by matrices called *Householder matrices*, and they play an important role in numerical matrix analysis. Householder matrices are symmetric and orthogonal.

Over an orthonormal basis $(e_1, \ldots, e_n)$, a hyperplane reflection about a hyperplane $H$ orthogonal to a nonnull vector $w$ is represented by the matrix

$$H = I_n - 2\,\frac{WW^\top}{\|W\|^2} = I_n - 2\,\frac{WW^\top}{W^\top W},$$

where $W$ is the column vector of the coordinates of $w$.

Since

$$p_G(u) = \frac{(u \cdot w)}{\|w\|^2}\, w,$$

the matrix representing $p_G$ is

$$\frac{WW^\top}{W^\top W},$$

and since $p_H + p_G = \mathrm{id}$, the matrix representing $p_H$ is

$$I_n - \frac{WW^\top}{W^\top W}.$$

The following fact is the key to the proof that every isometry can be decomposed as a product of reflections.

**Lemma 7.1.3** *Let $E$ be any nontrivial Euclidean space. For any two vectors $u, v \in E$, if $\|u\| = \|v\|$, then there is an hyperplane $H$ such that the reflection $s$ about $H$ maps $u$ to $v$, and if $u \neq v$, then this reflection is unique.*

## 7.2 The Cartan–Dieudonné Theorem for Linear Isometries

The fact that the group $\mathbf{O}(n)$ of linear isometries is generated by the reflections is a special case of a theorem known as the *Cartan–Dieudonné theorem*.

Elie Cartan proved a version of this theorem early in the twentieth century. A proof can be found in his book on spinors [**?**], which appeared in 1937 (Chapter I, Section 10, pages 10–12).

Cartan's version applies to nondegenerate quadratic forms over $\mathbb{R}$ or $\mathbb{C}$. The theorem was generalized to quadratic forms over arbitrary fields by Dieudonné [**?**].

One should also consult Emil Artin's book [**?**], which contains an in-depth study of the orthogonal group and another proof of the Cartan–Dieudonné theorem.

First, let us recall the notions of eigenvalues and eigenvectors.

Recall that given any linear map $f\colon E \to E$, a vector $u \in E$ is called an *eigenvector, or proper vector, or characteristic vector of f* iff there is some $\lambda \in K$ such that

$$f(u) = \lambda u.$$

In this case, we say that $u \in E$ is an *eigenvector associated with $\lambda$*.

A scalar $\lambda \in K$ is called an *eigenvalue, or proper value, or characteristic value of f* iff there is some nonnull vector $u \neq 0$ in $E$ such that

$$f(u) = \lambda u,$$

or equivalently if $\mathrm{Ker}\,(f - \lambda \mathrm{id}) \neq \{0\}$.

Given any scalar $\lambda \in K$, the set of all eigenvectors associated with $\lambda$ is the subspace $\mathrm{Ker}\,(f - \lambda \mathrm{id})$, also denoted as $E_\lambda(f)$ or $E(\lambda, f)$, called the *eigenspace associated with $\lambda$, or proper subspace associated with $\lambda$*.

**Theorem 7.2.1** *(Cartan-Dieudonné) Let $E$ be a Euclidean space of dimension $n \geq 1$. Every isometry $f \in \mathbf{O}(E)$ which is not the identity is the composition of at most $n$ reflections. For $n \geq 2$, the identity is the composition of any reflection with itself.*

*Remarks.*

(1) The proof of theorem 7.2.1 shows more than stated.

If 1 is an eigenvalue of $f$, for any eigenvector $w$ associated with 1 (i.e., $f(w) = w$, $w \neq 0$), then $f$ is the composition of $k \leq n-1$ reflections about hyperplanes $F_i$, such that $F_i = H_i \oplus L$, where $L$ is the line $\mathbb{R}w$, and the $H_i$ are subspaces of dimension $n-2$ all orthogonal to $L$.

If 1 is not an eigenvalue of $f$, then $f$ is the composition of $k \leq n$ reflections about hyperplanes $H, F_1, \ldots, F_{k-1}$, such that $F_i = H_i \oplus L$, where $L$ is a line intersecting $H$, and the $H_i$ are subspaces of dimension $n-2$ all orthogonal to $L$.

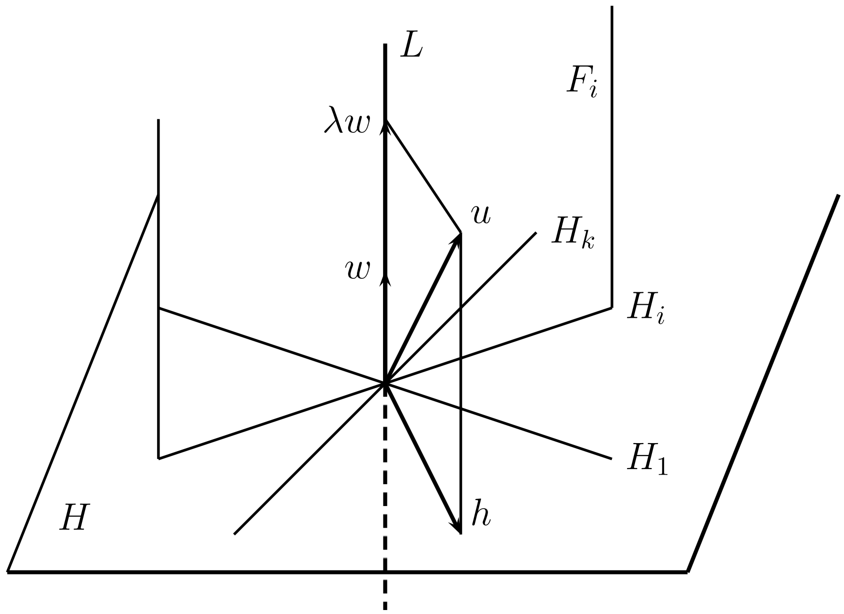


Figure 7.2: An Isometry $f$ as a composition of reflections, when 1 is an eigenvalue of $f$

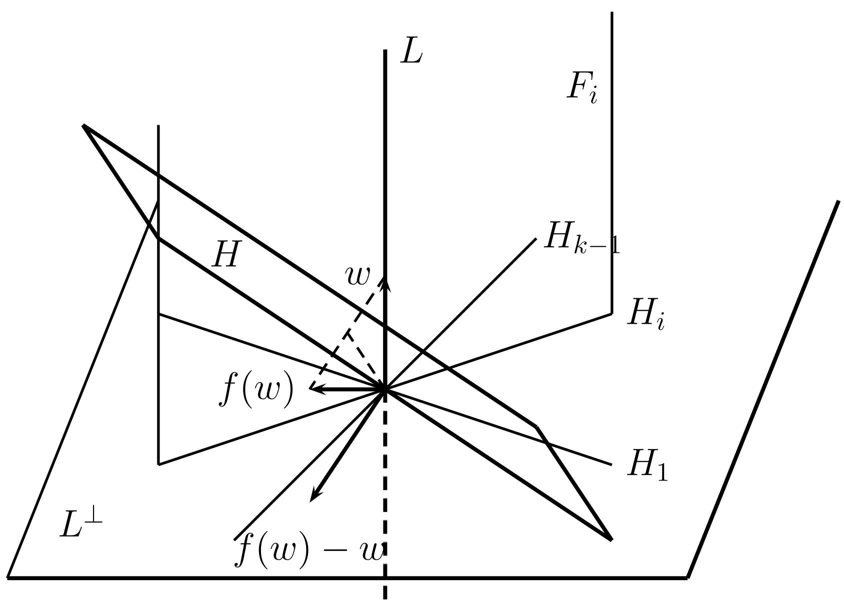


Figure 7.3: An Isometry $f$ as a composition of reflections, when 1 is not an eigenvalue of $f$

(2) It is natural to ask what is the minimal number of hyperplane reflections needed to obtain an isometry $f$.

This has to do with the dimension of the eigenspace $\mathrm{Ker}\,(f - \mathrm{id})$ associated with the eigenvalue 1.

We will prove later that every isometry is the composition of $k$ hyperplane reflections, where

$$k = n - \dim(\mathrm{Ker}\,(f - \mathrm{id})),$$

and that this number is minimal (where $n = \dim(E)$).

When $n = 2$, a reflection is a reflection about a line, and theorem 7.2.1 shows that every isometry in $\mathbf{O}(2)$ is either a reflection about a line or a rotation, and that every rotation is the product of two reflections about some lines.

In general, since $\det(s) = -1$ for a reflection $s$, when $n \geq 3$ is odd, every rotation is the product of an even number $\leq n-1$ of reflections, and when $n$ is even, every improper orthogonal transformation is the product of an odd number $\leq n-1$ of reflections.

In particular, for $n = 3$, every rotation is the product of two reflections about planes.

If $E$ is a Euclidean space of finite dimension and $f\colon E \to E$ is an isometry, if $\lambda$ is any eigenvalue of $f$ and $u$ is an eigenvector associated with $\lambda$, then

$$\|f(u)\| = \|\lambda u\| = |\lambda| \, \|u\| = \|u\| \, ,$$

which implies $|\lambda| = 1$, since $u \neq 0$.

Thus, the real eigenvalues of an isometry are either $+1$ or $-1$.

When $n$ is odd, we can say more about improper isometries. This is because they admit $-1$ as an eigenvalue. When $n$ is odd, an improper isometry is the composition of a reflection about a hyperplane $H$ with a rotation consisting of reflections about hyperplanes $F_1, \ldots, F_{k-1}$ containing a line, $L$, orthogonal to $H$.

**Lemma 7.2.2** *Let $E$ be a Euclidean space of finite dimension $n$, and let $f\colon E \to E$ be an isometry. For any subspace $F$ of $E$, if $f(F) = F$, then $f(F^{\perp}) \subseteq F^{\perp}$ and $E = F \oplus F^{\perp}$.*

Lemma 7.2.2 is the starting point of the proof that every orthogonal matrix can be diagonalized over the field of complex numbers.

Indeed, if $\lambda$ is any eigenvalue of $f$, then
$f(E_\lambda(f)) = E_\lambda(f)$, and thus the orthogonal $E_\lambda(f)^\perp$ is closed under $f$, and

$$E = E_\lambda(f) \oplus E_\lambda(f)^\perp.$$

The problem over $\mathbb{R}$ is that there may not be any real eigenvalues.

However, when $n$ is odd, the following lemma shows that every rotation admits 1 as an eigenvalue (and similarly, when $n$ is even, every improper orthogonal transformation admits 1 as an eigenvalue).

**Lemma 7.2.3** *Let $E$ be a Euclidean space.*

*(1) If $E$ has odd dimension $n = 2m+1$, then every rotation $f$ admits $1$ as an eigenvalue and the eigenspace $F$ of all eigenvectors left invariant under $f$ has an odd dimension $2p+1$. Furthermore, there is an orthonormal basis of $E$, in which $f$ is represented by a matrix of the form*

$$\begin{pmatrix} R_{2(m-p)} & 0 \\ 0 & I_{2p+1} \end{pmatrix}$$

*where $R_{2(m-p)}$ is a rotation matrix that does not have $1$ as an eigenvalue.*

*(2) If $E$ has even dimension $n = 2m$, then every improper orthogonal transformation $f$ admits 1 as an eigenvalue and the eigenspace $F$ of all eigenvectors left invariant under $f$ has an odd dimension $2p+1$. Furthermore, there is an orthonormal basis of $E$, in which $f$ is represented by a matrix of the form*

$$\begin{pmatrix} S_{2(m-p)-1} & 0 \\ 0 & I_{2p+1} \end{pmatrix}$$

*where $S_{2(m-p)-1}$ is an improper orthogonal matrix that does not have 1 as an eigenvalue.*

An example showing that lemma 7.2.3 fails for $n$ even is the following rotation matrix (when $n = 2$):

$$R = \begin{pmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{pmatrix}$$

The above matrix does not have real eigenvalues if $\theta \neq k\pi$.

It is easily shown that for $n = 2$, with respect to any chosen orthonormal basis $(e_1, e_2)$, every rotation is represented by a matrix of form

$$R = \begin{pmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{pmatrix}$$

where $\theta \in [0, 2\pi[$, and that every improper orthogonal transformation is represented by a matrix of the form

$$S = \begin{pmatrix} \cos\theta & \sin\theta \\ \sin\theta & -\cos\theta \end{pmatrix}$$

In the first case, we call $\theta \in [0, 2\pi[$ the *measure* of the angle of rotation of $R$ w.r.t. the orthonormal basis $(e_1, e_2)$.

In the second case, we have a reflection about a line, and it is easy to determine what this line is. It is also easy to see that $S$ is the composition of a reflection about the $x$-axis with a rotation (of matrix $R$).

We refrained from calling $\theta$ "the angle of rotation", because there are some subtleties involved in defining rigorously the notion of angle of two vectors (or two lines).

For example, note that with respect to the "opposite basis" $(e_2, e_1)$, the measure $\theta$ must be changed to $2\pi - \theta$ (or $-\theta$ if we consider the quotient set $\mathbb{R}/2\pi$ of the real numbers modulo $2\pi$).

We will come back to this point after having defined the notion of orientation (see Section 7.8).

It is easily shown that the group $\mathbf{SO}(2)$ of rotations in the plane is abelian.

We can perform the following calculation, using some elementary trigonometry:

$$\begin{pmatrix} \cos\varphi & \sin\varphi \\ \sin\varphi & -\cos\varphi \end{pmatrix} \begin{pmatrix} \cos\psi & \sin\psi \\ \sin\psi & -\cos\psi \end{pmatrix} = \begin{pmatrix} \cos(\varphi+\psi) & \sin(\varphi+\psi) \\ \sin(\varphi+\psi) & -\cos(\varphi+\psi) \end{pmatrix}.$$

The above also shows that the inverse of a rotation matrix

$$R = \begin{pmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{pmatrix}$$

is obtained by changing $\theta$ to $-\theta$ (or $2\pi - \theta$).

Incidently, note that in writing a rotation $r$ as the product of two reflections $r = s_2 s_1$, the first reflection $s_1$ can be chosen arbitrarily, since $s_1^2 = \mathrm{id}$, $r = (r s_1) s_1$, and $r s_1$ is a reflection.

For $n = 3$, the only two choices for $p$ are $p = 1$, which corresponds to the identity, or $p = 0$, in which case, $f$ is a rotation leaving a line invariant.

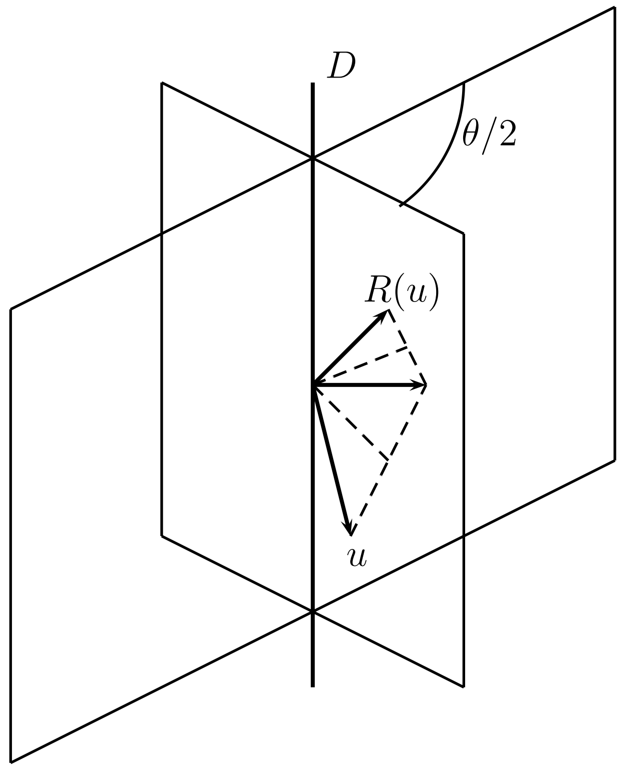


Figure 7.4: $3D$ rotation as the composition of two reflections

This line is called the *axis of rotation*. The rotation $R$ behaves like a two dimentional rotation around the axis of rotation.

The measure of the angle of rotation $\theta$ can be determined through its cosine via the formula

$$\cos\theta = u \cdot R(u),$$

where $u$ is any unit vector orthogonal to the direction of the axis of rotation.

However, this does not determine $\theta \in [0, 2\pi[$ uniquely, since both $\theta$ and $2\pi - \theta$ are possible candidates.

What is missing is an orientation of the plane (through the origin) orthogonal to the axis of rotation. We will come back to this point in Section 7.8.

In the orthonormal basis of the lemma, a rotation is represented by a matrix of the form

$$R = \begin{pmatrix} \cos\theta & -\sin\theta & 0 \\ \sin\theta & \cos\theta & 0 \\ 0 & 0 & 1 \end{pmatrix}.$$

*Remark*: For an arbitrary rotation matrix $A$, since

$$a_{1\,1} + a_{2\,2} + a_{3\,3}$$

(the *trace* of $A$) is the sum of the eigenvalues of $A$, and since these eigenvalues are $\cos\theta + i\sin\theta$, $\cos\theta - i\sin\theta$, and 1, for some $\theta \in [0, 2\pi[$, we can compute $\cos\theta$ from

$$1 + 2\cos\theta = a_{1\,1} + a_{2\,2} + a_{3\,3}.$$

It is also possible to determine the axis of rotation (see the problems).

An improper transformation is either a reflection about a plane, or the product of three reflections, or equivalently the product of a reflection about a plane with a rotation, and a closer look at theorem 7.2.1 shows that the axis of rotation is orthogonal to the plane of the reflection.

Thus, an improper transformation is represented by a matrix of the form

$$S = \begin{pmatrix} \cos\theta & -\sin\theta & 0 \\ \sin\theta & \cos\theta & 0 \\ 0 & 0 & -1 \end{pmatrix}.$$

When $n \geq 3$, the group of rotations $\mathbf{SO}(n)$ is not only generated by hyperplane reflections, but also by flips (about subspaces of dimension $n-2$).

We will also see in Section 7.4 that every proper affine rigid motion can be expressed as the composition of at most $n$ flips, which is perhaps even more surprising!

The proof of these results uses the following key lemma.

**Lemma 7.2.4** *Given any Euclidean space $E$ of dimension $n \geq 3$, for any two reflections $h_1$ and $h_2$ about some hyperplanes $H_1$ and $H_2$, there exist two flips $f_1$ and $f_2$ such that $h_2 \circ h_1 = f_2 \circ f_1$.*

Using lemma 7.2.4 and the Cartan-Dieudonné theorem, we obtain the following characterization of rotations when $n \geq 3$.

**Theorem 7.2.5** *Let $E$ be a Euclidean space of dimension $n \geq 3$. Every rotation $f \in \mathbf{SO}(E)$ is the composition of an even number of flips $f = f_{2k} \circ \cdots \circ f_1$, where $2k \leq n$. Furthermore, if $u \neq 0$ is invariant under $f$ (i.e. $u \in \mathrm{Ker}\,(f - \mathrm{id})$), we can pick the last flip $f_{2k}$ such that $u \in F_{2k}^{\perp}$, where $F_{2k}$ is the subspace of dimension $n - 2$ determining $f_{2k}$.*

*Remarks*:

(1) It is easy to prove that if $f$ is a rotation in $\mathbf{SO}(3)$, if $D$ is its axis and $\theta$ is its angle of rotation, then $f$ is the composition of two flips about lines $D_1$ and $D_2$ orthogonal to $D$ and making an angle $\theta/2$.

(2) It is natural to ask what is the minimal number of flips needed to obtain a rotation $f$ (when $n \geq 3$). As for arbitrary isometries, we will prove later that every rotation is the composition of $k$ flips, where

$$k = n - \dim(\mathrm{Ker}\,(f - \mathrm{id})),$$

and that this number is minimal (where $n = \dim(E)$).

Hyperplane reflections can be used to obtain another proof of the $QR$-decomposition.

## 7.3 $QR$-Decomposition Using Householder Matrices

First, we state the result geometrically. When translated in terms of Householder matrices, we obtain the fact advertised earlier that every matrix (not necessarily invertible) has a $QR$-decomposition.

**Lemma 7.3.1** *Let $E$ be a nontrivial Euclidean space of dimension $n$. Given any orthonormal basis $(e_1, \ldots, e_n)$, for any $n$-tuple of vectors $(v_1, \ldots, v_n)$, there is a sequence of $n$ isometries $h_1, \ldots, h_n$, such that $h_i$ is a hyperplane reflection or the identity, and if $(r_1, \ldots, r_n)$ are the vectors given by*

$$r_j = h_n \circ \cdots \circ h_2 \circ h_1(v_j),$$

*then every $r_j$ is a linear combination of the vectors $(e_1, \ldots, e_j)$, $(1 \leq j \leq n)$. Equivalently, the matrix $R$ whose columns are the components of the $r_j$ over the basis $(e_1, \ldots, e_n)$ is an upper triangular matrix. Furthermore, the $h_i$ can be chosen so that the diagonal entries of $R$ are nonnegative.*

*Remarks*. (1) Since every $h_i$ is a hyperplane reflection or the identity,

$$\rho = h_n \circ \cdots \circ h_2 \circ h_1$$

is an isometry.

(2) If we allow negative diagonal entries in $R$, the last isometry $h_n$ may be omitted.

(3) Instead of picking $r_{k,k} = \|u''_k\|$, which means that

$$w_k = r_{k,k}\, e_k - u''_k,$$

where $1 \leq k \leq n$, it might be preferable to pick $r_{k,k} = -\|u''_k\|$ if this makes $\|w_k\|^2$ larger, in which case

$$w_k = r_{k,k}\, e_k + u''_k.$$

Indeed, since the definition of $h_k$ involves division by $\|w_k\|^2$, it is desirable to avoid division by very small numbers.

Lemma 7.3.1 immediately yields the $QR$-decomposition in terms of Householder transformations.

**Lemma 7.3.2** *For every real $n \times n$-matrix $A$, there is a sequence $H_1, \ldots, H_n$ of matrices, where each $H_i$ is either a Householder matrix or the identity, and an upper triangular matrix $R$, such that*

$$R = H_n \cdots H_2 H_1 A.$$

*As a corollary, there is a pair of matrices $Q, R$, where $Q$ is orthogonal and $R$ is upper triangular, such that $A = QR$ (a QR-decomposition of $A$). Furthermore, $R$ can be chosen so that its diagonal entries are non-negative.*

*Remarks.* (1) Letting

$$A_{k+1} = H_k \cdots H_2 H_1 A,$$

with $A_1 = A$, $1 \leq k \leq n$, the proof of lemma 7.3.1 can be interpreted in terms of the computation of the sequence of matrices $A_1, \ldots, A_{n+1} = R$.

The matrix $A_{k+1}$ has the shape

$$A_{k+1} = \begin{pmatrix} \times & \times & \times & u_1^{k+1} & \times & \times & \times & \times \\ 0 & \times & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & \times & u_k^{k+1} & \times & \times & \times & \times \\ 0 & 0 & 0 & u_{k+1}^{k+1} & \times & \times & \times & \times \\ 0 & 0 & 0 & u_{k+2}^{k+1} & \times & \times & \times & \times \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & 0 & u_{n-1}^{k+1} & \times & \times & \times & \times \\ 0 & 0 & 0 & u_n^{k+1} & \times & \times & \times & \times \end{pmatrix}$$

where the $(k+1)$th column of the matrix is the vector

$$u_{k+1} = h_k \circ \cdots \circ h_2 \circ h_1(v_{k+1}),$$

and thus

$$u'_{k+1} = (u_1^{k+1}, \ldots, u_k^{k+1}),$$

and

$$u''_{k+1} = (u_{k+1}^{k+1}, u_{k+2}^{k+1}, \ldots, u_n^{k+1}).$$

If the last $n-k-1$ entries in column $k+1$ are all zero, there is nothing to do and we let $H_{k+1} = I$.

Otherwise, we kill these $n-k-1$ entries by multiplying $A_{k+1}$ on the left by the Householder matrix $H_{k+1}$ sending $(0,\ldots,0,u^{k+1}_{k+1},\ldots,u^{k+1}_n)$ to $(0,\ldots,0,r_{k+1,k+1},0,\ldots,0)$, where

$$r_{k+1,k+1} = \left\|(u^{k+1}_{k+1},\ldots,u^{k+1}_n)\right\|.$$

(2) If we allow negative diagonal entries in $R$, the matrix $H_n$ may be omitted ($H_n = I$).

(3) If $A$ is invertible and the diagonal entries of $R$ are positive, it can be shown that $Q$ and $R$ are unique.

(4) The method allows the computation of the determinant of $A$. We have

$$\det(A) = (-1)^m r_{1,1} \cdots r_{n,n},$$

where $m$ is the number of Householder matrices (not the identity) among the $H_i$.

(5) The *condition number* of the matrix $A$ is preserved (see Strang [**?**]). This is very good for numerical stability.

We conclude our discussion of isometries with a brief discussion of affine isometries.