April 11, 2016

We assume the reader is familiar with linear algebra, for example, finite-dimensional real vector spaces, the standard inner product, subspaces, direct sums, the matrix representation of a linear transformation.

Let $\alpha \in \mathbf{R}^2$ be a nonzero vector. The set of vectors orthogonal to α form a line L, and $\mathbf{R}^2 = \mathbf{R}\alpha \oplus L$ holds. Given $\lambda \in \mathbf{R}^2$ can be expressed as

$$\lambda = c\alpha + \mu \quad \text{for some } c \in \mathbf{R} \text{ and } \mu \in L. \tag{1}$$

Since $(\mu, \alpha) = 0$, we have

$$\begin{aligned} c &= \frac{(c\alpha + \mu, \alpha)}{(\alpha, \alpha)} \\ &= \frac{(\lambda, \alpha)}{(\alpha, \alpha)} && \text{(by (1))}. \end{aligned}$$

The *reflection* of λ with respect to the line L is obtained by negating the $\langle \alpha \rangle$-component of λ in (1), that is,

$$\begin{aligned} -c\alpha + \mu &= \lambda - 2c\alpha \\ &= \lambda - \frac{2(\lambda, \alpha)}{(\alpha, \alpha)}\alpha. \end{aligned}$$

Let $s_\alpha : \mathbf{R}^2 \to \mathbf{R}^2$ denote the mapping defined by the above formula, that is,

$$s_\alpha(\lambda) = \lambda - \frac{2(\lambda, \alpha)}{(\alpha, \alpha)}\alpha \quad (\lambda \in \mathbf{R}^2). \tag{2}$$

It is clear that s_α is a linear transformation of $\mathbf{R}^2$. This means that there exists a 2×2 matrix S_α such that

$$s_\alpha(\lambda) = S_\alpha \lambda \quad (\lambda \in \mathbf{R}^2). \tag{3}$$

To find S_α, recall that L is the line orthogonal to α. Let

$$\mu = \begin{bmatrix} \cos\theta \\ \sin\theta \end{bmatrix}$$

be a vector of length 1 in L. The vector

$$\nu = \begin{bmatrix} -\sin\theta \\ \cos\theta \end{bmatrix}$$

is orthogonal to μ, hence in $\mathbf{R}\alpha$. This implies that

$$\begin{aligned} s_\alpha(\mu) &= \mu, \\ s_\alpha(\nu) &= -\nu. \end{aligned}$$

Thus

$$S_\alpha \begin{bmatrix} \mu & \nu \end{bmatrix} = \begin{bmatrix} \mu & -\nu \end{bmatrix},$$

which implies

$$\begin{aligned} S_\alpha &= \begin{bmatrix} \mu & -\nu \end{bmatrix} \begin{bmatrix} \mu & \nu \end{bmatrix}^{-1} \\ &= \begin{bmatrix} \cos\theta & \sin\theta \\ \sin\theta & -\cos\theta \end{bmatrix} \begin{bmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{bmatrix}^{-1} \\ &= \begin{bmatrix} \cos\theta & \sin\theta \\ \sin\theta & -\cos\theta \end{bmatrix} \begin{bmatrix} \cos\theta & \sin\theta \\ -\sin\theta & \cos\theta \end{bmatrix} \\ &= \begin{bmatrix} \cos^2\theta - \sin^2\theta & 2\sin\theta\cos\theta \\ 2\sin\theta\cos\theta & -(\cos^2\theta - \sin^2) \end{bmatrix} \\ &= \begin{bmatrix} \cos 2\theta & \sin 2\theta \\ \sin 2\theta & -\cos 2\theta \end{bmatrix}. \end{aligned}$$

This is the matrix representation of a reflection on the plane $\mathbf{R}^2$.

We next consider the composition of two reflections. Let s_α and S_α be as before, and let s_β be another reflection, with matrix representation

$$S_\beta = \begin{bmatrix} \cos 2\varphi & \sin 2\varphi \\ \sin 2\varphi & -\cos 2\varphi \end{bmatrix}.$$

Then

$$\begin{aligned} S_\alpha S_\beta &= \begin{bmatrix} \cos 2\theta & \sin 2\theta \\ \sin 2\theta & -\cos 2\theta \end{bmatrix} \begin{bmatrix} \cos 2\varphi & \sin 2\varphi \\ \sin 2\varphi & -\cos 2\varphi \end{bmatrix} \\ &= \begin{bmatrix} \cos 2(\theta-\varphi) & -\sin 2(\theta-\varphi) \\ \sin 2(\theta-\varphi) & \cos 2(\theta-\varphi) \end{bmatrix} \\ &= \begin{bmatrix} \cos 2(\theta-\varphi) & \cos(2(\theta-\varphi)+\frac{\pi}{2}) \\ \sin 2(\theta-\varphi) & \sin(2(\theta-\varphi)+\frac{\pi}{2}) \end{bmatrix}. \end{aligned}$$

This matrix maps the standard basis vector

$$\begin{bmatrix} 1 \\ 0 \end{bmatrix} = \begin{bmatrix} \cos 0 \\ \sin 0 \end{bmatrix}, \begin{bmatrix} 0 \\ 1 \end{bmatrix} = \begin{bmatrix} \cos\frac{\pi}{2} \\ \sin\frac{\pi}{2} \end{bmatrix}$$

to

$$\begin{bmatrix} \cos 2(\theta-\varphi) \\ \sin 2(\theta-\varphi) \end{bmatrix}, \begin{bmatrix} \cos(2(\theta-\varphi)+\frac{\pi}{2}) \\ \sin(2(\theta-\varphi)+\frac{\pi}{2}) \end{bmatrix},$$

meaning that both vectors are rotated $2(\theta-\varphi)$. Therefore, the product of two reflection is a rotation.

We are interested in the case where the resulting rotation is of finite order, that is, $2(\theta-\varphi)$ is a rational multiple of 2π. For brevity, write $s = s_\alpha$, $t = s_\beta$ and $\mathrm{id} = 1$. In this case, there exists a positive integer m such that $(st)^m = 1$. We may assume $s \neq t$, so that $st \neq 1$. We may choose minimal such m, so that

$$st, (st)^2, \dots, (st)^{m-1} \neq 1.$$

Writing $r = st$, this implies

$$1, r, r^2, \dots, r^{m-1} \text{ are pairwise distinct.} \tag{4}$$

We aim to determine the set $\langle s, t\rangle$ of all linear transformations expressible as a product of s, t. We have already seen that this set contains at least m distinct elements (4). Since $s^2 = t^2 = 1$, possible product of s, t are one of the following four forms:

$$stst\cdots st, \tag{5}$$
$$stst\cdots sts, \tag{6}$$
$$tsts\cdots ts, \tag{7}$$
$$tsts\cdots tst. \tag{8}$$

Products of the form (5) are precisely described in (4). Products of the form (6) are

$$s, rs, r^2 s, \dots, r^{m-1}s, \tag{9}$$

and these are distinct by (4). Since $ts = t^{-1}s^{-1} = (st)^{-1} = r^{-1}$, products of the form (7) are nothing but those in (4). Finally, since $rt = s$, products of the form (8) are then those in (9). Therefore, $\langle s, t\rangle$ consists of $2m$ elements described in (4) and (9). To show that these $2m$ elements are distinct, it suffices to show that there is no common element in (4) and (9), which follows immediately from the fact that $\det r = 1$ and $\det s = -1$.

It is important to note that this last part of reasoning, except the distinctness, follows only from the transformation rule

$$s^2 = t^2 = 1, \quad (st)^m = 1. \tag{10}$$

Setting $r = st$, we have $r^m = 1$ and $srs = r^{-1}$. Written in terms of r and s, we can also say that the determination of all elements in $\langle s, t\rangle$ follows only from the transformation rule

$$s^2 = r^m = 1, \quad sr = r^{-1}s. \tag{11}$$

Indeed, one can always rewrite sr to $r^{m-1}s$, so every element in $\langle s, r\rangle$ is of the form $r^k s^j$ with $0 \le k < m$ and $j \in \{0, 1\}$.

In the next lecture, we will discuss a rigorous way of dealing with words in formal symbol subject to relations such as (10) and (11). In addition to this formal aspect, we will discuss explicit realizations of these symbols as linear transformation.

Definition 1. A linear transformation $s : \mathbf{R}^n \to \mathbf{R}^n$ is called a reflection if there exists a nonzero vector α such that $s(\alpha) = -\alpha$ and $s(h) = h$ for all $h \in (\mathbf{R}\alpha)^\perp$.

Note that, since $\mathbf{R}^n = \mathbf{R}\alpha \oplus (\mathbf{R}\alpha)^\perp$, the linear transformation is determined uniquely by the conditions $s(\alpha) = -\alpha$ and $s(h) = h$ for all $h \in (\mathbf{R}\alpha)^\perp$, so we denote this reflection by s_α. Moreover, any nonzero scalar multiple of α defines the same reflection, that is, $s_\alpha = s_{c\alpha}$ for any $c \in \mathbf{R}$ with $c \neq 0$.

Lemma 2. *Let $s : \mathbf{R}^n \to \mathbf{R}^n$ be a reflection. Then the matrix representation S of s is diagonalizable by an orthogonal matrix:*

$$P^{-1}SP = \begin{bmatrix} -1 & & & \\ & 1 & & \\ & & \ddots & \\ & & & 1 \end{bmatrix}$$

for some orthogonal matrix P. Conversely, if the matrix representation of s is of this form for some orthogonal matrix P, then s is a reflection.

Proof. Let $s = s_\alpha$. We may assume without loss of generality $(\alpha, \alpha) = 1$. Let $\beta_2, \ldots, \beta_n$ be an orthonormal basis of $(\mathbf{R}\alpha)^\perp$. Then $\alpha, \beta_2, \ldots, \beta_n$ is an orthonormal basis of $\mathbf{R}^n$. Let

$$P = \begin{bmatrix} \alpha & \beta_2 & \cdots & \beta_n \end{bmatrix}.$$

Then P is an orthogonal matrix, and

$$SP = P \begin{bmatrix} -1 & & & \\ & 1 & & \\ & & \ddots & \\ & & & 1 \end{bmatrix}.$$

To prove the converse, let α be the first column of P. Then clearly $s(\alpha) = -\alpha$ and $s(h) = h$ for any $h \in (\mathbf{R}\alpha)^\perp$. Thus $s = s_\alpha$. $\square$

April 18, 2016

Lemma 2 shows that S itself is also an orthogonal matrix. It is well known that this is equivalent to s being an orthogonal transformation, that is,

$$(s(\lambda), s(\mu)) = (\lambda, \mu) \quad (\lambda, \mu \in \mathbf{R}^n). \tag{12}$$

This can be directly verified as follows. First, let $s = s_\alpha$ with $\alpha \neq 0$ and set

$$\pi(\lambda) = \lambda - \frac{(\lambda, \alpha)}{(\alpha, \alpha)}\alpha.$$

Then $(\pi(\lambda), \alpha) = 0$, so

$$\lambda = \frac{(\lambda, \alpha)}{(\alpha, \alpha)}\alpha + \pi(\lambda)$$

is the representation of λ as an element of $\mathbf{R}\alpha \oplus (\mathbf{R}\alpha)^\perp$. By the definition of a reflection, we obtain

$$\begin{aligned} s_\alpha(\lambda) &= -\frac{(\lambda, \alpha)}{(\alpha, \alpha)}\alpha + \pi(\lambda) \\ &= \lambda - \frac{2(\lambda, \alpha)}{(\alpha, \alpha)}\alpha. \end{aligned}$$

Note that this is a direct generalization of our formula (2) originally established in $\mathbf{R}^2$ only. Now

$$\begin{aligned} (s_\alpha(\lambda), s_\alpha(\mu)) &= (\lambda - \frac{2(\lambda, \alpha)}{(\alpha, \alpha)}\alpha, \mu - \frac{2(\mu, \alpha)}{(\alpha, \alpha)}\alpha) \\ &= (\lambda, \mu) - (\lambda, \frac{2(\mu, \alpha)}{(\alpha, \alpha)}\alpha) - (\mu, \frac{2(\lambda, \alpha)}{(\alpha, \alpha)}\alpha) + (\frac{2(\lambda, \alpha)}{(\alpha, \alpha)}\alpha, \frac{2(\mu, \alpha)}{(\alpha, \alpha)}\alpha) \\ &= (\lambda, \mu) - \frac{2(\mu, \alpha)}{(\alpha, \alpha)}(\lambda, \alpha) - \frac{2(\lambda, \alpha)}{(\alpha, \alpha)}(\mu, \alpha) + \frac{2(\lambda, \alpha)}{(\alpha, \alpha)}\frac{2(\mu, \alpha)}{(\alpha, \alpha)}(\alpha, \alpha) \\ &= (\lambda, \mu) - \frac{2(\lambda, \alpha)(\mu, \alpha)}{(\alpha, \alpha)} - \frac{2(\lambda, \alpha)(\mu, \alpha)}{(\alpha, \alpha)} + \frac{4(\lambda, \alpha)(\mu, \alpha)}{(\alpha, \alpha)} \\ &= (\lambda, \mu). \end{aligned}$$

Therefore, s_α is an orthogonal transformation.

For a real vector space V with an inner product, the set of orthogonal transformation is denoted by $O(V)$. Thus, every reflection in V is an element of $O(V)$. It is necessary to consider a more general vector space V than just $\mathbf{R}^n$, since we sometimes need to consider linear transformation defined on a subspace of $\mathbf{R}^n$.

Let us recall how the transformation rule (10) was used to derive every word in $\langle s, t\rangle$ is one of the $2m$ possible forms. We now formalize this by ignoring the fact that s, t are reflections. Instead we only assume $s^2 = t^2 = 1$. In order to facilitate this, we consider a set of formal symbols X and consider the set of all words of length n. This is the set of sequence of length n, so it can be regarded as the cartesian product

$$X^n = \underbrace{X \times X \times \cdots \times X}_{n}.$$

Then we can form a disjoint union

$$X^* = \bigcup_{n=0}^{\infty} X^n,$$

where X^0 consists of a single element called the empty word, denoted by 1.

A word $x = (x_1, x_2, \ldots, x_n) \in X^n$ is said to be *reduced* if $x_i \neq x_{i+1}$ for $1 \leq i < n$. By definition, the word 1 of length 0 is reduced, and every word of length 1 is reduced. For brevity, we write $x = x_1 x_2 \cdots x_n \in X^n$ instead of $x = (x_1, x_2, \ldots, x_n) \in X^n$. We denote the set of all reduced words by $F(X)$.

We can define a binary operation $\mu : F(X) \times F(X) \to F(X)$ as follows.

$$\mu(1, x) = \mu(x, 1) = x \quad (x \in F(X)), \tag{13}$$

and for $x = x_1 \cdots x_m \in X^m \cap F(X)$ and $y = y_1 \cdots y_n \in X^n \cap F(X)$ with $m, n \geq 1$, we define

$$\mu(x, y) = \begin{cases} x_1 \cdots x_m y_1 \cdots y_n \in X^{m+n} & \text{if } x_m \neq y_1, \\ \mu(x_1 \cdots x_{m-1}, y_2 \cdots y_n) & \text{otherwise.} \end{cases} \tag{14}$$

This is a recursive definition. Note that if $x_m \neq y_1$, then $x_1 \cdots x_m y_1 \cdots y_n$ is a reduced word. Note also that there is no guarantee that $x_1 \cdots x_{m-1} y_2 \cdots y_n$ is a reduced word. If it is not, then $x_{m-1} = y_2$, so we define this to be $\mu(x_1 \cdots x_{m-2}, y_3 \cdots y_n)$. Since the length is finite, we eventually reach the case where the last symbol of x is different from the first symbol of y, or one of x, y is 1.

Definition 3. A set G with binary operation $\mu : G \times G \to G$ is said to be a *group* if

(i) μ is associative, that is, $\mu(\mu(a, b), c) = \mu(a, \mu(b, c))$ for all $a, b, c \in G$,

(ii) there exists an element $1 \in G$ such that $\mu(1, a) = \mu(a, 1) = a$ for all $a \in G$,

(iii) for each $a \in G$, there exists an element $a' \in G$ such that $\mu(a, a') = \mu(a', a) = 1$.

The element 1 is called the *identity* of G, and a' is called the *inverse* of a.

Theorem 4. *The set of reduced words $F(X)$ forms a group under the binary operation μ defined by* (13)–(14).

Proof. Clearly, the empty word 1 is the identity in $F(X)$, i.e.,

$$\mu(1, a) = \mu(a, 1) = a \quad (a \in F(X)). \tag{15}$$

Next we prove associativity (i), by a series of steps.

Step 1.

$$\mu(\mu(a,x),\mu(x,b)) = \mu(a,b) \quad (a,b \in F(X),\ x \in X). \tag{16}$$

Indeed, denote by a_{-1} the last entry of a, and by b_1 the first entry of b. Write

$$\begin{aligned} a &= a'x && \text{if } a_{-1} = x, \\ b &= xb' && \text{if } b_1 = x. \end{aligned}$$

Since

$$\begin{aligned} ax &\in F(X) && \text{if } a_{-1} \neq x, \\ xb &\in F(X) && \text{if } b_1 \neq x, \end{aligned}$$

we have

$$\begin{aligned} \mu(\mu(a,x),\mu(x,b)) &= \begin{cases} \mu(a',b') & \text{if } a_{-1} = x, b_1 = x, \\ \mu(a',xb) & \text{if } a_{-1} = x, b_1 \neq x, \\ \mu(ax,b') & \text{if } a_{-1} \neq x, b_1 = x, \\ \mu(ax,xb) & \text{if } a_{-1} \neq x, b_1 \neq x \end{cases} \\ &= \mu(a,b). \end{aligned}$$

Step 2.

$$\mu(x,\mu(x,c)) = c \quad (c \in F(X),\ x \in X). \tag{17}$$

Indeed,

$$\begin{aligned} \mu(x,\mu(x,c)) &= \mu(\mu(1,x),\mu(x,c)) && \text{(by (13))} \\ &= \mu(1,c) && \text{(by (16))} \\ &= c && \text{(by (13)).} \end{aligned}$$

Step 3.

$$\mu(x,\mu(b,c)) = \mu(\mu(x,b),c) \quad (b,c \in F(X),\ x \in X). \tag{18}$$

Assume $b \in X^m$. We prove (18) by induction on m. If $m = 0$, then $b = 1$, so

$$\begin{aligned} \mu(x,\mu(b,c)) &= \mu(x,\mu(1,c)) \\ &= \mu(x,c) && \text{(by (15))} \\ &= \mu(\mu(x,1),c) && \text{(by (15))} \\ &= \mu(\mu(x,b),c). \end{aligned}$$

Next assume $m > 0$. If $b = xb'$, then

$$\begin{aligned} \mu(x,\mu(b,c)) &= \mu(x,\mu(\mu(x,b'),c)) \\ &= \mu(x,\mu(x,\mu(b',c))) && \text{(by induction)} \end{aligned}$$

$$
\begin{aligned}
&= \mu(b', c) && \text{(by (17))} \\
&= \mu(\mu(x, b), c).
\end{aligned}
$$

If $b = b'y$ and $c = yc'$ for some $b', c' \in F(X)$ and $y \in X$, then

$$
\begin{aligned}
\mu(x, \mu(b, c)) &= \mu(x, \mu(b', c')) && \text{(by (14))} \\
&= \mu(\mu(x, b'), c') && \text{(by induction)} \\
&= \mu(\mu(\mu(x, b'), y), \mu(y, c')) && \text{(by (16))} \\
&= \mu(\mu(\mu(x, b'), y), c) \\
&= \mu(\mu(x, \mu(b', y)), c) && \text{(by induction)} \\
&= \mu(\mu(x, b), c).
\end{aligned}
$$

Finally, if $b_1 \neq x$ and $b_{-1} \neq c_1$, then $\mu(x, b) = xb$ and $\mu(b, c) = bc$, and $xbc \in F(X)$. Thus

$$
\begin{aligned}
\mu(x, \mu(b, c)) &= \mu(x, bc) \\
&= xbc \\
&= \mu(xb, c) \\
&= \mu(\mu(x, b), c).
\end{aligned}
$$

This completes the proof of (18).

Now we prove

$$
\mu(a, \mu(b, c)) = \mu(\mu(a, b), c) \quad (a, b, c \in F(X)). \tag{19}
$$

by induction on n, where $a \in X^n$. The cases $n = 0$ is trivial because of (15). Assume $a = a'x$, where $a' \in F(X)$ and $x \in X$. Then

$$
\begin{aligned}
\mu(a, \mu(b, c)) &= \mu(\mu(a', x), \mu(b, c)) \\
&= \mu(a', \mu(x, \mu(b, c))) && \text{(by induction)} \\
&= \mu(a', \mu(\mu(x, b), c)) && \text{(by (18))} \\
&= \mu(\mu(a', \mu(x, b)), c) && \text{(by induction)} \\
&= \mu(\mu(\mu(a', x), b), c) && \text{(by induction)} \\
&= \mu(\mu(a, b), c).
\end{aligned}
$$

Therefore, we have proved associativity.

If $a = x_1 \cdots x_n \in F(X) \cap X^n$, then the reversed word $a' = x_n \cdots x_1 \in F(X) \cap X^n$ is the inverse of a. □

We call $F(X)$ the *free group generated by the set of involutions* X. From now on, we omit μ to denote the binary operation in $F(X)$ by juxtaposition. So we write ab instead of $\mu(a, b)$ for $a, b \in F(X)$. Also, for $a = x_1 \cdots x_n \in F(X) \cap X^n$, its inverse $x_n \cdots x_1$ will be denoted by a^{-1}.

Let s and t be the linear transformation of $\mathbf{R}^2$ represented by the matrices

$$\begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix} \text{ and } \begin{bmatrix} \cos\frac{2\pi}{m} & \sin\frac{2\pi}{m} \\ \sin\frac{2\pi}{m} & -\cos\frac{2\pi}{m} \end{bmatrix},$$

respectively. Let $G = \langle s, t \rangle$ be the set of all linear transformation expressible as a product of s and t. We know

$$G = \{(st)^j \mid 0 \le j < m\} \cup \{(st)^j s \mid 0 \le j < m\}.$$

and $|G| = 2m$. The product of linear transformations defines a binary operation on G, and G forms a group under this operation. This group is called the *dihedral group* of order $2m$. In order to connect the dihedral group with a free group, we make a definition.

Definition 5. Let G_1 and G_2 be groups. A mapping $f : G_1 \to G_2$ is called a *homomorphism* if

$$f(ab) = f(a)f(b) \quad (\forall a, b \in G_1), \tag{20}$$

where the product ab is computed under the binary operation in G_1, the product $f(a)f(b)$ is computed under the binary operation in G_2. A bijective homomorphism is called an *isomorphism*. The groups G_1 and G_2 are said to be *isomorphic* if there exists an isomorphism from G_1 to G_2.

Let $X = \{x, y\}$ be a set of two distinct formal symbols. Clearly, there is a homomorphism $f : F(X) \to G$ with $f(x) = s$ and $f(y) = t$, where $G = \langle s, t \rangle$ is the dihedral group of order $2m$ defined above. Note that $f((xy)^m) = (st)^m = 1$, but $(xy)^m \in F(X)$ is not the identity. This suggests introducing another transformation rule $(xy)^m = 1$, in addition to $x^2 = y^2 = 1$ as we adopted when constructing the group $F(X)$. We do this by introducing an equivalence relation on $F(X)$. Let $a, b \in F(X)$. If there exists $c \in F(X)$ such that $a = bc^{-1}(xy)^m c$, then $f(a) = f(b)$ holds. So we write $a \sim b$ if there is a finite sequence $a = a_0, a_1, \ldots, a_n = b \in F(X)$ such that for each $i \in \{1, 2, \ldots, n\}$, a_i is obtained by multiplying a_{i-1} by an element of the form $c^{-1}(xy)^m c$ for some $c \in F(X)$. Then $\sim$ is an equivalence relation, since $a = bc^{-1}(xy)^m c$ implies $b = a(xc)^{-1}(xy)^m(xc)$. Clearly, $a \sim b$ implies $f(a) = f(b)$. In other words, f induces a mapping from the set of equivalence classes to G. In fact, the set of equivalence classes forms a group under the binary operation inherited from $F(X)$. We can now make this more precise.

May 2, 2016

Definition 6. Let X be a set of formal symbols, and let $F(X)$ be the free group generated by the set of involutions X. Let $R \subset F(X)$. Let N be the subgroup generated by the set

$$\{c^{-1}r^{\pm 1}c \mid c \in F(X),\ r \in R\}. \tag{21}$$

In other words, N is the set of elements of $F(X)$ expressible as a product of elements in the set (21). The set

$$F(X)/N = \{aN \mid a \in F(X)\},$$

where $aN = \{ab \mid b \in N\}$ for $a \in F(X)$, forms a group under the binary operation

$$\begin{array}{rcl} F(X)/N \times F(X)/N & \to & F(X)/N \\ (aN, bN) & \mapsto & abN \end{array}$$

and it is called the group with presentation $\langle X \mid R \rangle$.

In view of Definition 6, we show that the dihedral group G of order $2m$ is isomorphic to the the group with presentation $\langle x, y \mid (xy)^m \rangle$. Indeed, we have seen that there is a homomorphism $f : F(X) \to G$ with $f(x) = s$ and $f(y) = t$. In our case, $R = \{(xy)^m\}$ which is mapped to 1 under f. So f is constant on each equivalence class, and hence f induces a mapping $\overline{f} : F(X)/N \to G$ defined by $\overline{f}(aN) = f(a)$ ($a \in F(X)$). This mapping $\overline{f}$ is a homomorphism since

$$\begin{aligned} \overline{f}((aN)(bN)) &= \overline{f}(abN) \\ &= f(ab) \\ &= f(a)f(b) \\ &= \overline{f}(aN)\overline{f}(bN). \end{aligned}$$

Moreover, it is clear that both f and $\overline{f}$ are surjective, since $G = \langle s, t \rangle = \langle f(x), f(y) \rangle$. The most important part of the proof is injectivity of $\overline{f}$. The argument on the transformation rule defined by $(xy)^m$ shows

$$F(X)/N = \{(xy)^j N \mid 0 \le j < m\} \cup \{(xy)^j xN \mid 0 \le j < m\}.$$

In particular, $|F(X)/N| \le 2m = |G|$. Since $\overline{f}$ is surjective, equality and injectivity of $\overline{f}$ are forced.

Definition 7. Let V be a finite-dimensional vector space over $\mathbf{R}$ with positive definite inner product. The set $O(V)$ of orthogonal linear transformations of V forms a group under composition. We call $O(V)$ the *orthogonal group* of V.

Definition 8. Let V be a finite-dimensional vector space over $\mathbf{R}$ with positive definite inner product. A subgroup W of the group $O(V)$ is said to be a *finite reflection group* if

(i) $W \ne \{\mathrm{id}_V\}$,

(ii) W is finite,

(iii) W is generated by a set of reflections.

For example, the dihedral group G of order $2m$ is a finite reflection group, since $G \subset O(\mathbf{R}^2)$, $|G| = 2m$ is neither 1 nor infinite, and G is generated by two reflections. We have seen that G has presentation $\langle s, t \mid (st)^m \rangle$. One of the goal of these lectures is to show that every finite reflection group has presentation $\langle s_1, \dots, s_n \mid R \rangle$, where $R \subset F(\{s_1, \dots, s_n\})$ is of the form $\{(s_i s_j)^{m_{ij}} \mid 1 \le i, j \le n\}$.

Let $n \ge 2$ be an integer, and let $\mathcal{S}_n$ denote the symmetric group of degree n. In other words, $\mathcal{S}_n$ consists of all permutations of the set $\{1, 2, \dots, n\}$. Since permutations are bijections from $\{1, 2, \dots, n\}$ to itself, $\mathcal{S}_n$ forms a group under composition. Let $\varepsilon_1, \dots, \varepsilon_n$ denote the standard basis of $\mathbf{R}^n$. For each $\sigma \in \mathcal{S}_n$, we define $g_\sigma \in O(\mathbf{R}^n)$ by setting

$$g_\sigma(\sum_{i=1}^{n} c_i \varepsilon_i) = \sum_{i=1}^{n} c_i \varepsilon_{\sigma(i)},$$

and set

$$G_n = \{g_\sigma \mid \sigma \in \mathcal{S}_n\}.$$

It is easy to verify that G_n is a subgroup of $O(V)$ and, the mapping $\mathcal{S}_n \to G_n$ defined by $\sigma \mapsto g_\sigma$ is an isomorphism. We claim that g_σ is a reflection if σ is a transposition; more precisely,

$$g_\sigma = s_{\varepsilon_i - \varepsilon_j} \quad \text{if } \sigma = (i\ j). \tag{22}$$

Indeed, for $k \in \{1, 2, \dots, n\}$,

$$\begin{aligned}
s_{\varepsilon_i - \varepsilon_j}(\varepsilon_k) &= \varepsilon_k - \frac{2(\varepsilon_k, \varepsilon_i - \varepsilon_j)}{(\varepsilon_i - \varepsilon_j, \varepsilon_i - \varepsilon_j)}(\varepsilon_i - \varepsilon_j) \\
&= \varepsilon_k - (\varepsilon_k, \varepsilon_i - \varepsilon_j)(\varepsilon_i - \varepsilon_j) \\
&= \begin{cases} \varepsilon_i - (\varepsilon_i - \varepsilon_j) & \text{if } k = i, \\ \varepsilon_j + (\varepsilon_i - \varepsilon_j) & \text{if } k = j, \\ \varepsilon_k & \text{otherwise} \end{cases} \\
&= \begin{cases} \varepsilon_j & \text{if } k = i, \\ \varepsilon_i & \text{if } k = j, \\ \varepsilon_k & \text{otherwise} \end{cases} \\
&= \varepsilon_{\sigma(k)} \\
&= g_\sigma(\varepsilon_k).
\end{aligned}$$

It is well known that $\mathcal{S}_n$ is generated by its set of transposition. Via the isomorphism $\sigma \mapsto g_\sigma$, we see that G_n is generated by the set of reflections

$$\{s_{\varepsilon_i - \varepsilon_j} \mid 1 \le i < j \le n\}.$$

Therefore, G_n is a finite reflection group.

Observe that G_3 has order 6, and we know another finite reflection group of order 6, namely, the dihedral group of order 6. Although $G_3 \subset O(\mathbf{R}^3)$ while the dihedral group is a subgroup of $O(\mathbf{R}^2)$, these two groups are isomorphic. In order to see their connection, we make a definition.

Definition 9. Let V be a finite-dimensional vector space over $\mathbf{R}$ with positive definite inner product. Let $W \subset O(V)$ be a finite reflection group. We say that W is *not essential* if there exists a nonzero vector $\lambda \in V$ such that $t\lambda = \lambda$ for all $t \in W$. Otherwise, we say that W is *essential*.

For example, the dihedral group G of order $2m \geq 6$ is essential. Indeed, G contains a rotation t whose matrix representation is

$$\begin{bmatrix} \cos\frac{2\pi}{m} & -\sin\frac{2\pi}{m} \\ \sin\frac{2\pi}{m} & \cos\frac{2\pi}{m} \end{bmatrix}. \tag{23}$$

There exists no nonzero vector $\lambda \in V$ such that $t\lambda = \lambda$ since the matrix (23) does not have 1 as an eigenvalue:

$$\begin{vmatrix} \cos\frac{2\pi}{m} - 1 & -\sin\frac{2\pi}{m} \\ \sin\frac{2\pi}{m} & \cos\frac{2\pi}{m} - 1 \end{vmatrix} = 2(1 - \cos\frac{2\pi}{m}) \neq 0.$$

On the other hand, the group G_n which is isomorphic to $\mathcal{S}_n$ is not essential. Indeed, the vector $\lambda = \sum_{i=1}^{n} \varepsilon_i$ is fixed by every $t \in G_n$. In order to find connections between the dihedral group of order 6 and the group G_3, we need a method to produce an essential finite reflection group from non-essential one.

Given a finite reflection group $W \subset O(V)$, let

$$U = \{\lambda \in V \mid \forall t \in W,\ t\lambda = \lambda\}.$$

It is easy to see that U is a subspace of V. Let U' be the orthogonal complement of U in V. Since $tU = U$ for all $t \in W$, we have $tU' = U'$ for all $t \in W$. This allows to construct the restriction homomorphism $W \to O(U')$ defined by $t \mapsto t|_{U'}$.

Exercise 10. Show that the above restriction homomorphism is injective, and the image $W|_{U'}$ is an essential finite reflection group in $O(U')$.

For the group G_3, we have

$$\begin{aligned} U &= \mathbf{R}(\varepsilon_1 + \varepsilon_2 + \varepsilon_3), \\ U' &= \mathbf{R}(\varepsilon_1 - \varepsilon_2) + \mathbf{R}(\varepsilon_2 - \varepsilon_3) \\ &= \mathbf{R}\eta_1 + \mathbf{R}\eta_2, \end{aligned}$$

where

$$\begin{aligned} \eta_1 &= \frac{1}{\sqrt{2}}(\varepsilon_1 - \varepsilon_2), \\ \eta_2 &= \frac{1}{\sqrt{6}}(\varepsilon_1 + \varepsilon_2 - 2\varepsilon_3) \end{aligned}$$

is an orthonormal basis of U'.

Exercise 11. Compute the matrix representations of $g_{(1\ 2)}$ and $g_{(2\ 3)}$ with respect to the basis $\{\eta_1, \eta_2\}$. Show that they are reflections whose lines of symmetry form an angle $\pi/3$.

As a consequence of Exercise 10, we see that the group G_3, restricted to the subspace U' so that it becomes essential, is nothing but the dihedral group of order 6.

May 9, 2016

For today's lecture, we let V be a finite-dimensional vector space over $\mathbf{R}$, with positive-definite inner product. Recall that for $0 \neq \alpha \in V$, $s_\alpha \in O(V)$ denotes the reflection

$$s_\alpha(\lambda) = \lambda - \frac{2(\lambda, \alpha)}{(\alpha, \alpha)}\alpha \quad (\lambda \in V). \tag{24}$$

Lemma 12. *For $t \in O(V)$ and $0 \neq \alpha \in V$, we have $ts_\alpha t^{-1} = s_{t\alpha}$.*

Proof. For $\lambda \in V$, we have

$$\begin{aligned} ts_\alpha(\lambda) &= t\left(\lambda - \frac{2(\lambda, \alpha)}{(\alpha, \alpha)}\alpha\right) && \text{(by (24))} \\ &= t\lambda - \frac{2(\lambda, \alpha)}{(\alpha, \alpha)}t\alpha \\ &= t\lambda - \frac{2(t\lambda, t\alpha)}{(t\alpha, t\alpha)}t\alpha \\ &= s_{t\alpha}(t\lambda). \end{aligned}$$

This implies $ts_\alpha = s_{t\alpha}t$, and the result follows. $\square$

For example, if s_α is a reflection in a dihedral group G, and $t \in G$ is a rotation, then s_α and t are not necessarily commutative, but rotating before reflecting can be compensated by reflecting with respect to another line afterwards.

Proposition 13. *Let $W \subset O(V)$ be a finite reflection group, and let $0 \neq \alpha \in V$. If $w, s_\alpha \in W$, then $s_{w\alpha} \in W$.*

Proof. By Lemma 12, we have $s_{w\alpha} = ws_\alpha w^{-1} \in W$. $\square$

Definition 14. Let Φ be a nonempty finite set of nonzero vectors in V. We say that Φ is a *root system* if

(R1) $\Phi \cap \mathbf{R}\alpha = \{\alpha, -\alpha\}$ for all $\alpha \in \Phi$,

(R2) $s_\alpha\Phi = \Phi$ for all $\alpha \in \Phi$.

Proposition 15. *Let Φ be a root system in V. Then the subgroup*

$$W(\Phi) = \langle s_\alpha \mid \alpha \in \Phi \rangle$$

of $O(V)$ is a finite reflection group. Moreover, $W(\Phi)$ is essential if and only if Φ spans V. Conversely, for every finite reflection group $W \subset O(V)$, there exists a root system $\Phi \subset V$ such that $W = W(\Phi)$.

Proof. Since $\Phi \neq \emptyset$, the group $W(\Phi)$ contains at least one reflection. In particular, $W(\Phi) \neq \{\mathrm{id}_V\}$. By construction, W is generated by reflections. In order to show that W is finite, let U be the subspace of V spanned by Φ. Since $U^\perp \subset (\mathbf{R}\alpha)^\perp$ for all $\alpha \in \Phi$, we have $s_\alpha(\lambda) = \lambda$ for all $\alpha \in \Phi$ and $\lambda \in U^\perp$. This implies that

$$w|_{U^\perp} = \mathrm{id}_{U^\perp} \quad (w \in W). \tag{25}$$

In particular, W leaves $U^\perp$ invariant. Since $W \subset O(V)$, W also leaves U invariant. We can form the restriction homomorphism $W \to O(U)$ which is injective. Indeed, if an element $w \in W$ is in the kernel of the restriction homomorphism, then $w|_U = \mathrm{id}_U$. Together with (25), we see $w = \mathrm{id}_V$. By (R2), W permutes the finite set Φ, hence there is a homomorphism f from W to the symmetric group on Φ. An element $w \in \operatorname{Ker} f$ fixes every element of Φ, in particular, a basis of U. This implies that w is in the kernel of the restriction homomorphism, and hence $w = \mathrm{id}_V$. We have shown that f is an injection from W to the symmetric group of Φ which is finite. Therefore W is finite. This completes the proof of the first part.

Moreover, $W(\Phi)$ is not essential if and only if there exists a nonzero vector $\lambda \in V$ such that $t\lambda = \lambda$ for all $t \in W(\Phi)$. Since $W(\Phi)$ is generated by $\{s_\alpha \mid \alpha \in \Phi\}$,

$$\begin{aligned} t\lambda = \lambda \ (\forall t \in W(\Phi)) &\iff s_\alpha\lambda = \lambda \ (\forall \alpha \in \Phi) \\ &\iff (\lambda, \alpha) = 0 \ (\forall \alpha \in \Phi) \\ &\iff \lambda \in U^\perp. \end{aligned}$$

Thus, $W(\Phi)$ is not essential if and only if $U^\perp \neq 0$, or equivalently, Φ does not span V.

Conversely, let $W \subset O(V)$ be a finite reflection group, and let S be the set of all reflections of W. By Definition 8(iii), W is generated by S. Define

$$\Phi = \{\alpha \in V \mid s_\alpha \in S,\ \|\alpha\| = 1\}. \tag{26}$$

Observe

$$S = \{s_\alpha \mid \alpha \in \Phi\}. \tag{27}$$

We claim that Φ is a root system. First, since $W \neq \{\mathrm{id}_V\}$, we have $\Phi \neq \emptyset$. Let $\alpha \in \Phi$. Since $s_\alpha = s_{-\alpha}$ and $\|\alpha\| = \|-\alpha\|$, we see that Φ satisfies (R1). For $\beta \in \Phi$, we have $\|s_\alpha(\beta)\| = \|\beta\| = 1$, and $s_{s_\alpha(\beta)} \in W$ by Proposition 13, since $s_\alpha, s_\beta \in W$. This implies $s_\alpha(\beta) \in \Phi$, and hence $s_\alpha(\Phi) = \Phi$. Therefore, Φ is a root system. It remains to show that $W = W(\Phi)$. But this follows immediately from (27) since $W = \langle S \rangle$. □

Example 16. We have seen that the group G_n generated by reflections

$$\{s_{\varepsilon_i - \varepsilon_j} \mid 1 \le i < j \le n\}, \tag{28}$$

where $\varepsilon_1, \dots, \varepsilon_n$ is the standard basis of $\mathbf{R}^n$, is a finite reflection group which is abstractly isomorphic to the symmetric group of degree n. The set

$$\Phi = \{\pm(\varepsilon_i - \varepsilon_j) \mid 1 \le i < j \le n\} \tag{29}$$

is a root system. Indeed, Φ clearly satisfies (R1). It is also clear that $g_\sigma \Phi = \Phi$ for all $\sigma \in \mathcal{S}_n$, so in particular, (R2) holds.

Exercise 17. Show that (28) is precisely the set of reflections in G_n. In other words, show that g_σ is a reflection if and only if σ is a transposition.

Definition 18. A *total ordering* of V is a transitive relation on V (denoted $<$) satisfying the following axioms.

(i) For each pair $\lambda, \mu \in V$, exactly one of $\lambda < \mu$, $\lambda = \mu$, $\mu < \lambda$ holds.

(ii) For all $\lambda, \mu, \nu \in V$, $\mu < \nu$ implies $\lambda + \mu < \lambda + \nu$.

(iii) Let $\mu < \nu$ and $c \in \mathbf{R}$. If $c > 0$ then $c\mu < c\nu$, and if $c < 0$ then $c\nu < c\mu$.

For convenience, we write $\lambda > \mu$ if $\mu < \lambda$. By (ii), $\lambda > 0$ implies $0 > -\lambda$. Thus

$$V = V_+ \cup \{0\} \cup V_- \quad \text{(disjoint)}, \tag{30}$$

where

$$V_+ = \{\lambda \in V \mid \lambda > 0\}, \tag{31}$$
$$V_- = \{\lambda \in V \mid \lambda < 0\}. \tag{32}$$

We say that $\lambda \in V_+$ is *positive*, and $\lambda \in V_-$ is *negative*.

Example 19. Let $\lambda_1, \dots, \lambda_n$ be a basis of V. Define the lexicographic ordering of V with respect to $\lambda_1, \dots, \lambda_n$ by

$$\sum_{i=1}^{n} a_i\lambda_i < \sum_{i=1}^{n} b_i\lambda_i \iff \exists k \in \{1, 2, \dots, n\},\ a_1 = b_1, \dots, a_{k-1} = b_{k-1}, a_k < b_k.$$

Clearly, this is a total ordering of V. Note that $\lambda_i > 0$ for all $i \in \{1, \dots, n\}$. For $n = 2$, we have

$$V_+ = \{c_1\lambda_1 + c_2\lambda_2 \mid c_1 > 0,\ c_2 \in \mathbf{R}\} \cup \{c_2\lambda_2 \mid c_2 > 0\}.$$

Lemma 20. *Let $<$ be a total ordering of V, and let $\lambda, \mu \in V$.*

(i) *If $\lambda, \mu > 0$, then $\lambda + \mu > 0$.*

(ii) *If $\lambda > 0$, $c \in \mathbf{R}$ and $c > 0$, then $c\lambda > 0$.*

(iii) *If $\lambda > 0$, $c \in \mathbf{R}$ and $c < 0$, then $c\lambda < 0$. In particular, $-\lambda < 0$.*

Proof. (i) By Definition 18(ii), we have $\lambda + \mu > \lambda > 0$.

(ii) By Definition 18(iii), we have $c\lambda > c \cdot 0 = 0$.

(iii) By Definition 18(iii), we have $c\lambda < c \cdot 0 = 0$. Taking $c = -1$ gives the second statement. □

Definition 21. Let Φ be a root system in V. A subset Π of Φ is called a *positive system* if there exists a total ordering $<$ of V such that

$$\Pi = \{\alpha \in \Phi \mid \alpha > 0\}. \tag{33}$$

Since a total ordering of V always exists by Example 19, and every total ordering of V defines a positive system of a root system Φ in V, according to Definition 21, there are many positive systems in Φ.

Example 22. Continuing Example 16, let $<$ be the total ordering defined by the basis $\varepsilon_1, \dots, \varepsilon_n$. Then $\varepsilon_i > \varepsilon_j$ if $i < j$. Thus, according to (33),

$$\Pi = \{\varepsilon_i - \varepsilon_j \mid 1 \le i < j \le n\}.$$

Lemma 23. *If Π is a positive system in a root system Φ, then $\Phi = \Pi \cup (-\Pi)$ (disjoint), where*

$$-\Pi = \{-\alpha \mid \alpha \in \Pi\}. \tag{34}$$

In particular,

$$-\Pi = \{\alpha \in \Phi \mid \alpha < 0\}. \tag{35}$$

Proof. We have

$$\begin{aligned} \Pi \cap (-\Pi) &= \emptyset && \text{(by Lemma 20(iii))}, \\ \Pi &\subset \Phi && \text{(by Definition 21)}, \\ -\Pi &\subset \Phi && \text{(by Definition 14(R1))}. \end{aligned}$$

Thus, it remains to show $\Phi \subset \Pi \cup (-\Pi)$. Suppose $\alpha \in \Phi \setminus \Pi$. Then

$$\begin{aligned} \alpha \notin \Pi &\implies \alpha \not> 0 && \text{(by (33))} \\ &\implies \alpha < 0 && \text{(since } 0 \notin \Phi) \\ &\implies 0 < -\alpha && \text{(by Definition 18(ii))} \\ &\implies -\alpha \in \Pi && \text{(by (33))} \\ &\implies \alpha \in -\Pi && \text{(by (34))}. \end{aligned}$$

This proves $\Phi \setminus \Pi \subset (-\Pi)$, proving $\Phi \subset \Pi \cup (-\Pi)$.

Since $\Phi = \Pi \cup (-\Pi)$ (disjoint) and $0 \notin \Phi$, (33) implies (35). □

Definition 24. Let Π be a positive system in a root system Φ. We call $-\Pi$ defined by (34) the *negative system* in Φ with respect to Π.

Definition 25. Let Δ be a subset of a root system Φ. We call Δ a *simple system* if Δ is a basis of the subspace spanned by Φ, and if moreover each $\alpha \in \Phi$ is a linear combination of Δ with coefficients all of the same sign (all nonnegative or all nonpositive). In other words,

$$\Phi \subset \mathbf{R}_{\ge 0}\Delta \cup \mathbf{R}_{\le 0}\Delta, \tag{36}$$

where

$$\mathbf{R}_{\ge 0}\Delta = \{\sum_{\alpha \in \Delta} c_\alpha \alpha \mid c_\alpha \ge 0 \ (\alpha \in \Delta)\}.$$

If Δ is a simple system, we call its elements *simple roots*.

Example 26. Continuing Example 22,

$$\Delta = \{\varepsilon_i - \varepsilon_{i+1} \mid 1 \leq i < n\} \tag{37}$$

is a simple system. Indeed, for $\varepsilon_i - \varepsilon_j \in \Phi$, we have

$$\varepsilon_i - \varepsilon_j = \begin{cases} \sum_{k=i}^{j-1}(\varepsilon_k - \varepsilon_{k+1}) \in \mathbf{R}_{\geq 0}\Delta & \text{if } i < j, \\ \sum_{k=j}^{i-1}(-(\varepsilon_j - \varepsilon_{j+1})) \in \mathbf{R}_{\leq 0}\Delta & \text{otherwise.} \end{cases}$$

May 16, 2016

For today's lecture, we let V be a finite-dimensional vector space over $\mathbf{R}$, with positive-definite inner product.

Recall that a total ordering $<$ of V partitions V into three parts

$$V = V_+ \cup \{0\} \cup (-V_+),$$

such that

$$V_+ + V_+ \subset V_+, \tag{38}$$
$$\mathbf{R}_{\geq 0} V_+ \subset V_+ \cup \{0\}. \tag{39}$$

Lemma 27. *Let Δ be a finite set of nonzero vectors in V_+. If $(\alpha, \beta) \leq 0$ for any distinct $\alpha, \beta \in \Delta$, then Δ consists of linearly independent vectors.*

Proof. Let

$$\sum_{\alpha \in \Delta} a_\alpha \alpha = 0, \tag{40}$$

and define

$$\sigma = \sum_{\substack{\alpha \in \Delta \\ a_\alpha > 0}} a_\alpha \alpha.$$

Then

$$\begin{aligned} 0 &\leq (\sigma, \sigma) \\ &= \Big(\sum_{\substack{\alpha \in \Delta \\ a_\alpha > 0}} a_\alpha \alpha, \sum_{\alpha \in \Delta} a_\alpha \alpha - \sum_{\substack{\beta \in \Delta \\ a_\beta < 0}} a_\beta \beta\Big) \\ &= \Big(\sum_{\substack{\alpha \in \Delta \\ a_\alpha > 0}} a_\alpha \alpha, -\sum_{\substack{\beta \in \Delta \\ a_\beta < 0}} a_\beta \beta\Big) && \text{(by (40))} \\ &= -\sum_{\substack{\alpha \in \Delta \\ a_\alpha > 0}} \sum_{\substack{\beta \in \Delta \\ a_\beta < 0}} a_\alpha a_\beta (\alpha, \beta) \\ &\leq 0. \end{aligned}$$

This forces $\sigma = 0$, so there is no $\alpha \in \Delta$ with $a_\alpha > 0$. Similarly, we can show that there is no $\alpha \in \Delta$ with $a_\alpha < 0$. Therefore, $a_\alpha = 0$ for all $\alpha \in \Delta$. $\square$

Lemma 28. *Let $\Delta \subset V_+$ be a subset, and let $\alpha, \beta \in \Delta$ be linearly independent. If $\alpha \in \mathbf{R}_{>0}\beta + \mathbf{R}_{\geq 0}\Delta$, then $\alpha \in \mathbf{R}_{\geq 0}(\Delta \setminus \{\alpha\})$.*

Proof. Since

$$\alpha \in \mathbf{R}_{>0}\beta + \mathbf{R}_{\geq 0}\Delta$$

$$
\begin{aligned}
&= \mathbf{R}_{>0}\beta + \mathbf{R}_{\geq 0}\alpha + \mathbf{R}_{\geq 0}\beta + \mathbf{R}_{\geq 0}(\Delta \setminus \{\alpha, \beta\}) \\
&= \mathbf{R}_{\geq 0}\alpha + \mathbf{R}_{>0}\beta + \mathbf{R}_{\geq 0}(\Delta \setminus \{\alpha, \beta\}) \\
&\subset \mathbf{R}_{\geq 0}\alpha + V_+ \cap \mathbf{R}_{\geq 0}(\Delta \setminus \{\alpha\}),
\end{aligned}
$$

there exists $a \in \mathbf{R}_{\geq 0}$ such that

$$\alpha \in a\alpha + V_+ \cap \mathbf{R}_{\geq 0}(\Delta \setminus \{\alpha\}). \tag{41}$$

Thus

$$(1-a)\alpha \in V_+, \tag{42}$$
$$(1-a)\alpha \in \mathbf{R}_{\geq 0}(\Delta \setminus \{\alpha\}). \tag{43}$$

By (42), we have $1 - a > 0$. The result then follows from (43). $\square$

For a root system Φ in V, we denote by $\mathcal{P}(\Phi)$ and $\mathcal{S}(\Phi)$, the set of positive systems and that of simple systems, respectively, in Φ. More specifically,

$$
\begin{aligned}
\mathcal{P}(\Phi) &= \{\{\alpha \in \Phi \mid \alpha > 0\} \mid \text{“}{>}\text{” is a total ordering of } V\}, \\
\mathcal{S}(\Phi) &= \{\Delta \subset \Phi \mid \Phi \subset \mathbf{R}_{\geq 0}\Delta \cup \mathbf{R}_{\leq 0}\Delta,\ \Delta \text{ is linearly independent}\}.
\end{aligned}
$$

It is clear that $\mathcal{P}(\Phi)$ is non-empty, since V can be given a total ordering. We show that $\mathcal{S}(\Phi)$ is non-empty by establishing a bijection between $\mathcal{S}(\Phi)$ and $\mathcal{P}(\Phi)$, which is defined by

$$
\begin{array}{rcl}
\pi : \mathcal{S}(\Phi) & \to & \mathcal{P}(\Phi) \\
\Delta & \mapsto & \Phi \cap \mathbf{R}_{\geq 0}\Delta.
\end{array} \tag{44}
$$

Lemma 29. *Let Φ be a root system in V. If Δ is a simple system contained in a positive system Π, then*

(i) $\Pi = \Phi \cap \mathbf{R}_{\geq 0}\Delta$,

(ii) $\Delta = \{\alpha \in \Pi \mid \alpha \notin \mathbf{R}_{\geq 0}(\Pi \setminus \{\alpha\})\}$.

Proof. (i) Since Δ is a simple system, we have

$$\Phi \subset \mathbf{R}_{\geq 0}\Delta \cup \mathbf{R}_{\leq 0}\Delta. \tag{45}$$

Since $\Delta \subset \Pi \subset V_+$ for some total ordering of V, we have

$$\mathbf{R}_{\geq 0}\Delta \subset V_+ \cup \{0\}, \tag{46}$$
$$\mathbf{R}_{\leq 0}\Delta \subset V_- \cup \{0\}. \tag{47}$$

Thus

$$
\begin{aligned}
\Pi &= \Phi \cap V_+ \\
&= \Phi \cap (\mathbf{R}_{\geq 0}\Delta \cup \mathbf{R}_{\leq 0}\Delta) \cap V_+ && \text{(by (45))}
\end{aligned}
$$

$$\begin{aligned} &= \Phi \cap \mathbf{R}_{\geq 0}\Delta \cap V_+ && \text{(by (47))} \\ &= \Phi \cap (\mathbf{R}_{\geq 0}\Delta \setminus \{0\}) && \text{(by (46))} \\ &= \Phi \cap \mathbf{R}_{\geq 0}\Delta. \end{aligned}$$

(ii) If $\alpha \in \Pi \setminus \Delta$, then $\Delta \subset \Pi \setminus \{\alpha\}$, so $\mathbf{R}_{\geq 0}(\Pi \setminus \{\alpha\}) \supset \mathbf{R}_{\geq 0}\Delta \ni \alpha$. This proves

$$\Delta \supset \{\alpha \in \Pi \mid \alpha \notin \mathbf{R}_{\geq 0}(\Pi \setminus \{\alpha\})\}.$$

Conversely, suppose $\alpha \in \Pi$ and $\alpha \in \mathbf{R}_{\geq 0}(\Pi \setminus \{\alpha\})$. Then there exists $\beta \in \Pi \setminus \{\alpha\}$ such that

$$\begin{aligned} \alpha &\in \mathbf{R}_{>0}\beta + \mathbf{R}_{\geq 0}(\Pi \setminus \{\alpha, \beta\}) \\ &\subset \mathbf{R}_{>0}\beta + \mathbf{R}_{\geq 0}\Pi \\ &= \mathbf{R}_{>0}\beta + \mathbf{R}_{\geq 0}\Delta && \text{(by (i)).} \end{aligned}$$

Since $\beta \in \Pi \setminus \{\alpha\} \subset \mathbf{R}_{\geq 0}\Delta \setminus \mathbf{R}_{\geq 0}\alpha$, there exists $\delta \in \Delta \setminus \{\alpha\}$ such that

$$\beta \in \mathbf{R}_{>0}\delta + \mathbf{R}_{\geq 0}\Delta.$$

Thus $\alpha \in \mathbf{R}_{>0}\delta + \mathbf{R}_{\geq 0}\Delta$, and hence $\{\alpha\} \cup \Delta$ is linearly dependent. This implies $\alpha \notin \Delta$. □

Recall that for $0 \neq \alpha \in V$, $s_\alpha \in O(V)$ denotes the reflection

$$s_\alpha(\lambda) = \lambda - \frac{2(\lambda, \alpha)}{(\alpha, \alpha)}\alpha \quad (\lambda \in V). \tag{48}$$

Theorem 30. *Let Φ be a root system in V. Then the mapping $\pi : \mathcal{S}(\Phi) \to \mathcal{P}(\Phi)$ defined by* (44) *is a bijection whose inverse is given by*

$$\begin{array}{rcl} \pi^{-1} : \mathcal{P}(\Phi) & \to & \mathcal{S}(\Phi) \\ \Pi & \mapsto & \{\alpha \in \Pi \mid \alpha \notin \mathbf{R}_{\geq 0}(\Pi \setminus \{\alpha\})\}. \end{array} \tag{49}$$

Moreover,

(i) *for every simple system Δ in Φ, $\pi(\Delta)$ is the unique positive system containing Δ,*

(ii) *for every positive system Π in Φ, $\pi^{-1}(\Pi)$ is the unique simple system contained in* Π.

Proof. If $\Delta \in \mathcal{S}(\Phi)$, then Δ is a basis of the subspace spanned by Φ, so there exists a basis $\tilde{\Delta}$ of V containing Δ. By Example 19, there exists a total ordering $<$ of V such that $\alpha > 0$ for all $\alpha \in \tilde{\Delta}$. Then

$$\begin{aligned} \pi(\Delta) &= \Phi \cap \mathbf{R}_{\geq 0}\Delta \\ &= \Phi \cap (\mathbf{R}_{\geq 0}\Delta \cup \mathbf{R}_{\leq 0}\Delta) \cap V_+ \\ &= \Phi \cap V_+ \end{aligned}$$

is a positive system containing Δ.

Next we show that π is injective. Suppose $\Delta, \Delta' \in \mathcal{S}(\Phi)$ and $\pi(\Delta) = \pi(\Delta')$. Then both Δ and Δ' are simple system contained in $\Pi = \pi(\Delta)$. By Lemma 29(ii), we have

$$\Delta = \{\alpha \in \Pi \mid \alpha \notin \mathbf{R}_{\geq 0}(\Pi \setminus \{\alpha\})\} = \Delta'.$$

Therefore, π is injective. Note that this shows

$$\pi^{-1}(\Pi) \subset \{\{\alpha \in \Pi \mid \alpha \notin \mathbf{R}_{\geq 0}(\Pi \setminus \{\alpha\})\}\}. \tag{50}$$

Next we show that π is surjective. Suppose $\Pi \in \mathcal{P}(\Phi)$. Define $\mathcal{D}$ by

$$\mathcal{D} = \{\Delta \subset \Pi \mid \Pi \subset \mathbf{R}_{\geq 0}\Delta\}. \tag{51}$$

Since Φ is a finite set, so are Π and $\mathcal{D}$. Since $\Pi \in \mathcal{D}$, $\mathcal{D}$ is non-empty. Thus, there exists a minimal member Δ of $\mathcal{D}$. This means

$$\Pi \subset \mathbf{R}_{\geq 0}\Delta, \tag{52}$$

$$\forall \alpha \in \Delta,\ \Pi \not\subset \mathbf{R}_{\geq 0}(\Delta \setminus \{\alpha\}). \tag{53}$$

Since Π is a positive system, there exists a total ordering of V such that $\Pi = \Phi \cap V_+$. In particular, $\Delta \subset V_+$. We claim

$$(\alpha, \beta) \leq 0 \text{ for all pairs } \alpha \neq \beta \text{ in } \Delta. \tag{54}$$

Indeed, suppose, to the contrary, $(\alpha, \beta) > 0$ for some distinct $\alpha, \beta \in \Delta$. Since $\pm s_\alpha(\beta) \in \Phi = \Pi \cup (-\Pi)$, in view of (48), we may assume without loss of generality $\alpha \in \mathbf{R}_{>0}\beta + \mathbf{R}_{\geq 0}\Delta$. Then by Lemma 28, we obtain $\alpha \in \mathbf{R}_{\geq 0}(\Delta \setminus \{\alpha\})$. Now

$$\begin{aligned} \mathbf{R}_{\geq 0}(\Delta \setminus \{\alpha\}) &= \mathbf{R}_{\geq 0}\alpha + \mathbf{R}_{\geq 0}(\Delta \setminus \{\alpha\}) \\ &= \mathbf{R}_{\geq 0}\Delta \\ &\supset \Pi, \end{aligned}$$

contradicting (53). This proves (54). Now, by Lemma 27, Δ consists of linearly independent vectors. We have shown that Δ is a simple system, and by construction, $\Delta \subset \Pi$. Lemma 29(i) then implies $\Pi = \pi(\Delta)$. Therefore, π is surjective. This also implies that equality holds in (50), which shows that the inverse π^{-1} is given by (49).

Finally, (i) follows from Lemma 29(i), while (ii) follows from Lemma 29(ii). □

May 30, 2016

For today's lecture, we let V be a finite-dimensional vector space over $\mathbf{R}$, with positive-definite inner product. We also let Φ be a root system in V. Recall that $\mathcal{P}(\Phi)$ and $\mathcal{S}(\Phi)$ denote the set of positive systems and that of simple systems, respectively, in Φ. Define

$$\begin{array}{rcl} \pi : \mathcal{S}(\Phi) & \to & \mathcal{P}(\Phi) \\ \Delta & \mapsto & \Phi \cap \mathbf{R}_{\geq 0}\Delta. \end{array}$$

Theorem 30 is proved in an awkward manner, in the sense that $\pi^{-1}(\Pi) \in \mathcal{S}(\Phi)$ for $\Pi \in \mathcal{P}(\Phi)$ is not explicitly shown. Lemma 29(ii) shows that the existence of a simple system in Π does imply $\pi^{-1}(\Pi) \in \mathcal{S}(\Phi)$, but showing the existence of a simple system in Π is a separate problem. Here is how one can show $\pi^{-1}(\Pi) \in \mathcal{S}(\Phi)$ directly. We need a lemma.

Lemma 31. *Suppose that V is given a total ordering, let $A \subset V_+$ be a subset, $\alpha_1, \dots, \alpha_n \in V_+$, and $\beta \in V_+ \setminus \bigcup_{i=1}^n \mathbf{R}\alpha_i$. If*

$$\alpha_i \in \mathbf{R}_{\geq 0}(A \cup \{\beta\}), \tag{55}$$

$$\beta \in \mathbf{R}_{\geq 0}(A \cup \{\alpha_1, \dots, \alpha_n\}), \tag{56}$$

then $\alpha_1, \dots, \alpha_n, \beta \in \mathbf{R}_{\geq 0}A$.

Proof. Let $\mathcal{A} = \mathbf{R}_{\geq 0}A$, $\mathcal{A}_+ = \mathcal{A} \setminus \{0\}$. By the assumption, we have $\mathcal{A}_+ \subset V_+$. Then it suffices to show

$$\beta \in \mathcal{A} \tag{57}$$

only, since $\alpha_i \in \mathcal{A}$ follows immediately from (55) and (57).

By (55), there exist $b_i \in \mathbf{R}_{\geq 0}$ and $\lambda_i \in \mathcal{A}$ such that

$$\alpha_i = b_i\beta + \lambda_i. \tag{58}$$

Since $\beta \notin \mathbf{R}\alpha_i$, we have $\lambda_i \neq 0$, i.e.,

$$\lambda_i \in \mathcal{A}_+. \tag{59}$$

By (56), there exist $a_1, \dots, a_n \in \mathbf{R}_{\geq 0}$ such that

$$\beta \in \sum_{i=1}^n a_i\alpha_i + \mathcal{A}. \tag{60}$$

If $a_i = 0$ for all i, then (57) holds, so we may assume $a_i > 0$ for some i. Then (59) implies

$$\sum_{i=1}^n a_i\lambda_i \in \mathcal{A}_+. \tag{61}$$

By (58) and (60), we obtain

$$\beta \in \sum_{i=1}^n a_i(b_i\beta + \lambda_i) + \mathcal{A}$$

$$
\begin{aligned}
&= \sum_{i=1}^{n} a_i b_i \beta + \sum_{i=1}^{n} a_i \lambda_i + \mathcal{A} \\
&\subset \sum_{i=1}^{n} a_i b_i \beta + \mathcal{A}_+ && \text{(by (61))} \\
&= \sum_{i=1}^{n} a_i b_i \beta + V_+ \cap \mathcal{A}.
\end{aligned}
$$

This implies

$$\left(1 - \sum_{i=1}^{n} a_i b_i\right) \beta \in V_+, \tag{62}$$

$$\left(1 - \sum_{i=1}^{n} a_i b_i\right) \beta \in \mathcal{A}. \tag{63}$$

By (62), we have $1 - \sum_{i=1}^{n} a_i b_i > 0$. Then (57) follows from (63). $\square$

Proposition 32. *Let* $\Pi \in \mathcal{P}(\Phi)$*, and set*

$$\Delta = \{\alpha \in \Pi \mid \alpha \notin \mathbf{R}_{\geq 0}(\Pi \setminus \{\alpha\})\}.$$

Then

(i) $(\alpha, \beta) \leq 0$ *for all* $\alpha \neq \beta$ *in* Δ*,*

(ii) Δ *is a simple system in* Φ*.*

Proof. (i) Suppose, to the contrary, $(\alpha, \beta) > 0$ for some distinct $\alpha, \beta \in \Delta$. Since $\pm s_\alpha(\beta) \in \Phi = \Pi \cup (-\Pi)$, in view of (48), we may assume without loss of generality $\alpha \in \mathbf{R}_{>0}\beta + \mathbf{R}_{\geq 0}\Pi$. By Lemma 28, we obtain $\alpha \in \mathbf{R}_{\geq 0}(\Pi \setminus \{\alpha\})$, which contradicts $\alpha \in \Delta$.

(ii) By (i) and Lemma 27, Δ consists of linearly independent vectors. It remains to show $\Pi \subset \mathbf{R}_{\geq 0}\Delta$. We consider the set

$$\mathcal{B} = \{B \subset \Pi \setminus \Delta \mid B \subset \mathbf{R}_{\geq 0}(\Pi \setminus B)\}.$$

For all $\alpha \in \Pi \setminus \Delta$, we have $\alpha \in \mathbf{R}_{\geq 0}(\Pi \setminus \{\alpha\})$. Thus $\{\alpha\} \in \mathcal{B}$, and hence $\mathcal{B} \neq \emptyset$.

Let $B = \{\alpha_1, \dots, \alpha_n\}$ be a maximal member of $\mathcal{B}$. Suppose $B \subsetneq \Pi \setminus \Delta$. Then there exists $\beta \in \Pi \setminus (B \cup \Delta)$. Set $A = \Pi \setminus (B \cup \{\beta\})$. Then (55) holds since $B \in \mathcal{B}$, while (56) holds since $\beta \notin \Delta$. Lemma 31 then implies $\alpha_1, \dots, \alpha_n, \beta \in \mathbf{R}_{\geq 0}(\Pi \setminus (B \cup \{\beta\})$. This implies $B \cup \{\beta\} \in \mathcal{B}$, contradicting maximality of B. Therefore, $B = \Pi \setminus \Delta$. This implies $\Pi \setminus \Delta \in \mathcal{B}$, which in turn implies $\Pi \setminus \Delta \subset \mathbf{R}_{\geq 0}\Delta$. Since $\Delta \subset \mathbf{R}_{\geq 0}\Delta$ holds trivially, we obtain $\Pi \subset \mathbf{R}_{\geq 0}\Delta$. This completes the proof of (ii). $\square$

Recall

$$W(\Phi) = \langle s_\alpha \mid \alpha \in \Phi \rangle.$$

By Definition 14(R2), we have

$$w\Phi = \Phi \quad (w \in W(\Phi)). \tag{64}$$

Lemma 33. *Let $w \in W(\Phi)$. Then*

(i) $w\Delta \in \mathcal{S}(\Phi)$ *and* $\pi(w\Delta) = w\pi(\Delta)$ *for all* $\Delta \in \mathcal{S}(\Phi)$*,*

(ii) $w\Pi \in \mathcal{P}(\Phi)$ *and* $\pi^{-1}(w\Pi) = w\pi^{-1}(\Pi)$ *for all* $\Pi \in \mathcal{P}(\Phi)$*.*

Proof. (i) Clear from (64) and (44).

(ii) For $\Pi \in \mathcal{P}(\Phi)$, let $\Delta = \pi^{-1}(\Pi) \in \mathcal{S}(\Phi)$. Then $w\Pi = w\pi(\Delta) = \pi(w\Delta) \in \pi(\mathcal{S}(\Phi)) = \mathcal{P}(\Phi)$ by (i). Also, $\pi^{-1}(w\Pi) = w\Delta = w\pi^{-1}(\Pi)$. □

Lemma 34. *Let $\alpha \in \Delta \in \mathcal{S}(\Phi)$ and $\Pi = \pi(\Delta)$. Then $s_\alpha(\Pi \setminus \{\alpha\}) = \Pi \setminus \{\alpha\}$.*

Proof. Let $\beta \in \Pi \setminus \{\alpha\}$, and write $\beta = \sum_{\gamma\in\Delta} c_\gamma \gamma$. Then

$$\exists \gamma \in \Delta \setminus \{\alpha\},\ c_\gamma > 0. \tag{65}$$

Set

$$c = \frac{2(\beta, \alpha)}{(\alpha, \alpha)},$$

so that

$$\begin{aligned} s_\alpha\beta &= \beta - c\alpha \\ &= \sum_{\gamma\in\Delta} c_\gamma\gamma - c\alpha \\ &= \sum_{\gamma\in\Delta\setminus\{\alpha\}} c_\gamma\gamma + (c_\alpha - c)\alpha. \end{aligned}$$

Since $s_\alpha\beta \in \Phi \subset \mathbf{R}_{\geq 0}\Delta \cup \mathbf{R}_{\leq 0}\Delta$, (65) implies $s_\alpha\beta \in \Phi \cap \mathbf{R}_{\geq 0}\Delta = \pi(\Delta) = \Pi$. Since $\beta \in \Pi \not\ni -\alpha$, we have $\beta \neq -\alpha = s_\alpha\alpha$. Thus $s_\alpha\beta \neq \alpha$. Therefore, $s_\alpha\beta \in \Pi \setminus \{\alpha\}$. □

Definition 35. Let G be a group, and let Ω be a set. We say that G *acts on* Ω if there is a mapping

$$\begin{array}{ccc} G \times \Omega & \to & \Omega \\ (g, \alpha) & \mapsto & g.\alpha \end{array} \quad (g \in G,\ \alpha \in \Omega)$$

such that

(i) $1.\alpha = \alpha$ for all $\alpha \in \Omega$,

(ii) $g.(h.\alpha) = (gh).\alpha$ for all $g, h \in G$ and $\alpha \in \Omega$.

We say that G acts *transitively* on Ω, or the action of G is *transitive*, if

$$\forall \alpha, \beta \in \Omega,\ \exists g \in G,\ g.\alpha = \beta.$$

Observe, by Lemma 23,

$$|\Pi| = \frac{1}{2}|\Phi| \quad (\Pi \in \mathcal{P}(\Phi)). \tag{66}$$

Theorem 36. *The group $W(\Phi)$ acts transitively on both $\mathcal{P}(\Phi)$ and $\mathcal{S}(\Phi)$.*

Proof. First we show that

$$\forall\Pi, \Pi' \in \mathcal{P}(\Phi),\ \exists w \in W(\Phi),\ w\Pi = \Pi' \tag{67}$$

by induction on $r = |\Pi \cap (-\Pi')|$. If $r = 0$, then $\Pi \subset \Pi'$, and we obtain $\Pi = \Pi'$ by (66).

If $r > 0$, then $\Pi \neq \Pi'$. Let $\Delta = \pi^{-1}(\Pi)$. Then $\Delta \neq \pi^{-1}(\Pi')$, so Δ is not contained in Π' by Theorem 30(ii). This implies $\Delta \cap (-\Pi') \neq \emptyset$ since $\Phi = \Pi' \cup (-\Pi')$. Choose $\alpha \in \Delta \cap (-\Pi')$. Then

$$-\alpha \notin -\Pi'. \tag{68}$$

Since

$$\begin{aligned} s_\alpha\Pi &= s_\alpha(\{\alpha\} \cup (\Pi \setminus \{\alpha\})) \\ &= \{s_\alpha\alpha\} \cup (s_\alpha(\Pi \setminus \{\alpha\})) \\ &= \{-\alpha\} \cup s_\alpha(\Pi \setminus \{\alpha\}) \\ &= \{-\alpha\} \cup (\Pi \setminus \{\alpha\}) && \text{(by Lemma 34)}, \end{aligned}$$

we have

$$\begin{aligned} |s_\alpha\Pi \cap (-\Pi')| &= |(\{-\alpha\} \cup (\Pi \setminus \{\alpha\})) \cap (-\Pi')| \\ &= |(\Pi \setminus \{\alpha\}) \cap (-\Pi')| && \text{(by (68))} \\ &= |(\Pi \cap (-\Pi')) \setminus \{\alpha\}| \\ &= r - 1. \end{aligned}$$

Since $s_\alpha\Pi \in \mathcal{P}(\Phi)$ by Lemma 33(ii), the inductive hypothesis applied to the pair $s_\alpha\Pi, \Pi'$ implies that there exists $w \in W(\Phi)$ such that $ws_\alpha\Pi = \Pi'$. Therefore, we have proved (67), which implies that $W(\Phi)$ acts transitively on $\mathcal{P}(\Phi)$. The transitivity of $W(\Phi)$ on $\mathcal{S}(\Phi)$ now follows immediately from Lemma 33 using the fact that π is a bijection from $\mathcal{S}(\Phi)$ to $\mathcal{P}(\Phi)$. □

Definition 37. Let $\Delta \in \mathcal{S}(\Phi)$. For $\beta = \sum_{\alpha\in\Delta} c_\alpha\alpha \in \Phi$, the *height* of β relative to Δ, denoted $\mathrm{ht}(\beta)$, is defined as

$$\mathrm{ht}(\beta) = \sum_{\alpha\in\Delta} c_\alpha.$$

Example 38. Continuing Example 26, let

$$\Delta = \{\varepsilon_i - \varepsilon_{i+1} \mid 1 \leq i < n\} \in \mathcal{S}(\Phi),$$

where

$$\Phi = \{\pm(\varepsilon_i - \varepsilon_j) \mid 1 \leq i < j \leq n\}.$$

Then for $i < j$,

$$\mathrm{ht}(\varepsilon_i - \varepsilon_j) = \mathrm{ht}(\sum_{k=i}^{j-1}(\varepsilon_k - \varepsilon_{k+1})) = j - i.$$

June 6, 2016

For today's lecture, we let V be a finite-dimensional vector space over $\mathbf{R}$, with positive-definite inner product. We also let Φ be a root system in V, and fix a simple system Δ in Φ. Let $\Pi = \Phi \cap \mathbf{R}_{\geq 0}\Delta$ be the unique positive system containing Δ. Recall

$$W(\Phi) = \langle s_\alpha \mid \alpha \in \Phi \rangle,$$

which we denote by W for brevity.

Lemma 39. *If $\beta \in \Pi \backslash \Delta$, then there exists $\alpha \in \Delta$ such that $s_\alpha \beta \in \Pi$ and $\mathrm{ht}(\beta) > \mathrm{ht}(s_\alpha \beta)$.*

Proof. Write $\beta = \sum_{\alpha \in \Delta} c_\alpha \alpha$, where $c_\alpha \in \mathbf{R}_{\geq 0}$ for $\alpha \in \Delta$. Since

$$\begin{aligned} 0 &< (\beta, \beta) \\ &= \sum_{\alpha \in \Delta} c_\alpha (\alpha, \beta), \end{aligned}$$

there exists $\alpha \in \Delta$ such that $c_\alpha(\alpha, \beta) > 0$. In particular, as $c_\alpha \geq 0$, we have

$$c = \frac{2(\alpha, \beta)}{(\alpha, \alpha)} > 0.$$

Since

$$\begin{aligned} s_\alpha \beta &= \beta - c\alpha \\ &= \sum_{\gamma \in \Delta \backslash \{\alpha\}} c_\gamma \gamma + (c_\alpha - c)\alpha, \end{aligned}$$

we have $\mathrm{ht}(s_\alpha \beta) = \mathrm{ht}(\beta) - c < \mathrm{ht}(\beta)$. Since $\beta \in \Pi \setminus \Delta \subset \Pi \setminus \{\alpha\}$, Lemma 34 implies $s_\alpha \beta \in \Pi$. □

Lemma 40. *If $\beta \in \Phi$, then there exists a sequence $\alpha_1, \ldots, \alpha_m$ of elements in Δ such that $s_{\alpha_1} \cdots s_{\alpha_m} \beta \in \Delta$.*

Proof. We first prove the assertion for $\beta \in \Pi$. Suppose there exists $\beta \in \Pi$ such that the assertion does not hold. Then clearly $\beta \notin \Delta$. We may assume that β has minimal height among such elements. By Lemma 39, there exists $\alpha \in \Delta$ such that $s_\alpha \beta \in \Pi$ and $\mathrm{ht}(\beta) > \mathrm{ht}(s_\alpha \beta)$. By the minimality of $\mathrm{ht}(\beta)$, there exists a sequence $\alpha_1, \ldots, \alpha_m$ of elements of Δ such that $s_{\alpha_1} \cdots s_{\alpha_m}(s_\alpha \beta) \in \Delta$. This is a contradiction.

If $\beta \in -\Pi$, then $-\beta \in \Pi$, so there exist $\alpha, \alpha_1, \ldots, \alpha_m \in \Delta$ such that

$$\alpha = s_{\alpha_1} \cdots s_{\alpha_m}(-\beta).$$

Then

$$s_\alpha s_{\alpha_1} \cdots s_{\alpha_m} \beta = -s_\alpha s_{\alpha_1} \cdots s_{\alpha_m}(-\beta)$$

$$
\begin{aligned}
&= -s_\alpha \alpha \\
&= \alpha \\
&\in \Delta.
\end{aligned}
$$

$\square$

Theorem 41. *If Δ is a simple system in a root system Φ, then $W = \langle s_\alpha \mid \alpha \in \Delta \rangle$.*

Proof. Let $\beta \in \Phi$. By Lemma 40, there exist $\alpha_0, \alpha_1, \ldots, \alpha_m \in \Delta$ such that $s_{\alpha_1} \cdots s_{\alpha_m} \beta = \alpha_0$. Then

$$
\begin{aligned}
s_\beta &= s_{(s_{\alpha_1} \cdots s_{\alpha_m})^{-1} \alpha_0} \\
&= (s_{\alpha_1} \cdots s_{\alpha_m})^{-1} s_{\alpha_0} s_{\alpha_1} \cdots s_{\alpha_m} && \text{(by Lemma 12)} \\
&= s_{\alpha_m} \cdots s_{\alpha_1} s_{\alpha_0} s_{\alpha_1} \cdots s_{\alpha_m} \\
&\in \langle s_\alpha \mid \alpha \in \Delta \rangle.
\end{aligned}
$$

$\square$

Definition 42. For $w \in W$, we define the *length* of w, denoted $\ell(w)$, to be

$$
\ell(w) = \min\{r \in \mathbf{Z} \mid r \geq 0,\ \exists \alpha_1, \ldots, \alpha_r \in \Delta,\ w = s_{\alpha_1} \cdots s_{\alpha_r}\}.
$$

By convention, $\ell(1) = 0$.

Clearly, $\ell(w) = 1$ if and only if $w = s_\alpha$ for some $\alpha \in \Delta$. It is also clear that $\ell(w) = \ell(w^{-1})$.

Lemma 43. *For $w \in W$, $\det(w) = (-1)^{\ell(w)}$.*

Proof. Since $\det(s_\alpha) = -1$ for all $\alpha \in \Phi$, the result follows immediately. $\square$

Lemma 44. *For $w \in W$ and $\alpha \in \Delta$, $\ell(s_\alpha w) = \ell(w) + 1$ or $\ell(w) - 1$.*

Proof. It is clear from the definition that $\ell(s_\alpha w) \leq \ell(w) + 1$. Switching the role of w and $s_\alpha w$, we obtain $\ell(s_\alpha w) \geq \ell(w) - 1$. Thus

$$
\ell(s_\alpha w) \in \{\ell(w) - 1, \ell(w), \ell(w) + 1\}.
$$

Since

$$
\begin{aligned}
(-1)^{\ell(s_\alpha w)} &= \det(s_\alpha w) && \text{(by Lemma 43)} \\
&= -\det w \\
&= -(-1)^{\ell(w)} && \text{(by Lemma 43).}
\end{aligned}
$$

This implies $\ell(s_\alpha w) \neq \ell(w)$. $\square$

Notation 45. For $w \in W$, we write

$$n(w) = |\Pi \cap w^{-1}(-\Pi)|.$$

Lemma 46. *For $w \in W$, $n(w^{-1}) = n(w)$.*

Proof.

$$\begin{aligned} n(w^{-1}) &= |\Pi \cap w(-\Pi)| \\ &= |w^{-1}\Pi \cap (-\Pi)| \\ &= |w^{-1}(-\Pi) \cap \Pi| \\ &= n(w). \end{aligned}$$

□

Lemma 47. *For $w \in W$ and $\alpha \in \Delta$, the following statements hold:*

(i) $w\alpha > 0 \implies n(ws_\alpha) = n(w) + 1.$

(ii) $w\alpha < 0 \implies n(ws_\alpha) = n(w) - 1.$

(iii) $w^{-1}\alpha > 0 \implies n(s_\alpha w) = n(w) + 1.$

(iv) $w^{-1}\alpha < 0 \implies n(s_\alpha w) = n(w) - 1.$

Proof. (i) Since $w\alpha \in \Pi$, we have $\alpha \in w^{-1}\Pi$. Thus

$$\alpha \notin w^{-1}(-\Pi), \tag{69}$$

and

$$\begin{aligned} \alpha &= -s_\alpha \alpha \\ &\in -s_\alpha w^{-1}\Pi \\ &= s_\alpha w^{-1}(-\Pi). \end{aligned} \tag{70}$$

Thus

$$\begin{aligned} n(ws_\alpha) &= |\Pi \cap (ws_\alpha)^{-1}(-\Pi)| \\ &= |\Pi \cap s_\alpha w^{-1}(-\Pi)| \\ &= |(\Pi \setminus \{\alpha\}) \cap s_\alpha w^{-1}(-\Pi)| + 1 && \text{(by (70))} \\ &= |s_\alpha(\Pi \setminus \{\alpha\}) \cap s_\alpha w^{-1}(-\Pi)| + 1 && \text{(by Lemma 34)} \\ &= |(\Pi \setminus \{\alpha\}) \cap w^{-1}(-\Pi)| + 1 \\ &= |\Pi \cap w^{-1}(-\Pi)| + 1 && \text{(by (69))} \\ &= n(w) + 1. \end{aligned}$$

(ii) Since $w\alpha \in -\Pi$, we have

$$\alpha \in w^{-1}(-\Pi), \tag{71}$$

and $\alpha \notin w^{-1}\Pi$, so

$$\begin{aligned} \alpha &= -s_\alpha \alpha \\ &\notin -s_\alpha w^{-1}\Pi \\ &= s_\alpha w^{-1}(-\Pi). \end{aligned} \tag{72}$$

Thus

$$\begin{aligned} n(ws_\alpha) &= |\Pi \cap (ws_\alpha)^{-1}(-\Pi)| \\ &= |\Pi \cap s_\alpha w^{-1}(-\Pi)| \\ &= |(\Pi \setminus \{\alpha\}) \cap s_\alpha w^{-1}(-\Pi)| && \text{(by (72))} \\ &= |s_\alpha(\Pi \setminus \{\alpha\}) \cap s_\alpha w^{-1}(-\Pi)| && \text{(by Lemma 34)} \\ &= |(\Pi \setminus \{\alpha\}) \cap w^{-1}(-\Pi)| \\ &= |\Pi \cap w^{-1}(-\Pi)| - 1 && \text{(by (71))} \\ &= n(w) - 1. \end{aligned}$$

(iii) and (iv)

$$\begin{aligned} n(s_\alpha w) &= n((s_\alpha w)^{-1}) && \text{(by Lemma 46)} \\ &= n(w^{-1}s_\alpha) \\ &= \begin{cases} n(w^{-1}) + 1 & \text{if } w^{-1}\alpha > 0, \\ n(w^{-1}) - 1 & \text{if } w^{-1}\alpha < 0 \end{cases} \\ &= \begin{cases} n(w) + 1 & \text{if } w^{-1}\alpha > 0, \\ n(w) - 1 & \text{if } w^{-1}\alpha < 0 \end{cases} && \text{(by Lemma 46).} \end{aligned}$$

□

Theorem 48. *Let Δ be a simple system in a root system Φ. Let $\alpha_1, \dots, \alpha_r \in \Delta$ and $w = s_1 \cdots s_r \in W$, where $s_i = s_{\alpha_i}$ for $1 \le i \le r$. If $n(w) < r$, then there exist i, j with $1 \le i < j \le r$ satisfying the following conditions:*

(i) $\alpha_i = s_{i+1} \cdots s_{j-1}\alpha_j$,

(ii) $s_{i+1}s_{i+2} \cdots s_j = s_i s_{i+1} \cdots s_{j-1}$,

(iii) $w = s_1 \cdots s_{i-1}s_{i+1} \cdots s_{j-1}s_{j+1} \cdots s_r$.

In particular, $n(w) \ge \ell(w)$.

Proof. (i) Setting $w = 1$ in Lemma 47(i), we find $n(s_\alpha) = 1$ for every $\alpha \in \Delta$. This implies that, if $r = 1$, then $n(w) = 1$. Therefore, we may assume $r \geq 2$.

We claim that there exists j with $2 \leq j \leq r$ such that $s_1 \cdots s_{j-1}\alpha_j < 0$. Suppose, to the contrary,

$$s_1 \cdots s_{j-1}\alpha_j > 0 \tag{73}$$

for all j with $2 \leq j \leq r$. Since $\alpha_1 > 0$, (73) holds also for $j = 1$. By Lemma 47(i), we obtain $n(s_1 \cdots s_j) = n(s_1 \cdots s_{j-1}) + 1$ for $1 \leq j \leq r$. By using induction, we obtain $n(w) = r$, contrary to our hypothesis.

Since $\alpha_j > 0$, there exists i with $1 \leq i < j$ such that

$$\begin{aligned} s_{i+1} \cdots s_{j-1}\alpha_j &> 0, \\ s_i s_{i+1} \cdots s_{j-1}\alpha_j &< 0. \end{aligned}$$

Thus

$$\begin{aligned} s_i s_{i+1} \cdots s_{j-1}\alpha_j &\in s_i\Pi \cap (-\Pi) \\ &= s_{\alpha_i}((\Pi \setminus \{\alpha_i\}) \cup \{\alpha_i\}) \cap (-\Pi) \\ &= ((\Pi \setminus \{\alpha_i\}) \cup \{-\alpha_i\}) \cap (-\Pi) && \text{(by Lemma 34)} \\ &= \{-\alpha_i\} \\ &= \{s_i(\alpha_i)\}. \end{aligned}$$

This implies $s_{i+1} \cdots s_{j-1}\alpha_j = \alpha_i$.

(ii)

$$\begin{aligned} s_{i+1} \cdots s_j &= s_{i+1} \cdots s_{j-1} s_{\alpha_j} (s_{i+1} \cdots s_{j-1})^{-1} (s_{i+1} \cdots s_{j-1}) \\ &= s_{s_{i+1} \cdots s_{j-1}\alpha_j} (s_{i+1} \cdots s_{j-1}) && \text{(by Lemma 12)} \\ &= s_{\alpha_i} (s_{i+1} \cdots s_{j-1}) && \text{(by (i))} \\ &= s_i s_{i+1} \cdots s_{j-1}. \end{aligned}$$

(iii)

$$\begin{aligned} w &= s_1 \cdots s_r \\ &= s_1 \cdots s_{i-1}(s_i \cdots s_{j-1}) s_j \cdots s_r \\ &= s_1 \cdots s_{i-1}(s_{i+1} \cdots s_j) s_j \cdots s_r && \text{(by (ii))} \\ &= s_1 \cdots s_{i-1} s_{i+1} \cdots s_{j-1} s_{j+1} \cdots s_r. \end{aligned}$$

In particular, $n(w) < r$ implies $r \neq \ell(w)$. Thus $n(w) \geq \ell(w)$. □

Corollary 49. *If $w \in W$, then $n(w) = \ell(w)$.*

Proof. From the last part of Theorem 48, it suffices to prove

$$n(w) \leq \ell(w) \quad (w \in W). \tag{74}$$

By the definition of $\ell(w)$, there exists $\alpha_1, \ldots, \alpha_{\ell(w)} \in \Delta$ such that $w = s_{\alpha_1} \cdots s_{\alpha_{\ell(w)}}$. We prove (74) by induction on $m = \ell(w)$. If $m = 0$, then $w = 1$, and $n(w) = 0 = \ell(w)$. Assume the result holds for up to $m - 1$. Then

$$\begin{aligned} n(s_{\alpha_1} \cdots s_{\alpha_{\ell(w)-1}}) &\leq \ell(s_{\alpha_1} \cdots s_{\alpha_{\ell(w)-1}}) \\ &\leq \ell(w) - 1. \end{aligned} \tag{75}$$

$$\begin{aligned} n(w) &= n((s_{\alpha_1} \cdots s_{\alpha_{\ell(w)-1}}) s_{\alpha_{\ell(w)}}) \\ &\leq n(s_{\alpha_1} \cdots s_{\alpha_{\ell(w)-1}}) + 1 && \text{(by Lemma 47(i),(ii))} \\ &\leq \ell(w) && \text{(by (75)).} \end{aligned}$$

$\square$

June 13, 2016

Lemma 50. *With reference to Definition 6, if $a, b, x, y \in F(X)$ and $xN = yN$, then $axbN = aybN$.*

Proof.

$$\begin{aligned} xN = yN &\implies x^{-1}y \in N \\ &\implies b^{-1}x^{-1}yb \in N \\ &\implies xbN = ybN \\ &\implies axbN = aybN. \end{aligned}$$

□

Lemma 51. *With reference to Definition 6, suppose $t_1, \dots, t_r \in X$. If there exist i, j with $1 \le i < j \le r$ such that*

$$t_i \cdots t_{j-1} t_j t_{j-1} \cdots t_{i+1} \in N,$$

then

$$t_1 \cdots t_r N = t_1 \cdots \hat{t}_i \cdots \hat{t}_j \cdots t_r N,$$

where the hat denotes omission.

Proof. Setting $a = t_1 \cdots t_i$, $b = t_{i+1} \cdots t_r$, $x = 1$ and $y = t_i \cdots t_{j-1} t_j t_{j-1} \cdots t_{i+1}$ in Lemma 50 gives the result. □

Theorem 52. *Let Δ be a simple system in a root system Φ. For $\alpha, \beta \in \Delta$, let $m(\alpha, \beta)$ denote the order of $s_\alpha s_\beta$, that is, the least positive integer k such that $(s_\alpha s_\beta)^k = 1$ holds. Then the group $W = W(\Phi)$ has presentation $\langle X \mid R \rangle$, where*

$$\begin{aligned} X &= \{t_\alpha \mid \alpha \in \Delta\} \quad \textit{(a set of formal symbols),} \\ R &= \{(t_\alpha t_\beta)^{m(\alpha,\beta)} \mid \alpha, \beta \in \Delta,\ \alpha \ne \beta\}. \end{aligned}$$

Proof. As in Definition 6, let $F(X)$ denote the free group generated by the set of involutions X. Let N be the subgroup generated by the set

$$\{c^{-1} r^{\pm 1} c \mid c \in F(X),\ r \in R\}. \tag{76}$$

We need to show that W is isomorphic to $F(X)/N$.

Clearly, there is a homomorphism from $F(X)$ to W mapping t_α to s_α for all $\alpha \in \Delta$. By Theorem 41, this homomorphism is surjective. Moreover, since the set (76) is mapped to 1 by this homomorphism, there exists a surjective homomorphism $f : F(X)/N \to W$ satisfying $f(t_\alpha N) = s_\alpha$ for all $\alpha \in \Delta$. We need to show that f is injective. This will follow if

$$t_1, \dots, t_r \in T,\ f(t_1 \cdots t_r N) = 1 \implies t_1 \cdots t_r \in N. \tag{77}$$

We prove this by induction on r. First we note that r is even. Indeed, $f(t_1 \cdots t_r N) = 1$ implies

$$s_1 \cdots s_r = 1, \tag{78}$$

where $s_i = f(t_i N) \in \{s_\alpha \mid \alpha \in \Delta\}$ is a reflection. Thus $\det s_i = -1$, so $(-1)^r = 1$. This implies that r is even. Clearly, (77) holds for $r = 0$. Also, if $r = 2$, then $s_1 s_2 = 1$. This implies $s_1 = s_2$, so $t_1 = t_2$. Thus $t_1 t_2 = 1 \in N$.

Now assume $r = 2q$, where $q \geq 2$. We first prove the special case where

$$t_1 = t_3 = \cdots = t_{2q-1},\ t_2 = t_4 = \cdots = t_{2q}. \tag{79}$$

In this case, let $t_1 = t_\alpha$ and $t_2 = t_\beta$. then (78) implies $(s_\alpha s_\beta)^q = 1$, which in turn implies $m(\alpha, \beta) \mid q$. Thus

$$t_1 \cdots t_{2q} = ((t_\alpha t_\beta)^{m(\alpha,\beta)})^{q/m(\alpha,\beta)} \in N.$$

Next we prove another special case where

$$1 \leq \exists i < \exists j \leq 2q,\ j - i < q,\ s_1 \cdots \hat{s}_i \cdots \hat{s}_j \cdots s_{2q} = 1. \tag{80}$$

Indeed, comparing this with (78) yields

$$s_i \cdots s_j = s_{i+1} \cdots s_{j-1},$$

or equivalently,

$$f(t_i \cdots t_{j-1} t_j t_{j-1} \cdots t_{i+1} N) = 1.$$

Since $j - i < q$, we can apply the inductive hypothesis to conclude

$$t_i \cdots t_{j-1} t_j t_{j-1} \cdots t_{i+1} \in N.$$

Using Lemma 51, we obtain

$$t_1 \cdots t_{2q} N = t_1 \cdots \hat{t}_i \cdots \hat{t}_j \cdots t_{2q} N. \tag{81}$$

Together with the assumption of (77), we obtain

$$f(t_1 \cdots \hat{t}_i \cdots \hat{t}_j \cdots t_{2q} N) = 1,$$

which, by the inductive hypothesis, shows

$$t_1 \cdots \hat{t}_i \cdots \hat{t}_j \cdots t_{2q} \in N.$$

The result then follows from (81).

Before proceeding to the general case, observe

$$\begin{aligned} s_1 \cdots s_r = 1 &\iff s_i \cdots s_r s_1 \cdots s_{i-1} = 1, \\ t_1 \cdots t_r \in N &\iff t_i \cdots t_r t_1 \cdots t_{i-1} \in N. \end{aligned}$$

Define $s_{r+i} = s_i$ for $1 \leq i \leq r$ and $t_{r+i} = t_i$ for $1 \leq i \leq r$. Then the second special case treated above actually takes care of the case:

$$1 \leq \exists i < \exists j \leq 4q,\ j - i < q,\ s_i \cdots s_j = s_{i+1} \cdots s_{j-1}. \tag{82}$$

Also, since the first special case has already been established, we may assume that there exists i with $1 \leq i \leq 2q$ such that $t_i \neq t_{i+2}$. Without loss of generality, we may assume $t_1 \neq t_3$, so

$$s_1 \neq s_3. \tag{83}$$

Since

$$s_k s_{k+1} \cdots s_{k+q} = s_{k+2q-1} s_{k+2q-2} \cdots s_{k+q+1} \quad (1 \leq k \leq 2q),$$

we have

$$\ell(s_k s_{k+1} \cdots s_{k+q}) \leq q - 1 < q + 1.$$

Theorem 48(iii) implies that there exist i, j with $k \leq i < j \leq k + q$ such that

$$s_k s_{k+1} \cdots s_{k+q} = s_k \cdots \hat{s}_i \cdots \hat{s}_j \cdots s_{k+q},$$

or equivalently,

$$s_i \cdots s_j = s_{i+1} \cdots s_{j-1}.$$

Since the second special case includes (82), we may assume $k = i$ and $j = k + q$, that is,

$$s_k s_{k+1} \cdots s_{k+q} = s_{k+1} \cdots s_{k+q-1} \quad (1 \leq k \leq 2q).$$

In particular, as $q \geq 2$,

$$\begin{aligned} s_1 s_2 \cdots s_{q+1} &= s_2 \cdots s_q, \qquad (84)\\ s_2 s_3 \cdots s_{q+2} &= s_3 \cdots s_{q+1},\\ s_3 s_4 \cdots s_{q+3} &= s_4 \cdots s_{q+2}, \end{aligned}$$

or equivalently,

$$\begin{aligned} s_1 s_2 \cdots s_q &= s_2 \cdots s_{q+1},\\ s_2 s_3 \cdots s_{q+1} &= s_3 \cdots s_{q+2}, \qquad (85)\\ s_3 s_4 \cdots s_{q+2} &= s_4 \cdots s_{q+3}. \qquad (86) \end{aligned}$$

By (85), we have

$$s_3 (s_2 \cdots s_{q+1})(s_{q+2} \cdots s_4) = 1. \tag{87}$$

In particular,

$$\ell(s_3 (s_2 \cdots s_{q+1})) \leq q - 1 < q + 1.$$

If

$$s_3 (s_2 \cdots s_{q+1}) = s_2 \cdots s_q, \tag{88}$$

then (84) implies $s_1 = s_3$, contradicting (83). Thus $s_3(s_2 \cdots s_{q+1}) \neq s_2 \cdots s_q$, and hence Theorem 48(iii) implies that we are in the second special case for the relation (87), and hence

$$t_3(t_2 \cdots t_{q+1})(t_{q+2} \cdots t_4) \in N.$$

This implies

$$t_2 \cdots t_{q+1} t_{q+2} t_{q+1} \cdots t_3 \in N.$$

By Lemma 51, we obtain

$$t_1 \cdots t_{2q} N = t_1 \hat{t}_2 \cdots \hat{t}_{q+2} \cdots t_{2q} N. \tag{89}$$

Together with the assumption of (77), we obtain

$$f(t_1 \hat{t}_2 \cdots \hat{t}_{q+2} \cdots t_{2q} N) = 1,$$

which, by the inductive hypothesis, shows

$$t_1 \hat{t}_2 \cdots \hat{t}_{q+2} \cdots t_{2q} \in N.$$

The result then follows from (89). □

June 20, 2016

Definition 53. Let G be a group acting on a set Ω. We say that G acts *simply transitively* on Ω if

(i) G acts transitively on Ω,

(ii) for every pair α, β of elements in Ω, there exists a unique element $g \in G$ such that $g.\alpha = \beta$.

Lemma 54. *Let G be a finite group acting transitively on a set Ω. Let G_α denote the stabilizer of α in G, that is,*

$$G_\alpha = \{g \in G \mid g.\alpha = \alpha\}.$$

Then the following are equivalent:

(i) *G acts simply transitively on Ω,*

(ii) *for every $\alpha \in \Omega$, $G_\alpha = \{1\}$,*

(iii) *for some $\alpha \in \Omega$, $G_\alpha = \{1\}$,*

(iv) $|G| = |\Omega|$.

Proof. (i) $\Longrightarrow$ (ii): Immediate from Definition 53(ii) by setting $\alpha = \beta$.

(ii) $\Longrightarrow$ (iii): Trivial.

(iii) $\Longrightarrow$ (iv): The mapping $\phi : G \to \Omega$ defined by $g \mapsto g.\alpha$ is a bijection. Indeed, ϕ is surjective since G is transitive. If $\phi(g) = \phi(h)$, then $g.\alpha = h.\alpha$, hence $g^{-1}h \in G_\alpha = \{1\}$. This implies $g = h$. Thus ϕ is injective.

(iv) $\Longrightarrow$ (i): Let $\alpha \in \Omega$. Then

$$\begin{aligned}
|G| &= |\Omega| \\
&= \sum_{\beta \in \Omega} 1 \\
&\leq \sum_{\beta \in \Omega} |\{g \in G \mid g.\alpha = \beta\}| \\
&= |\bigcup_{\beta \in \Omega} \{g \in G \mid g.\alpha = \beta\}| \\
&= |\{g \in G \mid g.\alpha \in \Omega\}| \\
&= |G|.
\end{aligned}$$

This forces

$$|\{g \in G \mid g.\alpha = \beta\}| = 1 \quad (\forall \beta \in \Omega).$$

Since $\alpha \in \Omega$ was arbitrary, we obtain (i). □

For the remainder of today's lecture, we let Φ be a root system.

Theorem 55. *The group $W(\Phi)$ acts simply transitively on $\mathcal{P}(\Phi)$ and $\mathcal{S}(\Phi)$.*

Proof. By Theorem 36, $W(\Phi)$ acts transitively on $\mathcal{P}(\Phi)$ and $\mathcal{S}(\Phi)$. Let $w \in W(\Phi)$ and $\Pi \in \mathcal{P}(\Phi)$, and suppose $w\Pi = \Pi$. Let Δ be the unique simple system contained in Π. Then by Corollary 49 and Notation 45,

$$\begin{aligned}\ell(w) &= n(w)\\ &= |\Pi \cap w^{-1}(-\Pi)|\\ &= |\Pi \cap (-w^{-1}\Pi)|\\ &= |\Pi \cap (-\Pi)|\\ &= |\emptyset|\\ &= 0.\end{aligned}$$

Thus $w = 1$. Therefore, $W(\Phi)$ acts simply transitively on $\mathcal{P}(\Phi)$.

Next suppose $w\Delta = \Delta$. Then by Lemma 33(i), we obtain $w\Pi = \Pi$, and hence $w = 1$. Therefore, $W(\Phi)$ acts simply transitively on $\mathcal{S}(\Phi)$. □

In what follows, we fix a simple system $\Delta \in \mathcal{S}(\Phi)$. Let $\Pi = \Phi \cap \mathbf{R}_{\geq 0}\Delta$ be the unique positive system in Φ containing Δ.

Notation 56. Let $S = \{s_\alpha \mid \alpha \in \Delta\}$. For $I \subset S$, we define

$$\begin{aligned}W_I &= \langle I \rangle,\\ \Delta_I &= \{\alpha \in \Delta \mid s_\alpha \in I\},\\ V_I &= \mathbf{R}\Delta_I,\\ \Phi_I &= \Phi \cap V_I,\\ \Pi_I &= \Pi \cap V_I.\end{aligned}$$

Lemma 57. *For $w \in \langle s_\alpha \mid \alpha \in \Phi_I \rangle$, we have*

(i) $wV_I = V_I$,

(ii) $w(\Pi \setminus \Pi_I) = \Pi \setminus \Pi_I$.

Proof. It suffices to show (i) and (ii) for $w = s_\alpha$ with $\alpha \in \Phi_I$. Let $\alpha \in \Phi_I$.

(i) For $\beta \in \Delta_I \subset V_I$, $s_\alpha\beta \in \mathbf{R}\alpha + \mathbf{R}\beta \subset V_I$. Thus $s_\alpha\Delta_I \subset V_I$, and this implies $s_\alpha V_I = V_I$.

(ii) Let $\beta \in \Pi \setminus \Pi_I$. Then $\beta \notin V_I = \mathbf{R}\Delta_I$, so there exists $\gamma \in \Delta \setminus \Delta_I$ such that

$$\beta \in \mathbf{R}_{>0}\gamma + \mathbf{R}_{\geq 0}\Delta.$$

Since $\alpha \in \Phi_I \subset V_I = \mathbf{R}\Delta_I$, we have

$$\begin{aligned} s_\alpha\beta &= \beta - \frac{2(\beta,\alpha)}{(\alpha,\alpha)}\alpha \\ &\in \mathbf{R}_{>0}\gamma + \mathbf{R}_{\geq 0}\Delta + \mathbf{R}\alpha \\ &\subset \mathbf{R}_{>0}\gamma + \mathbf{R}_{\geq 0}\Delta + \mathbf{R}\Delta_I. \end{aligned}$$

Since $\gamma \notin \Delta_I$, the coefficient of γ in the expansion of $s_\alpha\beta$ is positive. This implies $s_\alpha\beta \in \Phi \cap \mathbf{R}_{\geq 0}\Delta = \Pi$. Since $\beta \in \Pi \setminus \Pi_I$ was arbitrary, we obtain $s_\alpha(\Pi \setminus \Pi_I) \subset \Pi$. Since

$$\begin{aligned} s_\alpha(\Pi \setminus \Pi_I) \cap V_I &= s_\alpha(\Pi \setminus V_I) \cap V_I \\ &= s_\alpha(\Pi \setminus V_I) \cap s_\alpha V_I && \text{(by (i))} \\ &= s_\alpha((\Pi \setminus V_I) \cap V_I) \\ &= \emptyset, \end{aligned}$$

we have $s_\alpha(\Pi \setminus \Pi_I) \subset \Pi \setminus V_I = \Pi \setminus \Pi_I$. Since s_α is a bijection, we conclude $s_\alpha(\Pi \setminus \Pi_I) = \Pi \setminus \Pi_I$. □

Proposition 58. *Let $I \subset S$.*

(i) *Φ_I is a root system with simple system Δ_I.*

(ii) *Π_I is the unique positive system of Φ_I containing the simple system Δ_I.*

(iii) *$W(\Phi_I) = W_I$.*

(iv) *Let ℓ be the length function of W with respect to Δ. Then the restriction of ℓ to W_I coincides with the length function ℓ_I of W_I with respect to the simple system Δ_I.*

Proof. (i) For $\alpha \in \Phi_I \subset V_I$,

$$\begin{aligned} \mathbf{R}\alpha \cap \Phi_I &= (\mathbf{R}\alpha \cap \Phi) \cap V_I \\ &= \{\alpha, -\alpha\} \cap V_I \\ &= \{\alpha, -\alpha\}. \end{aligned}$$

Since

$$\begin{aligned} s_\alpha\Phi_I &= s_\alpha\Phi \cap s_\alpha V_I \\ &= \Phi \cap V_I && \text{(by Lemma 57(i))} \\ &= \Phi_I. \end{aligned}$$

we see that Φ_I is a root system. Since Δ is linearly independent, so is Δ_I. Since

$$\begin{aligned} \Phi_I &= \Phi \cap V_I \\ &\subset (\mathbf{R}_{\geq 0}\Delta \cup \mathbf{R}_{\leq 0}\Delta) \cap \mathbf{R}\Delta_I \end{aligned}$$

$$
\begin{aligned}
&= (\mathbf{R}_{\geq 0}\Delta \cap \mathbf{R}\Delta_I) \cup (\mathbf{R}_{\leq 0}\Delta \cap \mathbf{R}\Delta_I) \\
&= (\mathbf{R}_{\geq 0}\Delta_I) \cup (\mathbf{R}_{\leq 0}\Delta_I),
\end{aligned}
$$

we see that Δ_I is a simple system in Φ_I.

(ii) Since

$$
\begin{aligned}
\Pi_I &= \Pi \cap V_I \\
&= \Phi \cap \mathbf{R}_{\geq 0}\Delta \cap V_I \\
&= \Phi \cap V_I \cap \mathbf{R}_{\geq 0}\Delta \cap \mathbf{R}\Delta_I \\
&= \Phi_I \cap \mathbf{R}_{\geq 0}\Delta_I,
\end{aligned}
$$

the result follows from Lemma 29(i).

(iii)

$$
\begin{aligned}
W(\Phi_I) &= \langle s_\alpha \mid \alpha \in \Delta_I \rangle && \text{(by Theorem 41)} \\
&= \langle I \rangle \\
&= W_I.
\end{aligned}
$$

(iv) Let $w \in W_I = W(\Phi)$. Then by Lemma 57(i), we have

$$
w\Phi_I = \Phi_I. \tag{90}
$$

and by Lemma 57(ii), we have $w(\Pi \setminus \Pi_I) = \Pi \setminus \Pi_I \subset \Pi$. This implies $w(\Pi \setminus \Pi_I) \cap (-\Pi) = \emptyset$. Thus

$$
\begin{aligned}
w\Pi \cap (-\Pi) &= w(\Pi_I \cup (\Pi \setminus \Pi_I)) \cap (-\Pi) \\
&= (w\Pi_I \cup w(\Pi \setminus \Pi_I)) \cap (-\Pi) \\
&= (w(\Pi_I) \cap (-\Pi)) \cup (w(\Pi \setminus \Pi_I) \cap (-\Pi)) \\
&= w(\Pi_I) \cap (-\Pi) \\
&= w(\Pi \cap V_I) \cap (-\Pi) \\
&= w\Pi \cap wV_I \cap V_I \cap (-\Pi) \\
&= w(\Pi \cap V_I) \cap (-\Pi \cap V_I) \\
&= w(\Pi_I) \cap (-\Pi_I) && \text{(by (90)).}
\end{aligned} \tag{91}
$$

Therefore,

$$
\begin{aligned}
\ell(w) &= |\Pi \cap w^{-1}(-\Pi)| && \text{(by Corollary 49)} \\
&= |w\Pi \cap (-\Pi)| \\
&= |w(\Pi_I) \cap (-\Pi_I)| && \text{(by (91))} \\
&= |\Pi_I \cap w^{-1}(-\Pi_I)| \\
&= \ell_I(w) && \text{(by Corollary 49).}
\end{aligned}
$$

□

June 27, 2016

For today's lecture, we let V be a finite-dimensional vector space over $\mathbf{R}$, with positive-definite inner product. Let Φ be a root system in V with simple system Δ. Let $W = W(\Phi) = \langle s_\alpha \mid \alpha \in \Phi \rangle$. Recall Notation 56.

Lemma 59. *Let $I \subset S$. If $u \in W$ satisfies*

$$\ell(u) = \min\{\ell(x) \mid x \in uW_I\},$$

then

$$\ell(uv) = \ell(u) + \ell(v) \quad (\forall v \in W_I).$$

Proof. Let $q = \ell(u)$. Then there exist $s_1, \dots, s_q \in S$ such that

$$u = s_1 \cdots s_q.$$

Let $v \in W_I$. Then by Proposition 58(iv), we have $\ell(v) = \ell_I(v)$. This implies that there exist $s_{q+1}, \dots, s_{q+r} \in I$ such that

$$v = s_{q+1} \cdots s_{q+r},$$

where $r = \ell(v)$. Then $uv = s_1 \cdots s_{q+r}$, hence $\ell(uv) \leq q + r$.

Suppose $\ell(w) < q + r$. Then by Theorem 48, there exist i, j with $1 \leq i < j \leq q + r$ such that

$$uv = s_1 \cdots \hat{s}_i \cdots \hat{s}_j \cdots s_{q+r}.$$

If $i < j \leq q$, then

$$uv = s_1 \cdots \hat{s}_i \cdots \hat{s}_j \cdots s_q v,$$

hence $u = s_1 \cdots \hat{s}_i \cdots \hat{s}_j \cdots s_q$, contradicting $\ell(u) = q$. Similarly, if $q + 1 \leq i < j$, then

$$uv = us_{q+1} \cdots \hat{s}_i \cdots \hat{s}_j \cdots s_{q+r},$$

hence $v = s_{q+1} \cdots \hat{s}_i \cdots \hat{s}_j \cdots s_{q+r}$, contradicting $\ell(v) = r$. Thus

$$1 \leq i \leq q < j \leq q + r.$$

Setting

$$\begin{aligned} u' &= s_1 \cdots \hat{s}_i \cdots s_q, \\ v' &= s_{q+1} \cdots \hat{s}_j \cdots s_{q+r} \in W_I, \end{aligned}$$

we have $u'v' = uv$, and hence $u' = uvv'^{-1} \in uW_I$. But $\ell(u') < q = \ell(u)$, contrary to the minimality of $\ell(u)$. Therefore, we conclude $\ell(w) = q + r = \ell(u) + \ell(v)$. $\square$

Notation 60. For $I \subset S$, we define

$$W^I = \{w \in W \mid \ell(ws) > \ell(w) \text{ for all } s \in I\}.$$

Lemma 61. *Let $I \subset S$ and $w \in W$. If $u_0 \in wW_I$ satisfies*

$$\ell(u_0) = \min\{\ell(x) \mid x \in wW_I\},$$

and $u_1 \in W^I \cap wW_I$, then $u_0 = u_1$. In particular,

(i) *$W^I \cap wW_I$ consists of a single element,*

(ii) *$\min\{\ell(x) \mid x \in wW_I\}$ is achieved by a unique element,*

and the elements described in (i) *and* (ii) *coincide.*

Proof. Since $u_1 \in wW_I = u_0W_I$, there exists $v \in W_I$ such that $u_1 = u_0v$. Suppose $v \neq 1$. Then there exists $s \in I$ such that $\ell(vs) < \ell(v)$. This implies

$$\begin{aligned}
\ell(u_1s) &= \ell(u_0vs) \\
&= \ell(u_0) + \ell(vs) && \text{(by Lemma 59)} \\
&< \ell(u_0) + \ell(v) \\
&= \ell(u_0v) && \text{(by Lemma 59)} \\
&= \ell(u_1).
\end{aligned}$$

This contradicts $u_1 \in W^I$. Thus, we conclude $v = 1$, or equivalently, $u_1 = u_0$. The rest of the statements are immediate. □

Lemma 62. *Let $I \subset S$. The mapping $\phi : W^I \times W_I \to W$ defined by $\phi(u, v) = uv$ is a bijection, and it satisfies*

$$\ell(\phi(u, v)) = \ell(u) + \ell(v) \quad (u \in W^I,\ v \in W_I).$$

Proof. Let $w \in W$. Choose $u_0 = u_1 \in W^I \cap wW_I$ as in Lemma 61. Then there exists $v \in W_I$ such that $u_0 = wv$. Then $w = \phi(u_0, v^{-1})$. Thus ϕ is surjective.

Suppose $(u, v), (u', v') \in W^I \times W_I$ and $\phi(u, v) = \phi(u', v')$. Then $uv = u'v'$. Thus $u, u' \in W^I \cap uW_I$, which forces $u = u'$ by Lemma 61(i). Then we also have $v = v'$. Thus ϕ is injective.

Finally, for $u \in W^I$, we have $u \in W^I \cap uW_I$, so Lemma 61 implies $\ell(u) = \min\{\ell(x) \mid x \in uW_I\}$. Then by Lemma 59, we have $\ell(uv) = \ell(u) + \ell(v)$ for all $v \in W_I$. □

Notation 63. Let t be an indeterminate over $\mathbf{Q}$, or in other words, consider the polynomial ring $\mathbf{Q}[t]$ (or its field of fractions $\mathbf{Q}(t)$). For a subset X of W, write

$$X(t) = \sum_{w \in X} t^{\ell(w)}.$$

Definition 64. The *Poincaré polynomial* $W(t)$ of W is defined as

$$W(t) = \sum_{w \in W} t^{\ell(w)}.$$

We remark that $W(t)$ is independent of the choice of a simple system, even though the length function ℓ does depend on it. Indeed, let Δ' be another simple system. Then there exists $z \in W$ such that $\Delta' = z\Delta$ by Theorem 36. Let

$$\begin{aligned} S &= \{s_\alpha \mid \alpha \in \Delta\}, \\ S' &= \{s_\alpha \mid \alpha \in \Delta'\}. \end{aligned}$$

Then

$$\begin{aligned} zSz^{-1} &= \{zs_\alpha z^{-1} \mid \alpha \in \Delta\} \\ &= \{s_{z\alpha} \mid \alpha \in \Delta\} && \text{(by Lemma 12)} \\ &= \{s_\alpha \mid \alpha \in z\Delta\} \\ &= \{s_\alpha \mid \alpha \in \Delta'\} \\ &= S'. \end{aligned}$$

If we denote by the length function with respect to Δ and Δ' by ℓ_Δ and $\ell_{\Delta'}$, respectively, then $\ell_\Delta(w) = \ell_{\Delta'}(zwz^{-1})$ for all $w \in W$. Thus

$$\sum_{w \in W} t^{\ell_\Delta(w)} = \sum_{w \in W} t^{\ell_{\Delta'}(zwz^{-1})} = \sum_{w \in W} t^{\ell_{\Delta'}(w)}.$$

Lemma 65. *For $I \subset S$,*

$$W(t) = W^I(t) W_I(t).$$

Proof. By Lemma 62,

$$\begin{aligned} W(t) &= \sum_{w \in W} t^{\ell(w)} \\ &= \sum_{(u,v) \in W^I \times W_I} t^{\ell(\phi(u,v))} \\ &= \sum_{u \in W^I} \sum_{v \in W_I} t^{\ell(u) + \ell(v)} \\ &= \sum_{u \in W^I} t^{\ell(u)} \sum_{v \in W_I} t^{\ell(v)} \\ &= W^I(t) W_I(t). \end{aligned}$$

□

Lemma 66. *Let Π be the unique positive system containing Δ. For $w \in W$, set*

$$K(w) = \{s \in S \mid \ell(ws) > \ell(w)\}.$$

Then the following are equivalent:

(i) $K(w) = \emptyset$,

(ii) $w\Pi = -\Pi$,

(iii) $\ell(w) = |\Pi|$.

Moreover, there exists a unique $w \in W$ satisfying these conditions.

Proof. Equivalence of (ii) and (iii) follows from Corollary 49.

$$\begin{aligned} \text{(i)} &\iff \ell(ws) < \ell(w) \quad (\forall s \in S) \\ &\iff w\Delta \subset -\Pi && \text{(by Lemma 47)} \\ &\iff w\Pi \subset -\Pi \\ &\iff \text{(ii)}. \end{aligned}$$

The uniqueness of w follows from Theorem 55. $\square$

Proposition 67. *Then*

$$\sum_{I \subset S} (-1)^{|I|} \frac{W(t)}{W_I(t)} = \sum_{I \subset S} (-1)^{|I|} W^I(t) = t^{|\Pi|}.$$

Proof. The first equality follows immediately from Lemma 65. For $I \subset S$, we have

$$w \in W^I \iff K(w) \supset I.$$

Thus

$$\begin{aligned} \sum_{I \subset S} (-1)^{|I|} W^I(t) &= \sum_{I \subset S} (-1)^{|I|} \sum_{w \in W^I} t^{\ell(w)} \\ &= \sum_{w \in W} \sum_{\substack{I \subset S \\ w \in W^I}} (-1)^{|I|} t^{\ell(w)} \\ &= \sum_{w \in W} \sum_{I \subset K(w)} (-1)^{|I|} t^{\ell(w)} \\ &= \sum_{w \in W} t^{\ell(w)} \sum_{i=0}^{|K(w)|} \sum_{\substack{I \subset K(w) \\ |I| = i}} (-1)^i \\ &= \sum_{w \in W} t^{\ell(w)} \sum_{i=0}^{|K(w)|} (-1)^i \binom{|K(w)|}{i} \\ &= \sum_{\substack{w \in W \\ |K(w)| = 0}} t^{\ell(w)} + \sum_{\substack{w \in W \\ |K(w)| \geq 1}} t^{\ell(w)} (1 + (-1))^{|K(w)|} \\ &= \sum_{\substack{w \in W \\ K(w) = \emptyset}} t^{\ell(w)} \\ &= t^{|\Pi|} \end{aligned}$$

by Lemma 66. $\square$

July 4, 2016

For today's lecture, we let V be a finite-dimensional vector space over $\mathbf{R}$, with positive-definite inner product. Let Φ be a root system in V with simple system Δ, and let $W = W(\Phi) = \langle s_\alpha \mid \alpha \in \Phi \rangle$. Let $\Pi = \Phi \cap \mathbf{R}_{\geq 0}\Delta$ be the unique positive system in Φ containing Δ.

Recall Notation 56 and Proposition 67:

$$\sum_{I \subsetneqq S} \frac{(-1)^{|I|}}{W_I(t)} = \frac{t^{|\Pi|} - (-1)^{|S|}}{W(t)}. \tag{92}$$

Continuing Example 16 with $n = 4$, write $W = G_4$, $s_i = s_{\varepsilon_i - \varepsilon_{i+1}}$ for $i = 1, 2, 3$, so that $S = \{s_1, s_2, s_3\}$. Then

$$\begin{aligned} W_\emptyset(t) &= 1, \\ W_{\{s_i\}}(t) &= t + 1, \\ W_{\{s_1, s_2\}}(t) &= (t+1)(t^2 + t + 1). \end{aligned}$$

If we compute $W_I(t)$ for all $I \subsetneqq S$, then (92) can be used to determine $W(t)$ and, in particular, $|W|$.

Define

$$\begin{aligned} C &= \{\lambda \in V \mid (\lambda, \alpha) > 0 \ (\forall \alpha \in \Delta)\}, \\ D &= \{\lambda \in V \mid (\lambda, \alpha) \geq 0 \ (\forall \alpha \in \Delta)\}. \end{aligned}$$

Lemma 68. *For each $\lambda \in V$, there exist $w \in W$ such that $w\lambda \in D$. Moreover, in this case, $w\lambda - \lambda \in \mathbf{R}_{\geq 0}\Delta$.*

Proof. Let $\lambda \in V$. Define a partial order on the set $W\lambda = \{w\lambda \mid w \in W\}$ by setting

$$\mu \preceq \mu' \iff \mu' - \mu \in \mathbf{R}_{\geq 0}\Delta \quad (\mu, \mu' \in W\lambda).$$

Since $W\lambda$ is finite, so is its subset

$$M = \{\mu \in W\lambda \mid \lambda \preceq \mu\}.$$

The set M is non-empty since $\lambda \in M$. Thus, there exists a maximal element μ in M. Since $\mu = w\lambda$ for some $w \in W$ and $\mu - \lambda \in \mathbf{R}_{\geq 0}\Delta$, it remains to show $\mu \in D$.

Suppose, to the contrary, $\mu \notin D$. Then there exists $\alpha \in \Delta$ such that $(\mu, \alpha) < 0$. By the definition of a reflection, we have $s_\alpha\mu - \mu \in \mathbf{R}_{>0}\alpha \subset \mathbf{R}_{\geq 0}\Delta$, so $\mu \preceq s_\alpha\mu$ and $\mu \neq s_\alpha\mu$. Since $\lambda \preceq \mu$, we have $\lambda \preceq s_\alpha\mu$. Moreover, $s_\alpha\mu = s_\alpha w\lambda \in W\lambda$. Therefore, $s_\alpha\mu \in M$, and this contradicts maximality of μ in M. $\square$

Notation 69. For a subset U of V, define

$$\mathrm{Stab}_W(U) = \{w \in W \mid w\lambda = \lambda \ (\forall \lambda \in U)\}.$$

Lemma 70. (i) *If $\lambda \in D$, then*

$$\mathrm{Stab}_W(\{\lambda\}) = \langle s_\alpha \mid \alpha \in \Delta,\ s_\alpha\lambda = \lambda\rangle.$$

(ii) *If $\lambda, \mu \in D$, $w \in W$ and $w\lambda = \mu$, then $\lambda = \mu$.*

(iii) *If $\lambda \in C$, then* $\mathrm{Stab}_W(\{\lambda\}) = \{1\}$.

(iv) *If $\lambda \in V$, then*

$$\mathrm{Stab}_W(\{\lambda\}) = \langle s_\alpha \mid \alpha \in \Phi,\ s_\alpha\lambda = \lambda\rangle.$$

Proof. First we prove, for $w \in W$,

$$\lambda, \mu \in D,\ w\lambda = \mu \implies \lambda = \mu,\ w \in \langle s_\alpha \mid \alpha \in \Delta,\ s_\alpha\lambda = \lambda\rangle, \tag{93}$$
$$\lambda \in C,\ \mu \in D,\ w\lambda = \mu \implies w = 1 \tag{94}$$

by induction on $n(w) = |w\Pi \cap (-\Pi)|$. If $n(w) = 0$, then $\ell(w) = 0$ by Corollary 49, hence $w = 1$. Then (93) and (94) hold. Suppose $n(w) > 0$. Then there exists $\beta \in \Pi$ such that $w\beta \in -\Pi$. Since $\Pi \subset \mathbf{R}_{\geq 0}\Delta$, this implies $w\mathbf{R}_{\geq 0}\Delta \cap \mathbf{R}_{\leq 0}\Delta \supsetneqq \{0\}$, which in turn implies $w\Delta \cap (-\Pi) \neq \emptyset$. Suppose $w\gamma \in -\Pi$, where $\gamma \in \Delta$. Then by Lemma 47,

$$\begin{aligned} \ell(ws_\gamma) &= \ell(w) - 1 \\ &= n(w) - 1 && \text{(by Corollary 49)} \\ &< n(w). \end{aligned} \tag{95}$$

Since $\mu \in D$ and $-w\gamma \in \Pi \subset \mathbf{R}_{\geq 0}\Delta$, we have

$$\begin{aligned} 0 &\leq (\mu, -w\gamma) \\ &= -(w^{-1}\mu, \gamma) \\ &= -(\lambda, \gamma). \end{aligned}$$

If $\lambda \in C$, this is impossible. This implies that (94) holds. If $\lambda \in D$, then this forces $(\lambda, \gamma) = 0$, implying $s_\gamma \in \mathrm{Stab}_W(\{\lambda\})$. Now, we have $ws_\gamma\lambda = \mu$ and (95), so we can apply inductive hypothesis to conclude $\lambda = \mu$ and

$$ws_\gamma \in \langle s_\alpha \mid \alpha \in \Delta,\ s_\alpha\lambda = \lambda\rangle.$$

Thus (93) holds.

Now (ii) follows from (93), while (i) and (iii) follow from (93) and (94), respectively, by setting $\lambda = \mu$.

Finally we prove (iv). Let $\lambda \in V$. Clearly,

$$\mathrm{Stab}_W(\{\lambda\}) \supset \langle s_\alpha \mid \alpha \in \Phi,\ s_\alpha\lambda = \lambda\rangle.$$

To prove the reverse containment, observe that, by Lemma 68, there exists $z \in W$ such that $z\lambda \in D$. Then

$$\mathrm{Stab}_W(\{\lambda\}) = \{w \in W \mid w\lambda = \lambda\}$$

$$
\begin{aligned}
&= \{w \in W \mid zwz^{-1}z\lambda = z\lambda\} \\
&= \{z^{-1}xz \in W \mid xz\lambda = z\lambda\} \\
&= z^{-1}\,\mathrm{Stab}_W(\{z\lambda\})z \\
&= z^{-1}\langle s_\beta \mid \beta \in \Delta,\ s_\beta z\lambda = z\lambda\rangle z && \text{(by (i))} \\
&= \langle z^{-1}s_\beta z \mid \beta \in \Delta,\ z^{-1}s_\beta z\lambda = \lambda\rangle \\
&= \langle s_{z^{-1}\beta} \mid \beta \in \Delta,\ s_{z^{-1}\beta}\lambda = \lambda\rangle && \text{(by Lemma 12)} \\
&\subset \langle s_\alpha \mid \alpha \in \Phi,\ s_\alpha\lambda = \lambda\rangle.
\end{aligned}
$$

□

The following property of the set D is referred to as D being a *fundamental domain* for the action of W on V.

Theorem 71. *For each* $\lambda \in V$*,* $|W\lambda \cap D| = 1$.

Proof. By Lemma 68, we have $W\lambda \cap D \neq \emptyset$. Suppose $\mu, \mu' \in W\lambda \cap D$. Then Lemma 70(ii) implies $\mu = \mu'$. □

July 11, 2016

For today's lecture, we let V be a finite-dimensional vector space over $\mathbf{R}$, with positive-definite inner product. Let Φ be a root system in V with simple system Δ, and let $W = W(\Phi) = \langle s_\alpha \mid \alpha \in \Phi \rangle$.

Notation 72. Let $\alpha \in \Phi$. We define

$$\begin{aligned} H_\alpha &= \{\lambda \in V \mid (\alpha, \lambda) = 0\}, \\ H_\alpha^+ &= \{\lambda \in V \mid (\alpha, \lambda) > 0\}, \\ H_\alpha^- &= \{\lambda \in V \mid (\alpha, \lambda) < 0\}, \end{aligned}$$

so that $V = H_\alpha^+ \cup H_\alpha \cup H_\alpha^-$ (disjoint).

Recall

$$\begin{aligned} C &= \bigcap_{\alpha \in \Delta} H_\alpha^+, \\ D &= \bigcap_{\alpha \in \Delta} (H_\alpha^+ \cup H_\alpha). \end{aligned}$$

Lemma 73. *For $w \in W$ and $\alpha \in \Phi$,*

$$wH_\alpha = H_{w\alpha}, \tag{96}$$

$$wH_\alpha^\pm = H_{w\alpha}^\pm. \tag{97}$$

In particular,

$$s_\alpha H_\alpha^\pm = H_\alpha^\mp, \tag{98}$$

$$\bigcup_{\alpha \in \Phi} H_\alpha = w \bigcup_{\alpha \in \Phi} H_\alpha. \tag{99}$$

Proof. Observe

$$\begin{aligned} wH_\alpha &= \{w\lambda \mid \lambda \in V,\ (\alpha, \lambda) = 0\} \\ &= \{\mu \mid \mu \in V,\ (w\alpha, \mu) = 0\} \\ &= H_{w\alpha}. \end{aligned}$$

This proves (96). Replacing "$=$" by "$>$" or "$<$", we obtain (97). Moreover, (97) implies

$$\begin{aligned} s_\alpha H_\alpha^\pm &= H_{s_\alpha \alpha}^\pm \\ &= H_{-\alpha}^\pm \\ &= H_\alpha^\mp, \end{aligned}$$

while (96) implies

$$w \bigcup_{\alpha \in \Phi} H_\alpha = \bigcup_{\alpha \in \Phi} wH_\alpha$$

$$
\begin{aligned}
&= \bigcup_{\alpha\in\Phi} H_{w\alpha} \\
&= \bigcup_{\alpha\in w\Phi} H_{\alpha} \\
&= \bigcup_{\alpha\in\Phi} H_{\alpha}.
\end{aligned}
$$

□

Lemma 74. *If U is a linear subspace of V such that $\Phi \cap U \neq \emptyset$, then $\Phi \cap U$ is a root system.*

Proof. Clearly, $\Phi \cap U$ satisfies (R1) of Definition 14. As for (R2), let $\alpha, \beta \in \Phi \cap U$. Then $s_\alpha\beta \in \Phi \cap (\mathbf{R}\alpha + \mathbf{R}\beta) \subset \Phi \cap U$. Thus $s_\alpha(\Phi \cap U) \subset \Phi \cap U$. This implies $s_\alpha(\Phi \cap U) = \Phi \cap U$. □

Lemma 75. *If U is a linear subspace of V, then*

$$
\mathrm{Stab}_W(U) = \begin{cases} W(\Phi \cap U^\perp) & \text{if } \Phi \cap U^\perp \neq \emptyset, \\ \{1\} & \text{otherwise.} \end{cases}
$$

Proof. We prove the assertion by induction on $\dim U$. The assertion is trivial if $\dim U = 0$. If $\dim U = 1$, then write $U = \mathbf{R}\lambda$. We have

$$
\begin{aligned}
\mathrm{Stab}_W(U) &= \mathrm{Stab}_W(\{\lambda\}) \\
&= \langle s_\alpha \mid \alpha \in \Phi,\ s_\alpha\lambda = \lambda \rangle && \text{(by Lemma 70(iv))} \\
&= \langle s_\alpha \mid \alpha \in \Phi,\ (\alpha, \lambda) = 0 \rangle \\
&= \langle s_\alpha \mid \alpha \in \Phi \cap (\mathbf{R}\lambda)^\perp \rangle \\
&= \begin{cases} W(\Phi \cap U^\perp) & \text{if } \Phi \cap U^\perp \neq \emptyset, \\ \{1\} & \text{otherwise,} \end{cases}
\end{aligned}
$$

since $\Phi \cap U^\perp$ is a root system by Lemma 74 as long as it is nonempty.

Now assume $\dim U \geq 2$. Then there exist nonzero subspaces U_1, U_2 of U such that $U = U_1 \oplus U_2$. Then

$$
\begin{aligned}
U_1^\perp \cap U_2^\perp &= (U_1 \oplus U_2)^\perp \\
&= U^\perp. \qquad (100)
\end{aligned}
$$

Since $\dim U_1, \dim U_2 < \dim U$, the inductive hypothesis implies

$$
\mathrm{Stab}_W(U_i) = \begin{cases} W(\Phi \cap U_i^\perp) & \text{if } \Phi \cap U_i^\perp \neq \emptyset, \\ \{1\} & \text{otherwise} \end{cases}
$$

for $i = 1, 2$. Suppose first that $\Phi \cap U_1^\perp = \emptyset$. Then $\Phi \cap U^\perp = \emptyset$, and

$$\begin{aligned}\mathrm{Stab}_W(U) &\subset \mathrm{Stab}_W(U_1)\\ &= \{1\}.\end{aligned}$$

Next suppose that $\Phi \cap U_1^\perp \neq \emptyset$. Then

$$\begin{aligned}\mathrm{Stab}_W(U) &= \mathrm{Stab}_W(U_1) \cap \mathrm{Stab}_W(U_2)\\ &= W(\Phi \cap U_1^\perp) \cap \mathrm{Stab}_W(U_2)\\ &= \mathrm{Stab}_{W(\Phi\cap U_1^\perp)}(U_2)\\ &= \begin{cases} W(\Phi \cap U_1^\perp \cap U_2^\perp) & \text{if } \Phi \cap U_1^\perp \cap U_2^\perp \neq \emptyset,\\ \{1\} & \text{otherwise}\end{cases}\\ &= \begin{cases} W(\Phi \cap U^\perp) & \text{if } \Phi \cap U^\perp \neq \emptyset,\\ \{1\} & \text{otherwise}\end{cases} & \text{(by (100)).}\end{aligned}$$

□

Proposition 76. *If U is a subset of V, then*

$$\mathrm{Stab}_W(U) = \langle s_\alpha \mid \alpha \in \Phi,\ s_\alpha \in \mathrm{Stab}_W(U)\rangle.$$

Proof. Replacing U by its span, we may assume without loss of generality U is a linear subspace of V. Then by Lemma 75, we have

$$\begin{aligned}\mathrm{Stab}_W(U) &= \begin{cases} W(\Phi \cap U^\perp) & \text{if } \Phi \cap U^\perp \neq \emptyset,\\ \{1\} & \text{otherwise}\end{cases}\\ &= \langle s_\alpha \mid \alpha \in \Phi \cap U^\perp\rangle\\ &= \langle s_\alpha \mid \alpha \in \Phi,\ \forall \lambda \in U,\ (\alpha, \lambda) = 0\rangle\\ &= \langle s_\alpha \mid \alpha \in \Phi,\ \forall \lambda \in U,\ s_\alpha\lambda = \lambda\rangle\\ &= \langle s_\alpha \mid \alpha \in \Phi,\ s_\alpha \in \mathrm{Stab}_W(U)\rangle.\end{aligned}$$

□

Definition 77. The members of the family

$$\{wC \mid w \in W\}$$

are called *chambers*.

Lemma 78. *Let $\Pi = \Phi \cap \mathbf{R}_{\geq 0}\Delta$ be the unique positive system containing Δ. Then*

$$C = \bigcap_{\alpha\in\Pi} H_\alpha^+. \tag{101}$$

In particular,

$$C \subset V \setminus \bigcup_{\beta\in\Phi} H_\beta. \tag{102}$$

Proof. If $\lambda \in C$, then $(\lambda, \alpha) > 0$ for all $\alpha \in \Delta$. Since $\Phi \subset (\mathbf{R}_{\geq 0}\Delta) \cup (\mathbf{R}_{\leq 0}\Delta) \setminus \{0\}$, we see that $(\lambda, \beta) > 0$ for all $\beta \in \Pi$. This implies (101). Since $\Phi = \Pi \cup (-\Pi)$, we see that $(\lambda, \beta) \neq 0$ for all $\beta \in \Phi$. This implies $\lambda \notin \bigcup_{\beta \in \Phi} H_\beta$, proving (102). □

Lemma 79. *If $w \in W$ and $wC \cap C \neq \emptyset$, then $w = 1$. In particular, the group W acts simply transitively on the set of chambers.*

Proof. Suppose $w \in W$ satisfies $wC \cap C \neq \emptyset$. Then there exists $\lambda, \mu \in C$ such that $w\lambda = \mu$. This implies $\{\lambda, \mu\} \subset W\lambda \cap C \subset W\lambda \cap D$. By Theorem 71, we conclude $\lambda = \mu$. This also implies $w \in \mathrm{Stab}_W(\{\lambda\})$, hence $w = 1$ by Lemma 70(iii). In particular, $wC = C$ implies $w = 1$. This shows that W acts simply transitively on the set of chambers. □

Proposition 80.
$$V \setminus \bigcup_{\alpha \in \Phi} H_\alpha = \bigcup_{w \in W} wC \quad \textit{(disjoint).}$$

Proof. By Lemma 79, the chambers are disjoint from each other. Observe

$$\begin{aligned} wC &\subset V \setminus w \bigcup_{\alpha \in \Phi} H_\alpha && \text{(by Lemma 78)} \\ &= V \setminus \bigcup_{\alpha \in \Phi} H_\alpha && \text{(by (99)).} \end{aligned}$$

Thus
$$V \setminus \bigcup_{\alpha \in \Phi} H_\alpha \supset \bigcup_{w \in W} wC \quad \text{(disjoint).}$$

Conversely, let $\lambda \in V \setminus \bigcup_{\alpha \in \Phi} H_\alpha$. By Theorem 71, there exists $w \in W$ such that $w\lambda \in D$, or equivalently, $\lambda \in w^{-1}D$. We claim $\lambda \in w^{-1}C$. Indeed, if $\lambda \notin w^{-1}C$, then

$$\begin{aligned} w\lambda &\in D \setminus C \\ &= \{\mu \in V \mid (\mu, \alpha) \geq 0 \ (\forall \alpha \in \Delta),\ (\mu, \beta) \leq 0 \ (\exists \beta \in \Delta)\} \\ &\subset \{\mu \in V \mid (\mu, \beta) = 0 \ (\exists \beta \in \Delta)\} \\ &= \bigcup_{\beta \in \Delta} H_\beta \\ &\subset \bigcup_{\beta \in \Phi} H_\beta \\ &= w \bigcup_{\beta \in \Phi} H_\beta && \text{(by (99)).} \end{aligned}$$

This implies $\lambda \in \bigcup_{\beta \in \Phi} H_\beta$ which is absurd. This proves the claim, and hence

$$V \setminus \bigcup_{\alpha \in \Phi} H_\alpha \subset \bigcup_{w \in W} wC.$$

□

July 25, 2016

For today's lecture, we let V be a finite-dimensional vector space over $\mathbf{R}$, with positive-definite inner product. Let Φ be a root system in V, and let $W = W(\Phi) = \langle s_\alpha \mid \alpha \in \Phi \rangle$. Fix a simple system Δ in Φ.

Definition 81. Let $\alpha \in \Phi$ and $w \in W$. The hyperplane H_α is called a *wall* of a chamber wC if $\alpha \in w\Delta$.

Notation 82. For $\lambda \in V$ and $\varepsilon > 0$, denote by $B(\lambda, \varepsilon)$ the ε-ball centered at λ:

$$B(\lambda, \varepsilon) = \{\lambda + \mu \mid \mu \in V,\ \|\mu\| < \varepsilon\}.$$

Lemma 83. *Let $\lambda \in V$ and $\varepsilon > 0$. If w is an orthogonal transformation of V, then $wB(\lambda, \varepsilon) = B(w\lambda, \varepsilon)$.*

Proof.

$$\begin{aligned} wB(\lambda, \varepsilon) &= \{w(\lambda + \mu) \mid \mu \in V,\ \|\mu\| < \varepsilon\} \\ &= \{w\lambda + w\mu \mid \mu \in V,\ \|w\mu\| < \varepsilon\} \\ &= \{w\lambda + \mu \mid \mu \in V,\ \|\mu\| < \varepsilon\} \\ &= B(w\lambda, \varepsilon). \end{aligned}$$

□

Lemma 84. *Let $\alpha \in \Phi$ and $\lambda \in H_\alpha^+$. Then there exists $\varepsilon > 0$ such that $B(\lambda, \varepsilon) \subset H_\alpha^+$.*

Proof. Since $\lambda \in H_\alpha^+$, we have $(\lambda, \alpha) > 0$. Set

$$\varepsilon = \frac{(\lambda, \alpha)}{2\|\alpha\|}.$$

Then for $\mu \in V$ with $\|\mu\| < \varepsilon$, we have

$$\begin{aligned} (\lambda + \mu, \alpha) &= (\lambda, \alpha) + (\mu, \alpha) \\ &\geq (\lambda, \alpha) - |(\mu, \alpha)| \\ &\geq (\lambda, \alpha) - \|\mu\|\|\alpha\| \\ &> (\lambda, \alpha) - \varepsilon\|\alpha\| \\ &= \frac{(\lambda, \alpha)}{2} \\ &> 0. \end{aligned}$$

Thus $\lambda + \mu \in H_\alpha^+$. This implies $B(\lambda, \varepsilon) \subset H_\alpha^+$. □

Lemma 85. *Let $\alpha \in \Phi$ and $\lambda, \mu \in H_\alpha^+$. Then for $0 \leq t \leq 1$, $t\lambda + (1-t)\mu \in H_\alpha^+$.*

Proof. We have

$$(t\lambda + (1-t)\mu, \alpha) = t(\lambda, \alpha) + (1-t)(\mu, \alpha) > 0.$$

□

Proposition 86. *For $\alpha \in \Phi$ and $w \in W$, the following are equivalent:*

(i) *H_α is a wall of wC,*

(ii) *there exist $\lambda \in H_\alpha$ and $\varepsilon > 0$ such that $H_\alpha \cap B(\lambda, \varepsilon) \subset wD$.*

Proof. First we prove the assertion for $w = 1$. Suppose H_α is a wall of C. Then $\alpha \in \Delta$. Then by Lemma 34,

$$s_\alpha(\Pi \setminus \{\alpha\}) = \Pi \setminus \{\alpha\}. \tag{103}$$

Let

$$C' = \bigcap_{\beta \in \Pi \setminus \{\alpha\}} H_\beta^+.$$

Then $C \subset C'$, and

$$\begin{aligned}
s_\alpha C &= \bigcap_{\beta \in \Pi} s_\alpha H_\beta^+ \\
&= \bigcap_{\beta \in \Pi} H_{s_\alpha \beta}^+ && \text{(by (97))} \\
&\subset \bigcap_{\beta \in \Pi \setminus \{\alpha\}} H_{s_\alpha \beta}^+ \\
&= \bigcap_{\beta \in s_\alpha(\Pi \setminus \{\alpha\})} H_\beta^+ \\
&= \bigcap_{\beta \in \Pi \setminus \{\alpha\}} H_\beta^+ && \text{(by (103))} \\
&= C'.
\end{aligned}$$

Thus

$$C \cup s_\alpha C \subset C'. \tag{104}$$

Let $\lambda_1 \in C$. Then $s_\alpha \lambda_1 \in s_\alpha C$. Set $\lambda = \frac{1}{2}(\lambda_1 + s_\alpha \lambda_1)$. Then $(\lambda, \alpha) = 0$, so $\lambda \in H_\alpha$. Since $\lambda_1, s_\alpha \lambda_1 \in C'$ by (104), Lemma 85 implies $\lambda \in C'$. Then by Lemma 84, for each $\beta \in \Pi \setminus \{\alpha\}$, there exists $\varepsilon_\beta > 0$ such that $B(\lambda, \varepsilon_\beta) \subset H_\beta^+$. Setting

$$\varepsilon = \min\{\varepsilon_\beta \mid \beta \in \Pi \setminus \{\alpha\}\},$$

we obtain $B(\lambda, \varepsilon) \subset C'$. Thus

$$H_\alpha \cap B(\lambda, \varepsilon) \subset H_\alpha \cap C'$$

$$
\begin{aligned}
&= H_\alpha \cap \left(\bigcap_{\beta \in \Pi \setminus \{\alpha\}} H_\beta^+ \right) \\
&\subset (H_\alpha^+ \cup H_\alpha) \cap \left(\bigcap_{\beta \in \Pi \setminus \{\alpha\}} (H_\beta^+ \cup H_\beta) \right) \\
&= D.
\end{aligned}
$$

Conversely, suppose there exist $\lambda \in H_\alpha$ and $\varepsilon > 0$ such that $H_\alpha \cap B(\lambda, \varepsilon) \subset D$. Since $s_\alpha \lambda = \lambda$, we have $s_\alpha B(\lambda, \varepsilon) = B(\lambda, \varepsilon)$ by Lemma 83. This, together with $s_\alpha H_\alpha = H_\alpha$ implies

$$H_\alpha \cap B(\lambda, \varepsilon) \subset s_\alpha D.$$

Thus

$$H_\alpha \cap B(\lambda, \varepsilon) \subset D \cap s_\alpha D. \tag{105}$$

We aim to show $\alpha \in \Delta$. Suppose, by way of contradiction, $\alpha \notin \Delta$. Then $n(s_\alpha) > 1$, so $\Pi \cap s_\alpha(-\Pi) \supsetneqq \{\alpha\}$. This implies that there exists $\beta \in \Pi \setminus \{\alpha\}$ such that $s_\alpha \beta \in -\Pi$. Thus $-s_\alpha \beta \in \Pi$, and hence

$$
\begin{aligned}
D &\subset H_{-s_\alpha\beta}^+ \cup H_{-s_\alpha\beta} \\
&= H_{s_\alpha\beta}^- \cup H_{s_\alpha\beta}.
\end{aligned} \tag{106}
$$

Also, since $\beta \in \Pi$, we have

$$
\begin{aligned}
s_\alpha D &\subset s_\alpha(H_\beta^+ \cup H_\beta) \\
&= H_{s_\alpha\beta}^+ \cup H_{s_\alpha\beta} && \text{(by (96),(97)).}
\end{aligned} \tag{107}
$$

Thus, combining (105)–(107), we find

$$H_\alpha \cap B(\lambda, \varepsilon) \subset H_{s_\alpha\beta}. \tag{108}$$

Since $\beta \neq \pm\alpha$, we have $s_\alpha \beta \neq \pm\alpha$. Thus $H_{s_\alpha\beta} \neq H_\alpha$, which implies that there exists $\mu \in H_\alpha \setminus H_{s_\alpha\beta}$. We may assume $\|\mu\| < \varepsilon$. Then

$$
\begin{aligned}
\lambda + \mu &\in B(\lambda, \varepsilon) \cap H_\alpha \\
&\subset H_{s_\alpha\beta} && \text{(by (108)).}
\end{aligned} \tag{109}
$$

Since

$$
\begin{aligned}
\lambda &\in B(\lambda, \varepsilon) \cap H_\alpha \\
&\subset H_{s_\alpha\beta} && \text{(by (108)),}
\end{aligned}
$$

while $\mu \notin H_{s_\alpha\beta}$, we obtain $\lambda + \mu \notin H_{s_\alpha\beta}$. This contradicts (109).

We have shown that the assertion holds for $w = 1$. We next consider the general case. Let $\alpha \in \Phi$ and $w \in W$. Then

$$\begin{aligned}
\text{(i)} &\iff \alpha \in w\Delta \\
&\iff w^{-1}\alpha \in \Delta \\
&\iff H_{w^{-1}\alpha} \text{ is a wall of } C \\
&\iff \exists\lambda \in H_{w^{-1}\alpha},\ \exists\varepsilon > 0,\ H_{w^{-1}\alpha} \cap B(\lambda, \varepsilon) \subset D \\
&\iff \exists\lambda \in w^{-1}H_\alpha,\ \exists\varepsilon > 0,\ w^{-1}H_\alpha \cap B(\lambda, \varepsilon) \subset D && \text{(by (96))} \\
&\iff \exists\lambda \in w^{-1}H_\alpha,\ \exists\varepsilon > 0,\ w^{-1}H_\alpha \cap w^{-1}B(w\lambda, \varepsilon) \subset D && \text{(by Lemma 83)} \\
&\iff \exists\mu \in H_\alpha,\ \exists\varepsilon > 0,\ H_\alpha \cap B(\mu, \varepsilon) \subset wD \\
&\iff \text{(ii)}.
\end{aligned}$$

□

Proposition 87. *If $s \in W$ is a reflection, then there exists $\alpha \in \Phi$ such that $s = s_\alpha$.*

Proof. Since s is a reflection, s fixes a hyperplane H. Let $H^\perp = \mathbf{R}\beta$, where $0 \neq \beta \in V$. Then $s = s_\beta$. Since $s \in \mathrm{Stab}_W(H)$, we have

$$\begin{aligned}
\{1\} &\neq \mathrm{Stab}_W(H) \\
&= \langle s_\alpha \mid \alpha \in \Phi,\ s_\alpha \in \mathrm{Stab}_W(H) \rangle && \text{(by Proposition 76).}
\end{aligned}$$

This implies that there exists $\alpha \in \Phi$ such that $s_\alpha \in \mathrm{Stab}_W(H)$. The latter implies $s_\alpha = s_\beta = s$. □

Note that Proposition 15 implies that the mapping which sends a root system to a reflection group is a surjection, the following proposition implies that it is essentially an injection.

Proposition 88. *If Φ and Φ' are root systems in V such that $W(\Phi) = W(\Phi')$, then*

$$\{H_\alpha \mid \alpha \in \Phi\} = \{H_{\alpha'} \mid \alpha' \in \Phi'\},$$

or equivalently,

$$\{\mathbf{R}\alpha \mid \alpha \in \Phi\} = \{\mathbf{R}\alpha' \mid \alpha' \in \Phi'\}.$$

Proof. If $\alpha \in \Phi$, then s_α is a reflection in $W(\Phi) = W(\Phi')$. By Proposition 87, there exists $\alpha' \in \Phi'$ such that $s_\alpha = s_{\alpha'}$. This implies $H_\alpha = H_{\alpha'}$. Therefore, we have shown

$$\{H_\alpha \mid \alpha \in \Phi\} \subset \{H_{\alpha'} \mid \alpha' \in \Phi'\}.$$

The reverse containment can be shown in a similar manner. □

August 1, 2016

Today, we describe briefly how to classify essential finite reflection groups. We have shown that every finite reflection group W comes from some root system, in the sense that $W = W(\Phi)$ for some root system Φ. Since $W(\Phi)$ is unchanged if we replace $\alpha \in \Phi$ by any nonzero scalar multiple, we assume Φ consists of vectors of length 1. We also assume that a root system spans the underlying vector space.

First, we consider the case $\dim V = 2$. A finite reflection group is of the form $W(\Phi)$ for some root system $\Phi \subset V$. Let Δ be a simple system in Φ. Then $|\Delta| = \dim V = 2$. Let $\Delta = \{\alpha, \beta\}$. By Theorem 41, we have $W(\Phi) = \langle s_\alpha, s_\beta \rangle$. Since $W(\Phi)$ is finite, there exists a positive integer m such that $(s_\alpha s_\beta)^m = 1$. We choose minimal such m, which is called the *order* of $s_\alpha s_\beta$. Then from the lecture on April 11, $s_\alpha s_\beta$ is a rotation. By the minimality of m, $W(\Phi)$ is the dihedral group of order m. Writing $r = st$ where $s = s_\alpha$ and $t = s_\beta$, $W(\Phi)$ consists of m rotations

$$1, r, r^2, \dots, r^{m-1},$$

and m other elements

$$s, rs, r^2 s, \dots, r^{m-1} s$$

which are reflections since

$$s = s_\alpha, rs = s_{s_\alpha \beta}, r^2 s = s_{s_\alpha s_\beta \alpha}, \dots.$$

By Proposition 87, the root system Φ consists of $2m$ vertices of regular $2m$-gons. It follows from the definition of a simple system that the angle formed by α and β is $\pi - \frac{\pi}{m}$. In particular,

$$(\alpha, \beta) = -\cos \frac{\pi}{m}. \tag{110}$$

Lemma 89. *Let Φ be a root system with a simple system Δ, and let $\alpha, \beta \in \Delta$. If $\alpha \neq \pm\beta$ and $s_\alpha s_\beta$ has order m, then* (110) *holds.*

Proof. Let $I = \{s_\alpha, s_\beta\}$. Then $W_I = \langle I \rangle$ is a dihedral group of order $2m$, and Φ_I is a root system in the 2-dimensional space $V_I = \mathbf{R}\alpha + \mathbf{R}\beta$. By Proposition 58(iii), $W_I = W(\Phi_I)$, so Φ_I consists of $2m$ vertices of regular $2m$-gons. As shown above, $\Delta_I = \{\alpha, \beta\}$ consists of vectors α, β which satisfy (110). □

Lemma 90. *Let Φ and Φ' be root systems in $\mathbf{R}^n$, with respective simple systems Δ and Δ'. Then the following are equivalent:*

(i) *there exists $t \in O(V)$ such that $W(\Phi') = tW(\Phi)t^{-1}$,*

(ii) *$\Delta = \{\alpha_1, \dots, \alpha_n\}$, $\Delta' = \{\alpha'_1, \dots, \alpha'_n\}$ such that $(\alpha_i, \alpha_j) = (\alpha'_i, \alpha'_j)$ for all $i, j \in \{1, \dots, n\}$.*

Proof. Suppose first (i) holds. Then $W(\Phi') = W(t\Phi)$. Thus, by Proposition 88, we obtain $\Phi' = t\Phi$. Since t is an orthogonal transformation, (ii) holds.

Next suppose (ii) holds. Let C and C' be square matrices whose column vectors are α_i's and α_i''s, respectively. Then $C^\top C = C'^\top C'$, hence $t = C'C^{-1}$ is an orthogonal matrix. Clearly, $\Delta' = t\Delta$, hence

$$\begin{aligned}
W(\Phi') &= \langle s_\alpha \mid \alpha \in \Delta' \rangle && \text{(by Theorem 41)}\\
&= \langle s_\alpha \mid \alpha \in t\Delta \rangle\\
&= \langle s_{t\alpha} \mid \alpha \in \Delta \rangle\\
&= \langle t s_\alpha t^{-1} \mid \alpha \in \Delta \rangle\\
&= t\langle s_\alpha \mid \alpha \in \Delta \rangle t^{-1}\\
&= tW(\Phi)t^{-1} && \text{(by Theorem 41).}
\end{aligned}$$

□

Combining Lemmas 89 and 90, we see that a finite reflection group in $\mathbf{R}^n$ is completely described by $n(n-1)/2$ integers $m_{ij} \geq 2$ $(1 \leq i < j \leq n)$, where the corresponding simple system is $\{\alpha_1, \dots, \alpha_n\}$ with

$$(\alpha_i, \alpha_j) = -\cos\frac{\pi}{m_{ij}}. \tag{111}$$

When $n = 2$, every integer $m_{12} \geq 2$ gives a finite reflection group, namely, the dihedral group $D_{m_{12}}$. However, for higher dimensions, m_{ij}'s are not arbitrary; rather quite restricted.

Lemma 91. *Let B be a real symmetric $n \times n$ matrix. Then the following are equivalent:*

(i) *B is positive definite,*

(ii) *there exist linearly independent vectors $\alpha_1, \dots, \alpha_n \in \mathbf{R}^n$ such that $(\alpha_i, \alpha_j) = B_{ij}$ for $1 \leq i < j \leq n$.*

Proof. Suppose first (ii) holds. Let C be the $n \times n$ matrix whose column vectors are $\alpha_1, \dots, \alpha_n$. Then $C^\top C = B$. This implies that B is positive definite.

Next suppose (i) holds. Then there exists an orthogonal matrix P such that $P^\top BP$ is a diagonal matrix with positive diagonal entries. This implies that there exists a diagonal matrix D with positive diagonal entries such that $P^\top BP = D^2$. Set $C = DP^\top$. Then $C^\top C = B$, hence the column vectors $\alpha_1, \dots, \alpha_n$ of C have the property required in (ii). □

Let $\Delta = \{\alpha_1, \dots, \alpha_n\}$ be a simple system, and define integers m_{ij} by (111). Then the real symmetric matrix B defined by

$$B_{ij} = \begin{cases} 1 & \text{if } i = j,\\ -\cos\frac{\pi}{m_{ij}} & \text{otherwise} \end{cases}$$

is positive definite. It turns out that this is the only condition needed to classify root systems or finite reflection groups, but it is already quite strong. For example, $n = 3$, $m_{12} = m_{13} =$

$m_{23} = 4$ fails to satisfy this condition, since

$$\begin{bmatrix} 1 & -\frac{1}{\sqrt{2}} & -\frac{1}{\sqrt{2}} \\ -\frac{1}{\sqrt{2}} & 1 & -\frac{1}{\sqrt{2}} \\ -\frac{1}{\sqrt{2}} & -\frac{1}{\sqrt{2}} & 1 \end{bmatrix}$$

is not positive definite. For $n = 3$, unless B is block diagonal, we have only three possibilities:

$$(m_{12}, m_{13}, m_{23}) = (2, 3, 3), (2, 3, 4), (2, 3, 5).$$

Bibliography

[1] J.E. Humphreys, Reflection Groups and Coxeter Groups, Cambridge University Press, 1990.

[2] J. Rotman, Advanced Modern Algebra, Prentice Hall, 2002.