Definition 4.2.9 An affine space $(E, \overrightarrow{E})$ is a *Euclidean affine space* iff its underlying vector space $\overrightarrow{E}$ is a Euclidean vector space. Given any two points $a, b \in E$, we define the *distance between a and b, or length of the segment* (a, b), as $\|\mathbf{ab}\|$, the Euclidean norm of $\mathbf{ab}$. Given any two pairs of points (a, b) and (c, d), we define their inner product as $\mathbf{ab} \cdot \mathbf{cd}$. We say that (a, b) and (c, d) are *orthogonal, or perpendicular* iff $\mathbf{ab} \cdot \mathbf{cd} = 0$. We say that two affine subspaces F_1 and F_2 of E are *orthogonal* iff their directions $\overrightarrow{F_1}$ and $\overrightarrow{F_2}$ are orthogonal.

Note that a Euclidean affine space is a normed affine space, in the sense of definition 4.2.10 below.

Definition 4.2.10 Given an affine space $(E, \overrightarrow{E})$, where the space of translations $\overrightarrow{E}$ is a vector space over $\mathbb{R}$ or $\mathbb{C}$, we say that $(E, \overrightarrow{E})$ is a *normed affine space* iff $\overrightarrow{E}$ is a normed vector space with norm $\| \, \|$.

We denote as $\mathbb{E}^m$ the Euclidean affine space obtained from the affine space $\mathbb{A}^m$ by defining on the vector space $\mathbb{R}^m$ the standard inner product

$$(x_1, \ldots, x_m) \cdot (y_1, \ldots, y_m) = x_1 y_1 + \cdots + x_m y_m.$$

The corresponding Euclidean norm is

$$\|(x_1, \ldots, x_m)\| = \sqrt{x_1^2 + \cdots + x_m^2}.$$

We now consider linear maps between Euclidean spaces that preserve the Euclidean norm. These transformations sometimes called *rigid motions* play an important role in geometry.

4.3 Linear Isometries (Orthogonal Transformations)

In this section, we consider linear maps between Euclidean spaces that preserve the Euclidean norm.

Definition 4.3.1 Given any two nontrivial Euclidean spaces E and F of the same finite dimension n, a function $f\colon E \to F$ is *an orthogonal transformation, or a linear isometry* iff it is linear and

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

for all $u \in E$.

Thus, a linear isometry is a linear map that preserves the norm.

Remarks: (1) A linear isometry is often defined as a linear map such that

$$\|f(v) - f(u)\| = \|v - u\|,$$

for all $u, v \in E$. Since the map f is linear, the two definitions are equivalent. The second definition just focuses on preserving the distance between vectors.

(2) Sometimes, a linear map satisfying the condition of definition 4.3.1 is called a *metric map*, and a linear isometry is defined as a *bijective* metric map.

Also, an isometry (without the word linear) is sometimes defined as a function $f\colon E \to F$ (not necessarily linear) such that

$$\|f(v) - f(u)\| = \|v - u\|,$$

for all $u, v \in E$, i.e., as a function that preserves the distance.

This requirement turns out to be very strong. Indeed, the next lemma shows that all these definitions are equivalent when E and F are of finite dimension, and for functions such that $f(0) = 0$.

Lemma 4.3.2 *Given any two nontrivial Euclidean spaces E and F of the same finite dimension n, for every function $f\colon E \to F$, the following properties are equivalent:*

(1) f is a linear map and $\|f(u)\| = \|u\|$, for all $u \in E$;

(2) $\|f(v) - f(u)\| = \|v - u\|$, for all $u, v \in E$, and $f(0) = 0$;

(3) $f(u) \cdot f(v) = u \cdot v$, for all $u, v \in E$.

Furthermore, such a map is bijective.

For (2), we shall prove a slightly stronger result. We prove that if

$$\|f(v) - f(u)\| = \|v - u\|$$

for all $u, v \in E$, for any vector $\tau \in E$, the function $g\colon E \to F$ defined such that

$$g(u) = f(\tau + u) - f(\tau)$$

for all $u \in E$ is a linear map such that $g(0) = 0$ and (3) holds.

Remarks: (i) The dimension assumption is only needed to prove that (3) implies (1) when f is not known to be linear, and to prove that f is surjective, but the proof shows that (1) implies that f is injective.

(ii) In (2), when f does not satisfy the condition $f(0) = 0$, the proof shows that f is an affine map.

Indeed, taking any vector τ as an origin, the map g is linear, and

$$f(\tau + u) = f(\tau) + g(u)$$

for all $u \in E$, proving that f is affine with associated linear map g.

(iii) The implication that (3) implies (1) holds if we also assume that f is surjective, even if E has infinite dimension.

In view of lemma 4.3.2, we will drop the word "linear" in "linear isometry", unless we wish to emphasize that we are dealing with a map between vector spaces.

We are now going to take a closer look at the isometries $f\colon E \to E$ of a Euclidean space of finite dimension.

4.4 The Orthogonal Group, Orthogonal Matrices

In this section, we explore some of the fundamental properties of the orthogonal group and of orthogonal matrices.

As an immediate corollary of the Gram–Schmidt orthonormalization procedure, we obtain the QR-decomposition for invertible matrices.

We prove an important structure theorem for the isometries, namely that they can always be written as a composition of reflections (Theorem 5.2.1).

Lemma 4.4.1 *Let E be any Euclidean space of finite dimension n, and let $f\colon E \to E$ be any linear map. The following properties hold:*

(1) The linear map $f\colon E \to E$ is an isometry iff

$$f \circ f^* = f^* \circ f = \mathrm{id}.$$

(2) For every orthonormal basis $(e_1, \ldots, e_n)$ of E, if the matrix of f is A, then the matrix of f^* is the transpose $A^\top$ of A, and f is an isometry iff A satisfies the identities

$$A\, A^\top = A^\top A = I_n,$$

where I_n denotes the identity matrix of order n, iff the columns of A form an orthonormal basis of E, iff the rows of A form an orthonormal basis of E.

Lemma 4.4.1 shows that the inverse of an isometry f is its adjoint f^*. Lemma 4.4.1 also motivates the following definition:

Definition 4.4.2 A real $n \times n$ matrix is an *orthogonal matrix* iff

$$A\,A^{\top} = A^{\top}A = I_n.$$

Remarks: It is easy to show that the conditions $A\,A^{\top} = I_n$, $A^{\top}A = I_n$, and $A^{-1} = A^{\top}$, are equivalent.

Given any two orthonormal bases $(u_1, \ldots, u_n)$ and $(v_1, \ldots, v_n)$, if P is the change of basis matrix from $(u_1, \ldots, u_n)$ to $(v_1, \ldots, v_n)$ since the columns of P are the coordinates of the vectors v_j with respect to the basis $(u_1, \ldots, u_n)$, and since $(v_1, \ldots, v_n)$ is orthonormal, the columns of P are orthonormal, and by lemma 4.4.1 (2), the matrix P is orthogonal.

The proof of lemma 4.3.2 (3) also shows that if f is an isometry, then the image of an orthonormal basis $(u_1, \ldots, u_n)$ is an orthonormal basis.

Recall that the determinant $\det(f)$ of an endomorphism $f\colon E \to E$ is independent of the choice of a basis in E.

Also, for every matrix $A \in \mathrm{M}_n(\mathbb{R})$, we have $\det(A) = \det(A^\top)$, and for any two $n \times n$-matrices A and B, we have $\det(AB) = \det(A)\det(B)$ (for all these basic results, see Lang [**?**]).

Then, if f is an isometry, and A is its matrix with respect to any orthonormal basis, $A\,A^\top = A^\top A = I_n$ implies that $\det(A)^2 = 1$, that is, either $\det(A) = 1$, or $\det(A) = -1$.

It is also clear that the isometries of a Euclidean space of dimension n form a group, and that the isometries of determinant $+1$ form a subgroup.

Definition 4.4.3 Given a Euclidean space E of dimension n, the set of isometries $f: E \to E$ forms a group denoted as $\mathbf{O}(E)$, or $\mathbf{O}(n)$ when $E = \mathbb{R}^n$, called the *orthogonal group (of E)*.

For every isometry, f, we have $\det(f) = \pm 1$, where $\det(f)$ denotes the determinant of f. The isometries such that $\det(f) = 1$ are called *rotations, or proper isometries, or proper orthogonal transformations*, and they form a subgroup of the special linear group $\mathbf{SL}(E)$ (and of $\mathbf{O}(E)$), denoted as $\mathbf{SO}(E)$, or $\mathbf{SO}(n)$ when $E = \mathbb{R}^n$, called the *special orthogonal group (of E)*.

The isometries such that $\det(f) = -1$ are called *improper isometries, or improper orthogonal transformations, or flip transformations*.

4.5 QR-Decomposition for Invertible Matrices

Now that we have the definition of an orthogonal matrix, we can explain how the Gram–Schmidt orthonormalization procedure immediately yields the QR-decomposition for matrices.

Lemma 4.5.1 *Given any $n \times n$ real matrix A, if A is invertible then there is an orthogonal matrix Q and an upper triangular matrix R with positive diagonal entries such that $A = QR$.*

Proof. We can view the columns of A as vectors $A_1, \ldots, A_n$ in $\mathbb{E}^n$.

If A is invertible, then they are linearly independent, and we can apply lemma 4.2.7 to produce an orthonormal basis using the Gram–Schmidt orthonormalization procedure.

Recall that we construct vectors Q_k and Q'_k as follows:

$$Q'_1 = A_1, \qquad Q_1 = \frac{Q'_1}{\|Q'_1\|},$$

and for the inductive step

$$Q'_{k+1} = A_{k+1} - \sum_{i=1}^{k} (A_{k+1} \cdot Q_i)\, Q_i, \qquad Q_{k+1} = \frac{Q'_{k+1}}{\left\|Q'_{k+1}\right\|},$$

where $1 \leq k \leq n-1$.

If we express the vectors A_k in terms of the Q_i and Q'_i, we get a triangular system

$$\begin{aligned}
A_1 &= \|Q'_1\|\, Q_1, \\
&\ \ \cdots \\
A_j &= (A_j \cdot Q_1)\, Q_1 + \cdots + (A_j \cdot Q_i)\, Q_i + \cdots + (A_j \cdot Q_{j-1})\, Q_{j-1} + \left\|Q'_j\right\| Q_j, \\
&\ \ \cdots \\
A_n &= (A_n \cdot Q_1)\, Q_1 + \cdots + (A_n \cdot Q_{n-2})\, Q_{n-2} + (A_n \cdot Q_{n-1})\, Q_{n-1} + \|Q'_n\|\, Q_n.
\end{aligned}$$

Remarks: (1) Because the diagonal entries of R are positive, it can be shown that Q and R are unique.

(2) The QR-decomposition holds even when A is not invertible. In this case, R has some zero on the diagonal. However, a different proof is needed. We will give a nice proof using Householder matrices (see also Strang [**?**]).

Example 6. Consider the matrix

$$A = \begin{pmatrix} 0 & 0 & 5 \\ 0 & 4 & 1 \\ 1 & 1 & 1 \end{pmatrix}$$

We leave as an exercise to show that $A = QR$ with

$$Q = \begin{pmatrix} 0 & 0 & 1 \\ 0 & 1 & 0 \\ 1 & 0 & 0 \end{pmatrix} \quad \text{and} \quad R = \begin{pmatrix} 1 & 1 & 1 \\ 0 & 4 & 1 \\ 0 & 0 & 5 \end{pmatrix}$$

Another example of QR-decomposition is

$$A = \begin{pmatrix} 1 & 1 & 2 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{pmatrix}$$

where

$$Q = \begin{pmatrix} 1/\sqrt{2} & 1/\sqrt{2} & 0 \\ 0 & 0 & 1 \\ 1/\sqrt{2} & -1/\sqrt{2} & 0 \end{pmatrix}$$

and

$$R = \begin{pmatrix} \sqrt{2} & 1/\sqrt{2} & \sqrt{2} \\ 0 & 1/\sqrt{2} & \sqrt{2} \\ 0 & 0 & 1 \end{pmatrix}$$

The QR-decomposition yields a rather efficient and numerically stable method for solving systems of linear equations.

Indeed, given a system $Ax = b$, where A is an $n \times n$ invertible matrix, writing $A = QR$, since Q is orthogonal, we get

$$Rx = Q^{\top} b,$$

and since R is upper triangular, we can solve it by Gaussian elimination, by solving for the last variable x_n first, substituting its value into the system, then solving for x_{n-1}, etc.

The QR-decomposition is also very useful in solving least squares problems (we will come back to this later on), and for finding eigenvalues.

It can be easily adapted to the case where A is a rectangular $m \times n$ matrix with independent columns (thus, $n \leq m$).

In this case, Q is not quite orthogonal. It is an $m \times n$ matrix whose columns are orthogonal, and R is an invertible $n \times n$ upper diagonal matrix with positive diagonal entries. For more on QR, see Strang [**?**].

It should also be said that the Gram–Schmidt orthonormalization procedure that we have presented is not very stable numerically, and instead, one should use the *modified Gram–Schmidt method*.

To compute Q'_{k+1}, instead of projecting A_{k+1} onto $Q_1, \ldots, Q_k$ in a single step, it is better to perform k projections.

We compute $Q^1_{k+1}, Q^2_{k+1}, \ldots, Q^k_{k+1}$ as follows:

$$\begin{aligned} Q^1_{k+1} &= A_{k+1} - (A_{k+1} \cdot Q_1)\, Q_1, \\ Q^{i+1}_{k+1} &= Q^i_{k+1} - (Q^i_{k+1} \cdot Q_{i+1})\, Q_{i+1}, \end{aligned}$$

where $1 \leq i \leq k-1$.

It is easily shown that $Q'_{k+1} = Q^k_{k+1}$. The reader is urged to code this method.

Chapter 5

The Cartan–Dieudonné Theorem

5.1 Orthogonal Reflections

Orthogonal symmetries are a very important example of isometries. First let us review the definition of projections.

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 5.1.1 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 5.1.2 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 $s\colon E \rightarrow E$, 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.

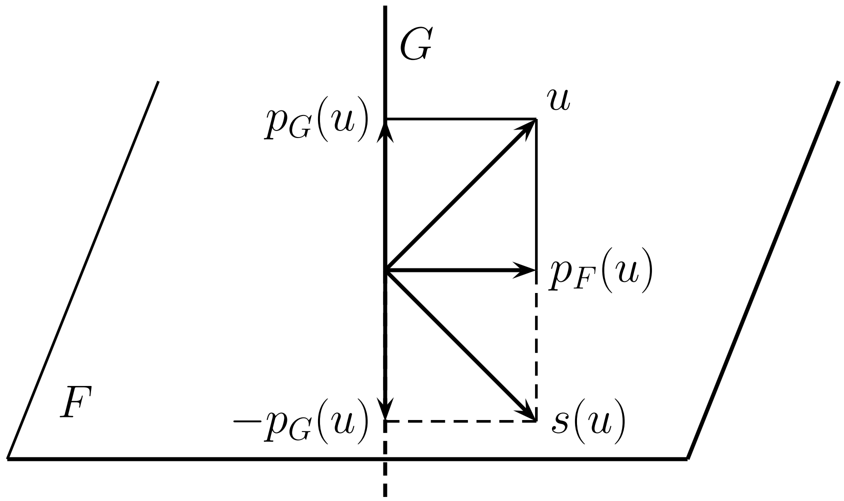

Figure 5.1: A reflection about a hyperplane F

Using lemma 4.2.7, 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 π.

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 5.1.3 *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.*

5.2 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 λ.*

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 λ is the subspace $\mathrm{Ker}\,(f - \lambda \mathrm{id})$, also denoted as $E_\lambda(f)$ or $E(\lambda, f)$, called the *eigenspace associated with λ, or proper subspace associated with λ.*

Theorem 5.2.1 *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 5.2.1 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.

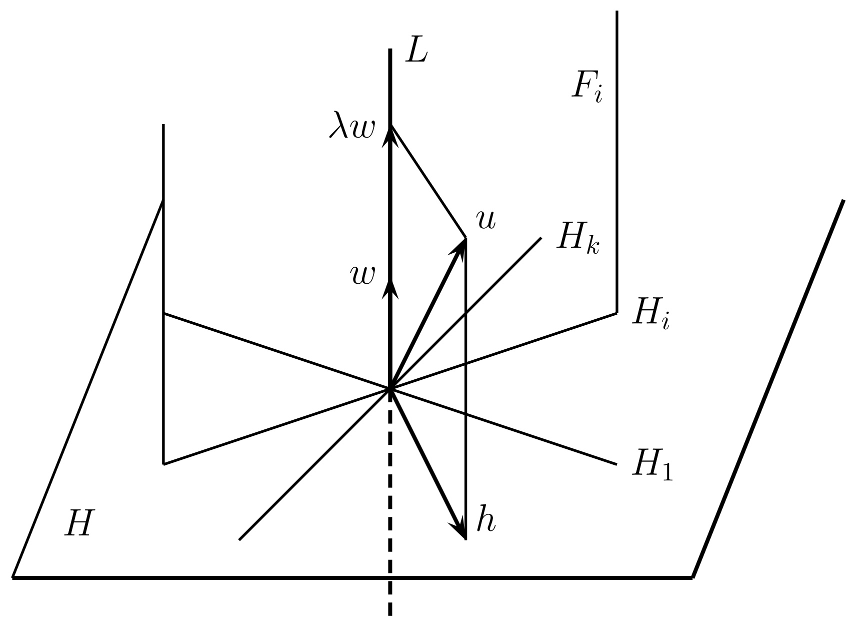

Figure 5.2: An Isometry f as a composition of reflections, when 1 is an eigenvalue of f

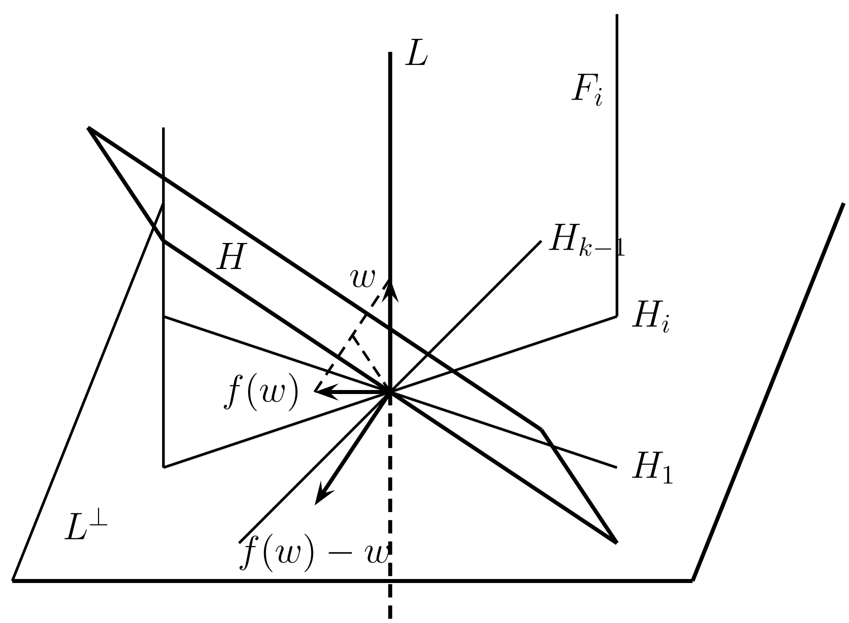

Figure 5.3: An Isometry f as a composition of reflections, when 1 is not an eigenvalue of f

(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 5.2.1 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 λ is any eigenvalue of f and u is an eigenvector associated with λ, 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 5.2.2 *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 5.2.2 is the starting point of the proof that every orthogonal matrix can be diagonalized over the field of complex numbers.

Indeed, if λ 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 5.2.3 *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 5.2.3 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 θ "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 θ must be changed to $2\pi - \theta$ (or $-\theta$ if we consider the quotient set $\mathbb{R}/2\pi$ of the real numbers modulo 2π).

We will come back to this point after having defined the notion of orientation (see Section 5.8).

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 θ 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 $s_1^2 = \mathrm{id}$, $r = (rs_1)s_1$, and rs_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.

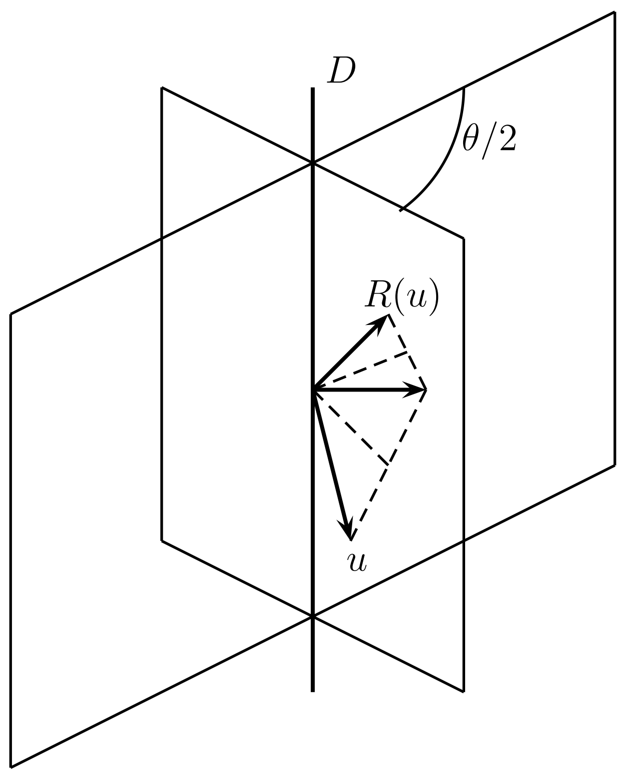

Figure 5.4: $3D$ rotation as the composition of two reflections

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 θ 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 θ 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 5.8.

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 5.2.1 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 5.4 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 5.2.4 *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 5.2.4 and the Cartan-Dieudonné theorem, we obtain the following characterization of rotations when $n \geq 3$.

Theorem 5.2.5 *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 θ 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.