7
The Cartan–Dieudonné Theorem

7.1 Orthogonal Reflections

In this chapter the structure of the orthogonal group is studied in more depth. In particular, we prove that every isometry in $\mathbf{O}(n)$ is the composition of at most n reflections about hyperplanes (for $n \geq 2$, see Theorem 7.2.1). This important result is a special case of the "Cartan–Dieudonné theorem" (Cartan [29], Dieudonné [47]). We also prove that every rotation in $\mathbf{SO}(n)$ is the composition of at most n flips (for $n \geq 3$).

Hyperplane reflections are represented by matrices called Householder matrices. These matrices play an important role in numerical methods, for instance for solving systems of linear equations, solving least squares problems, for computing eigenvalues, and for transforming a symmetric matrix into a tridiagonal matrix. We prove a simple geometric lemma that immediately yields the QR-decomposition of arbitrary matrices in terms of Householder matrices.

Affine isometries are defined, and their fixed points are investigated. First, we characterize the set of fixed points of an affine map. Using this characterization, we prove that every affine isometry f can be written uniquely as

$$f = t \circ g, \quad \text{with} \quad t \circ g = g \circ t,$$

where g is an isometry having a fixed point, and t is a translation by a vector τ such that $\overrightarrow{f}(\tau) = \tau$, and with some additional nice properties (see Lemma 7.6.2). This is a generalization of a classical result of Chasles about (proper) rigid motions in $\mathbb{R}^3$ (screw motions). We also show that the Cartan–Dieudonné theorem can be generalized to affine isometries: Every rigid motion in $\mathbf{Is}(n)$ is the composition of at most n affine reflections if it has a fixed point, or else of at most $n+2$ affine reflections. We prove that every rigid motion in $\mathbf{SE}(n)$ is the composition of at most n flips (for $n \geq 3$). Finally, the orientation of a Euclidean space is defined, and we discuss volume forms and cross products.

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 $p_F(u) = v$ and $p_G(u) = w$. 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 (or reflection) with respect to F and parallel to G* 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 (or reflection) with respect to F and parallel to G* 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 a *hyperplane symmetry with respect to F (or reflection about F)*, and when G is a plane (and thus $\dim(F) = n - 2$), we call s a *flip about F*.

A reflection about a hyperplane F is shown in Figure 7.1.

For any two vectors $u, v \in E$, it is easily verified using the bilinearity of the inner product that

$$\|u + v\|^2 - \|u - v\|^2 = 4(u \cdot v).$$

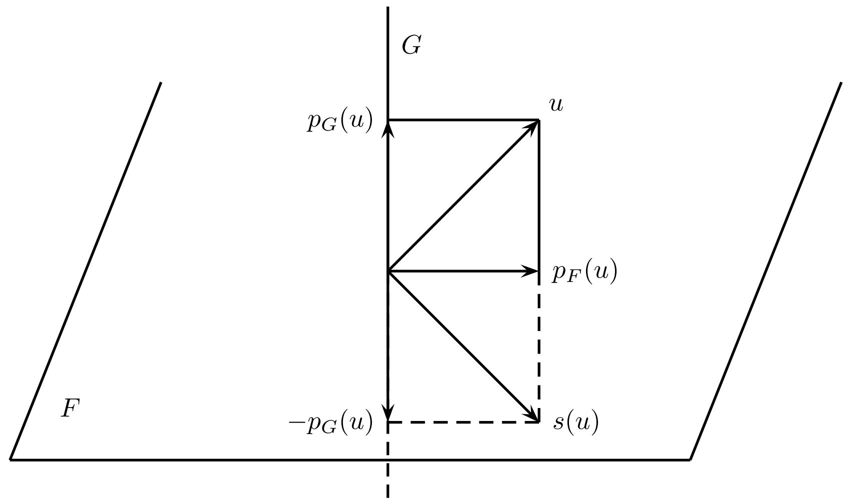

Figure 7.1. A reflection about a hyperplane F

Then, since

$$u = p_F(u) + p_G(u)$$

and

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

since F and G are orthogonal, it follows that

$$p_F(u) \cdot p_G(v) = 0,$$

and thus,

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

so that s is an isometry.

Using Lemma 6.2.7, 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.

Remark: Given any two orthogonal subspaces F, G forming a direct sum $E = F \oplus G$, let f be the symmetry with respect to F and parallel to G, and let g be the symmetry with respect to G and parallel to F. We leave as an exercise to show that

$$f \circ g = g \circ f = -\mathrm{id}.$$

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. Indeed, from

$$u = p_H(u) + p_G(u),$$

since $p_G(u) \in G$ and G is spanned by w, which is orthogonal to H, we have

$$p_G(u) = \lambda w$$

for some $\lambda \in \mathbb{R}$, and we get

$$u \cdot w = \lambda \|w\|^2,$$

and thus

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

Since

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

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 (see Kincaid and Cheney [100] or Ciarlet [33]). Householder matrices are symmetric and orthogonal. It is easily checked that 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 over the basis $(e_1, \ldots, e_n)$, and I_n is the identity $n \times n$ matrix. 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

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

These formulae will be used in Section 8.1 to derive a formula for a rotation of $\mathbb{R}^3$, given the direction w of its axis of rotation and given the angle θ of rotation.

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 a hyperplane H such that the reflection s about H maps u to v, and if $u \neq v$, then this reflection is unique.*

Proof. If $u = v$, then any hyperplane containing u does the job. Otherwise, we must have $H = \{v - u\}^\perp$, and by the above formula,

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

and since

$$\|(v-u)\|^2 = \|u\|^2 + \|v\|^2 - 2u \cdot v$$

and $\|u\| = \|v\|$, we have

$$\|(v-u)\|^2 = 2\|u\|^2 - 2u \cdot v,$$

and thus, $s(u) = v$. $\square$

If E is a complex vector space and the inner product is Hermitian, Lemma 7.1.3 is false. The problem is that the vector $v - u$ does not work unless the inner product $u \cdot v$ is real! We will see in the next chapter that the lemma can be salvaged enough to yield the QR-decomposition in terms of Householder transformations.

Using the above property, we can prove a fundamental property of isometries: They are generated by reflections about hyperplanes.

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 [29], 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 [47]. One should also consult Emil Artin's book [4], which contains an in-depth study of the orthogonal group and another proof of the Cartan–Dieudonné theorem.

First, let us review the notions of eigenvalues and eigenvectors. Recall that given any linear map $f: E \to E$, a vector $u \in E$ is called an *eigenvector, or proper vector, or characteristic vector, of* f if 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 if 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 by $E_\lambda(f)$ or $E(\lambda, f)$, called the *eigenspace associated with* λ*, or proper subspace associated with* λ.

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

Proof. We proceed by induction on n. When $n = 1$, every isometry $f \in \mathbf{O}(E)$ is either the identity or $-\mathrm{id}$, but $-\mathrm{id}$ is a reflection about $H = \{0\}$. When $n \geq 2$, we have $\mathrm{id} = s \circ s$ for every reflection s. Let us now consider the case where $n \geq 2$ and f is not the identity. There are two subcases.

Case 1. f admits 1 as an eigenvalue, i.e., there is some nonnull vector w such that $f(w) = w$. In this case, let H be the hyperplane orthogonal to w, so that $E = H \oplus \mathbb{R}w$. We claim that $f(H) \subseteq H$. Indeed, if

$$v \cdot w = 0$$

for any $v \in H$, since f is an isometry, we get

$$f(v) \cdot f(w) = v \cdot w = 0,$$

and since $f(w) = w$, we get

$$f(v) \cdot w = f(v) \cdot f(w) = 0,$$

and thus $f(v) \in H$. Furthermore, since f is not the identity, f is not the identity of H. Since H has dimension $n-1$, by the induction hypothesis applied to H, there are at most $k \leq n-1$ reflections $s_1, \ldots, s_k$ about some hyperplanes $H_1, \ldots, H_k$ in H, such that the restriction of f to H is the composition $s_k \circ \cdots \circ s_1$. Each s_i can be extended to a reflection in E as follows: If $H = H_i \oplus L_i$ (where $L_i = H_i^{\perp}$, the orthogonal complement of H_i in H), $L = \mathbb{R}w$, and $F_i = H_i \oplus L$, since H and L are orthogonal, F_i is indeed a hyperplane, $E = F_i \oplus L_i = H_i \oplus L \oplus L_i$, and for every $u = h + \lambda w \in H \oplus L = E$, since

$$s_i(h) = p_{H_i}(h) - p_{L_i}(h),$$

we can define s_i on E such that

$$s_i(h + \lambda w) = p_{H_i}(h) + \lambda w - p_{L_i}(h),$$

and since $h \in H$, $w \in L$, $F_i = H_i \oplus L$, and $H = H_i \oplus L_i$, we have

$$s_i(h + \lambda w) = p_{F_i}(h + \lambda w) - p_{L_i}(h + \lambda w),$$

which defines a reflection about $F_i = H_i \oplus L$. Now, since f is the identity on $L = \mathbb{R}w$, it is immediately verified that $f = s_k \circ \cdots \circ s_1$, with $k \leq n-1$.

Case 2. f does not admit 1 as an eigenvalue, i.e., $f(u) \neq u$ for all $u \neq 0$. Pick any $w \neq 0$ in E, and let H be the hyperplane orthogonal to $f(w) - w$. Since f is an isometry, we have $\|f(w)\| = \|w\|$, and by Lemma 7.1.3, we know that $s(w) = f(w)$, where s is the reflection about H, and we claim that $s \circ f$ leaves w invariant. Indeed, since $s^2 = \mathrm{id}$, we have

$$s(f(w)) = s(s(w)) = w.$$

Since $s^2 = \mathrm{id}$, we cannot have $s \circ f = \mathrm{id}$, since this would imply that $f = s$, where s is the identity on H, contradicting the fact that f is not the identity on any vector. Thus, we are back to Case 1. Thus, there are $k \leq n-1$ hyperplane reflections such that $s \circ f = s_k \circ \cdots \circ s_1$, from which we get

$$f = s \circ s_k \circ \cdots \circ s_1,$$

with at most $k + 1 \leq n$ reflections. $\square$

Remarks:

(1) A slightly different proof can be given. Either f is the identity, or there is some nonnull vector u such that $f(u) \neq u$. In the second case, proceed as in the second part of the proof, to get back to the case where f admits 1 as an eigenvalue.

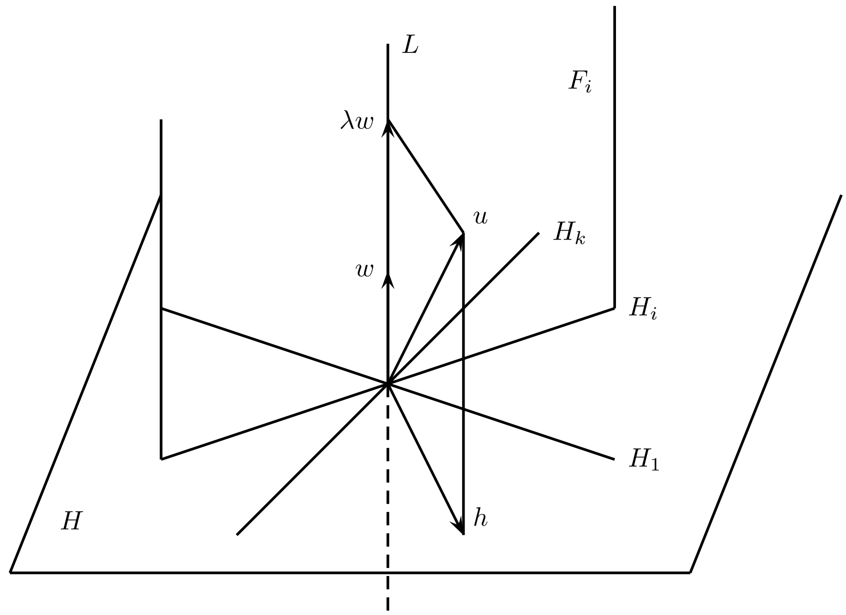

Figure 7.2. An isometry f as a composition of reflections, when 1 is an eigenvalue of f

(2) Theorem 7.2.1 still holds if the inner product on E is replaced by a nondegenerate symmetric bilinear form φ, but the proof is a lot harder.

(3) 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 (the H_i are hyperplanes in H). This situation is illustrated in Figure 7.2.
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 (the H_i are hyperplanes in $L^{\perp}$). This situation is illustrated in Figure 7.3.

(4) 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 $n = \dim(E)$).

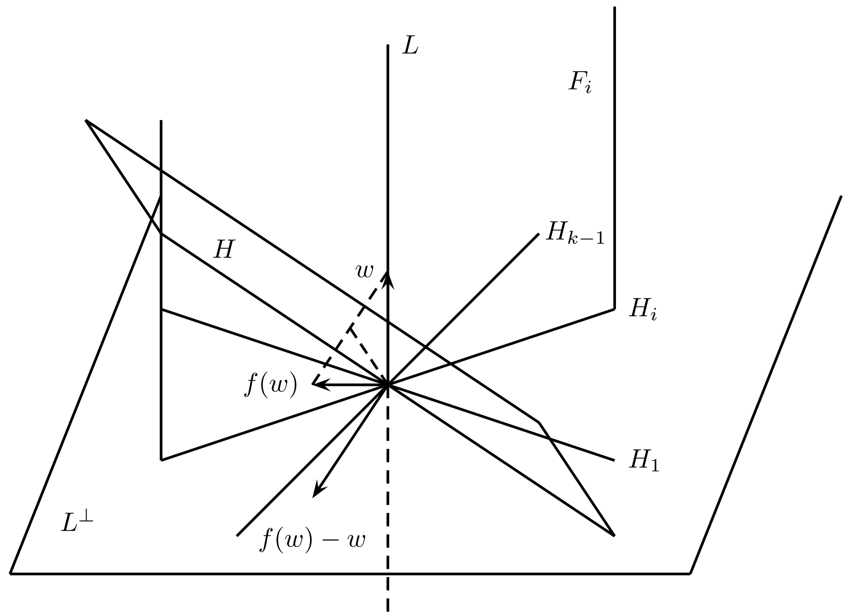

Figure 7.3. An isometry f as a composition of reflections when 1 is not an eigenvalue of f

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 less than or equal to $n - 1$ of reflections, and when n is even, every improper orthogonal transformation is the product of an odd number less than or equal to $n-1$ of reflections.

In particular, for $n = 3$, every rotation is the product of two reflections about planes. When n is odd, we can say more about improper isometries. Indeed, when n is odd, every improper isometry admits the eigenvalue -1. This is because if E is a Euclidean space of finite dimension and $f\colon E \to E$ is an isometry, because $\|f(u)\| = \|u\|$ for every $u \in E$, 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. However, it is well known that polynomials of odd degree always have some real root. As a consequence, the characteristic polynomial $\det(f - \lambda \mathrm{id})$ of f has some real root, which is either $+1$ or -1. Since f is an improper isometry, $\det(f) = -1$, and since $\det(f)$ is the product of the eigenvalues, the real roots cannot all be $+1$, and thus

-1 is an eigenvalue of f. Going back to the proof of Theorem 7.2.1, since -1 is an eigenvalue of f, there is some nonnull eigenvector w such that $f(w) = -w$. Using the second part of the proof, we see that the hyperplane H orthogonal to $f(w) - w = -2w$ is in fact orthogonal to w, and thus f is the product 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 orthogonal to H, and the H_i are hyperplanes in $H = L^{\perp}$ orthogonal to L. However, k must be odd, and so $k-1$ is even, and thus the composition of the reflections about $F_1, \ldots, F_{k-1}$ is a rotation. Thus, 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. In particular, when $n = 3$, every improper orthogonal transformation is the product of a rotation with a reflection about a plane orthogonal to the axis of rotation.

Using Theorem 7.2.1, we can also give a rather simple proof of the classical fact that in a Euclidean space of odd dimension, every rotation leaves some nonnull vector invariant, and thus a line invariant.

If λ is an eigenvalue of f, then the following lemma shows that the orthogonal complement $E_\lambda(f)^{\perp}$ of the eigenspace associated with λ is closed under f.

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 $E = F \oplus F^{\perp}$.*

Proof. We just have to prove that if $w \in E$ is orthogonal to every $u \in F$, then $f(w)$ is also orthogonal to every $u \in F$. However, since $f(F) = F$, for every $v \in F$, there is some $u \in F$ such that $f(u) = v$, and we have

$$f(w) \cdot v = f(w) \cdot f(u) = w \cdot u,$$

since f is an isometry. Since we assumed that $w \in E$ is orthogonal to every $u \in F$, we have

$$w \cdot u = 0,$$

and thus

$$f(w) \cdot v = 0,$$

and this for every $v \in F$. Thus, $f(F^{\perp}) \subseteq F^{\perp}$. The fact that $E = F \oplus F^{\perp}$ follows from Lemma 6.2.8. $\square$

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 λ is any eigenvalue of f, then $f(E_\lambda(f)) = E_\lambda(f)$, where $E_\lambda(f)$ is the eigenspace associated with λ, 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.

Proof. We prove only (1), the proof of (2) being similar. Since f is a rotation and $n = 2m+1$ is odd, by Theorem 7.2.1, f is the composition of an even number less than or equal to $2m$ of reflections. From Lemma 2.11.1, recall the Grassmann relation

$$\dim(M) + \dim(N) = \dim(M+N) + \dim(M \cap N),$$

where M and N are subspaces of E. Now, if M and N are hyperplanes, their dimension is $n-1$, and thus $\dim(M \cap N) \geq n-2$. Thus, if we intersect $k \leq n$ hyperplanes, we see that the dimension of their intersection is at least $n-k$. Since each of the reflections is the identity on the hyperplane defining it, and since there are at most $2m = n-1$ reflections, their composition is the identity on a subspace of dimension at least 1. This proves that 1 is an eigenvalue of f. Let F be the eigenspace associated with 1, and assume that its dimension is q. Let $G = F^{\perp}$ be the orthogonal of F. By Lemma 7.2.2, G is stable under f, and $E = F \oplus G$. Using Lemma 6.2.7, we can find an orthonormal basis of E consisting of an orthonormal basis for G and orthonormal basis for F. In this basis, the matrix of f is of the form

$$\begin{pmatrix} R_{2m+1-q} & 0 \\ 0 & I_q \end{pmatrix}.$$

Thus, $\det(f) = \det(R)$, and R must be a rotation, since f is a rotation and $\det(f) = 1$. Now, if f left some vector $u \neq 0$ in G invariant, this vector would be an eigenvector for 1, and we would have $u \in F$, the eigenspace associated with 1, which contradicts $E = F \oplus G$. Thus, by the first part of the proof, the dimension of G must be even, since otherwise, the restriction of f to G would admit 1 as an eigenvalue. Consequently, q must be odd, and R does not admit 1 as an eigenvalue. Letting $q = 2p + 1$, the lemma is established. $\square$

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 for $\theta \neq k\pi$.

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 7.8).

It is easily shown that the group $\mathbf{SO}(2)$ of rotations in the plane is abelian. First, recall that every plane rotation is the product of two reflections (about lines), and that every isometry in $\mathbf{O}(2)$ is either a reflection or a rotation. To alleviate the notation, we will omit the composition operator $\circ$, and write rs instead of $r \circ s$. Now, if r is a rotation and s is a reflection, rs being in $\mathbf{O}(2)$ must be a reflection (since $\det(rs) = \det(r)\det(s) = -1$), and thus $(rs)^2 = \mathrm{id}$, since a reflection is an involution, which implies that

$$srs = r^{-1}.$$

Then, given two rotations r_1 and r_2, writing r_1 as $r_1 = s_2 s_1$ for two reflections s_1, s_2, we have

$$r_1 r_2 r_1^{-1} = s_2 s_1 r_2 (s_2 s_1)^{-1} = s_2 s_1 r_2 s_1^{-1} s_2^{-1} = s_2 s_1 r_2 s_1 s_2 = s_2 r_2^{-1} s_2 = r_2,$$

since $srs = r^{-1}$ for all reflections s and rotations r, and thus $r_1 r_2 = r_2 r_1$.

We could also 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 $2\pi - \theta$). Incidentally, 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. This line D is called the *axis of rotation*. The rotation R behaves like a two-dimensional rotation around the axis of rotation. Thus, the rotation R is the composition of two reflections about planes containing the axis of rotation D and forming an angle $\theta/2$. This is illustrated in Figure 7.4.

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 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

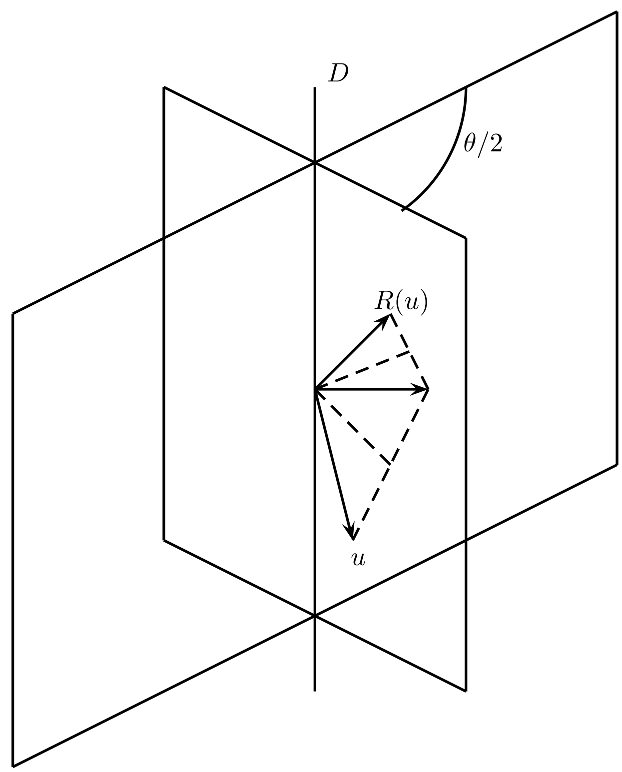

Figure 7.4. 3D rotation as the composition of two reflections

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 we noted in the discussion following Theorem 7.2.1 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 $h_2 \circ h_1 = f_2 \circ f_1$.*

Proof. If $h_1 = h_2$, it is obvious that

$$h_1 \circ h_2 = h_1 \circ h_1 = \mathrm{id} = f_1 \circ f_1$$

for any flip f_1. If $h_1 \neq h_2$, then $H_1 \cap H_2 = F$, where $\dim(F) = n - 2$ (by the Grassmann relation). We can pick an orthonormal basis $(e_1, \ldots, e_n)$ of E such that $(e_1, \ldots, e_{n-2})$ is an orthonormal basis of F. We can also extend $(e_1, \ldots, e_{n-2})$ to an orthonormal basis $(e_1, \ldots, e_{n-2}, u_1, v_1)$ of E, where $(e_1, \ldots, e_{n-2}, u_1)$ is an orthonormal basis of H_1, in which case

$$\begin{aligned} e_{n-1} &= \cos\theta_1\, u_1 + \sin\theta_1\, v_1, \\ e_n &= \sin\theta_1\, u_1 - \cos\theta_1\, v_1, \end{aligned}$$

for some $\theta_1 \in [0, 2\pi]$. Since h_1 is the identity on H_1 and v_1 is orthogonal to H_1, it follows that $h_1(u_1) = u_1$, $h_1(v_1) = -v_1$, and we get

$$\begin{aligned} h_1(e_{n-1}) &= \cos\theta_1\, u_1 - \sin\theta_1\, v_1, \\ h_1(e_n) &= \sin\theta_1\, u_1 + \cos\theta_1\, v_1. \end{aligned}$$

After some simple calculations, we get

$$\begin{aligned} h_1(e_{n-1}) &= \cos 2\theta_1\, e_{n-1} + \sin 2\theta_1\, e_n, \\ h_1(e_n) &= \sin 2\theta_1\, e_{n-1} - \cos 2\theta_1\, e_n. \end{aligned}$$

As a consequence, the matrix A_1 of h_1 over the basis $(e_1, \ldots, e_n)$ is of the form

$$A_1 = \begin{pmatrix} I_{n-2} & 0 & 0 \\ 0 & \cos 2\theta_1 & \sin 2\theta_1 \\ 0 & \sin 2\theta_1 & -\cos 2\theta_1 \end{pmatrix}.$$

Similarly, the matrix A_2 of h_2 over the basis $(e_1, \ldots, e_n)$ is of the form

$$A_2 = \begin{pmatrix} I_{n-2} & 0 & 0 \\ 0 & \cos 2\theta_2 & \sin 2\theta_2 \\ 0 & \sin 2\theta_2 & -\cos 2\theta_2 \end{pmatrix}.$$

Observe that both A_1 and A_2 have the eigenvalues -1 and $+1$ with multiplicity $n - 1$. The trick is to observe that if we change the last entry in I_{n-2} from $+1$ to -1 (which is possible since $n \geq 3$), we have the following product $A_2 A_1$:

$$\begin{pmatrix} I_{n-3} & 0 & 0 & 0 \\ 0 & -1 & 0 & 0 \\ 0 & 0 & \cos 2\theta_2 & \sin 2\theta_2 \\ 0 & 0 & \sin 2\theta_2 & -\cos 2\theta_2 \end{pmatrix} \begin{pmatrix} I_{n-3} & 0 & 0 & 0 \\ 0 & -1 & 0 & 0 \\ 0 & 0 & \cos 2\theta_1 & \sin 2\theta_1 \\ 0 & 0 & \sin 2\theta_1 & -\cos 2\theta_1 \end{pmatrix}.$$

Now, the two matrices above are clearly orthogonal, and they have the eigenvalues $-1, -1$, and $+1$ with multiplicity $n-2$, which implies that the corresponding isometries leave invariant a subspace of dimension $n-2$ and act as $-\mathrm{id}$ on its orthogonal complement (which has dimension 2). This means that the above two matrices represent two flips f_1 and f_2 such that $h_2 \circ h_1 = f_2 \circ f_1$. $\square$

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}.*

Proof. By Theorem 7.2.1, the rotation f can be expressed as an even number of hyperplane reflections $f = s_{2k} \circ s_{2k-1} \circ \cdots \circ s_2 \circ s_1$, with $2k \leq n$. By Lemma 7.2.4, every composition of two reflections $s_{2i} \circ s_{2i-1}$ can be replaced by the composition of two flips $f_{2i} \circ f_{2i-1}$ $(1 \leq i \leq k)$, which yields $f = f_{2k} \circ \cdots \circ f_1$, where $2k \leq n$.

Assume that $f(u) = u$, with $u \neq 0$. We have already made the remark that in the case where 1 is an eigenvalue of f, the proof of Theorem 7.2.1 shows that the reflections s_i can be chosen so that $s_i(u) = u$. In particular, if each reflection s_i is a reflection about the hyperplane H_i, we have $u \in H_{2k-1} \cap H_{2k}$. Letting $F = H_{2k-1} \cap H_{2k}$, pick an orthonormal basis $(e_1, \ldots, e_{n-3}, e_{n-2})$ of F, where

$$e_{n-2} = \frac{u}{\|u\|}.$$

The proof of Lemma 7.2.4 yields two flips f_{2k-1} and f_{2k} such that

$$f_{2k}(e_{n-2}) = -e_{n-2} \quad \text{and} \quad s_{2k} \circ s_{2k-1} = f_{2k} \circ f_{2k-1},$$

since the $(n-2)$th diagonal entry in both matrices is -1, which means that $e_{n-2} \in F_{2k}^{\perp}$, where F_{2k} is the subspace of dimension $n-2$ determining f_{2k}. Since $u = \|u\| e_{n-2}$, we also have $u \in F_{2k}^{\perp}$. $\square$

Remarks:

(1) It is easy to prove that if f is a rotation in $\mathbf{SO}(3)$ and 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 $n = \dim(E)$).

We now show that 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. For any orthonormal basis $(e_1, \ldots, e_n)$ and 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.

Proof. We proceed by induction on n. For $n = 1$, we have $v_1 = \lambda e_1$ for some $\lambda \in \mathbb{R}$. If $\lambda \geq 0$, we let $h_1 = \mathrm{id}$, else if $\lambda < 0$, we let $h_1 = -\mathrm{id}$, the reflection about the origin.

For $n \geq 2$, we first have to find h_1. Let

$$r_{1,1} = \|v_1\|.$$

If $v_1 = r_{1,1}e_1$, we let $h_1 = \mathrm{id}$. Otherwise, there is a unique hyperplane reflection h_1 such that

$$h_1(v_1) = r_{1,1}\, e_1,$$

defined such that

$$h_1(u) = u - 2\,\frac{(u \cdot w_1)}{\|w_1\|^2}\, w_1$$

for all $u \in E$, where

$$w_1 = r_{1,1}\, e_1 - v_1.$$

The map h_1 is the reflection about the hyperplane H_1 orthogonal to the vector $w_1 = r_{1,1}\, e_1 - v_1$. Letting

$$r_1 = h_1(v_1) = r_{1,1}\, e_1,$$

it is obvious that r_1 belongs to the subspace spanned by e_1, and $r_{1,1} = \|v_1\|$ is nonnegative.

Next, assume that we have found k linear maps $h_1, \ldots, h_k$, hyperplane reflections or the identity, where $1 \leq k \leq n-1$, such that if $(r_1, \ldots, r_k)$ are the vectors given by

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

then every r_j is a linear combination of the vectors $(e_1, \ldots, e_j)$, $1 \leq j \leq k$. The vectors $(e_1, \ldots, e_k)$ form a basis for the subspace denoted by U'_k, the vectors $(e_{k+1}, \ldots, e_n)$ form a basis for the subspace denoted by U''_k, the subspaces U'_k and U''_k are orthogonal, and $E = U'_k \oplus U''_k$. Let

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

We can write

$$u_{k+1} = u'_{k+1} + u''_{k+1},$$

where $u'_{k+1} \in U'_k$ and $u''_{k+1} \in U''_k$. Let

$$r_{k+1,k+1} = \|u''_{k+1}\|.$$

If $u''_{k+1} = r_{k+1,k+1}\, e_{k+1}$, we let $h_{k+1} = \mathrm{id}$. Otherwise, there is a unique hyperplane reflection h_{k+1} such that

$$h_{k+1}(u''_{k+1}) = r_{k+1,k+1}\, e_{k+1},$$

defined such that

$$h_{k+1}(u) = u - 2\,\frac{(u \cdot w_{k+1})}{\|w_{k+1}\|^2}\, w_{k+1}$$

for all $u \in E$, where

$$w_{k+1} = r_{k+1,k+1}\, e_{k+1} - u''_{k+1}.$$

The map h_{k+1} is the reflection about the hyperplane H_{k+1} orthogonal to the vector $w_{k+1} = r_{k+1,k+1}\, e_{k+1} - u''_{k+1}$. However, since $u''_{k+1}, e_{k+1} \in U''_k$ and U'_k is orthogonal to U''_k, the subspace U'_k is contained in H_{k+1}, and thus, the vectors $(r_1, \ldots, r_k)$ and u'_{k+1}, which belong to U'_k, are invariant under h_{k+1}. This proves that

$$h_{k+1}(u_{k+1}) = h_{k+1}(u'_{k+1}) + h_{k+1}(u''_{k+1}) = u'_{k+1} + r_{k+1,k+1}\, e_{k+1}$$

is a linear combination of $(e_1, \ldots, e_{k+1})$. Letting

$$r_{k+1} = h_{k+1}(u_{k+1}) = u'_{k+1} + r_{k+1,k+1}\, e_{k+1},$$

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

$$r_{k+1} = h_{k+1} \circ \cdots \circ h_2 \circ h_1(v_{k+1})$$

is a linear combination of $(e_1, \ldots, e_{k+1})$. The coefficient of r_{k+1} over e_{k+1} is $r_{k+1,k+1} = \|u''_{k+1}\|$, which is nonnegative. This concludes the induction step, and thus the proof. □

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.

(4) The method also applies to any m-tuple of vectors $(v_1, \ldots, v_m)$, where m is not necessarily equal to n (the dimension of E). In this case, R is an upper triangular $n \times m$ matrix we leave the minor adjustments to the method as an exercise to the reader (if $m > n$, the last $m - n$ vectors are unchanged).

Lemma 7.3.1 directly yields the QR-decomposition in terms of Householder transformations (see Strang [165, 166], Golub and Van Loan [75], Trefethen and Bau [170], Kincaid and Cheney [100], or Ciarlet [33]).

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 nonnegative.

Proof. The jth column of A can be viewed as a vector v_j over the canonical basis $(e_1, \ldots, e_n)$ of $\mathbb{E}^n$ (where $(e_j)_i = 1$ if $i = j$, and 0 otherwise, $1 \leq i, j \leq n$). Applying Lemma 7.3.1 to $(v_1, \ldots, v_n)$, 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 $(e_1, \ldots, e_j)$, $1 \leq j \leq n$. Letting R be the matrix whose columns are the vectors r_j, and H_i the matrix associated with h_i, it is clear that

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

where R is upper triangular and every H_i is either a Householder matrix or the identity. However, $h_i \circ h_i = \mathrm{id}$ for all i, $1 \leq i \leq n$, and so

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

for all j, $1 \leq j \leq n$. But $\rho = h_1 \circ h_2 \circ \cdots \circ h_n$ is an isometry, and by Lemma 6.4.1, ρ is represented by an orthogonal matrix Q. It is clear that $A = QR$, where R is upper triangular. As we noted in Lemma 7.3.1, the diagonal entries of R can be chosen to be nonnegative. $\square$

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

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

and

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

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

$$\left(0, \ldots, 0, u_{k+1}^{k+1}, \ldots, u_n^{k+1}\right) \quad \text{to} \quad (0, \ldots, 0, r_{k+1,k+1}, 0, \ldots, 0),$$

where $r_{k+1,k+1} = \|(u_{k+1}^{k+1}, \ldots, u_n^{k+1})\|$.

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

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

(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 [166], Golub and Van Loan [75], Trefethen and Bau [170], Kincaid and Cheney [100], or Ciarlet [33]). This is very good for numerical stability.

(6) The method also applies to a rectangular $m \times n$ matrix. In this case, R is also an $m \times n$ matrix (and it is upper triangular).

We now turn to affine isometries.

7.4 Affine Isometries (Rigid Motions)

In the remaining sections we study affine isometries. First, we characterize the set of fixed points of an affine map. Using this characterization, we prove that every affine isometry f can be written uniquely as

$$f = t \circ g, \quad \text{with} \quad t \circ g = g \circ t,$$

where g is an isometry having a fixed point, and t is a translation by a vector τ such that $\overrightarrow{f}(\tau) = \tau$, and with some additional nice properties (see Theorem 7.6.2). This is a generalization of a classical result of Chasles about (proper) rigid motions in $\mathbb{R}^3$ (screw motions). We prove a generalization of the Cartan–Dieudonné theorem for the affine isometries: Every isometry in $\mathbf{Is}(n)$ can be written as the composition of at most n reflections if it has a fixed point, or else as the composition of at most $n+2$ reflections. We also prove that every rigid motion in $\mathbf{SE}(n)$ is the composition of at most n flips (for $n \geq 3$). This is somewhat surprising, in view of the previous theorem.

Definition 7.4.1 Given any two nontrivial Euclidean affine spaces E and F of the same finite dimension n, a function $f\colon E \to F$ is *an affine isometry (or rigid map)* if it is an affine map and

$$\|\mathbf{f(a)f(b)}\| = \|\mathbf{ab}\|,$$

for all $a, b \in E$. When $E = F$, an affine isometry $f\colon E \to E$ is also called a *rigid motion*.

Thus, an affine isometry is an affine map that preserves the distance. This is a rather strong requirement. In fact, we will show that for any function $f\colon E \to F$, the assumption that

$$\|\mathbf{f}(\mathbf{a})\mathbf{f}(\mathbf{b})\| = \|\mathbf{ab}\|,$$

for all $a, b \in E$, forces f to be an affine map.

Remark: Sometimes, an affine isometry is defined as a *bijective* affine isometry. When E and F are of finite dimension, the definitions are equivalent.

The following simple lemma is left as an exercise.

Lemma 7.4.2 *Given any two nontrivial Euclidean affine spaces E and F of the same finite dimension n, an affine map $f\colon E \to F$ is an affine isometry iff its associated linear map $\overrightarrow{f}\colon \overrightarrow{E} \to \overrightarrow{F}$ is an isometry. An affine isometry is a bijection.*

Let us now consider affine isometries $f\colon E \to E$. If $\overrightarrow{f}$ is a rotation, we call f a *proper (or direct) affine isometry*, and if $\overrightarrow{f}$ is an improper linear isometry, we call f an *improper (or skew) affine isometry*. It is easily shown that the set of affine isometries $f\colon E \to E$ forms a group, and those for which $\overrightarrow{f}$ is a rotation is a subgroup. The group of affine isometries, or rigid motions, is a subgroup of the affine group $\mathbf{GA}(E)$, denoted by $\mathbf{Is}(E)$ (or $\mathbf{Is}(n)$ when $E = \mathbb{E}^n$). In Snapper and Troyer [160] the group of rigid motions is denoted by $\mathbf{Mo}(E)$. Since we denote the group of affine bijections as $\mathbf{GA}(E)$, perhaps we should denote the group of affine isometries by $\mathbf{IA}(E)$ (or $\mathbf{EA}(E)$!). The subgroup of $\mathbf{Is}(E)$ consisting of the direct rigid motions is also a subgroup of $\mathbf{SA}(E)$, and it is denoted by $\mathbf{SE}(E)$ (or $\mathbf{SE}(n)$, when $E = \mathbb{E}^n$). The translations are the affine isometries f for which $\overrightarrow{f} = \mathrm{id}$, the identity map on $\overrightarrow{E}$. The following lemma is the counterpart of Lemma 6.3.2 for isometries between Euclidean vector spaces.

Lemma 7.4.3 *Given any two nontrivial Euclidean affine 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 an affine map and $\|\mathbf{f}(\mathbf{a})\mathbf{f}(\mathbf{b})\| = \|\mathbf{ab}\|$, for all $a, b \in E$.

(2) $\|\mathbf{f}(\mathbf{a})\mathbf{f}(\mathbf{b})\| = \|\mathbf{ab}\|$, for all $a, b \in E$.

Proof. Obviously, (1) implies (2). In order to prove that (2) implies (1), we proceed as follows. First, we pick some arbitrary point $\Omega \in E$. We define the map $g\colon \overrightarrow{E} \to \overrightarrow{F}$ such that

$$g(u) = \mathbf{f(\Omega)f(\Omega + u)}$$

for all $u \in E$. Since

$$f(\Omega) + g(u) = f(\Omega) + \mathbf{f(\Omega)f(\Omega + u)} = f(\Omega + u)$$

for all $u \in \overrightarrow{E}$, f will be affine if we can show that g is linear, and f will be an affine isometry if we can show that g is a linear isometry.

Observe that

$$\begin{aligned} g(v) - g(u) &= \mathbf{f(\Omega)f(\Omega + v)} - \mathbf{f(\Omega)f(\Omega + u)} \\ &= \mathbf{f(\Omega + u)f(\Omega + v)}. \end{aligned}$$

Then, the hypothesis

$$\|\mathbf{f(a)f(b)}\| = \|\mathbf{ab}\|$$

for all $a, b \in E$, implies that

$$\|g(v) - g(u)\| = \|\mathbf{f(\Omega + u)f(\Omega + v)}\| = \|\mathbf{(\Omega + u)(\Omega + v)}\| = \|v - u\|.$$

Thus, g preserves the distance. Also, by definition, we have

$$g(0) = 0.$$

Thus, we can apply Lemma 6.3.2, which shows that g is indeed a linear isometry, and thus f is an affine isometry. $\square$

In order to understand the structure of affine isometries, it is important to investigate the fixed points of an affine map.

7.5 Fixed Points of Affine Maps

Recall that $E\big(1, \overrightarrow{f}\big)$ denotes the eigenspace of the linear map $\overrightarrow{f}$ associated with the scalar 1, that is, the subspace consisting of all vectors $u \in \overrightarrow{E}$ such that $\overrightarrow{f}(u) = u$. Clearly, $\operatorname{Ker}\big(\overrightarrow{f} - \mathrm{id}\big) = E\big(1, \overrightarrow{f}\big)$. Given some origin $\Omega \in E$, since

$$f(a) = f(\Omega + \mathbf{\Omega a}) = f(\Omega) + \overrightarrow{f}(\mathbf{\Omega a}),$$

we have $\mathbf{f(\Omega)f(a)} = \overrightarrow{f}(\mathbf{\Omega a})$, and thus

$$\mathbf{\Omega f(a)} = \mathbf{\Omega f(\Omega)} + \overrightarrow{f}(\mathbf{\Omega a}).$$

From the above, we get

$$\mathbf{\Omega f(a)} - \mathbf{\Omega a} = \mathbf{\Omega f(\Omega)} + \overrightarrow{f}(\mathbf{\Omega a}) - \mathbf{\Omega a}.$$

Using this, we show the following lemma, which holds for arbitrary affine spaces of finite dimension and for arbitrary affine maps.

Lemma 7.5.1 *Let E be any affine space of finite dimension. For every affine map $f\colon E \to E$, let $\mathrm{Fix}(f) = \{a \in E \mid f(a) = a\}$ be the set of fixed points of f. The following properties hold:*

(1) If f has some fixed point a, so that $\mathrm{Fix}(f) \neq \emptyset$, then $\mathrm{Fix}(f)$ is an affine subspace of E such that

$$\mathrm{Fix}(f) = a + E\big(1, \overrightarrow{f}\big) = a + \mathrm{Ker}\,\big(\overrightarrow{f} - \mathrm{id}\big),$$

where $E\big(1, \overrightarrow{f}\big)$ is the eigenspace of the linear map $\overrightarrow{f}$ for the eigenvalue 1.

(2) The affine map f has a unique fixed point iff $E\big(1, \overrightarrow{f}\big) = \mathrm{Ker}\,\big(\overrightarrow{f} - \mathrm{id}\big) = \{0\}$.

Proof. (1) Since the identity

$$\mathbf{\Omega f(b)} - \mathbf{\Omega b} = \mathbf{\Omega f(\Omega)} + \overrightarrow{f}(\mathbf{\Omega b}) - \mathbf{\Omega b}$$

holds for all $\Omega, b \in E$, if $f(a) = a$, then $\mathbf{af(a)} = 0$, and thus, letting $\Omega = a$, for any $b \in E$,

$$f(b) = b$$

iff

$$\mathbf{af(b)} - \mathbf{ab} = 0$$

iff

$$\overrightarrow{f}(\mathbf{ab}) - \mathbf{ab} = 0$$

iff

$$\mathbf{ab} \in E\big(1, \overrightarrow{f}\big) = \mathrm{Ker}\,\big(\overrightarrow{f} - \mathrm{id}\big),$$

which proves that

$$\mathrm{Fix}(f) = a + E\big(1, \overrightarrow{f}\big) = a + \mathrm{Ker}\,\big(\overrightarrow{f} - \mathrm{id}\big).$$

(2) Again, fix some origin Ω. Some a satisfies $f(a) = a$ iff

$$\mathbf{\Omega f(a)} - \mathbf{\Omega a} = 0$$

iff

$$\mathbf{\Omega f(\Omega)} + \overrightarrow{f}(\mathbf{\Omega a}) - \mathbf{\Omega a} = 0,$$

which can be rewritten as

$$\big(\overrightarrow{f} - \mathrm{id}\big)(\mathbf{\Omega a}) = -\mathbf{\Omega f(\Omega)}.$$

We have $E\big(1, \overrightarrow{f}\big) = \mathrm{Ker}\,\big(\overrightarrow{f} - \mathrm{id}\big) = \{0\}$ iff $\overrightarrow{f} - \mathrm{id}$ is injective, and since $\overrightarrow{E}$ has finite dimension, $\overrightarrow{f} - \mathrm{id}$ is also surjective, and thus, there is indeed some $a \in E$ such that

$$\big(\overrightarrow{f} - \mathrm{id}\big)(\mathbf{\Omega a}) = -\mathbf{\Omega f(\Omega)},$$

and it is unique, since $\overrightarrow{f} - \mathrm{id}$ is injective. Conversely, if f has a unique fixed point, say a, from

$$\big(\overrightarrow{f} - \mathrm{id}\big)(\mathbf{\Omega a}) = -\mathbf{\Omega f(\Omega)},$$

we have $\big(\overrightarrow{f} - \mathrm{id}\big)(\mathbf{\Omega a}) = 0$ iff $f(\Omega) = \Omega$, and since a is the unique fixed point of f, we must have $a = \Omega$, which shows that $\overrightarrow{f} - \mathrm{id}$ is injective. $\square$

Remark: The fact that E has finite dimension is used only to prove (2), and (1) holds in general.

If an isometry f leaves some point fixed, we can take such a point Ω as the origin, and then $f(\Omega) = \Omega$ and we can view f as a rotation or an improper orthogonal transformation, depending on the nature of $\overrightarrow{f}$. Note that it is quite possible that $\mathrm{Fix}(f) = \emptyset$. For example, nontrivial translations have no fixed points. A more interesting example is provided by the composition of a plane reflection about a line composed with a a nontrivial translation parallel to this line.

Otherwise, we will see in Theorem 7.6.2 that every affine isometry is the (commutative) composition of a translation with an isometry that always has a fixed point.

7.6 Affine Isometries and Fixed Points

Let E be an affine space. Given any two affine subspaces F, G, if F and G are orthogonal complements in E, which means that $\overrightarrow{F}$ and $\overrightarrow{G}$ are orthogonal subspaces of $\overrightarrow{E}$ such that $\overrightarrow{E} = \overrightarrow{F} \oplus \overrightarrow{G}$, for any point $\Omega \in F$, we define $q \colon E \to \overrightarrow{G}$ such that

$$q(a) = p_{\overrightarrow{G}}(\mathbf{\Omega a}).$$

Note that $q(a)$ is independent of the choice of $\Omega \in F$, since we have

$$\mathbf{\Omega a} = p_{\overrightarrow{F}}(\mathbf{\Omega a}) + p_{\overrightarrow{G}}(\mathbf{\Omega a}),$$

and for any $\Omega_1 \in F$, we have

$$\mathbf{\Omega_1 a} = \mathbf{\Omega_1 \Omega} + p_{\overrightarrow{F}}(\mathbf{\Omega a}) + p_{\overrightarrow{G}}(\mathbf{\Omega a}),$$

and since $\mathbf{\Omega_1\Omega} \in \overrightarrow{F}$, this shows that

$$p_{\overrightarrow{G}}(\mathbf{\Omega_1 a}) = p_{\overrightarrow{G}}(\mathbf{\Omega a}).$$

Then the map $g\colon E \to E$ such that $g(a) = a - 2q(a)$, or equivalently

$$\mathbf{ag(a)} = -2q(a) = -2p_{\overrightarrow{G}}(\mathbf{\Omega a}),$$

does not depend on the choice of $\Omega \in F$. If we identify E to $\overrightarrow{E}$ by choosing any origin Ω in F, we note that g is identified with the symmetry with respect to $\overrightarrow{F}$ and parallel to $\overrightarrow{G}$. Thus, the map g is an affine isometry, and it is called the *orthogonal symmetry about* F. Since

$$g(a) = \Omega + \mathbf{\Omega a} - 2p_{\overrightarrow{G}}(\mathbf{\Omega a})$$

for all $\Omega \in F$ and for all $a \in E$, we note that the linear map $\overrightarrow{g}$ associated with g is the (linear) symmetry about the subspace $\overrightarrow{F}$ (the direction of F), and parallel to $\overrightarrow{G}$ (the direction of G).

Remark: The map $p\colon E \to F$ such that $p(a) = a - q(a)$, or equivalently

$$\mathbf{ap(a)} = -q(a) = -p_{\overrightarrow{G}}(\mathbf{\Omega a}),$$

is also independent of $\Omega \in F$, and it is called the *orthogonal projection onto* F.

The following amusing lemma shows the extra power afforded by affine orthogonal symmetries: Translations are subsumed! Given two parallel affine subspaces F_1 and F_2 in E, letting $\overrightarrow{F}$ be the common direction of F_1 and F_2 and $\overrightarrow{G} = \overrightarrow{F}^{\perp}$ be its orthogonal complement, for any $a \in F_1$, the affine subspace $a + \overrightarrow{G}$ intersects F_2 in a single point b (see Lemma 2.11.2). We define the *distance between* F_1 *and* F_2 as $\|\mathbf{ab}\|$. It is easily seen that the distance between F_1 and F_2 is independent of the choice of a in F_1, and that it is the minimum of $\|\mathbf{xy}\|$ for all $x \in F_1$ and all $y \in F_2$.

Lemma 7.6.1 *Given any affine space E, if $f\colon E \to E$ and $g\colon E \to E$ are orthogonal symmetries about parallel affine subspaces F_1 and F_2, then $g \circ f$ is a translation defined by the vector $2\mathbf{ab}$, where $\mathbf{ab}$ is any vector perpendicular to the common direction $\overrightarrow{F}$ of F_1 and F_2 such that $\|\mathbf{ab}\|$ is the distance between F_1 and F_2, with $a \in F_1$ and $b \in F_2$. Conversely, every translation by a vector τ is obtained as the composition of two orthogonal symmetries about parallel affine subspaces F_1 and F_2 whose common direction is orthogonal to $\tau = \mathbf{ab}$, for some $a \in F_1$ and some $b \in F_2$ such that the distance between F_1 and F_2 is $\|\mathbf{ab}\|/2$.*

Proof. We observed earlier that the linear maps $\overrightarrow{f}$ and $\overrightarrow{g}$ associated with f and g are the linear reflections about the directions of F_1 and F_2.

However, F_1 and F_2 have the same direction, and so $\overrightarrow{f} = \overrightarrow{g}$. Since $\overrightarrow{g \circ f} = \overrightarrow{g} \circ \overrightarrow{f}$ and since $\overrightarrow{f} \circ \overrightarrow{g} = \overrightarrow{f} \circ \overrightarrow{f} = \mathrm{id}$, because every reflection is an involution, we have $\overrightarrow{g \circ f} = \mathrm{id}$, proving that $g \circ f$ is a translation. If we pick $a \in F_1$, then $g \circ f(a) = g(a)$, the reflection of $a \in F_1$ about F_2, and it is easily checked that $g \circ f$ is the translation by the vector $\tau = \mathbf{ag(a)}$ whose norm is twice the distance between F_1 and F_2. The second part of the lemma is left as an easy exercise. $\square$

We conclude our quick study of affine isometries by proving a result that plays a major role in characterizing the affine isometries. This result may be viewed as a generalization of Chasles's theorem about the direct rigid motions in $\mathbb{E}^3$.

Theorem 7.6.2 *Let E be a Euclidean affine space of finite dimension n. For every affine isometry $f\colon E \to E$, there is a unique isometry $g\colon E \to E$ and a unique translation $t = t_\tau$, with $\overrightarrow{f}(\tau) = \tau$ (i.e., $\tau \in \mathrm{Ker}\,\big(\overrightarrow{f} - \mathrm{id}\big)$), such that the set $\mathrm{Fix}(g) = \{a \in E \mid g(a) = a\}$ of fixed points of g is a nonempty affine subspace of E of direction*

$$\overrightarrow{G} = \mathrm{Ker}\,\big(\overrightarrow{f} - \mathrm{id}\big) = E\big(1, \overrightarrow{f}\big),$$

and such that

$$f = t \circ g \quad \textit{and} \quad t \circ g = g \circ t.$$

Furthermore, we have the following additional properties:

(a) $f = g$ and $\tau = 0$ iff f has some fixed point, i.e., iff $\mathrm{Fix}(f) \neq \emptyset$.

(b) If f has no fixed points, i.e., $\mathrm{Fix}(f) = \emptyset$, then $\dim\big(\mathrm{Ker}\,\big(\overrightarrow{f} - \mathrm{id}\big)\big) \geq 1$.

Proof. The proof rests on the following two key facts:

(1) If we can find some $x \in E$ such that $\mathbf{xf(x)} = \tau$ belongs to $\mathrm{Ker}\,\big(\overrightarrow{f} - \mathrm{id}\big)$, we get the existence of g and τ.

(2) $\overrightarrow{E} = \mathrm{Ker}\,\big(\overrightarrow{f} - \mathrm{id}\big) \oplus \mathrm{Im}\,\big(\overrightarrow{f} - \mathrm{id}\big)$, and the spaces $\mathrm{Ker}\,\big(\overrightarrow{f} - \mathrm{id}\big)$ and $\mathrm{Im}\,\big(\overrightarrow{f} - \mathrm{id}\big)$ are orthogonal. This implies the uniqueness of g and τ.

First, we prove that for every isometry $h\colon \overrightarrow{E} \to \overrightarrow{E}$, $\mathrm{Ker}\,(h - \mathrm{id})$ and $\mathrm{Im}\,(h - \mathrm{id})$ are orthogonal and that

$$\overrightarrow{E} = \mathrm{Ker}\,(h - \mathrm{id}) \oplus \mathrm{Im}\,(h - \mathrm{id}).$$

Recall that

$$\dim\big(\overrightarrow{E}\big) = \dim(\mathrm{Ker}\,\varphi) + \dim(\mathrm{Im}\,\varphi),$$

for any linear map $\varphi\colon \overrightarrow{E} \to \overrightarrow{E}$ (for instance, see Lang [107], or Strang [166]). To show that we have a direct sum, we prove orthogonality. Let $u \in \operatorname{Ker}(h - \mathrm{id})$, so that $h(u) = u$, let $v \in \overrightarrow{E}$, and compute

$$u \cdot (h(v) - v) = u \cdot h(v) - u \cdot v = h(u) \cdot h(v) - u \cdot v = 0,$$

since $h(u) = u$ and h is an isometry.

Next, assume that there is some $x \in E$ such that $\mathbf{xf(x)} = \tau$ belongs to $\operatorname{Ker}\big(\overrightarrow{f} - \mathrm{id}\big)$. If we define $g\colon E \to E$ such that

$$g = t_{(-\tau)} \circ f,$$

we have

$$g(x) = f(x) - \tau = x,$$

since $\mathbf{xf(x)} = \tau$ is equivalent to $x = f(x) - \tau$. As a composition of isometries, g is an isometry, x is a fixed point of g, and since $\tau \in \operatorname{Ker}\big(\overrightarrow{f} - \mathrm{id}\big)$, we have

$$\overrightarrow{f}(\tau) = \tau,$$

and since

$$g(b) = f(b) - \tau$$

for all $b \in E$, we have $\overrightarrow{g} = \overrightarrow{f}$. Since g has some fixed point x, by Lemma 7.5.1, $\operatorname{Fix}(g)$ is an affine subspace of E with direction $\operatorname{Ker}\big(\overrightarrow{g} - \mathrm{id}\big) = \operatorname{Ker}\big(\overrightarrow{f} - \mathrm{id}\big)$. We also have $f(b) = g(b) + \tau$ for all $b \in E$, and thus

$$(g \circ t_\tau)(b) = g(b + \tau) = g(b) + \overrightarrow{g}(\tau) = g(b) + \overrightarrow{f}(\tau) = g(b) + \tau = f(b),$$

and

$$(t_\tau \circ g)(b) = g(b) + \tau = f(b),$$

which proves that $t \circ g = g \circ t$.

To prove the existence of x as above, pick any arbitrary point $a \in E$. Since

$$\overrightarrow{E} = \operatorname{Ker}\big(\overrightarrow{f} - \mathrm{id}\big) \oplus \operatorname{Im}\big(\overrightarrow{f} - \mathrm{id}\big),$$

there is a unique vector $\tau \in \operatorname{Ker}\big(\overrightarrow{f} - \mathrm{id}\big)$ and some $v \in \overrightarrow{E}$ such that

$$\mathbf{af(a)} = \tau + \overrightarrow{f}(v) - v.$$

For any $x \in E$, since we also have

$$\mathbf{xf(x)} = \mathbf{xa} + \mathbf{af(a)} + \mathbf{f(a)f(x)} = \mathbf{xa} + \mathbf{af(a)} + \overrightarrow{f}(\mathbf{ax}),$$

we get

$$\mathbf{xf}(\mathbf{x}) = \mathbf{xa} + \tau + \overrightarrow{f}(v) - v + \overrightarrow{f}(\mathbf{ax}),$$

which can be rewritten as

$$\mathbf{xf}(\mathbf{x}) = \tau + \big(\overrightarrow{f} - \mathrm{id}\big)(v + \mathbf{ax}).$$

If we let $\mathbf{ax} = -v$, that is, $x = a - v$, we get

$$\mathbf{xf}(\mathbf{x}) = \tau,$$

with $\tau \in \operatorname{Ker}\big(\overrightarrow{f} - \mathrm{id}\big)$.

Finally, we show that τ is unique. Assume two decompositions (g_1, τ_1) and (g_2, τ_2). Since $\overrightarrow{f} = \overrightarrow{g_1}$, we have $\operatorname{Ker}(\overrightarrow{g_1} - \mathrm{id}) = \operatorname{Ker}\big(\overrightarrow{f} - \mathrm{id}\big)$. Since g_1 has some fixed point b, we get

$$f(b) = g_1(b) + \tau_1 = b + \tau_1,$$

that is, $\mathbf{bf}(\mathbf{b}) = \tau_1$, and $\mathbf{bf}(\mathbf{b}) \in \operatorname{Ker}\big(\overrightarrow{f} - \mathrm{id}\big)$, since $\tau_1 \in \operatorname{Ker}\big(\overrightarrow{f} - \mathrm{id}\big)$. Similarly, for some fixed point c of g_2, we get $\mathbf{cf}(\mathbf{c}) = \tau_2$ and $\mathbf{cf}(\mathbf{c}) \in \operatorname{Ker}\big(\overrightarrow{f} - \mathrm{id}\big)$. Then we have

$$\tau_2 - \tau_1 = \mathbf{cf}(\mathbf{c}) - \mathbf{bf}(\mathbf{b}) = \mathbf{cb} - \mathbf{f}(\mathbf{c})\mathbf{f}(\mathbf{b}) = \mathbf{cb} - \overrightarrow{f}(\mathbf{cb}),$$

which shows that

$$\tau_2 - \tau_1 \in \operatorname{Ker}\big(\overrightarrow{f} - \mathrm{id}\big) \cap \operatorname{Im}\big(\overrightarrow{f} - \mathrm{id}\big),$$

and thus that $\tau_2 = \tau_1$, since we have shown that

$$\overrightarrow{E} = \operatorname{Ker}\big(\overrightarrow{f} - \mathrm{id}\big) \oplus \operatorname{Im}\big(\overrightarrow{f} - \mathrm{id}\big).$$

The fact that (a) holds is a consequence of the uniqueness of g and τ, since f and 0 clearly satisfy the required conditions. That (b) holds follows from Lemma 7.5.1 (2), since the affine map f has a unique fixed point iff $E\big(1, \overrightarrow{f}\big) = \operatorname{Ker}\big(\overrightarrow{f} - \mathrm{id}\big) = \{0\}$. $\square$

The determination of x is illustrated in Figure 7.5.

Remarks:

(1) Note that $\operatorname{Ker}\big(\overrightarrow{f} - \mathrm{id}\big) = \{0\}$ iff $\tau = 0$, iff $\operatorname{Fix}(g)$ consists of a single element, which is the unique fixed point of f. However, even if f is not a translation, f may not have any fixed points. For example, this happens when E is the affine Euclidean plane and f is the composition of a reflection about a line composed with a nontrivial translation parallel to this line.

(2) The fact that E has finite dimension is used only to prove (b).

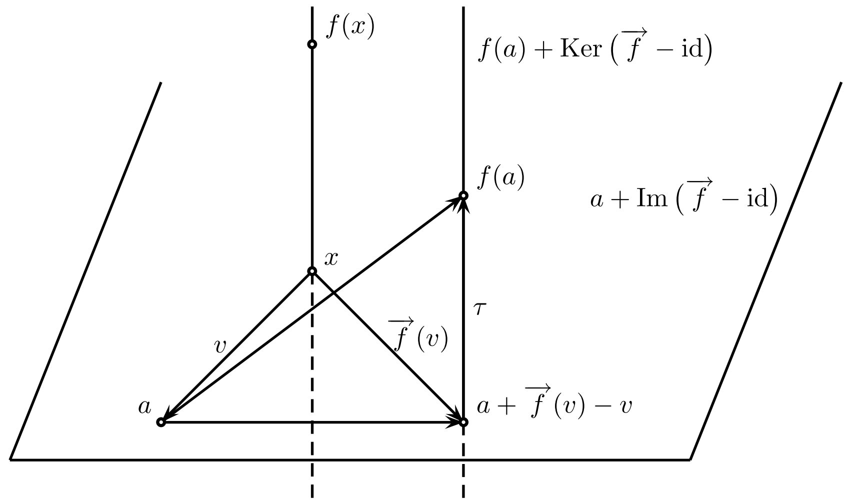

Figure 7.5. Rigid motion as $f = t \circ g$, where g has some fixed point x

(3) It is easily checked that $\mathrm{Fix}(g)$ consists of the set of points x such that $\|\mathbf{xf(x)}\|$ is minimal.

In the affine Euclidean plane it is easy to see that the affine isometries (besides the identity) are classified as follows. An isometry f that has a fixed point is a rotation if it is a direct isometry; otherwise, it is a reflection about a line. If f has no fixed point, then it is either a nontrivial translation or the composition of a reflection about a line with a nontrivial translation parallel to this line.

In an affine space of dimension 3 it is easy to see that the affine isometries (besides the identity) are classified as follows. There are three kinds of isometries that have a fixed point. A proper isometry with a fixed point is a rotation around a line D (its set of fixed points), as illustrated in Figure 7.6.

An improper isometry with a fixed point is either a reflection about a plane H (the set of fixed points) or the composition of a rotation followed by a reflection about a plane H orthogonal to the axis of rotation D, as illustrated in Figures 7.7 and 7.8. In the second case, there is a single fixed point $O = D \cap H$.

There are three types of isometries with no fixed point. The first kind is a nontrivial translation. The second kind is the composition of a rotation followed by a nontrivial translation parallel to the axis of rotation D. Such a rigid motion is proper, and is called a *screw motion*. A screw motion is illustrated in Figure 7.9.

The third kind is the composition of a reflection about a plane followed by a nontrivial translation by a vector parallel to the direction of the plane of the reflection, as illustrated in Figure 7.10.

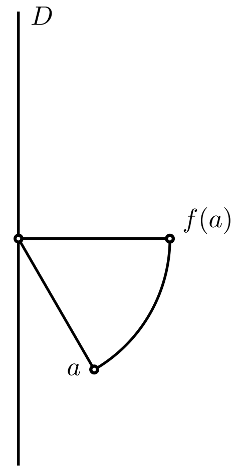

Figure 7.6. 3D proper rigid motion with line D of fixed points (rotation)

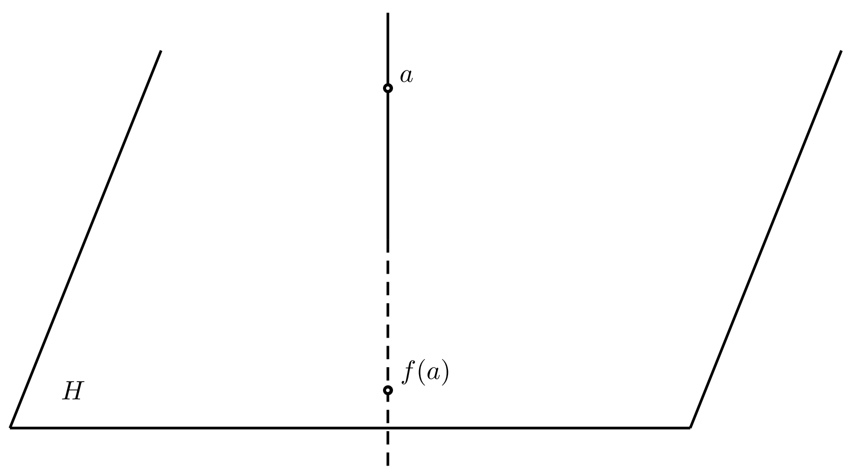

Figure 7.7. 3D improper rigid motion with a plane H of fixed points (reflection)

This last transformation is an improper isometry.

7.7 The Cartan–Dieudonné Theorem for Affine Isometries

The Cartan–Dieudonné theorem also holds for affine isometries, with a small twist due to translations. The reader is referred to Berger [12], Snap-

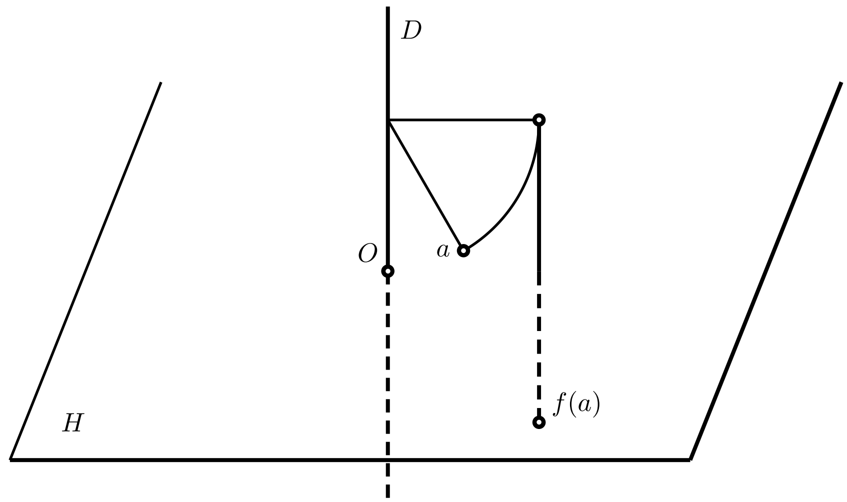

Figure 7.8. $3D$ improper rigid motion with a unique fixed point

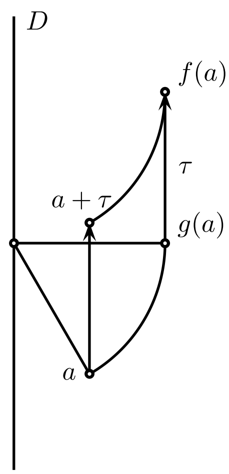

Figure 7.9. 3D proper rigid motion with no fixed point (screw motion)

per and Troyer [160], or Tisseron [169] for a detailed treatment of the Cartan–Dieudonné theorem and its variants.

Theorem 7.7.1 *Let E be an affine Euclidean space of dimension $n \geq 1$. Every isometry $f \in \mathbf{Is}(E)$ that has a fixed point and is not the identity is the composition of at most n reflections. Every isometry $f \in \mathbf{Is}(E)$ that has*

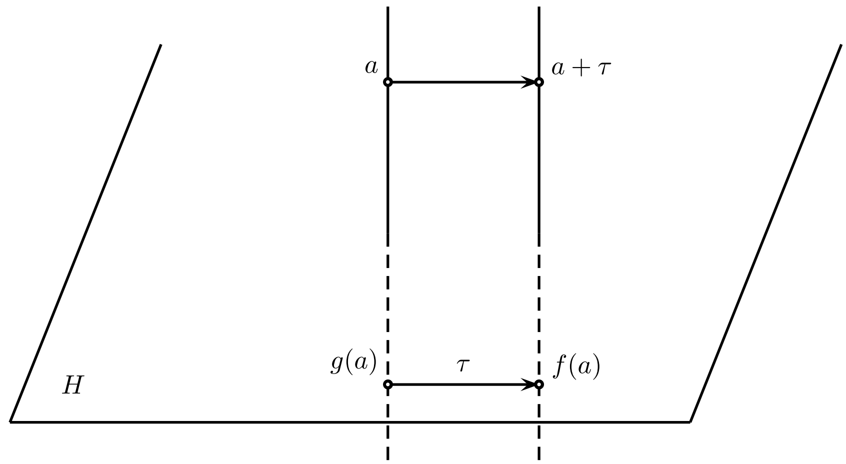

Figure 7.10. 3D improper rigid motion with no fixed points

no fixed point is the composition of at most $n+2$ *reflections. When* $n \geq 2$*, the identity is the composition of any reflection with itself.*

Proof. First, we use Theorem 7.6.2. If f has a fixed point Ω, we choose Ω as an origin and work in the vector space E_Ω. Since f behaves as a linear isometry, the result follows from Theorem 7.2.1. More specifically, we can write $\overrightarrow{f} = \overrightarrow{s_k} \circ \cdots \circ \overrightarrow{s_1}$ for $k \leq n$ hyperplane reflections $\overrightarrow{s_i}$. We define the affine reflections s_i such that

$$s_i(a) = \Omega + \overrightarrow{s_i}(\mathbf{\Omega a})$$

for all $a \in E$, and we note that $f = s_k \circ \cdots \circ s_1$, since

$$f(a) = \Omega + \overrightarrow{s_k} \circ \cdots \circ \overrightarrow{s_1}(\mathbf{\Omega a})$$

for all $a \in E$. If f has no fixed point, then $f = t \circ g$ for some isometry g that has a fixed point Ω and some translation $t = t_\tau$, with $\overrightarrow{f}(\tau) = \tau$. By the argument just given, we can write $g = s_k \circ \cdots \circ s_1$ for some affine reflections (at most n). However, by Lemma 7.6.1, the translation $t = t_\tau$ can be achieved by two reflections about parallel hyperplanes, and thus $f = s_{k+2} \circ \cdots \circ s_1$, for some affine reflections (at most $n+2$). $\square$

When $n \geq 3$, we can also characterize the affine isometries in $\mathbf{SE}(n)$ in terms of flips. Remarkably, not only we can do without translations, but we can even bound the number of flips by n.

Theorem 7.7.2 *Let* E *be a Euclidean affine space of dimension* $n \geq 3$*. Every rigid motion* $f \in \mathbf{SE}(E)$ *is the composition of an even number of flips* $f = f_{2k} \circ \cdots \circ f_1$*, where* $2k \leq n$*.*

Proof. As in the proof of Theorem 7.7.1, we distinguish between the two cases where f has some fixed point or not. If f has a fixed point Ω, we apply Theorem 7.2.5. More specifically, we can write $\overrightarrow{f} = \overrightarrow{f_{2k}} \circ \cdots \circ \overrightarrow{f_1}$ for some flips $\overrightarrow{f_i}$. We define the affine flips f_i such that

$$f_i(a) = \Omega + \overrightarrow{f_i}(\mathbf{\Omega a})$$

for all $a \in E$, and we note that $f = f_{2k} \circ \cdots \circ f_1$, since

$$f(a) = \Omega + \overrightarrow{f_{2k}} \circ \cdots \circ \overrightarrow{f_1}(\mathbf{\Omega a})$$

for all $a \in E$.

If f does not have a fixed point, as in the proof of Theorem 7.7.1, we get

$$f = t_\tau \circ f_{2k} \circ \cdots \circ f_1,$$

for some affine flips f_i. We need to get rid of the translation. However, $\overrightarrow{f}(\tau) = \tau$, and by the second part of Theorem 7.2.5, we can assume that $\tau \in \overrightarrow{F_{2k}}^{\perp}$, where $\overrightarrow{F_{2k}}$ is the direction of the affine subspace defining the affine flip f_{2k}. Finally, appealing to Lemma 7.6.1, since $\tau \in \overrightarrow{F_{2k}}^{\perp}$, the translation t_τ can be expressed as the composition $f'_{2k} \circ f'_{2k-1}$ of two flips f'_{2k-1} and f'_{2k} about the two parallel subspaces $\Omega + \overrightarrow{F_{2k}}$ and $\Omega + \tau/2 + \overrightarrow{F_{2k}}$, whose distance is $\|\tau\|/2$. However, since f'_{2k-1} and f_{2k} are both the identity on $\Omega + \overrightarrow{F_{2k}}$, we must have $f'_{2k-1} = f_{2k}$, and thus

$$\begin{aligned} f &= t_\tau \circ f_{2k} \circ f_{2k-1} \circ \cdots \circ f_1 \\ &= f'_{2k} \circ f'_{2k-1} \circ f_{2k} \circ f_{2k-1} \circ \cdots \circ f_1 \\ &= f'_{2k} \circ f_{2k-1} \circ \cdots \circ f_1, \end{aligned}$$

since $f'_{2k-1} = f_{2k}$ and $f'_{2k-1} \circ f_{2k} = f_{2k} \circ f_{2k} = \mathrm{id}$, since f_{2k} is a symmetry.
□

Remark: It is easy to prove that if f is a screw motion in $\mathbf{SE}(3)$, D its axis, θ is its angle of rotation, and τ the translation along the direction of D, then f is the composition of two flips about lines D_1 and D_2 orthogonal to D, at a distance $\|\tau\|/2$ and making an angle $\theta/2$.

There is one more topic that we would like to cover, since it is often useful in practice: The concept of *cross product of vectors*, also called vector product. But first, we need to discuss the question of orientation of bases.

7.8 Orientations of a Euclidean Space, Angles

In this section we return to vector spaces. In order to deal with the notion of orientation correctly, it is important to assume that every family $(u_1, \ldots, u_n)$ of vectors is ordered (by the natural ordering on $\{1, 2, \ldots, n\}$). Thus, we will assume that all families $(u_1, \ldots, u_n)$ of vectors, in particular bases and orthonormal bases, are ordered.

Let E be a vector space of finite dimension n over $\mathbb{R}$, and let $(u_1, \ldots, u_n)$ and $(v_1, \ldots, v_n)$ be any two bases for E. Recall that the change of basis matrix from $(u_1, \ldots, u_n)$ to $(v_1, \ldots, v_n)$ is the matrix P whose columns are the coordinates of the vectors v_j over the basis $(u_1, \ldots, u_n)$. It is immediately verified that the set of alternating n-linear forms on E is a vector space, which we denote by $\Lambda(E)$ (see Lang [107]).

We now show that $\Lambda(E)$ has dimension 1. For any alternating n-linear form $\varphi: E \times \cdots \times E \to K$ and any two sequences of vectors $(u_1, \ldots, u_n)$ and $(v_1, \ldots, v_n)$, if

$$(v_1, \ldots, v_n) = (u_1, \ldots, u_n)P,$$

then

$$\varphi(v_1, \ldots, v_n) = \det(P)\varphi(u_1, \ldots, u_n).$$

In particular, if we consider nonnull alternating n-linear forms $\varphi: E \times \cdots \times E \to K$, we must have $\varphi(u_1, \ldots, u_n) \neq 0$ for every basis $(u_1, \ldots, u_n)$. Since for any two alternating n-linear forms φ and ψ we have

$$\varphi(v_1, \ldots, v_n) = \det(P)\varphi(u_1, \ldots, u_n)$$

and

$$\psi(v_1, \ldots, v_n) = \det(P)\psi(u_1, \ldots, u_n),$$

we get

$$\varphi(u_1, \ldots, u_n)\psi(v_1, \ldots, v_n) - \psi(u_1, \ldots, u_n)\varphi(v_1, \ldots, v_n) = 0.$$

Fixing $(u_1, \ldots, u_n)$ and letting $(v_1, \ldots, v_n)$ vary, this shows that φ and ψ are linearly dependent, and since $\Lambda(E)$ is nontrivial, it has dimension 1.

We now define an equivalence relation on $\Lambda(E) - \{0\}$ (where we let 0 denote the null alternating n-linear form):

φ and ψ are equivalent if $\psi = \lambda\varphi$ for some $\lambda > 0$.

It is immediately verified that the above relation is an equivalence relation. Furthermore, it has exactly two equivalence classes O_1 and O_2.

The first way of defining an *orientation of E* is to pick one of these two equivalence classes, say O ($O \in \{O_1, O_2\}$). Given such a choice of a class O, we say that a basis $(w_1, \ldots, w_n)$ has *positive orientation* iff

$\varphi(w_1, \ldots, w_n) > 0$ for any alternating n-linear form $\varphi \in O$. Note that this makes sense, since for any other $\psi \in O$, $\varphi = \lambda\psi$ for some $\lambda > 0$.

According to the previous definition, two bases $(u_1, \ldots, u_n)$ and $(v_1, \ldots, v_n)$ have the same orientation iff $\varphi(u_1, \ldots, u_n)$ and $\varphi(v_1, \ldots, v_n)$ have the same sign for all $\varphi \in \Lambda(E) - \{0\}$. From

$$\varphi(v_1, \ldots, v_n) = \det(P)\varphi(u_1, \ldots, u_n)$$

we must have $\det(P) > 0$. Conversely, if $\det(P) > 0$, the same argument shows that $(u_1, \ldots, u_n)$ and $(v_1, \ldots, v_n)$ have the same orientation. This leads us to an equivalent and slightly less contorted definition of the notion of orientation. We define a relation between bases of E as follows: Two bases $(u_1, \ldots, u_n)$ and $(v_1, \ldots, v_n)$ are related if $\det(P) > 0$, where P is the change of basis matrix from $(u_1, \ldots, u_n)$ to $(v_1, \ldots, v_n)$.

Since $\det(PQ) = \det(P)\det(Q)$, and since change of basis matrices are invertible, the relation just defined is indeed an equivalence relation, and it has two equivalence classes. Furthermore, from the discussion above, any nonnull alternating n-linear form φ will have the same sign on any two equivalent bases.

The above discussion motivates the following definition.

Definition 7.8.1 Given any vector space E of finite dimension over $\mathbb{R}$, we define an *orientation of* E as the choice of one of the two equivalence classes of the equivalence relation on the set of bases defined such that $(u_1, \ldots, u_n)$ and $(v_1, \ldots, v_n)$ have the same orientation iff $\det(P) > 0$, where P is the change of basis matrix from $(u_1, \ldots, u_n)$ to $(v_1, \ldots, v_n)$. A basis in the chosen class is said to have *positive orientation, or to be positive*. An *orientation of a Euclidean affine space* E is an orientation of its underlying vector space $\overrightarrow{E}$.

In practice, to give an orientation, one simply picks a fixed basis considered as having positive orientation. The orientation of every other basis is determined by the sign of the determinant of the change of basis matrix.

Having the notation of orientation at hand, we wish to go back briefly to the concept of (oriented) angle. Let E be a Euclidean space of dimension $n = 2$, and assume a given orientation. In any given positive orthonormal basis for E, every rotation r is represented by a matrix

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

Actually, we claim that the matrix R representing the rotation r is the same in *all* orthonormal positive bases. This is because the change of basis matrix from one positive orthonormal basis to another positive orthonormal basis is a rotation represented by some matrix of the form

$$P = \begin{pmatrix} \cos\psi & -\sin\psi \\ \sin\psi & \cos\psi \end{pmatrix}$$

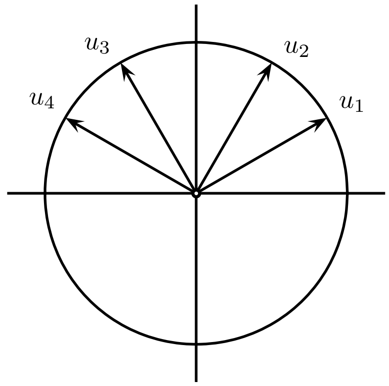

Figure 7.11. Defining angles

and that we have

$$P^{-1} = \begin{pmatrix} \cos(-\psi) & -\sin(-\psi) \\ \sin(-\psi) & \cos(-\psi) \end{pmatrix},$$

and after calculations, we find that PRP^{-1} is the rotation matrix associated with $\psi + \theta - \psi = \theta$. We can choose $\theta \in [0, 2\pi[$, and we call θ the *measure of the angle of rotation of* r *(and* R*)*. If the orientation is changed, the measure changes to $2\pi - \theta$.

We now let E be a Euclidean space of dimension $n = 2$, but we do not assume any orientation. It is easy to see that given any two unit vectors $u_1, u_2 \in E$ (unit means that $\|u_1\| = \|u_2\| = 1$), there is a unique rotation r such that

$$r(u_1) = u_2.$$

It is also possible to define an equivalence relation of pairs of unit vectors such that

$$\langle u_1, u_2 \rangle \equiv \langle u_3, u_4 \rangle$$

iff there is some rotation r such that $r(u_1) = u_3$ and $r(u_2) = u_4$.

Then the equivalence class of $\langle u_1, u_2 \rangle$ can be taken as the definition of the (oriented) *angle of* $\langle u_1, u_2 \rangle$, which is denoted by $\widehat{u_1 u_2}$.

Furthermore, it can be shown that there is a rotation mapping the pair $\langle u_1, u_2 \rangle$ to the pair $\langle u_3, u_4 \rangle$ iff there is a rotation mapping the pair $\langle u_1, u_3 \rangle$ to the pair $\langle u_2, u_4 \rangle$ (all vectors being unit vectors), as illustrated in Figure 7.11.

As a consequence of all this, since for any pair $\langle u_1, u_2 \rangle$ of unit vectors there is a unique rotation r mapping u_1 to u_2, the angle $\widehat{u_1 u_2}$ of $\langle u_1, u_2 \rangle$ corresponds bijectively to the rotation r, and there is a bijection between the set of angles of pairs of unit vectors and the set of rotations in the plane. As a matter of fact, the set of angles forms an abelian group isomorphic to the (abelian) group of rotations in the plane.

Thus, even though we can consider angles as oriented, note that the notion of orientation is not necessary to define angles. However, to define the *measure of an angle*, the notion of orientation is needed.

If we now assume that an orientation of E (still a Euclidean plane) is given, the unique rotation r associated with an angle $\widehat{u_1 u_2}$ corresponds to a unique matrix

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

The number θ is defined up to $2k\pi$ (with $k \in \mathbb{Z}$) and is called a *measure of the angle* $\widehat{u_1 u_2}$. There is a unique $\theta \in [0, 2\pi[$ that is a measure of the angle $\widehat{u_1 u_2}$. It is also immediately seen that

$$\cos\theta = u_1 \cdot u_2.$$

In fact, since $\cos\theta = \cos(2\pi - \theta) = \cos(-\theta)$, the quantity $\cos\theta$ does not depend on the orientation.

Now, still considering a Euclidean plane, given any pair $\langle u_1, u_2 \rangle$ of nonnull vectors, we define their angle as the angle of the unit vectors $u_1/\|u_1\|$ and $u_2/\|u_2\|$, and if E is oriented, we define the *measure* θ of this angle as the measure of the angle of these unit vectors. Note that

$$\cos\theta = \frac{u_1 \cdot u_2}{\|u_1\|\|u_2\|},$$

and this independently of the orientation.

Finally, if E is a Euclidean space of dimension $n \geq 2$, we define the angle of a pair $\langle u_1, u_2 \rangle$ of nonnull vectors as the angle of this pair in the Euclidean plane spanned by $\langle u_1, u_2 \rangle$ if they are linearly independent, or any Euclidean plane containing u_1 if they are collinear.

If E is a Euclidean affine space of dimension $n \geq 2$, for any two pairs $\langle a_1, b_1 \rangle$ and $\langle a_2, b_2 \rangle$ of points in E, where $a_1 \neq b_1$ and $a_2 \neq b_2$, we define the angle of the pair $\langle \langle a_1, b_1 \rangle, \langle a_2, b_2 \rangle \rangle$ as the angle of the pair $\langle \mathbf{a_1 b_1}, \mathbf{a_2 b_2} \rangle$.

As for the issue of measure of an angle when $n \geq 3$, all we can do is to define the measure of the angle $\widehat{u_1 u_2}$ as either θ or $2\pi - \theta$, where $\theta \in [0, 2\pi[$. For a detailed treatment, see Berger [12] or Cagnac, Ramis, and Commeau [25]. In particular, when $n = 3$, one should note that it is not enough to give a line D through the origin (the axis of rotation) and an angle θ to specify a rotation! The problem is that depending on the orientation of the plane H (through the origin) orthogonal to D, we get two different rotations: one of angle θ, the other of angle $2\pi - \theta$. Thus, to specify a rotation, we also need to give an orientation of the plane orthogonal to the axis of rotation. This can be done by specifying an orientation of the axis of rotation by some unit vector ω, and chosing the basis (e_1, e_2, ω) (where (e_1, e_2) is a basis of H) such that it has positive orientation w.r.t. the chosen orientation of E.

We now return to alternating multilinear forms on a Euclidean space.

When E is a Euclidean space, we have an interesting situation regarding the value of determinants over orthornormal bases described by the following lemma. Given any basis $B = (u_1, \ldots, u_n)$ for E, for any sequence $(w_1, \ldots, w_n)$ of n vectors, we denote by $\det_B(w_1, \ldots, w_n)$ the determinant of the matrix whose columns are the coordinates of the w_j over the basis $B = (u_1, \ldots, u_n)$.

Lemma 7.8.2 *Let E be a Euclidean space of dimension n, and assume that an orientation of E has been chosen. For any sequence $(w_1, \ldots, w_n)$ of n vectors and any two orthonormal bases $B_1 = (u_1, \ldots, u_n)$ and $B_2 = (v_1, \ldots, v_n)$ of positive orientation, we have*

$$\det_{B_1}(w_1, \ldots, w_n) = \det_{B_2}(w_1, \ldots, w_n).$$

Proof. Let P be the change of basis matrix from $B_1 = (u_1, \ldots, u_n)$ to $B_2 = (v_1, \ldots, v_n)$. Since $B_1 = (u_1, \ldots, u_n)$ and $B_2 = (v_1, \ldots, v_n)$ are orthonormal, P is orthogonal, and we must have $\det(P) = +1$, since the bases have positive orientation. Let U_1 be the matrix whose columns are the coordinates of the w_j over the basis $B_1 = (u_1, \ldots, u_n)$, and let U_2 be the matrix whose columns are the coordinates of the w_j over the basis $B_2 = (v_1, \ldots, v_n)$. Then, by definition of P, we have

$$(w_1, \ldots, w_n) = (u_1, \ldots, u_n)U_2P,$$

that is,

$$U_1 = U_2P.$$

Then, we have

$$\begin{aligned}\det_{B_1}(w_1, \ldots, w_n) &= \det(U_1) = \det(U_2P) = \det(U_2)\det(P)\\ &= \det_{B_2}(w_1, \ldots, w_n)\det(P) = \det_{B_2}(w_1, \ldots, w_n),\end{aligned}$$

since $\det(P) = +1$. $\square$

By Lemma 7.8.2, the determinant $\det_B(w_1, \ldots, w_n)$ is independent of the base B, provided that B is orthonormal and of positive orientation. Thus, Lemma 7.8.2 suggests the following definition.

7.9 Volume Forms, Cross Products

In this section we generalize the familiar notion of cross product of vectors in $\mathbb{R}^3$ to Euclidean spaces of any finite dimension. First, we define the mixed product, or volume form.

Definition 7.9.1 Given any Euclidean space E of finite dimension n over $\mathbb{R}$ and any orientation of E, for any sequence $(w_1, \ldots, w_n)$ of n vectors in E, the common value $\lambda_E(w_1, \ldots, w_n)$ of the determinant $\det_B(w_1, \ldots, w_n)$

over all positive orthonormal bases B of E is called the *mixed product (or volume form) of* $(w_1, \ldots, w_n)$.

The mixed product $\lambda_E(w_1, \ldots, w_n)$ will also be denoted by $(w_1, \ldots, w_n)$, even though the notation is overloaded. The following properties hold.

- The mixed product $\lambda_E(w_1, \ldots, w_n)$ changes sign when the orientation changes.
- The mixed product $\lambda_E(w_1, \ldots, w_n)$ is a scalar, and Definition 7.9.1 really defines an alternating multilinear form from E^n to $\mathbb{R}$.
- $\lambda_E(w_1, \ldots, w_n) = 0$ iff $(w_1, \ldots, w_n)$ is linearly dependent.
- A basis $(u_1, \ldots, u_n)$ is positive or negative iff $\lambda_E(u_1, \ldots, u_n)$ is positive or negative.
- $\lambda_E(w_1, \ldots, w_n)$ is invariant under every isometry f such that $\det(f) = 1$.

The terminology "volume form" is justified because $\lambda_E(w_1, \ldots, w_n)$ is indeed the volume of some geometric object. Indeed, viewing E as an affine space, the *parallelotope defined by* $(w_1, \ldots, w_n)$ is the set of points

$$\{\lambda_1 w_1 + \cdots + \lambda_n w_n \mid 0 \leq \lambda_i \leq 1,\ 1 \leq i \leq n\}.$$

Then, it can be shown (see Berger [12], Section 9.12) that the volume of the parallelotope defined by $(w_1, \ldots, w_n)$ is indeed $\lambda_E(w_1, \ldots, w_n)$. If $(E, \overrightarrow{E})$ is a Euclidean affine space of dimension n, given any $n+1$ affinely independent points $(a_0, \ldots, a_n)$, the set

$$\{a_0 + \lambda_1 \mathbf{a_0a_1} + \cdots + \lambda_n \mathbf{a_0a_n} \mid \text{where } 0 \leq \lambda_i \leq 1,\ 1 \leq i \leq n\}$$

is called the *parallelotope spanned by* $(a_0, \ldots, a_n)$. Then the volume of the parallelotope spanned by $(a_0, \ldots, a_n)$ is $\lambda_{\overrightarrow{E}}(\mathbf{a_0a_1}, \ldots, \mathbf{a_0a_n})$. It can also be shown that the volume $\mathrm{vol}(a_0, \ldots, a_n)$ of the n-simplex $(a_0, \ldots, a_n)$ is

$$\mathrm{vol}(a_0, \ldots, a_n) = \frac{1}{n!} \lambda_{\overrightarrow{E}}(\mathbf{a_0a_1}, \ldots, \mathbf{a_0a_n}).$$

Now, given a sequence $(w_1, \ldots, w_{n-1})$ of $n-1$ vectors in E, the map

$$x \mapsto \lambda_E(w_1, \ldots, w_{n-1}, x)$$

is a linear form. Thus, by Lemma 6.2.4, there is a unique vector $u \in E$ such that

$$\lambda_E(w_1, \ldots, w_{n-1}, x) = u \cdot x$$

for all $x \in E$. The vector u has some interesting properties that motivate the next definition.

Definition 7.9.2 Given any Euclidean space E of finite dimension n over $\mathbb{R}$, for any orientation of E and any sequence $(w_1, \ldots, w_{n-1})$ of $n-1$ vectors in E, the unique vector $w_1 \times \cdots \times w_{n-1}$ such that

$$\lambda_E(w_1, \ldots, w_{n-1}, x) = w_1 \times \cdots \times w_{n-1} \cdot x$$

for all $x \in E$ is the *cross product, or vector product, of* $(w_1, \ldots, w_{n-1})$.

The following properties hold.

- The cross product $w_1 \times \cdots \times w_{n-1}$ changes sign when the orientation changes.
- The cross product $w_1 \times \cdots \times w_{n-1}$ is a vector, and Definition 7.9.2 really defines an alternating multilinear map from E^{n-1} to E.
- $w_1 \times \cdots \times w_{n-1} = 0$ iff $(w_1, \ldots, w_{n-1})$ is linearly dependent. This is because
$$w_1 \times \cdots \times w_{n-1} = 0$$
iff
$$\lambda_E(w_1, \ldots, w_{n-1}, x) = 0$$
for all $x \in E$, and thus if $(w_1, \ldots, w_{n-1})$ were linearly independent, we could find a vector $x \in E$ to complete $(w_1, \ldots, w_{n-1})$ into a basis of E, and we would have
$$\lambda_E(w_1, \ldots, w_{n-1}, x) \neq 0.$$
- The cross product $w_1 \times \cdots \times w_{n-1}$ is orthogonal to each of the w_j.
- If $(w_1, \ldots, w_{n-1})$ is linearly independent, then the sequence
$$(w_1, \ldots, w_{n-1}, w_1 \times \cdots \times w_{n-1})$$
is a positive basis of E.

We now show how to compute the coordinates of $u_1 \times \cdots \times u_{n-1}$ over an orthonormal basis.

Given an orthonormal basis $(e_1, \ldots, e_n)$, for any sequence $(u_1, \ldots, u_{n-1})$ of $n-1$ vectors in E, if

$$u_j = \sum_{i=1}^{n} u_{i,j} e_i,$$

where $1 \leq j \leq n-1$, for any $x = x_1 e_1 + \cdots + x_n e_n$, consider the determinant

$$\lambda_E(u_1, \ldots, u_{n-1}, x) = \begin{vmatrix} u_{1\,1} & \ldots & u_{1\,n-1} & x_1 \\ u_{2\,1} & \ldots & u_{2\,n-1} & x_2 \\ \vdots & \vdots & \ddots & \vdots \\ u_{n\,1} & \ldots & u_{n\,n-1} & x_n \end{vmatrix}.$$

Calling the underlying matrix above A, we can expand $\det(A)$ according to the last column, using the Laplace formula (see Strang [166]), where $A_{i\,j}$ is the $(n-1)\times(n-1)$ matrix obtained from A by deleting row i and column j, and we get

$$\begin{vmatrix} u_{1\,1} & \dots & u_{1\,n-1} & x_1 \\ u_{2\,1} & \dots & u_{2\,n-1} & x_2 \\ \vdots & \vdots & \ddots & \vdots \\ u_{n\,1} & \dots & u_{n\,n-1} & x_n \end{vmatrix} = (-1)^{n+1} x_1 \det(A_{1\,n}) + \cdots + x_n \det(A_{n\,n}).$$

Each $(-1)^{i+n}\det(A_{i\,n})$ is called the *cofactor of* x_i. We note that $\det(A)$ is in fact the inner product

$$\det(A) = ((-1)^{n+1}\det(A_{1\,n})e_1 + \cdots + (-1)^{n+n}\det(A_{n\,n})e_n)\cdot x.$$

Since the cross product $u_1 \times \cdots \times u_{n-1}$ is the unique vector u such that

$$u \cdot x = \lambda_E(u_1, \ldots, u_{n-1}, x),$$

for all $x \in E$, the coordinates of the cross product $u_1 \times \cdots \times u_{n-1}$ must be

$$((-1)^{n+1}\det(A_{1\,n}), \ldots, (-1)^{n+n}\det(A_{n\,n})),$$

the sequence of cofactors of the x_i in the determinant $\det(A)$.

For example, when $n = 3$, the coordinates of the cross product $u \times v$ are given by the cofactors of x_1, x_2, x_3, in the determinant

$$\begin{vmatrix} u_1 & v_1 & x_1 \\ u_2 & v_2 & x_2 \\ u_3 & v_3 & x_3 \end{vmatrix},$$

or, more explicitly, by

$$(-1)^{3+1}\begin{vmatrix} u_2 & v_2 \\ u_3 & v_3 \end{vmatrix}, \qquad (-1)^{3+2}\begin{vmatrix} u_1 & v_1 \\ u_3 & v_3 \end{vmatrix}, \qquad (-1)^{3+3}\begin{vmatrix} u_1 & v_1 \\ u_2 & v_2 \end{vmatrix},$$

that is,

$$(u_2v_3 - u_3v_2,\; u_3v_1 - u_1v_3,\; u_1v_2 - u_2v_1).$$

It is also useful to observe that if we let U be the matrix

$$U = \begin{pmatrix} 0 & -u_3 & u_2 \\ u_3 & 0 & -u_1 \\ -u_2 & u_1 & 0 \end{pmatrix},$$

then the coordinates of the cross product $u \times v$ are given by

$$\begin{pmatrix} 0 & -u_3 & u_2 \\ u_3 & 0 & -u_1 \\ -u_2 & u_1 & 0 \end{pmatrix}\begin{pmatrix} v_1 \\ v_2 \\ v_3 \end{pmatrix} = \begin{pmatrix} u_2v_3 - u_3v_2 \\ u_3v_1 - u_1v_3 \\ u_1v_2 - u_2v_1 \end{pmatrix}.$$

We finish our discussion of cross products by mentioning without proof a few more of their properties, in the case $n = 3$. Firstly, the following so-called *Lagrange identity* holds:

$$(u \cdot v)^2 + \|u \times v\|^2 = \|u\|^2 \|v\|^2.$$

If u and v are linearly independent, and if θ (or $2\pi - \theta$) is a measure of the angle $\widehat{uv}$, then

$$|\sin\theta| = \frac{\|u \times v\|}{\|u\|\|v\|}.$$

It can also be shown that $u \times v$ is the only vector w such that the following properties hold:

(1) $w \cdot u = 0$, and $w \cdot v = 0$.

(2) $\lambda_E(u, v, w) \geq 0$.

(3) $(u \cdot v)^2 + \|w\|^2 = \|u\|^2 \|v\|^2$.

Recall that the mixed product $\lambda_E(w_1, w_1, w_3)$ is also denoted by (w_1, w_2, w_3), and that

$$w_1 \cdot (w_2 \times w_3) = (w_1, w_2, w_3).$$

7.10 Problems

Problem 7.1 Prove Lemma 7.4.2.

Problem 7.2 This problem is a warm-up for the next problem. Consider the set of matrices of the form

$$\begin{pmatrix} 0 & -a \\ a & 0 \end{pmatrix},$$

where $a \in \mathbb{R}$.

(a) Show that these matrices are invertible when $a \neq 0$ (give the inverse explicitly). Given any two such matrices A, B, show that $AB = BA$. Describe geometrically the action of such a matrix on points in the affine plane $\mathbb{A}^2$, with its usual Euclidean inner product. Verify that this set of matrices is a vector space isomorphic to $(\mathbb{R}, +)$. This vector space is denoted by $\mathfrak{so}(2)$.

(b) Given an $n \times n$ matrix A, we define the *exponential* e^A as

$$e^A = I_n + \sum_{k \geq 1} \frac{A^k}{k!},$$

where I_n denotes the $n \times n$ identity matrix. It can be shown rigorously that this power series is indeed convergent for every A (over $\mathbb{R}$ or $\mathbb{C}$), so that e^A makes sense (and you do not have to prove it!).

Given any matrix

$$A = \begin{pmatrix} 0 & -\theta \\ \theta & 0 \end{pmatrix},$$

prove that

$$e^A = \cos\theta \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} + \sin\theta \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{pmatrix}.$$

Hint. Check that

$$\begin{pmatrix} 0 & -\theta \\ \theta & 0 \end{pmatrix} = \theta \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \quad \text{and} \quad \begin{pmatrix} 0 & -\theta \\ \theta & 0 \end{pmatrix}^2 = -\theta^2 \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix},$$

and use the power series for $\cos\theta$ and $\sin\theta$. Conclude that the exponential map provides a surjective map $\exp\colon \mathfrak{so}(2) \to \mathbf{SO}(2)$ from $\mathfrak{so}(2)$ onto the group $\mathbf{SO}(2)$ of plane rotations. Is this map injective? How do you need to restrict θ to get an injective map?

Remark: By the way, $\mathfrak{so}(2)$ is the *Lie algebra* of the (Lie) group $\mathbf{SO}(2)$.

(c) Consider the set $\mathbf{U}(1)$ of complex numbers of the form $\cos\theta + i\sin\theta$. Check that this is a group under multiplication. Assuming that we use the standard affine frame for the affine plane $\mathbb{A}^2$, every point (x, y) corresponds to the complex number $z = x + iy$, and this correspondence is a bijection. Then, every $\alpha = \cos\theta + i\sin\theta \in \mathbf{U}(1)$ induces the map $R_\alpha\colon \mathbb{A}^2 \to \mathbb{A}^2$ defined such that

$$R_\alpha(z) = \alpha z.$$

Prove that R_α is the rotation of matrix

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

Prove that the map $R\colon \mathbf{U}(1) \to \mathbf{SO}(2)$ defined such that $R(\alpha) = R_\alpha$ is an isomorphism. Deduce that topologically, $\mathbf{SO}(2)$ is a circle. Using the exponential map from $\mathbb{R}$ to $\mathbf{U}(1)$ defined such that $\theta \mapsto e^{i\theta} = \cos\theta + i\sin\theta$, prove that there is a surjective homomorphism from $(R, +)$ to $\mathbf{SO}(2)$. What is the connection with the exponential map from $\mathfrak{so}(2)$ to $\mathbf{SO}(2)$?

Problem 7.3 (a) Recall that the coordinates of the cross product $u \times v$ of two vectors $u = (u_1, u_2, u_3)$ and $v = (v_1, v_2, v_3)$ in $\mathbb{R}^3$ are

$$(u_2v_3 - u_3v_2,\ u_3v_1 - u_1v_3,\ u_1v_2 - u_2v_1).$$

Letting U be the matrix

$$U = \begin{pmatrix} 0 & -u_3 & u_2 \\ u_3 & 0 & -u_1 \\ -u_2 & u_1 & 0 \end{pmatrix},$$

check that the coordinates of the cross product $u \times v$ are given by

$$\begin{pmatrix} 0 & -u_3 & u_2 \\ u_3 & 0 & -u_1 \\ -u_2 & u_1 & 0 \end{pmatrix} \begin{pmatrix} v_1 \\ v_2 \\ v_3 \end{pmatrix} = \begin{pmatrix} u_2v_3 - u_3v_2 \\ u_3v_1 - u_1v_3 \\ u_1v_2 - u_2v_1 \end{pmatrix}.$$

(b) Show that the set of matrices of the form

$$U = \begin{pmatrix} 0 & -u_3 & u_2 \\ u_3 & 0 & -u_1 \\ -u_2 & u_1 & 0 \end{pmatrix}$$

is a vector space isomorphic to $(\mathbb{R}^3 +)$. This vector space is denoted by $\mathfrak{so}(3)$. Show that such matrices are never invertible. Find the kernel of the linear map associated with a matrix U. Describe geometrically the action of the linear map defined by a matrix U. Show that when restricted to the plane orthogonal to $u = (u_1, u_2, u_3)$ through the origin, it is a rotation by $\pi/2$.

(c) Consider the map $\psi\colon (\mathbb{R}^3, \times) \to \mathfrak{so}(3)$ defined by the formula

$$\psi(u_1, u_2, u_3) = \begin{pmatrix} 0 & -u_3 & u_2 \\ u_3 & 0 & -u_1 \\ -u_2 & u_1 & 0 \end{pmatrix}.$$

For any two matrices $A, B \in \mathfrak{so}(3)$, defining $[A,\, B]$ as

$$[A,\, B] = AB - BA,$$

verify that

$$\psi(u \times v) = [\psi(u),\, \psi(v)].$$

Show that $[-,\, -]$ is not associative. Show that $[A,\, A] = 0$, and that the so-called *Jacobi identity* holds:

$$[A,\, [B,\, C]] + [C,\, [A,\, B]] + [B,\, [C,\, A]] = 0.$$

Show that $[A\, B]$ is bilinear (linear in both A and B).

Remark: $[A,\, B]$ is called a *Lie bracket*, and under this operation, the vector space $\mathfrak{so}(3)$ is called a *Lie algebra*. In fact, it is the Lie algebra of the (Lie) group $\mathbf{SO}(3)$.

(d) For any matrix

$$A = \begin{pmatrix} 0 & -c & b \\ c & 0 & -a \\ -b & a & 0 \end{pmatrix},$$

letting $\theta = \sqrt{a^2 + b^2 + c^2}$ and

$$B = \begin{pmatrix} a^2 & ab & ac \\ ab & b^2 & bc \\ ac & bc & c^2 \end{pmatrix},$$

prove that

$$\begin{aligned} A^2 &= -\theta^2 I + B, \\ AB &= BA = 0. \end{aligned}$$

From the above, deduce that

$$A^3 = -\theta^2 A,$$

and for any $k \geq 0$,

$$\begin{aligned} A^{4k+1} &= \theta^{4k} A, \\ A^{4k+2} &= \theta^{4k} A^2, \\ A^{4k+3} &= -\theta^{4k+2} A, \\ A^{4k+4} &= -\theta^{4k+2} A^2. \end{aligned}$$

Then prove that the exponential map $\exp\colon \mathfrak{so}(3) \to \mathbf{SO}(3)$ is given by

$$\exp A = e^A = \cos\theta\, I_3 + \frac{\sin\theta}{\theta} A + \frac{(1 - \cos\theta)}{\theta^2} B,$$

or, equivalently, by

$$e^A = I_3 + \frac{\sin\theta}{\theta} A + \frac{(1 - \cos\theta)}{\theta^2} A^2,$$

if $\theta \neq k2\pi$ $(k \in \mathbb{Z})$, with $\exp(0_3) = I_3$.

Remark: This formula is known as Rodrigues's formula (1840).

(e) Prove that $\exp A$ is a rotation of axis (a, b, c) and of angle $\theta = \sqrt{a^2 + b^2 + c^2}$.
Hint. Check that e^A is an orthogonal matrix of determinant $+1$, etc., or look up any textbook on kinematics or classical dynamics!

(f) Prove that the exponential map $\exp\colon \mathfrak{so}(3) \to \mathbf{SO}(3)$ is surjective. Prove that if R is a rotation matrix different from I_3, letting $\omega = (a, b, c)$ be a unit vector defining the axis of rotation, if $\operatorname{tr}(R) = -1$, then

$$(\exp(R))^{-1} = \left\{ \pm\pi \begin{pmatrix} 0 & -c & b \\ c & 0 & -a \\ -b & a & 0 \end{pmatrix} \right\},$$

and if $\operatorname{tr}(R) \neq -1$, then

$$(\exp(R))^{-1} = \left\{ \frac{\theta}{2\sin\theta}(R - R^T) \;\middle|\; 1 + 2\cos\theta = \operatorname{tr}(R) \right\}.$$

(Recall that $\mathrm{tr}(R) = r_{1\,1} + r_{2\,2} + r_{3\,3}$, the *trace* of the matrix R). Note that both θ and $2\pi - \theta$ yield the same matrix $\exp(R)$.

Problem 7.4 Prove that for any plane isometry f such that $\overrightarrow{f}$ is a reflection, f is the composition of a reflection about a line with a translation (possibly null) parallel to this line.

Problem 7.5 (1) Given a unit vector $(-\sin\theta, \cos\theta)$, prove that the Householder matrix determined by the vector $(-\sin\theta, \cos\theta)$ is

$$\begin{pmatrix} \cos 2\theta & \sin 2\theta \\ \sin 2\theta & -\cos 2\theta \end{pmatrix}.$$

Give a geometric interpretation (i.e., why the choice $(-\sin\theta, \cos\theta)$?).

(2) Given any matrix

$$A = \begin{pmatrix} a & b \\ c & d \end{pmatrix},$$

prove that there is a Householder matrix H such that AH is lower triangular, i.e.,

$$AH = \begin{pmatrix} a' & 0 \\ c' & d' \end{pmatrix}$$

for some $a', c', d' \in \mathbb{R}$.

Problem 7.6 Given a Euclidean space E of dimension n, if h is a reflection about some hyperplane orthogonal to a nonnull vector u and f is any isometry, prove that $f \circ h \circ f^{-1}$ is the reflection about the hyperplane orthogonal to $f(u)$.

Problem 7.7 Let E be a Euclidean space of dimension $n = 2$. Prove that given any two unit vectors $u_1, u_2 \in E$ (unit means that $\|u_1\| = \|u_2\| = 1$), there is a unique rotation r such that

$$r(u_1) = u_2.$$

Prove that there is a rotation mapping the pair $\langle u_1, u_2 \rangle$ to the pair $\langle u_3, u_4 \rangle$ iff there is a rotation mapping the pair $\langle u_1, u_3 \rangle$ to the pair $\langle u_2, u_4 \rangle$ (all vectors being unit vectors).

Problem 7.8 (1) Recall that

$$\det(v_1, \ldots, v_n) = \begin{vmatrix} v_{1\,1} & v_{1\,2} & \ldots & v_{1\,n} \\ v_{2\,1} & v_{2\,2} & \ldots & v_{2\,n} \\ \vdots & \vdots & \ddots & \vdots \\ v_{n\,1} & v_{n\,2} & \ldots & v_{n\,n} \end{vmatrix},$$

where v_i has coordinates $(v_{i\,1}, \ldots, v_{i\,n})$ with respect to a basis $(e_1, \ldots, e_n)$. Prove that the volume of the parallelotope spanned by $(a_0, \ldots, a_n)$ is given by

$$\lambda_E(a_0, \ldots, a_n) = (-1)^n \begin{vmatrix} a_{0\,1} & a_{0\,2} & \ldots & a_{0\,n} & 1 \\ a_{1\,1} & a_{1\,2} & \ldots & a_{1\,n} & 1 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ a_{n\,1} & a_{n\,2} & \ldots & a_{n\,n} & 1 \end{vmatrix},$$

and letting $\lambda_E(a_0, \ldots, a_n) = \lambda_{\overrightarrow{E}}(\mathbf{a_0a_1}, \ldots, \mathbf{a_0a_n})$, that

$$\lambda_E(a_0, \ldots, a_n) = \begin{vmatrix} a_{1\,1} - a_{0\,1} & a_{1\,2} - a_{0\,2} & \ldots & a_{1\,n} - a_{0\,n} \\ a_{2\,1} - a_{0\,1} & a_{2\,2} - a_{0\,2} & \ldots & a_{2\,n} - a_{0\,n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{n\,1} - a_{0\,1} & a_{n\,2} - a_{0\,2} & \ldots & a_{n\,n} - a_{0\,n} \end{vmatrix},$$

where a_i has coordinates $(a_{i\,1}, \ldots, a_{i\,n})$ with respect to the affine frame $(O, (e_1, \ldots, e_n))$.

(2) Prove that the volume $\mathrm{vol}(a_0, \ldots, a_n)$ of the n-simplex $(a_0, \ldots, a_n)$ is

$$\mathrm{vol}(a_0, \ldots, a_n) = \frac{1}{n!}\lambda_{\overrightarrow{E}}(\mathbf{a_0a_1}, \ldots, \mathbf{a_0a_n}).$$

Problem 7.9 Prove that the so-called *Lagrange identity* holds:

$$(u \cdot v)^2 + \|u \times v\|^2 = \|u\|^2\|v\|^2.$$

Problem 7.10 Given p vectors $(u_1, \ldots, u_p)$ in a Euclidean space E of dimension $n \geq p$, the *Gram determinant (or Gramian)* of the vectors $(u_1, \ldots, u_p)$ is the determinant

$$\mathrm{Gram}(u_1, \ldots, u_p) = \begin{vmatrix} \|u_1\|^2 & \langle u_1, u_2\rangle & \ldots & \langle u_1, u_p\rangle \\ \langle u_2, u_1\rangle & \|u_2\|^2 & \ldots & \langle u_2, u_p\rangle \\ \vdots & \vdots & \ddots & \vdots \\ \langle u_p, u_1\rangle & \langle u_p, u_2\rangle & \ldots & \|u_p\|^2 \end{vmatrix}.$$

(1) Prove that

$$\mathrm{Gram}(u_1, \ldots, u_n) = \lambda_E(u_1, \ldots, u_n)^2.$$

Hint. By a previous problem, if $(e_1, \ldots, e_n)$ is an orthonormal basis of E and A is the matrix of the vectors $(u_1, \ldots, u_n)$ over this basis,

$$\det(A)^2 = \det(A^\top A) = \det(A_i \cdot A_j),$$

where A_i denotes the ith column of the matrix A, and $(A_i \cdot A_j)$ denotes the $n \times n$ matrix with entries $A_i \cdot A_j$.

(2) Prove that

$$\|u_1 \times \cdots \times u_{n-1}\|^2 = \mathrm{Gram}(u_1, \ldots, u_{n-1}).$$

Hint. Letting $w = u_1 \times \cdots \times u_{n-1}$, observe that

$$\lambda_E(u_1, \ldots, u_{n-1}, w) = \langle w, w\rangle = \|w\|^2,$$

and show that

$$\begin{aligned}\|w\|^4 &= \lambda_E(u_1, \ldots, u_{n-1}, w)^2 = \mathrm{Gram}(u_1, \ldots, u_{n-1}, w)\\ &= \mathrm{Gram}(u_1, \ldots, u_{n-1})\|w\|^2.\end{aligned}$$

Problem 7.11 Given a Euclidean space E, let U be a nonempty affine subspace of E, and let a be any point in E. We define the *distance* $d(a, U)$ of a to U as

$$d(a, U) = \inf\{\|\mathbf{ab}\| \mid b \in U\}.$$

(a) Prove that the affine subspace $U_a^{\perp}$ defined such that

$$U_a^{\perp} = a + \overrightarrow{U}^{\perp}$$

intersects U in a single point b such that $d(a, U) = \|\mathbf{ab}\|$.
Hint. Recall the discussion after Lemma 2.11.2.

(b) Let $(a_0, \ldots, a_p)$ be a frame for U (not necessarily orthonormal). Prove that

$$d(a, U)^2 = \frac{\mathrm{Gram}(\mathbf{a_0a}, \mathbf{a_0a_1}, \ldots, \mathbf{a_0a_p})}{\mathrm{Gram}(\mathbf{a_0a_1}, \ldots, \mathbf{a_0a_p})}.$$

Hint. Gram is unchanged when a linear combination of other vectors is added to one of the vectors, and thus

$$\mathrm{Gram}(\mathbf{a_0a}, \mathbf{a_0a_1}, \ldots, \mathbf{a_0a_p}) = \mathrm{Gram}(\mathbf{ba}, \mathbf{a_0a_1}, \ldots, \mathbf{a_0a_p}),$$

where b is the unique point defined in question (a).

(c) If D and D' are two lines in E that are not coplanar, $a, b \in D$ are distinct points on D, and $a', b' \in D'$ are distinct points on D', prove that if $d(D, D')$ is the shortest distance between D and D' (why does it exist?), then

$$d(D, D')^2 = \frac{\mathrm{Gram}(\mathbf{aa'}, \mathbf{ab}, \mathbf{a'b'})}{\mathrm{Gram}(\mathbf{ab}, \mathbf{a'b'})}.$$

Problem 7.12 Given a hyperplane H in $\mathbb{E}^n$ of equation

$$u_1x_1 + \cdots + u_nx_n - v = 0,$$

for any point $a = (a_1, \ldots, a_n)$, prove that the distance $d(a, H)$ of a to H (see problem 7.11) is given by

$$d(a, H) = \frac{|u_1a_1 + \cdots + u_na_n - v|}{\sqrt{u_1^2 + \cdots + u_n^2}}.$$

Problem 7.13 Given a Euclidean space E, let U and V be two nonempty affine subspaces such that $U \cap V = \emptyset$. We define the *distance* $d(U, V)$ of U and V as

$$d(U, V) = \inf\{\|\mathbf{ab}\| \mid a \in U,\, b \in V\}.$$

(a) Prove that $\dim(\overrightarrow{U}+\overrightarrow{V}) \leq \dim(\overrightarrow{E})-1$, and that $\overrightarrow{U}^{\perp} \cap \overrightarrow{V}^{\perp} = (\overrightarrow{U}+\overrightarrow{V})^{\perp} \neq \{0\}$.
Hint. Recall the discussion after Lemma 2.11.2 in Chapter 2.

(b) Let $\overrightarrow{W} = \overrightarrow{U}^{\perp} \cap \overrightarrow{V}^{\perp} = (\overrightarrow{U}+\overrightarrow{V})^{\perp}$. Prove that $U' = U + \overrightarrow{W}$ is an affine subspace with direction $\overrightarrow{U} \oplus \overrightarrow{W}$, $V' = V + \overrightarrow{W}$ is an affine subspace with direction $\overrightarrow{V} \oplus \overrightarrow{W}$, and that $W' = U' \cap V'$ is a nonempty affine subspace with direction $(\overrightarrow{U} \cap \overrightarrow{V}) \oplus \overrightarrow{W}$ such that $U \cap W' \neq \emptyset$ and $V \cap W' \neq \emptyset$. Prove that $U \cap W'$ and $V \cap W'$ are parallel affine subspaces such that

$$\overrightarrow{U \cap W'} = \overrightarrow{V \cap W'} = \overrightarrow{U} \cap \overrightarrow{V}.$$

Prove that if $a, c \in U$, $b, d \in V$, and $\mathbf{ab}, \mathbf{cd} \in (\overrightarrow{U}+\overrightarrow{V})^{\perp}$, then $\mathbf{ab} = \mathbf{cd}$ and $\mathbf{ac} = \mathbf{bd}$. Prove that if $c \in W'$, then $c + (\overrightarrow{U}+\overrightarrow{V})^{\perp}$ intersects $U \cap W'$ and $V \cap W'$ in unique points $a \in U \cap W'$ and $b \in V \cap W'$ such that $\mathbf{ab} \in (\overrightarrow{U}+\overrightarrow{V})^{\perp}$.

Prove that for all $a \in U \cap W'$ and all $b \in V \cap W'$,

$$d(U, V) = \|\mathbf{ab}\| \quad \text{iff} \quad \mathbf{ab} \in (\overrightarrow{U}+\overrightarrow{V})^{\perp}.$$

Prove that $a \in U$ and $b \in V$ as above are unique iff $\overrightarrow{U} \cap \overrightarrow{V} = \{0\}$.

(c) If $m = \dim(\overrightarrow{U}+\overrightarrow{V})$, $(e_1, \ldots, e_m)$ is any basis of $\overrightarrow{U}+\overrightarrow{V}$, and $a_0 \in U$ and $b_0 \in V$ are any two points, prove that

$$d(U, V)^2 = \frac{\mathrm{Gram}(\mathbf{a_0 b_0}, e_1, \ldots, e_m)}{\mathrm{Gram}(e_1, \ldots, e_m)}.$$

Problem 7.14 Let E be a real vector space of dimension n, and let $\varphi\colon E \times E \to \mathbb{R}$ be a symmetric bilinear form. Recall that φ is *nondegenerate* if for every $u \in E$,

$$\text{if} \quad \varphi(u, v) = 0 \quad \text{for all } v \in E, \quad \text{then} \quad u = 0.$$

A linear map $f\colon E \to E$ is an *isometry w.r.t.* φ if

$$\varphi(f(x), f(y)) = \varphi(x, y)$$

for all $x, y \in E$. The purpose of this problem is to prove that the Cartan–Dieudonné theorem still holds when φ is nondegenerate. The difficulty is that there may be *isotropic vectors*, i.e., nonnull vectors u such that $\varphi(u, u) = 0$. A vector u is called *nonisotropic* if $\varphi(u, u) \neq 0$. Of course, a nonisotropic vector is nonnull.

(a) Assume that φ is nonnull and that f is an isometry w.r.t. φ. Prove that $f(u) - u$ and $f(u) + u$ are conjugate w.r.t. φ, i.e.,

$$\varphi(f(u) - u, f(u) + u) = 0.$$

Prove that there is some nonisotropic vector $u \in E$ such that either $f(u) - u$ or $f(u) + u$ is nonisotropic.

(b) Let φ be nondegenerate. Prove the following version of the Cartan–Dieudonné theorem:

Every isometry $f \in \mathbf{O}(\varphi)$ that is not the identity is the composition of at most $2n - 1$ reflections w.r.t. hyperplanes. When $n \geq 2$, the identity is the composition of any reflection with itself.

Proceed by induction. In the induction step, consider the following three cases:

(1) f admits 1 as an eigenvalue.

(2) f admits -1 as an eigenvalue.

(3) $f(u) \neq u$ and $f(u) \neq -u$ for every nonnull vector $u \in E$.

Argue that there is some nonisotropic vector u such that either $f(u) - u$ or $f(u) + u$ is nonisotropic, and use a suitable reflection s about the hyperplane orthogonal to $f(u) - u$ or $f(u) + u$, such that $s \circ f$ admits 1 or -1 as an eigenvalue.

(c) What goes wrong with the argument in (b) if φ is nonnull but possibly degenerate? Is $\mathbf{O}(\varphi)$ still a group?

Remark: A stronger version of the Cartan–Dieudonné theorem holds: in fact, at most n reflections are needed, but the proof is much harder (for instance, see Dieudonné [47]).