1 Last time: generation by simple reflection

As usual V is a real vector space with a symmetric, positive definite, bilinear form $(\cdot,\cdot) : V \times V \to \mathbb{R}$.

The *reflection* with respect to a nonzero vector $\alpha \in V$ is the linear map

$$s_\alpha : v \mapsto v - \tfrac{2(v,\alpha)}{(\alpha,\alpha)}\alpha.$$

A *reflection group* is a subgroup of the general linear group $\mathrm{GL}(V)$ generated by a finite set of reflections.

Our goal is to classify the finite groups which are reflection groups.

Definition. A *root system* is a finite set Φ of nonzero vectors in V such that

(R1) $\Phi \cap \mathbb{R}\alpha = \{\alpha, -\alpha\}$ for each $\alpha \in \Phi$.

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

Elements of Φ are called *roots*. The group $W = \langle s_\alpha : \alpha \in \Phi\rangle$ is the *reflection group associated to* Φ.

Some properties shown in previous lectures which clarify the relationship between W and Φ:

Fact. If $W \subset \mathrm{GL}(V)$ is a finite reflection group then $\Phi = \{\alpha \in V : (\alpha,\alpha) = 1 \text{ and } s_\alpha \in W\}$ is a root system, for which $W = \langle s_\alpha : \alpha \in \Phi\rangle$ is the associated reflection group

Fact. On the other hand, if Φ is a root system then the associated reflection group is finite.

Definition. A *total order* on V is a transitive relation $<$ on V such that

(1) Exactly one of $a < b$ or $a = b$ or $b < a$ holds for each $a, b \in V$.

(2) If $a < b$ then $a + c < b + c$ for all $a, b, c \in V$.

(3) If $x < y$ and $c \in \mathbb{R}$ is positive then $cx < cy$ and $-cy < -cx$.

(How many total orders does V have if the space is 1-dimensional?)

To construct a total order on V, choose a basis $v_1, v_2, \dots, v_n$ and set $\sum_i a_i v_i < \sum_i b_i v_i$ if for some $j \in [n]$ it holds that $a_1 = b_1$, $a_2 = b_2$, $\dots$, $a_{j-1} = b_{j-1}$, and $a_j < b_j$.

Let Φ be a root sytsem.

Definition. A *positive system* Π is a set of the form $\{\alpha \in \Phi : 0 < \alpha\}$ where $<$ is some total order on V.

Note: $\Phi = \Pi \sqcup -\Pi$ if Π is a positive system.

Definition. A *simple system* Δ is a linearly independent subset of Φ with $\Phi = (\mathbb{R}^+\Delta \cap \Phi) \sqcup (\mathbb{R}^-\Delta \cap \Phi)$.

Summarizing the important properties of root systems that have been shown so far:

Theorem. Let Φ be a root system with associated reflection group $W = \langle s_\alpha : \alpha \in \Phi\rangle$.

(1) Each positive system in Φ contains a unique simple system.

(2) Each simple system in Φ is contained in a unique positive system.

(3) If Δ_1 and Δ_2 are two simple systems in Φ then $\Delta_1 = w\Delta_2$ for some $w \in W$.

(4) If Δ is a simple system in Φ then $W = \langle s_\alpha : \alpha \in \Delta\rangle$.

Two noteworthy properties that went into the proofs of the preceding list:

Proposition. Let Φ be a root system and $W = \langle s_\alpha : \alpha \in \Phi\rangle$.

(1) If $\Delta \subset \Phi$ is a simple system then $(\alpha, \beta) \leq 0$ for all $\alpha \neq \beta$ in Δ.

(2) If $\beta \in \Phi$ then $w\beta \in \Delta$ for some $w \in W$.

(3) If $\Delta \subset \Pi$ are simple/positive systems in Φ and $\alpha \in \Delta$ then $s_\alpha \Pi = (\Pi \setminus \{\alpha\}) \cup \{-\alpha\}$.

Probably in the next lecture we will stop repeating all of these definitions and foundational properties, which are getting quite familiar!

2 Length function

Fix a root system Φ with simple system Δ. Write Π for the unique positive system containing Δ and $<$ for the associated total order. Let $W = \langle s_\alpha : \alpha \in \Phi \rangle = \langle s_\alpha : \alpha \in \Delta \rangle$. Not only is the reflection group W generated by the set of simple reflections, but W is isomorphic to the finitely presented group

$$W \cong \langle x_\alpha \text{ for } \alpha \in \Delta : (x_\alpha x_\beta)^{m(\alpha,\beta)} = 1 \text{ for } \alpha, \beta \in \Delta \rangle$$

where $m(\alpha, \beta)$ denotes the order of the product $s_\alpha s_\beta$ in W. Here "x_α" is just a formal symbol, since the right hand group is a quotient of the free group on Δ. On the other hand, note that s_α is a specific invertible linear map. By construction, there exists a unique surjective homomorphism from the group on the right to W, mapping $x_\alpha \mapsto s_\alpha$ for each $\alpha \in \Delta$. (This claim is more or less the definition of a group presentation.) The miracle is that this homomorphism is actually a bijection.

As a tool for proving this fact next time, today we introduce the *length function* on W. Let

$$S = \{s_\alpha : \alpha \in \Delta\}$$

and define the *length* of $w \in W$ (relative to Δ) as the smallest integer $r \geq 0$ such that $w = s_1 s_2 \cdots s_r$ where each $s_i \in S$. Denote this number by $\ell(w)$.

Remarks. Some simple properties that fall right out of the definition:

(1) $\ell(1) = 0$, since products with zero factors evaluate to the identity by convention.

(2) $\ell(w) = 1$ if and only if $w \in S$, certainly.

(3) $\ell(w^{-1}) = \ell(w)$, since each factorization of w is the reverse of a factorization of w^{-1}.

Implicitly, Φ is a subset of some vector space V with a positive definite symmetric bilinear form. We might as well assume that $V = \mathbb{R}\Delta$ so that the simple system Δ is a basis for V.

Proposition. The determinant of $s \in S$ as a linear map $V \to V$ is -1.

Therefore $\det(w) = (-1)^{\ell(w)}$ for each $w \in W$.

Proof. With respect to the basis $b_1, b_2, \ldots, b_n$ of V, where $b_1 = \alpha$ and $b_2, \ldots, b_n$ span the hyperplane orthogonal to α, the matrix of $s = s_\alpha$ is $\text{diag}(-1, 1, \ldots, 1)$ so has determinant -1. The statement about $\det(w)$ follows since $\det(AB) = \det(A)\det(B)$. □

Corollary. If $u, v \in W$ then $\ell(uv)$ and $\ell(u) + \ell(v)$ are either both even or both odd.

Proof. Note that $(-1)^{\ell(uv)} = \det(uv) = \det(u)\det(v) = (-1)^{\ell(u)+\ell(v)}$. □

Corollary. If $w \in W$ and $s \in S$ and $\ell(w) = r$, then $\ell(ws) = r \pm 1$.

Proof. Certainly $r - 1 \leq \ell(ws) \leq r + 1$ (why?) and $\ell(ws) \not\equiv \ell(w) \pmod 2$. □

The definition of $\ell : W \to \mathbb{N}$ is very general, and would make sense for any group relative to a given generating set. The remarkable thing about the length function of a reflection group is that $\ell(w)$ also has a very concrete geometric formula in terms of how w acts on the root system Φ.

For $w \in W$, define $n(w)$ as the number of positive roots $\alpha \in \Pi$ with $w\alpha \in -\Pi$

Recall that "$\alpha \in \Pi$" means the same thing as "$\alpha > 0$."

Lemma. Let $\alpha \in \Delta$ and $w \in W$.

(a) If $w\alpha > 0$ then $n(ws_\alpha) = n(w) + 1$.

(b) If $w\alpha < 0$ then $n(ws_\alpha) = n(w) - 1$.

(c) If $w^{-1}\alpha > 0$ then $n(s_\alpha w) = n(w) + 1$.

(d) If $w^{-1}\alpha < 0$ then $n(s_\alpha w) = n(w) - 1$.

Proof. Define $\Pi(w) = \{\beta \in \Pi : w\beta \in -\Pi\}$ so that $n(w) = |\Pi(w)|$.

If $w\alpha > 0$ then $\Pi(ws_\alpha) = s_\alpha\Pi(w) \sqcup \{\alpha\}$ since s_α permutes $\Pi \setminus \{\alpha\}$. Part (a) follows.

If $w\alpha < 0$ then, by the same observation, $s_\alpha\Pi(ws_\alpha) = \Pi(w) \setminus \{\alpha\}$ while $\alpha \in \Pi(w)$. Part (b) follows.

Parts (c) and (d) follow by replacing w by w^{-1} and noting that $n(w^{-1}) = n(w)$. □

Corollary. If $w \in W$ and $w = s_1 s_2 \cdots s_r$ where each $s_i \in S$ then $n(w) \leq r$, so $n(w) \leq \ell(w)$.

Proof. The lemma shows that applying n to the elements 1, s_1, s_1s_2, $s_1s_2s_3$, $\dots$, $s_1s_2\cdots s_r$ yields a sequence of integers, beginning with 0, in which successive numbers differ by at most one. □

We require a stronger result to deduce the opposite inequality.

Theorem (Exchange principle)**.** Let $w = s_1s_2\cdots s_r$ where each $s_i \in S$ and $s_i = s_{\alpha_i}$ for the simple root $\alpha_i \in \Delta$. Assume $n(w) < r$. Then there exist indices $1 \leq i < j \leq r$ such that

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

(b) $s_{i+1}s_{i+2}\cdots s_j = s_is_{i+1}\cdots s_{j-1}$.

(c) $w = s_1 \cdots \widehat{s_i} \cdots \widehat{s_j} \cdots s_r$ where for each $\widehat{\ }$ we omit the capped factor.

In other words, we can omit two factors from $s_1s_2\cdots s_r$ without changing the product.

Proof. Iterate part (a) of the lemma to deduce that there exists an index $j \leq r$ with $(s_1\cdots s_{j-1})\alpha_j < 0$. Since $\alpha_j > 0$, there exists $i < j$ with $s_i(s_{i+1}\cdots s_{j-1})\alpha_j < 0$ while $(s_{i+1}\cdots s_{j-1})\alpha_j > 0$. Let $\alpha = (s_{i+1}\cdots s_{j-1})\alpha_j \in \Pi$. Since $s_i\alpha < 0$, it must hold that $\alpha = \alpha_i$ since this is the only positive root which s_i makes negative. We thus obtain part (a).

Now set $\alpha = \alpha_j$ and $v = s_{i+1}\cdots s_{j-1}$ so that $v\alpha = \alpha_i$ by the first part. We then have $vs_\alpha v^{-1} = s_{v\alpha} = s_i$, so $vs_j = s_iv$. Replacing v by $s_{i+1}\cdots s_{j-1}$ gives part (b).

Part (c) follows by multiplying both sides of the identity in part (b) by $s_1\cdots s_{i-1}$ on the left and by $s_{j+1}\cdots s_r$ on the right. □

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

Proof. We already saw that $n(w) \leq \ell(w)$. This inequality cannot be strict since the exchange principle would then imply that we could write w as a product of $\ell(w) - 2$ simple generators, a contradiction. □

The proof of the theorem indicates an effective procedure for determining precisely which positive roots $w \in W$ makes negative. We call "$w = s_1 s_2 \cdots s_r$" a *reduced expression* if each $s_i \in S$ and $\ell(w) = r$.

Proposition. Let $w \in W$. Suppose $w = s_1 s_2 \cdots s_r$ is a reduced expression. Let $\alpha_i \in \Delta$ be such that $s_i = s_{\alpha_i}$. Define $\beta_r = \alpha_r$ and $\beta_i = (s_r s_{r-1} \cdots s_{i+1})\alpha_i$ for $i \in [r-1]$. Then $\beta_1, \beta_2, \ldots, \beta_r$ are distinct positive roots and $\{\alpha \in \Pi : w\alpha \in -\Pi\} = \{\beta_1, \ldots, \beta_r\}$.

Proof. Let $\beta \in \Pi$ be such that $w\beta < 0$.

We can then find an index $i \leq r$ such that $(s_{i+1} \cdots s_r)\beta > 0$ but $(s_i s_{i+1} \cdots s_r)\beta < 0$. Let $\alpha = s_{i+1} \cdots s_r \beta \in \Pi$. Since $s_i \alpha < 0$, we must have $\alpha = \alpha_i$, so $\beta = s_r \cdots s_{i+1}\alpha_i = \beta_i$.

Thus $\{\alpha \in \Pi : w\alpha \in -\Pi\} \subset \{\beta_1, \ldots, \beta_r\}$. The containment is equality and the β_i's are distinct since the first set has size r by assumption. □

Next time: a presentation for W.