Part III

The Geometry of Bilinear Forms

Chapter 27

The Cartan–Dieudonné Theorem

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 27.1). This important result is a special case of the "Cartan–Dieudonné theorem" (Cartan [33], Dieudonné [51]). We also prove that every rotation in $\mathbf{SO}(n)$ is the composition of at most n flips (for $n \geq 3$).

Affine isometries are defined, and their fixed points are investigated. First, we characterize the set of fixed points of an affine map. Then we 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 affine flips (for $n \geq 3$).

27.1 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 [33], 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 [51]. One should also consult Emil Artin's book [6], which contains an in-depth study of the orthogonal group and another proof of the Cartan–Dieudonné theorem.

Theorem 27.1. *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. The map 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 $k \leq n-1$. See Figure 27.1.

Case 2. The map 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 13.2, 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

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

See Figure 27.2.

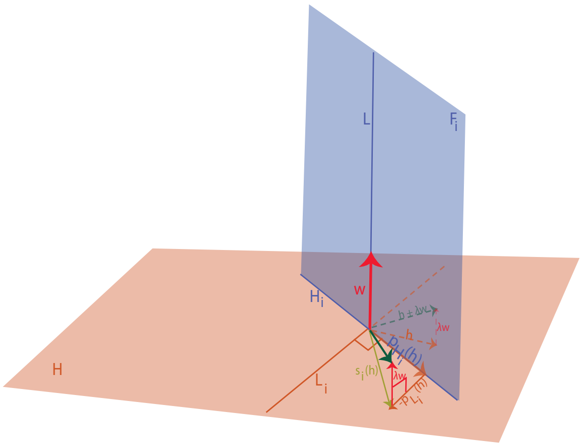

Figure 27.1: An illustration of how to extend the reflection s_i of Case 1 in Theorem 27.1 to E. The result of this extended reflection is the bold green vector.

Since $s^2 = \text{id}$, we cannot have $s \circ f = \text{id}$, 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. □

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.

(2) Theorem 27.1 still holds if the inner product on E is replaced by a nondegenerate symmetric bilinear form φ, but the proof is a lot harder; see Section 29.9.

(3) The proof of Theorem 27.1 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 27.3.

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 27.4.

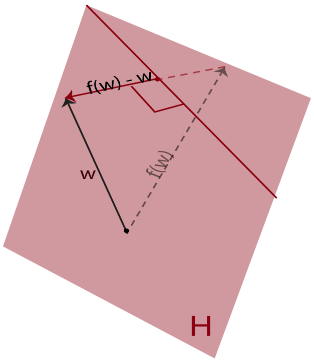

Figure 27.2: The construction of the hyperplane H for Case 2 of Theorem 27.1.

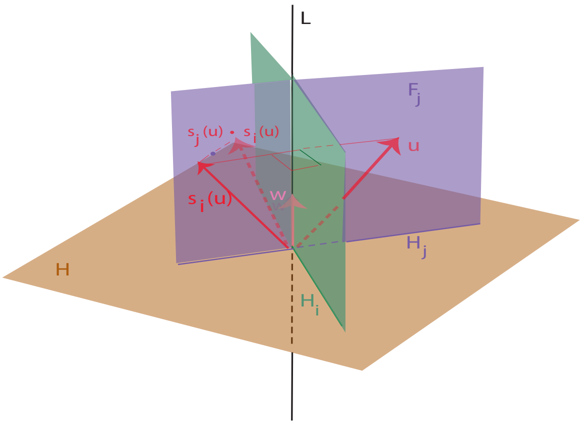

Figure 27.3: An isometry f as a composition of reflections, when 1 is an eigenvalue of f.

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

When $n = 2$, a reflection is a reflection about a line, and Theorem 27.1 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

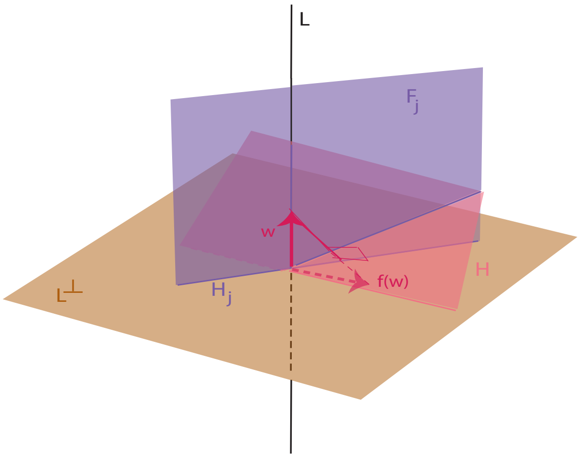

Figure 27.4: An isometry f as a composition of reflections when 1 is not an eigenvalue of f. Note that the pink plane H is perpendicular to $f(w) - w$.

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 27.1, 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 27.1, 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.

Proposition 27.2. *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 12.11. □

Lemma 27.2 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).

Proposition 27.3. *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 27.1, f is the composition of an even number less than or equal to $2m$ of reflections. From Lemma 24.15, 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 27.2, G is stable under f, and $E = F \oplus G$. Using Lemma 12.10, 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. □

An example showing that Lemma 27.3 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).

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 $r_1 = s_2s_1$ for two reflections s_1, s_2, we have

$$r_1r_2r_1^{-1} = s_2s_1r_2(s_2s_1)^{-1} = s_2s_1r_2s_1^{-1}s_2^{-1} = s_2s_1r_2s_1s_2 = s_2r_2^{-1}s_2 = r_2,$$

since $srs = r^{-1}$ for all reflections s and rotations r, and thus $r_1r_2 = r_2r_1$.

We can 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 $r = s_2s_1$, 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*

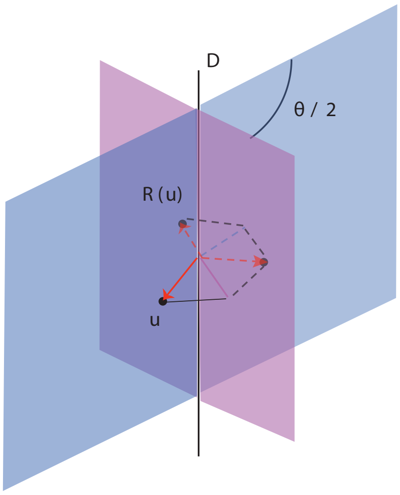

Figure 27.5: 3D rotation as the composition of two reflections.

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 27.5.

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.

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

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

Remark: For an arbitrary rotation matrix A, since $a_{1\,1} + a_{2\,2} + a_{3\,3}$ (the *trace* of A) is the sum of the eigenvalues of A, and since these eigenvalues are $\cos\theta + i\sin\theta$, $\cos\theta - i\sin\theta$, and 1, for some $\theta \in [0, 2\pi[$, we can compute $\cos\theta$ from

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

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

An improper transformation is either a reflection about a plane or the product of three reflections, or equivalently the product of a reflection about a plane with a rotation, and we noted in the discussion following Theorem 27.1 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 27.2, 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.

Proposition 27.4. *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 $\theta_1 \in [0, 2\pi]$. See Figure 27.6

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

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

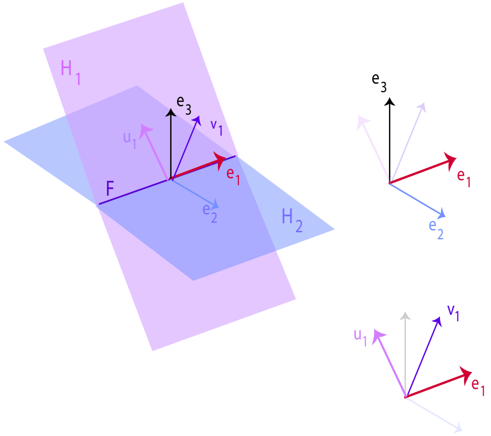

Figure 27.6: An illustration of the hyperplanes H_1, H_2, their intersection F, and the two orthonormal basis utilized in the proof of Proposition 27.4.

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_2A_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 $h_2 \circ h_1 = f_2 \circ f_1$. See Figure 27.7. $\square$

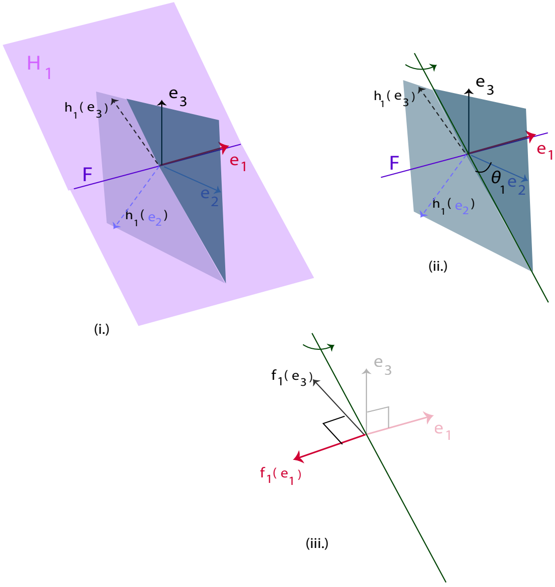

Figure 27.7: The conversion of the hyperplane reflection h_1 into the flip or 180° rotation around the green axis in the e_2e_3-plane. The green axis corresponds to the restriction of the eigenspace associated with eigenvalue 1.

Using Lemma 27.4 and the Cartan–Dieudonné theorem, we obtain the following characterization of rotations when $n \geq 3$.

Theorem 27.5. *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 27.1, 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 27.4, 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 27.1 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 27.4 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 $u \in F_{2k}^{\perp}$. □

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 turn to affine isometries.

27.2 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 27.10). 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 affine reflections if it has a fixed point, or else as the composition of at most $n+2$ affine reflections. We also prove that every rigid motion in $\mathbf{SE}(n)$ is the composition of at most n affine flips (for $n \geq 3$). This is somewhat surprising, in view of the previous theorem.

Definition 27.1. 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

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

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

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

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.

Proposition 27.6. *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 12.12 for isometries between Euclidean vector spaces.

Proposition 27.7. *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 $\|\overrightarrow{f(a)f(b)}\| = \|\overrightarrow{ab}\|$, for all $a, b \in E$.

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

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

for all $u \in E$. Since

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

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

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

Then, the hypothesis

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

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

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

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

$$g(0) = 0.$$

Thus, we can apply Lemma 12.12, which shows that g is indeed a linear isometry, and thus f is an affine isometry. □

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

27.3 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, $\mathrm{Ker}\,\big(\overrightarrow{f} - \mathrm{id}\big) = E\big(1, \overrightarrow{f}\big)$. Given some origin $\Omega \in E$, since

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

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

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

From the above, we get

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

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

Proposition 27.8. *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

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

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

$$\overrightarrow{af(b)} - \overrightarrow{ab} = \overrightarrow{af(a)} + \overrightarrow{f}(\overrightarrow{ab}) - \overrightarrow{ab} = \overrightarrow{f}(\overrightarrow{ab}) - \overrightarrow{ab},$$

and so

$$f(b) = b$$

iff

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

iff

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

iff

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

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

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

iff

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

which can be rewritten as

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

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

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

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

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

we have $\big(\overrightarrow{f} - \mathrm{id}\big)(\overrightarrow{\Omega a}) = 0$ 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. □

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

If an affine 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 27.10 that every affine isometry is the (commutative) composition of a translation with an affine isometry that always has a fixed point.

27.4 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

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

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

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

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

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

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

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

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

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

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 *affine orthogonal symmetry about F*. Since

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

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

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

is also independent of $\Omega \in F$, and it is called the *affine 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 24.16). We define the *distance between F_1 and F_2* as $\|\overrightarrow{ab}\|$. 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 $\|\overrightarrow{xy}\|$ for all $x \in F_1$ and all $y \in F_2$.

Proposition 27.9. *Given any affine space E, if $f\colon E \to E$ and $g\colon E \to E$ are affine orthogonal symmetries about parallel affine subspaces F_1 and F_2, then $g \circ f$ is a translation defined by the vector $2\overrightarrow{ab}$, where $\overrightarrow{ab}$ is any vector perpendicular to the common direction $\overrightarrow{F}$ of F_1 and F_2 such that $\|\overrightarrow{ab}\|$ 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 affine orthogonal symmetries about parallel affine subspaces F_1 and F_2 whose common direction is orthogonal to $\tau = \overrightarrow{ab}$, for some $a \in F_1$ and some $b \in F_2$ such that the distance between F_1 and F_2 is $\|\overrightarrow{ab}\|/2$.*

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 affine reflection of $a \in F_1$ about F_2, and it is easily checked that $g \circ f$ is the translation by the vector $\tau = \overrightarrow{ag(a)}$ 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 27.10. *Let E be a Euclidean affine space of finite dimension n. For every affine isometry $f\colon E \to E$, there is a unique affine 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

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

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 $\overrightarrow{xf(x)} = \tau$ 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 $\varphi\colon \overrightarrow{E} \to \overrightarrow{E}$; see Theorem 6.13. To show that we have a direct sum, we prove orthogonality. Let $u \in \mathrm{Ker}\,(h - \mathrm{id})$, 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 $\overrightarrow{xf(x)} = \tau$ belongs to the space $\mathrm{Ker}\,\big(\overrightarrow{f} - \mathrm{id}\big)$. If we define $g\colon E \to E$ such that

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

we have

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

since $\overrightarrow{xf(x)} = \tau$ is equivalent to $x = f(x) - \tau$. As a composition of affine isometries, g is an affine isometry, x is a fixed point of g, and since $\tau \in \mathrm{Ker}\,\big(\overrightarrow{f} - \mathrm{id}\big)$, 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 27.8, $\mathrm{Fix}(g)$ is an affine subspace of E with direction $\mathrm{Ker}\,\big(\overrightarrow{g} - \mathrm{id}\big) = \mathrm{Ker}\,\big(\overrightarrow{f} - \mathrm{id}\big)$. 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

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

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

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

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

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

we get

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

which can be rewritten as

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

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

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

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

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 $\mathrm{Ker}\,(\overrightarrow{g_1} - \mathrm{id}) = \mathrm{Ker}\,\big(\overrightarrow{f} - \mathrm{id}\big)$. Since g_1 has some fixed point b, we get

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

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

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

which shows that

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

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

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

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

The determination of x is illustrated in Figure 27.8.

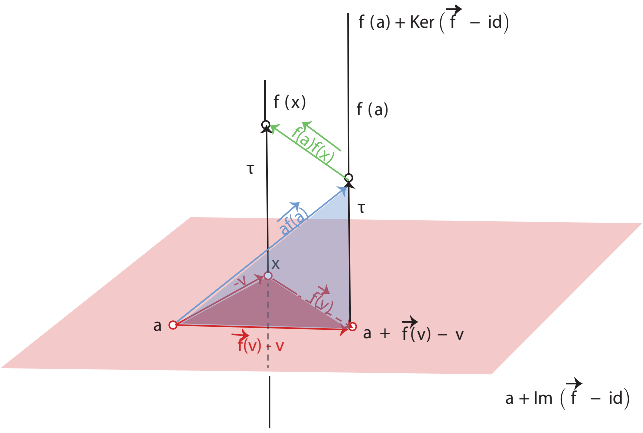
$f(a) + \mathrm{Ker}\,(\overrightarrow{f} - \mathrm{id})$
$f(x)$
$f(a)$
$\overrightarrow{f(a)f(x)}$
τ
τ
$\overrightarrow{af(a)}$
x
-v
$\overrightarrow{f}(v)$
a
$a + \overrightarrow{f}(v) - v$
$\overrightarrow{f}(v) - v$
$a + \mathrm{Im}\,(\overrightarrow{f} - \mathrm{id})$

Figure 27.8: Affine rigid motion as $f = t \circ g$, where g has some fixed point x.

Remarks:

(1) Note that $\mathrm{Ker}\left(\overrightarrow{f} - \mathrm{id}\right) = \{0\}$ iff $\mathrm{Fix}(g)$ 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).

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

In the affine Euclidean plane it is easy to see that the affine isometries (besides the identity) are classified as follows. An affine isometry f that has a fixed point is a rotation if it is a direct isometry; otherwise, it is an affine reflection about a line. If f has no fixed point, then it is either a nontrivial translation or the composition of an affine 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 affine isometries that have a fixed point. A proper affine isometry with a fixed point is a rotation around a line D (its set of fixed points), as illustrated in Figure 27.9.

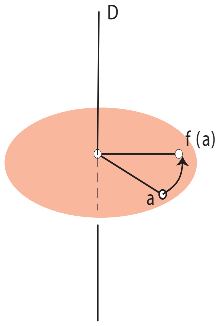

Figure 27.9: 3D proper affine rigid motion with line D of fixed points (rotation).

An improper affine isometry with a fixed point is either an affine reflection about a plane H (the set of fixed points) or the composition of a rotation followed by an affine reflection about a plane H orthogonal to the axis of rotation D, as illustrated in Figures 27.10 and 27.11. In the second case, there is a single fixed point $O = D \cap H$.

There are three types of affine 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 an affine rigid motion is proper, and is called a *screw motion*. A screw motion is illustrated in Figure 27.12.

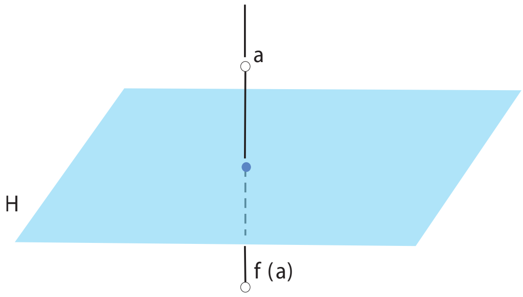

Figure 27.10: 3D improper affine rigid motion with a plane H of fixed points (reflection).

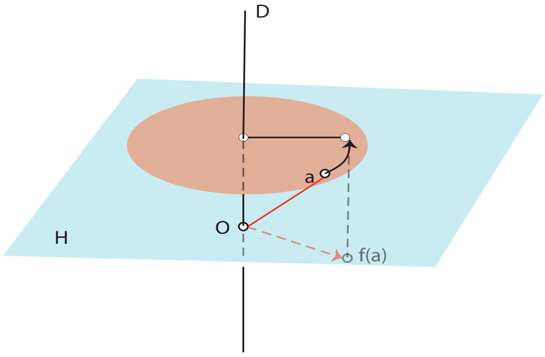

Figure 27.11: $3D$ improper affine rigid motion with a unique fixed point.

The third kind is the composition of an affine 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 27.13.

This last transformation is an improper affine isometry.

27.5 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 [11], Snapper and Troyer [160], or Tisseron [173] for a detailed treatment of the Cartan–Dieudonné theorem and its variants.

Theorem 27.11. *Let E be an affine Euclidean space of dimension $n \geq 1$. Every affine isometry $f \in \mathbf{Is}(E)$ that has a fixed point and is not the identity is the composition of at most n affine reflections. Every affine isometry $f \in \mathbf{Is}(E)$ that has no fixed point is the*

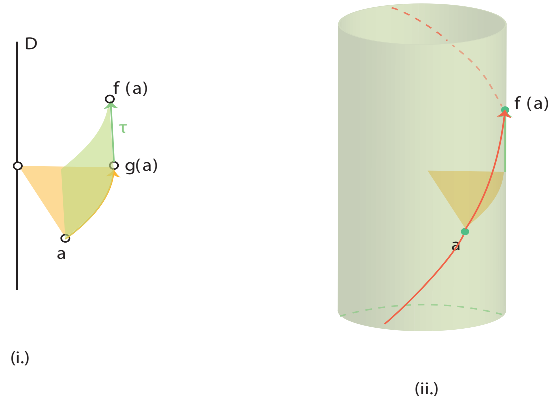

Figure 27.12: 3D proper affine rigid motion with no fixed point (screw motion). The second illustration demonstrates that a screw motion produces a helix path along the surface of a cylinder.

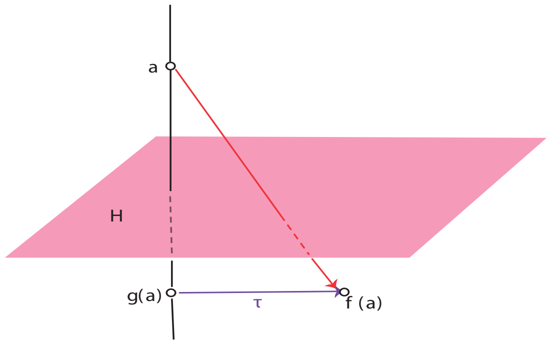

Figure 27.13: 3D improper affine rigid motion with no fixed points.

composition of at most $n+2$ affine reflections. When $n \geq 2$, the identity is the composition of any reflection with itself.

Proof. First, we use Theorem 27.10. 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 27.1. 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

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

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

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

for all $a \in E$. If f has no fixed point, then $f = t \circ g$ for some affine 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 27.9, the translation $t = t_\tau$ can be achieved by two affine reflections about parallel hyperplanes, and thus $f = s_{k+2} \circ \cdots \circ s_1$, for some affine reflections (at most $n+2$). □

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

Theorem 27.12. *Let E be a Euclidean affine space of dimension $n \geq 3$. Every affine rigid motion $f \in \mathbf{SE}(E)$ is the composition of an even number of affine flips $f = f_{2k} \circ \cdots \circ f_1$, where $2k \leq n$.*

Proof. As in the proof of Theorem 27.11, we distinguish between the two cases where f has some fixed point or not. If f has a fixed point Ω, we apply Theorem 27.5. 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

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

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

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

for all $a \in E$.

If f does not have a fixed point, as in the proof of Theorem 27.11, 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 27.5, 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 27.9, 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 affine 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 an affine 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 affine flips about lines D_1 and D_2 orthogonal to D, at a distance $\|\tau\|/2$ and making an angle $\theta/2$.

Chapter 28

Isometries of Hermitian Spaces

28.1 The Cartan–Dieudonné Theorem, Hermitian Case

The Cartan-Dieudonné theorem can be generalized (Theorem 28.2), but this requires allowing new types of hyperplane reflections that we call Hermitian reflections. After doing so, every isometry in $\mathbf{U}(n)$ can always be written as a composition of at most n Hermitian reflections (for $n \geq 2$). Better yet, every rotation in $\mathbf{SU}(n)$ can be expressed as the composition of at most $2n - 2$ (standard) hyperplane reflections! This implies that every unitary transformation in $\mathbf{U}(n)$ is the composition of at most $2n-1$ isometries, with at most one Hermitian reflection, the other isometries being (standard) hyperplane reflections. The crucial Proposition 13.2 is false as is, and needs to be amended. The QR-decomposition of arbitrary complex matrices in terms of Householder matrices can also be generalized, using a trick.

In order to generalize the Cartan–Dieudonné theorem and the QR-decomposition in terms of Householder transformations, we need to introduce new kinds of hyperplane reflections. This is not really surprising, since in the Hermitian case, there are improper isometries whose determinant can be any unit complex number. Hyperplane reflections are generalized as follows.

Definition 28.1. Let E be a Hermitian space of finite dimension. For any hyperplane H, for any nonnull vector w orthogonal to H, so that $E = H \oplus G$, where $G = \mathbb{C}w$, a *Hermitian reflection about H of angle θ* is a linear map of the form $\rho_{H,\theta}\colon E \to E$, defined such that

$$\rho_{H,\theta}(u) = p_H(u) + e^{i\theta} p_G(u),$$

for any unit complex number $e^{i\theta} \neq 1$ (i.e. $\theta \neq k2\pi$). For any nonzero vector $w \in E$, we denote by $\rho_{w,\theta}$ the Hermitian reflection given by $\rho_{H,\theta}$, where H is the hyperplane orthogonal to w.

Since $u = p_H(u) + p_G(u)$, the Hermitian reflection $\rho_{w,\theta}$ is also expressed as

$$\rho_{w,\theta}(u) = u + (e^{i\theta} - 1)p_G(u),$$

or as

$$\rho_{w,\theta}(u) = u + (e^{i\theta} - 1)\,\frac{(u \cdot w)}{\|w\|^2}\,w.$$

Note that the case of a standard hyperplane reflection is obtained when $e^{i\theta} = -1$, i.e., $\theta = \pi$.

We leave as an easy exercise to check that $\rho_{w,\theta}$ is indeed an isometry, and that the inverse of $\rho_{w,\theta}$ is $\rho_{w,-\theta}$. If we pick an orthonormal basis $(e_1, \ldots, e_n)$ such that $(e_1, \ldots, e_{n-1})$ is an orthonormal basis of H, the matrix of $\rho_{w,\theta}$ is

$$\begin{pmatrix} I_{n-1} & 0 \\ 0 & e^{i\theta} \end{pmatrix}$$

We now come to the main surprise. Given any two distinct vectors u and v such that $\|u\| = \|v\|$, there isn't always a hyperplane reflection mapping u to v, but this can be done using two Hermitian reflections!

Proposition 28.1. *Let E be any nontrivial Hermitian space.*

(1) For any two vectors $u, v \in E$ such that $u \neq v$ and $\|u\| = \|v\|$, if $u \cdot v = e^{i\theta}|u \cdot v|$, then the (usual) reflection s about the hyperplane orthogonal to the vector $v - e^{-i\theta}u$ is such that $s(u) = e^{i\theta}v$.

(2) For any nonnull vector $v \in E$, for any unit complex number $e^{i\theta} \neq 1$, there is a Hermitian reflection $\rho_{v,\theta}$ such that

$$\rho_{v,\theta}(v) = e^{i\theta}v.$$

As a consequence, for u and v as in (1), we have $\rho_{v,-\theta} \circ s(u) = v$.

Proof. (1) Consider the (usual) reflection about the hyperplane orthogonal to $w = v - e^{-i\theta}u$. We have

$$s(u) = u - 2\,\frac{(u \cdot (v - e^{-i\theta}u))}{\|v - e^{-i\theta}u\|^2}\,(v - e^{-i\theta}u).$$

We need to compute

$$-2u \cdot (v - e^{-i\theta}u) \quad \text{and} \quad (v - e^{-i\theta}u) \cdot (v - e^{-i\theta}u).$$

Since $u \cdot v = e^{i\theta}|u \cdot v|$, we have

$$e^{-i\theta}u \cdot v = |u \cdot v| \quad \text{and} \quad e^{i\theta}v \cdot u = |u \cdot v|.$$

Using the above and the fact that $\|u\| = \|v\|$, we get

$$\begin{aligned} -2u \cdot (v - e^{-i\theta}u) &= 2e^{i\theta}\,\|u\|^2 - 2u \cdot v, \\ &= 2e^{i\theta}(\|u\|^2 - |u \cdot v|), \end{aligned}$$

and

$$\begin{aligned}(v - e^{-i\theta}u)\cdot(v - e^{-i\theta}u) &= \|v\|^2 + \|u\|^2 - e^{-i\theta}u\cdot v - e^{i\theta}v\cdot u,\\ &= 2(\|u\|^2 - |u\cdot v|),\end{aligned}$$

and thus,

$$-2\,\frac{(u\cdot(v - e^{-i\theta}u))}{\|(v - e^{-i\theta}u)\|^2}\,(v - e^{-i\theta}u) = e^{i\theta}(v - e^{-i\theta}u).$$

But then,

$$s(u) = u + e^{i\theta}(v - e^{-i\theta}u) = u + e^{i\theta}v - u = e^{i\theta}v,$$

and $s(u) = e^{i\theta}v$, as claimed.

(2) This part is easier. Consider the Hermitian reflection

$$\rho_{v,\theta}(u) = u + (e^{i\theta} - 1)\,\frac{(u\cdot v)}{\|v\|^2}\,v.$$

We have

$$\begin{aligned}\rho_{v,\theta}(v) &= v + (e^{i\theta} - 1)\,\frac{(v\cdot v)}{\|v\|^2}\,v,\\ &= v + (e^{i\theta} - 1)v,\\ &= e^{i\theta}v.\end{aligned}$$

Thus, $\rho_{v,\theta}(v) = e^{i\theta}v$. Since $\rho_{v,\theta}$ is linear, changing the argument v to $e^{i\theta}v$, we get

$$\rho_{v,-\theta}(e^{i\theta}v) = v,$$

and thus, $\rho_{v,-\theta}\circ s(u) = v$. □

Remarks:

(1) If we use the vector $v + e^{-i\theta}u$ instead of $v - e^{-i\theta}u$, we get $s(u) = -e^{i\theta}v$.

(2) Certain authors, such as Kincaid and Cheney [101] and Ciarlet [41], use the vector $u + e^{i\theta}v$ instead of our vector $v + e^{-i\theta}u$. The effect of this choice is that they also get $s(u) = -e^{i\theta}v$.

(3) If $v = \|u\|\,e_1$, where e_1 is a basis vector, $u\cdot e_1 = a_1$, where a_1 is just the coefficient of u over the basis vector e_1. Then, since $u\cdot e_1 = e^{i\theta}|a_1|$, the choice of the plus sign in the vector $\|u\|\,e_1 + e^{-i\theta}u$ has the effect that the coefficient of this vector over e_1 is $\|u\| + |a_1|$, and no cancellations takes place, which is preferable for numerical stability (we need to divide by the square norm of this vector).

The last part of Proposition 28.1 shows that the Cartan–Dieudonné is salvaged, since we can send u to v by a sequence of two Hermitian reflections when $u \neq v$ and $\|u\| = \|v\|$, and since the inverse of a Hermitian reflection is a Hermitian reflection. Actually, because we are over the complex field, a linear map always have (complex) eigenvalues, and we can get a slightly improved result.

Theorem 28.2. *Let E be a Hermitian space of dimension $n \geq 1$. Every isometry $f \in \mathbf{U}(E)$ is the composition $f = \rho_n \circ \rho_{n-1} \circ \cdots \circ \rho_1$ of n isometries ρ_j, where each ρ_j is either the identity or a Hermitian reflection (possibly a standard hyperplane reflection). When $n \geq 2$, the identity is the composition of any hyperplane reflection with itself.*

Proof. We prove by induction on n that there is an orthonormal basis of eigenvectors $(u_1, \ldots, u_n)$ of f such that

$$f(u_j) = e^{i\theta_j} u_j,$$

where $e^{i\theta_j}$ is an eigenvalue associated with u_j, for all j, $1 \leq j \leq n$.

When $n = 1$, every isometry $f \in \mathbf{U}(E)$ is either the identity or a Hermitian reflection ρ_θ, since for any nonnull vector u, we have $f(u) = e^{i\theta} u$ for some θ. We let u_1 be any nonnull unit vector.

Let us now consider the case where $n \geq 2$. Since $\mathbb{C}$ is algebraically closed, the characteristic polynomial $\det(f - \lambda \mathrm{id})$ of f has n complex roots which must be the form $e^{i\theta}$, since they have absolute value 1. Pick any such eigenvalue $e^{i\theta_1}$, and pick any eigenvector $u_1 \neq 0$ of f for $e^{i\theta_1}$ of unit length. If $F = \mathbb{C}u_1$ is the subspace spanned by u_1, we have $f(F) = F$, since $f(u_1) = e^{i\theta_1} u_1$. Since $f(F) = F$ and f is an isometry, it is easy to see that $f(F^\perp) \subseteq F^\perp$, and by Proposition 14.13, we have $E = F \oplus F^\perp$. Furthermore, it is obvious that the restriction of f to $F^\perp$ is unitary. Since $\dim(F^\perp) = n - 1$, we can apply the induction hypothesis to $F^\perp$, and we get an orthonormal basis of eigenvectors $(u_2, \ldots, u_n)$ for $F^\perp$ such that

$$f(u_j) = e^{i\theta_j} u_j,$$

where $e^{i\theta_j}$ is an eigenvalue associated with u_j, for all j, $2 \leq j \leq n$ Since $E = F \oplus F^\perp$ and $F = \mathbb{C}u_1$, the claim is proved. But then, if ρ_j is the Hermitian reflection about the hyperplane H_j orthogonal to u_j and of angle θ_j, it is obvious that

$$f = \rho_{\theta_n} \circ \cdots \circ \rho_{\theta_1}.$$

When $n \geq 2$, we have $\mathrm{id} = s \circ s$ for every reflection s. □

Remarks:

(1) Any isometry $f \in \mathbf{U}(n)$ can be express as $f = \rho_\theta \circ g$, where $g \in \mathbf{SU}(n)$ is a rotation, and ρ_θ is a Hermitian reflection. Indeed, by the above theorem, with respect to the basis $(u_1, \ldots, u_n)$, $\det(f) = e^{i(\theta_1 + \cdots + \theta_n)}$, and letting $\theta = \theta_1 + \cdots + \theta_n$ and ρ_θ be the Hermitian

reflection about the hyperplane orthogonal to u_1 and of angle θ, since $\rho_\theta \circ \rho_{-\theta} = \mathrm{id}$, we have

$$f = (\rho_\theta \circ \rho_{-\theta}) \circ f = \rho_\theta \circ (\rho_{-\theta} \circ f).$$

Letting $g = \rho_{-\theta} \circ f$, it is obvious that $\det(g) = 1$. As a consequence, there is a bijection between $S^1 \times \mathbf{SU}(n)$ and $\mathbf{U}(n)$, where S^1 is the unit circle (which corresponds to the group of complex numbers $e^{i\theta}$ of unit length). In fact, it is a homeomorphism.

(2) We abandoned the style of proof used in theorem 27.1, because in the Hermitian case, eigenvalues and eigenvectors always exist, and the proof is simpler that way (in the real case, an isometry may not have any real eigenvalues!). The sacrifice is that the theorem yields no information on the number of (standard) hyperplane reflections. We shall rectify this situation shortly.

We will now reveal the beautiful trick (found in Mneimné and Testard [126]) that allows us to prove that every rotation in $\mathbf{SU}(n)$ is the composition of at most $2n - 2$ (standard) hyperplane reflections. For what follows, it is more convenient to denote a standard reflection about the hyperplane H as h_u (it is trivial that these do not depend on the choice of u in $H^\perp$). Then, given any two distinct orthogonal vectors u, v such that $\|u\| = \|v\|$, consider the composition $\rho_{v,-\theta} \circ \rho_{u,\theta}$. The trick is that this composition can be expressed as two standard hyperplane reflections! This wonderful fact is proved in the next Proposition.

Proposition 28.3. *Let E be a nontrivial Hermitian space. For any two distinct orthogonal vectors u, v such that $\|u\| = \|v\|$, we have*

$$\rho_{v,-\theta} \circ \rho_{u,\theta} = h_{v-u} \circ h_{v-e^{-i\theta}u} = h_{u+v} \circ h_{u+e^{i\theta}v}.$$

Proof. Since u and v are orthogonal, each one is in the hyperplane orthogonal to the other, and thus,

$$\begin{aligned}
\rho_{u,\theta}(u) &= e^{i\theta}u,\\
\rho_{u,\theta}(v) &= v,\\
\rho_{v,-\theta}(u) &= u,\\
\rho_{v,-\theta}(v) &= e^{-i\theta}v,\\
h_{v-u}(u) &= v,\\
h_{v-u}(v) &= u,\\
h_{v-e^{-i\theta}u}(u) &= e^{i\theta}v,\\
h_{v-e^{-i\theta}u}(v) &= e^{-i\theta}u.
\end{aligned}$$

Consequently, using linearity,

$$\begin{aligned}
\rho_{v,-\theta} \circ \rho_{u,\theta}(u) &= e^{i\theta}u,\\
\rho_{v,-\theta} \circ \rho_{u,\theta}(v) &= e^{-i\theta}v,\\
h_{v-u} \circ h_{v-e^{-i\theta}u}(u) &= e^{i\theta}u,\\
h_{v-u} \circ h_{v-e^{-i\theta}u}(v) &= e^{-i\theta}v,
\end{aligned}$$

and since both $\rho_{v,\,-\theta}\circ\rho_{u,\,\theta}$ and $h_{v-\,u}\circ h_{v-\,e^{-i\theta}u}$ are the identity on the orthogonal complement of $\{u,v\}$, they are equal. Since we also have

$$\begin{aligned} h_{u+\,v}(u) &= -v,\\ h_{u+\,v}(v) &= -u,\\ h_{u+\,e^{i\theta}v}(u) &= -e^{i\theta}v,\\ h_{u+\,e^{i\theta}v}(v) &= -e^{-i\theta}u, \end{aligned}$$

it is immediately verified that

$$h_{v-\,u}\circ h_{v-\,e^{-i\theta}u} = h_{u+\,v}\circ h_{u+\,e^{i\theta}v}.$$

□

We will use Proposition 28.3 as follows.

Proposition 28.4. *Let E be a nontrivial Hermitian space, and let $(u_1,\ldots,u_n)$ be some orthonormal basis for E. For any $\theta_1,\ldots,\theta_n$ such that $\theta_1+\cdots+\theta_n=0$, if $f\in\mathbf{U}(n)$ is the isometry defined such that*

$$f(u_j) = e^{i\theta_j}u_j,$$

for all j, $1\leq j\leq n$, then f is a rotation ($f\in\mathbf{SU}(n)$), and

$$\begin{aligned} f &= \rho_{u_n,\,\theta_n}\circ\cdots\circ\rho_{u_1,\,\theta_1}\\ &= \rho_{u_n,\,-(\theta_1+\cdots+\theta_{n-1})}\circ\rho_{u_{n-1},\,\theta_1+\cdots+\theta_{n-1}}\circ\cdots\circ\rho_{u_2,\,-\theta_1}\circ\rho_{u_1,\,\theta_1}\\ &= h_{u_n-\,u_{n-1}}\circ h_{u_n-\,e^{-i(\theta_1+\cdots+\theta_{n-1})}u_{n-1}}\circ\cdots\circ h_{u_2-\,u_1}\circ h_{u_2-\,e^{-i\theta_1}u_1}\\ &= h_{u_{n-1}+u_n}\circ h_{u_{n-1}+\,e^{i(\theta_1+\cdots+\theta_{n-1})}u_n}\circ\cdots\circ h_{u_1+u_2}\circ h_{u_1+\,e^{i\theta_1}u_2}. \end{aligned}$$

Proof. It is obvious from the definitions that

$$f = \rho_{u_n,\,\theta_n}\circ\cdots\circ\rho_{u_1,\,\theta_1},$$

and since the determinant of f is

$$D(f) = e^{i\theta_1}\cdots e^{i\theta_n} = e^{i(\theta_1+\cdots+\theta_n)}$$

and $\theta_1+\cdots+\theta_n=0$, we have $D(f)=e^0=1$, and f is a rotation. Letting

$$f_k = \rho_{u_k,\,-(\theta_1+\cdots+\theta_{k-1})}\circ\rho_{u_{k-1},\,\theta_1+\cdots+\theta_{k-1}}\circ\cdots\circ\rho_{u_3,\,-(\theta_1+\theta_2)}\circ\rho_{u_2,\,\theta_1+\theta_2}\circ\rho_{u_2,\,-\theta_1}\circ\rho_{u_1,\,\theta_1},$$

we prove by induction on k, $2\leq k\leq n$, that

$$f_k(u_j) = \begin{cases} e^{i\theta_j}u_j & \text{if } 1\leq j\leq k-1,\\ e^{-i(\theta_1+\cdots+\theta_{k-1})}u_k & \text{if } j=k, \text{ and}\\ u_j & \text{if } k+1\leq j\leq n. \end{cases}$$

The base case was treated in Proposition 28.3. Now, the proof of Proposition 28.3 also showed that

$$\begin{aligned}\rho_{u_{k+1},\,-(\theta_1+\cdots+\theta_k)}\circ\rho_{u_k,\,\theta_1+\cdots+\theta_k}(u_k)&=e^{i(\theta_1+\cdots+\theta_k)}u_k,\\ \rho_{u_{k+1},\,-(\theta_1+\cdots+\theta_k)}\circ\rho_{u_k,\,\theta_1+\cdots+\theta_k}(u_{k+1})&=e^{-i(\theta_1+\cdots+\theta_k)}u_{k+1},\end{aligned}$$

and thus, using the induction hypothesis for k $(2\leq k\leq n-1)$, we have

$$\begin{aligned}f_{k+1}(u_j)&=\rho_{u_{k+1},\,-(\theta_1+\cdots+\theta_k)}\circ\rho_{u_k,\,\theta_1+\cdots+\theta_k}\circ f_k(u_j)=e^{i\theta_j}u_j,\quad 1\leq j\leq k-1,\\ f_{k+1}(u_k)&=\rho_{u_{k+1},\,-(\theta_1+\cdots+\theta_k)}\circ\rho_{u_k,\,\theta_1+\cdots+\theta_k}\circ f_k(u_k)=e^{i(\theta_1+\cdots+\theta_k)}e^{-i(\theta_1+\cdots+\theta_{k-1})}u_k=e^{i\theta_k}u_k,\\ f_{k+1}(u_{k+1})&=\rho_{u_{k+1},\,-(\theta_1+\cdots+\theta_k)}\circ\rho_{u_k,\,\theta_1+\cdots+\theta_k}\circ f_k(u_{k+1})=e^{-i(\theta_1+\cdots+\theta_k)}u_{k+1},\\ f_{k+1}(u_j)&=\rho_{u_{k+1},\,-(\theta_1+\cdots+\theta_k)}\circ\rho_{u_k,\,\theta_1+\cdots+\theta_k}\circ f_k(u_j)=u_j,\quad k+1\leq j\leq n,\end{aligned}$$

which proves the induction step.

As a summary, we proved that

$$f_n(u_j)=\begin{cases}e^{i\theta_j}u_j & \text{if } 1\leq j\leq n-1,\\ e^{-i(\theta_1+\cdots+\theta_{n-1})}u_n & \text{when } j=n,\end{cases}$$

but since $\theta_1+\cdots+\theta_n=0$, we have $\theta_n=-(\theta_1+\cdots+\theta_{n-1})$, and the last expression is in fact

$$f_n(u_n)=e^{i\theta_n}u_n.$$

Therefore, we proved that

$$f=\rho_{u_n,\theta_n}\circ\cdots\circ\rho_{u_1,\theta_1}=\rho_{u_n,\,-(\theta_1+\cdots+\theta_{n-1})}\circ\rho_{u_{n-1},\,\theta_1+\cdots+\theta_{n-1}}\circ\cdots\circ\rho_{u_2,\,-\theta_1}\circ\rho_{u_1,\theta_1},$$

and using Proposition 28.3, we also have

$$\begin{aligned}f&=\rho_{u_n,\,-(\theta_1+\cdots+\theta_{n-1})}\circ\rho_{u_{n-1},\,\theta_1+\cdots+\theta_{n-1}}\circ\cdots\circ\rho_{u_2,\,-\theta_1}\circ\rho_{u_1,\theta_1}\\ &=h_{u_n-u_{n-1}}\circ h_{u_n-e^{-i(\theta_1+\cdots+\theta_{n-1})}u_{n-1}}\circ\cdots\circ h_{u_2-u_1}\circ h_{u_2-e^{-i\theta_1}u_1}\\ &=h_{u_{n-1}+u_n}\circ h_{u_{n-1}+e^{i(\theta_1+\cdots+\theta_{n-1})}u_n}\circ\cdots\circ h_{u_1+u_2}\circ h_{u_1+e^{i\theta_1}u_2},\end{aligned}$$

which completes the proof. □

We finally get our improved version of the Cartan–Dieudonné theorem.

Theorem 28.5. *Let E be a Hermitian space of dimension $n\geq 1$. Every rotation $f\in\mathbf{SU}(E)$ different from the identity is the composition of at most $2n-2$ standard hyperplane reflections. Every isometry $f\in\mathbf{U}(E)$ different from the identity is the composition of at most $2n-1$ isometries, all standard hyperplane reflections, except for possibly one Hermitian reflection. When $n\geq 2$, the identity is the composition of any reflection with itself.*

Proof. By Theorem 28.2, $f \in \mathbf{SU}(n)$ can be written as a composition

$$\rho_{u_n,\theta_n} \circ \cdots \circ \rho_{u_1,\theta_1},$$

where $(u_1, \ldots, u_n)$ is an orthonormal basis of eigenvectors. Since f is a rotation, $\det(f) = 1$, and this implies that $\theta_1 + \cdots + \theta_n = 0$. By Proposition 28.4,

$$f = h_{u_n - u_{n-1}} \circ h_{u_n - e^{-i(\theta_1 + \cdots + \theta_{n-1})} u_{n-1}} \circ \cdots \circ h_{u_2 - u_1} \circ h_{u_2 - e^{-i\theta_1} u_1},$$

a composition of $2n - 2$ hyperplane reflections. In general, if $f \in \mathbf{U}(n)$, by the remark after Theorem 28.2, f can be written as $f = \rho_\theta \circ g$, where $g \in \mathbf{SU}(n)$ is a rotation, and ρ_θ is a Hermitian reflection. We conclude by applying what we just proved to g. □

As a corollary of Theorem 28.5, the following interesting result can be shown (this is not hard, do it!). First, recall that a linear map $f \colon E \to E$ is *self-adjoint* (or *Hermitian*) iff $f = f^*$. Then, the subgroup of $\mathbf{U}(n)$ generated by the Hermitian isometries is equal to the group

$$\mathbf{SU}(n)^{\pm} = \{f \in \mathbf{U}(n) \mid \det(f) = \pm 1\}.$$

Equivalently, $\mathbf{SU}(n)^{\pm}$ is equal to the subgroup of $\mathbf{U}(n)$ generated by the hyperplane reflections.

This problem had been left open by Dieudonné in [50]. Evidently, it was settled since the publication of the third edition of the book [50].

Inspection of the proof of Proposition 27.4 reveals that this Proposition also holds for Hermitian spaces. Thus, when $n \geq 3$, the composition of any two hyperplane reflections is equal to the composition of two flips. As a consequence, a version of Theorem 27.5 holds for rotations in a Hermitian space of dimension at least 3.

Theorem 28.6. *Let E be a Hermitan space of dimension $n \geq 3$. Every rotation $f \in \mathbf{SU}(E)$ is the composition of an even number of flips $f = f_{2k} \circ \cdots \circ f_1$, where $k \leq n-1$. 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. It is identical to that of Theorem 27.5, except that it uses Theorem 28.5 instead of Theorem 27.1. The second part of the Proposition also holds, because if $u \neq 0$ is an eigenvector of f for 1, then u is one of the vectors in the orthonormal basis of eigenvectors used in 28.2. The details are left as an exercise. □

We now show that the QR-decomposition in terms of (complex) Householder matrices holds for complex matrices. We need the version of Proposition 28.1 and a trick at the end of the argument, but the proof is basically unchanged.

Proposition 28.7. *Let E be a nontrivial Hermitian space of dimension n. Given any orthonormal basis $(e_1, \ldots, e_n)$, for any n-tuple of vectors $(v_1, \ldots, v_n)$, there is a sequence of $n-1$ isometries $h_1, \ldots, h_{n-1}$, such that h_i is a hyperplane reflection or the identity, and if $(r_1, \ldots, r_n)$ are the vectors given by*

$$r_j = h_{n-1} \circ \cdots \circ h_2 \circ h_1(v_j) \quad 1 \leq j \leq n,$$

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, if we allow one more isometry h_n of the form

$$h_n = \rho_{e_n, \varphi_n} \circ \cdots \circ \rho_{e_1, \varphi_1}$$

after $h_1, \ldots, h_{n-1}$, we can ensure that the diagonal entries of R are nonnegative.

Proof. The proof is very similar to the proof of Proposition 13.3, but it needs to be modified a little bit since Proposition 28.1 is weaker than Proposition 13.2. We explain how to modify the induction step, leaving the base case and the rest of the proof as an exercise.

As in the proof of Proposition 13.3, the vectors $(e_1, \ldots, e_k)$ form a basis for the subspace denoted as U'_k, the vectors $(e_{k+1}, \ldots, e_n)$ form a basis for the subspace denoted as 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

$$r_{k+1,k+1} = \left\| u''_{k+1} \right\|, \quad \text{and} \quad e^{i\theta_{k+1}} |u''_{k+1} \cdot e_{k+1}| = u''_{k+1} \cdot e_{k+1}.$$

If $u''_{k+1} = e^{i\theta_{k+1}} r_{k+1,k+1}\, e_{k+1}$, we let $h_{k+1} = \mathrm{id}$. Otherwise, by Proposition 28.1, there is a unique hyperplane reflection h_{k+1} such that

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

where h_{k+1} is the reflection about the hyperplane H_{k+1} orthogonal to the vector

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

At the end of the induction, we have a triangular matrix R, but the diagonal entries $e^{i\theta_j} r_{j,j}$ of R may be complex. Letting

$$h_{n+1} = \rho_{e_n, -\theta_n} \circ \cdots \circ \rho_{e_1, -\theta_1},$$

we observe that the diagonal entries of the matrix of vectors

$$r'_j = h_{n+1} \circ h_n \circ \cdots \circ h_2 \circ h_1(v_j)$$

is triangular with nonnegative entries. □

Remark: For numerical stability, it is preferable to use $w_{k+1} = r_{k+1,k+1}\, e_{k+1} + e^{-i\theta_{k+1}} u''_{k+1}$ instead of $w_{k+1} = r_{k+1,k+1}\, e_{k+1} - e^{-i\theta_{k+1}} u''_{k+1}$. The effect of that choice is that the diagonal entries in R will be of the form $-e^{i\theta_j} r_{j,j} = e^{i(\theta_j+\pi)} r_{j,j}$. Of course, we can make these entries nonnegative by applying

$$h_{n+1} = \rho_{e_n,\pi-\theta_n} \circ \cdots \circ \rho_{e_1,\pi-\theta_1}$$

after h_n.

As in the Euclidean case, Proposition 28.7 immediately implies the QR-decomposition for arbitrary complex $n \times n$-matrices, where Q is now unitary (see Kincaid and Cheney [101], Golub and Van Loan [80], Trefethen and Bau [174], or Ciarlet [41]).

Proposition 28.8. *For every complex $n \times n$-matrix A, there is a sequence $H_1, \ldots, H_{n-1}$ of matrices, where each H_i is either a Householder matrix or the identity, and an upper triangular matrix R, such that*

$$R = H_{n-1} \cdots H_2 H_1 A.$$

As a corollary, there is a pair of matrices Q, R, where Q is unitary 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. This can be achieved by a diagonal matrix D with entries such that $|d_{ii}| = 1$ for $i = 1, \ldots, n$, and we have $A = \widetilde{Q}\widetilde{R}$ with

$$\widetilde{Q} = H_1 \cdots H_{n-1} D, \quad \widetilde{R} = D^* R,$$

where $\widetilde{R}$ is upper triangular and has nonnegative diagonal entries

Proof. It is essentially identical to the proof of Proposition 13.4, and we leave the details as an exercise. For the last statement, observe that $h_n \circ \cdots \circ h_1$ is also an isometry. □

As in the Euclidean case, the QR-decomposition has applications to least squares problems. It is also possible to convert any complex matrix to bidiagonal form.

28.2 Affine Isometries (Rigid Motions)

In this section, we study very briefly the affine isometries of a Hermitian space. Most results holding for Euclidean affine spaces generalize without any problems to Hermitian spaces.

The characterization of the set of fixed points of an affine map is unchanged. Similarly, every affine isometry f (of a Hermitian space) 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 Proposition 28.13). A generalization of the Cartan–Dieudonné theorem can easily be shown: every affine isometry in $\mathbf{Is}(n, \mathbb{C})$ can be written as the composition of at most $2n-1$ isometries if it has a fixed point, or else as the composition of at most $2n+1$ isometries, where all these isometries are affine hyperplane reflections except for possibly one affine Hermitian reflection. We also prove that every rigid motion in $\mathbf{SE}(n, \mathbb{C})$ is the composition of at most $2n-2$ flips (for $n \geq 3$).

Definition 28.2. Given any two nontrivial Hermitian 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)* iff it is an affine map and

$$\left\| \overrightarrow{f(a)f(b)} \right\| = \left\| \overrightarrow{ab} \right\|,$$

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, but unlike the Euclidean case, not strong enough to force f to be an affine map.

The following simple Proposition is left as an exercise.

Proposition 28.9. *Given any two nontrivial Hermitian 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.*

As in the Euclidean case, given an affine isometry $f\colon E \to E$, if $\overrightarrow{f}$ is a rotation, we call f a *proper (or direct) affine isometry*, and if $\overrightarrow{f}$ is a an improper linear isometry, we call f a *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 $\mathbf{GA}(E, \mathbb{C})$ denoted as $\mathbf{Is}(E, \mathbb{C})$ (or $\mathbf{Is}(n, \mathbb{C})$ when $E = \mathbb{C}^n$). The subgroup of $\mathbf{Is}(E, \mathbb{C})$ consisting of the direct rigid motions is also a subgroup of $\mathbf{SA}(E, \mathbb{C})$, and it is denoted as $\mathbf{SE}(E, \mathbb{C})$ (or $\mathbf{SE}(n, \mathbb{C})$, when $E = \mathbb{C}^n$). The translations are the affine isometries f for which $\overrightarrow{f} = \mathrm{id}$, the identity map on $\overrightarrow{E}$. The following Proposition is the counterpart of Proposition 14.14 for isometries between Hermitian vector spaces.

Proposition 28.10. *Given any two nontrivial Hermitian 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 $\left\| \overrightarrow{f(a)f(b)} \right\| = \left\| \overrightarrow{ab} \right\|$, for all $a, b \in E$.

(2) $\left\| \overrightarrow{f(a)f(b)} \right\| = \left\| \overrightarrow{ab} \right\|$, and there is some $\Omega \in E$ such that

$$f(\Omega + i\overrightarrow{ab}) = f(\Omega) + i(\overrightarrow{f(\Omega)f(\Omega + \overrightarrow{ab})}),$$

for all $a, b \in E$.

Proof. Obviously, (1) implies (2). The proof that that (2) implies (1) is similar to the proof of Proposition 27.7, but uses Proposition 14.14 instead of Proposition 12.12. The details are left as an exercise. □

Inspection of the proof shows immediately that Proposition 27.8 holds for Hermitian spaces. For the sake of completeness, we restate the Proposition in the complex case.

Proposition 28.11. *Let E be any complex affine space of finite dimension For every affine map $f\colon E \to E$, let $Fix(f) = \{a \in E \mid f(a) = a\}$ be the set of fixed points of f. The following properties hold:*

(1) If f has some fixed point a, so that $Fix(f) \neq \emptyset$, then $Fix(f)$ is an affine subspace of E such that
$$Fix(f) = a + E(1, \overrightarrow{f}) = a + \mathrm{Ker}\,(\overrightarrow{f} - \mathrm{id}),$$
where $E(1, \overrightarrow{f})$ is the eigenspace of the linear map $\overrightarrow{f}$ for the eigenvalue 1.

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

Affine orthogonal symmetries are defined just as in the Euclidean case, and Proposition 27.9 also applies to complex affine spaces.

Proposition 28.12. *Given any affine complex space E, if $f\colon E \to E$ and $g\colon E \to E$ are affine orthogonal symmetries about parallel affine subspaces F_1 and F_2, then $g \circ f$ is a translation defined by the vector $2\overrightarrow{ab}$, where $\overrightarrow{ab}$ is any vector perpendicular to the common direction $\overrightarrow{F}$ of F_1 and F_2 such that $\left\|\overrightarrow{ab}\right\|$ 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 affine orthogonal symmetries about parallel affine subspaces F_1 and F_2 whose common direction is orthogonal to $\tau = \overrightarrow{ab}$, for some $a \in F_1$ and some $b \in F_2$ such that the distance betwen F_1 and F_2 is $\left\|\overrightarrow{ab}\right\|/2$.*

It is easy to check that the proof of Proposition 27.10 also holds in the Hermitian case.

Proposition 28.13. *Let E be a Hermitian affine space of finite dimension n. For every affine isometry $f\colon E \to E$, there is a unique affine isometry $g\colon E \to E$ and a unique translation $t = t_\tau$, with $\overrightarrow{f}(\tau) = \tau$ (i.e., $\tau \in \mathrm{Ker}\,(\overrightarrow{f} - \mathrm{id})$), such that the set $Fix(g) = \{a \in E, \mid g(a) = a\}$ of fixed points of g is a nonempty affine subspace of E of direction*
$$\overrightarrow{G} = \mathrm{Ker}\,(\overrightarrow{f} - \mathrm{id}) = E(1, \overrightarrow{f}),$$
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 $Fix(f) \neq \emptyset$.*

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

The remarks made in the Euclidean case also apply to the Hermitian case. In particular, the fact that E has finite dimension is only used to prove (b).

A version of the Cartan–Dieudonné also holds for affine isometries, but it may not be possible to get rid of Hermitian reflections entirely.

Theorem 28.14. *Let E be an affine Hermitian space of dimension $n \geq 1$. Every affine isometry in $\mathbf{Is}(n, \mathbb{C})$ can be written as the composition of at most $2n - 1$ affine isometries if it has a fixed point, or else as the composition of at most $2n + 1$ affine isometries, where all these isometries are affine hyperplane reflections except for possibly one affine Hermitian reflection. When $n \geq 2$, the identity is the composition of any reflection with itself.*

Proof. The proof is very similar to the proof of Theorem 27.11, except that it uses Theorem 28.5 instead of Theorem 27.1. The details are left as an exercise. □

When $n \geq 3$, as in the Euclidean case, we can characterize the affine isometries in $\mathbf{SE}(n, \mathbb{C})$ in terms of flips, and we can even bound the number of flips by $2n - 2$.

Theorem 28.15. *Let E be a Hermitian affine space of dimension $n \geq 3$. Every rigid motion $f \in \mathbf{SE}(E, \mathbb{C})$ is the composition of an even number of affine flips $f = f_{2k} \circ \cdots \circ f_1$, where $k \leq n - 1$.*

Proof. It is very similar to the proof of theorem 27.12, but it uses Proposition 28.6 instead of Proposition 27.5. The details are left as an exercise. □

A more detailed study of the rigid motions of Hermitian spaces of dimension 2 and 3 would seem worthwhile, but we are not aware of any reference on this subject.

Chapter 29

The Geometry of Bilinear Forms; Witt's Theorem; The Cartan–Dieudonné Theorem

29.1 Bilinear Forms

In this chapter, we study the structure of a K-vector space E endowed with a nondegenerate bilinear form $\varphi\colon E \times E \to K$ (for any field K), which can be viewed as a kind of generalized inner product. Unlike the case of an inner product, there may be nonzero vectors $u \in E$ such that $\varphi(u, u) = 0$ so the map $u \mapsto \varphi(u, u)$ can no longer be interpreted as a notion of square length (also, $\varphi(u, u)$ may not be real and positive!). However, the notion of orthogonality survives: we say that $u, v \in E$ are orthogonal iff $\varphi(u, v) = 0$. Under some additional conditions on φ, it is then possible to split E into orthogonal subspaces having some special properties. It turns out that the special cases where φ is symmetric (or Hermitian) or skew-symmetric (or skew-Hermitian) can be handled uniformly using a deep theorem due to Witt (the Witt decomposition theorem (1936)).

We begin with the very general situation of a bilinear form $\varphi\colon E \times F \to K$, where K is an arbitrary field, possibly of characteristic 2. Actually, even though at first glance this may appear to be an uncessary abstraction, it turns out that this situation arises in attempting to prove properties of a bilinear map $\varphi\colon E \times E \to K$, because it may be necessary to restrict φ to different subspaces U and V of E. This general approach was pioneered by Chevalley [37], E. Artin [6], and Bourbaki [24]. The third source was a major source of inspiration, and many proofs are taken from it. Other useful references include Snapper and Troyer [160], Berger [12], Jacobson [97], Grove [83], Taylor [172], and Berndt [14].

Definition 29.1. Given two vector spaces E and F over a field K, a map $\varphi\colon E \times F \to K$ is a *bilinear form* iff the following conditions hold: For all $u, u_1, u_2 \in E$, all $v, v_1, v_2 \in F$, for all $\lambda, \mu \in K$, we have

$$\begin{aligned}\varphi(u_1 + u_2, v) &= \varphi(u_1, v) + \varphi(u_2, v)\\ \varphi(u, v_1 + v_2) &= \varphi(u, v_1) + \varphi(u, v_2)\\ \varphi(\lambda u, v) &= \lambda\varphi(u, v)\\ \varphi(u, \mu v) &= \mu\varphi(u, v).\end{aligned}$$

A bilinear form as in Definition 29.1 is sometimes called a *pairing*. The first two conditions imply that $\varphi(0, v) = \varphi(u, 0) = 0$ for all $u \in E$ and all $v \in F$.

If $E = F$, observe that

$$\begin{aligned}\varphi(\lambda u + \mu v, \lambda u + \mu v) &= \lambda\varphi(u, \lambda u + \mu v) + \mu\varphi(v, \lambda u + \mu v)\\ &= \lambda^2\varphi(u, u) + \lambda\mu\varphi(u, v) + \lambda\mu\varphi(v, u) + \mu^2\varphi(v, v).\end{aligned}$$

If we let $\lambda = \mu = 1$, we get

$$\varphi(u + v, u + v) = \varphi(u, u) + \varphi(u, v) + \varphi(v, u) + \varphi(v, v).$$

If φ is *symmetric*, which means that

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

then

$$2\varphi(u, v) = \varphi(u + v, u + v) - \varphi(u, u) - \varphi(v, v). \tag{$*$}$$

The function Φ defined such that

$$\Phi(u) = \varphi(u, u) \quad u \in E,$$

is called the *quadratic form* associated with φ. If the field K is not of characteristic 2, then φ is completely determined by its quadratic form Φ. The symmetric bilinear form φ is called the *polar form* of Φ. This suggests the following definition.

Definition 29.2. A function $\Phi\colon E \to K$ is a *quadratic form* on E if the following conditions hold:

(1) We have $\Phi(\lambda u) = \lambda^2\Phi(u)$, for all $u \in E$ and all $\lambda \in E$.

(2) The map φ' given by $\varphi'(u, v) = \Phi(u + v) - \Phi(u) - \Phi(v)$ is bilinear. Obviously, the map φ' is symmetric.

Since $\Phi(x + x) = \Phi(2x) = 4\Phi(x)$, we have

$$\varphi'(u, u) = 2\Phi(u) \quad u \in E.$$

If the field K is not of characteristic 2, then $\varphi = \frac{1}{2}\varphi'$ is the unique symmetric bilinear form such that that $\varphi(u, u) = \Phi(u)$ for all $u \in E$. The bilinear form $\varphi = \frac{1}{2}\varphi'$ is called the *polar form* of Φ. In this case, there is a bijection between the set of bilinear forms on E and the set of quadratic forms on E.

If K is a field of characteristic 2, then φ' is *alternating*, which means that

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

Thus if K is a field of characteristic 2, then Φ cannot be recovered from the symmetric bilinear form φ'.

If $(e_1, \ldots, e_n)$ is a basis of E, it is easy to show that

$$\Phi\Big(\sum_{i=1}^{n} \lambda_i e_i\Big) = \sum_{i=1}^{n} \lambda_i^2 \Phi(e_i) + \sum_{i \neq j} \lambda_i \lambda_j \varphi'(e_i, e_j).$$

This shows that the quadratic form Φ is completely determined by the scalars $\Phi(e_i)$ and $\varphi'(e_i, e_j)$ $(i \neq j)$. Furthermore, given any bilinear form $\psi \colon E \times E \to K$ (not necessarily symmetric) we can define a quadratic form Φ by setting $\Phi(x) = \psi(x, x)$, and we immediately check that the symmetric bilinear form φ' associated with Φ is given by $\varphi'(u, v) = \psi(u, v) + \psi(v, u)$. Using the above facts, it is not hard to prove that given any quadratic form Φ, there is some (nonsymmetric) bilinear form ψ such that $\Phi(u) = \psi(u, u)$ for all $u \in E$ (see Bourbaki [24], Section §3.4, Proposition 2). Thus, quadratic forms are more general than symmetric bilinear forms (except in characteristic $\neq 2$).

Definition 29.3. Given any bilinear form $\varphi \colon E \times E \to K$ where K is a field of any characteristic, we say that φ is *alternating* if

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

and *skew-symmetric* if

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

If K is a field of any characteristic, the identity

$$\varphi(u + v, u + v) = \varphi(u, u) + \varphi(u, v) + \varphi(v, u) + \varphi(v, v)$$

shows that if φ is alternating, then

$$\varphi(v, u) = -\varphi(u, v) \quad \text{for all } u, v \in E,$$

that is, φ is skew-symmetric. Conversely, if the field K is not of characteristic 2, then a skew-symmetric bilinear map is alternating, since $\varphi(u, u) = -\varphi(u, u)$ implies $\varphi(u, u) = 0$.

An important consequence of bilinearity is that a pairing yields a linear map from E into F^* and a linear map from F into E^* (where $E^* = \mathrm{Hom}_K(E, K)$, the *dual* of E, is the set of linear maps from E to K, called *linear forms*).

Definition 29.4. Given a bilinear map $\varphi\colon E \times F \to K$, for every $u \in E$, let $l_\varphi(u)$ be the linear form in F^* given by

$$l_\varphi(u)(y) = \varphi(u, y) \quad \text{for all } y \in F,$$

and for every $v \in F$, let $r_\varphi(v)$ be the linear form in E^* given by

$$r_\varphi(v)(x) = \varphi(x, v) \quad \text{for all } x \in E.$$

Because φ is bilinear, the maps $l_\varphi\colon E \to F^*$ and $r_\varphi\colon F \to E^*$ are linear.

Definition 29.5. A bilinear map $\varphi\colon E \times F \to K$ is said to be *nondegenerate* iff the following conditions hold:

(1) For every $u \in E$, if $\varphi(u, v) = 0$ for all $v \in F$, then $u = 0$, and

(2) For every $v \in F$, if $\varphi(u, v) = 0$ for all $u \in E$, then $v = 0$.

The following proposition shows the importance of l_φ and r_φ.

Proposition 29.1. *Given a bilinear map $\varphi\colon E \times F \to K$, the following properties hold:*

(a) The map l_φ is injective iff Property (1) of Definition 29.5 holds.

(b) The map r_φ is injective iff Property (2) of Definition 29.5 holds.

(c) The bilinear form φ is nondegenerate and iff l_φ and r_φ are injective.

(d) If the bilinear form φ is nondegenerate and if E and F have finite dimensions, then $\dim(E) = \dim(F)$, and $l_\varphi\colon E \to F^*$ and $r_\varphi\colon F \to E^*$ are linear isomorphisms.

Proof. (a) Assume that (1) of Definition 29.5 holds. If $l_\varphi(u) = 0$, then $l_\varphi(u)$ is the linear form whose value is 0 for all y; that is,

$$l_\varphi(u)(y) = \varphi(u, y) = 0 \quad \text{for all } y \in F,$$

and by (1) of Definition 29.5, we must have $u = 0$. Therefore, l_φ is injective. Conversely, if l_φ is injective, and if

$$l_\varphi(u)(y) = \varphi(u, y) = 0 \quad \text{for all } y \in F,$$

then $l_\varphi(u)$ is the zero form, and by injectivity of l_φ, we get $u = 0$; that is, (1) of Definition 29.5 holds.

(b) The proof is obtained by swapping the arguments of φ.

(c) This follows from (a) and (b).

(d) If E and F are finite dimensional, then $\dim(E) = \dim(E^*)$ and $\dim(F) = \dim(F^*)$. Since φ is nondegenerate, $l_\varphi\colon E \to F^*$ and $r_\varphi\colon F \to E^*$ are injective, so $\dim(E) \leq \dim(F^*) = \dim(F)$ and $\dim(F) \leq \dim(E^*) = \dim(E)$, which implies that

$$\dim(E) = \dim(F),$$

and thus, $l_\varphi\colon E \to F^*$ and $r_\varphi\colon F \to E^*$ are bijective. ∎

As a corollary of Proposition 29.1, we have the following characterization of a nondegenerate bilinear map. The proof is left as an exercise.

Proposition 29.2. *Given a bilinear map $\varphi\colon E \times F \to K$, if E and F have the same finite dimension, then the following properties are equivalent:*

(1) The map l_φ is injective.

(2) The map l_φ is surjective.

(3) The map r_φ is injective.

(4) The map r_φ is surjective.

(5) The bilinear form φ is nondegenerate.

Observe that in terms of the canonical pairing between E^* and E given by

$$\langle f, u\rangle = f(u), \quad f \in E^*, u \in E,$$

(and the canonical pairing between F^* and F), we have

$$\varphi(u, v) = \langle l_\varphi(u), v\rangle = \langle r_\varphi(v), u\rangle \quad u \in E, v \in F.$$

Proposition 29.3. *Given a bilinear map $\varphi\colon E \times F \to K$, if φ is nondegenerate and E and F are finite-dimensional, then* $\dim(E) = \dim(F) = n$, *and for every basis $(e_1, \ldots, e_n)$ of E, there is a basis $(f_1, \ldots, f_n)$ of F such that $\varphi(e_i, f_j) = \delta_{ij}$, for all $i, j = 1, \ldots, n$.*

Proof. Since φ is nondegenerate, by Proposition 29.1 we have $\dim(E) = \dim(F) = n$, and by Proposition 29.2, the linear map r_φ is bijective. Then, if $(e_1^*, \ldots, e_n^*)$ is the dual basis (in E^*) of the basis $(e_1, \ldots, e_n)$, the vectors $(f_1, \ldots, f_n)$ given by $f_i = r_\varphi^{-1}(e_i^*)$ form a basis of F, and we have

$$\varphi(e_i, f_j) = \langle r_\varphi(f_j), e_i\rangle = \langle e_i^*, e_j\rangle = \delta_{ij},$$

as claimed. □

If $E = F$ and φ is symmetric, then we have the following interesting result.

Theorem 29.4. *Given any bilinear form $\varphi\colon E \times E \to K$ with* $\dim(E) = n$, *if φ is symmetric (possibly degenerate) and K does not have characteristic* 2, *then there is a basis* $(e_1, \ldots, e_n)$ *of E such that $\varphi(e_i, e_j) = 0$, for all $i \neq j$.*

Proof. We proceed by induction on $n \geq 0$, following a proof due to Chevalley. The base case $n = 0$ is trivial. For the induction step, assume that $n \geq 1$ and that the induction hypothesis holds for all vector spaces of dimension $n - 1$. If $\varphi(u, v) = 0$ for all $u, v \in E$, then the statement holds trivially. Otherwise, since K does not have characteristic 2, equation

$$2\varphi(u, v) = \varphi(u + v, u + v) - \varphi(u, u) - \varphi(v, v) \tag{$*$}$$

show that there is some nonzero vector $e_1 \in E$ such that $\varphi(e_1, e_1) \neq 0$ since otherwise φ would vanish for all $u, v \in E$. We claim that the set

$$H = \{v \in E \mid \varphi(e_1, v) = 0\}$$

has dimension $n - 1$, and that $e_1 \notin H$.

This is because

$$H = \mathrm{Ker}\,(l_\varphi(e_1)),$$

where $l_\varphi(e_1)$ is the linear form in E^* determined by e_1. Since $\varphi(e_1, e_1) \neq 0$, we have $e_1 \notin H$, the linear form $l_\varphi(e_1)$ is not the zero form, and thus its kernel is a hyperplane H (a subspace of dimension $n - 1$). Since $\dim(H) = n - 1$ and $e_1 \notin H$, we have the direct sum

$$E = H \oplus Ke_1.$$

By the induction hypothesis applied to H, we get a basis $(e_2, \ldots, e_n)$ of vectors in H such that $\varphi(e_i, e_j) = 0$, for all $i \neq j$ with $2 \leq i, j \leq n$. Since $\varphi(e_1, v) = 0$ for all $v \in H$ and since φ is symmetric, we also have $\varphi(v, e_1) = 0$ for all $v \in H$, so we obtain a basis $(e_1, \ldots, e_n)$ of E such that $\varphi(e_i, e_j) = 0$, for all $i \neq j$. □

If E and F are finite-dimensional vector spaces and if $(e_1, \ldots, e_m)$ is a basis of E and $(f_1, \ldots, f_n)$ is a basis of F then the bilinearity of φ yields

$$\varphi\biggl(\sum_{i=1}^m x_i e_i, \sum_{j=1}^n y_j f_j\biggr) = \sum_{i=1}^m \sum_{j=1}^n x_i \varphi(e_i, f_j) y_j.$$

This shows that φ is completely determined by the $n \times m$ matrix $M = (m_{ij})$ with $m_{ij} = \varphi(e_j, f_i)$, and in matrix form, we have

$$\varphi(x, y) = x^\top M^\top y = y^\top M x,$$

where x and y are the column vectors associated with $(x_1, \ldots, x_m) \in K^m$ and $(y_1, \ldots, y_n) \in K^n$. As in Section 12.1, we are committing the slight abuse of notation of letting x denote both the vector $x = \sum_{i=1}^n x_i e_i$ and the column vector associated with $(x_1, \ldots, x_n)$ (and similarly for y).

Definition 29.6. If $(e_1, \ldots, e_m)$ is a basis of E and $(f_1, \ldots, f_n)$ is a basis of F, for any bilinear form $\varphi\colon E \times F \to K$, the $n \times m$ matrix $M = (m_{ij})$ given by $m_{ij} = \varphi(e_j, f_i)$ for $i = 1, \ldots, n$ and $j = 1, \ldots, m$ is called the *matrix of φ with respect to the bases* $(e_1, \ldots, e_m)$ *and* $(f_1, \ldots, f_n)$.

The following fact is easily proved.

Proposition 29.5. *If $m = \dim(E) = \dim(F) = n$, then φ is nondegenerate iff the matrix M is invertible iff* $\det(M) \neq 0$.

As we will see later, most bilinear forms that we will encounter are equivalent to one whose matrix is of the following form:

1. I_n, $-I_n$.

2. If $p + q = n$, with $p, q \geq 1$,
$$I_{p,q} = \begin{pmatrix} I_p & 0 \\ 0 & -I_q \end{pmatrix}$$

3. If $n = 2m$,
$$J_{m.m} = \begin{pmatrix} 0 & I_m \\ -I_m & 0 \end{pmatrix}$$

4. If $n = 2m$,
$$A_{m,m} = I_{m.m}J_{m.m} = \begin{pmatrix} 0 & I_m \\ I_m & 0 \end{pmatrix}.$$

If we make changes of bases given by matrices P and Q, so that $x = Px'$ and $y = Qy'$, then the new matrix expressing φ is $P^\top MQ$. In particular, if $E = F$ and the same basis is used, then the new matrix is $P^\top MP$. This shows that if φ is nondegenerate, then the determinant of φ is determined up to a square element.

Observe that if φ is a symmetric bilinear form ($E = F$) and if K does not have characteristic 2, then by Theorem 29.4, there is a basis of E with respect to which the matrix M representing φ is a diagonal matrix. If $K = \mathbb{R}$ or $K = \mathbb{C}$, this allows us to classify completely the symmetric bilinear forms. Recall that $\Phi(u) = \varphi(u, u)$ for all $u \in E$.

Proposition 29.6. *Given any bilinear form $\varphi\colon E \times E \to K$ with $\dim(E) = n$, if φ is symmetric and K does not have characteristic 2, then there is a basis $(e_1, \ldots, e_n)$ of E such that*
$$\Phi\biggl(\sum_{i=1}^n x_i e_i\biggr) = \sum_{i=1}^r \lambda_i x_i^2,$$
for some $\lambda_i \in K - \{0\}$ and with $r \leq n$. Furthermore, if $K = \mathbb{C}$, then there is a basis $(e_1, \ldots, e_n)$ of E such that
$$\Phi\biggl(\sum_{i=1}^n x_i e_i\biggr) = \sum_{i=1}^r x_i^2,$$
and if $K = \mathbb{R}$, then there is a basis $(e_1, \ldots, e_n)$ of E such that
$$\Phi\biggl(\sum_{i=1}^n x_i e_i\biggr) = \sum_{i=1}^p x_i^2 - \sum_{i=p+1}^{p+q} x_i^2,$$
with $0 \leq p, q$ and $p + q \leq n$.

Proof. The first statement is a direct consequence of Theorem 29.4. If $K = \mathbb{C}$, then every λ_i has a square root μ_i, and if replace e_i by e_i/μ_i, we obtained the desired form.

If $K = \mathbb{R}$, then there are two cases:

1. If $\lambda_i > 0$, let μ_i be a positive square root of λ_i and replace e_i by e_i/μ_i.
2. If $\lambda_i < 0$, et μ_i be a positive square root of $-\lambda_i$ and replace e_i by e_i/μ_i.

□

In the nondegenerate case, the matrices corresponding to the complex and the real case are, $I_n, -I_n$, and $I_{p,q}$. Observe that the second statement of Proposition 29.6 holds in any field in which every element has a square root. In the case $K = \mathbb{R}$, we can show that(p, q) only depends on φ.

Definition 29.7. Let $\varphi\colon E \times E \to \mathbb{R}$ be any symmetric real bilinear form. For any subspace U of E, we say that φ is *positive definite on* U iff $\varphi(u, u) > 0$ for all nonzero $u \in U$, and we say that φ is *negative definite on* U iff $\varphi(u, u) < 0$ for all nonzero $u \in U$. Then, let

$$r = \max\{\dim(U) \mid U \subseteq E,\ \varphi \text{ is positive definite on } U\}$$

and let

$$s = \max\{\dim(U) \mid U \subseteq E,\ \varphi \text{ is negative definite on } U\}$$

Proposition 29.7. *(Sylvester's inertia law) Given any symmetric bilinear form $\varphi\colon E\times E \to \mathbb{R}$ with $\dim(E) = n$, for any basis $(e_1, \ldots, e_n)$ of E such that*

$$\Phi\left(\sum_{i=1}^{n} x_i e_i\right) = \sum_{i=1}^{p} x_i^2 - \sum_{i=p+1}^{p+q} x_i^2,$$

with $0 \leq p, q$ and $p + q \leq n$, the integers p, q depend only on φ; in fact, $p = r$ and $q = s$, with r and s as defined above.

Proof. If we let U be the subspace spanned by $(e_1, \ldots, e_p)$, then φ is positive definite on U, so $r \geq p$. Similarly, if we let V be the subspace spanned by $(e_{p+1}, \ldots, e_{p+q})$, then φ is negative definite on V, so $s \geq q$.

Next, if W_1 is any subspace of maximum dimension such that φ is positive definite on W_1, and if we let V' be the subspace spanned by $(e_{p+1}, \ldots, e_n)$, then $\varphi(u, u) \leq 0$ on V', so $W_1 \cap V' = (0)$, which implies that $\dim(W_1) + \dim(V') \leq n$, and thus, $r + n - p \leq n$; that is, $r \leq p$. Similarly, if W_2 is any subspace of maximum dimension such that φ is negative definite on W_2, and if we let U' be the subspace spanned by $(e_1, \ldots, e_p, e_{p+q+1}, \ldots, e_n)$, then $\varphi(u, u) \geq 0$ on U', so $W_2 \cap U' = (0)$, which implies that $s + n - q \leq n$; that is, $s \leq q$. Therefore, $p = r$ and $q = s$, as claimed □

These last two results can be generalized to ordered fields. For example, see Snapper and Troyer [160], Artin [6], and Bourbaki [24].

29.2 Sesquilinear Forms

In order to accomodate Hermitian forms, we assume that some involutive automorphism, $\lambda \mapsto \overline{\lambda}$, of the field K is given. This automorphism of K satisfies the following properties:

$$\begin{aligned}\overline{(\lambda + \mu)} &= \overline{\lambda} + \overline{\mu}\\ \overline{(\lambda\mu)} &= \overline{\lambda}\,\overline{\mu}\\ \overline{\overline{\lambda}} &= \lambda.\end{aligned}$$

Since any field automorphism maps the multiplicative unit 1 to itself, we have $\overline{1} = 1$.

If the automorphism $\lambda \mapsto \overline{\lambda}$ is the identity, then we are in the standard situation of a bilinear form. When $K = \mathbb{C}$ (the complex numbers), then we usually pick the automorphism of $\mathbb{C}$ to be *conjugation*; namely, the map

$$a + ib \mapsto a - ib.$$

Definition 29.8. Given two vector spaces E and F over a field K with an involutive automorphism $\lambda \mapsto \overline{\lambda}$, a map $\varphi\colon E \times F \to K$ is a (right) *sesquilinear form* iff the following conditions hold: For all $u, u_1, u_2 \in E$, all $v, v_1, v_2 \in F$, for all $\lambda, \mu \in K$, we have

$$\begin{aligned}\varphi(u_1 + u_2, v) &= \varphi(u_1, v) + \varphi(u_2, v)\\ \varphi(u, v_1 + v_2) &= \varphi(u, v_1) + \varphi(u, v_2)\\ \varphi(\lambda u, v) &= \lambda\varphi(u, v)\\ \varphi(u, \mu v) &= \overline{\mu}\varphi(u, v).\end{aligned}$$

Again, $\varphi(0, v) = \varphi(u, 0) = 0$. If $E = F$, then we have

$$\begin{aligned}\varphi(\lambda u + \mu v, \lambda u + \mu v) &= \lambda\varphi(u, \lambda u + \mu v) + \mu\varphi(v, \lambda u + \mu v)\\ &= \lambda\overline{\lambda}\varphi(u, u) + \lambda\overline{\mu}\varphi(u, v) + \overline{\lambda}\mu\varphi(v, u) + \mu\overline{\mu}\varphi(v, v).\end{aligned}$$

If we let $\lambda = \mu = 1$ and then $\lambda = 1, \mu = -1$, we get

$$\begin{aligned}\varphi(u + v, u + v) &= \varphi(u, u) + \varphi(u, v) + \varphi(v, u) + \varphi(v, v)\\ \varphi(u - v, u - v) &= \varphi(u, u) - \varphi(u, v) - \varphi(v, u) + \varphi(v, v),\end{aligned}$$

so by subtraction, we get

$$2(\varphi(u, v) + \varphi(v, u)) = \varphi(u + v, u + v) - \varphi(u - v, u - v) \quad \text{for } u, v \in E.$$

If we replace v by λv (with $\lambda \neq 0$), we get

$$2(\overline{\lambda}\varphi(u, v) + \lambda\varphi(v, u)) = \varphi(u + \lambda v, u + \lambda v) - \varphi(u - \lambda v, u - \lambda v),$$

and by combining the above two equations, we get

$$\begin{aligned} 2(\lambda - \overline{\lambda})\varphi(u, v) &= \lambda\varphi(u + v, u + v) - \lambda\varphi(u - v, u - v) \\ &\quad - \varphi(u + \lambda v, u + \lambda v) + \varphi(u - \lambda v, u - \lambda v). \end{aligned} \tag{$*$}$$

If the automorphism $\lambda \mapsto \overline{\lambda}$ is not the identity, then there is some $\lambda \in K$ such that $\lambda - \overline{\lambda} \neq 0$, and if K is not of characteristic 2, then we see that the sesquilinear form φ is completely determined by its restriction to the diagonal (that is, the set of values $\{\varphi(u, u) \mid u \in E\}$). In the special case where $K = \mathbb{C}$, we can pick $\lambda = i$, and we get

$$4\varphi(u, v) = \varphi(u + v, u + v) - \varphi(u - v, u - v) + i\varphi(u + \lambda v, u + \lambda v) - i\varphi(u - \lambda v, u - \lambda v).$$

Remark: If the automorphism $\lambda \mapsto \overline{\lambda}$ is the identity, then in general φ is not determined by its value on the diagonal, unless φ is symmetric.

In the sesquilinear setting, it turns out that the following two cases are of interest:

1. We have
$$\varphi(v, u) = \overline{\varphi(u, v)}, \quad \text{for all } u, v \in E,$$
in which case we say that φ is *Hermitian*. In the special case where $K = \mathbb{C}$ and the involutive automorphism is conjugation, we see that $\varphi(u, u) \in \mathbb{R}$, for $u \in E$.

2. We have
$$\varphi(v, u) = -\overline{\varphi(u, v)}, \quad \text{for all } u, v \in E,$$
in which case we say that φ is *skew-Hermitian*.

We observed that in characteristic different from 2, a sesquilinear form is determined by its restriction to the diagonal. For Hermitian and skew-Hermitian forms, we have the following kind of converse.

Proposition 29.8. *If φ is a nonzero Hermitian or skew-Hermitian form and if $\varphi(u, u) = 0$ for all $u \in E$, then K is of characteristic 2 and the automorphism $\lambda \mapsto \overline{\lambda}$ is the identity.*

Proof. We give the proof in the Hermitian case, the skew-Hermitian case being left as an exercise. Assume that φ is alternating. From the identity

$$\varphi(u + v, u + v) = \varphi(u, u) + \varphi(u, v) + \overline{\varphi(u, v)} + \varphi(v, v),$$

we get

$$\varphi(u, v) = -\overline{\varphi(u, v)} \quad \text{for all } u, v \in E.$$

Since φ is not the zero form, there exist some nonzero vectors $u, v \in E$ such that $\varphi(u, v) = 1$. For any $\lambda \in K$, we have

$$\lambda\varphi(u, v) = \varphi(\lambda u, v) = -\overline{\varphi(\lambda u, v)} = -\overline{\lambda}\,\overline{\varphi(u, v)},$$

and since $\varphi(u, v) = 1$, we get

$$\lambda = -\overline{\lambda} \quad \text{for all } \lambda \in K.$$

For $\lambda = 1$, we get $1 = -1$, which means that K has characterictic 2. But then

$$\lambda = -\overline{\lambda} = \overline{\lambda} \quad \text{for all } \lambda \in K,$$

so the automorphism $\lambda \mapsto \overline{\lambda}$ is the identity. □

The definition of the linear maps l_φ and r_φ requires a small twist due to the automorphism $\lambda \mapsto \overline{\lambda}$.

Definition 29.9. Given a vector space E over a field K with an involutive automorphism $\lambda \mapsto \overline{\lambda}$, we define the K-vector space $\overline{E}$ as E with its abelian group structure, but with scalar multiplication given by

$$(\lambda, u) \mapsto \overline{\lambda}u.$$

Given two K-vector spaces E and F, a *semilinear map* $f\colon E \to F$ is a function, such that for all $u, v \in E$, for all $\lambda \in K$, we have

$$\begin{aligned} f(u + v) &= f(u) + f(v) \\ f(\lambda u) &= \overline{\lambda} f(u). \end{aligned}$$

Because $\overline{\overline{\lambda}} = \lambda$, observe that a function $f\colon E \to F$ is semilinear iff it is a linear map $f\colon \overline{E} \to F$. The K-vector spaces E and $\overline{E}$ are isomorphic, since any basis $(e_i)_{i\in I}$ of E is also a basis of $\overline{E}$.

The maps l_φ and r_φ are defined as follows:

For every $u \in E$, let $l_\varphi(u)$ be the linear form in F^* defined so that

$$l_\varphi(u)(y) = \overline{\varphi(u, y)} \quad \text{for all } y \in F,$$

and for every $v \in F$, let $r_\varphi(v)$ be the linear form in E^* defined so that

$$r_\varphi(v)(x) = \varphi(x, v) \quad \text{for all } x \in E.$$

The reader should check that because we used $\overline{\varphi(u, y)}$ in the definition of $l_\varphi(u)(y)$, the function $l_\varphi(u)$ is indeed a linear form in F^*. It is also easy to check that l_φ is a linear map $l_\varphi\colon \overline{E} \to F^*$, and that r_φ is a linear map $r_\varphi\colon \overline{F} \to E^*$ (equivalently, $l_\varphi\colon E \to F^*$ and $r_\varphi\colon F \to E^*$ are semilinear).

The notion of a nondegenerate sesquilinear form is identical to the notion for bilinear forms. For the convenience of the reader, we repeat the definition.

Definition 29.10. A sesquilinear map $\varphi\colon E \times F \to K$ is said to be *nondegenerate* iff the following conditions hold:

(1) For every $u \in E$, if $\varphi(u, v) = 0$ for all $v \in F$, then $u = 0$, and

(2) For every $v \in F$, if $\varphi(u, v) = 0$ for all $u \in E$, then $v = 0$.

Proposition 29.1 translates into the following proposition. The proof is left as an exercise.

Proposition 29.9. *Given a sesquilinear map $\varphi\colon E \times F \to K$, the following properties hold:*

(a) The map l_φ is injective iff Property (1) of Definition 29.10 holds.

(b) The map r_φ is injective iff Property (2) of Definition 29.10 holds.

(c) The sesquilinear form φ is nondegenerate and iff l_φ and r_φ are injective.

(d) If the sesquillinear form φ is nondegenerate and if E and F have finite dimensions, then $\dim(E) = \dim(F)$, and $l_\varphi\colon \overline{E} \to F^*$ and $r_\varphi\colon \overline{F} \to E^*$ are linear isomorphisms.

Propositions 29.2 and 29.3 also generalize to sesquilinear forms. We also have the following version of Theorem 29.4, whose proof is left as an exercise.

Theorem 29.10. *Given any sesquilinear form $\varphi\colon E \times E \to K$ with $\dim(E) = n$, if φ is Hermitian and K does not have characteristic 2, then there is a basis $(e_1, \ldots, e_n)$ of E such that $\varphi(e_i, e_j) = 0$, for all $i \neq j$.*

As in Section 29.1, if E and F are finite-dimensional vector spaces and if $(e_1, \ldots, e_m)$ is a basis of E and $(f_1, \ldots, f_n)$ is a basis of F then the sesquilinearity of φ yields

$$\varphi\Big(\sum_{i=1}^m x_i e_i, \sum_{j=1}^n y_j f_j\Big) = \sum_{i=1}^m \sum_{j=1}^n x_i \varphi(e_i, f_j) \overline{y}_j.$$

This shows that φ is completely determined by the $n \times m$ matrix $M = (m_{ij})$ with $m_{ij} = \varphi(e_j, f_i)$, and in matrix form, we have

$$\varphi(x, y) = x^\top M^\top \overline{y} = y^* M x,$$

where x and $\overline{y}$ are the column vectors associated with $(x_1, \ldots, x_m) \in K^m$ and $(\overline{y}_1, \ldots, \overline{y}_n) \in K^n$, and $y^* = \overline{y}^\top$. As earlier, we are committing the slight abuse of notation of letting x denote both the vector $x = \sum_{i=1}^n x_i e_i$ and the column vector associated with $(x_1, \ldots, x_n)$ (and similarly for y).

Definition 29.11. If $(e_1, \ldots, e_m)$ is a basis of E and $(f_1, \ldots, f_n)$ is a basis of F, for any sesquilinear form $\varphi\colon E \times F \to K$, the $n \times m$ matrix $M = (m_{ij})$ given by $m_{ij} = \varphi(e_j, f_i)$ for $i = 1, \ldots, n$ and $j = 1, \ldots, m$ is called the *matrix of φ with respect to the bases $(e_1, \ldots, e_m)$ and $(f_1, \ldots, f_n)$.*

Proposition 29.5 also holds for sesquilinear forms and their matrix representations.

Observe that if φ is a Hermitian form ($E = F$) and if K does not have characteristic 2, then by Theorem 29.10, there is a basis of E with respect to which the matrix M representing φ is a diagonal matrix. If $K = \mathbb{C}$, then these entries are real, and this allows us to classify completely the Hermitian forms.

Proposition 29.11. *Given any Hermitian form $\varphi\colon E \times E \to \mathbb{C}$ with $\dim(E) = n$, there is a basis $(e_1, \ldots, e_n)$ of E such that*

$$\Phi\biggl(\sum_{i=1}^{n} x_i e_i\biggr) = \sum_{i=1}^{p} x_i^2 - \sum_{i=p+1}^{p+q} x_i^2,$$

with $0 \leq p, q$ and $p + q \leq n$.

The proof of Proposition 29.11 is the same as the real case of Proposition 29.6. Sylvester's inertia law (Proposition 29.7) also holds for Hermitian forms: p and q only depend on φ.

29.3 Orthogonality

In this section we assume that we are dealing with a sesquilinear form $\varphi\colon E \times F \to K$. We allow the automorphism $\lambda \mapsto \overline{\lambda}$ to be the identity, in which case φ is a bilinear form. This way, we can deal with properties shared by bilinear forms and sesquilinear forms in a uniform fashion. Orthogonality is such a property.

Definition 29.12. Given a sesquilinear form $\varphi\colon E \times F \to K$, we say that two vectors $u \in E$ and $v \in F$ are *orthogonal* (or *conjugate*) if $\varphi(u, v) = 0$. Two subsets $E' \subseteq E$ and $F' \subseteq F$ are *orthogonal* if $\varphi(u, v) = 0$ for all $u \in E'$ and all $v \in F'$. Given a subspace U of E, the *right orthogonal space* of U, denoted $U^{\perp}$, is the subspace of F given by

$$U^{\perp} = \{v \in F \mid \varphi(u, v) = 0 \quad \text{for all } u \in U\},$$

and given a subspace V of F, the *left orthogonal space* of V, denoted $V^{\perp}$, is the subspace of E given by

$$V^{\perp} = \{u \in E \mid \varphi(u, v) = 0 \quad \text{for all } v \in V\}.$$

When E and F are distinct, there is little chance of confusing the right orthogonal subspace $U^{\perp}$ of a subspace U of E and the left orthogonal subspace $V^{\perp}$ of a subspace V of F. However, if $E = F$, then $\varphi(u, v) = 0$ *does not necessarily imply* that $\varphi(v, u) = 0$, that is, orthogonality is not necessarily symmetric. Thus, if both U and V are subsets of E, there is a notational ambiguity if $U = V$. In this case, we may write $U^{\perp_r}$ for the right orthogonal and $U^{\perp_l}$ for the left orthogonal.

The above discussion brings up the following point: When is orthogonality symmetric?

If φ is bilinear, it is shown in E. Artin [6] (and in Jacobson [97]) that orthogonality is symmetric iff either φ is symmetric or φ is alternating ($\varphi(u, u) = 0$ for all $u \in E$).

If φ is sesquilinear, the answer is more complicated. In addition to the previous two cases, there is a third possibility:

$$\varphi(u, v) = \epsilon\overline{\varphi(v, u)} \quad \text{for all } u, v \in E,$$

where ϵ is some nonzero element in K. We say that φ is *ϵ-Hermitian*. Observe that

$$\varphi(u, u) = \epsilon\overline{\epsilon}\varphi(u, u),$$

so if φ is not alternating, then $\varphi(u, u) \neq 0$ for some u, and we must have $\epsilon\overline{\epsilon} = 1$. The most common cases are

1. $\epsilon = 1$, in which case φ is *Hermitian*, and

2. $\epsilon = -1$, in which case φ is *skew-Hermitian*.

If φ is alternating and K is not of characteristic 2, then equation $(*)$ from Section 29.2 implies that the automorphism $\lambda \mapsto \overline{\lambda}$ must be the identity if φ is nonzero. If so, φ is skew-symmetric, so $\epsilon = -1$.

In summary, if φ is either symmetric, alternating, or ϵ-Hermitian, then orthogonality is symmetric, and it makes sense to talk about *the* orthogonal subspace $U^{\perp}$ of U.

Observe that if φ is ϵ-Hermitian, then

$$r_{\varphi} = \epsilon l_{\varphi}.$$

This is because

$$\begin{aligned} l_{\varphi}(u)(y) &= \overline{\varphi(u, y)} \\ r_{\varphi}(u)(y) &= \varphi(y, u) \\ &= \epsilon\overline{\varphi(u, y)}, \end{aligned}$$

so $r_{\varphi} = \epsilon l_{\varphi}$.

If E and F are finite-dimensional with bases $(e_1, \ldots, e_m)$ and $(f_1, \ldots, f_n)$, and if φ is represented by the $n \times m$ matrix M, then φ is ϵ-Hermitian iff

$$M = \epsilon M^*,$$

where $M^* = (\overline{M})^{\top}$ (as usual). This captures the following kinds of familiar matrices:

1. Symmetric matrices ($\epsilon = 1$)

2. Skew-symmetric matrices ($\epsilon = -1$)

3. Hermitian matrices ($\epsilon = 1$)

4. Skew-Hermitian matrices ($\epsilon = -1$).

Going back to a sesquilinear form $\varphi\colon E \times F \to K$, for any subspace U of E, it is easy to check that

$$U \subseteq (U^{\perp})^{\perp},$$

and that for any subspace V of F, we have

$$V \subseteq (V^{\perp})^{\perp}.$$

For simplicity of notation, we write $U^{\perp\perp}$ instead of $(U^{\perp})^{\perp}$ (and $V^{\perp\perp}$ instead of $(V^{\perp})^{\perp}$).

Given any two subspaces U_1 and U_2 of E, if $U_1 \subseteq U_2$, then $U_2^{\perp} \subseteq U_1^{\perp}$. Indeed, if $v \in U_2^{\perp}$ then $\varphi(u_2, v) = 0$ for all $u_2 \in U_2$, and since $U_1 \subseteq U_2$ this implies that $\varphi(u_1, v) = 0$ for all $u_1 \in U_1$, which shows that $v \in U_1^{\perp}$. Similarly for any two subspaces V_1, V_2 of F, if $V_1 \subseteq V_2$, then $V_2^{\perp} \subseteq V_1^{\perp}$. As a consequence,

$$U^{\perp} = U^{\perp\perp\perp}, \quad V^{\perp} = V^{\perp\perp\perp}.$$

First, we have $U^{\perp} \subseteq U^{\perp\perp\perp}$. Second, from $U \subseteq U^{\perp\perp}$, we get $U^{\perp\perp\perp} \subseteq U^{\perp}$, so $U^{\perp} = U^{\perp\perp\perp}$. The other equation is proved is a similar way.

Observe that φ is nondegenerate iff $E^{\perp} = \{0\}$ and $F^{\perp} = \{0\}$. Furthermore, since

$$\begin{aligned}
\varphi(u + x, v) &= \varphi(u, v)\\
\varphi(u, v + y) &= \varphi(u, v)
\end{aligned}$$

for any $x \in F^{\perp}$ and any $y \in E^{\perp}$, we see that we obtain by passing to the quotient a sesquilinear form

$$[\varphi]\colon (E/F^{\perp}) \times (F/E^{\perp}) \to K$$

which is nondegenerate.

Proposition 29.12. *For any sesquilinear form $\varphi\colon E \times F \to K$, the space $E/F^{\perp}$ is finite-dimensional iff the space $F/E^{\perp}$ is finite-dimensional; if so,* $\dim(E/F^{\perp}) = \dim(F/E^{\perp})$.

Proof. Since the sesquilinear form $[\varphi]\colon (E/F^{\perp}) \times (F/E^{\perp}) \to K$ is nondegenerate, the maps $l_{[\varphi]}\colon \overline{(E/F^{\perp})} \to (F/E^{\perp})^*$ and $r_{[\varphi]}\colon \overline{(F/E^{\perp})} \to (E/F^{\perp})^*$ are injective. If $\dim(E/F^{\perp}) = m$, then $\dim(E/F^{\perp}) = \dim((E/F^{\perp})^*)$, so by injectivity of $r_{[\varphi]}$, we have $\dim(F/E^{\perp}) = \dim(\overline{(F/E^{\perp})}) \leq m$. A similar reasoning using the injectivity of $l_{[\varphi]}$ applies if $\dim(F/E^{\perp}) = n$, and we get $\dim(E/F^{\perp}) = \dim(\overline{(E/F^{\perp})}) \leq n$. Therefore, $\dim(E/F^{\perp}) = m$ is finite iff $\dim(F/E^{\perp}) = n$ is finite, in which case $m = n$ by Proposition 29.1(d). □

If U is a subspace of a space E, recall that the *codimension* of U is the dimension of E/U, which is also equal to the dimension of any subspace V such that E is a direct sum of U and V ($E = U \oplus V$).

Proposition 29.12 implies the following useful fact.

Proposition 29.13. *Let $\varphi\colon E \times F \to K$ be any nondegenerate sesquilinear form. A subspace U of E has finite dimension iff $U^{\perp}$ has finite codimension in F. If $\dim(U)$ is finite, then $\operatorname{codim}(U^{\perp}) = \dim(U)$, and $U^{\perp\perp} = U$.*

Proof. Since φ is nondegenerate $E^{\perp} = \{0\}$ and $F^{\perp} = \{0\}$, so Proposition 29.12 applied to the restriction of φ to $U \times F$ implies that a subspace U of E has finite dimension iff $U^{\perp}$ has finite codimension in F, and that if $\dim(U)$ is finite, then $\operatorname{codim}(U^{\perp}) = \dim(U)$. Since $U^{\perp}$ and $U^{\perp\perp}$ are orthogonal, and since $\operatorname{codim}(U^{\perp})$ is finite, $\dim(U^{\perp\perp})$ is finite and we have $\dim(U^{\perp\perp}) = \operatorname{codim}(U^{\perp\perp\perp}) = \operatorname{codim}(U^{\perp}) = \dim(U)$. Since $U \subseteq U^{\perp\perp}$, we must have $U = U^{\perp\perp}$. □

Proposition 29.14. *Let $\varphi\colon E \times F \to K$ be any sesquilinear form. Given any two subspaces U and V of E, we have*

$$(U + V)^{\perp} = U^{\perp} \cap V^{\perp}.$$

Furthermore, if φ is nondegenerate and if U and V are finite-dimensional, then

$$(U \cap V)^{\perp} = U^{\perp} + V^{\perp}.$$

Proof. If $w \in (U + V)^{\perp}$, then $\varphi(u + v, w) = 0$ for all $u \in U$ and all $v \in V$. In particular, with $v = 0$, we have $\varphi(u, w) = 0$ for all $u \in U$, and with $u = 0$, we have $\varphi(v, w) = 0$ for all $v \in V$, so $w \in U^{\perp} \cap V^{\perp}$. Conversely, if $w \in U^{\perp} \cap V^{\perp}$, then $\varphi(u, w) = 0$ for all $u \in U$ and $\varphi(v, w) = 0$ for all $v \in V$. By bilinearity, $\varphi(u + v, w) = \varphi(u, w) + \varphi(v, w) = 0$, which shows that $w \in (U + V)^{\perp}$. Therefore, the first identity holds.

Now, assume that φ is nondegenerate and that U and V are finite-dimensional, and let $W = U^{\perp} + V^{\perp}$. Using the equation that we just established and the fact that U and V are finite-dimensional, by Proposition 29.13, we get

$$W^{\perp} = U^{\perp\perp} \cap V^{\perp\perp} = U \cap V.$$

We can apply Proposition 29.12 to the restriction of φ to $U \times W$ (since $U^{\perp} \subseteq W$ and $W^{\perp} \subseteq U$), and we get

$$\dim(U/W^{\perp}) = \dim(U/(U \cap V)) = \dim(W/U^{\perp}).$$

If T is a supplement of $U^{\perp}$ in W so that $W = U^{\perp} \oplus T$ and if S is a supplement of W in E so that $E = W \oplus S$, then $\operatorname{codim}(W) = \dim(S)$, $\dim(T) = \dim(W/U^{\perp})$, and we have the direct sum

$$E = U^{\perp} \oplus T \oplus S$$

which implies that

$$\dim(T) = \operatorname{codim}(U^{\perp}) - \dim(S) = \operatorname{codim}(U^{\perp}) - \operatorname{codim}(W)$$

so

$$\dim(U/(U \cap V)) = \dim(W/U^{\perp}) = \operatorname{codim}(U^{\perp}) - \operatorname{codim}(W),$$

and since $\operatorname{codim}(U^{\perp}) = \dim(U)$, we deduce that

$$\dim(U \cap V) = \operatorname{codim}(W).$$

However, by Proposition 29.13, we have $\dim(U \cap V) = \operatorname{codim}((U \cap V)^{\perp})$, so $\operatorname{codim}(W) = \operatorname{codim}((U \cap V)^{\perp})$, and since $W \subseteq W^{\perp\perp} = (U \cap V)^{\perp}$, we must have $W = (U \cap V)^{\perp}$, as claimed. □

In view of Proposition 29.12, we can make the following definition.

Definition 29.13. Let $\varphi\colon E \times F \to K$ be any sesquilinear form. If $E/F^{\perp}$ and $F/E^{\perp}$ are finite-dimensional, then their common dimension is called the *rank* of the form φ. If $E/F^{\perp}$ and $F/E^{\perp}$ have infinite dimension, we say that φ has infinite rank.

Not surprisingly, the rank of φ is related to the ranks of l_{φ} and r_{φ}.

Proposition 29.15. *Let $\varphi\colon E \times F \to K$ be any sesquilinear form. If φ has finite rank r, then l_{φ} and r_{φ} have the same rank, which is equal to r.*

Proof. Because for every $u \in E$,

$$l_{\varphi}(u)(y) = \overline{\varphi(u, y)} \quad \text{for all } y \in F,$$

and for every $v \in F$,

$$r_{\varphi}(v)(x) = \varphi(x, v) \quad \text{for all } x \in E,$$

it is clear that the kernel of $l_{\varphi}\colon \overline{E} \to F^*$ is equal to $F^{\perp}$ and that, the kernel of $r_{\varphi}\colon \overline{F} \to E^*$ is equal to $E^{\perp}$. Therefore, $\operatorname{rank}(l_{\varphi}) = \dim(\operatorname{Im} l_{\varphi}) = \dim(E/F^{\perp}) = r$, and similarly $\operatorname{rank}(r_{\varphi}) = \dim(F/E^{\perp}) = r$. □

Remark: If the sesquilinear form φ is represented by the matrix $n \times m$ matrix M with respect to the bases $(e_1, \ldots, e_m)$ in E and $(f_1, \ldots, f_n)$ in F, it can be shown that the matrix representing l_{φ} with respect to the bases $(e_1, \ldots, e_m)$ and $(f_1^*, \ldots, f_n^*)$ is $\overline{M}$, and that the matrix representing r_{φ} with respect to the bases $(f_1, \ldots, f_n)$ and $(e_1^*, \ldots, e_m^*)$ is $M^{\top}$. It follows that the rank of φ is equal to the rank of M.

29.4 Adjoint of a Linear Map

Let E_1 and E_2 be two K-vector spaces, and let $\varphi_1\colon E_1 \times E_1 \to K$ be a sesquilinear form on E_1 and $\varphi_2\colon E_2 \times E_2 \to K$ be a sesquilinear form on E_2. It is also possible to deal with the more general situation where we have four vector spaces E_1, F_1, E_2, F_2 and two sesquilinear forms $\varphi_1\colon E_1 \times F_1 \to K$ and $\varphi_2\colon E_2 \times F_2 \to K$, but we will leave this generalization as an exercise. We also assume that l_{φ_1} and r_{φ_1} are bijective, which implies that that φ_1 is nondegenerate. This is automatic if the space E_1 is finite dimensional and φ_1 is nondegenerate.

Given any linear map $f\colon E_1 \to E_2$, for any fixed $u \in E_2$, we can consider the linear form in E_1^* given by

$$x \mapsto \varphi_2(f(x), u), \quad x \in E_1.$$

Since $r_{\varphi_1}\colon \overline{E_1} \to E_1^*$ is bijective, there is a unique $y \in E_1$ (because the vector spaces E_1 and $\overline{E_1}$ only differ by scalar multiplication), so that

$$\varphi_2(f(x), u) = \varphi_1(x, y), \quad \text{for all } x \in E_1.$$

If we denote this unique $y \in E_1$ by $f^{*l}(u)$, then we have

$$\varphi_2(f(x), u) = \varphi_1(x, f^{*l}(u)), \quad \text{for all } x \in E_1, \text{ and all } u \in E_2.$$

Thus, we get a function $f^{*l}\colon E_2 \to E_1$. We claim that this function is a linear map. For any $v_1, v_2 \in E_2$, we have

$$\begin{aligned}
\varphi_2(f(x), v_1 + v_2) &= \varphi_2(f(x), v_1) + \varphi_2(f(x), v_2) \\
&= \varphi_1(x, f^{*l}(v_1)) + \varphi_1(x, f^{*l}(v_2)) \\
&= \varphi_1(x, f^{*l}(v_1) + f^{*l}(v_2)) \\
&= \varphi_1(x, f^{*l}(v_1 + v_2)),
\end{aligned}$$

for all $x \in E_1$. Since r_{φ_1} is injective, we conclude that

$$f^{*l}(v_1 + v_2) = f^{*l}(v_1) + f^{*l}(v_2).$$

For any $\lambda \in K$, we have

$$\begin{aligned}
\varphi_2(f(x), \lambda v) &= \overline{\lambda}\varphi_2(f(x), v) \\
&= \overline{\lambda}\varphi_1(x, f^{*l}(v)) \\
&= \varphi_1(x, \lambda f^{*l}(v)) \\
&= \varphi_1(x, f^{*l}(\lambda v)),
\end{aligned}$$

for all $x \in E_1$. Since r_{φ_1} is injective, we conclude that

$$f^{*l}(\lambda v) = \lambda f^{*l}(v).$$

Therefore, f^{*l} is linear. We call it the *left adjoint* of f.

Now, for any fixed $u \in E_2$, we can consider the linear form in E_1^* given by

$$x \mapsto \overline{\varphi_2(u, f(x))} \quad x \in E_1.$$

Since $l_{\varphi_1} \colon \overline{E_1} \to E_1^*$ is bijective, there is a unique $y \in E_1$ so that

$$\overline{\varphi_2(u, f(x))} = \overline{\varphi_1(y, x)}, \quad \text{for all } x \in E_1.$$

If we denote this unique $y \in E_1$ by $f^{*r}(u)$, then we have

$$\varphi_2(u, f(x)) = \varphi_1(f^{*r}(u), x), \quad \text{for all } x \in E_1, \text{ and all } u \in E_2.$$

Thus, we get a function $f^{*r} \colon E_2 \to E_1$. As in the previous situation, it easy to check that f^{*r} is linear. We call it the *right adjoint* of f. In summary, we make the following definition.

Definition 29.14. Let E_1 and E_2 be two K-vector spaces, and let $\varphi_1 \colon E_1 \times E_1 \to K$ and $\varphi_2 \colon E_2 \times E_2 \to K$ be two sesquilinear forms. Assume that l_{φ_1} and r_{φ_1} are bijective, so that φ_1 is nondegnerate. For every linear map $f \colon E_1 \to E_2$, there exist unique linear maps $f^{*l} \colon E_2 \to E_1$ and $f^{*r} \colon E_2 \to E_1$, such that

$$\begin{aligned} \varphi_2(f(x), u) &= \varphi_1(x, f^{*l}(u)), \quad \text{for all } x \in E_1, \text{ and all } u \in E_2 \\ \varphi_2(u, f(x)) &= \varphi_1(f^{*r}(u), x), \quad \text{for all } x \in E_1, \text{ and all } u \in E_2. \end{aligned}$$

The map f^{*l} is called the *left adjoint* of f, and the map f^{*r} is called the *right adjoint* of f.

If E_1 and E_2 are finite-dimensional with bases $(e_1, \ldots, e_m)$ and $(f_1, \ldots, f_n)$, then we can work out the matrices A^{*l} and A^{*r} corresponding to the left adjoint f^{*l} and the right adjoint f^{*r} of f. Assumine that f is represented by the $n \times m$ matrix A, φ_1 is represented by the $m \times m$ matrix M_1, and φ_2 is represented by the $n \times n$ matrix M_2. Since

$$\begin{aligned} \varphi_1(x, f^{*l}(u)) &= (A^{*l}u)^* M_1 x = u^* (A^{*l})^* M_1 x \\ \varphi_2(f(x), u) &= u^* M_2 A x \end{aligned}$$

we find that $(A^{*l})^* M_1 = M_2 A$, that is $(A^{*l})^* = M_2 A M_1^{-1}$, and similarly

$$\begin{aligned} \varphi_1(f^{*r}(u), x) &= x^* M_1 A^{*r} u \\ \varphi_2(u, f(x)) &= (Ax)^* M_2 u = x^* A^* M_2 u, \end{aligned}$$

we have $M_1 A^{*r} = A^* M_2$, that is $A^{*r} = (M_1)^{-1} A^* M_2$. Thus, we obtain

$$\begin{aligned} A^{*l} &= (M_1^*)^{-1} A^* M_2^* \\ A^{*r} &= (M_1)^{-1} A^* M_2. \end{aligned}$$

If φ_1 and φ_2 are symmetric bilinear forms, then $f^{*l} = f^{*r}$. This also holds if φ is ϵ-Hermitian. Indeed, since

$$\varphi_2(u, f(x)) = \varphi_1(f^{*r}(u), x),$$

we get

$$\epsilon\overline{\varphi_2(f(x), u)} = \epsilon\overline{\varphi_1(x, f^{*r}(u))},$$

and since $\lambda \mapsto \overline{\lambda}$ is an involution, we get

$$\varphi_2(f(x), u) = \varphi_1(x, f^{*r}(u)).$$

Since we also have

$$\varphi_2(f(x), u) = \varphi_1(x, f^{*l}(u)),$$

we obtain

$$\varphi_1(x, f^{*r}(u)) = \varphi_1(x, f^{*l}(u)) \quad \text{for all } x \in E_1, \text{ and all } u \in E_2,$$

and since φ_1 is nondegenerate, we conclude that $f^{*l} = f^{*r}$. Whenever $f^{*l} = f^{*r}$, we use the simpler notation f^*.

If $f \colon E_1 \to E_2$ and $g \colon E_1 \to E_2$ are two linear maps, we have the following properties:

$$\begin{aligned}(f + g)^{*l} &= f^{*l} + g^{*l}\\ \mathrm{id}^{*l} &= \mathrm{id}\\ (\lambda f)^{*l} &= \overline{\lambda} f^{*l},\end{aligned}$$

and similarly for right adjoints. If E_3 is another space, φ_3 is a sesquilinear form on E_3, and if l_{φ_2} and r_{φ_2} are bijective, then for any linear maps $f \colon E_1 \to E_2$ and $g \colon E_2 \to E_3$, we have

$$(g \circ f)^{*l} = f^{*l} \circ g^{*l},$$

and similarly for right adjoints. Furthermore, if $E_1 = E_2 = E$ and $\varphi \colon E \times E \to K$ is ϵ-Hermitian, for any linear map $f \colon E \to E$ (recall that in this case $f^{*l} = f^{*r} = f^*$), we have

$$f^{**} = \epsilon\overline{\epsilon} f.$$

29.5 Isometries Associated with Sesquilinear Forms

The notion of adjoint is a good tool to investigate the notion of isometry between spaces equipped with sesquilinear forms. First, we define metric maps and isometries.

Definition 29.15. If (E_1, φ_1) and (E_2, φ_2) are two pairs of spaces and sesquilinear maps $\varphi_1 \colon E_1 \times E_1 \to K$ and $\varphi_2 \colon E_2 \times E_2 \to K$, a *metric map* from (E_1, φ_1) to (E_2, φ_2) is a linear map $f \colon E_1 \to E_2$ such that

$$\varphi_1(u, v) = \varphi_2(f(u), f(v)) \quad \text{for all } u, v \in E_1.$$

We say that φ_1 and φ_2 are *equivalent* iff there is a metric map $f \colon E_1 \to E_2$ which is bijective. Such a metric map is called an *isometry*.

The problem of classifying sesquilinear forms up to equivalence is an important but very difficult problem. Solving this problem depends intimately on properties of the field K, and a complete answer is only known in a few cases. The problem is easily solved for $K = \mathbb{R}$, $K = \mathbb{C}$. It is also solved for finite fields and for $K = \mathbb{Q}$ (the rationals), but the solution is surprisingly involved!

It is hard to say anything interesting if φ_1 is degenerate and if the linear map f does not have adjoints. The next few propositions make use of natural conditions on φ_1 that yield a useful criterion for being a metric map.

Proposition 29.16. *With the same assumptions as in Definition 29.14 (which imply that φ_1 is nondegenerate), if $f\colon E_1 \to E_2$ is a bijective linear map, then we have*

$$\begin{aligned}&\varphi_1(x, y) = \varphi_2(f(x), f(y)) \quad \textit{for all } x, y \in E_1 \textit{ iff}\\ &f^{-1} = f^{*_l} = f^{*_r}.\end{aligned}$$

Proof. We have

$$\varphi_1(x, y) = \varphi_2(f(x), f(y))$$

iff

$$\varphi_1(x, y) = \varphi_2(f(x), f(y)) = \varphi_1(x, f^{*_l}(f(y))$$

iff

$$\varphi_1(x, (\mathrm{id} - f^{*_l} \circ f)(y)) = 0 \quad \text{for all } x \in E_1 \text{ and all } y \in E_2.$$

Since φ_1 is nondegenerate, we must have

$$f^{*_l} \circ f = \mathrm{id},$$

which implies that $f^{-1} = f^{*_l}$. Similarly,

$$\varphi_1(x, y) = \varphi_2(f(x), f(y))$$

iff

$$\varphi_1(x, y) = \varphi_2(f(x), f(y)) = \varphi_1(f^{*_r}(f(x)), y)$$

iff

$$\varphi_1((\mathrm{id} - f^{*_r} \circ f)(x), y) = 0 \quad \text{for all } x \in E_1 \text{ and all } y \in E_2.$$

Since φ_1 is nondegenerate, we must have

$$f^{*_r} \circ f = \mathrm{id},$$

which implies that $f^{-1} = f^{*_r}$. Therefore, $f^{-1} = f^{*_l} = f^{*_r}$. For the converse, do the computations in reverse. □

As a corollary, we get the following important proposition.

Proposition 29.17. *If $\varphi\colon E \times E \to K$ is a sesquilinear map, and if l_φ and r_φ are bijective, for every bijective linear map $f\colon E \to E$, then we have*

$$\begin{aligned}&\varphi(f(x), f(y)) = \varphi(x, y) \quad \textit{for all } x, y \in E \textit{ iff}\\ &f^{-1} = f^{*l} = f^{*r}.\end{aligned}$$

We also have the following facts.

Proposition 29.18. *(1) If $\varphi\colon E \times E \to K$ is a sesquilinear map and if l_φ is injective, then for every linear map $f\colon E \to E$, if*

$$\varphi(f(x), f(y)) = \varphi(x, y) \quad \textit{for all } x, y \in E, \tag{$*$}$$

then f is injective.

(2) If E is finite-dimensional and if φ is nondegenerate, then the linear maps $f\colon E \to E$ satisfying $(*)$ form a group. The inverse of f is given by $f^{-1} = f^*$.

Proof. (1) If $f(x) = 0$, then

$$\varphi(x, y) = \varphi(f(x), f(y)) = \varphi(0, f(y)) = 0 \quad \text{for all } y \in E.$$

Since l_φ is injective, we must have $x = 0$, and thus f is injective.

(2) If E is finite-dimensional, since a linear map satisfying $(*)$ is injective, it is a bijection. By Proposition 29.17, we have $f^{-1} = f^*$. We also have

$$\varphi(f(x), f(y)) = \varphi((f^* \circ f)(x), y) = \varphi(x, y) = \varphi((f \circ f^*)(x), y) = \varphi(f^*(x), f^*(y)),$$

which shows that f^* satisfies $(*)$. If $\varphi(f(x), f(y)) = \varphi(x, y)$ for all $x, y \in E$ and $\varphi(g(x), g(y))$ $= \varphi(x, y)$ for all $x, y \in E$, then we have

$$\varphi((g \circ f)(x), (g \circ f)(y)) = \varphi(f(x), f(y)) = \varphi(x, y) \quad \text{for all } x, y \in E.$$

Obviously, the identity map id_E satisfies $(*)$. Therefore, the set of linear maps satisfying $(*)$ is a group. □

The above considerations motivate the following definition.

Definition 29.16. Let $\varphi\colon E \times E \to K$ be a sesquilinear map, and assume that E is finite-dimensional and that φ is nondegenerate. A linear map $f\colon E \to E$ is an *isometry* of E (with respect to φ) iff

$$\varphi(f(x), f(y)) = \varphi(x, y) \quad \text{for all } x, y \in E.$$

The set of all isometries of E is a group denoted by $\mathbf{Isom}(\varphi)$.

If φ is symmetric, then the group $\mathbf{Isom}(\varphi)$ is denoted $\mathbf{O}(\varphi)$ and called the *orthogonal group* of φ. If φ is alternating, then the group $\mathbf{Isom}(\varphi)$ is denoted $\mathbf{Sp}(\varphi)$ and called the *symplectic group* of φ. If φ is ϵ-Hermitian, then the group $\mathbf{Isom}(\varphi)$ is denoted $\mathbf{U}_\epsilon(\varphi)$ and called the *ϵ-unitary group* of φ. When $\epsilon = 1$, we drop ϵ and just say *unitary group*.

If $(e_1, \ldots, e_n)$ is a basis of E, φ is the represented by the $n \times n$ matrix M, and f is represented by the $n \times n$ matrix A, since $A^{-1} = A^{*_l} = A^{*_r} = M^{-1}A^*M$, then we find that $f \in \mathbf{Isom}(\varphi)$ iff

$$A^*MA = M,$$

and A^{-1} is given by $A^{-1} = M^{-1}A^*M$.

More specifically, we define the following groups, using the matrices $I_{p,q}$, $J_{m,m}$ and $A_{m,m}$ defined at the end of Section 29.1.

(1) $K = \mathbb{R}$. We have

$$\begin{aligned}
\mathbf{O}(n) &= \{A \in \mathrm{M}_n(\mathbb{R}) \mid A^\top A = I_n\}\\
\mathbf{O}(p,q) &= \{A \in \mathrm{M}_{p+q}(\mathbb{R}) \mid A^\top I_{p,q} A = I_{p,q}\}\\
\mathbf{Sp}(2n,\mathbb{R}) &= \{A \in \mathrm{M}_{2n}(\mathbb{R}) \mid A^\top J_{n,n} A = J_{n,n}\}\\
\mathbf{SO}(n) &= \{A \in \mathrm{M}_n(\mathbb{R}) \mid A^\top A = I_n,\ \det(A) = 1\}\\
\mathbf{SO}(p,q) &= \{A \in \mathrm{M}_{p+q}(\mathbb{R}) \mid A^\top I_{p,q} A = I_{p,q},\ \det(A) = 1\}.
\end{aligned}$$

The group $\mathbf{O}(n)$ is the *orthogonal group*, $\mathbf{Sp}(2n,\mathbb{R})$ is the *real symplectic group*, and $\mathbf{SO}(n)$ is the *special orthogonal group*. We can define the group

$$\{A \in \mathrm{M}_{2n}(\mathbb{R}) \mid A^\top A_{n,n} A = A_{n,n}\},$$

but it is isomorphic to $\mathbf{O}(n,n)$.

(2) $K = \mathbb{C}$. We have

$$\begin{aligned}
\mathbf{U}(n) &= \{A \in \mathrm{M}_n(\mathbb{C}) \mid A^* A = I_n\}\\
\mathbf{U}(p,q) &= \{A \in \mathrm{M}_{p+q}(\mathbb{C}) \mid A^* I_{p,q} A = I_{p,q}\}\\
\mathbf{Sp}(2n,\mathbb{C}) &= \{A \in \mathrm{M}_{2n}(\mathbb{C}) \mid A^\top J_{n,n} A = J_{n,n}\}\\
\mathbf{SU}(n) &= \{A \in \mathrm{M}_n(\mathbb{C}) \mid A^* A = I_n,\ \det(A) = 1\}\\
\mathbf{SU}(p,q) &= \{A \in \mathrm{M}_{p+q}(\mathbb{C}) \mid A^* I_{p,q} A = I_{p,q},\ \det(A) = 1\}.
\end{aligned}$$

The group $\mathbf{U}(n)$ is the *unitary group*, $\mathbf{Sp}(2n,\mathbb{C})$ is the *complex symplectic group*, and $\mathbf{SU}(n)$ is the *special unitary group*.

It can be shown that if $A \in \mathbf{Sp}(2n,\mathbb{R})$ or if $A \in \mathbf{Sp}(2n,\mathbb{C})$, then $\det(A) = 1$.

29.6 Totally Isotropic Subspaces

In this section, we deal with ϵ-Hermitian forms, $\varphi\colon E \times E \to K$. In general, E may have subspaces U such that $U \cap U^{\perp} \neq (0)$, or worse, such that $U \subseteq U^{\perp}$ (that is, φ is zero on U). We will see that such subspaces play a crucial in the decomposition of E into orthogonal subspaces.

Definition 29.17. Given an ϵ-Hermitian forms $\varphi\colon E \times E \to K$, a nonzero vector $u \in E$ is said to be *isotropic* if $\varphi(u, u) = 0$. It is convenient to consider 0 to be isotropic. Given any subspace U of E, the subspace $\mathrm{rad}(U) = U \cap U^{\perp}$ is called the *radical* of U. We say that

(i) U is *degenerate* if $\mathrm{rad}(U) \neq (0)$ (equivalently if there is some nonzero vector $u \in U$ such that $x \in U^{\perp}$). Otherwise, we say that U is *nondegenerate*.

(ii) U is *totally isotropic* if $U \subseteq U^{\perp}$ (equivalently if the restriction of φ to U is zero).

By definition, the trivial subspace $U = (0)$ $(= \{0\})$ is nondegenerate. Observe that a subspace U is nondegenerate iff the restriction of φ to U is nondegenerate. A degenerate subspace is sometimes called an *isotropic* subspace. Other authors say that a subspace U is *isotropic* if it contains some (nonzero) isotropic vector. A subspace which has no nonzero isotropic vector is often called *anisotropic*. The space of all isotropic vectors is a cone often called the *light cone* (a terminology coming from the theory of relativity). This is not to be confused with the cone of silence (from Get Smart)! It should also be noted that some authors (such as Serre) use the term *isotropic* instead of *totally isotropic*. The apparent lack of standard terminology is almost as bad as in graph theory!

It is clear that any direct sum of pairwise orthogonal totally isotropic subspaces is totally isotropic. Thus, every totally isotropic subspace is contained in some maximal totally isotropic subspace. Here is another fact that we will use all the time: if V is a totally isotropic subspace and if U is a subspace of V, then U is totally isotropic.

This is because by definition V is isotropic if $V \subseteq V^{\perp}$, and since $U \subseteq V$ we get $V^{\perp} \subseteq U^{\perp}$, so $U \subseteq V \subseteq V^{\perp} \subseteq U^{\perp}$, which shows that U is totally isotropic.

First, let us show that in order to sudy an ϵ-Hermitian form on a space E, it suffices to restrict our attention to nondegenerate forms.

Proposition 29.19. *Given an ϵ-Hermitian form $\varphi\colon E \times E \to K$ on E, we have:*

(a) If U and V are any two orthogonal subspaces of E, then

$$\mathrm{rad}(U + V) = \mathrm{rad}(U) + \mathrm{rad}(V).$$

(b) $\mathrm{rad}(\mathrm{rad}(E)) = \mathrm{rad}(E)$.

(c) If U is any subspace supplementary to $\mathrm{rad}(E)$*, so that*

$$E = \mathrm{rad}(E) \oplus U,$$

then U is nondegenerate, and $\mathrm{rad}(E)$ *and U are orthogonal.*

Proof. (a) If U and V are orthogonal, then $U \subseteq V^{\perp}$ and $V \subseteq U^{\perp}$. We get

$$\begin{aligned}\mathrm{rad}(U+V) &= (U+V) \cap (U+V)^{\perp}\\ &= (U+V) \cap U^{\perp} \cap V^{\perp}\\ &= U \cap U^{\perp} \cap V^{\perp} + V \cap U^{\perp} \cap V^{\perp}\\ &= U \cap U^{\perp} + V \cap V^{\perp}\\ &= \mathrm{rad}(U) + \mathrm{rad}(V).\end{aligned}$$

(b) By definition, $\mathrm{rad}(E) = E^{\perp}$, and obviously $E = E^{\perp\perp}$, so we get

$$\mathrm{rad}(\mathrm{rad}(E)) = E^{\perp} \cap E^{\perp\perp} = E^{\perp} \cap E = E^{\perp} = \mathrm{rad}(E).$$

(c) If $E = \mathrm{rad}(E) \oplus U$, by definition of $\mathrm{rad}(E)$, the subspaces $\mathrm{rad}(E)$ and U are orthogonal. From (a) and (b), we get

$$\mathrm{rad}(E) = \mathrm{rad}(E) + \mathrm{rad}(U).$$

Since $\mathrm{rad}(U) = U \cap U^{\perp} \subseteq U$ and since $\mathrm{rad}(E) \oplus U$ is a direct sum, we have a direct sum

$$\mathrm{rad}(E) = \mathrm{rad}(E) \oplus \mathrm{rad}(U),$$

which implies that $\mathrm{rad}(U) = (0)$; that is, U is nondegenerate. □

Proposition 29.19(c) shows that the restriction of φ to any supplement U of $\mathrm{rad}(E)$ is nondegenerate and φ is zero on $\mathrm{rad}(U)$, so we may restrict our attention to nondegenerate forms.

The following is also a key result.

Proposition 29.20. *Given an ϵ-Hermitian form $\varphi\colon E \times E \to K$ on E, if U is a finite-dimensional nondegenerate subspace of E, then $E = U \oplus U^{\perp}$.*

Proof. By hypothesis, the restriction φ_U of φ to U is nondegenerate, so the semilinear map $r_{\varphi_U} : U \to U^*$ is injective. Since U is finite-dimensional, r_{φ_U} is actually bijective, so for every $v \in E$, if we consider the linear form in U^* given by $u \mapsto \varphi(u, v)$ $(u \in U)$, there is a unique $v_0 \in U$ such that

$$\varphi(u, v_0) = \varphi(u, v) \quad \text{for all } u \in U;$$

that is, $\varphi(u, v - v_0) = 0$ for all $u \in U$, so $v - v_0 \in U^{\perp}$. It follows that $v = v_0 + v - v_0$, with $v_0 \in U$ and $v_0 - v \in U^{\perp}$, and since U is nondegenerate $U \cap U^{\perp} = (0)$, and $E = U \oplus U^{\perp}$. □

As a corollary of Proposition 29.20, we get the following result.

Proposition 29.21. *Given an ϵ-Hermitian form $\varphi\colon E \times E \to K$ on E, if φ is nondegenerate and if U is a finite-dimensional subspace of E, then* $\mathrm{rad}(U) = \mathrm{rad}(U^{\perp})$*, and the following conditions are equivalent:*

(i) U is nondegenerate.

(ii) $U^{\perp}$ is nondegenerate.

(iii) $E = U \oplus U^{\perp}$.

Proof. By definition, $\mathrm{rad}(U^{\perp}) = U^{\perp} \cap U^{\perp\perp}$, and since φ is nondegenerate and U is finite-dimensional, $U^{\perp\perp} = U$, so $\mathrm{rad}(U^{\perp}) = U^{\perp} \cap U^{\perp\perp} = U \cap U^{\perp} = \mathrm{rad}(U)$.

By Proposition 29.20, (i) implies (iii). If $E = U \oplus U^{\perp}$, then $\mathrm{rad}(U) = U \cap U^{\perp} = (0)$, so U is nondegenerate and (iii) implies (i). Since $\mathrm{rad}(U^{\perp}) = \mathrm{rad}(U)$, (iii) also implies (ii). Now, if $U^{\perp}$ is nondegenerate, we have $U^{\perp} \cap U^{\perp\perp} = (0)$, and since $U \subseteq U^{\perp\perp}$, we get

$$U \cap U^{\perp} \subseteq U^{\perp\perp} \cap U^{\perp} = (0),$$

which shows that U is nondegenerate, proving the implication (ii) $\Longrightarrow$ (i). □

If E is finite-dimensional, we have the following results.

Proposition 29.22. *Given an ϵ-Hermitian form $\varphi\colon E \times E \to K$ on a finite-dimensional space E, if φ is nondegenerate, then for every subspace U of E we have*

(i) $\dim(U) + \dim(U^{\perp}) = \dim(E)$.

(ii) $U^{\perp\perp} = U$.

Proof. (i) Since φ is nondegenerate and E is finite-dimensional, the semilinear map $l_{\varphi}\colon E \to E^*$ is bijective. By transposition, the inclusion $i\colon U \to E$ yields a surjection $r\colon E^* \to U^*$ (with $r(f) = f \circ i$ for every $f \in E^*$; the map $f \circ i$ is the restriction of the linear form f to U). It follows that the semilinear map $r \circ l_{\varphi}\colon E \to U^*$ given by

$$(r \circ l_{\varphi})(x)(u) = \overline{\varphi(x, u)} \quad x \in E, u \in U$$

is surjective, and its kernel is $U^{\perp}$. Thus, we have

$$\dim(U^*) + \dim(U^{\perp}) = \dim(E),$$

and since $\dim(U) = \dim(U^*)$ because U is finite-dimensional, we get

$$\dim(U) + \dim(U^{\perp}) = \dim(U^*) + \dim(U^{\perp}) = \dim(E).$$

(ii) Applying the above formula to $U^{\perp}$, we deduce that $\dim(U) = \dim(U^{\perp\perp})$. Since $U \subseteq U^{\perp\perp}$, we must have $U^{\perp\perp} = U$. □

Remark: We already proved in Proposition 29.13 that if U is finite-dimensional, then $\mathrm{codim}(U^{\perp}) = \dim(U)$ and $U^{\perp\perp} = U$, but it doesn't hurt to give another proof. Observe that (i) implies that

$$\dim(U) + \dim(\mathrm{rad}(U)) \leq \dim(E).$$

We can now proceed with the Witt decomposition, but before that, we quickly take care of the structure theorem for alternating bilinear forms (the case where $\varphi(u, u) = 0$ for all $u \in E$). For an alternating bilinear form, the space E is totally isotropic. For example in dimension 2, the matrix

$$B = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$$

defines the alternating form given by

$$\varphi((x_1, y_1), (x_2, y_2)) = x_1y_2 - x_2y_1.$$

This case is surprisingly general.

Proposition 29.23. *Let $\varphi\colon E \times E \to K$ be an alternating bilinear form on E. If $u, v \in E$ are two (nonzero) vectors such that $\varphi(u, v) = \lambda \neq 0$, then u and v are linearly independent. If we let $u_1 = \lambda^{-1}u$ and $v_1 = v$, then $\varphi(u_1, v_1) = 1$, and the restriction of φ to the plane spanned by u_1 and v_1 is represented by the matrix*

$$\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}.$$

Proof. If u and v were linearly dependent, as $u, v \neq 0$, we could write $v = \mu u$ for some $\mu \neq 0$, but then, since φ is alternating, we would have

$$\lambda = \varphi(u, v) = \varphi(u, \mu u) = \mu\varphi(u, u) = 0,$$

contradicting the fact that $\lambda \neq 0$. The rest is obvious. □

Proposition 29.23 yields a plane spanned by two vectors u_1, v_1 such that $\varphi(u_1, u_1) = \varphi(v_1, v_1) = 0$ and $\varphi(u_1, v_1) = 1$. Such a plane is called a *hyperbolic plane*. If E is finite-dimensional, we obtain the following theorem.

Theorem 29.24. *Let $\varphi\colon E \times E \to K$ be an alternating bilinear form on a space E of finite dimension n. Then, there is a direct sum decomposition of E into pairwise orthogonal subspaces*

$$E = W_1 \oplus \cdots \oplus W_r \oplus \mathrm{rad}(E),$$

where each W_i is a hyperbolic plane and $\mathrm{rad}(E) = E^{\perp}$. *Therefore, there is a basis of E of the form*

$$(u_1, v_1, \ldots, u_r, v_r, w_1, \ldots, w_{n-2r}),$$

with respect to which the matrix representing φ is a block diagonal matrix M of the form

$$M = \begin{pmatrix} J & & & & 0 \\ & J & & & \\ & & \ddots & & \\ & & & J & \\ 0 & & & & 0_{n-2r} \end{pmatrix},$$

with

$$J = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}.$$

Proof. If $\varphi = 0$, then $E = E^{\perp}$ and we are done. Otherwise, there are two nonzero vectors $u, v \in E$ such that $\varphi(u, v) \neq 0$, so by Proposition 29.23, we obtain a hyperbolic plane W_2 spanned by two vectors u_1, v_1 such that $\varphi(u_1, v_1) = 1$. The subspace W_1 is nondegenerate (for example, $\det(J) = -1$), so by Proposition 29.21, we get a direct sum

$$E = W_1 \oplus W_1^{\perp}.$$

By Proposition 29.14, we also have

$$E^{\perp} = (W_1 \oplus W_1^{\perp}) = W_1^{\perp} \cap W_1^{\perp\perp} = \mathrm{rad}(W_1^{\perp}).$$

By the induction hypothesis applied to $W_1^{\perp}$, we obtain our theorem. □

The following corollary follows immediately.

Proposition 29.25. *Let $\varphi \colon E \times E \to K$ be an alternating bilinear form on a space E of finite dimension n.*

(1) The rank of φ is even.

(2) If φ is nondegenerate, then $\dim(E) = n$ is even.

(3) Two alternating bilinear forms $\varphi_1 \colon E_1 \times E_1 \to K$ and $\varphi_2 \colon E_2 \times E_2 \to K$ are equivalent iff $\dim(E_1) = \dim(E_2)$ and φ_1 and φ_2 have the same rank.

The only part that requires a proof is part (3), which is left as an easy exercise.

If φ is nondegenerate, then $n = 2r$, and a basis of E as in Theorem 29.24 is called a *symplectic basis*. The space E is called a *hyperbolic space* (or *symplectic space*).

Observe that if we reorder the vectors in the basis

$$(u_1, v_1, \ldots, u_r, v_r, w_1, \ldots, w_{n-2r})$$

to obtain the basis

$$(u_1, \ldots, u_r, v_1, \ldots v_r, w_1, \ldots, w_{n-2r}),$$

then the matrix representing φ becomes

$$\begin{pmatrix} 0 & I_r & 0 \\ -I_r & 0 & 0 \\ 0 & 0 & 0_{n-2r} \end{pmatrix}.$$

This particularly simple matrix is often preferable, especially when dealing with the matrices (symplectic matrices) representing the isometries of φ (in which case $n = 2r$).

As a warm up for Proposition 29.29 of the next section, we prove an analog of Proposition 29.23 in the case of a symmetric bilinear form.

Proposition 29.26. *Let $\varphi\colon E\times E \to K$ be a nondegenerate symmetric bilinear form with K a field of characteristic different from 2. For any nonzero isotropic vector u, there is another nonzero isotropic vector v such that $\varphi(u, v) = 2$, and u and v are linearly independent. In the basis $(u, v/2)$, the restriction of φ to the plane spanned by u and $v/2$ is of the form*

$$\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}.$$

Proof. Since φ is nondegenerate, there is some nonzero vector z such that (rescaling z if necessary) $\varphi(u, z) = 1$. If

$$v = 2z - \varphi(z, z)u,$$

then since $\varphi(u, u) = 0$ and $\varphi(u, z) = 1$, note that

$$\varphi(u, v) = \varphi(u, 2z - \varphi(z, z)u) = 2\varphi(u, z) - \varphi(z, z)\varphi(u, u) = 2,$$

and

$$\begin{aligned} \varphi(v, v) &= \varphi(2z - \varphi(z, z)u, 2z - \varphi(z, z)u) \\ &= 4\varphi(z, z) - 4\varphi(z, z)\varphi(u, z) + \varphi(z, z)^2\varphi(u, u) \\ &= 4\varphi(z, z) - 4\varphi(z, z) = 0. \end{aligned}$$

If u and z were linearly dependent, as $u, z \neq 0$, we could write $z = \mu u$ for some $\mu \neq 0$, but then, we would have

$$\varphi(u, z) = \varphi(u, \mu u) = \mu\varphi(u, u) = 0,$$

contradicting the fact that $\varphi(u, z) \neq 0$. Then u and $v = 2z - \varphi(z, z)u$ are also linearly independent, since otherwise z could be expressed as a multiple of u. The rest is obvious. □

Proposition 29.26 yields a plane spanned by two vectors u_1, v_1 such that $\varphi(u_1, u_1) = \varphi(v_1, v_1) = 0$ and $\varphi(u_1, v_1) = 1$. Such a plane is called an *Artinian plane*. Proposition 29.26 also shows that nonzero isotropic vectors come in pair.

Proposition 29.26 has the following corollary which has applications in number theory; see Serre [155], Chapter IV.

Proposition 29.27. *If Φ is any nondegenerate quadratic form (over a field of characteristic $\neq 2$) such that there is some nonzero vector $x \in E$ with $\Phi(x) = 0$, then for every $\alpha \in K$, there is some $y \in E$ such that $\Phi(y) = \alpha$.*

Proof. Since by hypothesis there is some nonzero vector $u \in E$ with $\Phi(u) = 0$, by Proposition 29.26 there is another isotropic vector v such that u and v are linearly independent and such that (after rescaling) $\varphi(u, v) = 1$. Then for any $\alpha \in K$, check that

$$\Phi\left(u + \frac{\alpha}{2}v\right) = \alpha,$$

as desired. □

Remark: Some authors refer to the above plane as a *hyperbolic plane*. Berger (and others) point out that this terminology is undesirable because the notion of hyperbolic plane already exists in differential geometry and refers to a very different object.

We leave it as an exercice to figure out that the group of isometries of the Artinian plane, the set of all 2 × 2 matrices A such that

$$A^{\top}\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} A = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix},$$

consists of all matrices of the form

$$\begin{pmatrix} \lambda & 0 \\ 0 & \lambda^{-1} \end{pmatrix} \quad \text{or} \quad \begin{pmatrix} 0 & \lambda \\ \lambda^{-1} & 0 \end{pmatrix}, \quad \lambda \in K - \{0\}.$$

In particular, if $K = \mathbb{R}$, then this group denoted $\mathbf{O}(1, 1)$ has four connected components.

We now turn to the Witt decomposition.

29.7 Witt Decomposition

From now on, $\varphi\colon E \times E \to K$ is an ϵ-Hermitian form. The following assumption will be needed:

Property (T). For every $u \in E$, there is some $\alpha \in K$ such that $\varphi(u, u) = \alpha + \epsilon\overline{\alpha}$.

Property (T) is always satisfied if φ is alternating, or if K is of characteristic $\neq 2$ and $\epsilon = \pm 1$, with $\alpha = \frac{1}{2}\varphi(u, u)$.

The following (bizarre) technical lemma will be needed.

Lemma 29.28. *Let φ be an ϵ-Hermitian form on E and assume that φ satisfies property (T). For any totally isotropic subspace $U \neq (0)$ of E, for every $x \in E$ not orthogonal to U, and for every $\alpha \in K$, there is some $y \in U$ so that*

$$\varphi(x + y, x + y) = \alpha + \epsilon\overline{\alpha}.$$

Proof. By property (T), we have $\varphi(x,x) = \beta + \epsilon\overline{\beta}$ for some $\beta \in K$. For any $y \in U$, since φ is ϵ-Hermitian, $\varphi(y,x) = \epsilon\overline{\varphi(x,y)}$, and since U is totally isotropic $\varphi(y,y) = 0$, so we have

$$\begin{aligned}\varphi(x+y, x+y) &= \varphi(x,x) + \varphi(x,y) + \varphi(y,x) + \varphi(y,y)\\ &= \beta + \epsilon\overline{\beta} + \varphi(x,y) + \epsilon\overline{\varphi(x,y)}\\ &= \beta + \varphi(x,y) + \epsilon\overline{(\beta + \varphi(x,y)}.\end{aligned}$$

Since x is not orthogonal to U, the function $y \mapsto \varphi(x,y) + \beta$ is not the constant function. Consequently, this function takes the value α for some $y \in U$, which proves the lemma. □

Definition 29.18. Let φ be an ϵ-Hermitian form on E. A *weak Witt decomposition* of E is a triple (U, U', W), such that

(i) $E = U \oplus U' \oplus W$ (a direct sum).

(ii) U and U' are totally isotropic.

(iii) W is nondegenerate and orthogonal to $U \oplus U'$.

We say that a weak Witt decomposition (U, U', W) is *nontrivial* if $U \neq (0)$ and $U' \neq (0)$. Furthermore, if E is finite-dimensional, then $\dim(U) = \dim(U')$ and in a suitable basis, the matrix representing φ is of the form

$$\begin{pmatrix} 0 & A & 0 \\ \epsilon\overline{A} & 0 & 0 \\ 0 & 0 & B \end{pmatrix}$$

We say that φ is a *neutral form* if it is nondegenerate, E is finite-dimensional, and if $W = (0)$. In this case, the matrix B is missing.

A Witt decomposition for which W has no nonzero isotropic vectors (W is anisotropic) is called a *Witt decomposition*.

Observe that if Φ is nondegenerate, then we have the trivial weak Witt decomposition obtained by letting $U = U' = (0)$ and $W = E$. Thus a weak Witt decomposition is informative only if E is not anisotropic (there is some nonzero isotropic vector, *i.e.* some $u \neq 0$ such that $\Phi(u) = 0$), in which case the most informative nontrivial weak Witt decompositions are those for which W is anisotropic and U and U' are as big as possible.

Sometimes, we use the notation $U_1 \overset{\perp}{\oplus} U_2$ to indicate that in a direct sum $U_1 \oplus U_2$, the subspaces U_1 and U_2 are orthogonal. Then, in Definition 29.18, we can write that $E = (U \oplus U') \overset{\perp}{\oplus} W$.

The first step in showing the existence of a Witt decomposition is this.

Proposition 29.29. *Let φ be an ϵ-Hermitian form on E, assume that φ is nondegenerate and satisfies property (T), and let U be any totally isotropic subspace of E of finite dimension* $\dim(U) = r \geq 1$.

(1) If U' is any totally isotropic subspace of dimension r and if $U' \cap U^{\perp} = (0)$, then $U \oplus U'$ is nondegenerate, and for any basis $(u_1, \ldots, u_r)$ of U, there is a basis $(u'_1, \ldots, u'_r)$ of U' such that $\varphi(u_i, u'_j) = \delta_{ij}$, for all $i, j = 1, \ldots, r$.

(2) If W is any totally isotropic subspace of dimension at most r and if $W \cap U^{\perp} = (0)$, then there exists a totally isotropic subspace U' with $\dim(U') = r$ *such that $W \subseteq U'$ and $U' \cap U^{\perp} = (0)$.*

Proof. (1) Let φ' be the restriction of φ to $U \times U'$. Since $U' \cap U^{\perp} = (0)$, for any $v \in U'$, if $\varphi(u, v) = 0$ for all $u \in U$, then $v = 0$. Thus, φ' is nondegenerate (we only have to check on the left since φ is ϵ-Hermitian). Then, the assertion about bases follows from the version of Proposition 29.3 for sesquilinear forms. Since U is totally isotropic, $U \subseteq U^{\perp}$, and since $U' \cap U^{\perp} = (0)$, we must have $U' \cap U = (0)$, which show that we have a direct sum $U \oplus U'$.

It remains to prove that $U + U'$ is nondegenerate. Observe that

$$H = (U + U') \cap (U + U')^{\perp} = (U + U') \cap U^{\perp} \cap U'^{\perp}.$$

Since U is totally isotropic, $U \subseteq U^{\perp}$, and since $U' \cap U^{\perp} = (0)$, we have

$$(U + U') \cap U^{\perp} = (U \cap U^{\perp}) + (U' \cap U^{\perp}) = U + (0) = U,$$

thus $H = U \cap U'^{\perp}$. Since φ' is nondegenerate, $U \cap U'^{\perp} = (0)$, so $H = (0)$ and $U + U'$ is nondegenerate.

(2) We proceed by descending induction on $s = \dim(W)$. The base case $s = r$ is trivial. For the induction step, it suffices to prove that if $s < r$, then there is a totally isotropic subspace W' containing W such that $\dim(W') = s + 1$ and $W' \cap U^{\perp} = (0)$.

Since $s = \dim(W) < \dim(U)$, the restriction of φ to $U \times W$ is degenerate. Since $W \cap U^{\perp} = (0)$, we must have $U \cap W^{\perp} \neq (0)$. We claim that

$$W^{\perp} \not\subseteq W + U^{\perp}.$$

If we had

$$W^{\perp} \subseteq W + U^{\perp},$$

then because U and W are finite-dimensional and φ is nondegenerate, by Proposition 29.13, $U^{\perp\perp} = U$ and $W^{\perp\perp} = W$, so by taking orthogonals, $W^{\perp} \subseteq W + U^{\perp}$ would yield

$$(W + U^{\perp})^{\perp} \subseteq W^{\perp\perp},$$

that is,

$$W^{\perp} \cap U \subseteq W,$$

thus $W^{\perp} \cap U \subseteq W \cap U$, and since U is totally isotropic, $U \subseteq U^{\perp}$, which yields

$$W^{\perp} \cap U \subseteq W \cap U \subseteq W \cap U^{\perp} = (0),$$

contradicting the fact that $U \cap W^{\perp} \neq (0)$.

Therefore, there is some $u \in W^{\perp}$ such that $u \notin W + U^{\perp}$. Since $U \subseteq U^{\perp}$, we can add to u any vector $z \in W^{\perp} \cap U \subseteq U^{\perp}$ so that $u + z \in W^{\perp}$ and $u + z \notin W + U^{\perp}$ (if $u + z \in W + U^{\perp}$, since $z \in U^{\perp}$, then $u \in W + U^{\perp}$, a contradiction). Since $W^{\perp} \cap U \neq (0)$ is totally isotropic and $u \notin W + U^{\perp} = (W^{\perp} \cap U)^{\perp}$, we can invoke Lemma 29.28 to find a $z \in W^{\perp} \cap U$ such that $\varphi(u + z, u + z) = 0$. See Figure 29.1. If we write $x = u + z$, then $x \notin W + U^{\perp}$, so $W' = W + Kx$ is a totally isotropic subspace of dimension $s + 1$. Furthermore, we claim that $W' \cap U^{\perp} = 0$.

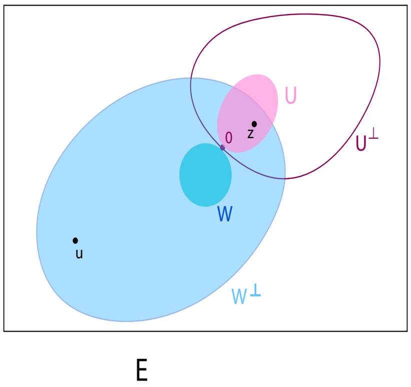

Figure 29.1: A schematic illustration of W and $x = u + z$

Otherwise, we would have $y = w + \lambda x \in U^{\perp}$, for some $w \in W$ and some $\lambda \in K$, and then we would have $\lambda x = -w + y \in W + U^{\perp}$. If $\lambda \neq 0$, then $x \in W + U^{\perp}$, a contradiction. Therefore, $\lambda = 0$, $y = w$, and since $y \in U^{\perp}$ and $w \in W$, we have $y \in W \cap U^{\perp} = (0)$, which means that $y = 0$. Therefore, W' is the required subspace and this completes the proof. □

Here are some consequences of Proposition 29.29. If we set $W = (0)$ in Proposition 29.29(2), then we get the following theorem showing that if E is not anisotropic (there is some nonzero isotropic vector) then weak nontrivial Witt decompositions exist.

Theorem 29.30. *Let φ be an ϵ-Hermitian form on E which is nondegenerate and satisfies property (T). For any totally isotropic subspace U of E of finite dimension $r \geq 1$, there exists a totally isotropic subspace U' of dimension r such that $U \cap U' = (0)$ and $U \oplus U'$ is nondegenerate. As a consequence, if E is not anisotropic, then $(U, U', (U \oplus U')^{\perp})$ is a weak nontrivial Witt decomposition for E. Furthermore, by Proposition 29.29(1), the block A in the matrix of φ is the identity matrix.*

Proposition 29.31. *Any two ϵ-Hermitian neutral forms satisfying property (T) defined on spaces of the same dimension are equivalent.*

The following proposition shows that every subspace U of E can be embedded into a nondegenerate subspace. It is needed to prove a version of the Witt extension theorem (Theorem 29.48).

Proposition 29.32. *Let φ be an ϵ-Hermitian form on E which is nondegenerate and satisfies property (T). For any subspace U of E of finite dimension, if we write*

$$U = V \overset{\perp}{\oplus} W,$$

for some orthogonal complement W of $V = \mathrm{rad}(U)$, and if we let $r = \dim(\mathrm{rad}(U))$, then there exists a totally isotropic subspace V' of dimension r such that $V \cap V' = (0)$, and $(V \oplus V') \overset{\perp}{\oplus} W = V' \oplus U$ is nondegenerate. Furthermore, any isometry f from U into another space (E', φ') where φ' is an ϵ-Hermitian form satisfying the same assumptions as φ can be extended to an isometry on $(V \oplus V') \overset{\perp}{\oplus} W$.

Proof. Since W is nondegenerate, $W^{\perp}$ is also nondegenerate, and $V \subseteq W^{\perp}$. Therefore, we can apply Theorem 29.30 to the restriction of φ to $W^{\perp}$ and to V to obtain the required V'. We know that $V \oplus V'$ is nondegenerate and orthogonal to W, which is also nondegenerate, so $(V \oplus V') \overset{\perp}{\oplus} W = V' \oplus U$ is nondegenerate.

We leave the second statement about extending f as an exercise (use the fact that $f(U) = f(V) \overset{\perp}{\oplus} f(W)$, where $V_1 = f(V)$ is totally isotropic of dimension r, to find another totally isotropic susbpace V_1' of dimension r such that $V_1 \cap V_1' = (0)$ and $V_1 \oplus V_1'$ is orthogonal to $f(W)$). □

The subspace $(V \oplus V') \overset{\perp}{\oplus} W = V' \oplus U$ is often called a *nondegenerate completion* of U. The subspace $V \oplus V'$ is called an *Artinian space*. Proposition 29.29 show that $V \oplus V'$ has a basis $(u_1, v_1, \ldots, u_r, v_r)$ consisting of vectors $u_i \in V$ and $v_j \in V'$ such that $\varphi(u_i, u_j) = \delta_{ij}$. The subspace spanned by (u_i, v_i) is an Artinian plane, so $V \oplus V'$ is the orthogonal direct sum of r Artinian planes. Such a space is often denoted by Ar_{2r}.

In order to obtain the stronger version of the Witt decomposition when φ has some nonzero isotropic vector and W is anisotropic we now sharpen Proposition 29.29

Theorem 29.33. *Let φ be an ϵ-Hermitian form on E which is nondegenerate and satisfies property (T). Let U_1 and U_2 be two totally isotropic maximal subspaces of E, with U_1 or U_2 of finite dimension ≥ 1. Write $U = U_1 \cap U_2$, let S_1 be a supplement of U in U_1 and S_2 be a supplement of U in U_2 (so that $U_1 = U \oplus S_1$, $U_2 = U \oplus S_2$), and let $S = S_1 + S_2$. Then, there exist two subspaces W and D of E such that:*

(a) The subspaces S, $U + W$, and D are nondegenerate and pairwise orthogonal.

(b) *We have a direct sum* $E = S \overset{\perp}{\oplus} (U \oplus W) \overset{\perp}{\oplus} D$.

(c) *The subspace* D *contains no nonzero isotropic vector* (D *is anisotropic).*

(d) *The subspace* W *is totally isotropic.*

Furthermore, U_1 *and* U_2 *are both finite dimensional, and we have* $\dim(U_1) = \dim(U_2)$*,* $\dim(W) = \dim(U)$*,* $\dim(S_1) = \dim(S_2)$*, and* $\operatorname{codim}(D) = 2\dim(F_1)$*.*

Proof. First observe that if X is a totally isotropic maximal subspace of E, then any isotropic vector $x \in E$ orthogonal to X must belong to X, since otherwise, $X + Kx$ would be a totally isotropic subspace strictly containing X, contradicting the maximality of X. As a consequence, if x_i is any isotropic vector such that $x_i \in U_i^{\perp}$ (for $i = 1, 2$), then $x_i \in U_i$.

We claim that
$$S_1 \cap S_2^{\perp} = (0) \quad \text{and} \quad S_2 \cap S_1^{\perp} = (0).$$
Assume that $y \in S_1$ is orthogonal to S_2. Since $U_1 = U \oplus S_1$ and U_1 is totally isotropic, y is orthogonal to U_1, and thus orthogonal to U, so that y is orthogonal to $U_2 = U \oplus S_2$. Since $S_1 \subseteq U_1$ and U_1 is totally isotropic, y is an isotropic vector orthogonal to U_2, which by a previous remark implies that $y \in U_2$. Then, since $S_1 \subseteq U_1$ and $U \oplus S_1$ is a direct sum, we have
$$y \in S_1 \cap U_2 = S_1 \cap U_1 \cap U_2 = S_1 \cap U = (0).$$
Therefore $S_1 \cap S_2^{\perp} = (0)$. A similar proof show that $S_2 \cap S_1^{\perp} = (0)$. If U_1 is finite-dimensional (the case where U_2 is finite-dimensional is similar), then S_1 is finite-dimensional, so by Proposition 29.13, $S_1^{\perp}$ has finite codimension. Since $S_2 \cap S_1^{\perp} = (0)$, and since any supplement of $S_1^{\perp}$ has finite dimension, we must have
$$\dim(S_2) \leq \operatorname{codim}(S_1^{\perp}) = \dim(S_1).$$
By a similar argument, $\dim(S_1) \leq \dim(S_2)$, so we have
$$\dim(S_1) = \dim(S_2).$$
By Proposition 29.29(1), we conclude that $S = S_1 + S_2$ is nondegenerate.

By Proposition 29.21, the subspace $N = S^{\perp} = (S_1 + S_2)^{\perp}$ is nondegenerate. Since $U_1 = U \oplus S_1$, $U_2 = U \oplus S_2$, and U_1, U_2 are totally isotropic, U is orthogonal to S_1 and to S_2, so $U \subseteq N$. Since U is totally isotropic, by Proposition 29.30 applied to N, there is a totally isotropic subspace W of N such that $\dim(W) = \dim(U)$, $U \cap W = (0)$, and $U + W$ is nondegenerate. Consequently, (d) is satisfied by W.

To satisfy (a) and (b), we pick D to be the orthogonal of $U \oplus W$ in N. Then, $N = (U \oplus W) \overset{\perp}{\oplus} D$ and $E = S \overset{\perp}{\oplus} N$, so $E = S \overset{\perp}{\oplus} (U \oplus W) \overset{\perp}{\oplus} D$.

As to (c), since D is orthogonal $U \oplus W$, D is orthogonal to U, and since $D \subseteq N$ and N is orthogonal to $S_1 + S_2$, D is orthogonal to S_1, so D is orthogonal to $U_1 = U \oplus S_1$. If $y \in D$

is any isotropic vector, since $y \in U_1^\perp$, by a previous remark, $y \in U_1$, so $y \in D \cap U_1$. But, $D \subseteq N$ with $N \cap (S_1 + S_2) = (0)$, and $D \cap (U + W) = (0)$, so $D \cap (U + S_1) = D \cap U_1 = (0)$, which yields $y = 0$. The statements about dimensions are easily obtained. □

Finally, Theorem 29.33 yields the strong form of the Witt decomposition in which W is anistropic. Given any matrix $A \in \mathrm{M}_n(K)$, we say that A is *definite* if $x^\top Ax \neq 0$ for all $x \in K^n$.

Theorem 29.34. *Let φ be an ϵ-Hermitian form on E which is nondegenerate and satisfies property (T).*

(1) Any two totally isotropic maximal spaces of finite dimension have the same dimension.

(2) For any totally isotropic maximal subspace U of finite dimension $r \geq 1$, there is another totally isotropic maximal subspace U' of dimension r such that $U \cap U' = (0)$, and $U \oplus U'$ is nondegenerate. Furthermore, if $D = (U \oplus U')^\perp$, then (U, U', D) is a Witt decomposition of E; that is, there are no nonzero isotropic vectors in D (D is anisotropic).

(3) If E has finite dimension $n \geq 1$ and there is some nonzero isotropic vector for φ (E is not anisotropic), then E has a nontrivial Witt decomposition (U, U', D) as in (2). There is a basis of E such that

(a) if φ is alternating ($\epsilon = -1$ and $\lambda = \overline{\lambda}$ for all $\lambda \in K$), then $n = 2m$ and φ is represented by a matrix of the form

$$\begin{pmatrix} 0 & I_m \\ -I_m & 0 \end{pmatrix}$$

(b) if φ is symmetric ($\epsilon = +1$ and $\lambda = \overline{\lambda}$ for all $\lambda \in K$), then φ is represented by a matrix of the form

$$\begin{pmatrix} 0 & I_r & 0 \\ I_r & 0 & 0 \\ 0 & 0 & P \end{pmatrix},$$

where either $n = 2r$ and P does not occur, or $n > 2r$ and P is a definite symmetric matrix.

(c) if φ is ϵ-Hermitian (the involutive automorphism $\lambda \mapsto \overline{\lambda}$ is not the identity), then φ is represented by a matrix of the form

$$\begin{pmatrix} 0 & I_r & 0 \\ \epsilon I_r & 0 & 0 \\ 0 & 0 & P \end{pmatrix},$$

where either $n = 2r$ and P does not occur, or $n > 2r$ and P is a definite matrix such that $P^* = \epsilon P$.

Proof. Part (1) follows from Theorem 29.33. By Proposition 29.30, we obtain a totally isotropic subspace U' of dimension r such that $U \cap U' = (0)$. By applying Theorem 29.33 to $U_1 = U$ and $U_2 = U'$, we get $U = W = (0)$, which proves (2). Part (3) is an immediate consequence of (2). □

As a consequence of Theorem 29.34, we make the following definition.

Definition 29.19. Let E be a vector space of finite dimension n, and let φ be an ϵ-Hermitian form on E which is nondegenerate and satisfies property (T). The *index* (or *Witt index*) ν of φ, is the common dimension of all totally isotropic maximal subspaces of E. We have $2\nu \leq n$.

Neutral forms only exist if n is even, in which case, $\nu = n/2$. Forms of index $\nu = 0$ have no nonzero isotropic vectors. When $K = \mathbb{R}$, this is satisfied by positive definite or negative definite symmetric forms. When $K = \mathbb{C}$, this is satisfied by positive definite or negative definite Hermitian forms. The vector space of a neutral Hermitian form ($\epsilon = +1$) is an Artinian space, and the vector space of a neutral alternating form is a hyperbolic space.

If the field K is algebraically closed, we can describe all nondegenerate quadratic forms.

Proposition 29.35. *If K is algebraically closed and E has dimension n, then for every nondegenerate quadratic form Φ, there is a basis $(e_1, \ldots, e_n)$ such that Φ is given by*

$$\Phi\left(\sum_{i-1}^{n} x_i e_i\right) = \begin{cases} \sum_{i=1}^{m} x_i x_{m+i} & \text{if } n = 2m \\ \sum_{i=1}^{m} x_i x_{m+i} + x_{2m+1}^2 & \text{if } n = 2m+1. \end{cases}$$

Proof. We work with the polar form φ of Φ. Let U_1 and U_2 be some totally isotropic subspaces such that $U_1 \cap U_2 = (0)$ given by Theorem 29.34, and let q be their common dimension. Then, $W = U = (0)$. Since we can pick bases $(e_1, \ldots e_q)$ in U_1 and $(e_{q+1}, \ldots, e_{2q})$ in U_2 such that $\varphi(e_i, e_{i+q}) = 0$, for $i, j = 1, \ldots, q$, it suffices to proves that $\dim(D) \leq 1$. If $x, y \in D$ with $x \neq 0$, from the identity

$$\Phi(y - \lambda x) = \Phi(y) - \lambda\varphi(x, y) + \lambda^2\Phi(x)$$

and the fact that $\Phi(x) \neq 0$ since $x \in D$ and $x \neq 0$, we see that the equation $\Phi(y - \lambda y) = 0$ has at least one solution. Since $\Phi(z) \neq 0$ for every nonzero $z \in D$, we get $y = \lambda x$, and thus $\dim(D) \leq 1$, as claimed. □

Proposition 29.35 shows that for every nondegenerate quadratic form Φ over an algebraically closed field, if $\dim(E) = 2m$ or $\dim(E) = 2m + 1$ with $m \geq 1$, then Φ has some nonzero isotropic vector.

29.8 Symplectic Groups

In this section, we are dealing with a nondegenerate alternating form φ on a vector space E of dimension n. As we saw earlier, n must be even, say $n = 2m$. By Theorem 29.24, there is a direct sum decomposition of E into pairwise orthogonal subspaces

$$E = W_1 \overset{\perp}{\oplus} \cdots \overset{\perp}{\oplus} W_m,$$

where each W_i is a hyperbolic plane. Each W_i has a basis (u_i, v_i), with $\varphi(u_i, u_i) = \varphi(v_i, v_i) = 0$ and $\varphi(u_i, v_i) = 1$, for $i = 1, \ldots, m$. In the basis

$$(u_1, \ldots, u_m, v_1, \ldots, v_m),$$

φ is represented by the matrix

$$J_{m,m} = \begin{pmatrix} 0 & I_m \\ -I_m & 0 \end{pmatrix}.$$

The symplectic group $\mathbf{Sp}(2m, K)$ is the group of isometries of φ. The maps in $\mathbf{Sp}(2m, K)$ are called *symplectic* maps. With respect to the above basis, $\mathbf{Sp}(2m, K)$ is the group of $2m \times 2m$ matrices A such that

$$A^\top J_{m,m} A = J_{m,m}.$$

Matrices satisfying the above identity are called *symplectic* matrices. In this section, we show that $\mathbf{Sp}(2m, K)$ is a subgroup of $\mathbf{SL}(2m, K)$ (that is, $\det(A) = +1$ for all $A \in \mathbf{Sp}(2m, K)$), and we show that $\mathbf{Sp}(2m, K)$ is generated by special linear maps called *symplectic transvections*.

First, we leave it as an easy exercise to show that $\mathbf{Sp}(2, K) = \mathbf{SL}(2, K)$. The reader should also prove that $\mathbf{Sp}(2m, K)$ has a subgroup isomorphic to $\mathbf{GL}(m, K)$.

Next we characterize the symplectic maps f that leave fixed every vector in some given hyperplane H, that is,

$$f(v) = v \quad \text{for all } v \in H.$$

Since φ is nondegenerate, by Proposition 29.22, the orthogonal $H^\perp$ of H is a line (that is, $\dim(H^\perp) = 1$). For every $u \in E$ and every $v \in H$, since f is an isometry and $f(v) = v$ for all $v \in H$, we have

$$\begin{aligned}
\varphi(f(u) - u, v) &= \varphi(f(u), v) - \varphi(u, v) \\
&= \varphi(f(u), v) - \varphi(f(u), f(v)) \\
&= \varphi(f(u), v - f(v))) \\
&= \varphi(f(u), 0) = 0,
\end{aligned}$$

which shows that $f(u) - u \in H^\perp$ for all $u \in E$. Therefore, $f - \mathrm{id}$ is a linear map from E into the line $H^\perp$ whose kernel contains H, which means that there is some nonzero vector $w \in H^\perp$ and some linear form ψ such that

$$f(u) = u + \psi(u)w, \quad u \in E.$$

Since f is an isometry, we must have $\varphi(f(u), f(v)) = \varphi(u, v)$ for all $u, v \in E$, which means that

$$\begin{aligned} \varphi(u, v) &= \varphi(f(u), f(v)) \\ &= \varphi(u + \psi(u)w, v + \psi(v)w) \\ &= \varphi(u, v) + \psi(u)\varphi(w, v) + \psi(v)\varphi(u, w) + \psi(u)\psi(v)\varphi(w, w) \\ &= \varphi(u, v) + \psi(u)\varphi(w, v) - \psi(v)\varphi(w, u), \end{aligned}$$

which yields

$$\psi(u)\varphi(w, v) = \psi(v)\varphi(w, u) \quad \text{for all } u, v \in E.$$

Since φ is nondegenerate, we can pick some v_0 such that $\varphi(w, v_0) \neq 0$, and we get $\psi(u)\varphi(w, v_0) = \psi(v_0)\varphi(w, u)$ for all $u \in E$; that is,

$$\psi(u) = \lambda\varphi(w, u) \quad \text{for all } u \in E,$$

for some $\lambda \in K$. Therefore, f is of the form

$$f(u) = u + \lambda\varphi(w, u)w, \quad \text{for all } u \in E.$$

It is also clear that every f of the above form is a symplectic map. If $\lambda = 0$, then $f = \mathrm{id}$. Otherwise, if $\lambda \neq 0$, then $f(u) = u$ iff $\varphi(w, u) = 0$ iff $u \in (Kw)^{\perp} = H$, where H is a hyperplane. Thus, f fixes every vector in the hyperplane H. Note that since φ is alternating, $\varphi(w, w) = 0$, which means that $w \in H$.

In summary, we have characterized all the symplectic maps that leave every vector in some hyperplane fixed, and we make the following definition.

Definition 29.20. Given a nondegenerate alternating form φ on a space E, a *symplectic transvection (of direction w)* is a linear map f of the form

$$f(u) = u + \lambda\varphi(w, u)w, \quad \text{for all } u \in E,$$

for some nonzero $w \in E$ and some $\lambda \in K$. If $\lambda \neq 0$, the subspace of vectors left fixed by f is the hyperplane $H = (Kw)^{\perp}$. The map f is also denoted $\tau_{w,\lambda}$.

Observe that

$$\tau_{w,\lambda} \circ \tau_{w,\mu} = \tau_{w,\lambda+\mu}$$

and $\tau_{w,\lambda} = \mathrm{id}$ iff $\lambda = 0$. The above shows that $\det(\tau_{w,\lambda}) = 1$, since when $\lambda \neq 0$, we have $\tau_{w,\lambda} = (\tau_{w,\lambda/2})^2$.

Our next goal is to show that if u and v are any two nonzero vectors in E, then there is a simple symplectic map f such that $f(u) = v$.

Proposition 29.36. *Given any two nonzero vectors $u, v \in E$, there is a symplectic map f such that $f(u) = v$, and f is either a symplectic transvection, or the composition of two symplectic transvections.*

Proof. There are two cases.

Case 1. $\varphi(u, v) \neq 0$.

In this case, $u \neq v$, since $\varphi(u, u) = 0$. Let us look for a symplectic transvection of the form $\tau_{v-u,\lambda}$. We want

$$v = u + \lambda\varphi(v - u, u)(v - u) = u + \lambda\varphi(v, u)(v - u),$$

which yields

$$(\lambda\varphi(v, u) - 1)(v - u) = 0.$$

Since $\varphi(u, v) \neq 0$ and $\varphi(v, u) = -\varphi(u, v)$, we can pick $\lambda = \varphi(v, u)^{-1}$ and $\tau_{v-u,\lambda}$ maps u to v.

Case 2. $\varphi(u, v) = 0$.

If $u = v$, use $\tau_{u,0} = \mathrm{id}$. Now, assume $u \neq v$. We claim that it is possible to pick some $w \in E$ such that $\varphi(u, w) \neq 0$ and $\varphi(v, w) \neq 0$. Indeed, if $(Ku)^{\perp} = (Kv)^{\perp}$, then pick any nonzero vector w not in the hyperplane $(Ku)^{\perp}$. Othwerwise, $(Ku)^{\perp}$ and $(Kv)^{\perp}$ are two distinct hyperplanes, so neither is contained in the other (they have the same dimension), so pick any nonzero vector w_1 such that $w_1 \in (Ku)^{\perp}$ and $w_1 \notin (Kv)^{\perp}$, and pick any nonzero vector w_2 such that $w_2 \in (Kv)^{\perp}$ and $w_2 \notin (Ku)^{\perp}$. If we let $w = w_1 + w_2$, then $\varphi(u, w) = \varphi(u, w_2) \neq 0$, and $\varphi(v, w) = \varphi(v, w_1) \neq 0$. From case 1, we have some symplectic transvection τ_{w-u,λ_1} such that $\tau_{w-u,\lambda_1}(u) = w$, and some symplectic transvection τ_{v-w,λ_2} such that $\tau_{v-w,\lambda_2}(w) = v$, so the composition $\tau_{v-w,\lambda_2} \circ \tau_{w-u,\lambda_1}$ maps u to v. □

Next, we would like to extend Proposition 29.36 to two hyperbolic planes W_1 and W_2.

Proposition 29.37. *Given any two hyperbolic planes W_1 and W_2 given by bases (u_1, v_1) and (u_2, v_2) (with $\varphi(u_i, u_i) = \varphi(v_i, v_i) = 0$ and $\varphi(u_i, v_i) = 1$, for $i = 1, 2$), there is a symplectic map f such that $f(u_1) = u_2$, $f(v_1) = v_2$, and f is the composition of at most four symplectic transvections.*

Proof. From Proposition 29.36, we can map u_1 to u_2, using a map f which is the composition of at most two symplectic transvections. Say $v_3 = f(v_1)$. We claim that there is a map g such that $g(u_2) = u_2$ and $g(v_3) = v_2$, and g is the composition of at most two symplectic transvections. If so, $g \circ f$ maps the pair (u_1, v_1) to the pair (u_2, v_2), and $g \circ f$ consists of at most four symplectic transvections. Thus, we need to prove the following claim:

Claim. If (u, v) and (u, v') are hyperbolic bases determining two hyperbolic planes, then there is a symplectic map g such that $g(u) = u$, $g(v) = v'$, and g is the composition of at most two symplectic transvections. There are two case.

Case 1. $\varphi(v, v') \neq 0$.

In this case, there is a symplectic transvection $\tau_{v'-v,\lambda}$ such that $\tau_{v'-v,\lambda}(v) = v'$. We also have

$$\varphi(u, v' - v) = \varphi(u, v') - \varphi(u, v) = 1 - 1 = 0.$$

Therefore, $\tau_{v'-v,\lambda}(u) = u$, and $g = \tau_{v'-v,\lambda}$ does the job.

Case 2. $\varphi(v, v') = 0$.

First, check that $(u, u + v)$ is a also hyperbolic basis. Furthermore,

$$\varphi(v, u + v) = \varphi(v, u) + \varphi(v, v) = \varphi(v, u) = -1 \neq 0.$$

Thus, there is a symplectic transvection τ_{v,λ_1} such that $\tau_{u,\lambda_1}(v) = u + v$ and $\tau_{u,\lambda_1}(u) = u$. We also have

$$\varphi(u + v, v') = \varphi(u, v') + \varphi(v, v') = \varphi(u, v') = 1 \neq 0,$$

so there is a symplectic transvection $\tau_{v'-u-v,\lambda_2}$ such that $\tau_{v'-u-v,\lambda_2}(u + v) = v'$. Since

$$\varphi(u, v' - u - v) = \varphi(u, v') - \varphi(u, u) - \varphi(u, v) = 1 - 0 - 1 = 0,$$

we have $\tau_{v'-u-v,\lambda_2}(u) = u$. Then, the composition $g = \tau_{v'-u-v,\lambda_2} \circ \tau_{u,\lambda_1}$ is such that $g(u) = u$ and $g(v) = v'$. □

We will use Proposition 29.37 in an inductive argument to prove that the symplectic transvections generate the symplectic group. First, make the following observation: If U is a nondegenerate subspace of E, so that

$$E = U \overset{\perp}{\oplus} U^{\perp},$$

and if τ is a transvection of $H^{\perp}$, then we can form the linear map $\mathrm{id}_U \overset{\perp}{\oplus} \tau$ whose restriction to U is the identity and whose restriction to $U^{\perp}$ is τ, and $\mathrm{id}_U \overset{\perp}{\oplus} \tau$ is a transvection of E.

Theorem 29.38. *The symplectic group* $\mathbf{Sp}(2m, K)$ *is generated by the symplectic transvections. For every transvection* $f \in \mathbf{Sp}(2m, K)$*, we have* $\det(f) = 1$.

Proof. Let G be the subgroup of $\mathbf{Sp}(2m, K)$ generated by the transvections. We need to prove that $G = \mathbf{Sp}(2m, K)$. Let $(u_1, v_1, \ldots, u_m, v_m)$ be a symplectic basis of E, and let $f \in \mathbf{Sp}(2m, K)$ be any symplectic map. Then, f maps $(u_1, v_1, \ldots, u_m, v_m)$ to another symplectic basis $(u'_1, v'_1, \ldots, u'_m, v'_m)$. If we prove that there is some $g \in G$ such that $g(u_i) = u'_i$ and $g(v_i) = v'_i$ for $i = 1, \ldots, m$, then $f = g$ and $G = \mathbf{Sp}(2m, K)$.

We use induction on i to prove that there is some $g_i \in G$ so that g_i maps $(u_1, v_1, \ldots, u_i, v_i)$ to $(u'_1, v'_1, \ldots, u'_i, v'_i)$.

The base case $i = 1$ follows from Proposition 29.37.

For the induction step, assume that we have some $g_i \in G$ mapping $(u_1, v_1, \ldots, u_i, v_i)$ to $(u'_1, v'_1, \ldots, u'_i, v'_i)$, and let $(u''_{i+1}, v''_{i+1}, \ldots, u''_m, v''_m)$ be the image of $(u_{i+1}, v_{i+1}, \ldots, u_m, v_m)$ by g_i. If U is the subspace spanned by $(u'_1, v'_1, \ldots, u'_m, v'_m)$, then each hyperbolic plane W'_{i+k} given by (u'_{i+k}, v'_{i+k}) and each hyperbolic plane W''_{i+k} given by (u''_{i+k}, v''_{i+k}) belongs to

$U^{\perp}$. Using the remark before the theorem and Proposition 29.37, we can find a transvection τ mapping W''_{i+1} onto W'_{i+1} and leaving every vector in U fixed. Then, $\tau \circ g_i$ maps $(u_1, v_1, \ldots, u_{i+1}, v_{i+1})$ to $(u'_1, v'_1, \ldots, u'_{i+1}, v'_{i+1})$, establishing the induction step.

For the second statement, since we already proved that every transvection has a determinant equal to $+1$, this also holds for any composition of transvections in G, and since $G = \mathbf{Sp}(2m, K)$, we are done. □

It can also be shown that the center of $\mathbf{Sp}(2m, K)$ is reduced to the subgroup $\{\mathrm{id}, -\mathrm{id}\}$. The *projective symplectic group* $\mathbf{PSp}(2m, K)$ is the quotient group $\mathbf{PSp}(2m, K)/\{\mathrm{id}, -\mathrm{id}\}$. All symplectic projective groups are simple, except $\mathbf{PSp}(2, \mathbb{F}_2), \mathbf{PSp}(2, \mathbb{F}_3)$, and $\mathbf{PSp}(4, \mathbb{F}_2)$, see Grove [83].

The orders of the symplectic groups over finite fields can be determined. For details, see Artin [6], Jacobson [97] and Grove [83].

An interesting property of symplectic spaces is that the determinant of a skew-symmetric matrix B is the square of some polynomial $\mathrm{Pf}(B)$ called the *Pfaffian*; see Jacobson [97] and Artin [6]. We leave considerations of the Pfaffian to the exercises.

We now take a look at the orthogonal groups.

29.9 Orthogonal Groups and the Cartan–Dieudonné Theorem

In this section we are dealing with a nondegenerate symmetric bilinear from φ over a finite-dimensional vector space E of dimension n over a field of characateristic not equal to 2. Recall that the orthogonal group $\mathbf{O}(\varphi)$ is the group of isometries of φ; that is, the group of linear maps $f \colon E \to E$ such that

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

The elements of $\mathbf{O}(\varphi)$ are also called *orthogonal transformations*. If M is the matrix of φ in any basis, then a matrix A represents an orthogonal transformation iff

$$A^{\top} M A = M.$$

Since φ is nondegenerate, M is invertible, so we see that $\det(A) = \pm 1$. The subgroup

$$\mathbf{SO}(\varphi) = \{f \in \mathbf{O}(\varphi) \mid \det(f) = 1\}$$

is called the *special orthogonal group* (of φ), and its members are called *rotations* (or *proper orthogonal transformations*). Isometries $f \in \mathbf{O}(\varphi)$ such that $\det(f) = -1$ are called *improper orthogonal transformations*, or sometimes *reversions*.

If H is any nondegenerate hyperplane in E, then $D = H^{\perp}$ is a nondegenerate line and we have

$$E = H \overset{\perp}{\oplus} H^{\perp}.$$

For any nonzero vector $u \in D = H^{\perp}$ Consider the map τ_u given by

$$\tau_u(v) = v - 2\frac{\varphi(v, u)}{\varphi(u, u)}u \quad \text{for all } v \in E.$$

If we replace u by λu with $\lambda \neq 0$, we have

$$\tau_{\lambda u}(v) = v - 2\frac{\varphi(v, \lambda u)}{\varphi(\lambda u, \lambda u)}\lambda u = v - 2\frac{\lambda\varphi(v, u)}{\lambda^2\varphi(u, u)}\lambda u = v - 2\frac{\varphi(v, u)}{\varphi(u, u)}u,$$

which shows that τ_u depends only on the line D, and thus only the hyperplane H. Therefore, denote by τ_H the linear map τ_u determined as above by any nonzero vector $u \in H^{\perp}$. Note that if $v \in H$, then

$$\tau_H(v) = v,$$

and if $v \in D$, then

$$\tau_H(v) = -v.$$

A simple computation shows that

$$\varphi(\tau_H(u), \tau_H(v)) = \varphi(u, v) \quad \text{for all } u, v \in E,$$

so $\tau_H \in \mathbf{O}(\varphi)$, and by picking a basis consisting of u and vectors in H, that $\det(\tau_H) = -1$. It is also clear that $\tau_H^2 = \mathrm{id}$.

Definition 29.21. If H is any nondegenerate hyperplane in E, for any nonzero vector $u \in H^{\perp}$, the linear map τ_H given by

$$\tau_H(v) = v - 2\frac{\varphi(v, u)}{\varphi(u, u)}u \quad \text{for all } v \in E$$

is an involutive isometry of E called the *reflection through (or about) the hyperplane H*.

Remarks:

1. It can be shown that if $f \in \mathbf{O}(\varphi)$ leaves every vector in some hyperplane H fixed, then either $f = \mathrm{id}$ or $f = \tau_H$; see Taylor [172] (Chapter 11). Thus, there is no analog to symplectic transvections in the orthogonal group.

2. If $K = \mathbb{R}$ and φ is the usual Euclidean inner product, the matrices corresponding to hyperplane reflections are called *Householder matrices*.

Our goal is to prove that $\mathbf{O}(\varphi)$ is generated by the hyperplane reflections. The following proposition is needed.

Proposition 29.39. *Let φ be a nondegenerate symmetric bilinear form on a vector space E. For any two nonzero vectors $u, v \in E$, if $\varphi(u, u) = \varphi(v, v)$ and $v - u$ is nonisotropic, then the hyperplane reflection $\tau_H = \tau_{v-u}$ maps u to v, with $H = (K(v-u))^{\perp}$.*

Proof. Since $v - u$ is not isotropic, $\varphi(v - u, v - u) \neq 0$, and we have

$$\begin{aligned}
\tau_{v-u}(u) &= u - 2\frac{\varphi(u, v-u)}{\varphi(v-u, v-u)}(v-u) \\
&= u - 2\frac{\varphi(u, v) - \varphi(u, u)}{\varphi(v, v) - 2\varphi(u, v) + \varphi(u, u)}(v-u) \\
&= u - \frac{2(\varphi(u, v) - \varphi(u, u))}{2(\varphi(u, u) - 2\varphi(u, v))}(v-u) \\
&= v,
\end{aligned}$$

which proves the proposition. □

We can now obtain a cheap version of the Cartan–Dieudonné theorem.

Theorem 29.40. *(Cartan–Dieudonné, weak form) Let φ be a nondegenerate symmetric bilinear form on a K-vector space E of dimension n (*$\mathrm{char}(K) \neq 2$*). Then, every isometry $f \in \mathbf{O}(\varphi)$ with $f \neq \mathrm{id}$ is the composition of at most $2n - 1$ hyperplane reflections.*

Proof. We proceed by induction on n. For $n = 0$, this is trivial (since $\mathbf{O}(\varphi) = \{\mathrm{id}\}$).

Next, assume that $n \geq 1$. Since φ is nondegenerate, we know that there is some nonisotropic vector $u \in E$. There are three cases.

Case 1. $f(u) = u$.

Since φ is nondegenrate and u is nonisotropic, the hyperplane $H = (Ku)^{\perp}$ is nondegenerate, $E = H \overset{\perp}{\oplus} Ku$, and since $f(u) = u$, we must have $f(H) = H$. The restriction f' of of f to H is an isometry of H. By the induction hypothesis, we can write

$$f' = \tau'_k \circ \cdots \circ \tau'_1,$$

where τ_i is some hyperplane reflection about a hyperplane L_i in H, with $k \leq 2n - 3$. We can extend each τ'_i to a reflection τ_i about the hyperplane $L_i \overset{\perp}{\oplus} Ku$ so that $\tau_i(u) = u$, and clearly,

$$f = \tau_k \circ \cdots \circ \tau_1.$$

Case 2. $f(u) = -u$.

If τ is the hyperplane reflection about the hyperplane $H = (Ku)^{\perp}$, then $g = \tau \circ f$ is an isometry of E such that $g(u) = u$, and we are back to Case (1). Since $\tau^2 = 1$ We obtain

$$f = \tau \circ \tau_k \circ \cdots \circ \tau_1$$

where τ and the τ_i are hyperplane reflections, with $k \geq 2n-3$, and we get a total of $2n-2$ hyperplane reflections.

Case 3. $f(u) \neq u$ and $f(u) \neq -u$.

Note that $f(u)-u$ and $f(u)+u$ are orthogonal, since

$$\begin{aligned}\varphi(f(u)-u, f(u)+u) &= \varphi(f(u), f(u)) + \varphi(f(u), u) - \varphi(u, f(u)) - \varphi(u,u)\\ &= \varphi(u,u) - \varphi(u,u) = 0.\end{aligned}$$

We also have

$$\begin{aligned}\varphi(u,u) &= \varphi((f(u)+u-(f(u)-u))/2, (f(u)+u-(f(u)-u))/2)\\ &= \frac{1}{4}\varphi(f(u)+u, f(u)+u) + \frac{1}{4}\varphi(f(u)-u, f(u)-u),\end{aligned}$$

so $f(u)+u$ and $f(u)-u$ cannot be both isotropic, since u is not isotropic.

If $f(u)-u$ is not isotropic, then the reflection $\tau_{f(u)-u}$ is such that

$$\tau_{f(u)-u}(u) = f(u),$$

and since $\tau_{f(u)-u}^2 = \mathrm{id}$, if $g = \tau_{f(u)-u} \circ f$, then $g(u) = u$, and we are back to case (1). We obtain

$$f = \tau_{f(u)-u} \circ \tau_k \circ \cdots \circ \tau_1$$

where $\tau_{f(u)-u}$ and the τ_i are hyperplane reflections, with $k \geq 2n-3$, and we get a total of $2n-2$ hyperplane reflections.

If $f(u)+u$ is not isotropic, then the reflection $\tau_{f(u)+u}$ is such that

$$\tau_{f(u)+u}(u) = -f(u),$$

and since $\tau_{f(u)+u}^2 = \mathrm{id}$, if $g = \tau_{f(u)+u} \circ f$, then $g(u) = -u$, and we are back to case (2). We obtain

$$f = \tau_{f(u)-u} \circ \tau \circ \tau_k \circ \cdots \circ \tau_1$$

where $\tau, \tau_{f(u)-u}$ and the τ_i are hyperplane reflections, with $k \geq 2n-3$, and we get a total of $2n-1$ hyperplane reflections. This proves the induction step. □

The bound $2n-1$ is not optimal. The strong version of the Cartan–Dieudonné theorem says that at most n reflections are needed, but the proof is harder. Here is a neat proof due to E. Artin (see [6], Chapter III, Section 4).

Case 1 remains unchanged. Case 2 is slightly different: $f(u)-u \neq 0$ is not isotropic. Since $\varphi(f(u)+u, f(u)-u) = 0$, as in the first subcase of Case (3), $g = \tau_{f(u)-u} \circ f$ is such that $g(u) = u$ and we are back to Case 1. This only costs one more reflection.

The new (bad) case is:

Case 3'. $f(u) - u$ is nonzero and isotropic for all nonisotropic $u \in E$. In this case, what saves us is that E must be an Artinian space of dimension $n = 2m$ and that f must be a rotation ($f \in \mathbf{SO}(\varphi)$).

If we acccept this fact proved in Proposition 29.43 then pick any hyperplane reflection τ. Then, since f is a rotation, $g = \tau \circ f$ is *not* a rotation because $\det(g) = \det(\tau)\det(f) = (-1)(+1) = -1$, so $g(u) - u$ is either 0 or not isotropic for some nonisotropic $u \in E$ (otherwise, g would be a rotation), we are back to either Case 1 or Case 2, and using the induction hypothesis, we get

$$\tau \circ f = \tau_k \circ \ldots, \tau_1,$$

where each τ_i is a hyperplane reflection, and $k \leq 2m$. Since $\tau \circ f$ is not a rotation, actually $k \leq 2m - 1$, and then $f = \tau \circ \tau_k \circ \ldots, \tau_1$, the composition of at most $k + 1 \leq 2m$ hyperplane reflections.

Therefore, except for the fact that in Case 3', E must be an Artinian space of dimension $n = 2m$ and that f must be a rotation, which has not been proven yet, we proved the following theorem.

Theorem 29.41. *(Cartan–Dieudonné, strong form) Let φ be a nondegenerate symmetric bilinear form on a K-vector space E of dimension n ($\mathrm{char}(K) \neq 2$). Then, every isometry $f \in \mathbf{O}(\varphi)$ with $f \neq \mathrm{id}$ is the composition of at most n hyperplane reflections.*

To fill in the gap, we need two propositions.

Proposition 29.42. *Let (E, φ) be an Artinian space of dimension $2m$, and let U be a totally isotropic subspace of dimension m. For any isometry $f \in \mathbf{O}(\varphi)$, if $f(U) = U$, then $\det(f) = 1$ (f is a rotation).*

Proof. We know that we can find a basis $(u_1, \ldots, u_m, v_1, \ldots, v_m)$ of E such $(u_1, \ldots, u_m)$ is a basis of U and φ is represented by the matrix

$$\begin{pmatrix} 0 & I_m \\ I_m & 0 \end{pmatrix}.$$

Since $f(U) = U$, the matrix representing f is of the form

$$A = \begin{pmatrix} B & C \\ 0 & D \end{pmatrix}.$$

The condition $A^\top A_{m,m} A = A_{m,m}$ translates as

$$\begin{pmatrix} B^\top & 0 \\ C^\top & D^\top \end{pmatrix} \begin{pmatrix} 0 & I_m \\ I_m & 0 \end{pmatrix} \begin{pmatrix} B & C \\ 0 & D \end{pmatrix} = \begin{pmatrix} 0 & I_m \\ I_m & 0 \end{pmatrix}$$

that is,

$$\begin{pmatrix} B^\top & 0 \\ C^\top & D^\top \end{pmatrix} \begin{pmatrix} 0 & D \\ B & C \end{pmatrix} = \begin{pmatrix} 0 & B^\top D \\ D^\top B & C^\top D + D^\top C \end{pmatrix} = \begin{pmatrix} 0 & I_m \\ I_m & 0 \end{pmatrix},$$

which implies that $B^\top D = I$, and so

$$\det(A) = \det(B)\det(D) = \det(B^\top)\det(D) = \det(B^\top D) = \det(I) = 1,$$

as claimed □

Proposition 29.43. *Let φ be a nondegenerate symmetric bilinear form on a space E of dimension n, and let f be any isometry $f \in \mathbf{O}(\varphi)$ such that $f(u) - u$ is nonzero and isotropic for every nonisotropic vector $u \in E$. Then, E is an Artinian space of dimension $n = 2m$, and f is a rotation ($f \in \mathbf{SO}(\varphi)$).*

Proof. We follow E. Artin's proof (see [6], Chapter III, Section 4). First, consider the case $n = 2$. Since we are assuming that E has some nonzero isotropic vector, by Proposition 29.26, E is an Artinian plane and there is a basis in which φ is represented by the matrix

$$\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix},$$

we have $\varphi((x_1, x_2), (x_1, x_2)) = 2x_1x_2$, and the matrices representing isometries are of the form

$$\begin{pmatrix} \lambda & 0 \\ 0 & \lambda^{-1} \end{pmatrix} \quad \text{or} \quad \begin{pmatrix} 0 & \lambda \\ \lambda^{-1} & 0 \end{pmatrix}, \quad \lambda \in K - \{0\}.$$

In the second case,

$$\begin{pmatrix} 0 & \lambda \\ \lambda^{-1} & 0 \end{pmatrix}\begin{pmatrix} \lambda \\ 1 \end{pmatrix} = \begin{pmatrix} \lambda \\ 1 \end{pmatrix},$$

but $u = (\lambda, 1)$ is a nonisotropic vector such that $f(u) - u = 0$. Therefore, we must be in the first case, and $\det(f) = +1$.

Let us now assume that $n \geq 3$. We are going to prove that $f(y) - y$ is isotropic for all nonzero isotropic vectors y. Let y be any nonzero isotropic vector. Since $n \geq 3$, the orthogonal space $(Ky)^\perp$ has dimension at least 2, and we know that $\mathrm{rad}(Ky) = \mathrm{rad}((Ky)^\perp)$, a space of dimension at most 1, which implies that $(Ky)^\perp$ contains some nonisotropic vector, say x. We have $\varphi(x, y) = 0$, so $\varphi(x + \epsilon y, x + \epsilon y) = \varphi(x, x) \neq 0$, for $\epsilon = \pm 1$. Then, by hypothesis, the vectors $f(x) - x, f(x + y) - (x + y) = f(x) - x + (f(y) - y)$, and $f(x - y) - (x - y) = f(x) - x - (f(y) - y)$ are isotropic. The last two vectors can be written as $f(x) - x) + \epsilon(f(y) - y)$ with $\epsilon = \pm 1$, so we have

$$\begin{aligned} 0 = \varphi(f(x) - x) + \epsilon(f(y) - y), f(x) - x) + \epsilon(f(y) - y)) \\ = 2\epsilon\varphi(f(x) - x, f(y) - y)) + \epsilon^2\varphi(f(y) - y, f(y) - y). \end{aligned}$$

If we write the two equations corresponding to $\epsilon = \pm 1$, and then add them up, we get

$$\varphi(f(y) - y, f(y) - y) = 0.$$

This proves that $f(y)-y$ is isotropic for any nonzero isotropic vector y. Since by hypothesis $f(u)-u$ is isotropic for every nonisotropic vector u, we proved that $f(u)-u$ is isotropic for *every* $u \in E$. If we let $W = \mathrm{Im}(f - \mathrm{id})$, then every vector in W is isotropic, and thus W is totally isotropic (recall that we assumed that $\mathrm{char}(K) \neq 2$, so φ is determined by Φ). For any $u \in E$ and any $v \in W^{\perp}$, since W is totally isotropic, we have

$$\varphi(f(u)-u, f(v)-v) = 0,$$

and since $f(u)-u \in W$ and $v \in W^{\perp}$, we have $\varphi(f(u)-u, v) = 0$, and so

$$\begin{aligned} 0 &= \varphi(f(u)-u, f(v)-v) \\ &= \varphi(f(u), f(v)) - \varphi(u, f(v)) - \varphi(f(u)-u, v) \\ &= \varphi(u,v) - \varphi(u, f(v)) \\ &= \varphi(u, v - f(v)), \end{aligned}$$

for all $u \in E$. Since φ is nonsingular, this means that $f(v) = v$, for all $v \in W^{\perp}$. However, by hypothesis, no nonisotropic vector is left fixed, which implies that $W^{\perp}$ is also totally isotropic. In summary, we proved that $W \subseteq W^{\perp}$ and $W^{\perp} \subseteq W^{\perp\perp} = W$, that is,

$$W = W^{\perp}.$$

Since, $\dim(W) + \dim(W^{\perp}) = n$, we conclude that W is a totally isotropic subspace of E such that

$$\dim(W) = n/2.$$

By Proposition 29.29, the space E is an Artinian space of dimension $n = 2m$. Since $W = W^{\perp}$ and $f(W) = W$, by Proposition 29.42, the isometry f is a rotation. □

Remarks:

1. Another way to finish the proof of Proposition 29.43 is to prove that if f is an isometry, then

   $$\mathrm{Ker}\,(f - \mathrm{id}) = (\mathrm{Im}(f - \mathrm{id}))^{\perp}.$$

   After having proved that $W = \mathrm{Im}(f - \mathrm{id})$ is totally isotropic, we get

   $$\mathrm{Ker}\,(f - \mathrm{id}) = \mathrm{Im}(f - \mathrm{id}),$$

   which implies that $(f - \mathrm{id})^2 = 0$. From this, we deduce that $\det(f) = 1$. For details, see Jacobson [97] (Chapter 6, Section 6).

2. If $f = \tau_{H_k} \circ \cdots \circ \tau_{H_1}$, where the H_i are hyperplanes, then it can be shown that

   $$\dim(H_1 \cap H_2 \cap \cdots \cap H_s) \geq n - s.$$

   Now, since each H_i is left fixed by τ_{H_i}, we see that every vector in $H_1 \cap \cdots \cap H_s$ is left fixed by f. In particular, if $s < n$, then f has some nonzero fixed point. As a consequence, an isometry without fixed points requires n hyperplane reflections.

29.10 Witt's Theorem

Witt's theorem was referred to as a "scandal" by Emil Artin. What he meant by this is that one had to wait until 1936 (Witt [188]) to formulate and prove a theorem at once so simple in its statement and underlying concepts, and so useful in various domains (geometry, arithmetic of quadratic forms).[1]

Besides Witt's original proof (Witt [188]), Chevalley's proof [37] seems to be the "best" proof that applies to the symmetric as well as the skew-symmetric case. The proof in Bourbaki [24] is based on Chevalley's proof, and so are a number of other proofs. This is the one we follow (slightly reorganized). In the symmetric case, Serre's exposition is hard to beat (see Serre [155], Chapter IV).

The following observation is one of the key ingredients in the proof of Theorem 29.45.

Proposition 29.44. *Given a finite-dimensional space E equipped with an ϵ-Hermitan form φ, if U_1 and U_2 are two subspaces of E such that $U_1 \cap U_2 = (0)$ and if we have metric linear maps $f_1 \colon U_1 \to E$ and $f_2 \colon U_2 \to E$ such that*

$$\varphi(f_1(u_1), f_2(u_2)) = \varphi(u_1, u_2) \quad \text{for } u_i \in U_i \ (i = 1, 2), \tag{$*$}$$

then the linear map $f \colon U_1 \oplus U_2 \to E$ given by $f(u_1 + u_2) = f_1(u_1) + f_2(u_2)$ extends f_1 and f_2 and is metric. Furthermore, if f_1 and f_2 are injective, then so if f.

Proof. Indeed, since f_1 and f_2 are metric and using $(*)$, we have

$$\begin{aligned}\varphi(f_1(u_1) + f_2(u_2), f_1(v_1) + f_2(v_2)) &= \varphi(f_1(u_1), f_1(v_1)) + \varphi(f_1(u_1), f_2(v_2)) \\ &\quad + \varphi(f_2(u_2), f_1(v_1)) + \varphi(f_2(u_2), f_2(v_2)) \\ &= \varphi(u_1, v_1) + \varphi(u_1, v_2) + \varphi(u_2, v_1) + \varphi(u_2, v_2) \\ &= \varphi(u_1 + u_2, v_2 + v_2).\end{aligned}$$

Thus f is a metric map extending f_1 and f_2. □

Theorem 29.45. *(Witt, 1936) Let E and E' be two finite-dimensional spaces respectively equipped with two nondegenerate ϵ-Hermitan forms φ and φ' satisfying condition (T), and assume that there is an isometry between (E, φ) and (E', φ'). For any subspace U of E, every injective metric linear map f from U into E' extends to an isometry from E to E'.*

Proof. Since (E, φ) and (E', φ') are isometric, we may assume that $E' = E$ and $\varphi' = \varphi$ (if $h \colon E \to E'$ is an isometry, then $h^{-1} \circ f$ is an injective metric map from U into E. The details are left to the reader).

[1] Curiously, some references to Witt's paper claim its date of publication to be 1936, but others say 1937. The answer to this mystery is that Volume 176 of *Crelle Journal* was published in four issues. The cover page of volume 176 mentions the year 1937, but Witt's paper is dated May 1936. This is not the only paper of Witt appearing in this volume!

We proceed by induction on the dimension r of U. Since the proof is quite intricate, we spell out the general plan of attack. For the induction step, we first show that we can reduce the situation to what we call *Case (H)*, namely that the subspace of U left fixed by f is a hyperplane H in U. Then, the set $D = \{f(u) - u \mid u \in U\}$ is a line in U and it turns out that $D^{\perp}$ is a hyperplane in E. We now introduce *Hypothesis (V)*, which says we can find a nontrivial subspace V of E orthogonal to D and such that $V \cap U = V \cap f(U) = (0)$. We show that if Hypothesis (V) holds, then f can be extended to an isometry of $U \oplus V$. It is then possible to further extend f to an isometry of E.

To prove that Hypothesis (V) holds we consider two cases. In Case (a), we obtain some V such that $E = U \oplus V$ and we are done. In Case (b), we obtain some V such that $D^{\perp} = U \oplus V$. We are then reduced to the situation where $U = D^{\perp}$ is a hyperplane in E and f is an isometry of U. To finish the proof we pick any $v \notin U$, so that $E = U \oplus Kv$, and we find some $v_1 \in E$ such that

$$\begin{aligned} \varphi(f(u), v_1) &= \varphi(u, v) \quad \text{for all } u \in U \\ \varphi(v_1, v_1) &= \varphi(v, v). \end{aligned}$$

Then, by Proposition 29.44, we can extend f to a metric map g of $U + Kv = E$ such that $g(v) = v_1$. The argument used to find v_1 makes use of (†) (see below) and is bit tricky. We also makes use of Property (T) in the form of Lemma 29.28.

We now go back to the proof. The case $r = 0$ is trivial. For the induction step, $r \geq 1$ so $U \neq (0)$, and let H be any hyperplane in U. Let $f\colon U \to E$ be an injective metric linear map. By the induction hypothesis, the restriction f_0 of f to H extends to an isometry g_0 of E. If g_0 extends f, we are done. Otherwise, H is the subspace of elements of U left fixed by $g_0^{-1} \circ f$. If the theorem holds in this situation, namely the subspace of U left fixed by $g_0^{-1} \circ f$ is a hyperplane H in U, then we have an isometry g_1 of E extending $g_0^{-1} \circ f$, and $g_0 \circ g_1$ is an isometry of E extending f. Therefore, we are reduced to the following situation:

Case (H). The subspace of U left fixed by f is a hyperplane H in U.

In this case, the set $D = \{f(u) - u \mid u \in U\}$ is a line in U (a one-dimensional subspace). For all $u, v \in U$, we have

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

that is

$$\varphi(f(u), f(v) - v) = \varphi(u - f(u), v) \quad \text{for all } u, v \in U, \tag{$**$}$$

and if $u \in H$, which means that $f(u) = u$, we get $u \in D^{\perp}$. Therefore, $H \subseteq D^{\perp}$. Since φ is nondegenerate, we have $\dim(D) + \dim(D^{\perp}) = \dim(E)$, and since $\dim(D) = 1$, the subspace $D^{\perp}$ is a hyperplane in E.

Hypothesis (V). We can find a nontrivial subspace V of E orthogonal to D and such that $V \cap U = V \cap f(U) = (0)$.

Claim. Hypothesis (V) implies that f can be extended to an isometry of $U \oplus V$.

Proof of Claim. If Hypothesis (V) holds, then we have

$$\varphi(f(u), v) = \varphi(u, v) \quad \text{for all } u \in U \text{ and all } v \in V,$$

since $\varphi(f(u), v) - \varphi(u, v) = \varphi(f(u) - u, v) = 0$, with $f(u) - u \in D$ and $v \in V$ orthogonal to D. By Proposition 29.44 with $f_1 = f$ and f_2 the inclusion of V into E, we can extend f to an injective metric map on $U \oplus V$ leaving all vectors in V fixed. In this case, the set $\{f(w) - w \mid w \in U \oplus V\}$ is still the line D. □

We show below that the fact that f can be extended to $U \oplus V$ implies that f can be extended to the whole of E. There are two cases. In Case (a), $E = U \oplus V$ and we are done. In case (b), $D^\perp = U \oplus V$ where $D^\perp$ is a hyperplane in E and f is an isometry of $D^\perp$. By a subtle argument, we will show that f can be extended to an isometry of E.

We are reduced to proving that a subspace V as above exists. We distinguish between two cases.

Case (a). $U \not\subseteq D^\perp$.

Proof of Case (a). In this case, formula (∗∗) show that $f(U)$ is not contained in $D^\perp$ (check this!). Consequently,

$$U \cap D^\perp = f(U) \cap D^\perp = H.$$

We can pick V to be any supplement of H in $D^\perp$, and the above formula shows that $V \cap U = V \cap f(U) = (0)$. Since $U \oplus V$ contains the hyperplane $D^\perp$ (since $D^\perp = H \oplus V$ and $H \subseteq U$), and $U \oplus V \neq D^\perp$ (since U is not contained in $D^\perp$ and $V \subseteq D^\perp$), we must have $E = U \oplus V$, and as we showed as a consequence of hypothesis (V), f can be extended to an isometry of $U \oplus V = E$. □

Case (b). $U \subseteq D^\perp$.

Proof of Case (b). In this case, formula (∗∗) shows that $f(U) \subseteq D^\perp$ so $U + f(U) \subseteq D^\perp$, and since $D = \{f(u) - u \mid u \in U\}$, we have $D \subseteq D^\perp$; that is, the line D is isotropic.

We show that there exists a subspace V of $D^\perp$, such that

$$D^\perp = U \oplus V = f(U) \oplus V.$$

Thus, case (b) shows that we are reduced to the situation where $U = D^\perp$ and f is an isometry of U.

If $U = f(U)$ we pick V to be a supplement of U in $D^\perp$. Otherwise, let $x \in U$ with $x \notin H$, and let $y \in f(U)$ with $y \notin H$. Since $f(H) = H$ (pointwise), f is injective, and H is a hyperplane in U, we have

$$U = H \oplus Kx, \quad f(U) = H \oplus Ky.$$

We claim that $x + y \notin U$. Otherwise, since $y = x + y - x$, with $x + y, x \in U$ and since $y \in f(U)$, we would have $y \in U \cap f(U) = H$, a contradiction. Similarly, $x + y \notin f(U)$. It follows that

$$U + f(U) = U \oplus K(x + y) = f(U) \oplus K(x + y).$$

Now, pick W to be any supplement of $U + f(U)$ in $D^{\perp}$ so that $D^{\perp} = (U + f(U)) \oplus W$, and let

$$V = K(x + y) + W.$$

Then, since $x \in U, y \in f(U)$, $W \subseteq D^{\perp}$, and $U + f(U) \subseteq D^{\perp}$, we have $V \subseteq D^{\perp}$. We also have

$$U \oplus V = U \oplus K(x + y) \oplus W = (U + f(U)) \oplus W = D^{\perp}$$

and

$$f(U) \oplus V = f(U) \oplus K(x + y) \oplus W = (U + f(U)) \oplus W = D^{\perp},$$

so as we showed as a consequence of hypothesis (V), f can be extended to an isometry of the hyperplane $D^{\perp} = U \oplus V$, and D is still the line $\{f(w) - w \mid w \in U \oplus V\}$. □

The argument in the proof of Case (b) shows that we are reduced to the situation where $U = D^{\perp}$ is a hyperplane in E and f is an isometry of U. If we pick any $v \notin U$, then $E = U \oplus Kv$, so suppose we can find some $v_1 \in E$ such that

$$\begin{aligned} \varphi(f(u), v_1) &= \varphi(u, v) \quad \text{for all } u \in U \\ \varphi(v_1, v_1) &= \varphi(v, v). \end{aligned}$$

The first condition is condition $(*)$ of Proposition 29.44, and the second condition asserts that the map $\lambda v \mapsto \lambda v_2$ from the line Kv to the line Kv_1 is a metric map. Then, by Proposition 29.44, we can extend f to a metric map g of $U + Kv = E$ such that $g(v) = v_1$.

To find v_1, let us prove that for every $v \in E$, there is some $v' \in E$ such that

$$\varphi(f(u), v') = \varphi(u, v) \quad \text{for all } u \in U. \tag{$\dagger$}$$

This is because the linear form $u \mapsto \varphi(f^{-1}(u), v)$ $(u \in U)$ is the restriction of a linear form $\psi \in E^*$, and since φ is nondegenerate, there is some (unique) $v' \in E$, such that

$$\psi(x) = \varphi(x, v') \quad \text{for all } x \in E,$$

which implies that

$$\varphi(u, v') = \varphi(f^{-1}(u), v) \quad \text{for all } u \in U,$$

and since f is an automorphism of U, that (†) holds. Furthermore, observe that formula (†) still holds if we add to v' any vector y in D, since $f(U) = U = D^{\perp}$. Therefore, for any $v_1 = v' + y$ with $y \in D$, if we extend f to a linear map of E by setting $g(v) = v_1$, then by (†) we have

$$\varphi(g(u), g(v)) = \varphi(u, v) \quad \text{for all } u \in U.$$

We still need to pick $y \in D$ so that $v_1 = v' + y$ satisfies $\varphi(v_1, v_1) = \varphi(v, v)$. However, since $v \notin U = D^{\perp}$, the vector v is not orthogonal D, and by Lemma 29.28, there is some $y_0 \in D$ such that

$$\varphi(v' + y_0, v' + y_0) = \varphi(v, v).$$

Then, if we let $v_1 = v' + y_0$, by Proposition 29.44, we can extend f to a metric map g of $U + Kv = E$ by setting $g(v) = v_1$. Since φ is nondegenerate, g is an isometry. □

The first corollary of Witt's theorem is sometimes called the Witt's cancellation theorem.

Theorem 29.46. *(Witt Cancellation Theorem) Let (E_1, φ_1) and (E_2, φ_2) be two pairs of finite-dimensional spaces and nondegenerate ϵ-Hermitian forms satisfying condition (T), and assume that (E_1, φ_1) and (E_2, φ_2) are isometric. For any subspace U of E_1 and any subspace V of E_2, if there is an isometry $f \colon U \to V$, then there is an isometry $g \colon U^{\perp} \to V^{\perp}$.*

Proof. If $f \colon U \to V$ is an isometry between U and V, by Witt's theorem (Theorem 29.46), the linear map f extends to an isometry g between E_1 and E_2. We claim that g maps $U^{\perp}$ into $V^{\perp}$. This is because if $v \in U^{\perp}$, we have $\varphi_1(u, v) = 0$ for all $u \in U$, so

$$\varphi_2(g(u), g(v)) = \varphi_1(u, v) = 0 \quad \text{for all } u \in U,$$

and since g is a bijection between U and V, we have $g(U) = V$, so we see that $g(v)$ is orthogonal to V for every $v \in U^{\perp}$; that is, $g(U^{\perp}) \subseteq V^{\perp}$. Since g is a metric map and since φ_1 is nondegenerate, the restriction of g to $U^{\perp}$ is an isometry from $U^{\perp}$ to $V^{\perp}$. □

A pair (E, φ) where E is finite-dimensional and φ is a nondegenerate ϵ-Hermitian form is often called an *ϵ-Hermitian space*. When $\epsilon = 1$ and φ is symmetric, we use the term *Euclidean* space or *quadratic* space. When $\epsilon = -1$ and φ is alternating, we use the term *symplectic* space. When $\epsilon = 1$ and the automorphism $\lambda \mapsto \overline{\lambda}$ is not the identity we use the term *Hermitian* space, and when $\epsilon = -1$, we use the term *skew-Hermitian* space.

We also have the following result showing that the group of isometries of an ϵ-Hermitian space is transitive on totally isotropic subspaces of the same dimension.

Theorem 29.47. *Let E be a finite-dimensional vector space and let φ be a nondegenerate ϵ-Hermitian form on E satisfying condition (T). Then for any two totally isotropic subspaces U and V of the same dimension, there is an isometry $f \in \mathbf{Isom}(\varphi)$ such that $f(U) = V$. Furthermore, every linear automorphism of U is induced by an isometry of E.*

Remark: Witt's cancelation theorem can be used to define an equivalence relation on ϵ-Hermitian spaces and to define a group structure on these equivalence classes. This way, we obtain the *Witt group*, but we will not discuss it here.

Witt's Theorem can be sharpened to isometries in $\mathbf{SO}(\varphi)$, but some condition on U is needed.

Theorem 29.48. *(Witt–Sharpened Version) Let E be a finite-dimensional space equipped with a nondegenerate symmetric bilinear forms φ. For any subspace U of E, every linear injective metric map f from U into E extends to an isometry g of E with a prescribed value ± 1 of $\det(g)$ iff*

$$\dim(U) + \dim(\mathrm{rad}(U)) < \dim(E) = n.$$

If

$$\dim(U) + \dim(\mathrm{rad}(U)) = \dim(E) = n,$$

and $\det(f) = -1$, then there is no $g \in \mathbf{SO}(\varphi)$ extending f.

Proof. If g_1 and g_2 are two extensions of f such that $\det(g_1)\det(g_2) = -1$, then $h = g_1^{-1} \circ g_2$ is an isometry such that $\det(h) = -1$, and h leaves every vector of U fixed. Conversely, if h is an isometry such that $\det(h) = -1$, and $h(u) = u$ for all $u \in U$, then for any extesnion g_1 of f, the map $g_2 = h \circ g_1$ is another extension of f such that $\det(g_2) = -\det(g_1)$. Therefore, we need to show that a map h as above exists.

If $\dim(U) + \dim(\mathrm{rad}(U)) < \dim(E)$, consider the nondegenerate completion $\overline{U}$ of U given by Proposition 29.32. We know that $\dim(\overline{U}) = \dim(U) + \dim(\mathrm{rad}(U)) < n$, and since $\overline{U}$ is nondegenerate, we have

$$E = \overline{U} \overset{\perp}{\oplus} \overline{U}^{\perp},$$

with $\overline{U}^{\perp} \neq (0)$. Pick any isometry τ of $\overline{U}^{\perp}$ such that $\det(\tau) = -1$, and extend it to an isometry h of E whose restriction to $\overline{U}$ is the identity.

If $\dim(U) + \dim(\mathrm{rad}(U)) = \dim(E) = n$, then $U = V \overset{\perp}{\oplus} W$ with $V = \mathrm{rad}(U)$ and since $\dim(\overline{U}) = \dim(U) + \dim(\mathrm{rad}(U)) = n$, we have

$$E = \overline{U} = (V \oplus V') \overset{\perp}{\oplus} W,$$

where $V \oplus V' = \mathrm{Ar}_{2r} = W^{\perp}$ is an Artinian space. Any isometry h of E which is the identity on U and with $\det(h) = -1$ is the identity on W, and thus it must map $W^{\perp} = \mathrm{Ar}_{2r} = V \oplus V'$ into itself, and the restriction h' of h to Ar_{2r} has $\det(h') = -1$. However, h' is the identity on $V = \mathrm{rad}(U)$, a totally isotropic subspace of Ar_{2r} of dimension r, and by Proposition 29.42, we have $\det(h') = +1$, a contradiction. □

It can be shown that the center of $\mathbf{O}(\varphi)$ is $\{\mathrm{id}, -\mathrm{id}\}$. For further properties of orthogonal groups, see Grove [83], Jacobson [97], Taylor [172], and Artin [6].