1 Preliminaries

Denote by W a multiplicative group generated by a set S where $S = S^{-1}$ and $1 \notin S$. This means every element of W is the product of a finite sequence of elements from S.

Definition 1.1 Length and reduced decomposition

For $w \in W$ define the length of w (denoted by $l_S(w)$ or just $l(w)$ when S is known) to be the smallest integer $q \geq 0$ such that w is the product of a sequence of q elements of S. Such a sequence is called a reduced decomposition of w.

Definition 1.2 The Cayley graph

The Cayley graph of W is the graph with vertex set W and edge set given by $x \to y \in E \iff l(xy^{-1}) = 1 \iff xy^{-1} \in S$. As $S = S^{-1}$ and $1 \notin S$ the Cayley graph is a simple undirected graph.

On any simple undirected graph there is a natural metric given by $d(x, y)$ is the length of the shortest xy-path in G. The following result relates this metric to the length.

Lemma 1.3 Lengths and the Cayley graph

$s_1 s_2 \ldots s_q$ is a reduced decomposition for xy^{-1} if and only if $y \to s_q y \to s_{q-1} s_q y \cdots \to xy$ is a shortest xy-path in G.

Proof: If there was a shorter xy-path in G it would define a sequence shorter than the reduced decomposition which is a contradiction.
Moreover, if $s_1 s_2 \ldots s_q$ was not a reduced decomposition for xy^{-1} then there would be a shorter sequence and this would define a shorter xy-path. $\square$

As a corollary to this it is clear that $d(x, y) = l(xy^{-1})$.

Proposition 1.4 Properties of the length

(i) $l(x) = 0 \iff x = 1$ *and* $l(x) = 1 \iff x \in S$

(ii) $l(x) = l(x^{-1})$

(iii) $l(w) + l(w') \geq l(ww')$

(iv) $|l(w) - l(w')| \leq l(ww')$

Proof: The proof is given by using the metric extensively. Each result can be proved just as easily using reduced decompositions directly as is done in the Bourbaki text.

(i) $d(x,y)=0 \iff x=y$ which implies that $l(xy^{-1})=0 \iff x=y$ and setting $y=1$ gives $l(x)=0 \iff x=1$. Also, $l(x)=1 \iff d(x,1)=1 \iff x\in S$.

(ii) $l(xy^{-1})=d(x,y)=d(y,x)=l(yx^{-1})$, setting $y=1$ gives $l(x)=l(x^{-1})$.

(iii) By the triangle inequality $l(xy^{-1})+l(yz^{-1})\geq l(xz^{-1})$. Setting $w=xy^{-1}$ and $w'=yz^{-1}$ gives $l(w)+l(w')\geq l(ww')$.

(iv) Switch the variables in (iii) twice.

2 Coxeter systems

Definition 2.1 Coxeter systems

Let W be a group generated by a set of involutions S. Let $m(s_i,s_j)$ be the order of s_is_j and let I be the set of all pairs (i,j) such that $m(s_i,s_j)$ is finite. (W,S) is called a Coxeter system if it satisfies the following property.

If G is a group and $f:S\rightarrow G$ satisfies $(f(s_i)f(s_j))^{m(s_i,s_j)}=1$ for all $(i,j)\in I$, then there exists a homomorphism $g:W\rightarrow G$ extending f.

When (W,S) is a Coxeter system, W is called a Coxeter group.

This property is equivalent to the following.

Let W' be a group, $f:W'\rightarrow W$ a homomorphism and $h:S\rightarrow W'$ a map such that $f(h(s)=s$, $(h(s_i)h(s_j))^{m(s_i,s_j)}=1$ for all $(i,j)\in I$ and $h(S)$ generates W'. Then f is an isomorphism.

Definition 2.2 Signature map

Let (W,S) be a Coxeter system and $\varepsilon':S\rightarrow\{-1,1\}$ given by $\varepsilon'(s)=-1$. This extends to a homomorphism $\varepsilon(w)$ which is called the signature of w.

The homomorphism rule $\varepsilon(ww')=\varepsilon(w)\varepsilon(w')$ gives the result

$$l(w)+l(w')\equiv l(ww') \mod 2$$

Proposition 2.3 Conjugacy in Coxeter groups

Let (W,S) be a Coxeter system and let $s,s'\in S$.
s is conjugate to s' if and only if (†) there is a finite sequence $s_1\dots s_q$ of elements from S such that $s_1=s, s_q=s'$ and the order of s_js_{j+1} is finite and odd for all j such that $1\leq j<q$.

Proof: Suppose $s, s' \in S$ are such that ss' has finite order $2n+1$. Then, by definition $(ss')^{2n+1} = 1$. This can be simply rearranged to give $s(s's)^n = (ss')^n s$ and hence $(ss')^n s(s's)^n = (ss')^n(ss')^n s = (s's)s = s'$ so s, s' are conjugate in S, as $[(ss')^n]^{-1} = (s's)^n$.

Conversely, for all $s \in S$ let A_s be the set of all $s' \in S$ satisfying (†). By hypothesis the elements s_j, s_{j+1} are conjugate for all $1 \leq j < q$.
Let f be the map from S to $M = \{-1, 1\}$ such that $f(A_s) = \{1\}$ and $f(w) = -1$ otherwise. Let $s', s'' \in S$ be such that $s's''$ is of finite order m. Then $(f(s')f(s''))^{m(s_i,s_j)} = 1$ as $f(s')f(s'') = 1$ if $s'), s''$ both lie in A_s or both lie in $S \setminus A_s$. If one lies in each then m must be even, so the claim holds. (If m was odd then we would deduce that both $s', s'' \in A_s$.)
Hence, as (W, S) is a Coxeter system f can be extended to a homomorphism $g : W \to M$ extending f. By definition $\ker g \cap S = A_s$ and as it is a normal subgroup which contains s it must contain all conjugates of s in S. ☐

3 Dihedral groups

Definition 3.1 Dihedral groups

A dihedral group is a group generated by two distinct involutions.

Let W_m be the dihedral group generated by involutions, $S = \{s, s'\}$ where $m \in \{2, 3 \dots\} \cup \{\infty\}$ is the order of ss'. Any element of W_m can be written as a product of a finite sequence in S. If any two consecutive terms of this sequence were the same then they would cancel, thus any element can be written as a the product of a finite alternating sequence from S.

The more common geometric definition of a dihedral group is the group of distance preserving permutations of the vertices of a regular m-gon, in other words all distance preserving permutations of the set $\{(r, \theta) \in \mathbb{R}^2 : r = 1, \theta = \frac{2\pi k}{m}\}$ when m is finite or of $mathbbZ$ when $m = \infty$. This definition of a dihedral group will be denoted by D_m. The next result shows these two definitions are equivalent.

Proposition 3.2 Dihedral groups

For each m, $W_m \cong D_m$.

Proof: In this proof $ref_{\theta=a}$ denotes reflection in the line $\theta = a$ in 2d polar coordinates and $ref_{y=a}$ denotes reflection in the line $y = a$ in 2d cartesian coordinates.

Firstly we deal with the case when m is finite. Note first that $|W_m| = |D_m| =$

$2m$. To see this consider the set of all $4m-1$ alternating products of length $< 2m$ (any longer alternating sequence will cancel). By uniqueness of inverses each non-zero element of this list is repeated, so $|W_m| = 2m$. (At this point it is useful to note that these two sequences always have opposite first terms and opposite last terms.)

Define a function $\phi : W_m \to D_m$ by $\phi(s) = ref_{\theta=\frac{\pi}{m}}$ and $\phi(s') = ref_{\theta=0}$. Note that $\phi(s), \phi(s')$ generate D_m so ϕ is an epimorphism. Moreover, as $|W_m| = |D_m|, \phi$ is injective.

If $m = \infty$ then define $\phi : W_\infty \to D_\infty$ by $\phi(s) = ref_{y=\frac{1}{2}}$ and $\phi(s') = ref_{y=0}$. Again, $\phi(s), \phi(s')$ generate D_∞ so ϕ is an epimorphism.
Consider any alternating sequence from $\phi(s), \phi(s')$. If it has odd length then its product is a reflection, so never equal to $1 = rot_0$. If the length is even then its product is a horizontal translation by some non-zero integer. Hence $\ker(\phi) = \{1\}$. $\square$

Theorem 3.3 *W_m is a Coxeter group for all m.*

Proof: $m = \infty$:

If G is a group such that $f : S \to G$ then as $I = \{(s,s),(s',s')\}$, we deduce that $f(s), f(s')$ are involutions in G. Moreover $< f(s), f(s') >$ is a subgroup of G, hence the natural extension of f is a homomorphism from W_m to G.

$m < \infty$:

Let f be such that $f : S \to G$ and $f(s)^2 = f(s')^2 = (f(s)f(s'))^m = 1$, then the natural extension $g : W_m \to G$ is a homomorphism. Note that if $x, y \in W_m$ then we can pick an alternating sequence $(\dots, s', s)$ whose product is x and another sequence $(s', s, \dots)$ whose product is y. Then $g(xy) = g((\dots, s)(s', \dots)) = (\dots f(s))(f(s')\dots) = g(x)g(y)$. $\square$