MATH4301 Lecture Notes

Lectures by Ole Warnaar
Notes taken by Jackson Gatenby

MATH4301 Advanced Algebra
The University of Queensland

Version 0.12.1

October 17, 2013

Contents

0.1 Meta

It is the author's intention that these notes, and the LaTeX source code, be publicly released and made available for future reference, so this section records notes about these notes.

At time of writing, this document can be found at `http://jgat.github.io/math4301-notes/lectures.pdf`, and its source code can be found at `https://github.com/jgat/math4301-notes`.

The 2013 offering of MATH4301 Advanced Algebra was divided into two halves, the first half on Galois Theory, taught by Victor Scharaschkin, and the second half on Coxeter Groups, taught by Ole Warnaar. Each half of the course was accompanied by an assignment worth 20% of the grade, and an exam worth 30% of the grade.

This document contains detailed lecture notes taken during the second half of the course. The notes correspond closely to what was written and said in lectures. Each section within this document corresponds to notes taken in a single lecture.

1 Introduction

1.1 Presentations

Let A be an alphabet, the free group $F(A)$ consists of all words over $A \cup A^{-1}$ in which the pairs aa^{-1} and $a^{-1}a$ are forbidden (i.e. $aa^{-1} = a^{-1}a = 1$). The group multiplication corresponds to concatenation of words and removal of forbidden pairs.

Example: if $A = \{a\}$, $F(A) = \{a^k \mid k \in \mathbb{Z}\} \cong (\mathbb{Z}, +)$. If $w_1 = a^4$, $w_2 = a^{-2}$, then $w_1w_2 = aaaaa^{-1}a^{-1} = a^2$.

To make life more interesting we need relations. For example, $A = \{a, b\}$ with relation $b = 1$ gives $(\mathbb{Z}, +)$.

A *presentation* (of a group) $\langle A \mid R\rangle$ consists of a set A of *generators* and a set of relations R between the generators (and their inverses). Elements of the group are again words in A, but two words represent the same element in the group if they can be transformed into each other by the use of R. More formally, $G \cong F(A)/N$ where N is the normal subgroup generated by R.

Example: $\langle a \mid a^k = 1\rangle \cong \mathbb{Z}/k\mathbb{Z} = \mathbb{Z}_k$ (for $k = 1, 2, \dots$). Formally, $\langle a \mid a^k = 1\rangle \cong F(a)/\langle a^k\rangle$.

Example: $\langle a, b \mid a^2 = b^2 = (ab)^2 = 1\rangle$ contains elements $1, a, b, ab, ba, \dots$, however note that $ba = (ab)^{-1} = ab$. Simply guessing which words are distinct is not going to work. The multiplication table of the group is (Exercise: Show that this is all of the elements in the group):

G	1	a	b	ab
1	1	a	b	ab
a	a	1	ab	b
b	b	ab	1	a
ab	ab	b	a	1

Note that $bab = a^{-1}abab = a^{-1} = a$. This is the Klein 4-group $\cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$. Geometrically it is the symmetry group of the (non-square) rectangle and a rhombus, where a and b are reflections and ab is rotation by π.

The *word problem* is to decide if two *distinct* words in the generators represent the same/different elements in the group. In 1955, Novikov showed that the word problem is undecidable. This is not the case for Coxeter groups.

1.2 Coxeter Groups

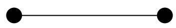
References:

- Bjorner & Brenti: Combinatorics of Coxeter groups (Springer GTM231, '05)
- Bourbaki: Lie groups & Lie algebras (Chap 4-6)
- Cohen: Coxeter groups
- Humphreys: Reflection Groups and Coxeter Groups
- Davis: The Geometry and Topolology of Coxeter Groups

Let M be an $r \times r$ symmetric matrix with entries m_{ij} in $\{1, 2, 3, \dots\} \cup \{\infty\}$ with $m_{ii} = 1$ and $m_{ij} = m_{ji} > 1$ for $i \neq j$. Such a matrix is called a *Coxeter matrix.* For example,

$$\begin{pmatrix} 1 & 3 \\ 3 & 1 \end{pmatrix}$$

Coxeter matrices are often represented as a graph with r labelled vertices $(1, 2, \dots, r)$, and if $m_{ij} \geq 3$, an edge between i and j with a labelling of the edge by m_{ij}. It is standard to drop edge labels which are 3. Hence the above example can be expressed as



Given a Coxeter matrix M (or graph), a *Coxeter system* (W, S) of type M is a set $S = \{s_1, \dots, s_r\}$ and a group

$$W = \langle S \mid (s_i s_j)^{m_{ij}} = 1, \quad 1 \leq i, j \leq r, m_{ij} \neq \infty \rangle.$$

(That is, whenever $m_{ij} \neq \infty$, impose a relation $(s_i s_j)^{m_{ij}} = 1$). The group W is called a *Coxeter group* (of type M). The number r is known as the *rank* of W. Note that $s_i^2 = 1$ for all $1 \leq i \leq r$.

Example: For rank 1, there is only one Coxeter group, $M = (1)$, with the trivial graph:

and the corresponding Coxeter group $W = \langle s \mid s^2 = 1 \rangle \cong \mathbb{Z}_2 = \mathbb{Z}/2\mathbb{Z}$.

For rank 2, we have first,

$$M = \begin{pmatrix} 1 & 2 \\ 2 & 1 \end{pmatrix},$$

with corresponding graph

and corresponding group

$$W = \langle s, t \mid s^2 = t^2 = (st)^2 = 1 \rangle \cong \mathbb{Z}_2 \times \mathbb{Z}_2$$

(Note that $(s_i s_j)^{m_{ij}} = 1$ implies that $(s_j s_i)^{m_{ij}} = 1$. Why: $(s_j s_i)^{m_{ij}} = (s_j s_i)^{m_{ij}} s_j^2 = s_j (s_i s_j)^{m_{ij}} s_j = s_j^2 = 1$) We will later show that if a Coxeter system has a disconnected graph, then the Coxeter group will be the direct product of the corresponding groups for each component; hence we will focus on connected graphs. We also have

$$M = \begin{pmatrix} 1 & m \\ m & 1 \end{pmatrix}, \quad m \geq 3,$$

and

$$W = \langle s, t \mid s^2 = t^2 = (st)^m = 1 \rangle.$$

This is known as the *dihedral* group of order $2m$ (D_m / D_{2m} / $I_2(m)$). The dihedral group is the symmetry group of the regular m-gon. For example, $I_2(3)$ is the symmetry group of the triangle, where $s, t, sts = tst$ are reflections and st, ts are rotations. $I_2(4)$ has reflections $s, t, sts = s(ts)^2 = (st)^2 s, tst = t(st)^2 = (ts)^2 t$.

Note that a word of odd length corresponds to a reflection, and a word of even length corresponds to a rotation; also note that the relation $(st)^m = 1$ embodies the “rotate m times to get the identity” property of the m-gon.

1.3 Dihedral Groups

Recall that a Coxeter group is of the form

$$W = \langle S \mid (s_i s_j)^{m_{ij}} = 1, 1 \leq i \leq j \leq r, m_{ij} \neq \infty \rangle,$$

with the associated matrix $M = (m_{ij})$ where $m_{ii} = 1$ and $M^T = M$. A special case is, for $m > 2$,

$$I_2(m) = \langle s, t \mid s^2 = t^2 = (st)^m = 1 \rangle,$$

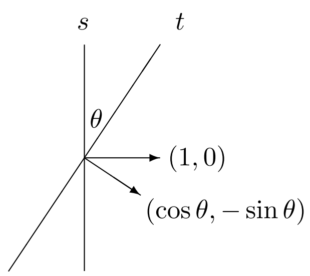
a Coxeter group of rank 2. We saw that $I_2(3)$ is the group of symmetries of the equilateral triangle, and $I_2(4)$ is the group of symmetries of the square. We claim that $I_2(m)$ is a group of order $2m$ consisting of m reflections and m rotations of the regular m-gon.

First, for a vector $\alpha \in \mathbb{R}^n$, let H_α denote the hyperplane with normal α, and denote reflection in H_α by r_α. Now, for any vector λ,

$$r_\alpha(\lambda) = \lambda - \frac{2(\alpha, \lambda)\alpha}{(\alpha, \alpha)}, \tag{1.1}$$

where (a, b) denotes the inner product (vector dot product). Note that $r_\alpha(\lambda) = \lambda$ for every $\lambda \in H_\alpha$, and $r_\alpha(\alpha) = \alpha - \frac{2(\alpha,\alpha)\alpha}{(\alpha,\alpha)} = -\alpha$ as expected. Since we have verified this for a hyperplane of codimension 1 and for a vector normal to the hyperplane, the result is true for all vectors (by Linear Algebra).

Proof. Let s and t be reflections, where the axes of symmetry have an angle of $\theta = \frac{\pi}{m}$, i.e. $s := r_{(1,0)}$ and $t := r_{(\cos\theta, -\sin\theta)}$:



Then, $s(1,0) = (-1,0)$ and $s(0,1) = (0,1)$, so

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

is a matrix representation of s, and

$$\hat{t} = \begin{pmatrix} -\cos 2\theta & \sin 2\theta \\ \sin 2\theta & \cos 2\theta \end{pmatrix}$$

is a matrix representation of t (Exercise).

If we can show that st is a rotation over $\frac{2\pi}{m}$, then $(st)^k$ will be a rotation over $\frac{2\pi k}{m}$, which will give m distinct rotations. Now,

$$\hat{s}\hat{t} = \begin{pmatrix} \cos 2\theta & -\sin 2\theta \\ \sin 2\theta & \cos 2\theta \end{pmatrix},$$

which is a rotation matrix for rotation over 2θ (Exercise). Then $(\hat{s}\hat{t})^k$ is a rotation by $2k\theta$ (easy to see geometrically, or show inductively that $(\hat{s}\hat{t})^k$ is a rotation matrix).

It remains to show that there are m distinct words of odd length, and they are all reflections. WLOG, we can say that all words of odd length are of the form $t(st)^{k-1}$ for some $k = 1, 2, \dots, m$, hence there are m distinct words of odd length. Now,

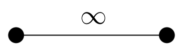
$$\hat{t}(\hat{s}\hat{t})^k = \begin{pmatrix} -\cos 2\theta & \sin 2\theta \\ \sin 2\theta & \cos 2\theta \end{pmatrix} \begin{pmatrix} \cos 2\theta(k-1) & -\sin 2\theta(k-1) \\ \sin 2\theta(k-1) & \cos 2\theta(k-1) \end{pmatrix} = \begin{pmatrix} -\cos(2k\theta) & \sin 2k\theta \\ \sin 2k\theta & \cos 2k\theta \end{pmatrix}$$

(Exercise), so $t(st)^{k-1} := r_{(\cos k\theta, -\sin k\theta)}$. Hence the m words of odd length are all reflections. $\square$

Finally, we consider the remaining Coxeter group of rank 2, given by

$$M = \begin{pmatrix} 1 & \infty \\ \infty & 1 \end{pmatrix},$$

with corresponding graph



and corresponding group

$$I_2(\infty) = \langle s, t \mid s^2 = t^2 = 1 \rangle.$$

Elements of this group, known as the ∞-dihedral group are the words of the form: $1, s, t, st, ts, sts, tst, \dots$. Again this group has a geometric interpretation in terms of reflections (etc.). Before we can describe this, we need some more notation.

Let $V = \mathbb{R}^n$ and for $\alpha \in V$ let H_α denote the hyperplane perpendicular to α. Algebraically, $H_\alpha = \{\lambda \in V : (\lambda, \alpha) = 0\}$. As we have seen, the reflextion r_α in H_α is given by its action on $\lambda \in V$ as

$$r_\alpha(\lambda) = \lambda - \frac{2(\alpha, \lambda)}{(\alpha, \alpha)}\alpha = \lambda - \frac{2(\lambda, \alpha)}{||\alpha||^2}\alpha = \lambda - (\lambda, \alpha^\vee)\alpha,$$

where $\alpha^\vee = \frac{2\alpha}{||\alpha||^2}$.

1.4 ...?

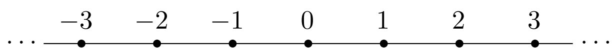
At some point I'll write this up in LaTeX, but for the time being:

- `http://jgat.github.io/math4301-notes/lec4-1.jpg`
- `http://jgat.github.io/math4301-notes/lec4-2.jpg`
- `http://jgat.github.io/math4301-notes/lec4-3.jpg`

1.5 $I_2(\infty)$ and Symmetric Groups

1.5.1 Affine Reflections

Consider the integer number line,



Let $s = r_0$, $t = r_1$, in the group $W = \langle s, t \mid s^2 = t^2 = 1\rangle$. From last time, we had the following claims:

Claim 1: $r_k = s(st)^k$, $t_{2k} = (ts)^k$, $k \in \mathbb{Z}$, where r_k is reflection about k, and t_{2k} is a transation by $2k$.

Claim 2: $\tilde{A}_1 = A_1 \ltimes T$, where $A_1 = \{1, r_0\}$, $T = \{t_{2k} : k \in \mathbb{Z}\}$.

Proof. Recall that

$$r_{\alpha,\kappa}(\lambda) = \lambda - \{(\lambda, \alpha) - \kappa\}\alpha^\vee,$$

if $\alpha = 1$, then $\alpha^\vee = 2$ (since the dot product between α and $\alpha^\vee$ must be 2), so

$$r_k = \lambda - 2\{\lambda - k\} = 2k - \lambda.$$

Then,

$$ts(\lambda) = r_1 r_0(\lambda) = r_1(-\lambda) = 2 + \lambda = t_2(\lambda),$$

thus $ts = t_2$, so $(ts)^k = t_{2k}$. Furthermore,

$$s(st)^k(\lambda) = r_0 t_{-2k}(\lambda) = r_0(\lambda - 2k) = -\lambda + 2k = r_k(\lambda),$$

so $s(st)^k = r_k$. □

Note that

$$r_{\alpha,\kappa}(\lambda + \mu) \neq r_{\alpha,\kappa}(\lambda) + r_{\alpha,\kappa}(\mu),$$

instead it holds that,

$$\begin{aligned} r_{\alpha,\kappa}(\lambda + \mu) &= \lambda + \mu - \{(\lambda + \mu, \alpha)\alpha^\vee - \kappa\} \\ &= \lambda + \mu - \{(\lambda, \alpha)\alpha^\vee + (\mu, \alpha)\alpha^\vee - \kappa\} \\ &= r_{\alpha,\kappa}(\lambda) + r_{\alpha,\kappa}(\mu) - \kappa\alpha^\vee \end{aligned}$$

Now,

$$\begin{aligned} r_{\alpha,\kappa} t_\lambda r_{\alpha,\kappa}(\mu) &= r_{\alpha,\kappa}(\lambda + r_{\alpha,\kappa}(\mu)) \\ &= r_{\alpha,\kappa}(\lambda) + \mu - \kappa\alpha^\vee \\ &= r_{\alpha,0}(\lambda) + \mu, \end{aligned}$$

so $r_{\alpha,\kappa} t_\lambda r_{\alpha,\kappa} = t_{r_\alpha(\lambda)}$.

1.5.2 Semi-direct products

Recall that, for a group G, if $K \leq G$, $N \triangleleft G$, $K \cap N = \{1\}$, and $G = NK$, then we say $G = K \ltimes N$ or $G = N \rtimes K$. Now, consider claim 2:

$$\tilde{A}_1 = \{t_{2k}, r_k \mid k \in \mathbb{Z}\},$$

and consider the subgroups

$$N = T = \{t_{2k} : k \in \mathbb{Z}\}, K = \{1, r_0\} = A_1.$$

Note that $r_k = r_0 t_{-2k}$, so $\tilde{A}_1 = A_1 T$. Thus, claim 2 holds.

1.5.3 Symmetric Groups

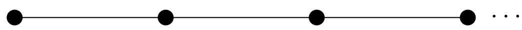
Before moving to the general theory, we will discuss one more important example of a finite reflection group (Coxeter group), the symmetric group S_n, also denoted A_{n-1} (not to be confused with the alternating group!) Let us define S_n to be

$$S_n = \langle s_1, \dots, s_{n-1} \mid s_i^2 = 1, (s_i s_{i+1})^3 = 1, (s_i s_j)^2 = 1, |i-j| > 1 \rangle.$$

Clearly the associated Coxeter matrix is

$$M = \begin{pmatrix} 1 & 3 & 2 & \cdots & 2 \\ 3 & 1 & 3 & \cdots & 2 \\ 2 & 3 & 1 & \ddots & \vdots \\ \vdots & \vdots & \ddots & \ddots & 3 \\ 2 & 2 & \cdots & 3 & 1 \end{pmatrix}$$

with Coxeter graph



The most common description of S_n is as the group of permutations on n letters with s_i acting as "adjacent" transpositions, interchanging the letters in positions i and $i+1$ (i.e. the cycle $(i \;\; i+1)$). For example, $s_2(2,3,6,4,5,1) = (2,6,3,4,5,1)$. The relation $(s_i s_j)^2 = 1$ for $|i-j| > 1$ may be recast as the commutation relation $s_i s_j = s_j s_i$. Finally, $(s_i s_{i+1})^3 = 1$ can be restated as $s_i s_{i+1} s_i = s_{i+1} s_i s_{i+1}$, known as Artin's braid relation.

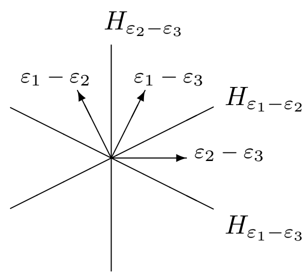
Of course, S_n can also be interpreted as a reflection group. Let $V = \mathbb{R}^n$ and s_i the reflection in the hyperplane $H_{\varepsilon_i - \varepsilon_{i+1}} = H_{\alpha_i}$, where ε_i is the i^{th} basis vector in the standard basis. Then, it holds that

$$s_i(\varepsilon_k) = \begin{cases} \varepsilon_k & k \neq i, i+1 \\ \varepsilon_{i+1} & k = i \\ \varepsilon_i & k = i+1 \end{cases}$$

That is, elements of A_{n-1} permute the basis elements of $\mathbb{R}^n$, so that indeed $s_i^2 = 1$, $s_i s_{i+1} s_i = s_{i+1} s_i s_{i+1}$, and $s_i s_j = s_j s_i$ for $|i-j| > 1$. (Exercise: show this).

Note that $\varepsilon_1 + \cdots + \varepsilon_n$ is fixed by the action of $A_{n-1}(= S_n)$, and no other vector linearly independent to this is fixed, hence A_{n-1} only acts on an $(n-1)$-dimensional subspace of $\mathbb{R}^n$, namely $\{\lambda \in \mathbb{R}^n \mid (\lambda, \varepsilon_1 + \cdots + \varepsilon_n) = 0\}$.

For example, in the case of $S_3 = A_2$, we have reflection in the three hyperplanes (planes) below (note that this is a 2-dimensional projection of $\mathbb{R}^3$, where the lines H_α are planes in $\mathbb{R}^3$):



Now, A_{n-1} is the symmetry group of the $(n-1)$-simplex, the generalisation of the tetrahedron to $n-1$ dimensions, where for instance the 2-simplex is the triangle, the 3-simplex is the tetrahedron, and so on.

2 Finite Reflection Groups

2.1 The General Theory of Finite Reflection Groups

Let V be an Euclidean space, that is, a vector space over $\mathbb{R}$ with a positive definite symmetric bilinear form $(\cdot,\cdot) : V \times V \to \mathbb{R}$, for example the dot product $(a, b) = a \cdot b$ in $\mathbb{R}^n$. (Here it suffices to think of $\mathbb{R}^n$ when using Euclidean spaces).

A *reflection* in V is a linear map s_α ($\alpha \in V$) such that

$$s_\alpha(\lambda) = \lambda - (\lambda, \alpha^\vee)\alpha,$$

where $\alpha^\vee := \frac{2\alpha}{(\alpha,\alpha)}$ (cf. Equation (1.1)). Note that s_α is an *involution* as well as an *orthogonal transformation*:

Proof.

$$\begin{aligned} s_\alpha^2(\lambda) &= s_\alpha(\lambda - (\lambda, \alpha^\vee)\alpha) \\ &= s_\alpha(\lambda) - (\lambda, \alpha^\vee)s_\alpha(\alpha) \\ &= \lambda - (\lambda, \alpha^\vee)\alpha + (\lambda, \alpha^\vee)\alpha \\ &= \lambda, \end{aligned}$$

so s_α is an involution. Also,

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

so s_α is an orthogonal transformation. (Exercise: convince yourself of these results.) $\square$

A *finite reflection group* is a finite subgroup of the group of orthogonal transformations on V generated by reflections. As we shall see (I hope), all finite reflection groups are Coxeter groups. The converse also holds, however we will not show this.

Lemma 1. *Let $O(V)$ be the group of orthogonal transformations on V, and $W < O(V)$ be a finite reflection group. If $s_\alpha \in W$ is a reflection and $g \in O(V)$ then $gs_\alpha g^{-1} = s_{g(\alpha)}$.*

(Note that there may be elements in W which are not reflections. Hence this does not say that W is normal in $O(V)$, since this lemma does not necessarily hold for all elements of W.)

Proof. Let $\beta = g(\alpha) \in V$. Then first,

$$gs_\alpha g^{-1}(\beta) = gs_\alpha g^{-1}g(\alpha) = gs_\alpha(\alpha) = g(-\alpha) = -g(\alpha) = -\beta.$$

If we can show that $gs_\alpha g^{-1}(H_\beta) = H_\beta$ pointwise, then we are done, because $gs_\alpha g^{-1}$ must then be the reflection s_β.

Let $\lambda \in H_\alpha$. Note that $\lambda \in H_\alpha \iff g(\lambda) \in H_\beta$, since $0 = (\lambda, \alpha) = (g(\lambda), \beta)$. Now,

$$gs_\alpha g^{-1}(g(\lambda)) = gs_\alpha(\lambda) = g(\lambda),$$

so indeed $g(\lambda)$ is fixed by $gs_\alpha g^{-1}$. □

Corollary 2. *If $s_\alpha, w \in W$ then $s_{w(\alpha)} \in W$. i.e. if H_α is a reflection hyperplane, so is $H_{w(\alpha)}$.*

Proof. Set $g = w$ in Lemma 1. □

We conclude that reflecting hyperplanes are permuted by the action of w. For example, take $W = A_2(= S_3)$, which contains the non-identity elements $s_\alpha, s_\beta, s_\alpha s_\beta, s_\beta s_\alpha, s_\alpha s_\beta s_\alpha$. Now,

$$\begin{aligned} H_\alpha &= s_\alpha(H_\alpha) = s_\beta(H_{\alpha+\beta}) = s_\alpha s_\beta(H_{\alpha+\beta}) = s_\beta s_\alpha(H_\beta) = s_\alpha s_\beta s_\alpha(H_\beta) \\ H_\beta &= s_\alpha(H_{\alpha+\beta}) = s_\beta(H_\beta) = s_\alpha s_\beta(H_\alpha) = s_\beta s_\alpha(H_{\alpha+\beta}) = s_\alpha s_\beta s_\alpha(H_\alpha) \\ H_{\alpha+\beta} &= s_\alpha(H_\beta) = s_\beta(H_\alpha) = s_\alpha s_\beta(H_\beta) = s_\beta s_\alpha(H_\alpha) = s_\alpha s_\beta s_\alpha(H_{\alpha+\beta}) \end{aligned}$$

We see that each hyperplane occurs twice as a permutation of each other hyperplane. What we don't see here is that the group elements will also permute the normals of the hyperplane.

To better understand the structure of W, we introduce the notion of a *root system.*

Definition: Let Φ be a finite subste of V. Φ is called a root system if, for all $\alpha \in \Phi$,

1. The only multiples of α in Φ are $\alpha, -\alpha$ (so that for each normal vector α, we only have it and its negative).
2. $s_\alpha(\Phi) = \Phi$.

Several remarks are in order:

- Sometimes, condition 1 is dropped from the definition, allowing for *non-reduced* root systems.
- Sometimes a third condition is assumed, that $(\alpha, \beta^\vee) \in \mathbb{Z}$ for $\alpha, \beta \in \Phi$. (We will not assume this.) This leads to *crystallographic* root systems, important in Lie theory.

Lemma 3. *The classification of finite reflection groups boils down to the classification of root systems.*

Proof. Homework. □

2.2 Root Systems

Claim: The classification of finite reflection groups is the same as the classification of root systems.

Recall that a root system $\Phi \subset V$ is a finite set such that for all $\alpha \in \Phi$, the only multiples of α are $\alpha, -\alpha$, and $s_\alpha(\Phi) = \Phi$.

For example, we have seen that A_2 is generated by reflection about three hyperplanes in $\mathbb{R}^3$; the six unit normals of these hyperplanes form a root system.

The direction $W \to \Phi$ follows from everything that has been said so far. (Since we observed that the elements of the reflection groups permute the hyperplanes and the normals, and this lead to the definition of a root system.)

For the direction $\Phi \to W$, we need to consider, if we start with a finite root system, could we get an infinite group? We need to show that the reflections induced by the hyperplanes perpendicular to the roots α form a finite group. (Recall that the group is generated by finitely many reflections, including things which are not reflections. Are there infinitely many of these?)

Let $\phi : W \to S_k$ be the natural homomorphism from W into the symmetric group on Φ. Since only $w = 1$ fixes all of Φ (in particular, $s_\alpha \in W$ sends α to $-\alpha$), $\ker \Phi = 1$, so W is finite.

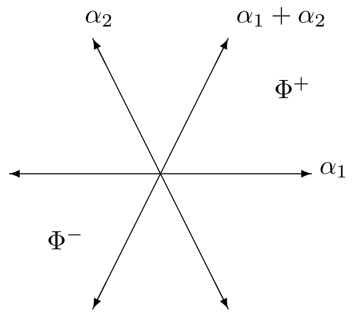
We have the remarkable fact each root system admits a decomposition into a positive and negative part,

$$\Phi = \Phi^+ \cup \Phi^-,$$

such that $\Phi^- = -\Phi^+$ and $\Phi^+ \cap \Phi^- = \emptyset$, where Φ^+ admits a unique basis (known as a *simple system* or *base*) $\Delta \subseteq \Phi^+$ such that for all $\beta \in \Phi^+$,

$$\beta = \sum_{\alpha \in \Delta} c_\alpha \alpha, \quad c_\alpha \geq 0.$$

(The key here is that the coefficients are all non-negative.) For example, in the root system



we have $\Delta = \{\alpha_1, \alpha_2\}$, $\Phi^- = -\Phi^+$.

Put formally,

Definition: Let Φ be a root system in V. $\Delta \subset \Phi$ is called a *simple system* (or base) if its elements are linearly independent (over $\mathbb{R}$), spans Φ, and each root $\beta \in \Phi$ can be written as

$$\beta = \sum_{\alpha \in \Delta} c_\alpha \alpha$$

with all $c_\alpha \geq 0$ or all $c_\alpha \leq 0$. Roots in Δ are called *simple roots*, and roots with positive/negative height are called positive/negative roots. Here, $\text{height}(\beta) = \text{ht}(\beta) = \sum_{\alpha \in \Delta} c_\alpha$. Roots with positive height form a set Φ^+, and roots with negative height form a set Φ^-.

It remains to be seen that every root system admits a simple system. (Assignment task.) We will look instead at simple consequences of the existence of a base.

Lemma 4. *Let $\Delta \subset \Phi$ be a base, and $\alpha, \beta \in \Delta$, $\alpha \neq \beta$. Then, $(\alpha, \beta) \leq 0$. (Then, angles between simple roots are $\frac{\pi}{2}$ or obtuse.)*

When we return to Coxeter groups, we will see that the distinction between $(\alpha, \beta) = 0$ and $(\alpha, \beta) < 0$ relates to whether or not α and β are connected in the Coxeter graph. (In particular, they are connected iff $(\alpha, \beta) < 0$.)

Proof of Lemma 4. Assume towards contradiction that $(\alpha, \beta) > 0$, i.e. $(\beta, \alpha^\vee) > 0$. Then,

$$s_\alpha(\beta) = \beta - (\beta, \alpha^\vee)\alpha = \beta - k\alpha,$$

for some $k > 0$. However, $s_\alpha(\beta) \in \Phi$, but its expression in terms of base elements contains positive and negative coefficients. Thus, $s_\alpha(\beta)$ is neither in Φ^+ nor in Φ^-. Contradiction. $\square$

Lemma 5. *Let $\Delta \subset \Phi$ be a base. Then, for $\alpha \in \Delta$, $s_\alpha(\Phi^+ \setminus \{\alpha\}) = \Phi^+ \setminus \{\alpha\}$.*

Note that clearly $s_\alpha(\alpha) - \alpha$, so the exclusion of α is necessary. In other words, Φ^+ and $s_\alpha(\Phi^+)$ differ in a simple root. This is also not true for reflections not corresponding to simple roots. For example, in A_2 above,

$$s_{\alpha_1}(\Phi^+) = \{-\alpha_1, \alpha_2, \alpha_1 + \alpha_2\}, \quad s_{\alpha_1+\alpha_2}(\Phi^+) = \Phi^-.$$

Proof of Lemma 5. Let $\beta \in \Phi^+ \setminus \{\alpha\}$. Then,

$$\begin{aligned} s_\alpha(\beta) &= \beta - (\beta, \alpha^\vee)\alpha \\ &= \sum_{\gamma \in \Delta, \gamma \neq \alpha} c_\gamma \gamma + k\alpha \quad (k \in \mathbb{R}, \text{ at least one } c_\gamma \neq 0), \end{aligned}$$

hence $s_\alpha(\beta) \notin \Phi^-$, so $s_\alpha(\beta) \in \Phi^+$. Since at least one $c_\gamma \neq 0$, $s_\beta(\alpha) \neq \alpha$. $\square$

2.3 Groups Generated by Simple Systems

Recall from last time the notion of a simple system $\Delta \subset \Phi$, Φ^+ the set of positive roots, and $\text{height}(\gamma) = \sum_{\alpha \in \Delta} c_\alpha$ where $\gamma = \sum_{\alpha \in \Delta} c_\alpha \alpha$. Recall also Lemmas 4, 5.

Lemma 6. *Let Δ and $\hat{\Delta}$ be simple systems with corresponding positive root sets Φ^+ and $\hat{\Phi}^+$, then $\hat{\Phi}^+ = w(\Phi^+)$ and $\hat{\Delta} = w(\Delta)$ for some $w \in \Phi$.*

Recall that when we fix Φ^+, then we have a unique simple system, so the statements $\hat{\Delta} = w(\Delta)$ and $\hat{\Phi}^+ = w(\Phi^+)$ are equivalent.

Note: clearly if Δ is a simple system then $s_\alpha(\Delta)$ is also simple: if $\beta = \sum_{\gamma \in \Delta} c_\gamma \gamma$ then

$$s_\alpha(\beta) = \sum_{\gamma \in \Delta} c_\gamma s_\alpha(\gamma) = \sum_{s_\alpha(\tau) \in \Delta} c_{s_\alpha(\tau)} \tau = \sum_{\tau \in s_\alpha(\Delta)} c_{s_\alpha(\tau)} \tau,$$

and since the coefficients $c_{s_\alpha(\tau)}$ have the same sign as c_γ, $s_\alpha(\beta)$ has the same sign in this new root system.

Hence, if Δ is simple with set of positive roots Φ^+, then $s_\alpha(\Delta)$ is simple with set of positive roots $s_\alpha(\Phi^+)$.

Proof of Lemma 6. We proceed by induction on $n = |\Phi^+ \cap \hat{\Phi}^-|$. If $n = 0$, then $\Phi^+ = \hat{\Phi}^+$ and $\Delta = \hat{\Delta}$, so we can take $w = 1$.

If statement is true for $0 \leq n \leq N - 1$, and suppose $|\Phi^+ \cap \hat{\Phi}^-| = N$. Then, $\Delta \not\subset \hat{\Phi}^+$, so there exists an $\alpha \in \Delta$ such that $\alpha \in \hat{\Phi}^-$. But then we can apply induction on $s_\alpha(\Phi^+)$ and $\hat{\Phi}^+$ since by Lemma 5, $s_\alpha(\Phi^+) = (\Phi^+ \setminus \{\alpha\}) \cup \{-\alpha\}$, so

$$\left| s_\alpha(\Phi^+) \cap \hat{\Phi}^- \right| = N - 1,$$

hence there exists a $v \in W$ such that $v(s_\alpha(\Phi^+)) = \hat{\Phi}^+$. Now take $w = v s_\alpha$. $\square$

Theorem 7. *Let W be a finite reflection group with simple system Δ. Then, W is generated by the simple reflections s_α, for $\alpha \in \Delta$.*

Proof. Let $V < W$ be the subgroup generated by the s_α, $\alpha \in \Delta$. The aim is to show that $V = W$ (by showing $W \subset V$). For $\beta \in \Phi^+$, let $\gamma \in V(\beta) \cap \Phi^+$ be of minimal height, where $V(\beta)$ is the V-orbit of β. Note that $\beta \in V(\beta) \cap \Phi^+$, so this set is indeed nonempty.

Then, we claim that $ht(\gamma) = 1$. To see this, write $\gamma = \sum_{\alpha \in \Delta} c_\alpha \alpha$. Then,

$$0 < (\gamma, \gamma) = ||\gamma||^2 = \sum_{\alpha \in \Delta} c_\alpha (\alpha, \gamma),$$

so that $(\gamma, \alpha^\vee) > 0$ for some $\alpha \in \Delta$. Now, assume towards contradiction that $ht(\gamma) > 1$. Then, $s_\alpha(\gamma) \in \Phi^+$ (by Lemma 5 and the fact that $\gamma \neq \alpha$). Also note that $s_\alpha(\gamma) = V(\beta)$ as $s_\alpha \in V$ and $\gamma \in V(\beta)$. But, $s_\alpha(\gamma) = \gamma - (\gamma, \alpha^\vee)\alpha$ so that $ht(s_\alpha(\gamma)) < ht(\gamma)$, contradicting minimality.

In other words, the V-orbit of $\beta \in \Phi^+$ contains a simple root $\alpha \in \Delta$. Hence, if we consider the above for β simple, we see $\Phi^+ \subset V(\Delta)$.

Similarly for $\beta \in \Phi^-$ there exists a $v \in V$ such that $-\beta = v(\alpha)$ for some $\alpha \in \Delta$, then $\beta = (vs_\alpha)(\alpha)$ so that $\Phi^- \subset V(\Delta)$. Therefore, $\Phi \subset V(\Delta)$.

To complete the proof, let s_γ be a generator of W. By above, $\gamma = v(\alpha)$ by some $v \in V$ and $\alpha \in \Delta$. Recall from Corollary 2 that $s_{v(\alpha)} \in V$ if $s_\alpha \in V$. Hence, $s_\gamma \in V$, so $V = W$. □

Now, for a simple system Δ, the group generated by $s_{\alpha_1}, \ldots, s_{\alpha_r}$ has the relations $s_\alpha^2 = 1$, $(s_\alpha, s_\beta)^{m_{\alpha,\beta}} = 1$, where $m_{\alpha,\beta} = m_{\beta,\alpha}$, so these relations look like those for a Coxeter group. It remains to show that there are no other relations within this group.

2.4 Reduced Words and Word Length

2.4.1 Linear Algebra Intermezzo

Let $g \in O(V)$. Then, g viewed as a linear transformation on V has determinant ± 1; transformations with determinant 1 are orientation preserving (e.g. rotations), and reflections correspond to determinant -1.

Recall that a matrix is orthogonal iff its columns form an orthonormal basis, or equivalently, $A^{-1} = A^t$. If this is the case, then $\det(AA^t) = \det(A)^2 = 1$, so $\det(A) = \pm 1$. Similarly, we could also define $A^* = A^{-1}$, where A^* is the adjoint matrix.

2.4.2 Reduced Words and Word Length

Definition: Let W be a finite reflection group generated by a simple system Δ. We say that a word $w = s_1 s_2 \ldots s_r \in W$ (where s_i are simple reflections) is *reduced* if there does not exist a shorter word in the generators representing w.[1] If $w = s_1 \ldots s_r$ is reduced, then the *length* of w, denoted $l(w)$, is r. By definition, $l(1) = 0$.

For example, in $A_2 = \langle s, t \mid s^2 = t^2 = 1, sts = tst \rangle$, we know that there are six words,

[1] There may be multiple words of shortest length.

$$
\begin{array}{ll}
\text{length:} & \\
0 & \begin{tikzcd}[column sep=small] & 1 \arrow[dl, dash] \arrow[dr, dash] & \\ s \arrow[d, dash] & & t \arrow[d, dash] \\ ts \arrow[dr, dash] & & st \arrow[dl, dash] \\ & sts(=tst) & \end{tikzcd} \\
1 & \\
2 & \\
3 & \\
\vdots &
\end{array}
$$

This is an example of a 'Strong Bruhat graph' (we may not have time to cover these in the course).

Some simple facts about the length function:

- $l(w) = 1$ iff w is a simple reflection.
- $l(w^{-1}) = l(w)$, since if $w = s_1 \dots s_r$, $w^{-1} = s_r \dots s_1$.
- $\det(w) = (-1)^{l(w)}$, since if $w = s_1 \dots s_r$ then $\det(w) = \det(s_1) \dots \det(s_r) = (-1)^r$.
- $|l(s_\alpha w) - l(w)| = 1$, we can see this in the example above.

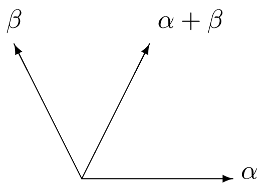
If $w = s_1 \dots s_r$ is reduced, can we have that $s_\alpha s_1 \dots s_l = 1$ for some l with $1 < l < r$, and so $s_\alpha s_1 \dots s_r$ is a lot shorter? If this were the case, then

$$w = s_\alpha^2 \dots s_r = s_\alpha(s_\alpha s_1 \dots s_l) s_{l+1} \dots s_r = s_\alpha s_{l+1} \dots s_r,$$

so $l(w) \leq l(w) - l + 1$, so $l = 1$ and $s_1 = s_\alpha$. So no, prepending a reduced word with a simple reflection will cancel out at most the first simple reflection of the word.

Let $\Phi^+(w) = \Phi^+ \cap w^{-1}(\Phi^-)$, that is, the set of positive roots which are sent to negative roots by the action w; and let $n(w) = |\Phi^+(w)|$. We aim to show that $n(w) = l(w)$.

In the familiar example of A_2, we have



$$
\begin{aligned}
\Phi^+(1) &= \Phi^+, \\
\Phi^+(s_\alpha) &= \{\alpha\}, \\
\Phi^+(s_\beta) &= \{\beta\}, \\
\Phi^+(s_\alpha s_\beta) &= \{\beta, \alpha + \beta\}, \\
\Phi^+(s_\beta s_\alpha) &= \{\alpha, \alpha + \beta\}, \\
\Phi^+(s_\alpha s_\beta s_\alpha) &= \Phi^+.
\end{aligned}
$$

Claim: $n(w) = n(w^{-1})$:

$$\Phi^+(w) = w^{-1} w \left(\Phi^+ \cap w^{-1}(\Phi^-)\right) = w^{-1}\left(w(\Phi^+) \cap \Phi^-\right) = -w^{-1}\left(w(\Phi^-) \cap \Phi^+\right) = -w^{-1}\left(\Phi^+(w^{-1})\right),$$

and since $-w^{-1}$ is a bijection, the cardinalities of $\Phi^+(w)$ and $\Phi^-(w^{-1})$ are the same. $\square$

Proposition 8. *Given $\alpha \in \Delta$ and $w \in W$, if $w(\alpha) \in \Phi^{\pm}$ then $n(ws_\alpha) = n(w) \pm 1$ – i.e. $n(w)+1$ if $w(\alpha) \in \Phi^+$ and $n(w)-1$ if $w(\alpha) \in \Phi^-$.*

Before proving this we note that equivalently, if $w^{-1}(\alpha) \in \Phi^{\pm}$ then $n(s_\alpha w) = n(w) \pm 1$. Indeed, $n((s_\alpha w)^{-1}) = n(w^{-1}s_\alpha) = n(w^{-1}) \pm 1$, so $n(s_\alpha w) = n(w) \pm 1$ by above.

Proof. If $w(\alpha) \in \Phi^-$, then $\alpha \in \Phi^+(w)$ in which case $\Phi^+(ws_\alpha) = \Phi^+(w) \setminus \{\alpha\}$ so that $n(ws_\alpha) = n(w) - 1$.

Similarly, if $w(\alpha) \in \Phi^+$, then $\alpha \notin \Phi^+(w)$, in which case $\Phi^+(ws_\alpha) = \Phi^+(w) \cup \{\alpha\}$ so that $n(ws_\alpha) = n(w) + 1$. □

2.5 Proof that $l(w) = n(w)$

Lemma 9. *Let $w \in W$. We have $n(w) \leq l(w)$.*

Proof. Let w admit the reduced expression $w = s_1 \dots s_r$ so that $l(w) = r$. But $n(s_1 \dots s_{r-1}s_r) = n(s_1 \dots s_{r-1}) \pm 1$ so that $n(w)$ is at most r. (Remember that $n(1) = 0$ and $n(s_i) = 1$.) □

We of course want to show that $n(w) = l(w)$. This will lead to the *deletion* and *exchange conditions.*

Given a word $w = s_1 s_2 \dots s_i \dots s_k$, write $s_1 \dots \hat{s_i} \dots s_k$ for the word $s_1 \dots s_{i-1}s_{i+1} \dots s_k$. For example, $s_1 s_2 \hat{s_1} s_2 s_3 = s_1 s_2^2 s_3 = s_1 s_3$.

Theorem 10 (Deletion condition)**.** *Let $w = s_1 \dots s_k$, for s_i simple reflections (w.r.t. some simple system), such that $n(w) < k$. Then there exists $1 \leq i < j \leq k$ such that*

(1) $s_i \dots s_{j-1} = s_{i+1} \dots s_j$

(2) $w = s_1 \dots \hat{s_i} \dots \hat{s_j} \dots s_k$

For example, in A_2 with $\Delta = \{\alpha, \beta\}$, write $s_\alpha = s$, $s_\beta = t$, and let $w = stst (= ts)$. (Note that $n(w) = 2 < 4$). Now, $w = (sts)t = s(tst)$, where $(sts) = (tst)$, and $w = (s)ts(t) = ts$.

Proof of Theroem 10. Warning: We will "identify" s_i with s_{α_i} for $\alpha_i \in \Delta$, meaning nothing more than that s_i is the simple reflection wrt some root we will denote by α_i. The subscripts of α should not be interpreted as a labelling of the simple roots.

According to Proposition 8, if $w(\alpha) \in \Phi^+$ then $n(ws_\alpha) = n(w) + 1$. Hence if $s_1(\alpha_2) \in \Phi^+$ then $n(s_1 s_2) = n(s_1) + 1 = 2$. Then, if it also holds that $s_1 s_2(\alpha_3) \in \Phi^+$, then $n(s_1 s_2 s_3) = n(s_1 s_2) + 1 = 3$, and so on. If this continues to s_k, it would hold that $n(s_1 \dots s_k) = k$.

Since $n(w) < k$, this must break at some point, so that there exists a $2 \leq j \leq k$ so that

$$s_1 \dots s_{j-1}(\alpha_j) \in \Phi^-.$$

But $1(\alpha_j) \in \Phi^+$, and if $s_{j-1} \neq s_j$ then $s_{j-1}(\alpha_j) \in \Phi^+$, so $n(s_{j-1}s_j) = 2$, etc.

So, there must be an $i < j$ so that

$$s_{i+1} \dots s_{j-1}(\alpha_j) \in \Phi^+ \quad \text{and} \quad s_i s_{i+1} \dots s_{j-1}(\alpha_j) \in \Phi^-.$$

This means that s_i maps $\lambda = s_{i+1} \dots s_{j-1}(\alpha_j)$ from Φ^+ to Φ^-, hence $\lambda = \alpha_i$ (by Lemma 5). We can summarise this as $\alpha_i = w(\alpha_j)$, $w = s_{i+1} \dots s_{j-1}$ for some $1 \leq i < j \leq k$).

By Lemma 1, $ws_{\alpha_j}w^{-1} = s_{w(\alpha_j)} = s_{\alpha_i} = s_i$, hence $ws_j = s_i w$. This is result (1).

(2) is essentially equivalent to (1):

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

$$\implies w = s_1 \dots s_k = s_1 \dots s_{i-1}(s_{i+1} \dots s_{j-1})s_{j+1} \dots s_k.$$

□

Theorem 11. *We have $l(w) = n(w)$.*

i.e. the length of w is the number of positive roots which are mapped to negative roots by w.

Proof. We already know that $n(w) \leq l(w)$. Let $w = s_1 \dots s_r$ be reduced. Assume that $n(w) < r$, then by Theorem 10, we can delete two letters from w, a contradiction. □

Note that as a consequence of Theorem 10, words with different parity cannot be equal.

2.6 Construction of $\Phi^+(w)$, Exchange Condition

Note that Theorem 10 can be restated as "Let $w = s_1 \dots s_k$ (s_i simple) such that w is not reduced. Then there exists ...".

Proposition 12. *Let $w = s_1 \dots s_r$ be reduced. Then, $\Phi^+(w) = \{s_r \dots s_{i+1}(\alpha_i) \mid 1 \leq i \leq r\}$.*

For example, in A_2 with simple roots $s = s_\alpha, t = s_\beta$,

- For $w = 1$, $\Phi^+(w) = \emptyset$,
- For $w = s$, $\Phi^+(w) = \{\alpha\}$,
- For $w = t$, $\Phi^+(w) = \{\beta\}$,
- For $w = ts = ts \cdot 1$, we have $1(\alpha) = \alpha$ and $s(\beta) = \alpha + \beta$, so $\Phi^+(w) = \{\alpha, \alpha + \beta\}$,
- For $w = st$, we have $1(\beta) = \beta$ and $t(\alpha) = \alpha + \beta$, so $\Phi^+(w) = \{\beta, \alpha + \beta\}$,
- For $w = sts$, we have $1(\alpha) = \alpha$, $s(\beta) = \alpha + \beta$, and $st(\alpha) = \beta$, so $\Phi^+(w) = \{\alpha, \alpha + \beta, \beta\}$.

Proof of Proposition 12. Since $n(w) = l(w) = r$, if we can show that

$$\Phi^+(w) \subseteq \{s_r \dots s_{i+1}(\alpha_i) \mid 1 \leq i \leq r\},$$

then we are done.

Let $\gamma \in \Phi^+(w)$, i.e. $\gamma \in \Phi^+$ and $w(\gamma) \in \Phi^-$. Hence there exists an $i \leq r$ such that

$$\lambda = s_{i+1} \dots s_r(\gamma) \in \Phi^+ \quad \text{but} \quad s_i(\lambda) = s_i \dots s_r(\gamma) \in \Phi^-.$$

Hence, $\lambda = \alpha_i = s_{i+1} \dots s_r(\gamma)$, hence $\gamma = s_r \dots s_{i+1}(\alpha_i)$. □

Theorem 13 (Exchange condition)**.** *Let $w = s_1 \dots s_k$. If $l(ws) < l(w)$ then there exists an i such that $w = s_1 \dots \hat{s}_i \dots s_k s$.*

For example, in A_2, consider the word $w = stst$. We know that $w = ts$, $l(w) = 2$. Now, $ws = ststs (= sttst = t)$, so $l(ws) = 1$. Then, $w = s\hat{t}sts = s^2ts = ts$.

Proof of Theorem 13. Let $w = s_1 \dots s_k$ where $l(ws) < l(w) = n(w)$. By Proposition 8, $w(\alpha) \in \Phi^-$ (where $s = s_\alpha$), so that there must exist an i such that $\lambda := s_{i+1} \dots s_k(\alpha) \in \Phi^+$ but $s_i(\lambda) \in \Phi^-$, so $\lambda = \alpha_i = s_{i+1} \dots s_k(\alpha)$.

Recall $ws_\alpha w^{-1} = s_{w(\alpha)}$, so

$$s_{i+1} \dots s_k \cdot s \cdot s_k \dots s_{i+1} = s_{\alpha_i} = s_i.$$

Then,

$$ws \cdot s_k \dots s_{i+1} = s_1 \dots s_i s_{i+1} \dots s_k \cdot s \cdot s_k \dots s_{i+1} = s_1 \dots s_{i-1},$$

so

$$w = s_1 \dots s_{i-1} s_{i+1} \dots s_k s.$$

□

We now state the main theorem:

Theorem 14. *Every finite reflection group W is a Coxeter group.*

The issue to consider is the following question: Is it possible to have a relation $s_1 s_2 \dots s_k = 1$ that cannot be derived from the relations $(s_\alpha s_\beta)^{m_{\alpha\beta}} = 1$?

2.7 Finite Reflection Groups are Coxeter Groups

Proof of Theorem 14. We can fix a simple system Δ such that $W = \langle s_\alpha, \alpha \in \Delta \mid \text{“relations”} \rangle$. We know that $s_\alpha s_\beta$ must have finite order, say $m_{\alpha,\beta}$, so

$$(s_\alpha s_\beta)^{m_{\alpha,\beta}} = 1. \qquad (*)$$

Since we know s_α is an involution (i.e. $s_\alpha^2 = 1$), we have $m_{\alpha,\beta} = m_{\beta,\alpha}$. We need to prove that any relation in W follows from $(*)$.

We begin by noting that any relation may be written as $s_1 \dots s_k = 1$ (indeed, if $s_1 \dots s_i = s_k \dots s_{i+1}$, then this is equivalent to $s_1 \dots s_k = 1$).

Now let (R) stand for the relation $s_1 \dots s_k = 1$ (where s_i are simple reflections). Taking the determinant on either side gives $(-1)^k = 1$, so k is even.

We will proceed by induction on k. For $k = 0$ we get a tautology. For $k = 2$ we get $s_1 s_2 = 1$, so $s_2 = s_1^{-1} = s_1$, so the only relations on two letters are simply that $s_\alpha^2 = 1$.

Now assume $k \geq 4$ and define $\kappa = \frac{k}{2}$. Then (R) can be written as

$$\underbrace{(s_1 \dots s_{\kappa+1})}_{\kappa+1 \text{ letters}} \underbrace{(s_{\kappa+2} \dots s_{2\kappa})}_{\kappa-1 \text{ letters}} = 1,$$

which is equivalent to

$$s_1 \dots s_{\kappa+1} = s_{2\kappa} \dots s_{\kappa+2}.$$

The length of the word on the right is at most $\kappa - 1$ so that the word on the left is *not* reduced. Hence we can apply the deletion condition (Theorem 10), so there exists a pair of indices $1 \leq i < j \leq \kappa+1$ such that

$$s_i \dots s_{j-1} = s_{i+1} \dots s_j, \quad \text{i.e.} \quad s_i \dots s_{j-1} s_j \dots s_{i+1} = 1.$$

The word on the left has $2j - 2i$ letters and $2 \leq 2(j-i) \leq 2\kappa = k$.

Case 1: If $2j - 2i < k$, then $s_i \dots s_{j-1} s_j \dots s_{i+1} = 1$ follows from $(*)$ (by the induction hypothesis), hence (R) can be written as

$$1 = s_1 \dots s_k = s_1 \dots s_i s_{i+1} \dots s_j s_{j+1} \dots s_k = s_1 \dots s_i s_i \dots s_{j-1} s_{j+1} \dots s_k = s_1 \dots \hat{s_i} \dots \hat{s_j} \dots s_k.$$

By induction this follows from $(*)$.

Case 2: $2j - 2i = k$, i.e. $i = 1$, $j = \kappa + 1$. In this case we must have $s_1 \dots s_\kappa = s_2 \dots s_{\kappa+1}$. Write (R) as $s_2 \dots s_k s_1 = 1$ (left-multiply and right-multiply both sides by s_1) and repeat the same steps as before. Again, there are two cases to consider, Case 2^1 and 2^2, and again we are done in case 2^1 and stuck in case 2^2 for which $s_2 \dots s_{\kappa+1} = s_3 \dots s_{\kappa+2}$.

Again, repeat the procedure, now on (R) written as $s_3 \dots s_k s_1 s_2 = 1$; we are stuck in the case of 2^{2^2} for which we get $s_3 \dots s_{\kappa+2} = s_4 \dots s_{\kappa+3}$.

Continuing, we end up with the system of relations:

$$\begin{aligned}
s_1 \dots s_{2\kappa} &= 1 && (R)\\
s_1 \dots s_\kappa &= s_2 \dots s_{\kappa+1} && (1 \; **)\\
s_2 \dots s_{\kappa+1} &= s_3 \dots s_{\kappa+2} && (2 \; **)\\
&\dots\\
s_i \dots s_{\kappa+i-1} &= s_{i+1} \dots s_{\kappa+i} && (i \; **)\\
&\dots\\
s_\kappa \dots s_{2\kappa-1} &= s_{\kappa+1} \dots s_{2\kappa} && (\kappa \; **)
\end{aligned}$$

Note the relation $s_i \dots s_{\kappa+i-1} = s_{i+1} \dots s_{\kappa+i}$ arises from $s_i \dots s_{2\kappa} s_1 \dots s_{i+1} = 1$, where $s_i \dots s_{2\kappa}$ has $2\kappa - i + 1$ letters, so we must have $\kappa + 1 \leq 2\kappa - i + 1$, so $i \leq \kappa$.

The case (i) can be written as

$$s_{i+1} = s_i \dots s_{\kappa+i-1} s_{\kappa+i} \dots s_{i+2},$$

or as

$$s_{i+1} s_i \dots s_{\kappa+i-1} s_{\kappa+i} \dots s_{i+2} = 1 \qquad (\hat{\imath})$$

(We continue the proof in the next lecture.)

Note: Lectures 13-15 haven't been cleaned up (there are still bits missing, and graphs I need to draw). You can see the current untidy version at `https://github.com/jgat/math4301-notes`.

A Version History

Below we describe briefly the version history of this document, based on versions which have been published at `http://jgat.github.io/math4301-notes/lectures.pdf`. Version numbers will roughly follow the format v0.n.m, where n indicates the number of lectures which notes have been written for, and m indicates the number of minor revisions. Once notes have been taken for all lectures, the version number will increment to v1.0.

v0.3.0: Initial publication with lectures 1 to 3, §1.1-1.3.

v0.4.0: Lecture 4 placeholder.

v0.7.0: Lectures 5-7. (Still haven't drawn some pictures).

v0.8.0: Lecture 8.

v0.8.1: Touching up some of lecture 5.

v0.11.0: Through to Lecture 11.

v0.11.1: Formatting, and a basic diagram of A_2 from lecture 5.

v0.12.0: Lecture 12 (First part of proof of Theorem 14).

v0.12.1: Links to Lecture 4 pictures.